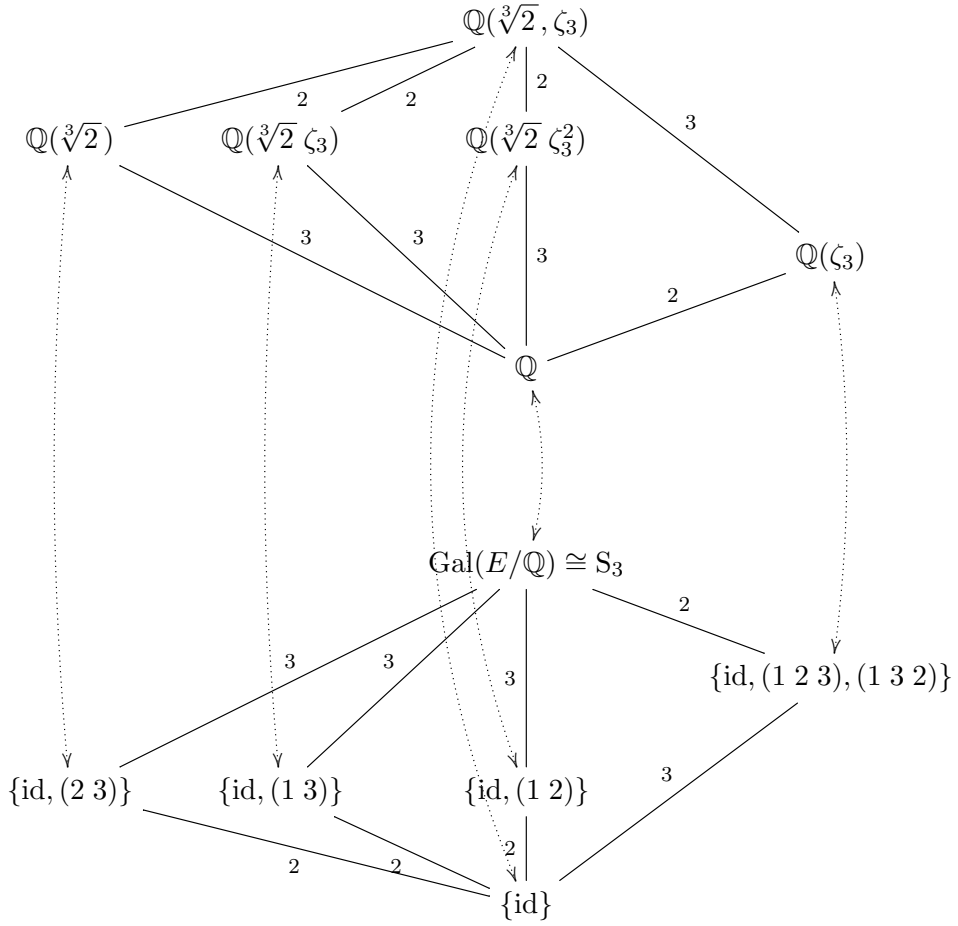
# An Introduction to Galois Theory

Andrew Baker



School of Mathematics & Statistics, University of Glasgow.
*Email address*: a.baker@maths.gla.ac.uk
*URL*: http://www.maths.gla.ac.uk/∼ajb




The Galois Correspondence for $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

## Introduction: What is Galois Theory?

Much of early algebra centred around the search for explicit formulae for roots of polynomial equations in one or more unknowns. The solution of linear and quadratic equations in a single unknown was well understood in antiquity, while formulae for the roots of general real cubics and quartics was solved by the 16th century. These solutions involved complex numbers rather than just real numbers. By the early 19th century no general solution of a general polynomial equation 'by radicals' (*i.e.*, by repeatedly taking $n$-th roots for various $n$) was found despite considerable effort by many outstanding mathematicians. Eventually, the work of Abel and Galois led to a satisfactory framework for fully understanding this problem and the realization that the general polynomial equation of degree at least 5 could not always be solved by radicals. At a more profound level, the algebraic structure of *Galois extensions* is mirrored in the subgroups of their *Galois groups*, which allows the application of group theoretic ideas to the study of fields. This *Galois Correspondence* is a powerful idea which can be generalized to apply to such diverse topics as ring theory, algebraic number theory, algebraic geometry, differential equations and algebraic topology. Because of this, Galois theory in its many manifestations is a central topic in modern mathematics.

In this course we will focus on the following topics.

- The solution of polynomial equations over a field, including relationships between roots, methods of solutions and location of roots.
- The structure of finite and algebraic extensions of fields and their automorphisms.

We will study these in detail, building up a theory of algebraic extensions of fields and their automorphism groups and applying it to solve questions about roots of polynomial equations. The techniques we will meet can also be applied to study the following some of which may be met by people studying more advanced courses.

- Classic topics such as *squaring the circle*, *duplication of the cube*, *constructible numbers* and *constructible polygons*.
- Applications of Galois theoretic ideas in Number Theory, the study of differential equations and Algebraic Geometry.

There are many good introductory books on Galois Theory, some of which are listed in the Bibliography. In particular, [**2, 3, 8**] are all excellent sources and have many similarities to the present approach to the material.

# Contents

CHAPTER 1

# Integral domains, fields and polynomial rings

### Basic notions, convention, etc

In these notes, a *ring* will always be a unital ring, *i.e.*, a ring with unity $1 \neq 0$. Most of the rings encountered will also be *commutative*. An *ideal* $I \lhd R$ will always mean a two-sided ideal. An ideal $I \lhd R$ in a ring $R$ is *proper* if $I \neq R$, or equivalently if $I \subsetneq R$. Under a ring homomorphism $\varphi\colon R \longrightarrow S$, $1 \in R$ is sent to $1 \in S$, *i.e.*, $\varphi(1) = 1$.

1.1. Definition. Let $\varphi\colon R \longrightarrow S$ be a ring homomorphism.

- $\varphi$ is a *monomorphism* if it is injective, *i.e.*, if for $r_1, r_2 \in R$,
$$\varphi(r_1) = \varphi(r_2) \quad \Longrightarrow \quad r_1 = r_2,$$
or equivalently if $\ker \varphi = \{0\}$.
- $\varphi$ is an *epimorphism* if it is surjective, *i.e.*, if for every $s \in S$ there is an $r \in R$ with $\varphi(r) = s$.
- $\varphi$ is an *isomorphism* if it is both a monomorphism and an epimorphism, *i.e.*, if it is invertible (in which case its inverse is also an isomorphism).

## 1.1. Recollections on integral domains and fields

The material in this section is standard and most of it should be familiar. Details may be found in [**3, 5**] or other books containing introductory ring theory. First we recall some important properties of elements in a ring.

1.2. Definition. Let $R$ be a ring. An element $u \in R$ is a *unit* if it is *invertible*, *i.e.*, there is an element $v \in R$ for which
$$uv = 1 = vu.$$
We usually write $u^{-1}$ for this element $v$, which is necessarily unique and is called the (*multiplicative*) *inverse* of $u$ in $R$. We will denote the set of all invertible elements of $R$ by $R^\times$ and note that it always forms a group under multiplication.

1.3. Definition. Let $R$ be a commutative ring. Then a non-zero element $z \in R$ is a *zero-divisor* if there is a non-zero element $w \in R$ for which
$$zw = wz = 0.$$
A commutative ring $R$ in which there are no zero-divisors is called an *integral domain* or an *entire ring*. This means that for $u, v \in R$,
$$uv = 0 \quad \Longrightarrow \quad u = 0 \text{ or } v = 0.$$

1.4. Example. The following rings are integral domains.

(i) The ring of integers, $\mathbb{Z}$.

(ii) If $p$ is a prime, the ring of integers modulo $p$, $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/(p)$.
(iii) The rings of rational numbers, $\mathbb{Q}$, real numbers, $\mathbb{R}$, and complex numbers, $\mathbb{C}$.
(iv) The polynomial ring $R[X]$, where $R$ is an integral domain; in particular, the polynomial rings $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$ are all integral domains.

1.5. Definition. Let $I \lhd R$ be a proper ideal in a commutative ring $R$.

- $I$ is a *prime ideal* if for $u, v \in R$,

$$uv \in I \quad \Longrightarrow \quad u \in I \text{ or } v \in I.$$

- $I$ is a *maximal ideal* $R$ if whenever $J \lhd R$ is a proper ideal and $I \subseteq J$ then $J = I$.
- $I \lhd R$ is *principal* if

$$I = (p) = \{rp : r \in R\}$$

for some $p \in R$. Notice that if $p, q \in R$, then $(q) = (p)$ if and only if $q = up$ for some unit $u \in R$. We also write $p \mid x$ if $x \in (p)$.
- $p \in R$ is *prime* (or is *a prime*) if $(p) \lhd R$ is a prime ideal; this is equivalent to the requirement that whenever $p \mid xy$ with $x, y \in R$ then $p \mid x$ or $p \mid y$.
- $R$ is a *principal ideal domain* if it is an integral domain and every ideal $I \lhd R$ is principal.
- A non-zero element $p \in R$ is *irreducible* (or is *an irreducible*) if for $u, v \in R$,

$$p = uv \quad \Longrightarrow \quad u \text{ or } v \text{ is a unit.}$$

1.6. Example. Every ideal $I \lhd \mathbb{Z}$ is principal, so $I = (n)$ for some $n \in \mathbb{Z}$ which we can always take to be non-negative, *i.e.*, $n \geqslant 0$. Hence $\mathbb{Z}$ is a principal ideal domain.

1.7. Proposition. *Let $R$ be a commutative ring and $I \lhd R$ an ideal.*

(i) *The quotient ring $R/I$ is an integral domain if and only if $I$ is a prime ideal.*
(ii) *The quotient ring $R/I$ is a field if and only if $I$ is a maximal ideal.*

1.8. Example. If $n \geqslant 0$, the quotient ring $\mathbb{Z}/n = \mathbb{Z}/(n)$ is an integral domain if and only if $n$ is a prime.

For any (not necessarily commutative) ring with unity there is an important ring homomorphism $\eta\colon \mathbb{Z} \longrightarrow R$ called the *unit* or *characteristic* homomorphism which is defined by

$$\eta(n) = n1 = \begin{cases} \underbrace{1 + \cdots + 1}_{n} & \text{if } n > 0, \\ -(\underbrace{1 + \cdots + 1}_{-n}) & \text{if } n < 0, \\ 0 & \text{if } n = 0. \end{cases}$$

Since $1 \in R$ is non-zero, $\ker \eta \lhd \mathbb{Z}$ is a proper ideal and using the Isomorphism Theorems we see that there is a quotient monomorphism $\overline{\eta}\colon \mathbb{Z}/\ker \eta \longrightarrow R$ which allows us to identify the quotient ring $\mathbb{Z}/\ker \eta$ with the image $\eta\mathbb{Z} \subseteq R$ as a subring of $R$. By Example 1.6, there is a unique non-negative integer $p \geqslant 0$ such that $\ker \eta = (p)$; this $p$ is called the *characteristic* of $R$ and denoted $\operatorname{char} R$.

1.9. Lemma. *If $R$ is an integral domain, its characteristic* $\operatorname{char} R$ *is a prime.*

PROOF. Consider $p = \operatorname{char} R$. If $p = 0$ we are done. So suppose that $p > 0$. The quotient monomorphism $\overline{\eta}\colon \mathbb{Z}/\ker\eta \longrightarrow R$ identifies $\mathbb{Z}/\ker\eta$ with the subring $\operatorname{im}\overline{\eta} = \operatorname{im}\eta$ of the integral domain $R$. But every subring of an integral domain is itself an integral domain, hence $\mathbb{Z}/\ker\eta$ is an integral domain. Now by Proposition 1.7(i), $\ker\eta = (p)$ is prime ideal and so by Example 1.8, $p$ is a prime. □

1.10. REMARK. When discussing a ring with unit $R$, we can consider it as containing as a subring of the form $\mathbb{Z}/(\operatorname{char} R)$ since the quotient homomorphism $\overline{\eta}\colon \mathbb{Z}/(\operatorname{char} R) \longrightarrow R$ gives an isomorphism $\mathbb{Z}/(\operatorname{char} R) \longrightarrow \operatorname{im}\eta$, allowing us to identify these rings. In particular, every integral domain contains as a subring either $\mathbb{Z} = \mathbb{Z}/(0)$ (if $\operatorname{char} R = 0$) or $\mathbb{Z}/(p)$ if $p = \operatorname{char} R > 0$ is a non-zero prime. This subring is sometimes called the *characteristic subring* of $R$. The rings $\mathbb{Z}$ and $\mathbb{Z}/n = \mathbb{Z}/(n)$ for $n > 0$ are often called *core rings*. When considering integral domains, the rings $\mathbb{Z}$ and $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/(p)$ for $p > 0$ a prime are called *prime rings*.

Here is a useful and important fact about rings which contain a *finite* prime ring $\mathbb{F}_p$.

1.11. THEOREM (Idiot's Binomial Theorem). *Let $R$ be a commutative ring containing $\mathbb{F}_p$ for some prime $p > 0$. If $u, v \in R$, then*

$$(u+v)^p = u^p + v^p.$$

PROOF. We have $p1 = 0$ in $R$, hence $pt = 0$ for any $t \in R$. The Binomial Expansion yields

$$(u+v)^p = u^p + \binom{p}{1}u^{p-1}v + \binom{p}{2}u^{p-2}v^2 + \cdots + \binom{p}{p-1}uv^{p-1} + v^p. \tag{1.1}$$

Now suppose that $1 \leqslant j \leqslant p-1$. Then we have

$$\binom{p}{j} = \frac{p\,(p-1)!}{j!\,(p-j)!} = p \times \frac{(p-1)!}{j!\,(p-j)!}\,.$$

There are no factors of $p$ appearing in $(p-1)!$, $j!$ or $(p-j)!$, so since this number is an integer it must be divisible by $p$, *i.e.*,

$$p \mid \binom{p}{j}, \tag{1.2a}$$

or equivalently

$$\binom{p}{j} \equiv 0 \pmod{p}. \tag{1.2b}$$

Hence in $R$ we have

$$\binom{p}{j}1 = 0.$$

Combining the divisibility conditions of (1.2) with the expansion of (1.1), we obtain the required equation in $R$,

$$(u+v)^p = u^p + v^p.$$ □

1.12. DEFINITION. A commutative ring $\Bbbk$ is a *field* if every non-zero element $u \in \Bbbk$ is a unit. This is equivalent to requiring that $\Bbbk^\times = \Bbbk - \{0\}$.

The familiar rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields.

1.13. EXAMPLE. If $n \geqslant 1$, the quotient ring $\mathbb{Z}/n$ is a field if and only if $n$ is a prime.

1.14. PROPOSITION. *Every field is an integral domain.*

PROOF. Let $\Bbbk$ be a field. Suppose that $u, v \in \Bbbk$ and $uv = 0$. If $u \neq 0$, we can multiply by $u^{-1}$ to obtain

$$v = u^{-1}uv = 0,$$

hence $v = 0$. So at least one of $u, v$ must be 0. □

1.15. LEMMA. *Let $R$ be an integral domain. If $p \in R$ is a non-zero prime then it is irreducible.*

PROOF. Suppose that $p = uv$ for some $u, v \in R$. Then $p \mid u$ or $p \mid v$, and we might as well assume that $u = tp$ for some $t \in R$. Then $(1 - tv)p = 0$ and so $tv = 1$, showing that $v$ is a unit with inverse $t$. □

Now let $D$ be an integral domain. A natural question to ask is whether $D$ is isomorphic to a subring of a field. This is certainly true for the integers $\mathbb{Z}$ which are contained in the field of rational numbers $\mathbb{Q}$, and for a prime $p > 0$, the prime ring $\mathbb{F}_p$ is itself a field.

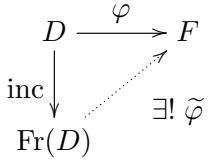
1.16. DEFINITION. The fields $\mathbb{Q}$ and $\mathbb{F}_p$ where $p > 0$ is a prime are the *prime fields*.

Of course, we can view $\mathbb{Z}$ as a subring of any subfield of the complex numbers so an answer to this question may not be unique! However, there is always a 'smallest' such field which is unique up to an isomorphism.

1.17. THEOREM. *Let $D$ be an integral domain.*

(i) *There is a* field of fractions *of $D$, $\mathrm{Fr}(D)$, which contains $D$ as a subring.*

(ii) *If $\varphi\colon D \longrightarrow F$ is a ring monomorphism into a field $F$, there is a unique homomorphism $\widetilde{\varphi}\colon \mathrm{Fr}(D) \longrightarrow F$ such that $\widetilde{\varphi}(t) = \varphi(t)$ for all $t \in D \subseteq \mathrm{Fr}(D)$.*




PROOF. (i) Consider the set

$$\mathrm{P}(D) = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

Now introduce an equivalence relation $\sim$ on $\mathrm{P}(D)$, namely

$$(a', b') \sim (a, b) \quad \Longleftrightarrow \quad ab' = a'b.$$

Of course, it is necessary to check that this relation *is* an equivalence relation; this is left as an exercise. We denote the equivalence class of $(a, b)$ by $[a, b]$ and the set of equivalence classes by $\mathrm{Fr}(D)$.

We define addition and multiplication on $\mathrm{Fr}(D)$ by

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b][c, d] = [ac, bd].$$

We need to verify that these operations are well defined. For example, if $[a', b'] = [a, b]$ and $[c', d'] = [c, d]$, then

$$(a'd' + b'c')bd = a'd'bd + b'c'bd = ab'd'd + b'bcd' = (ad + bc)b'd',$$

and so $(a'd' + b'c', b'd') \sim (ad + bc, bd)$; hence addition is well defined. A similar calculation shows that $(a'c', b'd') \sim (ac, bd)$, so multiplication is also well defined. It is now straightforward to show that $\mathrm{Fr}(D)$ is a commutative ring with zero $0 = [0, 1]$ and unit $1 = [1, 1]$. In fact, as we will soon see, $\mathrm{Fr}(D)$ is a field.

Let $[a, b] \in \mathrm{Fr}(D)$. Then $[a, b] = [0, 1]$ if and only if $(0, 1) \sim (a, b)$ which is equivalent to requiring that $a = 0$; notice that for any $b \neq 0$, $[0, b] = [0, 1]$. We also have $[a, b] = [1, 1]$ if and only if $a = b$.

Now let $[a, b] \in \mathrm{Fr}(D)$ be non-zero, *i.e.*, $a \neq 0$. Then $b \neq 0$ and $[a, b], [b, a] \in \mathrm{Fr}(D)$ satisfy

$$[a, b][b, a] = [ab, ba] = [1, 1] = 1,$$

so $[a, b]$ has $[b, a]$ as an inverse. This shows that $\mathrm{Fr}(D)$ is a field.

We can view $D$ as a subring of $\mathrm{Fr}(D)$ using the map

$$j\colon D \longrightarrow \mathrm{Fr}(D); \quad j(t) = [t, 1]$$

which is a ring homomorphism; it is easy to check that it is a monomorphism. Therefore we may identify $t \in D$ with $j(t) = [t, 1] \in \mathrm{Fr}(D)$ and $D$ with the subring $\operatorname{im} j \subseteq \mathrm{Fr}(D)$.
(ii) Consider the function

$$\Phi\colon \mathrm{P}(D) \longrightarrow F; \quad \Phi(a, b) = \varphi(a)\varphi(b)^{-1}.$$

If $(a', b') \sim (a, b)$, then

$$\begin{aligned}
\Phi(a', b') = \varphi(a')\varphi(b')^{-1} &= \varphi(a')\varphi(b)\varphi(b)^{-1}\varphi(b')^{-1} \\
&= \varphi(a'b)\varphi(b)^{-1}\varphi(b')^{-1} \\
&= \varphi(ab')\varphi(b')^{-1}\varphi(b)^{-1} \\
&= \varphi(a)\varphi(b')\varphi(b')^{-1}\varphi(b)^{-1} \\
&= \varphi(a)\varphi(b)^{-1} = \Phi(a, b),
\end{aligned}$$

so $\Phi$ is constant on each equivalence class of $\sim$. Hence we may define the function

$$\widetilde{\varphi}\colon \mathrm{Fr}(D) \longrightarrow F; \quad \widetilde{\varphi}([a, b]) = \Phi(a, b).$$

It is now easy to verify that $\widetilde{\varphi}$ is a ring homomorphism which agrees with $\varphi$ on $D \subseteq \mathrm{Fr}(D)$. □

The next three corollaries are left as an exercise.

1.18. Corollary. *If $F$ is a field then $F = \mathrm{Fr}(F)$.*

1.19. Corollary. *If $D$ is a subring of a field $F$, then $\mathrm{Fr}(D) \subseteq \mathrm{Fr}(F) = F$ and $\mathrm{Fr}(D)$ is the smallest subfield of $F$ containing $D$.*

1.20. Corollary. *Let $D_1$ and $D_2$ be integral domains and let $\varphi\colon D_1 \longrightarrow D_2$ be a ring monomorphism. Then there is a unique induced ring homomorphism $\varphi_*\colon \mathrm{Fr}(D_1) \longrightarrow \mathrm{Fr}(D_2)$ which satisfies $\varphi_*(t) = \varphi(t)$ whenever $t \in D_1 \subseteq \mathrm{Fr}(D_1)$.*

$$\begin{array}{ccc}
D_1 & \xrightarrow{\ \varphi\ } & D_2 \\
\big\downarrow \mathrm{inc} & & \big\downarrow \mathrm{inc} \\
\mathrm{Fr}(D_1) & \xrightarrow[\ \varphi_*\ ]{} & \mathrm{Fr}(D_2)
\end{array}$$

*Moreover, this construction has the following properties.*

- *If* $\varphi\colon D_1 \longrightarrow D_2$ *and* $\theta\colon D_2 \longrightarrow D_3$ *are monomorphisms between integral domains then* $\theta_* \circ \varphi_* = (\theta \circ \varphi)_*$ *as homomorphisms* $\mathrm{Fr}(D_1) \longrightarrow \mathrm{Fr}(D_3)$.
- *For any integral domain* $D$*, the identity homomorphism* $\mathrm{id}\colon D \longrightarrow D$ *induces the identity homomorphism* $(\mathrm{id})_* = \mathrm{id}\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$.

$$\begin{array}{ccccc} D_1 & \xrightarrow{\varphi} & D_2 & \xrightarrow{\theta} & D_3 \\ \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} \\ \mathrm{Fr}(D_1) & \xrightarrow[\varphi_*]{} & \mathrm{Fr}(D_2) & \xrightarrow[\theta_*]{} & \mathrm{Fr}(D_3) \end{array} \qquad \begin{array}{ccc} D & \xrightarrow{\mathrm{id}} & D \\ \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} \\ \mathrm{Fr}(D) & \xrightarrow[\mathrm{id}_* = \mathrm{id}]{} & \mathrm{Fr}(D) \end{array}$$

1.21. Remarks. (a) When working with a field of fractions we usually adopt the familiar notation

$$\frac{a}{b} = a/b = [a, b]$$

for the equivalence class of $(a, b)$. The rules for algebraic manipulation of such symbols are the usual ones for working with fractions, *i.e.*,

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\,, \quad \frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{a_1}{b_1}\,\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}\,.$$

The field of fractions of an integral domain is sometimes called its *field of quotients*, however as the word quotient is also associated with quotient rings we prefer to avoid using that terminology. (b) Corollary 1.20 is sometimes said to imply that the construction of $\mathrm{Fr}(D)$ is *functorial* in the integral domain $D$.

## 1.2. Polynomial rings

Let $R$ be a commutative ring. We will make frequent use of the *ring* $R[X]$ *of polynomials over* $R$ *in an indeterminate* $X$. This consists of elements of form

$$p(X) = p_0 + p_1 X + \cdots + p_m X^m$$

where $m \geqslant 0$ and $p_0, p_1, \ldots, p_m \in R$; such $p(X)$ are called *polynomials*. Addition and multiplication in $R[X]$ are defined by

$$(p_0 + p_1 X + \cdots + p_m X^m) + (q_0 + q_1 X + \cdots + q_m X^m) = \\ (p_0 + q_0) + (p_1 + q_1)X + \cdots + (p_m + q_m)X^m,$$

and

$$(p_0 + p_1 X + \cdots + p_m X^m)(q_0 + q_1 X + \cdots + q_m X^m) = \\ (p_0 q_0) + (p_0 q_1 + p_1 q_0)X + \cdots + (p_0 q_m + p_1 q_{m-1} + \cdots + p_{m-1} q_1 + p_m q_0)X^{2m}.$$

Then $R[X]$ is a commutative ring with the constant polynomials 0 and 1 as its zero and unit. We identify $r \in R$ with the obvious constant polynomial; this allows us to view $R$ as a subring of $R[X]$ and the inclusion function $\mathrm{inc}\colon R \longrightarrow R[X]$ is a monomorphism.

More generally, we inductively can define the ring of polynomials in $n$ indeterminates $X_1, \ldots, X_n$ over $R$,

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

for $n \geqslant 1$. Again there is an inclusion monomorphism $\mathrm{inc}\colon R \longrightarrow R[X_1, \ldots, X_n]$ which sends each element of $R$ to itself considered as a constant polynomial.

These polynomial rings have an important *universal property.*

1.22. Theorem (Homomorphism Extension Property). *Let $\varphi\colon R \longrightarrow S$ be a ring homomorphism.*

(i) *For each $s \in S$ there is a unique ring homomorphism $\varphi_s\colon R[X] \longrightarrow S$ for which*
- $\varphi_s(r) = \varphi(r)$ *for all* $r \in R$,
- $\varphi_s(X) = s$.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \text{inc}}\downarrow & \nearrow_{\exists!\ \varphi_s} & \\ R[X] & & \end{array}$$

(ii) *For $n \geqslant 1$ and $s_1, \ldots, s_n \in S$, there is a unique ring homomorphism*

$$\varphi_{s_1,\ldots,s_n}\colon R[X_1, \ldots, X_n] \longrightarrow S$$

*for which*
- $\varphi_{s_1,\ldots,s_n}(r) = \varphi(r)$ *for all* $r \in R$,
- $\varphi_{s_1,\ldots,s_n}(X_i) = s_i$ *for* $i = 1, \ldots, n$.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \text{inc}}\downarrow & \nearrow_{\exists!\ \varphi_{s_1,\ldots,s_n}} & \\ R[X_1, \ldots, X_n] & & \end{array}$$

Proof. (Sketch)
(i) For a polynomial $p(X) = p_0 + p_1X + \cdots + p_mX^m \in R[X]$, we define

$$\varphi_s(p(X)) = \varphi(p_0) + \varphi(p_1)s + \cdots + \varphi(p_m)s^m \in S. \tag{1.3}$$

It is then straightforward to check that $\varphi_s$ is a ring homomorphism with the stated properties and moreover is the unique such homomorphism.
(ii) is proved by induction on $n$ using (i). □

We will refer to $\varphi_{s_1,\ldots,s_n}$ as the *extension of $\varphi$ by evaluation at $s_1, \ldots, s_n$*. It is standard to write

$$p(s_1, \ldots, s_n) = \varphi_{s_1,\ldots,s_n}(p(X_1, \ldots, X_n)).$$

An important special case occurs when we start with the identity homomorphism $\mathrm{id}\colon R \longrightarrow R$ and $r_1, \ldots, r_n \in R$; then we have the homomorphism

$$\varepsilon_{r_1,\ldots,r_n} = \mathrm{id}_{r_1,\ldots,r_n}\colon R[X_1, \ldots, X_n] \longrightarrow R.$$

Slightly more generally we may take the inclusion of a subring $\mathrm{inc}\colon R \longrightarrow S$ and $s_1, \ldots, s_n \in S$; then

$$\varepsilon_{s_1,\ldots,s_n} = \mathrm{inc}_{s_1,\ldots,s_n}\colon R[X_1, \ldots, X_n] \longrightarrow S$$

is called *evaluation at $s_1, \ldots, s_n$* and we denote its image by

$$R[s_1, \ldots, s_n] = \varepsilon_{s_1,\ldots,s_n}\, R[X_1, \ldots, X_n] \subseteq S.$$

Then $R[s_1, \ldots, s_n]$ is a subring of $S$, called the *subring generated by $s_1, \ldots, s_n$ over $R$.*

Here is an example illustrating how we will use such evaluation homomorphisms.

1.23. Example. Consider the inclusion homomorphism $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$. We have the evaluation at $i$ homomorphism $\varepsilon_i$, for which $\varepsilon_i(X) = i$. We easily see that $\varepsilon_i\, \mathbb{Q}[X] \subseteq \mathbb{C}$ is a subring $\mathbb{Q}[i] \subseteq \mathbb{C}$ consisting of the complex numbers of form $a + bi$ with $a, b \in \mathbb{Q}$.

Notice that if we had used $-i$ instead of $i$, evaluation at $-i$, $\varepsilon_{-i}$, we would also have $\varepsilon_{-i}\, \mathbb{Q}[X] = \mathbb{Q}[i]$. These evaluation homomorphisms are related by complex conjugation since

$$\varepsilon_{-i}(p(X)) = \overline{\varepsilon_i(p(X))},$$

which is equivalent to the functional equation

$$\varepsilon_{-i} = (\overline{\ }) \circ \varepsilon_i\,.$$

Notice also that in these examples we have

$$\ker \varepsilon_{-i} = \ker \varepsilon_i = (X^2 + 1) \lhd \mathbb{Q}[X],$$

hence we also have

$$\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2 + 1).$$

In fact $(X^2 + 1)$ is actually a maximal ideal and so $\mathbb{Q}[i] \subseteq \mathbb{C}$ is a subfield; later we will write $\mathbb{Q}(i)$ for this subfield.

1.24. Proposition. *Let $R$ be an integral domain.*

(i) *The ring $R[X]$ of polynomials in an indeterminate $X$ over $R$ is an integral domain.*
(ii) *The ring $R[X_1, \ldots, X_n]$ of polynomials in the indeterminates $X_1, \ldots, X_n$ over $R$ is an integral domain.*

1.25. Corollary. *Let $\Bbbk$ be a field and $n \geqslant 1$. Then the polynomial ring $\Bbbk[X_1, \ldots, X_n]$ in the indeterminates $X_1, \ldots, X_n$ is an integral domain.*

As we will make considerable use of such rings we describe in detail some of their important properties. First we recall *long division* in a polynomial ring $\Bbbk[X]$ over a field $\Bbbk$; full details can be found in a basic course on commutative rings or any introductory book on this subject.

1.26. Theorem (Long Division). *Let $\Bbbk$ be a field. Let $f(X), d(X) \in \Bbbk[X]$ and assume that $d(X) \neq 0$ so that $\deg d(X) > 0$. Then there are unique polynomials $q(X), r(X) \in \Bbbk[X]$ for which*

$$f(X) = q(X)d(X) + r(X)$$

*and either $\deg r(X) < \deg d(X)$ or $r(X) = 0$.*

In the situation discussed in this result, the following names are often used. We refer to the process of finding $q(X)$ and $r(X)$ as *long division of $f(X)$ by $d(X)$*. Also,

$$f(X) = \text{the } \textit{dividend}, \quad d(X) = \text{the } \textit{divisor}, \quad q(X) = \text{the } \textit{quotient}, \quad r(X) = \text{the } \textit{remainder}.$$

1.27. Example. For $\Bbbk = \mathbb{Q}$, find the quotient and remainder when $f(X) = 6X^4 - 6X^3 + 3X^2 - 3X + 1$ is divided by $d(X) = 2X^2 + 1$.

SOLUTION. In the usual notation we have the following calculation.

$$\begin{array}{r|l} & 3X^2 - 3X \\ \hline 2X^2 + 1 & 6X^4 - 6X^3 + 3X^2 - 3X + 1 \\ & 6X^4 + 0X^3 + 3X^2 + 0X + 0 \\ \hline & -6X^3 + 0X^2 - 3X + 1 \\ & -6X^3 + 0X^2 - 3X + 0 \\ \hline & 1 \end{array}$$

Hence

$$6X^4 - 6X^3 + 3X^2 - 3X + 1 = (3X^2 - 3X)(2X^2 + 1) + 1,$$

giving $q(X) = 3X^2 - 3X$ and $r(X) = 1$. □

1.28. EXAMPLE. For $\Bbbk = \mathbb{F}_5$, find the quotient and remainder when $f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1$ is divided by $d(X) = 2X^2 + 1$.

SOLUTION. First notice that working modulo 5 we have

$$f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1 \equiv X^4 + 4X^3 + 3X^2 + 2X + 1 \pmod 5.$$

Notice also following multiplicative inverses in $\mathbb{F}_5$:

$$2^{-1} \equiv 3 \pmod 5, \quad 3^{-1} \equiv 2 \pmod 5, \quad 4^{-1} \equiv 4 \pmod 5.$$

We have the following calculation.

$$\begin{array}{r|l} & 3X^2 + 2X \\ \hline 2X^2 + 1 & 6X^4 + 4X^3 + 3X^2 + 2X + 1 \\ & 6X^4 + 0X^3 + 3X^2 + 0X + 0 \\ \hline & 4X^3 + 0X^2 + 2X + 1 \\ & 4X^3 + 0X^2 + 2X + 0 \\ \hline & 1 \end{array}$$

Hence

$$6X^4 - 6X^3 + 3X^2 - 3X + 1 \equiv (3X^2 + 2X)(2X^2 + 1) + 1 \pmod 5,$$

giving $q(X) = 3X^2 + 2X$ and $r(X) = 1$. □

An important consequence of Theorem 1.26 is the following which makes use of the *Euclidean Algorithm*.

1.29. COROLLARY. *Let $\Bbbk$ be a field and $X$ an indeterminate. Let $f(X), g(X) \in \Bbbk[X]$ be non-zero. Then there are $a(X), b(X) \in \Bbbk[X]$ such that*

$$a(X)f(X) + b(X)g(X) = \gcd(f(X), g(X)).$$

Here the *greatest common divisor* $\gcd(f(X), g(X))$ of $f(X), g(X)$ is the monic polynomial of greatest degree which divides both of $f(X), g(X)$.

1.30. Proposition. *Let $\Bbbk$ be a field and $X$ an indeterminate. Then a non-constant polynomial $p(X) \in \Bbbk[X]$ is irreducible if and only if it is a prime.*

Proof. By Lemma 1.15 we already know that $p(X)$ is irreducible if it is prime. So suppose that $p(X)$ is irreducible and that $p(X) \mid u(X)v(X)$ for $u(X), v(X) \in \Bbbk[X]$. Then by Corollary 1.29, there are $a(X), b(X) \in \Bbbk[X]$ such that

$$a(X)p(X) + b(X)u(X) = \gcd(p(X), u(X)).$$

But since $p(X)$ is irreducible, $\gcd(p(X), u(X)) = p(X)$ or $\gcd(p(X), u(X)) = 1$. In the latter case,

$$a(X)p(X) + b(X)u(X) = 1,$$

and multiplying through by $v(X)$ gives

$$a(X)p(X)v(X) + b(X)u(X)v(X) = v(X)$$

and so $p(X) \mid v(X)$. This shows that $p(X) \mid u(X)$ or $p(X) \mid v(X)$, and so $p(X)$ is prime. □

1.31. Theorem. *Let $\Bbbk$ be a field and $X$ an indeterminate.*

(i) *Every ideal $I \lhd \Bbbk[X]$ is principal,* i.e., *$I = (h(X))$ for some $h(X) \in \Bbbk[X]$.*
(ii) *The ideal $(p(X)) \lhd \Bbbk[X]$ is prime if and only if $p(X) = 0$ or $p(X)$ is irreducible in $\Bbbk[X]$.*
(iii) *The quotient ring $\Bbbk[X]/(p(X))$ is an integral domain if and only if $p(X) = 0$ or $p(X)$ is irreducible in $\Bbbk[X]$.*
(iv) *The quotient ring $\Bbbk[X]/(p(X))$ is a field if and only if $p(X)$ is an irreducible in $\Bbbk[X]$.*

Proof. (i) Let $I \lhd \Bbbk[X]$ and assume that $I \neq (0)$. Then there must be at least one element of $I$ with positive degree and so we can choose $h(X) \in I$ of minimal degree, say $d = \deg h(X)$.

Now let $p(X) \in I$. By Long Division, there are $q(X), r(X) \in \Bbbk[X]$ such that

$$p(X) = q(X)h(X) + r(X) \quad \text{and } \deg r(X) < d \text{ or } r(X) = 0.$$

Since $p(X)$ and $h(X)$ are in the ideal $I$, we also have

$$r(X) = p(X) - q(X)h(X) \in I.$$

If $r(X) \neq 0$, this would contradict the minimality of $d$, so we must have $r(X) = 0$, showing that $p(X) = q(X)h(X)$. Thus $I \subseteq (p(X)) \subseteq I$ and therefore $I = (p(X))$.
(ii) This follows from Proposition 1.30.
(iii) This follows from Proposition 1.7(i).
(iv) Since $\Bbbk[X]$ is an integral domain and not a field, it follows that if $\Bbbk[X]/(p(X))$ is a field then because it is an integral domain, $p(X)$ is an irreducible by (iii).

Suppose that $p(X)$ is irreducible (and hence is non-zero). Then for any $q(X) \in \Bbbk[X]$ with $q(X) \notin (p(X))$, by Corollary 1.29 we can find suitable $a(X), b(X) \in \Bbbk[X]$ for which

$$a(X)p(X) + b(X)q(X) = \gcd(p(X), q(X)).$$

But $\gcd(p(X), q(X)) = 1$ since $p(X)$ is irreducible, so

$$a(X)p(X) + b(X)q(X) = 1.$$

This shows that in the quotient ring $\Bbbk[X]/(p(X))$ the residue class of $q(X)$ has the residue class of $b(X)$ as its inverse. □

1.32. Remark. In connection with Theorem 1.31(i), notice that if $p(X) \in \Bbbk[X]$, then provided $d = \deg p(X) > 0$, we have for some $p_d \neq 0$,

$$p(X) = p_0 + p_1 X + \cdots + p_d X^d = p_d q(X),$$

where

$$q(X) = p_d^{-1} p_0 + p_d^{-1} p_1 X + \cdots + p_d^{-1} p_{d-1} X^{d-1} + X^d.$$

This easily implies that as ideals of $\Bbbk[X]$, $(p(X)) = (q(X))$. So we can always find a monic polynomial as the generator of a given ideal, and this monic polynomial is unique.

1.33. Proposition (Unique Factorization Property). *Every non-constant polynomial $f(x) \in \Bbbk[X]$ has a factorization*

$$f(x) = c p_1(X) \cdots p_k(X),$$

*where $c \in \Bbbk$, and $p_1(X), \ldots, p_k(X) \in \Bbbk[X]$ are irreducible monic polynomials. Moreover, $c$ is unique and the sequence of polynomials $p_1(X), \ldots, p_k(X)$ is unique apart from the order of the terms.*

Proof. (Sketch)
Existence is proved by induction on the degree of $f(X)$ and begins with the obvious case $\deg f(X) = 1$. If $\deg f(X) > 1$, then either $f(X)$ is already irreducible, or $f(X) = f_1(X) f_2(X)$ with both factors of positive degree, and therefore $\deg f_j(X) < \deg f(X)$. This gives the inductive step.

To prove uniqueness, suppose that

$$p_1(X) \cdots p_k(X) = q_1(X) \cdots q_\ell(X)$$

where $p_i(X), q_j(X) \in \Bbbk[X]$ are irreducible monic polynomials. Then by Proposition 1.30, each $p_i(X)$ is prime, hence divides one of the $q_j(X)$, hence must equal it. By reordering we can assume that $p_i(X) = q_i(X)$ and $k \leqslant \ell$. After cancelling common factors we obtain

$$q_{k+1}(X) \cdots q_\ell(X) = 1,$$

and so we see that $k = \ell$. □

1.34. Corollary. *Suppose that $f(X) \in \Bbbk[X]$ factors into linear factors*

$$f(X) = c(X - u_1) \cdots (X - u_d),$$

*where $u_1, \ldots, u_d \in \Bbbk$. Then the sequence of roots $u_1, \ldots, u_d$ is unique apart from the order. In particular, if $v_1, \ldots, v_r$ are the distinct roots, then*

$$f(X) = c(X - v_1)^{m_1} \cdots (X - v_r)^{m_r},$$

*where $m_i > 0$ and this factorization is unique apart from the order of the pairs $(v_i, m_i)$.*

1.35. Corollary. *The number of distinct roots of a non-constant polynomial $f(X) \in \Bbbk[X]$ is at most* $\deg f(X)$.

1.36. Definition. If $\Bbbk$ is a field and $X$ an indeterminate, then the field of fractions of $\Bbbk[X]$ is the *field of rational functions*, $\Bbbk(X)$. The elements of $\Bbbk(X)$ are fractions of the form

$$\frac{a_0 + a_1 X + \cdots + a_m X^m}{b_0 + b_1 X + \cdots + b_n X^n}$$

with $a_i, b_j \in \Bbbk$ and $b_0 + b_1 X + \cdots + b_n X^n \neq 0$.

### 1.3. Identifying irreducible polynomials

When $\Bbbk$ is a field, we will need some effective methods for deciding when a polynomial in $\Bbbk[X]$ is irreducible.

Let us consider factorisation of polynomials over $\mathbb{Q}$. If $f(X) \in \mathbb{Z}[X]$ then we can also consider $f(X)$ as an element of $\mathbb{Q}[X]$. If $R = \mathbb{Z}$ or $\mathbb{Q}$, we say that $f(X)$ has a *proper factorisation over* $R$ if $f(X) = g(X)h(X)$ for some $g(X), h(X) \in R[X]$ with $\deg g(X) > 0$ and $\deg h(X) > 0$.

1.37. Proposition (Gauss's Lemma). *Let $f(X) \in \mathbb{Z}[X]$. Then $f(X)$ has a proper factorisation over $\mathbb{Z}$ if and only it has a proper factorisation over $\mathbb{Q}$.*

So to find factors of $f(X)$ it is sufficient to look for factors in $\mathbb{Z}[X]$. Our next result is a special case of the *Eisenstein Irreducibility Test*. The version here is slightly more general than the more usual one which corresponds to taking $s = 0$.

1.38. Proposition (Eisenstein Test). *Let $f(X) \in \mathbb{Z}[X]$ and $s \in \mathbb{Z}$. Choose $a_i \in \mathbb{Z}$ so that*

$$f(X) = a_0 + a_1(X - s) + \cdots + a_{d-1}(X - s)^{d-1} + a_d(X - s)^d,$$

*where $d = \deg f(X)$. Suppose that $p > 0$ is a prime for which the following three conditions hold:*

- $a_k \equiv 0 \pmod{p}$ *for $k = 0, \ldots, d-1$;*
- $a_0 \not\equiv 0 \pmod{p^2}$;
- $a_d \not\equiv 0 \pmod{p}$.

*Then $f(X)$ is irreducible in $\mathbb{Q}[X]$ and hence also in $\mathbb{Z}[X]$.*

1.39. Example. Let $p \geqslant 2$ be a prime. Then the polynomial

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1} \in \mathbb{Z}[X]$$

is irreducible in $\mathbb{Q}[X]$ and hence also in $\mathbb{Z}[X]$.

Proof. Working in $\mathbb{Z}[X]$,

$$\begin{aligned}
\Phi_p(X)(X-1) &= (1 + X + \cdots + X^{p-1})(X-1) \\
&= X^p - 1 \\
&= (1 + (X-1))^p - 1 \\
&= \sum_{k=1}^{p} \binom{p}{k} (X-1)^k \\
&\equiv (X-1)^p \pmod{p},
\end{aligned}$$

since by (1.2a), $p$ divides

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

when $k = 1, \ldots, p-1$. Hence

$$\Phi_p(X) \equiv (X-1)^{p-1} \pmod{p}$$

Also,

$$\binom{p}{1} = p \not\equiv 0 \pmod{p^2},$$

giving

$$\Phi_p(X) = (X-1)^{p-1} + c_{p-2}(X-1)^{p-2} + \cdots + c_1(X-1) + c_0 \tag{1.4}$$

with $c_r \equiv 0 \pmod{p}$ and $c_0 = p$. So the Eisenstein Test can be applied here with $s = 1$ to show that $\Phi_p(X)$ is irreducible in $\mathbb{Z}[X]$. □

1.40. Example. As examples we have the irreducible polynomials

$$\begin{aligned}
\Phi_2(X) &= 1 + X, \\
\Phi_3(X) &= 1 + X + X^2, \\
\Phi_5(X) &= 1 + X + X^2 + X^3 + X^4, \\
\Phi_7(X) &= 1 + X + X^2 + X^3 + X^4 + X^5 + X^6, \\
\Phi_{11}(X) &= 1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8 + X^9 + X^{10}.
\end{aligned}$$

These are examples of the *cyclotomic polynomials* $\Phi_n(X) \in \mathbb{Z}[X]$ which are defined for all $n \geqslant 1$ by

$$X^n - 1 = \prod_{d|n} \Phi_d(X), \tag{1.5a}$$

where the product is taken over all the positive divisors of $n$ (including 1 and $n$). For example,

$$\begin{aligned}
X^2 - 1 &= (X-1)(X+1) = \Phi_1(X)\Phi_2(X), \\
X^3 - 1 &= (X-1)(X^2+X+1) = \Phi_1(X)\Phi_3(X), \\
X^4 - 1 &= (X-1)(X+1)(X^2+1) = \Phi_1(X)\Phi_2(X)\Phi_4(X), \\
X^5 - 1 &= (X-1)(X^4+X^3+X^2+X+1) = \Phi_1(X)\Phi_5(X), \\
X^6 - 1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1) = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_6(X), \\
X^{12} - 1 &= (X-1)(X+1)(X^2+X+1)(X^2+1)(X^2-X+1)(X^4-X^2+1) \\
&= \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X).
\end{aligned}$$

Cyclotomic polynomials can be computed recursively using Equation (1.5a). If we know $\Phi_k(X)$ for $k < n$, then

$$\Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}\,. \tag{1.5b}$$

The degree of $\Phi_n(X)$ involves a function of $n$ probably familiar from elementary Number Theory.

1.41. Definition. The *Euler function* $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$ is defined by

$$\begin{aligned}
\varphi(n) &= \text{number of } k = 1, \ldots, n \text{ for which } \gcd(n,k) = 1 \\
&= |(\mathbb{Z}/n)^\times| = \text{number of units in } \mathbb{Z}/n \\
&= \text{number of generators of the cyclic group } \mathbb{Z}/n.
\end{aligned}$$

In particular, if $p \geqslant 2$ is a prime then $\varphi(p) = p - 1$. Of course, $\varphi(1) = 1$.

It can be shown that for each natural number $n$,

$$\sum_{d|n} \varphi(d) = n. \tag{1.6}$$

Notice that we can inductively determine $\varphi(n)$ using this equation. For example, if $p$ and $q$ are *distinct* primes, then

$$\varphi(pq) = pq - (\varphi(p) + \varphi(q) + \varphi(1)) = pq - (p-1) - (q-1) - 1 = (p-1)(q-1).$$

It is also true that whenever $m, n$ are coprime, *i.e.*, when $\gcd(m,n) = 1$,

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{1.7}$$

Thus if $n = p_1^{r_1} \cdots p_s^{r_s}$ where $p_1 < p_2 < \cdots < p_s$ are the prime factors of $n$ and $r_j > 0$, then

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}). \tag{1.8}$$

Furthermore, if $p$ is a prime and $r > 0$, then

$$\varphi(p^r) = (p-1)p^{r-1}. \tag{1.9}$$

Notice that as a result, $\varphi(n)$ is even when $n > 2$.

1.42. Remark. For those who know about the *Möbius function* $\mu$ (which takes values $0, \pm 1$) and *Möbius inversion*, the latter can be used to solve Equation (1.6) for $\varphi$, giving

$$\varphi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d}\,. \tag{1.10}$$

Similarly, the formulae of (1.5) lead to

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}. \tag{1.11}$$

So for example, if $p, q$ are distinct primes, then using standard properties of $\mu$,

$$\begin{aligned} \Phi_{pq}(X) &= (X^{pq}-1)^{\mu(1)}(X^{pq/p}-1)^{\mu(p)}(X^{pq/q}-1)^{\mu(q)}(X^{pq/pq}-1)^{\mu(pq)} \\ &= (X^{pq}-1)(X^q-1)^{-1}(X^p-1)^{-1}(X-1) = \frac{(X^{pq}-1)(X-1)}{(X^q-1)(X^p-1)}\,. \end{aligned}$$

Recall that an element $\zeta$ of a field $K$ is a *primitive $n$-th root of unity* if

$$\min\{k : 1 \leqslant k \text{ and } \zeta^k = 1\} = n.$$

We think of $\zeta_n = e^{2\pi i/n}$ as the *standard complex primitive $n$-th root of unity.* Then every complex $n$-th root of unity has the form $\zeta_n^k = e^{2\pi ik/n}$ for $k = 0, 1, \ldots, n-1$.

1.43. Theorem. *For each $n \geqslant 1$, the cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$ and hence in $\mathbb{Z}[X]$. The complex roots of $\Phi_n(X)$ are the primitive $n$-th roots of unity,*

$$\zeta_n^k = e^{2\pi ik/n} \quad (0 \leqslant k \leqslant n-1,\ \gcd(k,n) = 1).$$

*and the number of these is* $\deg \Phi_n(X) = \varphi(n)$. *Hence,*

$$\Phi_n(X) = \prod_{\substack{t=1,\ldots,n-1 \\ \gcd(t,n)=1}} (X - \zeta_n^t).$$

Proof. We will give a reformulation and proof of this in Theorem 6.2. □

1.44. Example. For $n = 6$ we have

$$\zeta_6 = e^{2\pi i/6} = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}\, i.$$

Then $\varphi(6) = 2$ and

$$\Phi_6(X) = X^2 - X + 1 = (X - \zeta_6)(X - \zeta_6^5).$$

It is also worth recording a related general result on cyclic groups.

1.45. Proposition. *Let $n \geqslant 1$ and $C = \langle g \rangle$ be a cyclic group of order $n$ and a generator $g$. Then an element $g^r \in C$ is a generator if and only if $\gcd(r, n) = 1$; the number of such elements of $C$ is $\varphi(n)$.*

This leads to a useful group theoretic result.

1.46. Lemma. *Let $G$ be a finite group satisfying the following condition:*

- *For each $n \geqslant 1$, there are at most $n$ solutions of $x^n = \iota$ in $G$.*

*Then $G$ is cyclic and in particular is abelian.*

Proof. Let $\theta_G(d)$ denote the number of elements in $G$ of order $d$. By Lagrange's Theorem, $\theta_G(d) = 0$ unless $d$ divides $|G|$. Since

$$G = \bigcup_{d||G|} \{g \in G : |g| = d\},$$

we have

$$|G| = \sum_{d||G|} \theta_G(d).$$

Recall the Euler $\varphi$-function satisfies Equation (1.6), hence

$$|G| = \sum_{d||G|} \varphi(d).$$

Combining these we obtain

$$\sum_{d||G|} \theta_G(d) = \sum_{d||G|} \varphi(d). \tag{1.12}$$

Let $d$ be a divisor of $|G|$. By Proposition 1.45, for each element $g \in G$ of order $d$, the cyclic subgroup $\langle g \rangle \leqslant G$ has $\varphi(d)$ generators, each of order $d$. As there are at most $d$ such elements $g$ in $G$, this gives $\theta_G(d) \leqslant \varphi(d)$. So

$$\sum_{d||G|} \theta_G(d) \leqslant \sum_{d||G|} \varphi(d).$$

Now if $\theta_G(d) < \varphi(d)$ for some $d$, we would have a *strict* inequality in place of Equation (1.12). Hence $\theta_G(d) = \varphi(d)$ for all $d$. In particular, there are $\varphi(|G|)$ elements of order $|G|$, hence there must be an element of order $|G|$, so $G$ is cyclic. □

The above results for polynomials over $\mathbb{Q}$ and $\mathbb{Z}$ have analogues over the field of fractions $\Bbbk(T)$ and polynomial ring $\Bbbk[T]$, where $\Bbbk$ is a field.

A polynomial $f(X) \in \Bbbk[T][X]$ is an element of $\Bbbk(T)[X]$. If $R = \Bbbk[T]$ or $\Bbbk(T)$, we say that $f(X)$ has a *proper factorisation over $R$* if $f(X) = g(X)h(X)$ for some $g(X), h(X) \in R[X]$ with $\deg g(X) > 0$ and $\deg h(X) > 0$.

1.47. Proposition (Gauss's Lemma). *Let $f(X) \in \Bbbk[T][X]$. Then $f(X)$ has a proper factorisation over $\Bbbk[T]$ if and only it has a proper factorisation over $\Bbbk(T)$.*

Here is another version of the *Eisenstein Test*; again we state a version which is slightly more general than the usual one which corresponds to the case where $s = 0$.

1.48. Proposition (Eisenstein Test). *Let $f(X) \in \Bbbk[T][X]$ and $s \in \Bbbk[T]$. Choose $a_i \in \Bbbk[T]$ so that*

$$f(X) = a_0 + a_1(X - s) + \cdots + a_{d-1}(X - s)^{d-1} + a_d(X - s)^d,$$

*where $d = \deg f(X)$. Suppose that $p(T) \in \Bbbk[T]$ is an irreducible for which the following three conditions hold:*

- $a_k \equiv 0 \pmod{p(T)}$ *for $k = 0, \ldots, d-1$;*
- $a_0 \not\equiv 0 \pmod{p(T)^2}$;
- $a_d \not\equiv 0 \pmod{p(T)}$.

*Then $f(X)$ is irreducible in $\Bbbk(T)[X]$ and hence also in $\Bbbk[T][X]$.*

1.49. Example. Let $\Bbbk$ be a field. Then the polynomial $X^n - T$ is irreducible in $\Bbbk(T)[X]$.

### 1.4. Finding roots of complex polynomials of small degree

♡♠♣♢ In this section we work within the complex numbers and take $\Bbbk \subseteq \mathbb{C}$. In practice we will usually have $\Bbbk = \mathbb{R}$ or $\Bbbk = \mathbb{C}$.

For monic linear (degree 1) or quadratic (degree 2) polynomials, methods of finding roots are very familiar. Let us consider the cases of cubic (degree 3) and quartic (degree 4) polynomials.

**Cubic polynomials: Cardan's method.** The following 16th century method of finding roots of cubics is due to Jerôme Cardan who seems to have obtained some preliminary versions from Niccolò Tartaglia by somewhat disreputable means! For historical details see [**2, 3**].

A monic cubic

$$f(X) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$$

can be transformed into one with no quadratic term by a change of variables $X \longmapsto X - a_2/3$ giving

$$g(X) = f(X - a_2/3) = X^3 - \left(a_1 - \frac{1}{3}\,a_2^2\right) X + \left(a_0 - \frac{a_1a_2}{3} + \frac{2a_2^3}{27}\right) \in \mathbb{C}[X].$$

Clearly finding the roots of $f(X)$ is equivalent to finding those of $g(X)$, so we may as well assume that we want to find the complex roots of

$$f(X) = X^3 + pX + q \in \mathbb{C}[X].$$

Suppose that $x \in \mathbb{C}$ is a root of $f(X)$, *i.e.*,

$$x^3 + px + q = 0. \tag{1.13}$$

If we introduce $u \in \mathbb{C}$ for which

$$x = u - \frac{p}{3u}\,,$$

then

$$\left(u - \frac{p}{3u}\right)^3 + p\left(u - \frac{p}{3u}\right) + q = 0$$

and so

$$u^3 - \frac{p^3}{27u^3} + q = 0,$$

hence

$$u^6 + qu^3 - \frac{p^3}{27} = 0.$$

Solving for $u^3$ we obtain

$$u^3 = -\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}\,,$$

where $\sqrt{q^2 + \frac{4p^3}{27}}$ denotes one of the complex square roots of the discriminant of the quadratic equation

$$U^2 + qU - \frac{p^3}{27} = 0.$$

Now if we take $u$ to be a cube root of one of the complex numbers

$$-\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}$$

we obtain the desired root of $f(X)$ as $x = u - p/3u$. Notice that we have a choice of 2 values for $u^3$ and for each of these a choice of 3 values for $u$, differing by factors of the form $\omega^r$ for $r = 0, 1, 2$ where $\omega = e^{2\pi i/3}$ is a primitive cube root of 1. However, since

$$\frac{1}{-q + \sqrt{q^2 + \frac{4p^3}{27}}} = \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{q^2 - (q^2 + 4p^3/27)} = -27\,\frac{\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}{4p^3}\,,$$

it is easy to verify that there are in fact only 3 choices of the root $x$ which we can write symbolically as

$$x = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} \tag{1.14}$$

or more precisely as

$$x = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}}}\,. \tag{1.15}$$

1.50. Example. Find the complex roots of the polynomial

$$f(X) = X^3 + 3X - 10 \in \mathbb{R}[X].$$

Solution. Applying the method above, we reduce to the quadratic equation

$$U^2 - 10U - 1 = 0$$

whose roots are $5 \pm \sqrt{26} \in \mathbb{R}$. Notice that $5 + \sqrt{26} > 0$ and $5 - \sqrt{26} < 0$; we also have

$$5 - \sqrt{26} = \frac{-1}{5 + \sqrt{26}}\,.$$

Now $5 + \sqrt{26}$ has the complex cube roots

$$\sqrt[3]{5 + \sqrt{26}}\,,\ \sqrt[3]{5 + \sqrt{26}}\ \omega,\ \sqrt[3]{5 + \sqrt{26}}\ \omega^2.$$

Here we have $x = u - 1/u$, so the 3 complex roots of $f(X)$ are

$$\left( \sqrt[3]{5+\sqrt{26}} - \frac{1}{\sqrt[3]{5+\sqrt{26}}} \right) \omega^r \quad (r = 0, 1, 2).$$

Notice that one of these is real, namely

$$\sqrt[3]{5+\sqrt{26}} - \frac{1}{\sqrt[3]{5+\sqrt{26}}} = \frac{\left(\sqrt[3]{5+\sqrt{26}}\right)^2 - 1}{\sqrt[3]{5+\sqrt{26}}}. \qquad \square$$

**Quartic polynomials: Ferrari's method.** The following method of finding roots of quartics was publicised by Cardan who attributed it to his student Lodovicio Ferrari.

A general monic quartic polynomial

$$f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$$

can be transformed into one with no cubic term by a change of variables $X \longmapsto X - a_2/4$ giving

$$g(X) = f(X - a_3/4) =$$
$$Y^4 + \left(a_2 - \frac{3}{8}\,a_3^2\right) Y^2 + \left(\frac{1}{8}\,a_3^3 - \frac{1}{2}\,a_2a_3 + a_1\right) Y - \left(\frac{1}{16}\,a_2a_3^2 - \frac{3}{256}\,a_3^4 + \frac{1}{4}\,a_1a_3 + a_0\right).$$

Clearly finding the roots of $f(X)$ is equivalent to finding those of $g(X)$, so we may as well assume that we want to find the complex roots of

$$f(X) = X^4 + pX^2 + qX + r \in \mathbb{C}[X].$$

Suppose that $x$ is a root and introduce numbers $y, z$ such that $z = x^2 + y$ (we will fix the values of these later). Then

$$\begin{aligned} z^2 &= x^4 + 2x^2y + y^2 \\ &= -px^2 - qx - r + 2x^2y + y^2 \\ &= (2y - p)x^2 - qx + y^2 - r. \end{aligned}$$

Now choose $y$ to make the last quadratic expression in $x$ a square,

$$(2y - p)x^2 - qx + (y^2 - r) = (Ax + B)^2. \tag{1.16}$$

This can be done by requiring the vanishing of the discriminant

$$q^2 - 4(2y - p)(y^2 - r) = 0. \tag{1.17}$$

Notice that if $y = p/2$ then we would require $q = 0$ and then

$$f(X) = X^4 + pX^2 + r = (X^2)^2 + p(X^2) + r = 0$$

can be solved by solving

$$Z^2 + pZ + r = 0.$$

Since Equation (1.17) is a cubic in $y$, we can use the method of solution of cubics to find a root $y = t$ say. Then for Equation (1.16) we have

$$(x^2 + t)^2 = (Ax + B)^2,$$

whence

$$x^2 = -t \pm (Ax + B).$$

Thus taking the two square roots of the right hand side we obtain 4 values for $x$, which we write symbolically as

$$x = \pm\sqrt{-t \pm (Ax + B)}\,.$$

1.51. Remark. In the case of cubic and quartic polynomials over $\mathbb{C}$ we can obtain all the roots by repeatedly taking square or cube roots (or *radicals*). Consequently such polynomials are said to be *solvable by radicals*. Later we will see that this is not true in general for polynomials of degree at least 5; this is one of the great early successes of this theory.

## 1.5. Automorphisms of rings and fields

1.52. Definition. Let $R$ be a ring and $R_0 \subseteq R$ a subring.

- An *automorphism of* $R$ is a ring isomorphism $\alpha\colon R \longrightarrow R$. The set of all such automorphisms is denoted $\mathrm{Aut}(R)$.
- An *automorphism of* $R$ *over* $R_0$ is a ring isomorphism $\alpha\colon R \longrightarrow R$ for which $\alpha(r) = r$ whenever $r \in R_0$. The set of all automorphisms of $R$ over $R_0$ is denoted $\mathrm{Aut}_{R_0}(R)$.

1.53. Proposition. *For a ring $R$ with a subring $R_0 \subseteq R$, $\mathrm{Aut}(R)$ and $\mathrm{Aut}_{R_0}(R)$ form groups under composition of functions.*

Proof. The composition $\alpha \circ \beta$ of two automorphisms $\alpha, \beta\colon R \longrightarrow R$ is also an automorphism of $R$ as is the inverse of $\alpha$. The identity function $\mathrm{id} = \mathrm{id}_R\colon R \longrightarrow R$ is an automorphism. Hence $\mathrm{Aut}(R)$ forms a group under composition. The argument for $\mathrm{Aut}_{R_0}(R)$ is similar. □

1.54. Proposition. *Let $R$ be one of the core rings $\mathbb{Z}$ or $\mathbb{Z}/n$ with $n > 1$. Then*

(i) *The only automorphism of $R$ is the identity,* i.e., $\mathrm{Aut}(R) = \{\mathrm{id}\}$.

(ii) *If $S$ is a ring containing a core ring $R$ and $\alpha \in \mathrm{Aut}(S)$, then $\alpha$ restricts to the identity on $R$,* i.e., *$\alpha(r) = r$ for all $r \in R$. Hence,* $\mathrm{Aut}(S) = \mathrm{Aut}_R(S)$.

Proof. (i) For such a core ring $R$, every element has the form $k1$ for some $k \in \mathbb{Z}$. For an automorphism $\alpha$ of $R$,

$$\begin{aligned}
\alpha(k1) &= \begin{cases} \underbrace{\alpha(1) + \cdots + \alpha(1)}_{k} & \text{if } k > 0, \\ -(\underbrace{\alpha(1) + \cdots + \alpha(1)}_{-k}) & \text{if } k < 0, \\ \alpha(0) & \text{if } k = 0 \end{cases} \\
&= \begin{cases} \underbrace{1 + \cdots + 1}_{k} & \text{if } k > 0, \\ -(\underbrace{1 + \cdots + 1}_{-k}) & \text{if } k < 0, \\ 0 & \text{if } k = 0 \end{cases} \\
&= k1.
\end{aligned}$$

Thus $\alpha = \mathrm{id}$.

(ii) For $\alpha \in \mathrm{Aut}(S)$, $\alpha(1) = 1$ and a similar argument to that for (i) shows that $\alpha(r) = r$ for all $r \in R$. □

1.55. Proposition. *Let $D$ be an integral domain and $\alpha\colon D \longrightarrow D$ be an automorphism. Then the induced homomorphism gives an automorphism $\alpha_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$.*

Proof. Given $\alpha$, the induced homomorphism $\alpha_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$ exists and we need to show it has an inverse. The inverse automorphism $\alpha^{-1}\colon D \longrightarrow D$ also gives rise to an induced homomorphism $(\alpha^{-1})_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$. Since $\alpha^{-1} \circ \alpha = \mathrm{id} = \alpha \circ \alpha^{-1}$, we can apply Corollary 1.20 to show that

$$(\alpha^{-1})_* \circ (\alpha)_* = \mathrm{id} = (\alpha)_* \circ (\alpha^{-1})_*.$$

Hence $(\alpha)_*$ is invertible with inverse $(\alpha^{-1})_*$. □

1.56. Corollary. *There is a monomorphism of groups*

$$(\ )_*\colon \mathrm{Aut}(D) \longrightarrow \mathrm{Aut}(\mathrm{Fr}(D)); \quad \alpha \longmapsto \alpha_*.$$

1.57. Example. The field of fractions of the ring of integers $\mathbb{Z}$ is the field of rationals $\mathbb{Q}$. The homomorphism

$$(\ )_*\colon \mathrm{Aut}(\mathbb{Z}) \longrightarrow \mathrm{Aut}(\mathbb{Q}); \quad \alpha \longmapsto \alpha_*$$

is an isomorphism and hence $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$.

Combining this example with Proposition 1.54(ii) we obtain another useful result.

1.58. Proposition. *Let $\Bbbk$ be one of the prime fields $\mathbb{Q}$ or $\mathbb{F}_p$ with $p > 0$ prime. If $R$ is a ring containing $\Bbbk$ as a subring, then every automorphism of $R$ restricts to the identity on $\Bbbk$,* i.e., $\mathrm{Aut}(R) = \mathrm{Aut}_{\Bbbk}(R)$.

Recalling Definition 1.36, we have an example which shows that the monomorphism of Corollary 1.56 need not be an epimorphism. Here we take $D = \mathbb{Q}[X]$ and $\mathrm{Fr}(\mathbb{Q}[X]) = \mathbb{Q}(X)$.

1.59. Example. The homomorphism

$$(\ )_*\colon \mathrm{Aut}(\mathbb{Q}[X]) \longrightarrow \mathrm{Aut}(\mathbb{Q}(X)); \quad \alpha \longmapsto \alpha_*$$

is a monomorphism but it is not an epimorphism since there is an automorphism

$$\gamma\colon \mathbb{Q}(X) \longrightarrow \mathbb{Q}(X); \quad \gamma(f(X)) = f(1/X)$$

which sends $X \in \mathbb{Q}[X] \subseteq \mathbb{Q}(X)$ to $1/X \notin \mathbb{Q}[X]$ and so does not restrict to an automorphism of $\mathbb{Q}[X]$.

Let $\Bbbk$ be a field. The group of invertible $2 \times 2$ matrices over $\Bbbk$ is the $2 \times 2$ *general linear group over* $\Bbbk$,

$$\mathrm{GL}_2(\Bbbk) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} : a_{ij} \in \Bbbk,\ a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}$$

The scalar matrices form a normal subgroup

$$\mathrm{Scal}_2(\Bbbk) = \{\mathrm{diag}(t,t) : t \in \Bbbk,\ t \neq 0\} \lhd \mathrm{GL}_2(\Bbbk).$$

The quotient group is called the $2 \times 2$ *projective general linear group over* $\Bbbk$,

$$\mathrm{PGL}_2(\Bbbk) = \mathrm{GL}_2(\Bbbk)/\,\mathrm{Scal}_2(\Bbbk).$$

Notice that $\mathrm{GL}_2(\Bbbk)$ has another interesting subgroup called the *affine subgroup*,

$$\mathrm{Aff}_1(\Bbbk) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \Bbbk,\ a \neq 0 \right\} \leqslant \mathrm{GL}_2(\Bbbk).$$

1.60. Example. Let $\Bbbk$ be a field and $X$ an indeterminate. Then $\mathrm{Aut}_{\Bbbk}(\Bbbk[X])$ and hence $\mathrm{Aut}_{\Bbbk}(\Bbbk(X))$, contains a subgroup isomorphic to $\mathrm{Aff}_1(\Bbbk)$. In fact, $\mathrm{Aut}_{\Bbbk}(\Bbbk[X]) \cong \mathrm{Aff}_1(\Bbbk)$.

Proof. We begin by showing that to each affine matrix

$$A = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in \mathrm{Aff}_1(\Bbbk)$$

there is an associated automorphism $\alpha_A \colon \Bbbk[X] \longrightarrow \Bbbk[X]$.

For this we use the element $aX + b \in \Bbbk[X]$ together with the extension result of Theorem 1.22(i) to obtain a homomorphism $\alpha_A \colon \Bbbk[X] \longrightarrow \Bbbk[X]$ with $\alpha_A(X) = aX + b$. Using the inverse matrix

$$A^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{bmatrix}$$

we similarly obtain a homomorphism $\alpha_{A^{-1}} \colon \Bbbk[X] \longrightarrow \Bbbk[X]$ for which

$$\alpha_{A^{-1}}(X) = a^{-1}X - a^{-1}b.$$

Using the same line of argument as in the proof of Proposition 1.55 (or doing a direct calculation) we see that $\alpha_{A^{-1}}$ is the inverse of $\alpha_A$ an so $\alpha_A \in \mathrm{Aut}_{\Bbbk}(\Bbbk[X])$. It is straightforward to check that for $A_1, A_2 \in \mathrm{Aff}_1(\Bbbk)$,

$$\alpha_{A_2A_1} = \alpha_{A_1} \circ \alpha_{A_2},$$

(note the order!) hence there is a homomorphism of groups

$$\mathrm{Aff}_1(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk[X]); \quad A \longmapsto \alpha_{A^{-1}},$$

which is easily seen to be a monomorphism. Composing with $(\ )_*$ we see that there is a monomorphism $\mathrm{Aff}_1(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$. In fact, this is also an epimorphism and we leave the proof of this as an exercise. □

1.61. Example. Let $\Bbbk$ be a field and $X$ an indeterminate. Then

(i) $\mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ contains a subgroup isomorphic to $\mathrm{PGL}_2(\Bbbk)$.
(ii) In fact, $\mathrm{Aut}_{\Bbbk}(\Bbbk(X)) \cong \mathrm{PGL}_2(\Bbbk)$.

Proof. (i) We begin by showing that to each invertible matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(\Bbbk)$$

there is an associated automorphism $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$.

We begin by choosing the element $(a_{11}X + a_{12})/(a_{21}X + a_{22}) \in \Bbbk(X)$ and then using Theorem 1.22(i) to obtain a homomorphism $\Bbbk[X] \longrightarrow \Bbbk(X)$ that sends $X$ to $(a_{11}X+a_{12})/(a_{21}X+a_{22})$. By applying $(\ )_*$ to this we obtain a homomorphism (known as a *fractional linear transformation*) $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$ for which

$$\alpha^A(X) = \frac{a_{11}X + a_{12}}{a_{21}X + a_{22}}\,.$$

Again we find that

$$\alpha^{A_2A_1} = \alpha^{A_1} \circ \alpha^{A_2}.$$

There is an associated homomorphism of groups $\mathrm{GL}_2(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ sending $A$ to $\alpha^{A^{-1}}$. However, this is not an injection in general since for each scalar matrix $\mathrm{diag}(t,t)$,

$$\alpha^{\mathrm{diag}(t,t)}(X) = \frac{tX}{t} = X,$$

showing that $\alpha^{\mathrm{diag}(t,t)}$ is the identity function.

In fact it is easy to see that $\mathrm{Scal}_2(\Bbbk) \lhd \mathrm{GL}_2(\Bbbk)$ is the kernel of this homomorphism. Therefore passing to the quotient $\mathrm{PGL}_2(\Bbbk) = \mathrm{GL}_2(\Bbbk)/\mathrm{Scal}_2(\Bbbk)$ we obtain a monomorphism $\mathrm{PGL}_2(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$. There is one case where $\mathrm{Scal}_2(\Bbbk)$ is the trivial group, namely $\Bbbk = \mathbb{F}_2$.

(ii) To show that every automorphism of $\Bbbk(X)$ is a fractional linear transformation is less elementary. We give a sketch proof for the case of $\Bbbk = \mathbb{C}$; actually this argument can be modified to work for any *algebraically closed* field, but an easy argument then shows the general case.

Let $\alpha \in \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(X))$. There is an associated rational (hence meromorphic) function $f$ given by $z \longmapsto f(z)$, where $\alpha(X) = f(X)$, defined on $\mathbb{C}$ with the poles of $f$ deleted. If we write

$$f(X) = \frac{p(X)}{q(X)}$$

where $p(X), q(X) \in \mathbb{C}[X]$ have no common factors of positive degree, then the *order* of $f(X)$ is

$$\mathrm{ord}\, f = \max\{\deg p(X), \deg q(X)\}.$$

Now let $c \in \mathbb{C}$. Then the number of solutions counted with algebraic multiplicity of the equation $f(z) = c$ turns out to be $\mathrm{ord}\, f$. Also, if $\deg p(X) \leqslant \deg q(X)$ then the number of poles of $f$ counted with algebraic multiplicity is also $\mathrm{ord}\, f$. Finally, if $\deg p(X) > \deg q(X)$ then we can write

$$f(X) = p_1(X) + \frac{p_0(X)}{q(X)},$$

where $p_0(X), p_1(X) \in \mathbb{C}[X]$ and $\deg p_0(X) < \deg q(X)$. Then the number of poles of $f$ counted with algebraic multiplicity is

$$\deg p_1(X) + \mathrm{ord}\, \frac{p_0}{q}.$$

Now it is easy to see that since $\alpha$ is invertible so is the function $f$. But this can only happen if the function $f$ is injective which means that all of these numbers must be 1, hence $\mathrm{ord}\, f = 1$. Thus

$$f(X) = \frac{aX + b}{cX + d} \neq \text{constant}$$

and the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ must be invertible. □

Clearly not every fractional linear transformation $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$ maps polynomials to polynomials so $(\ )_* \colon \mathrm{Aut}_{\Bbbk}(\Bbbk[X]) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ is not an epimorphism.

Now we turn to a more familiar field $\mathbb{R}$, the real numbers.

1.62. Proposition. *The only automorphism of the field $\mathbb{R}$ is the identity function, hence* $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.

PROOF. First we note that $\mathbb{Q} \subseteq \mathbb{R}$ is a subring and if $\alpha \in \mathrm{Aut}(\mathbb{R})$ then $\alpha(q) = q$ for $q \in \mathbb{Q}$ by Example 1.57.

We recall from Analysis that the rational numbers are *dense* in the real numbers in the sense that each $r \in \mathbb{R}$ can be expressed as a limit $r = \lim_{n\to\infty} q_n$, where $q_n \in \mathbb{Q}$. Then for a continuous function $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, its value at $r$ depends on its values on $\mathbb{Q}$ since

$$f(r) = f(\lim_{n\to\infty} q_n) = \lim_{n\to\infty} f(q_n).$$

We will show that an automorphism $\alpha \in \mathrm{Aut}(\mathbb{R})$ is continuous.

First recall that for $x, y \in \mathbb{R}$,

$$x < y \iff 0 < y - x \iff y - x = t^2 \text{ for some non-zero } t \in \mathbb{R}.$$

Now for $\alpha \in \mathrm{Aut}(\mathbb{R})$ and $s \in \mathbb{R}$, we have $\alpha(s^2) = \alpha(s)^2$. Hence,

$$x < y \Longrightarrow \alpha(y) - \alpha(x) = \alpha(t)^2 \text{ for some non-zero } t \in \mathbb{R} \Longrightarrow \alpha(x) < \alpha(y).$$

So $\alpha$ preserves order and fixes rational numbers.

Now let $x \in \mathbb{R}$ and $\varepsilon > 0$. Then we can choose a rational number $q$ such that $0 < q \leqslant \varepsilon$. Taking $\delta = q$ we find that for $y \in \mathbb{R}$ with $|y - x| < \delta$ (*i.e.*, $-\delta < y - x < \delta$) we have

$$-\delta = \alpha(-\delta) < \alpha(y) - \alpha(x) < \alpha(\delta) = \delta,$$

hence

$$|\alpha(y) - \alpha(x)| < \delta \leqslant \varepsilon.$$

This shows that $\alpha$ is continuous at $x$.

Thus every automorphism of $\mathbb{R}$ is continuous function which fixes all the rational numbers, hence it must be the identity function. □

1.63. REMARK. If we try to determine $\mathrm{Aut}(\mathbb{C})$ the answer turns out to be much more complicated. It is easy to see that complex conjugation $\overline{(\ )}\colon \mathbb{C} \longrightarrow \mathbb{C}$ is an automorphism of $\mathbb{C}$ and fixes every real number, *i.e.*, $\overline{(\ )} \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$; in fact, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \overline{(\ )}\}$. However, it is *not* true that every $\alpha \in \mathrm{Aut}(\mathbb{C})$ fixes every real number! The automorphism group $\mathrm{Aut}(\mathbb{C})$ is actually enormous but it is hard to find an explicit element other than id and $\overline{(\ )}$. Note that given an automorphism $\alpha \in \mathrm{Aut}(\mathbb{C})$, the composition $\alpha \circ \overline{(\ )} \circ \alpha^{-1}$ is also self inverse, so there are many elements of order 2 in the group $\mathrm{Aut}(\mathbb{C})$.

## Exercises for Chapter 1

**1.1** Let $R$ be a ring. Show that

$$\{n \in \mathbb{Z} : n > 0 \text{ and } n1 = 0\} = \{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

Deduce that if $\operatorname{char} R > 0$ then these sets are non-empty and

$$\operatorname{char} R = \min\{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

**1.2** Let $R$ be an integral domain.

(a) Show that every subring $S \subseteq R$ is also an integral domain. What is the relationship between $\operatorname{char} S$ and $\operatorname{char} R$?

(b) If $R$ is a field, give an example to show that a subring of $R$ need not be a field.

**1.3** For each of the following rings $R$, find the characteristic $\operatorname{char} R$ and the characteristic subring of $R$. Determine which of these rings is an integral domain. In (b) and (c), $A$ is an arbitrary commutative ring.

(a) Any subring $R \subseteq \mathbb{C}$.

(b) The polynomial ring $R = A[X]$.

(c) The ring of $n \times n$ matrices over $A$,

$$R = \operatorname{Mat}_n(A) = \left\{ \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} : a_{ij} \in A \right\}.$$

**1.4** If $R$ is a commutative ring with unit containing the prime field $\mathbb{F}_p$ for some prime $p > 0$, show that the function $\varphi\colon R \longrightarrow R$ given by $\varphi(t) = t^p$, defines a ring homomorphism. Give examples to show that $\varphi$ need not be surjective or injective.

**1.5** Let $R$ and $S$ be rings with unity and $Q \lhd S$ a prime ideal.

(a) If $\varphi\colon R \longrightarrow S$ is a ring homomorphism, show that

$$\varphi^{-1}Q = \{r \in R : \varphi(r) \in Q\} \subseteq R$$

is a prime ideal of $R$.

(b) If $R \subseteq S$ is a subring, show that $Q \cap R$ is a prime ideal of $R$.

(c) If the word 'prime' is replaced by 'maximal' throughout, are the results in parts (a) and (b) still true? [*Hint: look for a counterexample.*]

(d) If $R \subseteq S$ is a subring and $P \lhd R$ is a maximal ideal, suppose that $Q \lhd S$ is a prime ideal for which $P \subseteq Q$. Show that $Q \cap R = P$.

**1.6** Let $\Bbbk$ be a field, $R$ be a ring with unit and let $\varphi\colon \Bbbk \longrightarrow R$ be a ring homomorphism. Show that $\varphi$ is a monomorphism.

**1.7** Consider the sets

$$\mathbb{Z}(i) = \{u + vi : u, v \in \mathbb{Z}\} \subseteq \mathbb{C}, \quad \mathbb{Q}(i) = \{u + vi : u, v \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

(a) Show that $\mathbb{Z}(i)$ and $\mathbb{Q}(i)$ are subrings of $\mathbb{C}$. Also show that $\mathbb{Z}(i)$ is an integral domain, $\mathbb{Q}(i)$ is a field and $\mathbb{Z}(i)$ is a subring of $\mathbb{Q}(i)$.

(b) Show that the inclusion homomorphism $\mathrm{inc}\colon \mathbb{Z}(i) \longrightarrow \mathbb{Q}(i)$ extends to a monomorphism $\mathrm{inc}_*\colon \mathrm{Fr}(\mathbb{Z}(i)) \longrightarrow \mathbb{Q}(i)$.

(c) Show that $\mathrm{inc}_*$ is an isomorphism, so $\mathrm{Fr}(\mathbb{Z}(i)) = \mathbb{Q}(i)$.

**1.8** Let $R$ be a commutative ring.

(a) If $a, b \in R$, show that there is a unique ring homomorphism $\psi_{a,b}\colon R[X] \longrightarrow R[X]$ for which $\psi_{a,b}(r) = r$ if $r \in R$ and $\psi_{a,b}(X) = aX + b$. If $c, d \in R$, determine $\psi_{a,b} \circ \psi_{c,d}$. If $a$ is a unit, show that $\psi_{a,b}$ is an isomorphism and find its inverse.

(b) Now suppose that $R = \Bbbk$ is a field and $a, b \in \Bbbk$ with $a \neq 0$. Prove the following.

(i) If $f(X) \in \Bbbk[X]$, the $\deg \psi_{a,b}(f(X)) = \deg f(X)$.

(ii) If $p(X) \in \Bbbk[X]$ is a prime then so is $\psi_{a,b}(p(X))$.

(iii) If $p(X) \in \Bbbk[X]$ is an irreducible then so is $\psi_{a,b}(p(X))$.

**1.9** Let $\Bbbk$ be a field and $\Bbbk[[X]]$ be the set consisting of all power series

$$\sum_{k=0}^{\infty} a_k X^k = a_0 + a_1 X + \cdots + a_k X^k + \cdots ,$$

with $a_k \in \Bbbk$.

(a) Show that this can be made into an integral domain containing $\Bbbk[X]$ as a subring by defining addition and multiplication in the obvious way.

(b) Show that $\sum_{k=0}^{\infty} a_k X^k \in \Bbbk[[X]]$ is a unit if and only if $a_0 \neq 0$.

(c) Show that $\mathrm{Fr}(\Bbbk[[X]])$ consists of all *finite-tailed Laurent series*

$$\sum_{k=\ell}^{\infty} a_k X^k = a_\ell X^\ell + a_{\ell+1} X^{\ell+1} + \cdots + a_k X^k + \cdots$$

for some $\ell \in \mathbb{Z}$ and $a_{\Bbbk} \in \Bbbk$.

**1.10** Taking $\Bbbk = \mathbb{Q}$, find the quotient and remainder when performing long division of $f(X) = 6X^4 - 6X^3 + 3X^2 - 3X - 2$ by $d(X) = 2X^3 + X + 3$.

**1.11** Taking $\Bbbk = \mathbb{F}_3$, find the quotient and remainder when performing long division of $f(X) = 2X^3 + 2X^2 + X + 1$ by $d(X) = 2X^3 + 2X$.

**1.12** Let $p > 0$ be a prime. Suppose that $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ with $p \nmid a_n$ and that $\overline{f(X)} \in \mathbb{F}_p[X]$ denotes the polynomial obtained by reducing the coefficients of $f(X)$ modulo $p$. If $\overline{f(X)}$ is irreducible, show that $f(X)$ is irreducible. Which of the following polynomials in $\mathbb{Z}[X]$ is irreducible?

$$X^3 - X + 1,\ X^3 + 2X + 1,\ X^3 + X - 1,\ X^5 - X + 1,\ X^5 + X - 1,\ 5X^3 - 10X + X^2 - 2.$$

**1.13** Find generators for each of the following ideals:

$$I_1 = \{f(X) \in \mathbb{Q}[X] : f(i) = 0\} \lhd \mathbb{Q}[X], \qquad I_2 = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}\, i) = 0\} \lhd \mathbb{Q}[X],$$
$$I_3 = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}\,) = 0\} \lhd \mathbb{Q}[X], \qquad I_4 = \{f(X) \in \mathbb{R}[X] : f(\sqrt{2}\,) = 0\} \lhd \mathbb{R}[X],$$
$$I_5 = \{f(X) \in \mathbb{R}[X] : f(\sqrt{2}\, i) = 0\} \lhd \mathbb{R}[X], \qquad I_6 = \{f(X) \in \mathbb{R}[X] : f(\zeta_3) = 0\} \lhd \mathbb{R}[X].$$

**1.14** Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_{\sqrt{2}}\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$. Determine the image $\varepsilon_{\sqrt{2}}\,\mathbb{Q}[X] \subseteq \mathbb{C}$. What is $\varepsilon_{-\sqrt{2}}\,\mathbb{Q}[X] \subseteq \mathbb{C}$? Find $\ker \varepsilon_{\sqrt{2}} \lhd \mathbb{Q}[X]$ and $\ker \varepsilon_{-\sqrt{2}} \lhd \mathbb{Q}[X]$. Are these ideals maximal?

**1.15** Let $\omega = (-1 + \sqrt{3}\,i)/2 \in \mathbb{C}$. Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_\omega\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$. Determine the image $\varepsilon_\omega\,\mathbb{Q}[X] \subseteq \mathbb{C}$. Determine $\ker \varepsilon_\omega \lhd \mathbb{Q}[X]$ and decide whether it is maximal. Find another evaluation homomorphism with the same kernel and image.

**1.16** Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_\alpha\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$ where $\alpha$ is one of the 4 complex roots of the polynomial $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. Determine the image $\varepsilon_\alpha\,\mathbb{Q}[X] \subseteq \mathbb{C}$ and the ideal $\ker \varepsilon_\alpha \lhd \mathbb{Q}[X]$; is the latter ideal maximal? What happens if $\alpha$ is replaced by one of the other roots of $f(X)$?

Repeat this problem starting with the inclusion of the real numbers into the complex numbers $\mathrm{inc}\colon \mathbb{R} \longrightarrow \mathbb{C}$ and $\varepsilon_\alpha\colon \mathbb{R}[X] \longrightarrow \mathbb{C}$.

**1.17** Use Cardan's method to find the complex roots of the polynomial

$$f(X) = X^3 - 9X^2 + 21X - 5.$$

**1.18** Consider the real numbers

$$\alpha = \sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}\,, \quad \beta = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}\,.$$

Find rational cubic polynomials $f(X)$ and $g(X)$ for which $f(\alpha) = 0 = g(\beta)$. Hence determine these real numbers.

**1.19** Prove the final part of Example 1.60 by showing that there is an isomorphism of groups $\mathrm{Aff}_1(\Bbbk) \cong \mathrm{Aut}_\Bbbk(\Bbbk[X])$.

**1.20** Let $\Bbbk$ be any field. Consider the 6 automorphisms $\alpha_j\colon \Bbbk(X) \longrightarrow \Bbbk(X)$ $(j = 1, \ldots, 6)$ defined by

$$\begin{aligned}
&\alpha_1(f(X)) = f(X), && \alpha_2(f(X)) = f(1 - X), && \alpha_3(f(X)) = f(1/X),\\
&\alpha_4(f(X)) = f((X-1)/X), && \alpha_5(f(X)) = f(1/(1-X)), && \alpha_6(f(X)) = f(X/(X-1)).
\end{aligned}$$

Show that the set consisting of these elements is a subgroup $\Gamma_\Bbbk \leqslant \mathrm{Aut}_\Bbbk(\Bbbk(X))$ isomorphic to the symmetric group $\mathrm{S}_3$. When $\Bbbk = \mathbb{F}_2$, show that $\Gamma_\Bbbk \cong \mathrm{GL}_2(\Bbbk)$.

**1.21** Determine the cyclotomic polynomial $\Phi_{20}(X)$.

**1.22** Let $p > 0$ be a prime.

(a) Show that for $k \geqslant 1$, the cyclotomic polynomial $\Phi_{p^k}(X)$ satisfies

$$\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$$

and has as its complex roots the primitive $p^k$-th roots of 1.

(b) Show that $\Phi_{p^k}(X) \in \mathbb{Q}[X]$ is irreducible.

(c) Generalize part (a) to show that if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime power factorization of $n$ with the $p_i$ being distinct primes and $r_i > 0$, then

$$\Phi_n(X) = \Phi_{p_1 \cdots p_k}(X^{p_1^{r_1 - 1} \cdots p_k^{r_k - 1}}).$$

**1.23** For $n \geqslant 2$, show that

$$X^{\varphi(n)}\Phi_n(X^{-1}) = \Phi_n(X).$$

**1.24** Show that for $n \geqslant 1$, $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$.
Find expressions for $\zeta_5+\zeta_5^{-1}$ and $\zeta_5^2+\zeta_5^{-2}$ in terms of $\cos(2\pi/5)$. Hence find a rational polynomial which has $\cos(2\pi/5)$ as a root.

**1.25** Let $p > 0$ be a prime and $K$ be a field with $\operatorname{char} K = p$.

(a) Show that if $\zeta \in K$ is a $p$-th root of 1 then $\zeta = 1$. Deduce that if $m, n > 0$ and $p \nmid n$, then every $np^m$-th root of 1 in $K$ is an $n$-th root of 1.

(b) If $a \in K$, show that the polynomial $X^p - a \in K[X]$ has either no roots or exactly one root in $K$.

CHAPTER 2

# Fields and their extensions

## 2.1. Fields and subfields

2.1. Definition. Let $K$ and $L$ be fields and suppose that $K \subseteq L$ is a subring. Then we say that $K$ is a *subfield* of $L$; $L$ is also said to be an *extension* (*field*) of $K$. We write $K \leqslant L$ or $L/K$ to indicate this, and write $K < L$ if $K$ is a proper subfield of $L$, *i.e.*, if $K \neq L$.

An important fact about an extension of fields $L/K$ is that $L$ is a $K$-vector space whose addition is the addition in the field $L$ while scalar multiplication is defined by

$$u \cdot x = ux \quad (u \in K,\ x \in L).$$

2.2. Definition. We will call $\dim_K L$ the *degree* or *index* of the extension $L/K$ and use the notation $[L : K] = \dim_K L$. An extension of fields $L/K$ is *finite* (*dimensional*) if $[L : K] < \infty$, otherwise it is *infinite* (*dimensional*).

2.3. Example. Show that the extension $\mathbb{C}/\mathbb{R}$ is finite, while $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ are both infinite.

Solution. We have

$$\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\},$$

so $1, i$ span $\mathbb{C}$ as a vector space over $\mathbb{R}$. Since $i \notin \mathbb{R}$, these elements are also linearly independent over $\mathbb{R}$ and therefore they form a basis, whence $[\mathbb{C} : \mathbb{R}] = 2$. The infiniteness of $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ are consequences of the fact that any finite dimensional vector space over $\mathbb{Q}$ is *countable*, however $\mathbb{R}$ and $\mathbb{C}$ are uncountable. A basis for the $\mathbb{Q}$-vector space $\mathbb{R}$ is known as a *Hamel basis*. □

2.4. Example. Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ where

$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} : x, y \in \mathbb{Q}\}.$$

Show that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Solution. The elements $1, \sqrt{2}$ clearly span the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{2})$. Now recall that $\sqrt{2} \notin \mathbb{Q}$. If the elements $1, \sqrt{2}$ were linearly dependent we would have $u + v\sqrt{2} = 0$ for some $u, v \in \mathbb{Q}$ not both zero; in fact it is easy to see that we would then also have $u, v$ both non-zero. Thus we would have

$$\sqrt{2} = -\frac{u}{v} \in \mathbb{Q},$$

which we know to be false. Hence $1, \sqrt{2}$ are linearly independent and so form a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. □

If we have two extensions $L/K$ and $M/L$ then it is a straightforward to verify that $K \leqslant M$ and so we have another extension $M/K$.

2.5. Definition. Given two extensions $L/K$ and $M/L$, we say that $L/K$ is a *subextension of* $M/K$ and sometimes write $L/K \leqslant M/K$.

2.6. THEOREM. *Let $L/K$ be a subextension of $M/K$.*

(i) *If one or both of the dimensions $[L:K]$ or $[M:L]$ is infinite then so is $[M:K]$.*

(ii) *If the dimensions $[L:K]$ and $[M:L]$ are both finite then so is $[M:K]$ and*

$$[M:K] = [M:L]\,[L:K].$$

PROOF. (i) If $[M:K]$ is finite, choose a basis $m_1, \ldots, m_r$ of $M$ over $K$. Now any element $u \in M$ can be expressed as

$$u = t_1 m_1 + \cdots + t_r m_r,$$

where $t_1, \ldots, t_r \in K$; but since $K \subseteq L$, this means that $m_1, \ldots, m_r$ spans $M$ over $L$ and so $[M:L] < \infty$. Also $L$ is a $K$-vector subspace of the finite dimensional $K$-vector space $M$, hence $[L:K] < \infty$.

(ii) Setting $r = [L:K]$ and $s = [M:L]$, choose a basis $\ell_1, \ldots, \ell_r$ of $L$ over $K$ and a basis $m_1, \ldots, m_s$ of $M$ over $L$.

Now let $v \in M$. Then there are elements $y_1, \ldots, y_s \in L$ for which

$$v = y_1 m_1 + \cdots + y_s m_s.$$

But each $y_j$ can be expressed in the form

$$y_j = x_{1j}\ell_1 + \cdots + x_{rj}\ell_r$$

for suitable $x_{ij} \in K$. Hence,

$$v = \sum_{j=1}^{s} \left( \sum_{i=1}^{r} x_{ij}\ell_i \right) m_j = \sum_{j=1}^{s} \sum_{i=1}^{r} x_{ij}(\ell_i m_j),$$

where each coefficient $x_{ij}$ is in $K$. Thus the elements $\ell_i m_j$ $(i = 1, \ldots, r,\ j = 1, \ldots, s)$ span the $K$-vector space $M$.

Now suppose that for some $t_{ij} \in K$ we have

$$\sum_{j=1}^{s} \sum_{i=1}^{r} t_{ij}(\ell_i m_j) = 0.$$

On collecting terms we obtain

$$\sum_{j=1}^{s} \left( \sum_{i=1}^{r} t_{ij}\ell_i \right) m_j = 0,$$

where each coefficient $\sum_{i=1}^{r} t_{ij}\ell_i$ is in $L$. By the linear independence of the $m_j$ over $L$, this means that for each $j$,

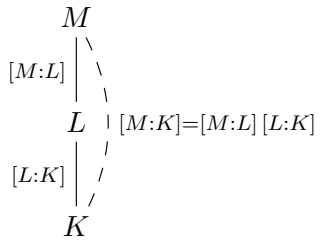
$$\sum_{i=1}^{r} t_{ij}\ell_i = 0.$$

By the linear independence of the $\ell_i$ over $K$, each $t_{ij} = 0$.

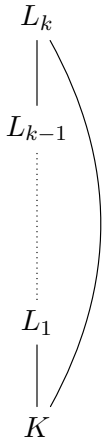
Hence the $\ell_i m_j$ form a basis of $M$ over $K$ and so

$$[M:K] = rs = [M:L]\,[L:K]. \qquad \square$$

We will often indicate subextensions in diagrammatic form where larger fields always go above smaller ones and the information on the lines indicates dimensions




We often suppress 'composite' lines such as the dashed one. Such *towers of extensions* are our main objects of study. We can build up sequences of extensions and form towers of arbitrary length. Thus, if $L_1/K,\ L_2/L_1, \ldots,\ L_k/L_{k-1}$ is a such a sequence of extensions, there is a diagram




## 2.2. Simple and finitely generated extensions

2.7. Definition. Let $F$ be a field and $K \leqslant F$. Given elements $u_1, \ldots, u_r \in F$ we set

$$K(u_1, \ldots, u_r) = \bigcap_{\substack{K \leqslant L \leqslant F \\ u_1, \ldots, u_r \in L}} L$$

which is the smallest subfield in $F$ that contains $K$ and the elements $u_1, \ldots, u_r$. The extension $K(u_1, \ldots, u_r)/K$ is said to be *generated* by the elements $u_1, \ldots, u_r$; we also say that $K(u_1, \ldots, u_r)/K$ is a *finitely generated* extension of $K$. An extension of the form $K(u)/K$ is called a *simple extension of $K$ with generator $u$*.

We can extend this to the case of an infinite sequence $u_1, \ldots, u_r, \ldots$ in $F$ and denote by $K(u_1, \ldots, u_r, \ldots) \leqslant F$ the smallest extension field of $K$ containing all the elements $u_r$.

It can be shown that

(2.1) $K(u_1, \ldots, u_r) =$

$$\left\{ \frac{f(u_1, \ldots, u_r)}{g(u_1, \ldots, u_r)} \in F : f(X_1, \ldots, X_r), g(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r],\ g(u_1, \ldots, u_r) \neq 0 \right\}.$$

Reordering the $u_i$ does not change $K(u_1, \ldots, u_n)$.

2.8. Proposition. *Let $K(u)/K$ and $K(u,v)/K(u)$ be simple extensions. Then*

$$K(u,v) = K(u)(v) = K(v)(u).$$

*More generally,*

$$K(u_1,\dots,u_n) = K(u_1,\dots,u_{n-1})(u_n)$$

*and this is independent of the order of the sequence $u_1,\dots,u_n$.*

2.9. Theorem. *For a simple extension $K(u)/K$, exactly one of the following conditions holds.*

(i) *The evaluation at $u$ homomorphism $\varepsilon_u\colon K[X] \longrightarrow K(u)$ is a monomorphism and on passing to the fraction field gives an isomorphism $(\varepsilon_u)_*\colon K(X) \longrightarrow K(u)$. In this case, $K(u)/K$ is infinite and $u$ is said to be* transcendental over $K$.

(ii) *The evaluation at $u$ homomorphism $\varepsilon_u\colon K[X] \longrightarrow K(u)$ has a non-trivial kernel $\ker\varepsilon_u = (p(X))$ where $p(X) \in K[X]$ is an irreducible monic polynomial of positive degree and the quotient homomorphism $\widetilde{\varepsilon}_u\colon K[X]/(p(X)) \longrightarrow K(u)$ is an isomorphism. In this case $K(u)/K$ is finite with $[K(u):K] = \deg p(X)$ and $u$ is said to be* algebraic over $K$.

Proof. (i) If $\ker\varepsilon_u = (0)$, all that needs checking is that $(\varepsilon_u)_*$ is an epimorphism; but as $u$ is in the image of $(\varepsilon_u)_*$ this is obvious.
(ii) When $\ker\varepsilon_u \neq (0)$, Theorem 1.31(iv) implies that the image of $\varepsilon_u$ is a subfield of $K(u)$ and since it contains $u$ it must equal $K(u)$. Hence $\widetilde{\varepsilon}_u$ is an isomorphism. Using Long Division, we find that every element of $K[X]/(p(X))$ can be uniquely expressed as a coset of the form

$$f(X) + (p(X)),$$

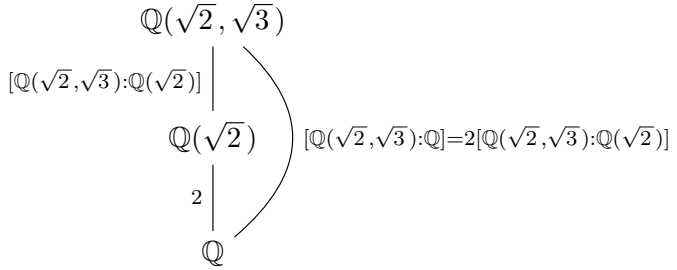
where $\deg f(X) < \deg p(X)$. Hence every element of $K[X]/(p(X))$ can be uniquely expressed as a linear combination over $K$ of the $d$ cosets

$$1 + (p(X)),\ X + (p(X)),\ X^2 + (p(X)),\dots,\ X^{d-1} + (p(X)),$$

where $d = \deg p(X)$. Via the isomorphism $\widetilde{\varepsilon}_u$ under which $\widetilde{\varepsilon}_u(X^k + (p(X))) = u^k$, we see that the elements $1, u, \dots, u^{d-1}$ form a basis for $K(u)$ over $K$. □

2.10. Example. For the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

Proof. By Example 2.4 we know that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. We have the following tower of extensions.




We will show that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$.

Notice that if $u \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ then $u = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}(\sqrt{2})$, so $1, \sqrt{3}$ span $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. But if these are linearly dependent then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Writing

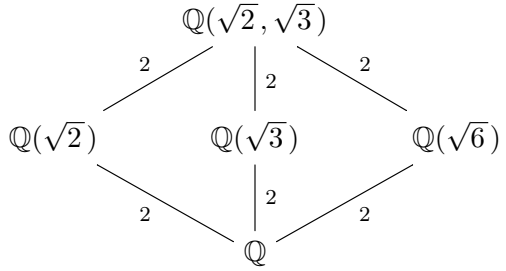
$$\sqrt{3} = v + w\sqrt{2}$$

with $v, w \in \mathbb{Q}$, we find that

$$v^2 + 2w^2 + 2vw\sqrt{2} = 3 \in \mathbb{Q},$$

and hence $2vw\sqrt{2} \in \mathbb{Q}$. The possibilities $v = 0$ or $w = 0$ are easily ruled out, while $v, w \neq 0$ would implies that $\sqrt{2} \in \mathbb{Q}$ which is false. So $1, \sqrt{3}$ are linearly independent over $\mathbb{Q}(\sqrt{2})$ and therefore form a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This shows that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. □

2.11. Remark. There are some other subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which are conveniently displayed in the following diagram.




One idea in the verification of Example 2.10 can be extended to provide a useful general result whose proof is left as an exercise.

2.12. Proposition. *Let $p_1, \ldots, p_n$ be a sequence of distinct primes $p_i > 0$. Then*

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}).$$

*Hence $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})] = 2$ and $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.*

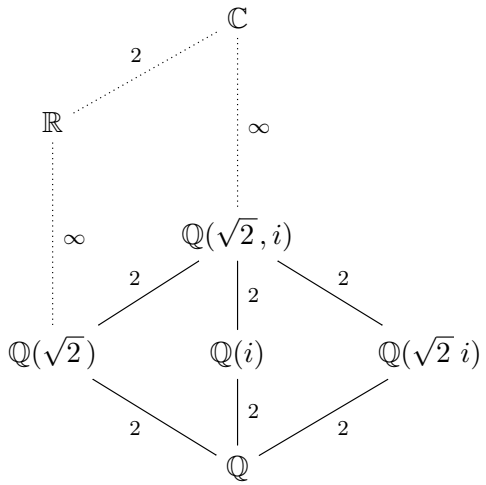
2.13. Example. For the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.

Proof. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Also, $i \notin \mathbb{Q}(\sqrt{2})$ since $i$ is not real and $\mathbb{Q}(\sqrt{2}) \leqslant \mathbb{R}$. Since $i^2 + 1 = 0$, we have $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$ and $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. Using the formula

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

we obtain $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. □

This example also has several other subfields, with only $\mathbb{Q}(\sqrt{2}\,) = \mathbb{Q}(\sqrt{2}\,, i) \cap \mathbb{R}$ being a subfield of $\mathbb{R}$.




2.14. Example. For $n \geqslant 1$, let $E_n = \mathbb{Q}(2^{1/n}) \leqslant \mathbb{R}$, where $2^{1/n} \in \mathbb{R}$ denotes the positive real $n$-th root of 2.

(i) Show that $[E_n : \mathbb{Q}] = n$.
(ii) If $m \geqslant 1$ with $m \mid n$, show that $E_m \leqslant E_n$ and determine $[E_n : E_m]$.
(iii) If $m, n$ are coprime, show that $E_{mn} = \mathbb{Q}(2^{1/m}, 2^{1/n})$.

Solution. (i) Consider the evaluation homomorphism $\varepsilon_{2^{1/n}} \colon \mathbb{Q}[X] \longrightarrow E_n$. Applying the Eisenstein Test 1.38 using the prime 2 to the polynomial $X^n - 2 \in \mathbb{Z}[X]$, we find that

$$\ker \varepsilon_{2^{1/n}} = (X^n - 2) \lhd \mathbb{Q}[X],$$

and the induced homomorphism $\widetilde{\varepsilon}_{2^{1/n}} \colon \mathbb{Q}[X]/(X^n - 2) \longrightarrow E_n$ is an isomorphism. Hence $[E_n : \mathbb{Q}] = n$.
(ii) Since $n/m$ is an integer,

$$2^{1/m} = (2^{1/n})^{n/m} \in E_n,$$

so

$$E_m = \mathbb{Q}(2^{1/m}) \subseteq E_n.$$

By Theorem 2.6 we have

$$n = [E_n : \mathbb{Q}] = [E_n : E_m]\,[E_m : \mathbb{Q}] = m[E_n : E_m],$$

whence $[E_n : E_m] = n/m$.
(iii) By (ii) we have $E_m \leqslant E_{mn}$ and $E_n \leqslant E_{mn}$, hence $\mathbb{Q}(2^{1/m}, 2^{1/n}) \leqslant E_{mn}$. As $\gcd(m, n) = 1$, there are integers $r, s$ for which $rm + sn = 1$ and so

$$\frac{1}{mn} = \frac{rm + sn}{mn} = \frac{r}{n} + \frac{s}{m}\,.$$

This shows that

$$2^{1/mn} = (2^{1/n})^r (2^{1/m})^s \in \mathbb{Q}(2^{1/m}, 2^{1/n}),$$

whence $E_{mn} \leqslant \mathbb{Q}(2^{1/m}, 2^{1/n})$. Combining these inclusions we obtain $E_{mn} = \mathbb{Q}(2^{1/m}, 2^{1/n})$. $\square$

## Exercises for Chapter 2

**2.1** Let $p \in \mathbb{N}$ be an prime. Show that the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ has $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

**2.2** Let $p, q > 0$ be distinct primes. Show that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$.

**2.3** Prove Proposition 2.12 by induction on $n$.

**2.4** Let $K$ a field with $\operatorname{char} K \neq 2$ and suppose that $L/K$ is an extension. If $a, b \in K$ are distinct, suppose that $u, v \in L$ satisfy $u^2 = a$ and $v^2 = b$. Show that $K(u, v) = K(u + v)$.
[*Hint: first show that* $u \pm v \neq 0$ *and deduce that* $u - v \in K(u+v)$*; then show that* $u, v \in K(u+v)$.]

**2.5** Show that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

**2.6** Show that $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$. Find the three subfields $L \leqslant \mathbb{Q}(\sqrt{3}, i)$ with $[L : \mathbb{Q}] = 2$ and display their relationship in a diagram, indicating which ones are subfields of $\mathbb{R}$.

**2.7** Let $\zeta_5 = e^{2\pi i/5} \in \mathbb{C}$.

(a) Explain why $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$.

(b) Show that $\cos(2\pi/5),\ \sin(2\pi/5)\, i \in \mathbb{Q}(\zeta_5)$.

(c) Show that for $t \in \mathbb{R}$,

$$\cos 5t = 16\cos^5 t - 20\cos^3 t + 5\cos t.$$

(d) Show that the numbers $\cos(2k\pi/5)$ with $k = 0, 1, 2, 3, 4$ are roots of the polynomial

$$f(X) = 16X^5 - 20X^3 + 5X - 1 = (X - 1)(4X^2 + 2X - 1)^2$$

and deduce that $[\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] = 2$.

(e) Display the relationship between the fields $\mathbb{Q}$, $\mathbb{Q}(\cos(2\pi/5))$, and $\mathbb{Q}(\zeta_5)$ in a suitable diagram.

**2.8** This question is for those who like lots of calculation or using Maple. Let $\zeta_7 = e^{2\pi i/7} \in \mathbb{C}$.

(a) Explain why $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$.

(b) Show that $\cos(2\pi/7),\ \sin(2\pi/7)\, i \in \mathbb{Q}(\zeta_7)$.

(c) Show

$$\cos 7t = 64\cos^7 t - 112\cos^5 t + 56\cos^3 t - 7\cos t.$$

Show that the numbers $\cos(2k\pi/7)$ with $k = 0, 1, \ldots, 6$ are roots of the polynomial

$$f(X) = 64X^7 - 112X^5 + 56X^3 - 7X - 1 = (X - 1)(8X^3 + 4X^2 - 4X - 1)^2$$

and deduce that $[\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 3$.

(d) Show that $\sin(2\pi/7)\, i$ is a root of

$$g(X) = 64X^7 + 112X^5 + 56X^3 + 7X = X(64X^6 + 112X^4 + 56X^2 + 7)$$

and that $64X^6 + 112X^4 + 56X^2 + 7 \in \mathbb{Q}[X]$ is irreducible. What is $[\mathbb{Q}(\sin(2\pi/7)\, i) : \mathbb{Q}]$?

(e) Display the relationship between the fields $\mathbb{Q}$, $\mathbb{Q}(\cos(2\pi/7))$, $\mathbb{Q}(\sin(2\pi/7)\, i)$ and $\mathbb{Q}(\zeta_7)$ in a diagram.

(f) Is $i \in \mathbb{Q}(\zeta_7)$?

**2.9** In this question we continue to consider the situation described in Example 2.14.

(a) Show that

$$\mathrm{Aut}_{\mathbb{Q}}(E_n) = \begin{cases} \{\mathrm{id}\} & \text{if } n \text{ is odd,} \\ \{\mathrm{id}, \tau_n\} \cong \mathbb{Z}/2 & \text{if } n \text{ is even,} \end{cases}$$

where $\tau_n$ has composition order 2.

(b) Let $E = \bigcup_{n \geqslant 1} E_n \leqslant \mathbb{R}$. Show that $\mathrm{Aut}_{\mathbb{Q}}(E) = \{\mathrm{id}\}$.

(c) Display the 6 subfields of $E_{12}$ in a diagram.

(d) Which of the subfields in part (c) contain the element $2^{1/2} + 2^{1/3}$ ?

CHAPTER 3

# Algebraic extensions of fields

## 3.1. Algebraic extensions

Let $L/K$ be an extension of fields. From Theorem 2.9(ii), recall the following notion.

3.1. Definition. An element $t \in L$ is *algebraic over* $K$ if there is a non-zero polynomial $p(X) \in K[X]$ for which $p(t) = 0$.

Notice in particular that for an element $t \in K$, the polynomial $p(X) = X - t \in K[X]$ satisfies $p(t) = 0$, so $t$ is algebraic over $K$.

Theorem 2.9 allows us to characterize algebraic elements in other ways.

3.2. Proposition. *Let $t \in L$. Then the following conditions are equivalent.*

(i) *$t$ is algebraic over $K$.*
(ii) *The evaluation homomorphism $\varepsilon_t \colon K[X] \longrightarrow L$ has non-trivial kernel.*
(iii) *The extension $K(t)/K$ is finite dimensional.*

3.3. Definition. If $t \in L$ is algebraic over $K$ then by Proposition 3.2,

$$\ker \varepsilon_t = (\operatorname{minpoly}_{K,t}(X)) \neq (0),$$

where $\operatorname{minpoly}_{K,t}(X) \in K[X]$ is an irreducible monic polynomial called the *minimal polynomial of $t$ over $K$*. The degree of $\operatorname{minpoly}_{K,t}(X)$ is called the *degree of $t$ over $K$* and is denoted $\deg_K t$.

3.4. Proposition. *If $t \in L$ is algebraic over $K$ then*

$$[K(t) : K] = \deg \operatorname{minpoly}_{K,t}(X) = \deg_K t.$$

Proof. This follows from Theorem 2.9(ii). □

3.5. Remark. Suppose that $t \in L$ is algebraic over $K$ and that $p(X) \in \ker \varepsilon_t$ with $\deg p(X) = \deg \operatorname{minpoly}_{K,t}(X)$. Then $\operatorname{minpoly}_{K,t}(X) \mid p(X)$ and so

$$p(X) = u \operatorname{minpoly}_{K,t}(X)$$

for some $u \in K$. In particular, when $p(X)$ is monic,

$$p(X) = \operatorname{minpoly}_{K,t}(X).$$

We will often use this without further comment.

3.6. Example. Consider $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$ is

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = X^2 - 2.$$

PROOF. Clearly $X^2-2 \in \ker \varepsilon_{\sqrt{2}}$ since $(\sqrt{2})^2-2=0$. By Example 2.4,

$$\deg \operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2,$$

hence

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = X^2-2. \qquad \square$$

3.7. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $i \in \mathbb{C}$ over $\mathbb{Q}$ is $X^2+1$.

PROOF. Clearly $X^2+1 \in \ker \varepsilon_i$ since $i^2+1=0$. As $[\mathbb{Q}(i):\mathbb{Q}]=2$, we have

$$\operatorname{minpoly}_{\mathbb{Q},i}(X) = X^2+1. \qquad \square$$

3.8. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. Find the minimal polynomial of the primitive 6-th root of unity, $\zeta_6 \in \mathbb{C}$ over $\mathbb{Q}$.

SOLUTION. Recall from Example 1.44 that $\zeta_6$ is a root of the irreducible cyclotomic polynomial

$$\Phi_6(X) = X^2 - X + 1.$$

Then $\Phi_6(X) \in \ker \varepsilon_{\zeta_6}$ so $\operatorname{minpoly}_{\mathbb{Q},\zeta_6}(X) \mid \Phi_6(X)$. Since $\Phi_6(X)$ is irreducible and monic, we must have

$$\operatorname{minpoly}_{\mathbb{Q},\zeta_6}(X) = \Phi_6(X)$$

and so $\deg_{\mathbb{Q}} \zeta_6 = 2$. $\square$

3.9. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

SOLUTION. Notice that

$$\sqrt{3}-\sqrt{2} = \frac{(\sqrt{3}-\sqrt{2})(\sqrt{3}+\sqrt{2})}{(\sqrt{3}+\sqrt{2})} = \frac{1}{\sqrt{2}+\sqrt{3}} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

So we have

$$\sqrt{2} = \frac{1}{2}\Big((\sqrt{2}+\sqrt{3})-(\sqrt{3}-\sqrt{2})\Big) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$
$$\sqrt{3} = \frac{1}{2}\Big((\sqrt{2}+\sqrt{3})+(\sqrt{3}-\sqrt{2})\Big) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$

hence $\mathbb{Q}(\sqrt{2},\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{2},\sqrt{3})$ we must have

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Referring to Example 2.10 we see that

$$\deg_{\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = 4.$$

Let us find a non-zero polynomial in $\ker \varepsilon_{\sqrt{2}+\sqrt{3}} \lhd \mathbb{Q}[X]$.

Referring to Example 2.10 or Proposition 2.12 we see that $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, hence

$$\deg_{\mathbb{Q}(\sqrt{2})}(\sqrt{2}+\sqrt{3}) = 2.$$

One polynomial in $\ker \varepsilon_{\sqrt{2}+\sqrt{3}} \lhd \mathbb{Q}(\sqrt{2})[X]$ is

$$(X-(\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3})) = X^2 - 2\sqrt{2}\,X - 1.$$

Since this is monic and of degree 2,

$$\operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),\sqrt{2}+\sqrt{3}}(X) = X^2 - 2\sqrt{2}\,X - 1.$$

Similarly,

$$\operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),-\sqrt{2}+\sqrt{3}}(X) = X^2 + 2\sqrt{2}\,X - 1.$$

Consider

$$\begin{aligned} p(X) &= \operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),\sqrt{2}+\sqrt{3}}(X)\operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),-\sqrt{2}+\sqrt{3}}(X) \\ &= (X^2 - 2\sqrt{2}\,X - 1)(X^2 + 2\sqrt{2}\,X - 1) \\ &= X^4 - 10X^2 + 1. \end{aligned}$$

Then $p(\sqrt{2}+\sqrt{3}) = 0$ so $p(X) \in \ker \varepsilon_t$. Since $\deg p(X) = 4$ and $p(X)$ is monic, we have

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}+\sqrt{3}}(X) = X^4 - 10X^2 + 1. \qquad \square$$

3.10. Definition. Let $L/K$ be a finite extension. An element $u \in L$ for which $L = K(u)$ is called a *primitive element* for the extension $L/K$. If $L/K$ such a primitive element exists, then $L/K$ is called a *simple extension.*

Later we will see that when $\operatorname{char} K = 0$ every finite extension $L/K$ has a primitive element, hence every such extension is simple.

3.11. Lemma. *Let $L/K$ be a finite extension and $u \in L$. Then $u$ is a primitive element for $L/K$ if and only if $\deg_K u = [L : K]$.*

Proof. $K(u) \subseteq L$ is a finite dimensional $K$-vector subspace. Then $K(u) = L$ if and only $\dim_K K(u) = \dim_K L$. Since $\deg_K u = \dim_K K(u)$ and $[L : K] = \dim_K L$ the result follows. $\square$

Sometimes the minimal polynomial of an element in an extension is introduced in a different but equivalent way.

3.12. Proposition. *Let $t \in L$ be algebraic over $K$. Then*

$$\mathfrak{I}(t) = \{f(X) \in K[X] : f(t) = 0\} \subseteq K[X]$$

*is an ideal which is principal and has an irreducible monic generator $q(X) \in K[X]$. In fact, $q(X) = \operatorname{minpoly}_{K,t}(X)$.*

Proof. It is easy to see that $\mathfrak{I}(t) \lhd K[X]$ and therefore $\mathfrak{I}(t) = (q(X))$ for some monic generator $q(X)$. To see that $q(X)$ is irreducible, suppose that $q(X) = q_1(X)q_2(X)$ with $\deg q_i(X) < \deg q(X)$. Now as $q_1(t)q_2(t) = 0$, we must have $q_1(t) = 0$ or $q_2(t) = 0$, hence $q_1(X) \in \mathfrak{I}(t)$ or $q_2(X) \in \mathfrak{I}(t)$. These possibilities give $q(X) \mid q_1(X)$ or $q(X) \mid q_2(X)$ and so $\deg q(X) \leqslant \deg q_1(X)$ or $\deg q(X) \leqslant \deg q_2(X)$, contradicting the above assumption that $\deg q_i(X) < \deg q(X)$.

The irreducible monic polynomial $\operatorname{minpoly}_{K,t}(X)$ is in $\mathfrak{I}(t)$ so $q(X) \mid \operatorname{minpoly}_{K,t}(X)$ and therefore $q(X) = \operatorname{minpoly}_{K,t}(X)$. $\square$

The next Lemma will often be useful.

3.13. Lemma. *Let $L/K$ be an extension and suppose that $u_1, \ldots, u_n \in L$ are algebraic. Then $K(u_1, \ldots, u_n)/K$ is a finite extension.*

Proof. Use induction on $n$ together with Proposition 2.8 and Theorem 2.6(ii). $\square$

We now come to an important notion for extensions.

3.14. Definition. The extension $L/K$ is *algebraic* or $L$ is *algebraic over* $K$ if every element $t \in L$ is algebraic over $K$.

3.15. Proposition. *Let $L/K$ be a finite extension. Then $L/K$ is algebraic.*

Proof. Let $t \in L$. Since the $K$-vector space $L$ is finite dimensional, when viewed as elements of this vector space, the powers $1, t, \ldots, t^n, \ldots$ must be linearly dependent over $K$. Hence for suitable coefficients $c_j \in K$ not all zero and some $m \geqslant 1$ we have

$$c_0 + c_1 t + \cdots + c_m t^m = 0.$$

But this means that $t$ is algebraic over $K$. □

3.16. Proposition. *Let $M/L$ and $L/K$ be algebraic extensions. Then the extension $M/K$ is algebraic.*

Proof. Let $u \in M$. Then $u$ is algebraic over $L$, so there is a polynomial

$$p(X) = p_0 + p_1 X + \cdots + p_m X^m \in L[X]$$

of positive degree with $p(u) = 0$. By Lemma 3.13, the extension $K(p_0, \ldots, p_m)/K$ is finite and so is $K(p_0, \ldots, p_m, u)/K(p_0, \ldots, p_m)$. By Theorem 2.6(ii), $K(p_0, \ldots, p_m, u)/K$ is finite, so by Proposition 3.15, $u$ is algebraic over $K$. □

3.17. Definition. For an extension $L/K$, let

$$L^{\mathrm{alg}} = \{t \in L : t \text{ is algebraic over } K\} \subseteq L.$$

3.18. Proposition. *For an extension $L/K$, $L^{\mathrm{alg}}$ is a subfield containing $K$ and $L^{\mathrm{alg}}/K$ is algebraic.*

Proof. Clearly $K \subseteq L^{\mathrm{alg}}$. We must show that $L^{\mathrm{alg}} \leqslant L$.

Let $u, v \in L^{\mathrm{alg}}$. Then by Lemma 3.13, $K(u, v)/K$ is a finite dimensional extension, hence every element of $K(u, v)$ is algebraic over $K$. In particular, $u + v$ and $uv$ are in $K(u, v)$ and if $u \neq 0$, $u^{-1}$ is also in $K(u, v)$. Therefore $u + v$, $uv$ and $u^{-1}$ are all algebraic over $K$. □

3.19. Example. In the extension $\mathbb{C}/\mathbb{Q}$ we can consider $\mathbb{C}^{\mathrm{alg}} \leqslant \mathbb{C}$ which is called the subfield of *algebraic numbers*. Similarly, in the extension $\mathbb{R}/\mathbb{Q}$ the subfield

$$\mathbb{R}^{\mathrm{alg}} = \mathbb{C}^{\mathrm{alg}} \cap \mathbb{R} \leqslant \mathbb{C}$$

consists of all the *real algebraic numbers*. Elements of $\mathbb{C} - \mathbb{C}^{\mathrm{alg}}$ are called *transcendental* complex numbers; examples are $e$ and $\pi$. The sets $\mathbb{C}^{\mathrm{alg}}$ and $\mathbb{R}^{\mathrm{alg}}$ are both countable, whereas $\mathbb{C}$ and $\mathbb{R}$ are uncountable, so there are in fact many more transcendental numbers but it can be hard to determine whether a given number is transcendental or not. A more usual notation for $\mathbb{C}^{\mathrm{alg}}$ is $\overline{\mathbb{Q}}$ since this is the *algebraic closure* of $\mathbb{Q}$ which will be discussed later. When dealing with algebraic extensions of $\mathbb{Q}$ we will usually work with subfields of $\overline{\mathbb{Q}} = \mathbb{C}^{\mathrm{alg}}$.

We end this section with a technical result.

3.20. Proposition. *Let $K(u)/K$ be a finite simple extension. Then there are only finitely many subextensions $F/K \leqslant K(u)/K$.*

PROOF. Consider the minimal polynomial $\operatorname{minpoly}_{K,u}(X) \in K[X]$. Now for any subextension $F/K \leqslant K(u)/K$ we can also consider

$$\operatorname{minpoly}_{F,u}(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1} + X^k \in F[X],$$

which divides $\operatorname{minpoly}_{K,u}(X)$ in $F[X]$. The Unique Factorization Property 1.33 implies that $\operatorname{minpoly}_{K,u}(X)$ has only finitely many monic divisors in $K(u)[X]$, so there are only a finite number of possibilities for $\operatorname{minpoly}_{F,u}(X)$. Now consider $F_0 = K(c_0, c_1, \ldots, c_{k-1})$, the extension field of $K$ generated by the coefficients of $\operatorname{minpoly}_{F,u}(X)$. Then $F_0 \leqslant F$ and so $\operatorname{minpoly}_{F,u}(X) \in F_0[X]$ is irreducible since it is irreducible in $F[X]$; hence $\operatorname{minpoly}_{F,u}(X) = \operatorname{minpoly}_{F_0,u}(X)$. We have

$$[K(u) : F] = \deg \operatorname{minpoly}_{F,u}(X) = \deg \operatorname{minpoly}_{F_0,u}(X) = [K(u) : F_0],$$

hence $F = F_0$.

This shows that there are only finitely many subextensions $F/K \leqslant K(u)/K$, each of which has the form $K(a_0, a_1, \ldots, a_{\ell-1})$, where

$$a_0 + a_1X + \cdots + a_{\ell-1}X^{\ell-1} + X^\ell \in K(u)[X]$$

is a factor of $\operatorname{minpoly}_{K,u}(X)$ in $K(u)[X]$. □

### 3.2. Splitting fields and Kronecker's Theorem

We can now answer a basic question. Let $K$ be a field and $p(X) \in K[X]$ be a polynomial of positive degree.

3.21. QUESTION. Is there an extension field $L/K$ for which $p(X)$ has a root in $L$?

A stronger version of this question is the following.

3.22. QUESTION. Is there an extension field $E/K$ for which $p(X)$ factorizes into linear factors in $E[X]$?

3.23. DEFINITION. $p(X) \in K[X]$ *splits in* $E/K$ or *over* $E$ if it factorizes into linear factors in $E[X]$.

Of course, if we have such a field $E$ then the distinct roots $u_1, \ldots, u_k$ of $p(X)$ in $E$ generate a subfield $K(u_1, \ldots, u_k) \leqslant E$ which is the smallest subfield of $E$ that answers Question 3.22.

3.24. DEFINITION. Such a minimal extension of $K$ is called a *splitting field* of $p(X)$ over $K$ and we will sometimes denote it by $K(p(X))$ or $K_p$.

We already know how to answer Question 3.21.

3.25. THEOREM (Kronecker's Theorem: first version). *Let $K$ be a field and $p(X) \in K[X]$ be a polynomial of positive degree. Then there is a finite extension $L/K$ for which $p(X)$ has a root in $L$.*

PROOF. We begin by factorizing $p(X) \in K[X]$ into irreducible monic factors $q_j(X)$ together with a constant factor $c$:

$$p(X) = cq_1(X) \cdots q_r(X).$$

Now for any $j$ we can form the quotient field $K[x]/(q_j(X))$ which is a finite dimensional (simple) extension of $K$ and in which the coset $X + (q_j(X))$ satisfies the equation

$$q_j(X + (q_j(X))) = 0 + (q_j(X)).$$

Hence $p(X)$ has a root in $K[x]/(q_j(X))$.

Of course, this construction is only interesting if $q_j(X)$ to has degree bigger than 1 since a linear polynomial already has a root in $K$. □

To answer Question 3.22 we iterate this construction. Namely, having found one root $u_1$ in an extension $L_1/K$ we discard the linear factor $X - u_1$ and consider the polynomial

$$p_1(X) = \frac{p(X)}{X - u_1} \in L_1[X].$$

We can repeat the argument to form a finite extension of $L_1$ (and hence of $K$) containing a root of $p_1(X)$ and so on. At each stage we either already have another root in $L_1$ or we need to enlarge the field to obtain one.

3.26. Theorem (Kronecker's Theorem: second version). *Let $K$ be a field and $p(X) \in K[X]$ be a polynomial of positive degree. Then there is a finite extension $E/K$ which is a splitting field of $p(X)$ over $K$.*

In practise we often have extension fields 'lying around in nature' containing roots and we can work inside of these. When working over $\mathbb{Q}$ (or any other subfield of $\mathbb{C}$) we can always find roots in $\mathbb{C}$ by the Fundamental Theorem of Algebra. We then refer to a subfield of $\mathbb{C}$ which is a splitting field as *the splitting subfield*.

3.27. Example. Find a splitting field $E/\mathbb{Q}$ for $p(X) = X^4 - 4$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$.

Solution. Notice that

$$p(X) = (X^2 - 2)(X^2 + 2),$$

so first we adjoin the roots $\pm\sqrt{2}$ of $(X^2 - 2)$ to form $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ which gives an extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ of degree 2.

Next consider the polynomial $X^2 + 2 \in \mathbb{Q}(\sqrt{2})[X]$. The complex roots of $X^2 + 2$ are $\pm\sqrt{2}\,i$ and these are not real, so this polynomial is irreducible in $\mathbb{Q}(\sqrt{2})[X]$. Hence we need to consider $\mathbb{Q}(\sqrt{2}, \sqrt{2}\,i) = \mathbb{Q}(\sqrt{2}, i)$ and the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2})$ which has degree 2.

$$\begin{array}{c} \mathbb{C} \\ \vdots\ \infty \\ \mathbb{Q}(\sqrt{2}, i) \\ \text{adjoin roots of } X^2+2 \;\Big|\; 2 \\ \mathbb{Q}(\sqrt{2}) \\ \text{adjoin roots of } X^2-2 \;\Big|\; 2 \\ \mathbb{Q} \end{array}$$

Thus the splitting subfield of $p(X)$ over $\mathbb{Q}$ in $\mathbb{C}$ is $\mathbb{Q}(\sqrt{2}, i)$ and $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. □

Of course we could have started by first adjoining roots of $X^2+2$ and then adjoining roots of $X^2-2$, thus giving the tower

$$\begin{array}{c} \mathbb{C} \\ \vdots \\ \infty \\ \vdots \\ \mathbb{Q}(\sqrt{2}\,,i) \\ \text{adjoin roots of } X^2-2 \;\Big|\; 2 \\ \mathbb{Q}(\sqrt{2}\,i) \\ \text{adjoin roots of } X^2+2 \;\Big|\; 2 \\ \mathbb{Q} \end{array}$$

An important point is that if a splitting field exists inside of a given extension field $F/K$, it is unique as a subfield of $F$.

3.28. Proposition. *Let $F/K$ be an extension field and $p(X) \in K[X]$. If $E_1, E_2 \leqslant F$ are splitting subfields for $p(X)$ over $K$ then $E_1 = E_2$.*

Proof. Let $u_1, \ldots, u_k \in F$ be the distinct roots of $p(X)$ in $F$. By definition, $K(u_1, \ldots, u_k)$ is the smallest subfield containing $K$ and all the $u_j$. But $K(u_1, \ldots, u_k)$ must be contained in any splitting subfield, so $E_1 = K(u_1, \ldots, u_k) = E_2$. □

Since we will frequently encounter quadratic polynomials we record a useful result on roots of such polynomials. Recall that $p(X) = aX^2 + bX + c \in K[X]$ is *quadratic* if $a \neq 0$ and its *discriminant* is

$$\Delta = b^2 - 4ac \in K.$$

The proof of the next result is the standard one which works provided 2 has an inverse in $K$, *i.e.*, when $\operatorname{char} K \neq 2$.

3.29. Proposition. *Let $K$ be a field of characteristic different from 2. Then the quadratic polynomial $p(X) = aX^2 + bX + c \in K[X]$ has*

- *no roots in $K$ if $\Delta$ is not a square in $K$;*
- *one root $-b/(2a) = -(2a)^{-1}b$ if $\Delta = 0$;*
- *two distinct roots*

$$\frac{-b+\delta}{2a} = (2a)^{-1}(-b+\delta), \quad \frac{-b-\delta}{2a} = (2a)^{-1}(-b-\delta),$$

*if $\Delta = \delta^2$ for some non-zero $\delta \in K$.*

In particular, the splitting field of $p(X)$ over $K$ is $K$ if $\Delta$ is a square in $K$ and $K(\delta)$ otherwise, where $\delta$ is one of the two square roots of $\Delta$ in some extension of $K$ such as the algebraic closure $\overline{K}$ which we will introduce in Section 3.4.

3.30. Example. Find a splitting field $E/\mathbb{Q}$ for $p(X) = X^3 - 2$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$.

Solution. By the Eisenstein Test 1.38, $p(X)$ is irreducible over $\mathbb{Q}$. One root of $p(X)$ is $\sqrt[3]{2} \in \mathbb{R}$ so we adjoin this to $\mathbb{Q}$ to form an extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ of degree 3. Now

$$p(X) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}\,X + (\sqrt[3]{2})^2)$$

and the second factor has the non-real complex roots $\sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2$ lying in the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\sqrt[3]{2})$ of degree 2. So the splitting subfield of $X^3 - 2$ in $\mathbb{C}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ with $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.

An alternative strategy would have been to adjoin one of the other roots $\sqrt[3]{2}\,\zeta_3$ or $\sqrt[3]{2}\,\zeta_3^2$ first. We could also have begun by adjoining $\zeta_3$ to form the extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, but none of the roots of $p(X)$ lie in this field so the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\zeta_3)$ of degree 3 is obtained by adjoining one and hence all of the roots.

Figure 3.1 shows all the subfields of the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$. □

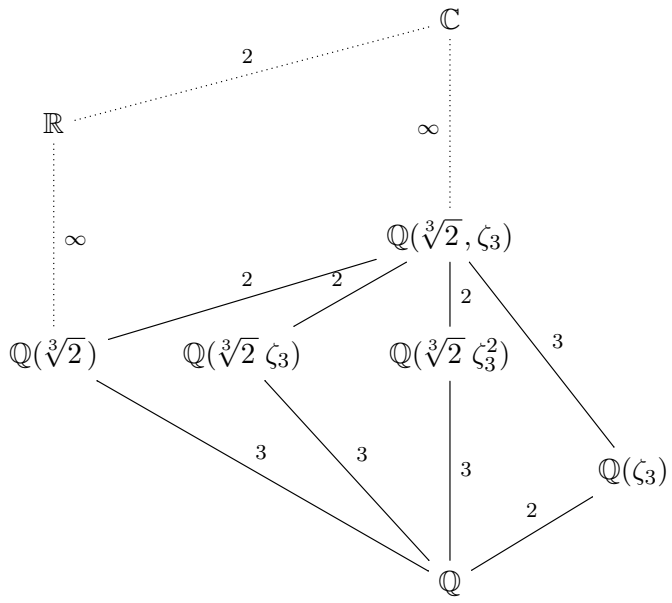



FIGURE 3.1. The subfields of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

### 3.3. Monomorphisms between extensions

3.31. DEFINITION. For extensions $F/K$ and $L/K$, let $\mathrm{Mono}_K(L, F)$ denote the set of all monomorphisms $L \longrightarrow F$ which fix the elements of $K$.

3.32. REMARK. We always have $\mathrm{Aut}_K(F) \subseteq \mathrm{Mono}_K(F, F)$ and $\mathrm{Mono}_K(F, F)$ is closed under composition but is not always a group since elements are not necessarily invertible. If $F/K$ is finite, then we do have $\mathrm{Mono}_K(F, F) = \mathrm{Aut}_K(F)$ since every injective $K$-linear transformation is surjective and so invertible.

We will also use the following notation.

3.33. DEFINITION. Let $F/K$ be an extension and $p(X) \in K[X]$. Set

$$\mathrm{Roots}(p, F) = \{u \in F : p(u) = 0\},$$

the set of roots of $p(X)$ in $F$. This is always a finite set which may of course be empty, which happens precisely when $p(X)$ has no root in $F$.

Suppose that $p(X) \in K[X]$ is an irreducible polynomial which we might as well assume is monic, and let $F/K$ be an extension. Then if $t \in F$ is a root of $p(X)$, the evaluation homomorphism $\varepsilon_t \colon K[X] \longrightarrow F$ factors through the quotient monomorphism $\widetilde{\varepsilon}_t \colon K[X]/(p(X)) \longrightarrow F$ whose image is $K(t) \leqslant F$. Of course, there is one such monomorphism for each root of $p(X)$ in $F$. If we fix one such root $t_0$ and identify $K[X]/(p(X))$ with $K(t_0)$ via $\widetilde{\varepsilon}_{t_0}$, then each root of $p(X)$ in $F$ gives rise to a monomorphism $\varphi_t = \widetilde{\varepsilon}_t \circ \widetilde{\varepsilon}_{t_0}^{-1} \colon K(t_0) \longrightarrow F$ for which $\varphi_t(t_0) = t$.

$$\begin{array}{ccccc} & & \overset{\varphi_t = \widetilde{\varepsilon}_t \circ \widetilde{\varepsilon}_{t_0}^{-1}}{\frown} & & \\ K(t_0) & \underset{\cong}{\overset{\widetilde{\varepsilon}_{t_0}}{\longleftarrow}} & K[X]/(p(X)) & \xrightarrow{\widetilde{\varepsilon}_t} & F \end{array}$$

Notice that if $\varphi \colon K[X]/(p(X)) \longrightarrow F$ is any homomorphism extending the identity function on $K$, then the coset $X + (p(X))$ must be sent by $\varphi$ to a root of $p(X)$ in $F$, hence every such homomorphism arises this way. This discussion is summarized in the following result.

3.34. Proposition. *Let $F/K$ be a field extension. Let $p(X) \in K[X]$ be an irreducible polynomial with $t_0 \in F$ be a root of $p(X)$. Then there is a bijection*

$$\mathrm{Roots}(p, F) \longleftrightarrow \mathrm{Mono}_K(K(t_0), F)$$

*given by $t \longleftrightarrow \varphi_t$, where $\varphi_t \colon K(t_0) \longrightarrow F$ has the effect $\varphi_t(t_0) = t$.*

3.35. Example. Show that $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})$ has two elements.

Solution. We have $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2 - 2)$ where $X^2 - 2$ is irreducible over $\mathbb{Q}$. Hence the $\mathbb{Q}$-monomorphisms we want send $\sqrt{2}$ to $\pm\sqrt{2}$ which are the complex roots of $X^2 - 2$. In fact both possibilities occur, giving monomorphisms $\mathrm{id}, \alpha \colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$, where

$$\alpha(a + b\sqrt{2}) = a - b\sqrt{2}\,.$$

We can replace $\mathbb{C}$ by $\mathbb{Q}(\sqrt{2})$ to obtain

$$\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})).$$

We will see that this is not always true. □

3.36. Example. Show that $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$ has 3 elements but $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}))$ contains only the identity function.

Solution. Here $\mathrm{minpoly}_{\mathbb{Q}, \sqrt[3]{2}}(X) = X^3 - 2$ and there are 3 complex roots $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$. As two of these roots are not real, $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}))$ contains only the identity since $\mathbb{Q}(\sqrt[3]{2}) \leqslant \mathbb{R}$.

Each of the above roots corresponds to one of the subfields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\,\zeta_3)$ or $\mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2)$ of $\mathbb{C}$ and there are 3 monomorphisms $\alpha_0, \alpha_1, \alpha_2 \colon \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ given by

$$\begin{aligned} \alpha_0(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \\ \alpha_1(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2}\,\zeta_3 + c(\sqrt[3]{2})^2\,\zeta_3^2, \\ \alpha_2(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2}\,\zeta_3^2 + c(\sqrt[3]{2})^2\,\zeta_3. \end{aligned}$$

These mappings have images

$$\alpha_0\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}), \quad \alpha_1\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\,\zeta_3), \quad \alpha_2\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2). \qquad \square$$

3.37. Proposition. *Let $F/K$ and $L/K$ be extensions.*

(i) *For $p(X) \in K[X]$, each monomorphism $\alpha \in \mathrm{Mono}_K(L, F)$ restricts to a function $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, F)$ which is an injection.*

(ii) *If $\alpha \in \mathrm{Mono}_K(L, L)$, then $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is a bijection.*

Proof. (i) For $u \in \mathrm{Roots}(p, L)$ we have

$$p(\alpha(u)) = \alpha(p(u)) = \alpha(0) = 0,$$

so $\alpha$ maps $\mathrm{Roots}(p, L)$ into $\mathrm{Roots}(p, F)$. Since $\alpha$ is an injection its restriction to $\mathrm{Roots}(p, L) \subseteq L$ is also an injection.
(ii) From (i), $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is an injective function from a finite set to itself, hence it is also surjective by the Pigeon Hole Principle. Thus $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is a bijection. □

Part (ii) says that any automorphism of $L/K$ permutes the set of roots in $L$ of a polynomial $p(X) \in K[X]$. This gives us a strong hold on the possible automorphisms. In the case of finite, or more generally algebraic, extensions it is the key to understanding the automorphism group and this is a fundamental insight of Galois Theory.

3.38. Example. Determine $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C})$.

Solution. We have already met the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ in Example 3.30 and we will make use of information from there. We build up the list of monomorphisms in stages.

First consider monomorphisms that fix $\sqrt[3]{2}$ and hence fix the subfield $\mathbb{Q}(\sqrt[3]{2})$. These form the subset

$$\mathrm{Mono}_{\mathbb{Q}(\sqrt[3]{2})}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) \subseteq \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}).$$

We know that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2})(\zeta_3)$ and that $\zeta_3$ is a root of the irreducible cyclotomic polynomial $\Phi_3(X) = X^2 + X + 1 \in \mathbb{Q}(\sqrt[3]{2})[X]$. So there are two monomorphisms $\mathrm{id}, \alpha_0$ fixing $\mathbb{Q}(\sqrt[3]{2})$, where $\alpha_0$ has the effect

$$\alpha_0\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

Next we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\zeta_3$. This time we have 2 distinct ways to extend to elements of $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}(\sqrt[3]{2}, \zeta_3))$ since again we can send $\zeta_3$ to either $\zeta_3$ or $\zeta_3^2$. The possibilities are

$$\alpha_1\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3 \\ \zeta_3 & \longmapsto & \zeta_3 \end{pmatrix}, \quad \alpha_1'\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3 \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

Finally we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\zeta_3^2$. There are again two possibilities

$$\alpha_2\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3^2 \\ \zeta_3 & \longmapsto & \zeta_3 \end{pmatrix}, \quad \alpha_2'\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3^2 \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

These are all 6 of the required monomorphisms. It is also the case here that

$$\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) = \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)),$$

so these form a group. It is a nice exercise to show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathrm{S}_3$, the symmetric group on 3 objects. It is also worth remarking that $|\,\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))| = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}]$. □

We end this section with another useful result.

3.39. Proposition. *Let $L/K$ be an extension and $\alpha \in \mathrm{Mono}_K(L,L)$. Then $\alpha$ restricts to an automorphism $\alpha^{\mathrm{alg}}\colon L^{\mathrm{alg}} \longrightarrow L^{\mathrm{alg}}$.*

Proof. Suppose that $u \in L^{\mathrm{alg}}$, say $p(u) = 0$ for some $p(X) \in K[X]$ of positive degree. Then

$$p(\alpha(u)) = \alpha(p(u)) = \alpha(0) = 0,$$

so $\alpha$ maps $L^{\mathrm{alg}} \subseteq L$ into itself and therefore gives rise to a restriction $\alpha^{\mathrm{alg}}\colon L^{\mathrm{alg}} \longrightarrow L^{\mathrm{alg}}$ which is also a monomorphism. We must show that $\alpha^{\mathrm{alg}}$ is a bijection by showing it is surjective.

Let $v \in L^{\mathrm{alg}}$ and suppose that $q(v) = 0$ for some $q(X) \in K[X]$ of positive degree. Now $\mathrm{Roots}(q,L) \neq \emptyset$ since it contains $v$, and it is also finite. Then $\alpha_q\colon \mathrm{Roots}(q,L) \longrightarrow \mathrm{Roots}(q,L)$ is a bijection by Proposition 3.37(ii), hence $v = \alpha_q(w) = \alpha(w)$ for some $w \in \mathrm{Roots}(q,L) \subseteq L^{\mathrm{alg}}$. This shows that $v \in \mathrm{im}\,\alpha$ and so $\alpha^{\mathrm{alg}}$ is surjective. □

## 3.4. Algebraic closures

An important property of the complex numbers is that $\mathbb{C}$ is *algebraically closed*.

3.40. Theorem (Fundamental Theorem of Algebra for $\mathbb{C}$). *Every non-constant polynomial $p(X) \in \mathbb{C}[X]$ has a root in $\mathbb{C}$.*

3.41. Corollary. *Every non-constant polynomial $p(X) \in \mathbb{C}[X]$ has a factorization*

$$p(X) = c(X - u_1)\cdots(X - u_d),$$

*where $c, u_1, \ldots, u_d \in \mathbb{C}$ and this is unique apart from the order of the roots $u_j$.*

It is natural to pose the following question.

3.42. Question. Let $K$ be a field. Is there an algebraically closed field $F$ containing $K$?

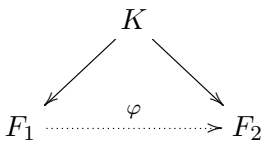
By taking $F^{\mathrm{alg}}$ we might as well ask that such a field be algebraic over $K$.

3.43. Definition. Let $K$ be a field. An extension $F/K$ is called an *algebraic closure of $K$* if $F$ is algebraic over $K$ and is algebraically closed.

3.44. Theorem. *Let $K$ be a field.*

(i) *There is an algebraic closure of $K$.*

(ii) *Let $F_1$ and $F_2$ be algebraic closures of $K$. Then there is an isomorphism $\varphi\colon F_1 \longrightarrow F_2$ which fixes the elements of $K$.*




*Hence algebraic closures are essentially unique.*

Proof. See [**3**] for a proof using *Zorn's Lemma* (see Axiom 3.48) which is logically equivalent to the *Axiom of Choice*. □

Because of the uniqueness we usually fix some choice of algebraic closure of $K$ and write $\overline{K}$ or $K^{\text{alg cl}}$, referring to it as *the* algebraic closure of $K$. We are already familiar with the example $\overline{\mathbb{C}} = \mathbb{C}$. There are some immediate consequences of Theorem 3.44. We will temporarily write $E_1 \doteq E_2$ to indicate that for extensions $E_1/K$ and $E_2/K$ there is an isomorphism $E_1 \longrightarrow E_2$ fixing the elements of $K$.

3.45. Proposition. *Let $K$ be a field.*

(i) *If $L/K$ is an algebraic extension, then $\overline{L} \doteq \overline{K}$.*
(ii) *If $L/K$ is an extension, then so is $\overline{L}/K$ and $(\overline{L})^{\text{alg}} \doteq \overline{K}$.*

Proof. (i) By Proposition 3.16, every element of $\overline{L}$ is algebraic over $K$. Since $\overline{L}$ is algebraically closed it is an algebraic closure of $K$.
(ii) Every non-constant polynomial in $(\overline{L})^{\text{alg}}[X]$ has a root in $\overline{L}$; indeed, by Proposition 3.16, all of its roots are in fact algebraic over $K$ since $(\overline{L})^{\text{alg}}$ is algebraic over $K$. Hence these roots lie in $(\overline{L})^{\text{alg}}$, which shows that it is algebraically closed. □

For example, we have $\overline{\mathbb{Q}} = \mathbb{C}^{\text{alg}}$ and $\overline{\mathbb{R}} = \mathbb{C}$.

There is a stronger result than Theorem 3.44(ii), the Monomorphism Extension Theorem, which we will find useful. Again the proof uses Zorn's Lemma which we state below. First we need some definitions.

3.46. Definition. A *partially ordered set* $(X, \preccurlyeq)$ consists of a set $X$ and a binary relation $\preccurlyeq$ such that whenever $x, y, z \in X$,

- $x \preccurlyeq x$;
- if $x \preccurlyeq y$ and $y \preccurlyeq z$ then $x \preccurlyeq z$;
- if $x \preccurlyeq y$ and $y \preccurlyeq x$ then $x = y$.

$(X, \preccurlyeq)$ is *totally ordered* if for every pair $x, y \in X$, at least one of $x \preccurlyeq y$ or $y \preccurlyeq x$ is true.

3.47. Definition. Let $(X, \preccurlyeq)$ be a partially ordered set and $Y \subseteq X$.

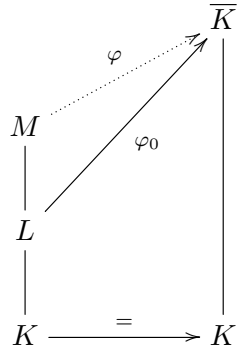
- $\overline{y} \in X$ is an *upper bound for $Y$* if for every $y \in Y$, $y \preccurlyeq \overline{y}$.
- An element $x \in X$ is a *maximal element of $X$* if

$$x \preccurlyeq y \quad \Longrightarrow \quad y = x.$$

3.48. Axiom (Zorn's Lemma). *Let $(X, \preccurlyeq)$ be a partially ordered set in which every totally ordered subset has an upper bound. Then $X$ has a maximal element.*

3.49. Theorem (Monomorphism Extension Theorem). *Let $M/K$ be an algebraic extension and $L/K \leqslant M/K$. Suppose that $\varphi_0 \colon L \longrightarrow \overline{K}$ is a monomorphism fixing the elements of $K$.*

*Then there is an extension of $\varphi_0$ to a monomorphism $\varphi\colon M \longrightarrow \overline{K}$.*




PROOF. We consider the set $X$ consisting of all pairs $(F, \theta)$, where $F/L \leqslant M/L$ and $\theta\colon F \longrightarrow \overline{K}$ extends $\varphi_0$. We order $X$ using the relation $\preccurlyeq$ for which $(F_1, \theta_1) \preccurlyeq (F_2, \theta_2)$ whenever $F_1 \leqslant F_2$ and $\theta_2$ extends $\theta_1$. Then $(X, \preccurlyeq)$ is a partially ordered set.

Suppose that $Y \subseteq X$ is a totally ordered subset. Let

$$\widetilde{F} = \bigcup_{(F,\theta)\in Y} F.$$

Then $\widetilde{F}/L \leqslant M/L$. Also there is a function $\widetilde{\theta}\colon \widetilde{F} \longrightarrow \overline{K}$ defined by

$$\widetilde{\theta}(u) = \theta(u)$$

whenever $u \in F$ for $(F, \theta) \in Y$. It is straightforward to check that if $u \in F'$ for $(F', \theta') \in Y$ then

$$\theta'(u) = \theta(u),$$

so $\widetilde{\theta}$ is well-defined. Then for every $(F, \theta) \in Y$ we have $(F, \theta) \preccurlyeq (\widetilde{F}, \widetilde{\theta})$, so $(\widetilde{F}, \widetilde{\theta})$ is an upper bound for $Y$. By Zorn's Lemma there must be a maximal element of $X$, $(M_0, \theta_0)$.

Suppose that $M_0 \neq M$, so there is an element $u \in M$ for which $u \notin M_0$. Since $M$ is algebraic over $K$ it is also algebraic over $M_0$, hence $u$ is algebraic over $M_0$. If

$$\operatorname{minpoly}_{M_0,u}(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n,$$

then the polynomial

$$f(X) = \theta_0(a_0) + \cdots + \theta_0(a_{n-1})X^{n-1} + X^n \in (\theta_0 M_0)[X]$$

is also irreducible and so it has a root $v$ in $\overline{K}$ (which is also an algebraic closure of $\theta_0 M_0 \leqslant \overline{K}$). The Homomorphism Extension Property 1.22 of the polynomial ring $M_0[X]$ applied to the monomorphism $\theta_0\colon M_0 \longrightarrow \overline{K}$ yields a homomorphism $\theta_0'\colon M_0[X] \longrightarrow \overline{K}$ extending $\theta_0$ and for which $\theta_0'(u) = v$. This factors through the quotient ring $M_0[X]/(\operatorname{minpoly}_{M_0,u}(X))$ to give a monomorphism $\theta_0''\colon M_0(u) \longrightarrow \overline{K}$ extending $\theta_0$. But then $(M_0, \theta_0) \preccurlyeq (M_0(u), \theta_0'')$ and $(M_0, \theta_0) \neq (M_0(u), \theta_0'')$, contradicting the maximality of $(M_0, \theta_0)$. Hence $M_0 = M$ and so we can take $\varphi = \theta_0$. □

3.50. EXAMPLE. Let $u \in \overline{K}$ and suppose that $p(X) = \operatorname{minpoly}_{K,u}(X) \in K[X]$. Then for any other root of $p(X)$, $v \in \overline{K}$ say, there is a monomorphism $\varphi_v\colon K(u) \longrightarrow \overline{K}$ with $\varphi_v(u) = v$. This extends to a monomorphism $\varphi\colon \overline{K} \longrightarrow \overline{K}$.

3.51. DEFINITION. Let $u, v \in \overline{K}$. Then $v$ is *conjugate to $u$ over $K$* or is a *conjugate of $u$ over $K$* if there is a monomorphism $\varphi\colon \overline{K} \longrightarrow \overline{K}$ fixing $K$ for which $v = \varphi(u)$.

3.52. Lemma. *If $u, v \in \overline{K}$, then $v$ is conjugate to $u$ over $K$ if and only if* $\operatorname{minpoly}_{K,u}(v) = 0$.

Proof. Suppose that $v = \varphi(u)$ for some $\varphi \in \operatorname{Mono}_K(\overline{K}, \overline{K})$. If

$$\operatorname{minpoly}_{K,u}(X) = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d,$$

then

$$a_0 + a_1 u + \cdots + a_{d-1}u^{d-1} + u^d = 0$$

and so

$$a_0 + a_1 v + \cdots + a_{d-1}v^{d-1} + v^d = \varphi(a_0 + a_1 u + \cdots + a_{d-1}u^{d-1} + u^d) = 0.$$

The converse follows from Example 3.50. □

### 3.5. Multiplicity of roots and separability

Let $K$ be a field. Suppose that $f(X) \in K[X]$ and $u \in K$ is a root of $f(X)$, *i.e.*, $f(u) = 0$. Then we can factor $f(X)$ as $f(X) = (X - u)f_1(X)$ for some $f_1(X) \in K[X]$.

3.53. Definition. If $f_1(u) = 0$ then $u$ is a *multiple* or *repeated root* of $f(X)$. If $f_1(u) \neq 0$ then $u$ is a *simple root* of $f(X)$.

We need to understand more clearly when an irreducible polynomial has a multiple root since this turns out to be important in what follows. Consider the *formal derivative on* $K[X]$, *i.e.*, the function $\partial\colon K[X] \longrightarrow K[X]$ given by

$$\partial(f(X)) = f'(X) = a_1 + 2a_2 X + \cdots + da_d X^{d-1},$$

where $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ with $a_j \in K$.

3.54. Proposition. *The formal derivative $\partial\colon K[X] \longrightarrow K[X]$ has the following properties.*

(i) *$\partial$ is $K$-linear.*

(ii) *$\partial$ is a* derivation, i.e., *for $f(X), g(X) \in K[X]$,*

$$\partial(f(X)g(X)) = \partial(f(X))g(X) + f(X)\partial(g(X)).$$

(iii) *If* $\operatorname{char} K = 0$, *then* $\ker \partial = K$ *and $\partial$ is surjective.*

(iv) *If* $\operatorname{char} K = p > 0$, *then*

$$\ker \partial = \{h(X^p) : h(X) \in K[X]\}$$

*and* $\operatorname{im} \partial$ *is spanned by the monomials $X^k$ with $p \nmid (k+1)$.*

Proof. (i) This is routine.

(ii) By $K$-linearity, it suffices to verify this for the case where $f(X) = X^r$ and $g(X) = X^s$ with $r, s \geqslant 0$. But then

$$\partial(X^{r+s}) = (r+s)X^{r+s-1} = rX^{r-1}X^s + sX^r X^{s-1} = \partial(X^r)X^s + X^r\partial(X^s).$$

(iii) If $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ then

$$\partial(f(X)) = 0 \quad \Longleftrightarrow \quad a_1 = 2a_2 = \cdots = da_d = 0.$$

So $\partial(f(X)) = 0$ if and only if $f(X) = a_0 \in K$. It is also clear that every polynomial $g(X) \in K[X]$ has the form $g(X) = \partial(f(X))$ where $f(X)$ is an anti-derivative of $g(X)$.

(iv) For a monomial $X^m$, $\partial(X^m) = mX^{m-1}$ and this is zero if and only if $p \mid m$. Using this we see that

$$\partial(a_0 + a_1X + a_2X^2 + \cdots + a_dX^d) = 0 \quad \iff \quad a_m = 0 \text{ whenever } p \nmid m.$$

Also, $\operatorname{im}\partial$ is spanned by the monomials $X^k$ for which $\partial(X^{k+1}) \neq 0$, which are the ones with $p \nmid (k+1)$. □

We now apply the formal derivative to detect multiple roots.

3.55. Proposition. *Let $f(X) \in K[X]$ have a root $u \in L$ for some extension $L/K$. Then $u$ is a multiple root of $f(X)$ if and only if $f(X)$ and $f'(X)$ have a common factor of positive degree in $K[X]$ which vanishes at $u$.*

Proof. Working in $L[X]$, let $f(X) = (X-u)f_1(X)$. Then

$$f'(X) = f_1(X) + (X-u)f_1'(X),$$

so $f'(u) = f_1(u)$. Hence $u$ is a multiple root if and only if $f(X)$ and $f'(X)$ have a common factor in $L[X]$ (and hence in $K[X]$ by Proposition 3.12) and which vanishes at $u$. □

3.56. Corollary. *If $f(X)$ is irreducible in $K[X]$ then a root $u$ is a multiple root if and only if $f'(X) = 0$. In particular, this can only happen if* $\operatorname{char} K > 0$.

3.57. Corollary. *If* $\operatorname{char} K = 0$ *and $f(X)$ is irreducible in $K[X]$, then every root of $f(X)$ is simple.*

3.58. Example. For $n \geqslant 1$, show that each of the roots of $f(X) = X^n - 1$ in $\mathbb{C}$ is simple.

Solution. We have $f'(X) = \partial(X^n - 1) = nX^{n-1}$, so for any root $\zeta$ of $f(X)$,

$$f'(\zeta) = n\zeta^{n-1} \neq 0.$$ □

3.59. Example. Show that $2i$ is a multiple root of $f(X) = X^4 + 8X^2 + 16$.

Solution. We have $f'(X) = 4X^3 + 16X$. Using Long Division and the Euclidean Algorithm we find that $\gcd(f(X), f'(X)) = X^2 + 4$, where $2i$ is also a root of $X^2 + 4$. Hence $2i$ is a multiple root of $f(X)$. In fact, $X^4 + 8X^2 + 16 = (X^2 + 4)^2$, so this is obvious. □

3.60. Example. Let $p > 0$ be a prime and suppose that $L/\mathbb{F}_p$ is an extension. Show that each of the roots of $f(X) = X^p - 1$ in $L$ is multiple.

Solution. We have $f'(X) = \partial(X^p - 1) = pX^{p-1} = 0$, so if $\zeta$ is any root of $f(X)$ then $f'(\zeta) = 0$. In fact, 1 is the *only* root of $X^p - 1$ since this polynomial factorises (essentially uniquely) as

$$X^p - 1 = (X-1)^p$$

because of the Idiot's Binomial Theorem 1.11 and the Unique Factorization Property 1.33. □

3.61. Definition. An irreducible polynomial $p(X) \in K[X]$ is *separable over $K$* if every root of $p(X)$ in an extension $L/K$ is simple. By Corollary 3.56, this is equivalent to requiring that $p'(X) \neq 0$. If $u \in L$ is a multiple root of $p(X)$, then the *multiplicity of $u$ in $p(X)$* is the maximum $m$ such that$p(X) = (X-u)^m q(X)$ for some $q(X) \in L[X]$.

3.62. Proposition. *Let $K$ be a field and let $\overline{K}$ be an algebraic closure. If the irreducible polynomial $p(X) \in K[X]$ has distinct roots $u_1, \ldots, u_k \in \overline{K}$, then the multiplicities of the $u_j$ are equal. Hence in $\overline{K}[X]$,*

$$p(X) = c(X - u_1)^m \cdots (X - u_k)^m,$$

*where $c \in K$ and $m \geqslant 1$.*

Proof. Let $u \in \overline{K}$ be a root of $p(X)$ and suppose that it has multiplicity $m$, so we can write $p(X) = (X - u)^m p_1(X)$ where $p_1(X) \in K(u)[X]$ and $p_1(u) \neq 0$.

Now let $v \in \overline{K}$ be any other root of $p(X)$. By Proposition 3.34, there is a monomorphism $\varphi_v \colon K(u) \longrightarrow \overline{K}$ for which $\varphi_v(u) = v$. When $p(X)$ is viewed as an element of $K(u)[X]$, the coefficients of $p(X)$ are fixed by $\varphi_v$. Then

$$\varphi_v((X - u)^m p_1(X)) = (X - u)^m p_1(X),$$

and so

$$(X - v)^m \widetilde{p}_1(X) = (X - u)^m p_1(X),$$

where $\widetilde{p}_1(X) \in \overline{K}[X]$ is obtained applying $\varphi_v$ to the coefficients of $p_1(X)$. Now by Corollary 1.34, $(X - v)^m$ must divide $p_1(X)$ in $\overline{K}[X]$, and therefore the multiplicity of $v$ must be at least $m$. Interchanging the rôles of $u$ and $v$ we find that the multiplicities of $u$ and $v$ are in fact equal. □

3.63. Corollary. *Let $K$ be a field and let $\overline{K}$ be an algebraic closure. If the irreducible polynomial $p(X) \in K[X]$ has distinct roots $u_1, \ldots, u_k \in \overline{K}$ which are all simple then in $\overline{K}[X]$,*

$$p(X) = c(X - u_1) \cdots (X - u_k),$$

*where $c \in K$ and $k = \deg p(X)$.*

3.64. Corollary. *Let $K$ be a field and let $u \in \overline{K}$. Then the number of distinct conjugates of $u$ is*

$$\frac{\deg \operatorname{minpoly}_{K,u}(X)}{m},$$

*where $m$ is the multiplicity of $u$ in $\operatorname{minpoly}_{K,u}(X)$.*

3.65. Definition. An algebraic element $u \in L$ in an extension $L/K$ is *separable* if its minimal polynomial $\operatorname{minpoly}_{K,u}(X) \in K[X]$ is separable.

3.66. Definition. An algebraic extension $L/K$ is called *separable* if every element of $L$ is separable over $K$.

3.67. Example. An algebraic extension $L/K$ of a field of characteristic 0 is separable by Corollary 3.57.

3.68. Definition. Let $L/K$ be a finite extension. The *separable degree of $L$ over $K$* is

$$(L : K) = |\operatorname{Mono}_K(L, \overline{K})|.$$

3.69. Lemma. *For a finite simple extension $K(u)/K$,*

$$(K(u) : K) = |\operatorname{Roots}(\operatorname{minpoly}_{K,u}, \overline{K})|.$$

*If $K(u)/K$ is separable, then $[K(u) : K] = (K(u) : K)$.*

Proof. This follows from Proposition 3.34 applied to the case $L = \overline{K}$. □

Any finite extension $L/K$ can be built up from a succession of simple extensions

$$K(u_1)/K,\ K(u_1,u_2)/K(u_1),\cdots,L=K(u_1,\ldots,u_k)/K(u_1,\ldots,u_{k-1}). \tag{3.1}$$

So we can use the following to compute $(L:K)=(K(u_1,\ldots,u_k):K)$.

3.70. Proposition. *Let $L/K$ and $M/L$ be finite extensions. Then*

$$(M:K)=(M:L)(L:K).$$

Proof. For $\alpha\in\mathrm{Mono}_K(M,\overline{K})$ let $\alpha_L\in\mathrm{Mono}_K(L,\overline{K})$ be its restriction to $L$. By the Monomorphism Extension Theorem 3.49, each element of $\mathrm{Mono}_K(L,\overline{K})$ extends to a monomorphism $M\longrightarrow\overline{K}$, so every element $\beta\in\mathrm{Mono}_K(L,\overline{K})$ has the form $\beta=\alpha_L$ for some $\alpha\in\mathrm{Mono}_K(M,\overline{K})$. Since $(L:K)=|\,\mathrm{Mono}_K(L,\overline{K})|$, we need to show that the number of such $\alpha$ is always $(M:L)=|\,\mathrm{Mono}_L(M,\overline{K})|$.

So given $\beta\in\mathrm{Mono}_K(L,\overline{K})$, choose any extension to a monomorphism $\widetilde{\beta}\colon\overline{K}\longrightarrow\overline{K}$; by Proposition 3.39, $\widetilde{\beta}$ is an automorphism. Of course, restricting to $M\leqslant\overline{K}$ we obtain a monomorphism $M\longrightarrow\overline{K}$. Now for any extension $\beta'\colon M\longrightarrow\overline{K}$ of $\beta$ we can form the composition $\widetilde{\beta}^{-1}\circ\beta'\colon M\longrightarrow\overline{K}$; notice that if $u\in L$, then

$$\widetilde{\beta}^{-1}\circ\beta'(u)=\widetilde{\beta}^{-1}(\beta(u))=u,$$

hence $\widetilde{\beta}^{-1}\circ\beta'\in\mathrm{Mono}_L(M,\overline{K})$. Conversely, each $\gamma\in\mathrm{Mono}_L(M,\overline{K})$ gives rise to a monomorphism $\widetilde{\beta}\circ\gamma\colon M\longrightarrow\overline{K}$ which extends $\beta$. In effect, this shows that there is a bijection

$$\big\{\text{extensions of }\beta\text{ to monomorphism a }M\longrightarrow\overline{K}\big\}\longleftrightarrow\mathrm{Mono}_L(M,\overline{K}),$$

so $(M:L)=|\,\mathrm{Mono}_L(M,\overline{K})|$ agrees with the number of extensions of $\beta$ to a monomorphism $M\longrightarrow\overline{K}$. Therefore we have the desired formula $(M:K)=(M:L)(L:K)$. □

3.71. Corollary. *Let $L/K$ be a finite extension. Then $(L:K)\mid[L:K]$.*

Proof. If $L/K$ is a simple extension then by Propositions 3.62 and 3.34 we know that this is true. The general result follows by building up $L/K$ as a sequence of simple extensions as in (3.1) and then using Theorem 2.6(ii) which gives

$$[L:K]=[K(u_1):K]\,[K(u_1,u_2):K(u_1)]\cdots[K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1})].$$

For each $k$, $(K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1}))$ divides $[K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1})]$, so the desired result follows. □

3.72. Proposition. *Let $L/K$ be a finite extension. Then $L/K$ is separable if and only if $(L:K)=[L:K]$.*

Proof. Suppose that $L/K$ is separable. If $K\leqslant E\leqslant L$, then for any $u\in L$, $u$ is algebraic over $E$, and in the polynomial ring $E[X]$ we have $\mathrm{minpoly}_{E,u}(X)\mid\mathrm{minpoly}_{K,u}(X)$. As $\mathrm{minpoly}_{K,u}(X)$ is separable, so is $\mathrm{minpoly}_{E,u}(X)$, and therefore $L/E$ is separable. Clearly $E/K$ is also separable. We have $(L:K)=(L:E)\,(E:K)$ and $[L:K]=[L:E]\,[E:K]$, so to verify that $(L:K)=[L:K]$ it suffices to show that $(L:E)=[L:E]$ and $(E:K)=[E:K]$. Expressing $L/K$ in terms of a sequence of simple extensions as in (3.1), we have

$$(L:K)=(K(u_1):K)\cdots(L:K(u_1,\ldots,u_{k-1})),$$
$$[L:K]=[K(u_1):K]\cdots[L:K(u_1,\ldots,u_{k-1})].$$

Now we can apply Lemma 3.69 to each of these intermediate separable simple extensions to obtain $(L : K) = [L : K]$.

For the converse, suppose that $(L : K) = [L : K]$. We must show that for each $u \in L$, $u$ is separable. For the extensions $K(u)/K$ and $L/K(u)$ we have $(L : K) = (L : K(u))\,(K(u) : K)$ and $[L : K] = [L : K(u)]\,[K(u) : K]$. By Corollary 3.71, there are some positive integers $r, s$ for which $[L : K(u)] = r(L : K(u))$ and $[K(u) : K] = s(K(u) : K)$. Hence

$$(L : K(u))(K(u) : K) = rs(L : K(u))(K(u) : K),$$

which can only happen if $r = s = 1$. Thus $(K(u) : K) = [K(u) : K]$ and so $u$ is separable. □

3.73. Proposition. *Let $L/K$ and $M/L$ be finite extensions. Then $M/K$ is separable if and only if $L/K$ and $M/L$ are separable.*

Proof. If $M/K$ is separable then $[M : K] = (M : K)$ and so by Proposition 3.70,

$$[M : L][L : K] = (M : L)(L : K).$$

This can only happen if $[M : L] = (M : L)$ and $[L : K] = (L : K)$, since $(M : L) \leqslant [M : L]$ and $(L : K) \leqslant [L : K]$. By Proposition 3.72 this implies that $L/K$ and $M/L$ are separable.

Conversely, if $L/K$ and $M/L$ are separable then $[M : L] = (M : L)$ and $[L : K] = (L : K)$, hence

$$[M : K] = [M : L][L : K] = (M : L)(L : K) = (M : K).$$

Therefore $M/K$ is separable. □

## 3.6. The Primitive Element Theorem

Recall from Definition 3.10 that a finite extension $L/K$ is simple if there is an element $u \in L$ for which $L = K(u)$, and such an element is called a primitive element.

3.74. Theorem (Primitive Element Theorem). *Let $L/K$ be a finite separable extension. Then $L$ has a primitive element, hence $L/K$ is a simple extension.*

Proof. The case where $K$ is a finite field will be dealt with in Proposition 5.16, so we will assume that $K$ is infinite.

Since $L$ is built up from a sequence of simple extensions it suffices to consider the case $L = K(u, v)$. Let $p(X), q(X) \in K[X]$ be the minimal polynomials of $u$ and $v$ over $K$. Suppose that the distinct roots of $p(X)$ in $\overline{K}$ are $u = u_1, \ldots, u_r$, while the distinct roots of $q(X)$ are $v = v_1, \ldots, v_s$. By the separability assumption, $r = \deg p(X)$ and $s = \deg q(X)$.

Since $K$ is infinite, we can choose an element $t \in K$ for which

$$t \neq \frac{u - u_i}{v_j - v}$$

whenever $i, j \neq 1$. Then taking $w = u + tv \in L$, we find that $w \neq u_i + tv_j$ whenever $i, j \neq 1$. Define the polynomial $h(X)$ of degree $r$ by

$$h(X) = p(w - tX) \in K(w)[X] \subseteq L[X].$$

Then $h(v) = p(u) = 0$, but $h(v_j) \neq p(u_i) = 0$ for any $i, j \neq 1$ by construction of $t$, so none of the other $v_j$ is a zero of $h(X)$.

Now since the polynomials $h(X), q(X) \in K(w)[X]$ have exactly one common root in $\overline{K}$, namely $v$, by separability their greatest common divisor in $K(w)[X]$ is a linear polynomial which

must be $X - v$, hence $v \in K(w)$ and so $u = w - tv \in K(w)$. This shows that $K(u, v) \leqslant K(w)$ and therefore $K(w) = K(u, v)$. □

3.75. Corollary. *Let $L/K$ be a finite extension of a field of characteristic 0. Then $L$ has a primitive element.*

Proof. Since $\mathbb{Q} \leqslant K$, $K$ is infinite and by Example 3.67 $L/K$ is separable. □

To find a primitive element we can always use the method suggested by the proof of Theorem 3.74, however a 'try it and see' approach is often sufficient.

3.76. Example. Find a primitive element for the extension $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$.

Solution. Consider $\sqrt{3} + i$. Then working over the subfield $\mathbb{Q}(\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{3}, i)$ we find that $i \notin \mathbb{Q}(\sqrt{3}) \leqslant \mathbb{R}$ and

$$(X - (\sqrt{3} + i))(X - (\sqrt{3} - i)) = X^2 - 2\sqrt{3}\,X + 4 \in \mathbb{Q}(\sqrt{3})[X],$$

hence

$$X^2 - 2\sqrt{3}\,X + 4 = \operatorname{minpoly}_{\mathbb{Q}(\sqrt{3}),\sqrt{3}+i}(X).$$

Now taking

$$(X^2 - 2\sqrt{3}\,X + 4)(X^2 + 2\sqrt{3}\,X + 4) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X],$$

we see that $\operatorname{minpoly}_{\mathbb{Q},\sqrt{3}+i}(X) \mid (X^4 - 4X^2 + 16)$ in $\mathbb{Q}[X]$. Notice that

$$(\sqrt{3} + i)^{-1} = \frac{(\sqrt{3} - i)}{(\sqrt{3} + i)(\sqrt{3} - i)} = \frac{(\sqrt{3} - i)}{3 + 1} = \frac{1}{4}(\sqrt{3} - i) \in \mathbb{Q}(\sqrt{3} + i),$$

since $(\sqrt{3} + i)^{-1} \in \mathbb{Q}(\sqrt{3} + i)$. Hence

$$\sqrt{3} = \frac{1}{2}((\sqrt{3} + i) + (\sqrt{3} - i)), \quad i = \frac{1}{2}((\sqrt{3} + i) - (\sqrt{3} - i)),$$

are both in $\mathbb{Q}(\sqrt{3} + i)$, showing that $\mathbb{Q}(\sqrt{3}, i) \leqslant \mathbb{Q}(\sqrt{3} + i)$ and so $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3} + i)$. Thus we must have $\deg \operatorname{minpoly}_{\mathbb{Q},\sqrt{3}+i}(X) = 4$, and so $\operatorname{minpoly}_{\mathbb{Q},\sqrt{3}+i}(X) = X^4 - 4X^2 + 16$. □

There is a general phenomenon illustrated by Example 3.76.

3.77. Proposition. *Let $u \in \overline{K}$ be separable over $K$. Then*

$$\operatorname{minpoly}_{K,u}(X) = (X - \alpha_1(u)) \cdots (X - \alpha_d(u)),$$

*where $\alpha_1, \ldots, \alpha_d$ are the elements of $\operatorname{Mono}_K(K(u), \overline{K})$. In particular, the polynomial*

$$(X - \alpha_1(u)) \cdots (X - \alpha_d(u)) \in \overline{K}[X]$$

*is in $K[X]$ and is irreducible therein.*

Proof. Since $K(u)$ is separable then by Lemma 3.52,

$$d = \deg \operatorname{minpoly}_{K,u}(X) = [K(u) : K] = (K(u) : K).$$ □

In Example 3.76 we have

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

There are four monomorphisms $\alpha_k\colon \mathbb{Q}(\sqrt{3}\,,i) \longrightarrow \mathbb{Q}(\sqrt{3}\,,i)$ given by

$$\alpha_1 = \mathrm{id}, \quad \alpha_2 = \begin{pmatrix} \sqrt{3} & \longmapsto & \sqrt{3} \\ i & \longmapsto & -i \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{3} & \longmapsto & -\sqrt{3} \\ i & \longmapsto & i \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{3} & \longmapsto & -\sqrt{3} \\ i & \longmapsto & -i \end{pmatrix}.$$

Then

$$\alpha_2(\sqrt{3}+i) = (\sqrt{3}-i), \quad \alpha_3(\sqrt{3}+i) = (-\sqrt{3}+i), \quad \alpha_4(\sqrt{3}+i) = (-\sqrt{3}-i),$$

so

$$(X-\sqrt{3}-i)(X-\sqrt{3}+i)(X+\sqrt{3}-i)(X+\sqrt{3}+i) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X].$$

Hence this polynomial is irreducible. So we have $[\mathbb{Q}(\sqrt{3}+i):\mathbb{Q}] = 4$ and $\mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}\,,i)$.

## 3.7. Normal extensions and splitting fields

Let $\overline{K}$ be an algebraic closure for the field $K$ and let $E/K \leqslant \overline{K}/K$ be a finite extension. If $\varphi \in \mathrm{Mono}_K(E,\overline{K})$, then by Remark 3.32, $\varphi E = E$ if and only if $\varphi E \leqslant E$.

3.78. Definition. $E/K$ is *normal* if $\varphi E = E$ for every $\varphi \in \mathrm{Mono}_K(E,\overline{K})$.

3.79. Remark. If $E/K$ is a normal extension then whenever an irreducible polynomial $p(X) \in K[X]$ has a root in $E$, it splits in $E$ since by Lemma 3.52 each pair of roots of $p(X)$ is conjugate over $K$ and one can be mapped to the other by a monomorphism $\overline{K} \longrightarrow \overline{K}$ which must map $E$ into itself.

3.80. Theorem. *A finite extension $E/K$ is normal if and only if it is a splitting field over $K$ for some polynomial $f(X) \in K[X]$.*

Proof. Suppose that $E/K$ is normal. Then there is a sequence of extensions

$$K \leqslant K(u_1) \leqslant K(u_1,u_2) \leqslant \cdots \leqslant K(u_1,\ldots,u_n) = E$$

Construct a polynomial by taking

$$f(X) = \mathrm{minpoly}_{K,u_1}(X)\,\mathrm{minpoly}_{K,u_2}(X)\cdots\mathrm{minpoly}_{K,u_n}(X).$$

Then by Remark 3.79, $f(X)$ splits in $E$. Also, $E$ is generated by some of the roots of $f(X)$. Hence $E$ is a splitting field for $f(X)$ over $K$.

Now suppose that $E$ is a splitting field for $g(X) \in K[X]$, so that $E = K(v_1,\ldots,v_k)$, where $v_1,\ldots,v_k$ are the distinct roots of $g(X)$ in $E$. Now any monomorphism $\theta \in \mathrm{Mono}_K(E,\overline{K})$ must map these roots to $\theta(v_1),\ldots,\theta(v_k)$ which are also roots of $g(X)$ and therefore lie in $E$ (see Proposition 3.34). Since $\theta$ permutes the roots $v_j$, we have

$$\theta E = \theta K(v_1,\ldots,v_k) = K(\theta(v_1),\ldots,\theta(v_k)) = K(v_1,\ldots,v_k) = E. \qquad \square$$

3.81. Corollary. *Let $E/L$ and $L/K$ be finite extensions. If $E/K$ is normal then $E/L$ is normal.*

Proof. If $E$ is the splitting field of a polynomial $f(X) \in K[X]$ over $K$, then $E$ is the splitting field of $f(X)$ over $L$. $\square$

These result makes it easy to recognize a normal extension since it is sufficient to describe it as a splitting field for *some* polynomial over $K$. In Chapter 4 we will see that separable normal extensions play a central rôle in Galois Theory, indeed these are known as *Galois extensions*.

## Exercises for Chapter 3

**3.1** Prove Proposition 3.2.

**3.2** Finding splitting subfields $E \leqslant \mathbb{C}$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$ for each of the following polynomials.

$p_1(X) = X^4 - X^2 + 1, \quad p_2(X) = X^6 - 2, \quad p_3(X) = X^4 + 2, \quad p_4(X) = X^4 + 5X^3 + 10X^2 + 10X + 5.$

[*Hint: for $p_4(X)$, consider $p_4(Y - 1) \in \mathbb{Q}[Y]$.*]

**3.3** Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathrm{S}_3$, the symmetric group on 3 elements, as claimed in the solution of Example 3.38. [*Hint: work out the effect of each automorphism on the three roots of the polynomial $X^3 - 2$.*]

**3.4** Let $\Bbbk$ be a field of characteristic $\mathrm{char}\,\Bbbk = p > 0$ and $\Bbbk(T)$ be the field of rational functions in $T$ over $\Bbbk$. Show that the polynomial $g(X) = X^p - T \in \Bbbk(T)[X]$ is irreducible and has a multiple root in $\overline{\Bbbk(T)}$. How does $g(X)$ factor in $\overline{\Bbbk(T)}[X]$?

**3.5** Find primitive elements for the extensions $\mathbb{Q}(\sqrt{5}, \sqrt{10})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}$, in each case finding it minimal polynomial over $\mathbb{Q}$. [*Hint: look for elements of high degree over $\mathbb{Q}$, or use the method of proof of Theorem 3.74.*]

**3.6** Prove the following converse of Proposition 3.20:

*Let $L/K$ be a finite extension. If there are only finitely many subextensions $F/K \leqslant L/K$, then $L/K$ is simple,* i.e., *$L = K(w)$ for some $w \in L$.*

[*Hint: First deal with the case where $L = K(u, v)$, then use induction on $n$ to prove the general case $L = K(u_1, \ldots, u_n)$.*]

**3.7** Let $K$ be a field. Show that every quadratic (*i.e.*, of degree 2) extension $E/K$ is normal. Is such an extension always separable?

**3.8** Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of odd degree greater than 1 and having only one real root $u \in \mathbb{R}$. Show that $\mathbb{Q}(u)/\mathbb{Q}$ is not a normal extension.

CHAPTER 4

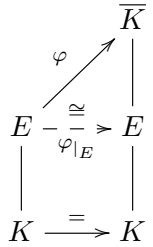
# Galois extensions and the Galois Correspondence

In this Chapter we will study the structure of *Galois extensions* and their associated *Galois groups*, in particular we will explain how these are related through the *Galois Correspondence*. Throughout the chapter, let $K$ be a field.

## 4.1. Galois extensions

4.1. Definition. A finite extension $E/K$ is a (*finite*) *Galois extension* if it is both normal and separable.

From Section 3.5 we know that for such a Galois extension $E/K$, $[E : K] = (E : K)$ and also every monomorphism $\varphi \in \mathrm{Mono}_K(E, \overline{K})$ maps $E$ into itself, hence restricts to an automorphism of $E$ which will be denoted $\varphi_{|E}$.




Also, by the Monomorphism Extension Theorem 3.49, every automorphism $\alpha \in \mathrm{Aut}_K(E)$ extends to a monomorphism $E \longrightarrow \overline{K}$ fixing elements of $K$. So there is a bijection

$$\mathrm{Mono}_K(E, \overline{K}) \longleftrightarrow \mathrm{Aut}_K(E)$$

and we have

$$|\mathrm{Aut}_K(E)| = (E : K) = [E : K]. \tag{4.1}$$

4.2. Definition. For a finite Galois extension $E/K$, the group

$$\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E)$$

is called the *Galois group of the extension* or the *Galois group of $E$ over $K$*. The elements of $\mathrm{Gal}(E/K)$ are called (*Galois*) *automorphisms* of $E/K$.

Notice that Equation (4.1) implies

$$|\mathrm{Gal}(E/K)| = (E : K) = [E : K]. \tag{4.2}$$

We can also reformulate the notion of conjugacy introduced in Definition 3.51.

4.3. Definition. Let $E/K$ a finite Galois extension and $u, v \in E$. Then $v$ is *conjugate to $u$* if there is a $\varphi \in \mathrm{Gal}(E/K)$ for which $v = \varphi(u)$; we also say that $v$ is a *conjugate of $u$*.

It is easy to see that for $u, v \in \overline{K}$, there is a finite Galois extension $E/K$ in which $v$ is a conjugate of $u$ if and only $v$ is a conjugate of $u$ over $K$ in the old sense. Here is a slightly different way to understand this. First notice that every element $\varphi \in \mathrm{Aut}_K(\overline{K}, \overline{K})$ restricts to a monomorphism $E \longrightarrow \overline{K}$ whose image is contained in $E$, hence gives rise to an automorphism $\varphi_E \colon E \longrightarrow E$. Similarly, if $F/K$ is any finite normal extension with $E \leqslant F$, every automorphism $\theta \colon F \longrightarrow F$ restricts to an automorphism $\theta_E^F \colon E \longrightarrow E$. The proof of the next result is left as an exercise.

4.4. Proposition. *If $E/K$ is a finite Galois extension, then the function*

$$\mathrm{Aut}_K(\overline{K}, \overline{K}) \longrightarrow \mathrm{Aut}_K(E, E); \quad \varphi \longmapsto \varphi_E$$

*is a surjective group homomorphism. If $F/K \leqslant \overline{K}/K$ is any finite normal extension with $E \leqslant F$ then there is a surjective group homomorphism*

$$\mathrm{Aut}_K(F, F) \longrightarrow \mathrm{Aut}_K(E, E); \quad \theta \longmapsto \theta_E^F.$$

*Furthermore, for $\varphi \in \mathrm{Aut}_K(\overline{K}, \overline{K})$ we have*

$$(\varphi_F)_E^F = \varphi_E.$$

### 4.2. Working with Galois groups

Let $E/K$ be a finite Galois extension. Then we know that $E$ is a splitting field for some polynomial over $K$ since $E/K$ is normal. We also know that $E$ is a simple extension of $K$ since $E/K$ is separable. Hence $E$ is a splitting field for the minimal polynomial of any primitive element for $E/K$; this minimal polynomial has degree $[E : K]$. It is often convenient to use these facts to interpret elements of the Galois group as permutations of the roots of some polynomial which splits over $E$.

4.5. Example. Describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ as a subgroup of the group of permutations of the roots of $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$.

Solution. We have

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

and the following non-trivial elements of the Galois group together with the element identity $\alpha_1 = \mathrm{id}$:

$$\alpha_2 = \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & \sqrt{3} \\ -\sqrt{3} & \longmapsto & -\sqrt{3} \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{2} & \longmapsto & \sqrt{2} \\ -\sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ -\sqrt{3} & \longmapsto & \sqrt{3} \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ -\sqrt{3} & \longmapsto & \sqrt{3} \end{pmatrix}.$$

Writing the roots in the list $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ and numbering them from 1 to 4, these automorphisms correspond to the following permutations in $\mathrm{S}_4$ expressed in cycle notation:

$$\alpha_2 \longleftrightarrow (1\ 2), \quad \alpha_3 \longleftrightarrow (3\ 4), \quad \alpha_4 \longleftrightarrow (1\ 2)(3\ 4). \qquad \square$$

4.6. Example. Using a primitive element $u$ for the extension, describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ as a subgroup of the group of permutations of the roots of $\mathrm{minpoly}_{\mathbb{Q},u}(X) \in \mathbb{Q}[X]$.

SOLUTION. We have $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and the conjugates of $u = \sqrt{2}+\sqrt{3}$ are $\pm\sqrt{2} \pm \sqrt{3}$. Listing these as

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

and after numbering them accordingly, we find the correspondences

$$\alpha_2 \longleftrightarrow (1\ 3)(2\ 4), \quad \alpha_3 \longleftrightarrow (1\ 2)(3\ 4), \quad \alpha_4 \longleftrightarrow (1\ 4)(2\ 3). \qquad \square$$

Next we summarize the properties of Galois groups that can be deduced from what we have established so far. Recall that for an extension $F/K$ and a polynomial $f(X) \in K[X]$, $\mathrm{Roots}(f,F)$ denotes the set of roots of $f(X)$ in $F$.

4.7. RECOLLECTION. Recall that an action of a group $G$ on a set $X$ is *transitive* if for every pair of elements $x, y \in X$, there is an element $g \in G$ such that $y = gx$ (so there is only one orbit); the action is *faithful* or *effective* if for every non-identity element $h \in G$, there is an element $z \in X$ such that $hz \neq z$.

4.8. THEOREM. *Let $E/K$ be a finite Galois extension. Suppose that $E$ is the splitting field of a separable irreducible polynomial $f(X) \in K[X]$ of degree $n$. Then the following are true.*

(i) $\mathrm{Gal}(E/K)$ *acts transitively and faithfully on* $\mathrm{Roots}(f,E)$.
(ii) $\mathrm{Gal}(E/K)$ *can be identified with a subgroup of the group of permutations of* $\mathrm{Roots}(f,E)$. *If we order the roots $u_1,\dots,u_n$ then* $\mathrm{Gal}(E/K)$ *can be identified with a subgroup of* $\mathrm{S}_n$.
(iii) $|\mathrm{Gal}(E/K)|$ *divides $n!$ and is divisible by $n$.*

As we have seen in Examples 4.5 and 4.6, in practise it is often easier to use a not necessarily irreducible polynomial to determine and work with a Galois group.

4.9. EXAMPLE. The Galois extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ has degree $[\mathbb{Q}(\zeta_8):\mathbb{Q}] = 4$ and it has the following automorphisms apart from the identity:

$$\alpha\colon \zeta_8 \longmapsto \zeta_8^3, \quad \beta\colon \zeta_8 \longmapsto \zeta_8^5, \quad \gamma\colon \zeta_8 \longmapsto \zeta_8^7.$$

If we list the roots of the minimal polynomial

$$\mathrm{minpoly}_{\mathbb{Q},\zeta}(X) = \Phi_8(X) = X^4+1$$

in the order $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$, we find that these automorphisms correspond to the following permutations in $\mathrm{S}_4$:

$$\alpha \longleftrightarrow (1\ 2)(3\ 4), \quad \beta \longleftrightarrow (1\ 3)(2\ 4), \quad \gamma \longleftrightarrow (1\ 4)(2\ 3).$$

So the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ corresponds to

$$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leqslant \mathrm{S}_4.$$

Noticing that

$$\zeta_8 = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,i,$$

we easily find that $\sqrt{2}, i \in \mathbb{Q}(\zeta_8)$; hence $\mathbb{Q}(\sqrt{2},i) \leqslant \mathbb{Q}(\zeta_8)$. Since $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = 4$, we have $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\zeta_8)$. Notice that $\mathbb{Q}(\sqrt{2},i)$ is the splitting field of $f(X) = (X^2-2)(X^2+1)$ over

$\mathbb{Q}$. Now list the roots of $f(X)$ in the order $\sqrt{2}, -\sqrt{2}, i, -i$, and observe that

$$\alpha\colon \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ i & \longmapsto & -i \\ -i & \longmapsto & i \end{pmatrix} \longleftrightarrow (1\ 2)(3\ 4), \qquad \beta\colon \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ i & \longmapsto & i \\ -i & \longmapsto & -i \end{pmatrix} \longleftrightarrow (1\ 2),$$

$$\gamma\colon \begin{pmatrix} \sqrt{2} & \longmapsto & \sqrt{2} \\ -\sqrt{2} & \longmapsto & -\sqrt{2} \\ i & \longmapsto & -i \\ -i & \longmapsto & i \end{pmatrix} \longleftrightarrow (3\ 4).$$

In this description, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ corresponds to the subgroup

$$\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leqslant \mathrm{S}_4.$$

While it can be hard to determine Galois groups in general, special arguments can sometimes be exploited.

4.10. Example. Suppose that $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ is an irreducible cubic and that $f(X)$ has only one real root. Then $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{S}_3$.

Proof. Let $u_1 \in \mathbb{R}$ be the real root of $f(X)$ and let $u_2, u_3$ be the remaining complex roots. Then $\mathbb{Q}(f(X)) = \mathbb{Q}(u_1, u_2, u_3)$ and in fact $[\mathbb{Q}(f(X)) : \mathbb{Q}] = 6$ since $[\mathbb{Q}(f(X)) : \mathbb{Q}] \mid 6$ and $u_2 \notin \mathbb{Q}(u_1) \leqslant \mathbb{R}$. Hence $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{S}_3$ and so $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{S}_3$ since the orders agree. We also have $\mathbb{Q}(f(X)) \cap \mathbb{R} = \mathbb{Q}(u_1)$.

The Galois group $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q})$ contains an element of order 3 which corresponds to a 3-cycle when viewed as a permutation of the roots $u_1, u_2, u_3$; we can assume that this is $(1\ 2\ 3)$. It also contains an element of order 2 obtained by restricting complex conjugation to $\mathbb{Q}(f(X))$; this fixes $u_1$ and interchanges $u_2, u_3$, so it corresponds to the transposition $(2\ 3)$. □

4.11. Remark. Such examples occur when the cubic polynomial $f(X)$ has local maximum and minimum at real values $c_+$ and $c_-$ with $f(c_+), f(c_-) > 0$ or $f(c_+), f(c_-) < 0$. This happens for example with $f(X) = X^3 - 3X + 3$ which has local extrema at $\pm 1$ and $f(1) = 1$, $f(-1) = 5$.

Given a Galois extension $E/K$, we will next study subextensions $L/K \leqslant E/K$ and subgroups $\Gamma \leqslant \mathrm{Gal}(E/K)$, focusing on the relationship between objects of these types.

### 4.3. Subgroups of Galois groups and their fixed fields

Let $E/K$ a Galois extension and suppose that $\Gamma \leqslant \mathrm{Gal}(E/K)$. Consider the subset of elements of $E$ fixed by $\Gamma$,

$$E^\Gamma = \{u \in E : \forall \gamma \in \Gamma,\ \gamma(u) = u\}.$$

4.12. Lemma. *$E^\Gamma \leqslant E$ is a subfield of $E$ containing $K$.*

Proof. For $u, v \in E^\Gamma$ and $\gamma \in \Gamma$,

$$\gamma(u + v) = \gamma(u) + \gamma(v) = u + v, \quad \gamma(uv) = \gamma(u)\gamma(v) = uv.$$

Also, if $u \neq 0$,

$$\gamma(u^{-1}) = \gamma(u)^{-1} = u^{-1}.$$

Finally, if $t \in K$ then $\gamma(t) = t$, so $K \leqslant E^\Gamma$. □

4.13. Definition. $E^\Gamma \leqslant E$ is the *fixed subfield of* $\Gamma$.

By Proposition 3.73, the extensions $E/E^\Gamma$ and $E^\Gamma/K$ are separable. $E/E^\Gamma$ is also normal, so this is a Galois extension; we will identify its Galois group. Notice that

$$[E : E^\Gamma] = (E : E^\Gamma) = |\operatorname{Gal}(E/E^\Gamma)|.$$

Now each element of $\operatorname{Gal}(E/E^\Gamma)$ is also an element of $\operatorname{Gal}(E/K)$ and $\operatorname{Gal}(E/E^\Gamma) \leqslant \operatorname{Gal}(E/K)$. Notice that by definition $\Gamma \leqslant \operatorname{Gal}(E/E^\Gamma)$, so Lagrange's Theorem implies that $|\Gamma|$ divides $|\operatorname{Gal}(E/E^\Gamma)|$. In fact we have

4.14. Proposition. *For* $\Gamma \leqslant \operatorname{Gal}(E/K)$*, we have* $\operatorname{Gal}(E/E^\Gamma) = \Gamma$ *and the equations*

$$[E : E^\Gamma] = |\operatorname{Gal}(E/E^\Gamma)| = |\Gamma|, \quad [E^\Gamma : K] = \frac{|\operatorname{Gal}(E/K)|}{|\Gamma|}.$$

Proof. We know that $E/E^\Gamma$ is separable, so by the Primitive Element Theorem 3.74 it is simple, say $E = E^\Gamma(u)$. Now let the distinct elements of $\Gamma$ be $\gamma_1 = \mathrm{id}, \gamma_2, \ldots, \gamma_h$, where $h = |\Gamma|$. Consider the polynomial of degree $h$

$$f(X) = (X - u)(X - \gamma_2(u)) \cdots (X - \gamma_h(u)) \in E[X].$$

Notice that $f(X)$ is unchanged by applying any $\gamma_k$ to its coefficients since the roots $\gamma_j(u)$ are permuted by $\gamma_k$. Hence, $f(X) \in E^\Gamma[X]$. This shows that

$$[E : E^\Gamma] = [E^\Gamma(u) : E^\Gamma] \leqslant h = |\Gamma|.$$

Since $\Gamma \leqslant \operatorname{Gal}(E/E^\Gamma)$, we also have

$$h = |\Gamma| \leqslant |\operatorname{Gal}(E/E^\Gamma)| = [E : E^\Gamma].$$

Combining these two inequalities we obtain

$$[E : E^\Gamma] = |\operatorname{Gal}(E/E^\Gamma)| = |\Gamma| = h$$

and therefore $\Gamma = \operatorname{Gal}(E/E^\Gamma)$. □

### 4.4. Subfields of Galois extensions and relative Galois groups

Let $E/K$ a Galois extension and suppose that $L/K \leqslant E/K$ (*i.e.*, $K \leqslant L \leqslant E$). Then $E/L$ is also a Galois extension whose Galois group $\operatorname{Gal}(E/L)$ is sometimes called the *relative Galois group of the pair of extensions* $E/K$ *and* $L/K$. The following is immediate.

4.15. Lemma. *The relative Galois group of the pair of extensions* $L/K \leqslant E/K$ *is a subgroup of* $\operatorname{Gal}(E/K)$, i.e., $\operatorname{Gal}(E/L) \leqslant \operatorname{Gal}(E/K)$*, and its order is* $|\operatorname{Gal}(E/L)| = [E : L]$.

4.16. Proposition. *Let* $L/K \leqslant E/K$*. Then* $L = E^{\operatorname{Gal}(E/L)}$.

Proof. Clearly $L \leqslant E^{\operatorname{Gal}(E/L)}$. Suppose that $u \in E - L$. By Theorem 4.8(i), there is an automorphism $\theta \in \operatorname{Gal}(E/L)$ such that $\theta(u) \neq u$, hence $u \notin E^{\operatorname{Gal}(E/L)}$. This shows that $E^{\operatorname{Gal}(E/L)} \leqslant L$ and therefore $E^{\operatorname{Gal}(E/L)} = L$. □

We need to understand when $\operatorname{Gal}(E/L) \leqslant \operatorname{Gal}(E/K)$ is actually a normal subgroup. The next result explains the connection between the two uses of the word *normal* which both ultimately derive from their use in Galois theory.

4.17. Proposition. *Let $E/K$ be a finite Galois extension and $L/K \leqslant E/K$.*

(i) *The relative Galois group* $\mathrm{Gal}(E/L)$ *of the pair of extensions $L/K \leqslant E/K$ is a normal subgroup of* $\mathrm{Gal}(E/K)$ *if and only if $L/K$ is a normal extension.*

(ii) *If $L/K$ is normal and hence a Galois extension, then there is a group isomorphism*

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \xrightarrow{\cong} \mathrm{Gal}(L/K); \quad \alpha\,\mathrm{Gal}(E/L) \longmapsto \alpha_{|_L}.$$

Proof. (i) Suppose that $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/K)$, *i.e.*, for all $\alpha \in \mathrm{Gal}(E/L)$ and $\beta \in \mathrm{Gal}(E/K)$, we have $\beta\alpha\beta^{-1} \in \mathrm{Gal}(E/L)$. Now if $u \in L$, then for any $\gamma \in \mathrm{Gal}(E/K)$ and $\alpha \in \mathrm{Gal}(E/L)$, $\gamma(u) \in E$ satisfies

$$\alpha\gamma(u) = \gamma(\gamma^{-1}\alpha\gamma(u)) = \gamma(u),$$

since $\gamma^{-1}\alpha\gamma \in \mathrm{Gal}(E/L)$; hence $\gamma(u) \in E^{\mathrm{Gal}(E/L)} = L$. By the Monomorphism Extension Theorem 3.49, every monomorphism $L \longrightarrow \overline{K}$ fixing $K$ extends to a monomorphism $E \longrightarrow \overline{K}$ which must have image $E$, so the above argument shows that $L/K$ is normal.

Conversely, if $L/K$ is normal, then for every $\varphi \in \mathrm{Gal}(E/K)$ and $v \in L$, $\varphi(v) \in L$, so for every $\theta \in \mathrm{Gal}(E/L)$, $\theta(\varphi(v)) = \varphi(v)$ and therefore

$$\varphi^{-1}\theta\varphi(v) = v.$$

This shows that $\varphi^{-1}\theta\varphi \in \mathrm{Gal}(E/L)$. Hence for every $\varphi \in \mathrm{Gal}(E/K)$,

$$\varphi\,\mathrm{Gal}(E/L)\varphi^{-1} = \mathrm{Gal}(E/L),$$

which shows that $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/K)$.

(ii) If $\alpha \in \mathrm{Gal}(E/K)$, then $\alpha L = L$ since $L/K$ is normal. Hence we can restrict $\alpha$ to an automorphism of $L$,

$$\alpha_{|_L} : L \longrightarrow L; \quad \alpha_{|_L}(u) = \alpha(u).$$

Then $\alpha_{|_L}$ is the identity function on $L$ if and only if $\alpha \in \mathrm{Gal}(E/L)$. It is easy to see that the function

$$\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(L/K); \quad \alpha \longmapsto \alpha_{|_L}$$

is a group homomorphism whose kernel is $\mathrm{Gal}(E/L)$. Thus we obtain an injective homomorphism

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \longrightarrow \mathrm{Gal}(L/K)$$

for which

$$|\,\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)| = \frac{[E:K]}{[E:L]} = [L:K] = |\,\mathrm{Gal}(L/K)|.$$

Hence this homomorphism is an isomorphism. □

## 4.5. The Galois Correspondence and the Main Theorem of Galois Theory

We are now almost ready to state our central result which describes the *Galois Correspondence* associated with a finite Galois extension. We will use the following notation. For a finite Galois extension $E/K$, let

$$\mathcal{S}(E/K) = \text{the set of all subgroups of } \mathrm{Gal}(E/K);$$
$$\mathcal{F}(E/K) = \text{the set of all subextensions } L/K \text{ of } E/K.$$

Each of these sets is ordered by inclusion. Since every subgroup of a finite group is a finite subset of a finite set, $\mathcal{S}(E/K)$ is also a finite set. Define two functions by

$$\Phi_{E/K}\colon \mathcal{F}(E/K) \longrightarrow \mathcal{S}(E/K); \quad \Phi_{E/K}(L) = \mathrm{Gal}(E/L),$$
$$\Theta_{E/K}\colon \mathcal{S}(E/K) \longrightarrow \mathcal{F}(E/K); \quad \Theta_{E/K}(\Gamma) = E^{\Gamma}.$$

4.18. Theorem (Main Theorem of Galois Theory). *Let $E/K$ be a finite Galois extension. Then the functions $\Phi_{E/K}$ and $\Theta_{E/K}$ are mutually inverse bijections which are order-reversing.*

$$\mathcal{F}(E/K) \underset{\Theta_{E/K}}{\overset{\Phi_{E/K}}{\rightleftarrows}} \mathcal{S}(E/K)$$

*Under this correspondence, normal subextensions of $E/K$ correspond to normal subgroups of $\mathrm{Gal}(E/K)$ and vice versa.*

Proof. We know from Proposition 4.16 that for an extension $L/K$ in $\mathcal{F}(E/K)$,

$$\Theta_{E/K}(\Phi_{E/K}(L)) = \Theta_{E/K}(\mathrm{Gal}(E/L)) = E^{\mathrm{Gal}(E/L)} = L.$$

Also, by Proposition 4.14 for $H \in \mathcal{S}(E/K)$ we have

$$\Phi_{E/K}(\Theta_{E/K}(\Gamma)) = \Phi_{E/K}(E^{\Gamma}) = \mathrm{Gal}(E/E^{\Gamma}) = \Gamma.$$

This shows that $\Phi_{E/K}$ and $\Theta_{E/K}$ are mutually inverse and so are inverse bijections.

Let $L_1/K,\ L_2/K \in \mathcal{F}(E/K)$ satisfy $L_1/K \leqslant L_2/K$. Then $\mathrm{Gal}(E/L_2) \leqslant \mathrm{Gal}(E/L_1)$ since $L_1 \subseteq L_2$ and so if $\alpha \in \mathrm{Gal}(E/L_2)$ then $\alpha$ fixes every element of $L_1$. Hence $\Phi_{E/K}(L_2) \leqslant \Phi_{E/K}(L_1)$ and so $\Phi_{E/K}$ reverses order.

Similarly, if $\Gamma_1, \Gamma_2 \in \mathcal{S}(E/K)$ and $\Gamma_1 \leqslant \Gamma_2$, then $E^{\Gamma_2} \leqslant E^{\Gamma_1}$ since if $w \in E^{\Gamma_2}$ then it is fixed by every element of $\Gamma_1$ (as $\Gamma_1$ is a subset of $\Gamma_2$). Hence $\Theta_{E/K}$ reverses order. □

There is an immediate consequence of the Main Theorem 4.18 which is closely related to Proposition 3.20.

4.19. Corollary. *Let $E/K$ be a finite Galois extension. Then there are only finitely many subextensions $L/K \leqslant E/K$.*

Proof. Since the set $\mathcal{S}(E/K)$ is finite, so is $\mathcal{F}(E/K)$. □

When dealing with a finite Galois extension $E/K$, we indicate the subextensions in a diagram with a line going upwards indicating an inclusion. We can also do this with the subgroups of the Galois group $\mathrm{Gal}(E/K)$ with labels indicating the index of the subgroups. In effect, the Galois Correspondence inverts these diagrams.

4.20. Example. Figure 4.1 shows the Galois Correspondence for the extension of Example 3.30.

As noted at the end of Example 3.38, the Galois group here is $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathrm{S}_3$. It is useful to make this isomorphism explicit. First take the 3 roots of the polynomial $X^3 - 2$ for which $E$ is the splitting field over $\mathbb{Q}$; these are $\sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2$ which we number in the order they are listed. Then the monomorphisms $\mathrm{id}, \alpha_0, \alpha_1, \alpha_1', \alpha_2, \alpha_2'$ extend to automorphisms of $E$, each of which permutes these 3 roots in the following ways given by cycle notation:

$$\alpha_0 = (2\ 3), \quad \alpha_1 = (1\ 2\ 3), \quad \alpha_1' = (1\ 2), \quad \alpha_2 = (1\ 3\ 2), \quad \alpha_2' = (1\ 3).$$

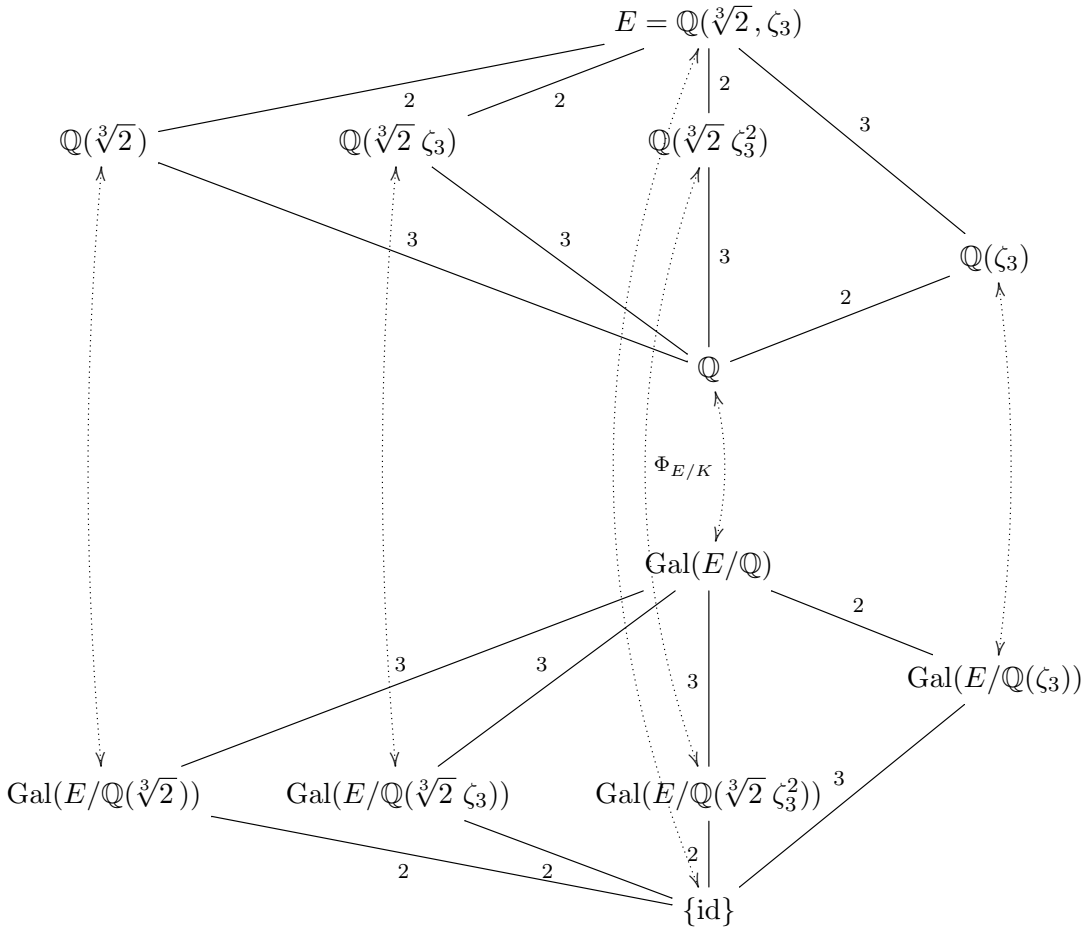



FIGURE 4.1. The Galois Correspondence for $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

We find that

$$\mathrm{Gal}(E/\mathbb{Q}(\zeta_3)) = \{\mathrm{id}, \alpha_1, \alpha_2\} \cong \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \qquad \mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}, \alpha_0\} \cong \{\mathrm{id}, (2\ 3)\},$$
$$\mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2}\,\zeta_3)) = \{\mathrm{id}, \alpha_2'\} \cong \{\mathrm{id}, (1\ 3)\}, \qquad \mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2)) = \{\mathrm{id}, \alpha_1'\} \cong \{\mathrm{id}, (1\ 2)\}.$$

Notice that $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} \lhd \mathrm{S}_3$ and so $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is a normal extension. Of course $\mathbb{Q}(\zeta_3)$ is the splitting field of $X^3 - 1$ over $\mathbb{Q}$.

### 4.6. Galois extensions inside the complex numbers and complex conjugation

When working with Galois extensions contained in the complex numbers it is often useful to make use of complex conjugation as an element of a Galois group. Let $E/\mathbb{Q}$ be a finite Galois extension with $E/\mathbb{Q} \leqslant \mathbb{C}/\mathbb{Q}$. Setting $E_{\mathbb{R}} = \mathbb{R} \cap E$, we have $\mathbb{Q} \leqslant E_{\mathbb{R}} \leqslant E$.

4.21. PROPOSITION. *Complex conjugation* $\overline{(\ )}\colon \mathbb{C} \longrightarrow \mathbb{C}$ *restricts to an automorphism of* $E$ *over* $\mathbb{Q}$, $\overline{(\ )}_{E/\mathbb{Q}}\colon E \longrightarrow E$. *Furthermore,*

(i) $\overline{(\ )}_{E/\mathbb{Q}}$ *agrees with the identity function if and only if* $E_{\mathbb{R}} = E$.

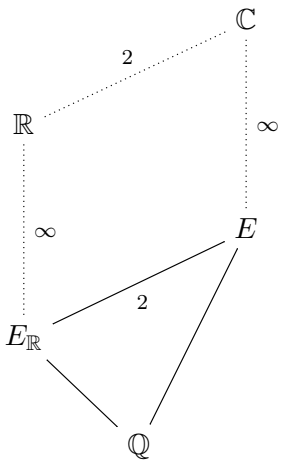
(ii) *If* $E_{\mathbb{R}} \neq E$, *then*

$$\left\langle \overline{(\ )}_{E/\mathbb{Q}} \right\rangle = \{\mathrm{id}, \overline{(\ )}_{E/\mathbb{Q}}\} \cong \mathbb{Z}/2,$$

*hence,* $E_{\mathbb{R}} = E^{\left\langle \overline{(\ )}_{E/\mathbb{Q}} \right\rangle}$ *and* $[E : E_{\mathbb{R}}] = 2$.

PROOF. Let $u \in E$. As $E/\mathbb{Q}$ is normal, $\mathrm{minpoly}_{\mathbb{Q},u}(X) \in \mathbb{Q}[X]$ splits over $E$, so all of its complex roots lie in $E$. But $\overline{(\ )}$ permutes the roots of this minimal polynomial. Therefore $\overline{(\ )}$ maps $E$ into itself.
(i) For $z \in \mathbb{C}$, $\overline{z} = z$ if and only if $z \in \mathbb{R}$.
(ii) Here $|\langle \overline{(\ )}_{E/\mathbb{Q}} \rangle| = 2$, and

$$E^{\langle \overline{(\ )}_{E/\mathbb{Q}} \rangle} = \{u \in E : \overline{u} = u\} = E_{\mathbb{R}}.$$




□

We will usually write $\overline{(\ )}$ rather than $\overline{(\ )}_{E/\mathbb{Q}}$ when no confusion seems likely to result.

4.22. EXAMPLE. Consider the cyclotomic extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ where

$$\zeta_8 = e^{\pi i/4} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\, i.$$

From Example 4.9 we know that

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}\,, i), \quad [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4,$$

and we easily see that

$$\mathbb{Q}(\zeta_8)_{\mathbb{R}} = \mathbb{Q}(\sqrt{2}\,).$$

## 4.7. Galois groups of even and odd permutations

We have seen that for a monic separable polynomial $f(X) \in K[X]$ of degree $n$, the Galois group of its splitting field $E$ over $K$ can naturally be thought of as a subgroup of the symmetric group $\mathrm{S}_n$, where we view the latter as permuting the roots of $f(X)$. It is reasonable to ask when $\mathrm{Gal}(E/K) \leqslant \mathrm{A}_n$ rather than just $\mathrm{Gal}(E/K) \leqslant \mathrm{S}_n$.

We first recall an interpretation of the *sign* of a permutation $\sigma \in \mathrm{S}_n$, $\operatorname{sgn}\sigma = \pm 1$. For each pair $i, j$ with $1 \leqslant i < j \leqslant n$, exactly one of the inequalities $\sigma(i) < \sigma(j)$ or $\sigma(j) < \sigma(i)$ must hold and the ratio $(\sigma(j) - \sigma(i))/(j - i)$ is either positive or negative. It is easily verified that the right-hand side of the following equation must have value $\pm 1$ and so

$$\operatorname{sgn}\sigma = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}\,. \tag{4.3}$$

Note that this is sometimes used as the definition of $\operatorname{sgn}\sigma$.

Suppose that $f(X)$ factorizes over $E$ as

$$f(X) = (X - u_1)\cdots(X - u_n) = \prod_{i=1}^{n}(X - u_i).$$

Here $u_1, \ldots, u_n \in E$ are the roots of $f(X)$; as we have assumed that $f(X)$ is separable, the $u_i$ are distinct.

4.23. Definition. The *discriminant* of $f(X)$ is

$$\operatorname{Discr}(f(X)) = \prod_{1\leqslant i<j\leqslant n} (u_j - u_i)^2 \in E.$$

Notice that $\operatorname{Discr}(f(X)) \neq 0$ since $u_i \neq u_j$ if $i \neq j$.

4.24. Remark. There is an explicit formula for computing $\operatorname{Discr}(f(X))$ is terms of its coefficients. For polynomials

$$p(X) = a_0 + a_1X + \cdots + a_mX^m, \quad q(X) = b_0 + b_1X + \cdots + b_nX^n,$$

their *resultant* is the $(m+n)\times(m+n)$ determinant (with $n$ rows of $a_i$'s and $m$ rows of $b_i$'s)

$$\operatorname{Res}(p(X), q(X)) = \begin{vmatrix} a_0 & a_1 & \ldots & a_m & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_m & 0 & \ldots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_m \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_n \end{vmatrix}. \tag{4.4}$$

In particular, if $f(X)$ is monic with $\deg f(X) = n$,

$$\operatorname{Discr}(f(X)) = (-1)^{n(n-1)/2}\operatorname{Res}(f(X), f'(X)). \tag{4.5}$$

So for example,

$$\begin{aligned}\operatorname{Discr}(X^3 + pX + q) &= (-1)^3\operatorname{Res}(X^3 + pX + q, 3X^2 + p) \\ &= (-1)\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = -4p^3 - 27q^2.\end{aligned}$$

Here are some low degree examples of discriminants obtained with the aid of Maple.

$n = 2$: $$\operatorname{Discr}(a_0 + a_1X + X^2) = -4a_0 + a_1^2.$$

$n = 3$: $$\operatorname{Discr}(a_0 + a_1X + a_2X^2 + X^3) = -27a_0^2 + 18a_0a_1a_2 + a_1^2a_2^2 - 4a_2^3a_0 - 4a_1^3.$$

$n = 4$: $$\begin{aligned}\operatorname{Discr}(a_0 + a_1X + a_2X^2 + a_3X^3 + X^4) &= 18a_3a_1^3a_2 - 6a_3^2a_1^2a_0 - 192a_3a_1a_0^2 - 27a_1^4 \\ &+ 144a_2a_3^2a_0^2 + 144a_0a_1^2a_2 + 256a_0^3 - 4a_3^3a_1^3 - 128a_2^2a_0^2 + 16a_2^4a_0 - 4a_2^3a_1^2 \\ &+ 18a_3^3a_1a_2a_0 - 80a_3a_1a_2^2a_0 - 27a_3^4a_0^2 + a_2^2a_3^2a_1^2 - 4a_2^3a_3^2a_0.\end{aligned}$$

$$\begin{aligned}n=5:\quad \operatorname{Discr}(a_0+a_1X+a_2X^2+a_3X^3+a_4X^4+X^5) &= 2250a_4a_3^2a_0^3 - 36a_0a_4^3a_1^3 - 128a_3^2a_1^4\\ &+ 2000a_0^2a_3a_1^2 - 900a_1a_3^3a_0^2 - 2500a_0^3a_4a_1 - 50a_0^2a_4^2a_1^2 - 900a_4a_2^3a_0^2 - 27a_4^4a_1^4 - 3750a_3a_2a_0^3\\ &+ 356{a_3}^2{a_2}^2a_4a_1a_0 + 560a_3a_2^2a_4^2a_0^2 - 2050a_3a_2a_0^2a_4a_1 - 80a_3^2a_2a_4{a_1}^3 + 825a_3^2a_2^2a_0^2\\ &+ 16a_3^3a_2^3a_0 + 2000a_2a_4^2a_0^3 - 6a_2^2a_4^2a_1^3 - 128a_2^2a_4^4a_0^2 + 16a_2^4a_4^3a_0 - 4a_2^3a_4^3a_1^2 - 630{a_3}^3a_2a_4{a_0}^2\\ &+ 108a_3^5a_0^2 + 108a_2^5a_0 - 746a_3a_2a_0a_4{a_1}^2a_1^2 - 27a_2^4a_1^2 + 256a_4^5a_0^3 - 4a_3^3a_2^2a_1^2 + 144a_3a_2^2a_1^3\\ &+ 144a_4^2a_1^4a_3 + 3125a_0^4 + 256a_1^5 - 72a_3^4a_2a_1a_0 + 18a_3a_2a_3^3a_4^3a_1^3 + 560a_3^2a_2a_0a_1^2 + 16a_3^4a_1^3\\ &+ 18a_3{a_2}^3a_4{a_1}^2 - 72a_3{a_2}^4a_4a_0 + 144{a_3}^2a_2{a_4}^3{a_0}^2 - 192{a_4}^4a_1a_3{a_0}^2 - 630a_3{a_2}^3a_1a_0\\ &+ 24{a_2}^3{a_4}^2a_1a_0 + {a_3}^2{a_2}^2{a_4}^2{a_1}^2 - 6{a_4}^3{a_1}^2{a_3}^2a_0 - 80a_3{a_2}^2{a_4}^3a_1a_0 - 4{a_3}^2{a_2}^3{a_4}^2a_0\\ &+ 2250a_1a_2^2a_0^2 - 1600a_3a_4^3a_0^3 - 192a_4a_1^4a_2 - 1600a_0a_1^3a_2 - 4a_3^3a_1^3a_4^2 - 27a_3^4a_4^2a_0^2\\ &+ 1020{a_4}^2{a_3}^2{a_0}^2a_1 + 18{a_3}^3a_2{a_4}^2a_0a_1 + 160a_2{a_4}^3{a_0}^2a_1 + 144a_2{a_4}^4a_0{a_1}^2\\ &+ 24a_4{a_1}^2{a_3}^3a_0 + 1020a_0a_4{a_2}^2{a_1}^2 + 160a_0a_4{a_1}^3a_3.\end{aligned}$$

So for example,

$$\operatorname{Discr}(X^5+a_4X^4+a_0) = a_0^3(3125a_0+256a_4^5),\quad \operatorname{Discr}(X^5+a_1X+a_0) = 256a_1^5+3125a_0^4.$$

4.25. Proposition. *For every* $\sigma\in\operatorname{Gal}(E/K)$,

$$\sigma(\operatorname{Discr}(f(X))) = \operatorname{Discr}(f(X)).$$

*Hence* $\operatorname{Discr}(f(X))\in E^{\operatorname{Gal}(E/K)} = K$.

Proof. For $\sigma\in\operatorname{Gal}(E/K)\leqslant \mathrm{S}_n$, we have

$$\sigma(\operatorname{Discr}(f(X))) = \prod_{1\leqslant i<j\leqslant n}(u_{\sigma(j)}-u_{\sigma(i)})^2 = \left(\prod_{1\leqslant i<j\leqslant n}(u_{\sigma(j)}-u_{\sigma(i)})\right)^2.$$

Now for each pair $i,j$ with $i<j$,

$$\sigma(u_j-u_i) = u_{\sigma(j)}-u_{\sigma(i)},$$

and by Equation (4.3)

$$\prod_{1\leqslant i<j\leqslant n}(u_{\sigma(j)}-u_{\sigma(i)}) = \operatorname{sgn}\sigma\prod_{1\leqslant i<j\leqslant n}(u_j-u_i) = (\pm1)\prod_{1\leqslant i<j\leqslant n}(u_j-u_i). \tag{4.6}$$

Hence $\sigma(\operatorname{Discr}(f(X))) = \operatorname{Discr}(f(X))$. Since $E^{\operatorname{Gal}(E/K)} = K$, we have $\operatorname{Discr}(f(X))\in K$. □

Now let

$$\delta(f(X)) = \prod_{1\leqslant i<j\leqslant n}(u_j-u_i)\in E.$$

Then $\delta(f(X))^2 = \operatorname{Discr}(f(X))$, so the square roots of $\operatorname{Discr}(f(X))$ are $\pm\delta(f(X))$. Now consider the effect of $\sigma\in\operatorname{Gal}(E/K)$ on $\delta(f(X))\in E$. By Equation (4.6),

$$\sigma(\delta(f(X))) = \operatorname{sgn}\sigma\,\delta(f(X)) = \pm\delta(f(X)).$$

If $\delta(f(X))\in K$, this means that $\operatorname{sgn}\sigma = 1$. On the other hand, if $\delta(f(X))\notin K$ then

$$K(\delta(f(X))) = E^{\operatorname{Gal}(E/K)\cap \mathrm{A}_n}.$$

Of course $|\operatorname{Gal}(E/K)/\operatorname{Gal}(E/K)\cap \mathrm{A}_n| = 2$.

4.26. Proposition. *The Galois group* $\mathrm{Gal}(E/K) \leqslant \mathrm{S}_n$ *is contained in* $\mathrm{A}_n$ *if and only if* $\mathrm{Discr}(f(X))$ *is a square in* $K$.

4.27. Example. For the polynomials of Examples 6.40 and 6.42 we obtain

$$\begin{aligned}
\mathrm{Discr}(X^5 - 35X^4 + 7) &= -4611833296875 = -3^3 \cdot 5^6 \cdot 7^4 \cdot 29 \cdot 157, \\
\delta(X^5 - 35X^4 + 7) &= \pm 5^3 \cdot 3 \cdot 7^2 \cdot \sqrt{3 \cdot 29 \cdot 157}\, i = \pm 18375\sqrt{13659}\, i \notin \mathbb{Q}; \\
\mathrm{Discr}(X^5 + 20X + 16) &= 1024000000 = 2^{16} \cdot 5^6, \\
\delta(X^5 + 20X + 16) &= \pm 2^8 5^3 \in \mathbb{Q}.
\end{aligned}$$

## 4.8. Kaplansky's Theorem

In this section we give a detailed account of the Galois theory of irreducible rational polynomials $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$. The following result describes the Galois groups that occur and the proof introduces some useful computational techniques.

4.28. Theorem (Kaplansky's Theorem). *Let* $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ *be irreducible.*

(i) *If* $b$ *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
(ii) *If* $b(a^2 - 4b)$ *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}/4$.
(iii) *If neither* $b$ *nor* $b(a^2 - 4b)$ *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{D}_8$.

Proof. Let $g(X) = X^2 + aX + b \in \mathbb{Q}[X]$. Notice that $g(X)$ must be irreducible since otherwise $f(X)$ would factorize, hence $(a^2 - 4b)$ is not a square in $\mathbb{Q}$. Setting $d = (a^2 - 4b) \in \mathbb{Q}$ and taking $\delta$ to be a square root of $d$ (so $\delta \notin \mathbb{Q}$), we find that the roots of $g(X)$ are $(-a \pm \delta)/2 \notin \mathbb{Q}$. Then the roots of $f(X)$ are $\pm u, \pm v$, where

$$u^2 = \frac{(-a + \delta)}{2}, \quad v^2 = \frac{(-a - \delta)}{2},$$

so the splitting field of $f(X)$ over $\mathbb{Q}$ is $E = \mathbb{Q}(u, v)$ which contains the quadratic extension $\mathbb{Q}(\delta)/\mathbb{Q}$. Since $\deg f(X) = 4$, we also have $4 \mid [E : \mathbb{Q}]$. In fact, since $E$ is obtained by at most 3 successive quadratic extensions we also have $[E : \mathbb{Q}] \mid 8$.
(i) We have

$$(uv)^2 = u^2 v^2 = \frac{a^2 - d}{4} = \frac{4b}{4} = b,$$

hence $uv$ is a square root of $b$ which is in $\mathbb{Q}$. Setting $c = uv \in \mathbb{Q}$, we find that $v = c/u \in \mathbb{Q}(u)$. This shows that $E = \mathbb{Q}(u)$ and we have the following Galois tower.

$$\begin{array}{c} E = \mathbb{Q}(u) \\ \Big| \, 2 \\ \mathbb{Q}(\delta) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

In particular $[E : \mathbb{Q}] = 4 = |\mathrm{Gal}(E/\mathbb{Q})|$. Notice that for the Galois extension $\mathbb{Q}(\delta)/\mathbb{Q}$ there must be a normal subgroup $N \lhd \mathrm{Gal}(E/\mathbb{Q})$ with

$$\mathbb{Q}(\delta) = E^N, \quad \mathrm{Gal}(\mathbb{Q}(\delta)/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q})/N.$$

Hence there is an element $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ for which $\sigma(\delta) = -\delta$. This element must also have the effects $\sigma(u) = \pm v$ and $\sigma(v) = \pm u$. Given $u$ we might as well choose $v$ so that $\sigma(u) = v$. There is also an element $\tau \in N$ for which $\tau(u) = -u$ and we also have $\tau(v) = -v$. Notice that if $\sigma(v) = -u$ then easy calculation shows that

$$\tau\sigma(v) = \sigma\tau(v) = u, \quad \tau\sigma(\delta) = \sigma\tau(\delta) = -\delta,$$

hence we might as assume that $\sigma(v) = u$ since if necessary we can replace our original choice by $\tau\sigma$.

We now have

$$\sigma(u) = \frac{c}{u}, \quad \tau(u) = -u, \quad \tau\sigma(u) = \sigma\tau(u) = -\frac{c}{u}.$$

These satisfy

$$\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id} = \text{the identity}, \quad \sigma\tau = \tau\sigma.$$

This shows that

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2 = \text{the Klein 4-group}.$$

(ii) If $bd$ is a square in $\mathbb{Q}$, then

$$(uv\delta)^2 = u^2v^2d = bd,$$

which is a square in $\mathbb{Q}$, so we can write $uv\delta = c \in \mathbb{Q}$ or equivalently $v = c/(u\delta) \in \mathbb{Q}(u)$ since $\mathbb{Q}(\delta) \leqslant \mathbb{Q}(u)$. This shows that $E = \mathbb{Q}(u, v) = \mathbb{Q}(u)$ and again we have a Galois tower

$$\begin{array}{c} E = \mathbb{Q}(u) \\ \Big| \, 2 \\ \mathbb{Q}(\delta) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

with $[E : \mathbb{Q}] = 4 = |\,\mathrm{Gal}(E/\mathbb{Q})|$.

Since $\mathbb{Q}(\delta)/\mathbb{Q}$ is Galois there is an element $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ with $\sigma(\delta) = -\delta$ and this has the effect $\sigma(u) = \pm v$; given $u$ we might as well choose $v$ so that $\sigma(u) = v$. Notice that

$$\sigma(v) = \frac{c}{\sigma(u\delta)} = -\frac{c}{v\delta} = -u,$$

so $\sigma^2(u) = -u$. This shows that

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2\sigma^3\} \cong \mathbb{Z}/4 = \text{a cyclic group of order 4}.$$

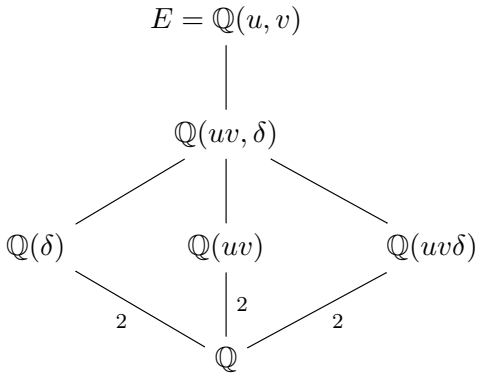
(iii) Suppose that $d$, $b$ and $bd$ are not squares in $\mathbb{Q}$. By an easy calculation we find that $(uv)^2 = b$, so $uv \in E$ is a square root of $b$ in $E$. Suppose that $uv \in \mathbb{Q}(\delta)$; then $uv = p + q\delta$ for some $p, q \in \mathbb{Q}$. By squaring we obtain

$$b = (p^2 + q^2d) + 2pq\delta,$$

and so $pq = 0$. We cannot have $q = 0$ since this would imply that $b$ was a square in $\mathbb{Q}$; if $p = 0$ then $b = q^2d$ and so $bd = (qd)^2$, implying that $bd$ was a square in $\mathbb{Q}$. Thus we have $\mathbb{Q}(uv) \cap \mathbb{Q}(\delta) = \mathbb{Q}$. A similar discussion shows that

$$\mathbb{Q}(uv\delta) \cap \mathbb{Q}(\delta) = \mathbb{Q} = \mathbb{Q}(uv\delta) \cap \mathbb{Q}(uv).$$

So we have a Galois tower which includes the following subfields.




Choose

$$\alpha \in \mathrm{Gal}(E/\mathbb{Q}(uv)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

so that $\alpha(\delta) = -\delta$. By renaming $-v$ to $v$ if necessary, we may assume that $v = \alpha(u)$ and so $u = \alpha(v)$. Notice that $\alpha^2 = \mathrm{id}$.

Choose

$$\beta \in \mathrm{Gal}(E/\mathbb{Q}(\delta)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

with $\beta(uv) = -uv$. We must have either $\beta(u) = -u$ or $\beta(v) = -v$, so by interchanging $\pm\delta$ if necessary we can assume that $\beta(u) = -u$ and $\beta(v) = v$. Notice that $\beta^2 = \mathrm{id}$.

Choose

$$\gamma \in \mathrm{Gal}(E/\mathbb{Q}(\delta, uv)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

so that $\gamma(u) = -u$. Then we must have $\gamma(v) = -v$ since $\gamma(uv) = uv$. Notice that $\gamma^2 = \mathrm{id}$.

Setting $\sigma = \alpha\beta$ we find $\sigma(u) = -v$ and $\sigma(v) = u$. Then $\sigma^2 = \gamma$ and $\sigma$ has order 4. Also,

$$\alpha\sigma\alpha = \beta\sigma\beta = \sigma^{-1}.$$

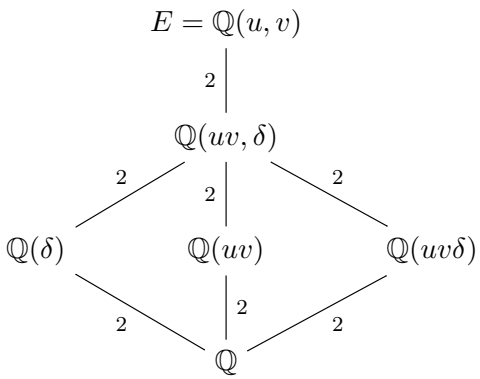
The eight elements

$$\mathrm{id}, \sigma, \gamma, \sigma^{-1}, \alpha, \alpha\sigma, \alpha\gamma, \alpha\sigma^{-1}$$

form a group isomorphic to the dihedral group of order 8, $\mathrm{D}_8$. Therefore we have

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{D}_8,$$

and $[E : \mathbb{Q}] = 8$. The corresponding Galois tower is




□

4.29. Example. We have the following Galois groups:

$$\mathrm{Gal}(\mathbb{Q}(X^4+1)/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2; \quad \mathrm{Gal}(\mathbb{Q}(X^4+4X^2+2)/\mathbb{Q}) \cong \mathbb{Z}/4;$$
$$\mathrm{Gal}(\mathbb{Q}(X^4+2X^2+2)/\mathbb{Q}) \cong \mathrm{D}_8\,.$$

## Exercises for Chapter 4

**4.1** If $f(X) \in K[X]$ is a separable polynomial, prove that the splitting field of $f(X)$ over $K$ is a finite Galois extension of $K$.

**4.2** Let $K$ be a field for which $\operatorname{char} K \neq 2, 3$ and suppose that $f(X) \in K[x]$ is a cubic polynomial.

(a) Show that there $u, v \in \overline{K}$ with $u \neq 0$ such that $f(uX + v) = X^3 + aX + b$ for some $a, b \in \overline{K}$. If $f(X)$ is monic, deduce that $a, b \in K$; under what conditions is this always true?

(b) If $g(X) = X^3 + aX + b \in K[x]$ is irreducible and $E = K(g(X))$ is its splitting field over $K$, explain why $\operatorname{Gal}(E/K)$ is isomorphic to one of the groups $\mathrm{S}_3$ or $\mathrm{A}_3$.

(c) Continuing with the notation and assumptions of (b), suppose that $w_1, w_2, w_3$ are the distinct roots of $g(X)$ in $E$ and let

$$\Delta = (w_1 - w_2)^2(w_2 - w_3)^2(w_1 - w_3)^2 \in E.$$

Show that

$$\Delta = -4b^3 - 27a^2,$$

and hence $\Delta \in K$. If $\delta = (w_1 - w_2)(w_3 - w_3)(w_1 - w_3)$, show that

$$\operatorname{Gal}(E/K) \cong \begin{cases} \mathrm{A}_3 & \text{if } \delta \in K, \\ \mathrm{S}_3 & \text{if } \delta \notin K. \end{cases}$$

[*Hint: Consider $K(\delta) \leqslant E$ and the effect on the element $\delta$ of even and odd permutations in* $\operatorname{Gal}(E/K) \leqslant \mathrm{S}_3$.]

**4.3** Show that $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$, and show that its discriminant is a square in $\mathbb{Q}$. Prove that the Galois group of $f(X)$ over $\mathbb{Q}$ is cyclic.

**4.4** This is a revision exercise on finite groups of small order.

(a) Show that every non-abelian finite group has order at least 6.

(b) Let $\mathrm{D}_8$ be the dihedral group with the eight elements

$$\iota, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$$

satisfying

$$\alpha^4 = \iota, \quad \beta^2 = \iota, \quad \beta\alpha\beta = \alpha^{-1} = \alpha^3.$$

Find all the normal subgroups of $\mathrm{D}_8$.

**4.5** Use Kaplansky's Theorem 4.28 to find the Galois group of the splitting field $E$ of the polynomial $X^4 + 3 \in \mathbb{Q}[X]$ over $\mathbb{Q}$. Determine all the subextensions $F \leqslant E$ for which $F/\mathbb{Q}$ is Galois.

**4.6** Find the Galois groups for each of the following extensions:
$\mathbb{Q}(X^3 - 10)/\mathbb{Q}$; $\mathbb{Q}(\sqrt{2})(X^3 - 10)/\mathbb{Q}(\sqrt{2})$; $\mathbb{Q}(\sqrt{3}\,i)(X^3 - 10)/\mathbb{Q}(\sqrt{3}\,i)$;
$\mathbb{Q}(\sqrt{23}\,i)(X^3 - X - 1)/\mathbb{Q}(\sqrt{23}\,i)$; $K(X^3 - X - 1)/K$ for $K = \mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{5}\,i)$, $\mathbb{Q}(i)$.

**4.7** Let $p > 0$ be a prime. Let $K$ be a field with $\operatorname{char} K \neq p$. Suppose that $0 \neq a \in K$ and $f(X) = X^p - a \in K[X]$. Let $L/K$ where $L$ is a splitting field for $f(X)$ over $K$.

(a) Show that $f(X)$ has $p$ distinct roots in $L$. If $u \in L$ is one such root, describe the remaining roots and show that $L$ contains $p$ distinct $p$-th roots of 1.

(b) Suppose that $K$ contains $p$ distinct $p$-th roots of 1. Show that either $f(X)$ is irreducible over $K$ or it factors into $p$ distinct linear factors over $K$.

(c) Suppose that the only $p$-th root of 1 in $K$ is 1. Show that either $f(X)$ is irreducible over $K$ or it has a root in $K$.

**4.8** Let $K$ be a field of characteristic $\operatorname{char} K = p$ where $p > 0$ is a prime. Suppose that $0 \neq a \in K$ and $f(X) = X^p - a \in K[X]$. Show that if $f(X)$ has no root in $K$ then it is irreducible over $K$.

**4.9** (a) Verify that the resultant of Definition 4.24 satisfies the following identities:

$$\begin{aligned}
\operatorname{Res}(p(X), q(X) + X^r p(X)) &= \operatorname{Res}(p(X), q(X)), \\
\operatorname{Res}(p(X) + X^s q(X), q(X)) &= \operatorname{Res}(p(X), q(X)), \\
\operatorname{Res}(q(X), p(X)) &= (-1)^{mn} \operatorname{Res}(p(X), q(X)), \\
\operatorname{Res}(aq(X), bp(X)) &= a^n b^m \operatorname{Res}(p(X), q(X)),
\end{aligned}$$

where $a, b \in K$, $r \leqslant n$ and $s \leqslant n$.

(b) Deduce that $\operatorname{Res}(p(X), q(X)) = 0$ if and only if $\gcd(p(X), q(X)) \neq 1$.

(c) Show that for a non-constant polynomial $f(X)$, $\operatorname{Res}(f(X), f'(X)) = 0$ if and only if $f(X)$ has no multiple roots in any extension field of $K$.

CHAPTER 5

# Galois extensions for fields of positive characteristic

In this chapter we will investigate extensions of fields of positive characteristic, especially finite fields. A thorough account of finite fields and their applications can be found in [**6**].

Throughout this chapter we will assume that $K$ is a field of prime characteristic $p = \operatorname{char} K > 0$, containing the prime subfield $\mathbb{F}_p$.

## 5.1. Finite fields

If $K$ is a finite field, then $K$ is an $\mathbb{F}_p$-vector space. Our first goal is to count the elements of $K$. Here is a more general result.

5.1. Lemma. *Let $F$ be a finite field with $q$ elements and let $V$ be an $F$-vector space. Then $\dim_F V < \infty$ if and only if $V$ is finite in which case $|V| = q^{\dim_F V}$.*

Proof. If $d = \dim_F V < \infty$, then for a basis $v_1, \dots, v_d$ we can express each element $v \in V$ uniquely in the form $v = t_1 v_1 + \cdots + t_d v_d$, where $t_1, \dots, t_d \in F$. Clearly there are exactly $q^d$ such expressions, so $|V| = q^d$.

Conversely, if $V$ is finite then any basis has finitely many elements and so $\dim_F V < \infty$. □

5.2. Corollary. *Let $F$ be a finite field and $E/F$ an extension. Then $E$ is finite if and only if $E/F$ is finite and then $|E| = |F|^{[E:F]}$.*

5.3. Corollary. *Let $K$ be a finite field. Then $K/\mathbb{F}_p$ is finite and $|K| = p^{[K:\mathbb{F}_p]}$.*

Our next task is to show that for each power $p^d$ there is a finite field with $p^d$ elements. We start with the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ and consider the polynomial

$$\Theta_{p^d}(X) = X^{p^d} - X \in \mathbb{F}_p[X].$$

Notice that $\Theta'_{p^d}(X) = -1$, hence by Proposition 3.55 every root of $\Theta_{p^d}(X)$ in $\overline{\mathbb{F}}_p$ is simple. Therefore by Corollary 1.35 $\Theta_{p^d}(X)$ must have exactly $p^d$ distinct roots in $\overline{\mathbb{F}}_p$, say $0, u_1, \dots, u_{p^d-1}$. Then in $\overline{\mathbb{F}}_p[X]$ we have

$$X^{p^d} - X = X(X - u_1) \cdots (X - u_{p^d-1}),$$

and each root is separable over $\mathbb{F}_p$. Let

$$\mathbb{F}_{p^d} = \{u \in \overline{\mathbb{F}}_p : \Theta_{p^d}(u) = 0\} \subseteq \overline{\mathbb{F}}_p, \quad \mathbb{F}^0_{p^d} = \{u \in \mathbb{F}_{p^d} : u \neq 0\}.$$

Notice that $u \in \mathbb{F}^0_{p^d}$ if and only if $u^{p^d-1} = 1$.

5.4. Proposition. *For each $d \geqslant 1$, $\mathbb{F}_{p^d}$ is a finite subfield of $\overline{\mathbb{F}}_p$ with $p^d$ elements and $\mathbb{F}^0_{p^d} = \mathbb{F}^\times_{p^d}$. Furthermore, the extension $\mathbb{F}_{p^d}/\mathbb{F}_p$ is a separable splitting field.*

PROOF. If $u, v \in \mathbb{F}_{p^d}$ then by the Idiot's Binomial Theorem 1.11,

$$(u+v)^{p^d} - (u+v) = (u^{p^d} + v^{p^d}) - (u+v) = (u^{p^d} - u) + (v^{p^d} - v) = 0,$$
$$(uv)^{p^d} - uv = u^{p^d} v^{p^d} - uv = uv - uv = 0.$$

Furthermore, if $u \neq 0$ then $u^{p^d-1} = 1$ and so $u$ has multiplicative inverse $u^{p^d-2}$. Hence $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$. Notice that $\mathbb{F}_p \leqslant \mathbb{F}_{p^d}$, so $\mathbb{F}_{p^d}/\mathbb{F}_p$ is a finite extension. In any field the non-zero elements are always invertible, hence $\mathbb{F}_{p^d}^0 = \mathbb{F}_{p^d}^\times$. □

5.5. DEFINITION. The finite subfield $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ is called the *Galois field of order* $p^d$.

The notation $\mathrm{GF}(p^d)$ is often used in place of $\mathbb{F}_{p^d}$. Of course, $\mathbb{F}_{p^1} = \mathrm{GF}(p^1) = \mathrm{GF}(p) = \mathbb{F}_p$ and $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$.

5.6. PROPOSITION. *Let* $d \geqslant 1$.

(i) $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ *is the splitting subfield for each of the polynomials* $X^{p^d} - X$ *and* $X^{p^d-1} - 1$ *over* $\mathbb{F}_p$.
(ii) $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ *is the unique subfield with* $p^d$ *elements.*
(iii) *If* $F$ *is any field with* $p^d$ *elements then there is a monomorphism* $F \longrightarrow \overline{\mathbb{F}}_p$ *with image* $\mathbb{F}_{p^d}$, *hence* $F \cong \mathbb{F}_{p^d}$.

PROOF. (i) As $\mathbb{F}_{p^d}$ consists of exactly the roots of $\Theta_{p^d}(X)$ in $\overline{\mathbb{F}}_p$, it is the splitting subfield. The non-zero elements of $\mathbb{F}_{p^d}$ are the roots of $X^{p^d-1} - 1$, so $\mathbb{F}_{p^d}$ is also the splitting subfield for this polynomial.
(ii) Let $F \leqslant \overline{\mathbb{F}}_p$ have $p^d$ elements. Notice that the non-zero elements of $F$ form a group $F^\times$ under multiplication. This group is abelian and has $p^d - 1$ elements, so by Lagrange's Theorem, each element $u \in F^\times$ has order dividing $p^d - 1$, therefore $u^{p^d-1} = 1$ and so $u^{p^d} = u$. But this means every element of $F$ is a root of $\Theta_{p^d}(X)$ and so $F \leqslant \mathbb{F}_{p^d}$; equality follows since these subfields both have $p^d$ elements.
(iii) Apply the Monomorphism Extension Theorem 3.49 for $K = L = \mathbb{F}_p$ and $M = F$. By (ii), the image of the resulting monomorphism must be $\mathbb{F}_{p^d}$, therefore $F \cong \mathbb{F}_{p^d}$. □

It is worth noting the following consequence of this result and the construction of $\mathbb{F}_{p^d}$.

5.7. COROLLARY. *Let* $K$ *be a finite field of characteristic* $p$. *Then* $K/\mathbb{F}_p$ *is a finite Galois extension.*

5.8. EXAMPLE. Consider the polynomial $X^4 - X \in \mathbb{F}_2[X]$. By inspection, in the ring $\mathbb{F}_2[X]$ we find that

$$X^4 - X = X^4 + X = X(X^3 + 1) = X(X+1)(X^2 + X + 1).$$

Now $X^2 + X + 1$ has no root in $\mathbb{F}_2$ so it must be irreducible in $\mathbb{F}_2[X]$. Its splitting field is a quadratic extension $\mathbb{F}_2(w)/\mathbb{F}_2$ where $w$ is one of the roots of $X^2 + X + 1$, the other being $w + 1$ since the sum of the roots is the coefficient of $X$. This tells us that every element of $\mathbb{F}_4 = \mathbb{F}_2(w)$ can be uniquely expressed in the form $a + bw$ with $a, b \in \mathbb{F}_2$. To calculate products we use the fact that $w^2 = w + 1$, so for $a, b, c, d \in \mathbb{F}_2$ we have

$$(a+bw)(c+dw) = ac + (ad+bc)w + bdw^2 = (ac+bd) + (ad+bc+bd)w.$$

5.9. Example. Consider the polynomial $X^9 - X \in \mathbb{F}_3[X]$. Let us find an irreducible polynomial of degree 2 in $\mathbb{F}_3[X]$. Notice that $X^2+1$ has no root in $\mathbb{F}_3$, hence $X^2+1 \in \mathbb{F}_3[X]$ is irreducible; so if $u \in \overline{\mathbb{F}}_3$ is a root of $X^2+1$ then $\mathbb{F}_3(u)/\mathbb{F}_3$ has degree 2 and $\mathbb{F}_3(u) = \mathbb{F}_9$. Every element of $\mathbb{F}_9$ can be uniquely expressed in the form $a + bu$ with $a, b \in \mathbb{F}_3$. Multiplication is carried out using the relation $u^2 = -1 = 2$.

By inspection, in the ring $\mathbb{F}_3[X]$ we find that

$$X^9 - X = X(X^8 - 1) = (X^3 - X)(X^2 + 1)(X^2 + X - 1)(X^2 - X - 1).$$

So $X^2 + X - 1$ and $X^2 - X - 1$ are also quadratic irreducibles in $\mathbb{F}_3[X]$. We can find their roots in $\mathbb{F}_9$ using the quadratic formula since in $\mathbb{F}_3$ we have $2^{-1} = (-1)^{-1} = -1$. The discriminant of $X^2 + X - 1$ is

$$1 - 4(-1) = 5 = 2 = u^2,$$

so its roots are $(-1)(-1 \pm u) = 1 \pm u$. Similarly, the discriminant of $X^2 - X - 1$ is

$$1 - 4(-1) = 5 = 2 = u^2$$

and its roots are $(-1)(1 \pm u) = -1 \pm u$. Then we have

$$\mathbb{F}_9 = \mathbb{F}_3(u) = \mathbb{F}_3(1 \pm u) = \mathbb{F}_3(-1 \pm u).$$

There are two issues we can now clarify.

5.10. Proposition. *Let $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ be two Galois fields of characteristic $p$. Then $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. If $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$, then by Corollary 5.2,

$$p^n = (p^m)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]} = p^{m[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]},$$

so $m \mid n$.

If $m \mid n$, write $n = km$ with $k \geqslant 1$. Then for $u \in \mathbb{F}_{p^m}$ we have $u^{p^m} = u$, so

$$u^{p^n} = u^{p^{mk}} = (u^{p^m})^{p^{m(k-1)}} = u^{p^{m(k-1)}} = \cdots = u^{p^m} = u.$$

Hence $u \in \mathbb{F}_{p^n}$ and therefore $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$. □

This means that we can think of the Galois fields $\mathbb{F}_{p^n}$ as ordered by divisibility of $n$. The diagram of subfields for $\mathbb{F}_{p^{24}}$ can be seen in Figure 5.1 which shows extensions with no intermediate subextensions.

5.11. Theorem. *The algebraic closure of $\mathbb{F}_p$ is the union of all the Galois fields of characteristic $p$,*

$$\overline{\mathbb{F}}_p = \bigcup_{n \geqslant 1} \mathbb{F}_{p^n}.$$

*Furthermore, each element $u \in \overline{\mathbb{F}}_p$ is separable over $\mathbb{F}_p$.*

Proof. Let $u \in \overline{\mathbb{F}}_p$. Then $u$ is algebraic over $\mathbb{F}_p$ and the extension $\mathbb{F}_p(u)/\mathbb{F}_p$ is finite. Hence by Corollary 5.2, $\mathbb{F}_p(u) \leqslant \overline{\mathbb{F}}_p$ is a finite subfield. Proposition 5.10 now implies that $\mathbb{F}_p(u) = \mathbb{F}_{p^n}$ for some $n$. The separability statement follows from Corollary 5.7. □

We will require a useful fact about Galois fields.

5.12. Proposition. *The group of units $\mathbb{F}_{p^d}^\times$ in $\mathbb{F}_{p^d}$ is cyclic.*

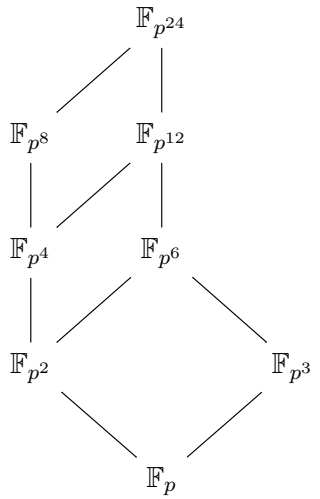



FIGURE 5.1. The subfields of $\mathbb{F}_{p^{24}}$

This is a special case of a more general result about arbitrary fields.

5.13. PROPOSITION. *Let $K$ be a field. Then every finite subgroup $U \leqslant K^\times$ is cyclic.*

PROOF. Use Corollary 1.35 and Lemma 1.46. □

5.14. DEFINITION. $w \in \mathbb{F}_{p^d}^\times$ is called a *primitive root* if it is a primitive $(p^d-1)$-th root of unity, *i.e.*, its order in the group $\mathbb{F}_{p^d}^\times$ is $(p^d-1)$, hence $\langle w\rangle = \mathbb{F}_{p^d}^\times$.

5.15. REMARK. Unfortunately the word *primitive* has two confusingly similar uses in the context of finite fields. Indeed, some authors use the term *primitive element* for what we have called a *primitive root*, but that conflicts with our usage, although as we will in the next result, every primitive root is indeed a primitive element in our sense!

5.16. PROPOSITION. *The extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ is simple,* i.e., *$\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(u)$ for some $u \in \mathbb{F}_{p^{nd}}$.*

PROOF. By Proposition 5.12, $\mathbb{F}_{p^{nd}}$ has a primitive root $w$ say. Then every element of $\mathbb{F}_{p^{nd}}$ can be expressed as a polynomial in $w$, so $\mathbb{F}_{p^{nd}} \leqslant \mathbb{F}_{p^d}(w) \leqslant \mathbb{F}_{p^{nd}}$. This implies that $\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(w)$. □

5.17. REMARK. This completes the proof of the Primitive Element Theorem 3.74 which we had previously only established for infinite fields.

5.18. EXAMPLE. In Example 5.8 we find that $\mathbb{F}_4 = \mathbb{F}_2(w)$ has the two primitive roots $w$ and $w+1$.

5.19. EXAMPLE. In Example 5.9 we have $\mathbb{F}_9 = \mathbb{F}_3(u)$ and $\mathbb{F}_9^\times$ is cyclic of order 8. Since $\varphi(8) = 4$, there are four primitive roots and these are the roots of the polynomials $X^2+X-1$ and $X^2-X-1$ which we found to be $\pm 1 \pm u$.

We record a fact that is very important in Number Theory.

5.20. PROPOSITION. *Let $p > 0$ be an odd prime.*

(i) *If $p \equiv 1 \pmod 4$, the polynomial $X^2+1 \in \mathbb{F}_p[X]$ has two roots in $\mathbb{F}_p$.*

(ii) *If* $p \equiv 3 \pmod 4$ *the polynomial* $X^2+1 \in \mathbb{F}_p[X]$ *is irreducible, so* $\mathbb{F}_{p^2} \cong \mathbb{F}_p[X]/(X^2+1)$.

PROOF. (i) We have $4 \mid (p-1) = |\mathbb{F}_p^\times|$, so if $u \in \mathbb{F}_p^\times$ is a generator of this cyclic group, the order of $u^{|\mathbb{F}_p^\times|/4}$ is 4, hence this is a root of $X^2+1$ (the other root is $-u^{|\mathbb{F}_p^\times|/4}$).
(ii) If $v \in \mathbb{F}_p$ is a root of $X^2+1$ then $v$ has order 4 in $\mathbb{F}_p^\times$. But then $4 \mid (p-1) = |\mathbb{F}_p^\times|$, which is impossible since $p-1 \equiv 2 \pmod 4$. □

Here is a generalization of Proposition 5.20.

5.21. PROPOSITION. $\mathbb{F}_{p^d}$ *contains a primitive* $n$*-th root of unity if and only if* $p^d \equiv 1 \pmod n$ *and* $p \nmid n$.

## 5.2. Galois groups of finite fields and Frobenius mappings

Consider an extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$. By Proposition 5.6(i), Corollary 5.7 and Proposition 3.73, this extension is Galois and

$$|\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})| = [\mathbb{F}_{p^{nd}} : \mathbb{F}_{p^d}] = n.$$

We next introduce an important element of the Galois group $\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$.

5.22. DEFINITION. The (*relative*) *Frobenius mapping* for the extension $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ is the function $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ given by $\mathrm{F}_d(t) = t^{p^d}$.

5.23. PROPOSITION. *The relative Frobenius mapping* $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ *is an automorphism of* $\mathbb{F}_{p^{nd}}$ *that fixes the elements of* $\mathbb{F}_{p^d}$, *so* $\mathrm{F}_d \in \operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$. *The order of* $\mathrm{F}_d$ *is* $n$, *so* $\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle \mathrm{F}_d \rangle$, *the cyclic group generated by* $\mathrm{F}_d$.

PROOF. For $u, v \in \mathbb{F}_{p^{nd}}$, we have the identities

$$\mathrm{F}_d(u+v) = (u+v)^{p^d} = u^{p^d} + v^{p^d}, \quad \mathrm{F}_d(uv) = (uv)^{p^d} = u^{p^d} v^{p^d},$$

so $\mathrm{F}_d$ is a ring homomorphism. Also, for $u \in \mathbb{F}_{p^d}$ we have

$$\mathrm{F}_d(u) = u^{p^d} = u,$$

so $\mathrm{F}_d$ fixes the elements of $\mathbb{F}_{p^d}$. To see that $\mathrm{F}_d$ is an automorphism, notice that the composition power $\mathrm{F}_d^n = \mathrm{F}_d \circ \cdots \circ \mathrm{F}_d$ (with $n$ factors) satisfies

$$\mathrm{F}_d^n(t) = t^{p^{nd}} = t$$

for all $t \in \mathbb{F}_{p^{nd}}$, hence $\mathrm{F}_d^n = \mathrm{id}$. Then $\mathrm{F}_d$ is invertible with inverse $\mathrm{F}_d^{-1} = \mathrm{F}_d^{n-1}$. This also shows that the order of $\mathrm{F}_d$ in the group $\operatorname{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^{nd}})$ is at most $n$. Suppose the order is $k$ with $k \leqslant n$; then every element $u \in \mathbb{F}_{p^{nd}}$ satisfies the equation $\mathrm{F}_d^k(u) = u$ which expands to $u^{p^{kd}} = u$, hence $u \in \mathbb{F}_{p^{kd}}$. But this can only be true if $k = n$. □

Frobenius mappings exist on the algebraic closure $\overline{\mathbb{F}}_p$. For $d \geqslant 1$, consider the function

$$\mathrm{F}_d\colon \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p\,; \quad \mathrm{F}_d(t) = t^{p^d}.$$

5.24. PROPOSITION. *Let* $d \geqslant 1$.

(i) $\mathrm{F}_d\colon \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$ *is an automorphism of* $\overline{\mathbb{F}}_p$ *which fixes the elements of* $\mathbb{F}_{p^d}$. *In fact for* $u \in \overline{\mathbb{F}}_p$, $\mathrm{F}_d(u) = u$ *if and only if* $u \in \mathbb{F}_{p^d}$.

(ii) *The restriction of* $\mathrm{F}_d$ *to the Galois subfield* $\mathbb{F}_{p^{dn}}$ *agrees with the relative Frobenius mapping* $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$.

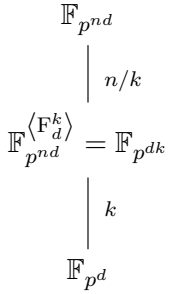
(ii) *If* $k \geqslant 1$, *then* $\mathrm{F}_d^k = \mathrm{F}_{kd}$. *Hence in the automorphism group* $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$, $\mathrm{F}_d$ *has infinite order, so* $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ *is infinite.*

PROOF. This is left as an exercise. □

The Frobenius mapping $\mathrm{F} = \mathrm{F}_1$ is often called the *absolute Frobenius mapping* since it exists as an element of each of the groups $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ and $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ for every $n \geqslant 1$.

In $\mathrm{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle \mathrm{F}_d \rangle$, for each $k$ with $k \mid n$ there is the cyclic subgroup $\langle \mathrm{F}_d^k \rangle$ of order $|\langle \mathrm{F}_d^k \rangle| = n/k$.

5.25. PROPOSITION. *For* $k \mid n$, *the fixed subfield of* $\langle \mathrm{F}_d^k \rangle$ *in* $\mathbb{F}_{p^{nd}}$ *is* $\mathbb{F}_{p^{nd}}^{\langle \mathrm{F}_d^k \rangle} = \mathbb{F}_{p^{dk}}$.




PROOF. For $u \in \mathbb{F}_{p^{nd}}$ we have $\mathrm{F}_d^k(u) = u^{p^{dk}}$, hence $\mathrm{F}_d^k(u) = u$ if and only if $u \in \mathbb{F}_{p^{dk}}$. □

Figure 5.2 shows the subgroup diagram corresponding to the lattice of subfields of $\mathbb{F}_{p^{24}}$ shown in Figure 5.1.

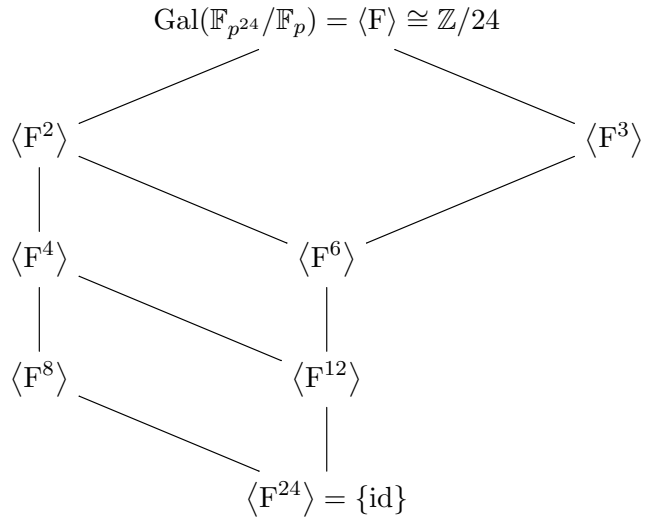



FIGURE 5.2. The subgroups of the Galois groups of $\mathbb{F}_{p^{24}}/\mathbb{F}_p$

### 5.3. The trace and norm mappings

For an extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$, consider the function $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ defined by

$$\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = u + u^{p^d} + u^{p^{2d}} + \cdots + u^{p^{(n-1)d}} = u + \mathrm{F}_d(u) + \mathrm{F}_{2d}(u) + \cdots + \mathrm{F}_{(n-1)d}(u).$$

Notice that

$$\begin{aligned}\mathrm{F}_d(\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u)) &= u^{p^d} + u^{p^{2d}} + u^{p^{3d}} + \cdots + u^{p^{nd}} \\ &= u^{p^d} + u^{p^{2d}} + u^{p^{3d}} + \cdots + u^{p^{(n-1)d}} + u = \mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u).\end{aligned}$$

So by Proposition 5.24(i), $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) \in \mathbb{F}_{p^d}$. If we modify $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ to have codomain $\mathbb{F}_{p^d}$, we obtain the *relative trace*

$$\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^d}; \quad \mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = u + u^{p^d} + u^{p^{2d}} + \cdots + u^{p^{(n-1)d}}.$$

5.26. Proposition. *The relative trace* $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ *is a surjective* $\mathbb{F}_{p^d}$*-linear mapping and whose kernel is an* $\mathbb{F}_{p^d}$*-vector subspace of dimension* $n-1$*.*

Proof. Clearly $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is additive. For $t \in \mathbb{F}_{p^d}$ we have $t^{p^d} = t$, so $\mathbb{F}_{p^d}$-linearity follows from the formula

$$tu + (tu)^{p^d} + (tu)^{p^{2d}} + \cdots + (tu)^{p^{(n-1)d}} = tu + tu^{p^d} + tu^{p^{2d}} + \cdots + tu^{p^{(n-1)d}}.$$

To see that $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is surjective, notice that $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = 0$ if and only if $u$ is a root of the polynomial

$$X + X^{p^d} + X^{p^{2d}} + \cdots + X^{p^{(n-1)d}} \in \mathbb{F}_{p^d}[X]$$

which has degree $p^{(n-1)d}$ and so has at most $p^{(n-1)d} < p^{nd}$ roots in $\mathbb{F}_{p^{nd}}$. This means that $\ker \mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ cannot be the whole of $\mathbb{F}_{p^{nd}}$. $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is surjective since its codomain has dimension 1. □

There is a multiplicative version of this construction. Consider the function

$$\mathrm{N}\colon \mathbb{F}_{p^{nd}}^{\times} \longrightarrow \mathbb{F}_{p^{nd}}^{\times}$$

for which

$$\mathrm{N}(u) = uu^{p^d}u^{p^{2d}}\cdots u^{p^{(n-1)d}} = u\,\mathrm{F}_d(u)\,\mathrm{F}_{2d}(u)\cdots\mathrm{F}_{(n-1)d}(u).$$

Then we have

$$\begin{aligned}\mathrm{F}_d(\mathrm{N}(u)) &= u^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{nd}} \\ &= u^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{(n-1)d}}u \\ &= uu^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{(n-1)d}} \\ &= \mathrm{N}(u).\end{aligned}$$

So by Proposition 5.24(i), $\mathrm{N}(u) \in \mathbb{F}_{p^d}$. By redefining the codomain we obtain the *relative norm*

$$\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}}^{\times} \longrightarrow \mathbb{F}_{p^d}^{\times}; \quad \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = uu^{p^d}u^{p^{2d}}\cdots u^{p^{(n-1)d}}.$$

5.27. Proposition. *The relative norm* $\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ *is a surjective group homomorphism.*

PROOF. Multiplicativity is obvious. The kernel of $\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ consists of the roots in $\mathbb{F}_{p^{nd}}$ of the polynomial

$$X^{1+p^d+\cdots+p^{(n-1)d}} - 1 \in \mathbb{F}_{p^d}[X],$$

so

$$|\ker \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| \leqslant 1 + p^d + \cdots + p^{(n-1)d} = \frac{p^{nd}-1}{p^d-1}\,.$$

Hence

$$|\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| = \frac{p^{nd}-1}{|\ker \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}|} \geqslant p^d - 1.$$

Since $\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}} \leqslant \mathbb{F}_{p^d}^{\times}$, we also have

$$|\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| \leqslant p^d - 1,$$

therefore

$$\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}} = \mathbb{F}_{p^d}^{\times}.$$

□

## Exercises for Chapter 5

**5.1** Show that Proposition 5.13 also applies to an integral domain in place of a field.

**5.2** What happens to Theorem 5.20 if we try to take $p = 2$.

**5.3** Let $f(X) \in \mathbb{F}_{p^d}[X]$ be an irreducible polynomial with $\deg f(X) = n$. Find the splitting field of $f(X)$. Deduce that for any other irreducible polynomial $g(X) \in \mathbb{F}_{p^d}[X]$ with $\deg g(X) = n$, the splitting fields of $f(X)$ and $g(X)$ over $\mathbb{F}_{p^d}$ agree.

**5.4** Find the smallest Galois fields containing all the roots of the following polynomials, in each case find a primitive root of this Galois field:

(a) $X^8 - 1 \in \mathbb{F}_{41}[X]$; (b) $X^8 - 1 \in \mathbb{F}_5[X]$; (c) $X^8 - 1 \in \mathbb{F}_{11}[X]$; (d) $X^8 - 1 \in \mathbb{F}_2[X]$.

**5.5** Let $w \in \mathbb{F}_{p^d}^\times$ be a primitive root. If $\ell < d$, show that $w \notin \mathbb{F}_{p^\ell}^\times$. Deduce that $\deg_{\mathbb{F}_p} w = d$ and $d \mid \varphi(p^d - 1)$.

**5.6** Let $p > 0$ be a prime. Suppose that $d \geqslant 1$, and $K/\mathbb{F}_{p^d}$ is an extension. For $a \in K$, let $g_a(X) = X^{p^d} - X - a \in K[X]$.

(a) If the polynomial $g_a(X)$ is irreducible over $K$, show that the splitting field $E$ of $g_a(X)$ over $K$ is separable and $\mathrm{Gal}(E/K) \cong \mathbb{F}_{p^d}$. [*Hint: show that if $u \in E$ is a root of $g_a(X)$ in an extension $E/K$, then so is $u + t$ for every $t \in \mathbb{F}_p$.*]

(b) If $d = 1$, show that $g_a(X)$ is irreducible over $K$ if and only if it has no root in $K$.

(c) If $K$ is a finite field and $d > 1$, explain why $g_a(X)$ can never be irreducible over $K$.

**5.7** Let $p$ be an odd prime, $d \geqslant 1$ and write $q = p^d$.

(a) Consider $\{\pm 1\} = \{1, -1\}$ as a group under multiplication. Show that there is a unique group homomorphism $\lambda_q \colon \mathbb{F}_q^\times \longrightarrow \{\pm 1\}$ which is characterized by the requirement that for every $u \in \mathbb{F}_q^\times$, $\lambda_q(u) = 1$ if and only if $u = v^2$ for some $v \in \mathbb{F}_q^\times$. Is $\lambda_q$ always surjective?

(b) Consider the set of all squares in $\mathbb{F}_q$,

$$\Sigma_q = \{u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\} \subseteq \mathbb{F}_q.$$

Show that the number of elements of $\Sigma_q$ is $|\Sigma_q| = (q + 1)/2$. Deduce that if $t \in \mathbb{F}_q$ then the set

$$t - \Sigma_q = \{t - u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\}$$

has $|t - \Sigma_q| = (q + 1)/2$ elements.

(c) If $t \in \mathbb{F}_q$, show that

$$|\Sigma_q \cap (t - \Sigma_q)| \geqslant 1.$$

Deduce that every element of $\mathbb{F}_q$ is either a square or can be written as the sum of two squares.

(d) Deduce that the equation $x^2 + y^2 + z^2 = 0$ has at least one non-trivial solution in $\mathbb{F}_q$.

(e) What can you say about the case $p = 2$?

CHAPTER 6

# A Galois Miscellany

In this chapter we will explore some miscellaneous topics in Galois Theory. Historically, Galois Theory has always been an important tool in Number Theory and Algebra, stimulating the development of subjects such as Group Theory, Ring Theory and such diverse areas as Differential Equations, Complex Analysis and Algebraic Geometry. Many of the ideas introduced in this chapter are of great importance in these and other mathematical areas.

## 6.1. A proof of the Fundamental Theorem of Algebra

We will prove the *Fundamental Theorem of Algebra* for the complex numbers $\mathbb{C}$. This proof is essentially due to Gauss but he did not use the historically more recent Sylow theory. It is interesting to compare the proof below with others which use the topology of the plane and circle or Complex Analysis; our proof only uses the connectivity of the real line (via the Intermediate Value Theorem) together with explicit calculations in $\mathbb{C}$ involving square roots.

6.1. Theorem (The Fundamental Theorem of Algebra). *The field of complex numbers $\mathbb{C}$ is algebraically closed and $\overline{\mathbb{R}} = \mathbb{C}$.*

Proof. We know that $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}/\mathbb{R}$ is algebraic. Let $p(X) \in \mathbb{C}[X]$ be irreducible. Then any root $u$ of $p(X)$ in the algebraic closure $\overline{\mathbb{C}}$ is algebraic over $\mathbb{R}$, so in $\mathbb{C}[X]$ we have $p(X) \mid \operatorname{minpoly}_{\mathbb{R},u}(X)$. The splitting field of $p(X)$ over $\mathbb{C}$ is contained in the splitting field $E$ of $\operatorname{minpoly}_{\mathbb{R},u}(X)(X^2+1)$ over $\mathbb{R}$. Since $\mathbb{C} \leqslant E$, we have $2 \mid [E : \mathbb{R}]$ and so $2 \mid |\operatorname{Gal}(E/\mathbb{R})|$.

Now consider a 2-Sylow subgroup $P \leqslant \operatorname{Gal}(E/\mathbb{R})$ and recall that $|\operatorname{Gal}(E/\mathbb{R})|/|P|$ is odd. For the fixed subfield of $P$, we have

$$[E^P : \mathbb{R}] = \frac{|\operatorname{Gal}(E/\mathbb{R})|}{|P|},$$

which shows that $E^P/\mathbb{R}$ has odd degree. The Primitive Element Theorem 3.74 allows us to write $E^P = \mathbb{R}(v)$ for some $v$ whose minimal polynomial over $\mathbb{R}$ must also have odd degree. But by the Intermediate Value Theorem, every real polynomial of odd degree has a real root, so irreducibility implies that $v$ has degree 1 over $\mathbb{R}$ and therefore $E^P = \mathbb{R}$. This shows that $\operatorname{Gal}(E/\mathbb{R}) = P$, hence $\operatorname{Gal}(E/\mathbb{R})$ is a 2-group.

As $\mathbb{C}/\mathbb{R}$ is a Galois extension, we can consider the normal subgroup $\operatorname{Gal}(E/\mathbb{C}) \triangleleft \operatorname{Gal}(E/\mathbb{R})$ for which $|\operatorname{Gal}(E/\mathbb{R})| = 2\,|\operatorname{Gal}(E/\mathbb{C})|$. We must show that $|\operatorname{Gal}(E/\mathbb{C})| = 1$, so suppose not. From the theory of 2-groups, there is a normal subgroup $N \triangleleft \operatorname{Gal}(E/\mathbb{C})$ of index 2, so we can consider the Galois extension $E^N/\mathbb{C}$ of degree 2. But from known properties of $\mathbb{C}$ (see Proposition 3.29), every quadratic $aX^2 + bX + c \in \mathbb{C}[X]$ has complex roots (because we can find square roots of every complex number). So we cannot have an irreducible quadratic polynomial in $\mathbb{C}[X]$. Therefore $|\operatorname{Gal}(E/\mathbb{C})| = 1$ and $E = \mathbb{C}$. □

## 6.2. Cyclotomic extensions

We begin by discussing the situation for *cyclotomic extensions* over $\mathbb{Q}$ using material discussed in Section 1.3. Let $\zeta_n = e^{2\pi i/n}$, the standard primitive $n$-th root of 1 in $\mathbb{C}$. In Theorem 1.43, it was claimed that the irreducible polynomial over $\mathbb{Q}$ which has $\zeta_n$ as a root was the $n$-th cyclotomic polynomial

$$\Phi_n(X) = \prod_{\substack{t=1,\dots,n-1 \\ \gcd(t,n)=1}} (X - \zeta_n^t).$$

6.2. Theorem. *Let $n \geqslant 2$. Then*

- $\mathbb{Q}(\zeta_n) = \mathbb{Q}[X]/(\Phi_n(X))$;
- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$;
- $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$, *where the element $t_n \in (\mathbb{Z}/n)^\times$ acts on $\mathbb{Q}(\zeta_n)$ by $t_n \cdot \zeta_n = \zeta_n^t$.*

Proof. Since the complex roots of $\Phi_n(X)$ are the powers $\zeta_n^t$ with $t = 1, \dots, n-1$ and $\gcd(t, n) = 1$, $\mathbb{Q}(\zeta_n)$ is the splitting field of $\Phi_n(X)$ over $\mathbb{Q}$ and indeed $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^t)$ whenever $t$ has the above properties and so $\zeta_n^t$ is a primitive $n$-th root of unity. The main step in the proof is to show that $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible. To do this we will show that every power $\zeta_n^t$ as above is actually a Galois conjugate of $\zeta_n$ over $\mathbb{Q}$, therefore

$$\Phi_n(X) = \mathrm{minpoly}_{\mathbb{Q},\zeta_n}(X) = \mathrm{minpoly}_{\mathbb{Q},\zeta_n^t}(X)$$

and hence $\Phi_n(X)$ is irreducible.

Consider

$$\mathbb{Z}(\zeta_n) = \{a_0 + a_1\zeta_n + \cdots + a_r\zeta_n^r : r \geqslant 0,\ a_j \in \mathbb{Z}\} \subseteq \mathbb{Q}(\zeta_n).$$

Then $\mathbb{Z}(\zeta_n)$ is a subring of $\mathbb{Q}(\zeta_n)$ and so is an integral domain. Its group of units contains the cyclic subgroup $\langle\zeta_n\rangle$ of order $n$.

Let $p > 0$ be a prime which does not divide $n$. Let $P \lhd \mathbb{Z}(\zeta_n)$ be a maximal ideal which contains $p$; then the quotient ring $\mathbb{Z}(\zeta_n)/P$ is a field of characteristic $p$. In fact, it is a finite field, say $\mathbb{F}_{p^d}$ for some $d$. Let $\pi\colon \mathbb{Z}(\zeta_n) \longrightarrow \mathbb{F}_{p^d}$ be the quotient homomorphism.

Inside the group of units of $\mathbb{Z}(\zeta_n)$ is the subgroup of powers of $\zeta_n$, $\langle\zeta_n\rangle \leqslant \mathbb{Z}(\zeta_n)^\times$; this is a cyclic subgroup of order $n$. We claim that when restricted to $\langle\zeta_n\rangle$, $\pi$ gives an injective group homomorphism, $\pi'\colon \langle\zeta_n\rangle \longrightarrow \mathbb{F}_{p^d}^\times$. To see this, suppose that $\pi'(\zeta_n^r) = 1$ for some $r = 1, 2, \dots, n-1$; then $\zeta_n^r - 1 \in P$. By elementary Group Theory we can assume that $r \mid n$ and so $p \nmid r$. On factoring we have

$$(\zeta_n - 1)(\zeta_n^{r-1} + \cdots + \zeta_n + 1) \equiv (\zeta_n - 1)r \pmod{P},$$

so $\zeta_n - 1 \in P$ or $r \in P$ since maximal ideals are prime. But $\mathbb{Z} \cap P = (p)$ and so $r \notin P$, hence $\zeta_n - 1 \in P$. Recalling that

$$\zeta_n^{n-1} + \cdots + \zeta_n + 1 = 0,$$

we see that $n \in P$ and hence $p \mid n$, thus contradicting our original assumption on $n$. So $\pi'$ is injective.

Writing $\overline{u} = \pi'(u)$, we can consider the effect of the absolute Frobenius map $\mathrm{F}\colon \mathbb{F}_{p^d} \longrightarrow \mathbb{F}_{p^d}$ on $\overline{\zeta}_n^t = \overline{\zeta_n^t}$,

$$\mathrm{F}(\overline{\zeta}_n^t) = (\overline{\zeta}_n^t)^p = \overline{\zeta_n^{tp}}.$$

This shows that in the Galois extension $\mathbb{F}_{p^d}/\mathbb{F}_p$, $\overline{\zeta}_n^t$ is conjugate to $\overline{\zeta_n^{tp}}$; by iterating this we find that $\overline{\zeta}_n^t$ is conjugate to every power of the form $\overline{\zeta_n^{tp^k}}$.

Now let $t = 1, \ldots, n-1$ and $\gcd(t, n) = 1$. Suppose there is a factorization

$$\Phi_n(X) = f(X)\,\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(X)$$

for some monic polynomial $f(X) \in \mathbb{Z}[X]$ and $f(\zeta_n^t) = 0$. Consider the prime power factorization $t = p_1^{r_1} \cdots p_m^{r_m}$, where the $p_j$ are primes with $2 \leqslant p_1 < \cdots < p_m$ and $r_j \geqslant 1$ with. Since $\gcd(t, n) = 1$ we also have $p_j \nmid n$ s.

Now consider a maximal ideal $P_1 \lhd \mathbb{Z}[\zeta_n]$ containing $p_1$. Reducing modulo $P_1$ and working in the resulting extension $\mathbb{F}_{p_1^{d_1}}/\mathbb{F}_{p_1}$, we find that $\overline{\zeta}_n$ is conjugate to $\overline{\zeta}_n^{p_1^{r_1}}$. By separability and the fact that the reduction map $\pi_1 \colon \mathbb{Z}[\zeta_n] \longrightarrow \mathbb{F}_{p_1^{d_1}}$ is injective on the powers of $\zeta_n$, we find that $\overline{f(\zeta_n^{p_1^{r_1}})} \neq 0$ and so $f(\zeta_n^{p_1^{r_1}}) \neq 0$ in $\mathbb{Z}[\zeta_n]$. This shows that $\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}}) = 0$ and so $\zeta_n^{p_1^{r_1}}$ is conjugate to $\zeta_n$.

Repeating this argument starting with $\zeta_n^{p_1^{r_1}}$ and using the prime $p_2$ we find that

$$\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}p_2^{r_2}}) = 0$$

and so $\zeta_n^{p_1^{r_1}p_2^{r_2}}$ is conjugate to $\zeta_n$. Continuing in this fashion, for each $j = 1, \ldots, m$ we have

$$\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}p_2^{r_2}\cdots p_j^{r_j}}) = 0$$

and so $\zeta_n^{p_1^{r_1}\cdots p_j^{r_j}}$ is conjugate to $\zeta_n$. When $j = m$, this shows that $\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^t) = 0$. Hence $\zeta_n^t$ is conjugate to $\zeta_n$ in the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. □

6.3. Theorem. *For $n > 2$, consider the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ where $\zeta_n = e^{2\pi i/n}$. Then $\mathbb{Q}(\zeta_n)_{\mathbb{R}} \neq \mathbb{Q}(\zeta_n)$. Furthermore,*

$$\mathbb{Q}(\zeta_n)_{\mathbb{R}} = \mathbb{Q}(\zeta_n)^{\langle(\overline{\ })\rangle} = \mathbb{Q}(\zeta_n + \overline{\zeta}_n) = \mathbb{Q}(\cos(2\pi/n)),$$

*and*

$$[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \frac{\varphi(n)}{2}\,.$$

Proof. Recall that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n^\times,$$

where the residue class of $r$ acts by sending $\zeta_n$ to $\zeta_n^r$. Complex conjugation corresponds to the residue class of $-1 \equiv n-1 \pmod{n}$. Making use of the identities

$$e^{\theta i} = \cos\theta + \sin\theta\, i, \quad \cos\theta = \frac{1}{2}\,(e^{\theta i} + e^{-\theta i}),$$

we obtain

$$\cos(2\pi/n) = \frac{1}{2}\,(\zeta_n + \overline{\zeta}_n) = \frac{1}{2}\,(\zeta_n + \zeta_n^{-1}).$$

Complex conjugation fixes each of the real numbers $\cos(2\pi k/n)$ for $k = 1, 2, \ldots, n-1$. The residue class of $r$ acts by sending $\cos(2\pi/n)$ to $\cos(2\pi r/n)$; it is elementary to show that $\cos(2\pi r/n) \neq \cos(2\pi/n)$ unless $r \equiv 1 \pmod{n}$. Hence

$$\langle(\overline{\ })\rangle = \{\mathrm{id}, (\overline{\ })\} = \mathrm{Gal}(\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}).$$

Thus we have

$$\mathbb{Q}(\zeta_n)^{\langle(\overline{\ })\rangle} = \mathbb{Q}(\cos(2\pi/n)),$$

and so $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \varphi(n)/2$. Notice that $\zeta_n$ is a root of the polynomial

$$X^2 - 2\cos(2\pi/n)X + 1 \in \mathbb{Q}(\cos(2\pi/n))[X],$$

so we also have

$$\operatorname{minpoly}_{\mathbb{Q}(\cos(2\pi/n)),\zeta_n}(X) = X^2 - 2\cos(2\pi/n)X + 1. \tag{6.1}$$

□

6.4. Example. We have

$$[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = \varphi(24) = 8$$

and

$$\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Proof. By Theorem 1.43 we have $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = 8$. Also,

$$\zeta_{24}^6 = i, \quad \zeta_{24}^3 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i, \quad \zeta_{24}^8 = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i,$$

and all of these numbers are in $\mathbb{Q}(\zeta_{24})$, hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \leqslant \mathbb{Q}(\zeta_{24})$. It is easy to check that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}] = 8,$$

which implies that

$$\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i).$$

Using this we find that

$$\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

We also have $\cos(2\pi/24) = \cos(\pi/12) \in \mathbb{Q}(\zeta_{24})$. Since

$$\cos(2\pi/12) = \cos(\pi/6) = \frac{\sqrt{3}}{2}\,,$$

we have

$$2\cos^2(\pi/12) - 1 = \frac{\sqrt{3}}{2}$$

and so

$$4\cos^4(\pi/12) - 4\cos^2(\pi/12) + 1 = \frac{3}{4}\,,$$

giving

$$16\cos^4(\pi/12) - 16\cos^2(\pi/12) + 1 = 0.$$

Then

$$16X^4 - 16X^2 + 1 = 16\operatorname{minpoly}_{\mathbb{Q},\cos(\pi/12)}(X).$$

Note that case (i) of Kaplansky's Theorem 4.28 applies to the polynomial $\operatorname{minpoly}_{\mathbb{Q},\cos(\pi/12)}(X)$.

For this example, $\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q})$ has $2^3 - 1 = 7$ subgroups of each of the orders 2 and 4; it is an interesting exercise to find them all together with their fixed subfields. □

6.5. Remark. The minimal polynomial for $\cos(\pi/12)$ can also be found as follows. We have $\Phi_{24}(\zeta_{24}) = 0$, hence since

$$\Phi_{24}(X) = X^8 - X^4 + 1,$$

we obtain

$$\zeta_{24}^8 - \zeta_{24}^4 + 1 = 0.$$

Then after multiplying by $\zeta_{24}^{-4}$ we have

$$\zeta_{24}^4 - 1 + \zeta_{24}^{-4} = 0,$$

giving

$$(\zeta_{24}^4 + \zeta_{24}^{-4}) - 1 = 0.$$

Now

$$(\zeta_{24} + \zeta_{24}^{-1})^4 = (\zeta_{24}^4 + \zeta_{24}^{-4}) + 4(\zeta_{24}^2 + \zeta_{24}^{-2}) + 6,$$

hence

$$\zeta_{24}^4 + \zeta_{24}^{-4} = (\zeta_{24} + \zeta_{24}^{-1})^4 - 4(\zeta_{24}^2 + \zeta_{24}^{-2}) - 6.$$

Similarly,

$$(\zeta_{24} + \zeta_{24}^{-1})^2 = \zeta_{24}^2 + \zeta_{24}^{-2} + 2,$$

so

$$\zeta_{24}^2 + \zeta_{24}^{-2} = (\zeta_{24} + \zeta_{24}^{-1})^2 - 2.$$

Combining these we have

$$(\zeta_{24} + \zeta_{24}^{-1})^4 - 4(\zeta_{24} + \zeta_{24}^{-1})^2 + 1 = 0,$$

and so

$$16\cos^4(\pi/12) - 16\cos^2(\pi/12) + 1 = 0.$$

This method will work for any $n$ where $\varphi(n)$ is even, *i.e.*, when $n > 2$.

6.6. Remark. The polynomial that expresses $\cos n\theta$ as a polynomial in $\cos\theta$ is the $n$-th *Chebsyhev polynomial of the first kind* $\mathrm{T}_n(X) \in \mathbb{Z}[X]$. Here are the first few of these polynomials:

$$\mathrm{T}_2(X) = 2X^2 - 1, \qquad \mathrm{T}_3(X) = 4X^3 - 3X,$$
$$\mathrm{T}_4(X) = 8X^4 - 8X^2 + 1, \qquad \mathrm{T}_5(X) = 16X^5 - 20X^3 + 5X,$$
$$\mathrm{T}_6(X) = 32X^6 - 48X^4 + 18X^2 - 1, \qquad \mathrm{T}_7(X) = 64X^7 - 112X^5 + 56X^3 - 7X.$$

These form a system of *orthogonal polynomials* which can be computed in Maple using the command `orthopoly[T](n,X)`.

Now let $K$ be a field with characteristic $\operatorname{char} K \nmid n$. The polynomial $\Phi_n(X)$ has integer coefficients, so we can view it as an element of $K[X]$ since either $\mathbb{Q} \leqslant K$ or $\mathbb{F}_p \leqslant K$ and we can reduce the coefficients modulo $p$. In either case it can happen that $\Phi_n(X)$ factors in $K[X]$. However, we can still describe the splitting field of $X^n - 1$ over $K$ and its Galois group.

6.7. Theorem. *If* $\operatorname{char} K \nmid n$, *then the splitting field of* $X^n - 1$ *over* $K$ *is* $K(\zeta)$, *where* $\zeta \in \overline{K}$ *is a primitive* $n$*-th root of unity. The Galois group* $\mathrm{Gal}(K(\zeta)/K)$ *is isomorphic to a subgroup of* $(\mathbb{Z}/n)^\times$, *hence it is abelian with order dividing* $\varphi(n)$.

PROOF. Working in $\overline{K}$, we know that $\Phi_n(\zeta) = 0$, hence the roots of $\operatorname{minpoly}_{K,\zeta}(X) \in K[X]$ are primitive roots of 1. So $X^n - 1$ splits over $K(\zeta)$ and each element $\alpha \in \operatorname{Gal}(K(\zeta)/K)$ has the action $\alpha(\zeta) = \zeta^{r_\alpha}$, where $\gcd(r_\alpha, n) = 1$. Hence $\operatorname{Gal}(K(\zeta)/K)$ is isomorphic to a subgroup of $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$ which implies that it is abelian and its order divides $\varphi(n)$. □

6.8. REMARK. When $p = \operatorname{char} K > 0$, this Galois group only depends on the largest subfield of $K$ which is algebraic over $\mathbb{F}_p$. For example, if $K = \mathbb{F}_{p^d}(T)$ then the value of $d$ is the crucial factor. The precise outcome can be determined with the aid of Proposition 5.21.

6.9. EXAMPLE. We have the following splitting fields and Galois groups.

(i) The splitting field of $X^4 - 1$ over $\mathbb{F}_3(T)$ is $\mathbb{F}_9(T)$ and

$$\operatorname{Gal}(\mathbb{F}_9(T)/\mathbb{F}_3(T)) \cong (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2.$$

(ii) By Proposition 5.20, $X^4 - 1$ splits over $\mathbb{F}_5(T)$ and the Galois group $\operatorname{Gal}(\mathbb{F}_5(T)/\mathbb{F}_5(T))$ is trivial.

PROOF. (i) By Proposition 5.20, $X^4 - 1$ is separable over $\mathbb{F}_3(T)$ and has irreducible factors $(X - 1)$, $(X + 1)$ and $(X^2 + 1)$. The splitting field of $(X^2 + 1)$ over $\mathbb{F}_3$ is $\mathbb{F}_9 = \mathbb{F}_3(\zeta)$, where $\zeta^2 + 1 = 0$, so $(X^2 + 1)$ splits over $\mathbb{F}_9(T)$. Also,

$$\operatorname{Gal}(\mathbb{F}_9/\mathbb{F}_3) \cong (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2,$$

with generator $\sigma$ satisfying $\sigma(\zeta) = \zeta^{-1} = -\zeta$. This generator clearly extends to an automorphism of $\mathbb{F}_9(T)$ which fixes $T$.
(ii) By Proposition 5.20, $X^4 - 1$ splits over $\mathbb{F}_5$. □

### 6.3. Artin's Theorem on linear independence of characters

Let $G$ be a group and $K$ a field.

6.10. DEFINITION. A group homomorphism $\chi\colon G \longrightarrow K^\times$ is called a *character of $G$ with values in $K$*.

6.11. EXAMPLE. Given any ring homomorphism $\varphi\colon R \longrightarrow K$ we obtain a character of $R^\times$ in $K$ by restricting $\varphi$ to a map $\chi_\varphi\colon R^\times \longrightarrow K^\times$.

6.12. EXAMPLE. Given an automorphism $\alpha\colon K \longrightarrow K$, $\chi_\alpha\colon K^\times \longrightarrow K^\times$ is a character of $K^\times$ in $K$.

6.13. EXAMPLE. Let $E/K$ be a Galois extension and $\sigma \in \operatorname{Gal}(E/K)$. Then $\chi_\sigma\colon E^\times \longrightarrow E^\times$ is a character.

6.14. DEFINITION. Let $\chi_1, \ldots, \chi_n$ be characters of a group $G$ in a field $K$. Then $\chi_1, \ldots, \chi_n$ are *linearly independent* if for $t_1, \ldots, t_n \in K$,

$$t_1\chi_1 + \cdots + t_n\chi_n = 0 \quad \Longrightarrow \quad t_1 = \cdots = t_n = 0.$$

If $\chi_1, \ldots, \chi_n$ are not linearly independent then they are *linearly dependent*.

In this definition, the functional equation means that for all $g \in G$,

$$t_1\chi_1(g) + \cdots + t_n\chi_n(g) = 0.$$

6.15. THEOREM (Artin's Theorem). *Let $\chi_1, \ldots, \chi_n$ be distinct characters of a group $G$ in a field $K$. Then $\chi_1, \ldots, \chi_n$ are linearly independent.*

PROOF. We proceed by induction on $n$. For $n = 1$ the result is easily verified. For the inductive assumption, suppose that it holds for any $n \leqslant k$.

Let $\chi_1, \ldots, \chi_{k+1}$ be a set of $k+1$ distinct characters for which there are $t_1, \ldots, t_{k+1} \in K$ not all zero and such that

$$t_1\chi_1 + \cdots + t_{k+1}\chi_{k+1} = 0. \tag{6.2}$$

If one of the $t_i$ is zero, say $t_r = 0$, then $\chi_1, \ldots, \chi_{r-1}, \chi_{r+1}, \ldots, \chi_{k+1}$ is linearly dependent, contradicting the inductive assumption. Hence all of the $t_i$ must be non-zero. As $\chi_1 \neq \chi_2$, there must be an element $g_0 \in G$ for which $\chi_1(g_0) \neq \chi_2(g_0)$. So for all $g \in G$, Equation (6.2) applied to $g_0 g$ yields

$$t_1\chi_1(g_0g) + \cdots + t_{k+1}\chi_{k+1}(g_0g) = 0,$$

and therefore since $\chi_j(g_0g) = \chi_j(g_0)\chi_j(g)$, we see that

$$t_1\chi_1(g_0)\chi_1 + \cdots + t_{k+1}\chi_{k+1}(g_0)\chi_{k+1} = 0.$$

Multiplying Equation (6.2) by $\chi_1(g_0)$ and subtracting gives

$$t_2(\chi_2(g_0) - \chi_1(g_0))\chi_2 + t_3(\chi_3(g_0) - \chi_1(g_0))\chi_3 + \cdots + t_{k+1}(\chi_{k+1}(g_0) - \chi_1(g_0))\chi_{k+1} = 0,$$

in which the coefficient $t_2(\chi_2(g_0) - \chi_1(g_0))$ is not zero. Hence $\chi_2, \ldots, \chi_{k+1}$ is linearly dependent, again contradicting the inductive assumption. So $\chi_1, \ldots, \chi_{k+1}$ is linearly independent, which demonstrates the inductive step. □

6.16. COROLLARY. *Suppose that $\alpha_1, \ldots, \alpha_n$ are distinct automorphisms of the field $K$. Let $t_1, \ldots, t_n \in K$ be a sequence of elements, not all of which are 0. Then there is a $z \in K$ for which*

$$t_1\alpha_1(z) + \cdots + t_n\alpha_n(z) \neq 0.$$

*Hence the $K$-linear transformation $t_1\alpha_1 + \cdots + t_n\alpha_n \colon K \longrightarrow K$ is non-trivial.*

6.17. COROLLARY. *Let $E/K$ be a finite Galois extension of degree $n$ and let $\alpha_1, \ldots, \alpha_n$ be the distinct elements of $\mathrm{Gal}(E/K)$. Then the function $\alpha_1 + \cdots + \alpha_n \colon E \longrightarrow E$ is a non-trivial $K$-linear transformation whose image is contained in $K$. Hence the associated $K$-linear transformation*

$$\mathrm{Tr}_{E/K} \colon E \longrightarrow K; \quad \mathrm{Tr}_{E/K}(x) = \alpha_1(x) + \cdots + \alpha_n(x)$$

*is surjective.*

The function $\mathrm{Tr}_{E/K} \colon E \longrightarrow K$ is called the *trace mapping* of $E/K$.

PROOF. First note that for $x \in E$ and $\gamma \in \mathrm{Gal}(E/K)$,

$$\gamma(\alpha_1(x) + \cdots + \alpha_n(x)) = \gamma\alpha_1(x) + \cdots + \gamma\alpha_n(x) = \alpha_1(x) + \cdots + \alpha_n(x),$$

since the list $\gamma\alpha_1, \ldots, \gamma\alpha_n$ is the same as $\alpha_1, \ldots, \alpha_n$ apart from its order. Hence,

$$\alpha_1(x) + \cdots + \alpha_n(x) \in E^{\mathrm{Gal}(E/K)} = K.$$

The rest of the statement follows directly from Corollary 6.16. □

Suppose that $E/K$ is a finite Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order $n$. For each $u \in E^\times$, the element $u\sigma(u)\cdots\sigma^{n-1}(u) \in E$ satisfies

$$\sigma(u\sigma(u)\cdots\sigma^{n-1}(u)) = \sigma(u)\cdots\sigma^{n-1}(u)\sigma^n(u) = \sigma(u)\cdots\sigma^{n-1}(u)u,$$

hence in $u\sigma(u)\cdots\sigma^{n-1}(u) \in E^{\langle\sigma\rangle} = K$. Now using this we define a group homomorphism

$$\mathrm{N}_{E/K}\colon E^\times \longrightarrow K^\times; \quad \mathrm{N}_{E/K}(u) = u\sigma(u)\cdots\sigma^{n-1}(u).$$

$\mathrm{N}_{E/K}$ is called the *norm mapping* for $E/K$ and generalizes the norm mapping for finite fields of Section 5.3.

There is another homomorphism

$$\delta_{E/K}\colon E^\times \longrightarrow E^\times; \quad \delta_{E/K}(u) = u\sigma(u)^{-1}.$$

Notice that for $u \in E^\times$,

$$\mathrm{N}_{E/K}(\delta_{E/K}(u)) = (u\sigma(u)^{-1})(\sigma(u)\sigma^2(u)^{-1}\cdots\sigma^{n-1}(u)\sigma^n(u)^{-1}) = 1,$$

since $\sigma^n(u) = u$. So $\operatorname{im}\delta_{E/K} \leqslant \ker \mathrm{N}_{E/K}$. Our next result is an important generalization of Proposition 5.27.

6.18. Theorem (Hilbert's Theorem 90). *Let $E/K$ be a finite Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order $n$. Then $\operatorname{im}\delta_{E/K} = \ker \mathrm{N}_{E/K}$. Explicitly, if $u \in E^\times$ and $u\,\sigma(u)\cdots\sigma^{n-1}(u) = 1$, then there is a $v \in E^\times$ such that $u = v\sigma(v)^{-1}$.*

Proof. Let $u \in \ker \mathrm{N}_{E/K}$.

The characters $\sigma^k\colon E^\times \longrightarrow E^\times$ with $k = 0, 1, \ldots, n-1$ are distinct and linearly independent by Artin's Theorem 6.15. Consider the function

$$\mathrm{id} + u\sigma + u\sigma(u)\sigma^2 + \cdots + u\sigma(u)\cdots\sigma^{n-2}(u)\sigma^{n-1}\colon E^\times \longrightarrow E.$$

This cannot be identically zero, so for some $w \in E$, the element

$$v = w + u\sigma(w) + u\sigma(u)\sigma^2(w) + \cdots + u\sigma(u)\cdots\sigma^{n-2}(u)\sigma^{n-1}(w)$$

is non-zero. Notice that

$$u\sigma(v) = u\sigma(w) + u\sigma(u)\sigma^2(w) + u\sigma(u)\sigma^2(u)\sigma^3(w) + \cdots + u\sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^n(w) = v,$$

since

$$u\sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^n(w) = w.$$

Thus we have $u = v\sigma(v)^{-1}$ as required. □

## 6.4. Simple radical extensions

In this section we will investigate splitting fields of polynomials of the form $X^n - a$, where $\mathrm{char}\, K \nmid n$. We call these *simple radical extensions* and later in Definition 6.33 we introduce a more general notion of *radical extension*.

6.19. Proposition. *Let $f(X) = X^n - a \in K[X]$ be irreducible and separable over $K$. Then the splitting field of $f(X)$ over $K$ has the form $K(u, \zeta)$, where $u$ is a root of $f(X)$ and $\zeta$ is a primitive $n$-th root of 1.*

6.20. Corollary. *If $K$ contains a primitive $n$-th root of 1, $\zeta$, then the splitting field of $f(X) = X^n - a$ over $K$ has the form $K(u)$, where $u$ is a root of $f(X)$. The Galois group* $\mathrm{Gal}(K(u)/K)$ *is cyclic of order $n$ with a generator $\sigma$ for which $\sigma(u) = \zeta u$.*

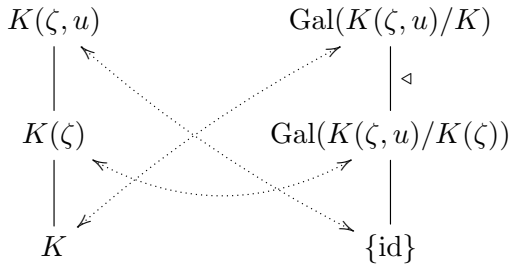
In the more general situation of Proposition 6.19,

$$\{\mathrm{id}\} \lhd \mathrm{Gal}(K(\zeta,u)/K(\zeta)) \lhd \mathrm{Gal}(K(\zeta,u)/K),$$

where $\mathrm{Gal}(K(\zeta,u)/K(\zeta))$ is cyclic and

$$\mathrm{Gal}(K(\zeta)/K)) \cong \mathrm{Gal}(K(\zeta,u)/K))/\,\mathrm{Gal}(K(\zeta,u)/K(\zeta))$$

is abelian. The Galois Correspondence identifies the following towers of subfields and subgroups.




6.21. Definition. Let $K$ be a field with $\mathrm{char}\, K \nmid n$ and which contains a primitive $n$-th root of 1, $\zeta$ say. Then $L/K$ is a *simple $n$-Kummer extension* if $L = K(u)$ where $u^n = a$ for some $a \in K$. $L/K$ is an (*iterated*) *$n$-Kummer extension* if $L = K(u_1, \ldots, u_k)$ where $u_1^n = a_1,\ \ldots,\ u_k^n = a_k$ for some elements $a_1, \ldots, a_k \in K$.

Note that in this definition we do not require the polynomials $X^n - a_j \in K[X]$ to be irreducible.

6.22. Proposition. *Let $K(u)/K$ be a simple $n$-Kummer extension. Then $K(u)/K$ is a Galois extension and* $\mathrm{Gal}(K(u)/K)$ *is cyclic with order dividing $n$.*

Proof. Suppose that $u^n = a \in K$. Then in $\overline{K}[X]$ we have

$$X^n - a = (X-u)(X-\zeta u)\cdots(X-\zeta^{n-1}u).$$

Clearly the roots of $X^n - a$ are distinct and so $K(u)/K$ is separable over $K$; in fact, $K(u)$ is a splitting field of $X^n - a$ over $K$. This means that $K(u)/K$ is Galois.

For each $\alpha \in \mathrm{Gal}(K(u)/K)$ we have $\alpha(u) = \zeta^{r_\alpha} u$ for some $r_\alpha = 0, 1 \ldots, n-1$. Notice that for $\beta \in \mathrm{Gal}(K(u)/K)$,

$$\beta\alpha(u) = \beta(\zeta^{r_\alpha}u) = \zeta^{r_\alpha}\beta(u) = \zeta^{r_\alpha}\zeta^{r_\beta}u = \zeta^{r_\alpha + r_\beta}u,$$

and so $r_{\beta\alpha} = r_\alpha + r_\beta$. Hence the function

$$\rho\colon\ \mathrm{Gal}(K(u)/K) \longrightarrow \langle\zeta\rangle\,; \quad \rho(\alpha) = \zeta^{r_\alpha},$$

is a group homomorphism. As $\langle\zeta\rangle$ is cyclic of order $n$, Lagrange's Theorem implies that the image of $\rho$ has order dividing $n$. Since every element of $\mathrm{Gal}(K(u)/K)$ is determined by its effect on $u$, $\rho$ is injective, hence $|\,\mathrm{Gal}(K(u)/K)|$ divides $n$. In fact, $\mathrm{Gal}(K(u)/K)$ is cyclic since every subgroup of a cyclic group is cyclic. □

6.23. Example. Let $n \geqslant 1$ and $q \in \mathbb{Q}$. Then $\mathbb{Q}(\zeta_n, \sqrt[n]{q})/\mathbb{Q}(\zeta_n)$ is a simple $n$-Kummer extension.

6.24. Example. $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i)$ is a simple 4-Kummer extension with $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i))$ cyclic of order 2.

Proof. We have $(\sqrt{2})^4 - 4 = 0$, but

$$X^4 - 4 = (X^2 - 2)(X^2 + 2),$$

and

$$X^2 - 2 = \mathrm{minpoly}_{\mathbb{Q}(i),\sqrt{2}}(X).$$

The corresponding group homomorphism $\rho\colon \mathrm{Gal}(\mathbb{Q}(i)(\sqrt{2})/\mathbb{Q}(i)) \longrightarrow \langle i\rangle$ has image

$$\mathrm{im}\,\rho = \{1,-1\} \leqslant \langle i\rangle\,. \qquad \square$$

Here is a converse to Proposition 6.22.

6.25. Proposition. *Suppose that* $\mathrm{char}\,K \nmid n$ *and there is an element* $\zeta \in K$ *which is a primitive* $n$*-th root of unity. If* $E/K$ *is a finite Galois extension with cyclic Galois group of order* $n$*, then there is an element* $a \in E$ *such that* $E = K(a)$ *and* $a$ *is a root of a polynomial of the form* $X^n - b$ *with* $b \in K$*. Hence* $E/K$ *is a simple* $n$*-Kummer extension.*

Proof. We have

$$\mathrm{N}_{E/K}(\zeta^{-1}) = \zeta^{-n} = 1,$$

so by Hilbert's Theorem 6.18, there is an element $a \in E$ for which $\zeta^{-1} = a\sigma(a)^{-1}$. Then $\sigma(a) = \zeta a$ and the elements $\sigma^k(a) = \zeta^k a$ for $k = 0, 1, \ldots, n-1$ are distinct, so they must be the $n$ conjugates of $a$. Also note that

$$X^n - a^n = (X-a)(X-\zeta a)\cdots(X-\zeta^{n-1}a) = (X-a)(X-\sigma(a))\cdots(X-\sigma^{n-1}(a)),$$

hence $a^n \in K$ since it is fixed by $\sigma$. Since $K(a) \leqslant E$, this shows that

$$n = [K(a):K] \leqslant [E:K] = n$$

and therefore

$$[K(a):K] = [E:K] = n,$$

whence $K(a) = E$. $\square$

## 6.5. Solvability and radical extensions

We begin by recalling some ideas about groups, see [**3, 5**] for further details.

6.26. Definition. A group $G$ is *solvable*, *soluble* or *soluable* if there is a chain of subgroups (called a *subnormal series*)

$$\{1\} = G_\ell \leqslant G_{\ell-1} \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$$

in which $G_{k+1} \triangleleft G_k$ and each *composition factor* $G_k/G_{k+1}$ is abelian; we usually write

$$\{1\} = G_\ell \triangleleft G_{\ell-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G.$$

If each composition factor is a cyclic group of prime order the subnormal series is called a *composition series*. A group which is not solvable is called *insolvable*.

6.27. Remark. It is a standard result that we can always refine (*i.e.*, add extra terms) a subnormal series of a solvable group to obtain a composition series. The primes appearing as well as the number of times each occurs are all determined by $|G|$, only their order varying for different composition series.

6.28. Example. Let $G$ be a finite abelian group. Then $G$ is solvable.

6.29. Example. Let $G$ be a finite $p$-group, where $p$ is a prime. Then $G$ is solvable.

In fact, for a finite $p$-group $G$, there is always a normal subgroup of a $p$-group with index $p$, so in this case we can assume each quotient $G_k/G_{k+1}$ is cyclic of order $p$.

6.30. Proposition. *Let $G$ be a group.*

(i) *If $G$ is solvable then every subgroup $H \leqslant G$ and every quotient group $G/N$ is solvable.*
(ii) *If $N \triangleleft G$ and $G/N$ are solvable then so is $G$.*

In the opposite direction we can sometimes see that a group is insolvable. Recall that a group is *simple* if it has no non-trivial proper normal subgroups.

6.31. Proposition. *Let $G$ be a finite group. Then $G$ is insolvable if any of the following conditions holds:*

(i) *$G$ contains a subgroup which is a non-abelian simple group.*
(ii) *$G$ has a quotient group which is a non-abelian simple group.*
(iii) *$G$ has a composition series in which one of the terms is a non-abelian simple group.*

6.32. Example. For $n \geqslant 5$, the alternating and symmetric groups $\mathrm{A}_n$ and $\mathrm{S}_n$ are insolvable.

Proof. This follows from the fact that if $n \geqslant 5$, $\mathrm{A}_n$ is a simple group and $\mathrm{A}_n \triangleleft \mathrm{S}_n$ with quotient group $\mathrm{S}_n/\mathrm{A}_n \cong \mathbb{Z}/2$. □

Now we explain how this relates to fields and their extensions. Let $K$ be a field and $L/K$ a finite extension. For simplicity, we assume also that $\operatorname{char} K = 0$.

6.33. Definition. $L/K$ is a *radical extension* of $K$ if it has the form $L = K(a_1, a_2, \ldots, a_n)$ with

$$a_k^{d_k} \in K(a_1, a_2, \ldots, a_{k-1})$$

for some $d_k \geqslant 1$. Thus every element of $L$ is expressible in terms of iterated roots of elements of $K$.

We will need the following Lemma and its Corollary. According to [**4**], several text books make subtle errors or omissions related to this result, so beware when reading other sources!

6.34. Lemma. *Let $L/K$ be a finite Galois extensions and let $L(u)/L$ be a radical extension. Let $E/L$ be an extension where $E$ is a splitting field for the polynomial* $\operatorname{minpoly}_{K,u}(X) \in L[X]$. *Then $E/L$ is a radical Galois extension. In particular, if $L/K$ is a radical Galois extension then so is $E/K$.*

Proof. Suppose that $u^d = a \in L$ with $a \neq 0$. Then $X^d - a$ has a $d$ distinct roots in $E$, and if $v$ is any other root then $(v/u)^d = 1$, so there are $d$ distinct $d$-th roots of unity in $E$. Hence there is a primitive $d$-th root of unity $\zeta \in E$ and the subfield $L(\zeta, u) \leqslant E$ is normal over

$L$, so $L(\zeta,u)/L$ is a radical Galois extension. But $L(\zeta,u)/K$ need not be Galois. However, if $u=u_1,\dots,u_t\in E$ are the distinct roots of $\operatorname{minpoly}_{K,u}(X)$ in $E$, then

$$E=L(\zeta,u,u_1,\dots,u_t).$$

But this is clearly a radical extension of $L$.

If $L/K$ is a radical Galois extension, say $L=K(a_1,\dots,a_n)$, then

$$E=L(a_1,\dots,a_n,\zeta,u,u_1,\dots,u_t),$$

which is a radical Galois extension of $K$. □

6.35. Corollary. *If $L/K$ is a radical extension then it is contained in a radical Galois extension $L'/K$.*

Proof. Writing $L=K(a_1,a_2,\dots,a_n)$ as in Definition 6.33, this is proved by induction on $n$ using Lemma 6.34. □

In the next definition, the word Galois is superfluous because of the preceding results.

6.36. Definition. If $L$ is the splitting field of a polynomial $f(X)\in K[X]$, then $f(X)$ is *solvable by radicals* over $K$ if $L$ is contained in a radical (Galois) extension of $K$.

6.37. Definition. $L/K$ is *solvable* if $L\leqslant L'$ where $L'/K$ is a finite radical Galois extension of $K$.

6.38. Theorem. *Let $E/K$ be a finite Galois extension. Then $E/K$ is solvable if and only if the group* $\operatorname{Gal}(E/K)$ *is solvable.*

Proof. Suppose that $E\leqslant E'$ where $E'/K$ is a finite radical Galois extension, so

$$E'=K(\zeta,u_1,\dots,u_m),$$

where $\zeta^d=1$, $u_1^{d_1}\in K(\zeta)$ and $u_r^{d_r}\in K(\zeta,u_1,\dots,u_{r-1})$ for $r=2,\dots,m$ with $d_1\cdots d_m\mid d$. If $G_r\lhd\operatorname{Gal}(E'/K)$ and

$$(E')^{G_r}=K(\zeta,u_1,\dots,u_r),$$

with

$$(E')^{G_0}=K(\zeta),$$

then

$$\{1\}=G_m\lhd G_{m-1}\lhd\cdots\lhd G_0\lhd\operatorname{Gal}(E'/K)$$

and

$$G_{r-1}/G_r\cong\operatorname{Gal}(K(\zeta,u_1,\dots,u_r)/K(\zeta,u_1,\dots,u_{r-1})),$$

which is abelian by Proposition 6.22. Hence $\operatorname{Gal}(E'/K)$ is solvable, and since $\operatorname{Gal}(E/K)$ is a quotient group of $\operatorname{Gal}(E'/K)$, is also solvable by Proposition 6.30.

Now suppose that $\operatorname{Gal}(E/K)$ is solvable and let $n=|\operatorname{Gal}(E/K)|$. Let $E'$ be the splitting field of $X^n-1$ over $E$, so $E'$ contains a primitive $n$-th root of unity $\zeta$ and therefore it contains a primitive $d$-th root of unity for every divisor $d$ of $n$. Now $\operatorname{Gal}(E'/E)\lhd\operatorname{Gal}(E'/K)$ and by Theorem 6.7, $\operatorname{Gal}(E'/E)$ is abelian. Also, $\operatorname{Gal}(E'/K)/\operatorname{Gal}(E'/E)\cong\operatorname{Gal}(E/K)$ which is solvable, so $\operatorname{Gal}(E'/K)$ is solvable by Proposition 6.30. We will now show that $E'/K$ is a radical extension.

Clearly $K(\zeta)/K$ is radical. Then $\mathrm{Gal}(E'/K(\zeta)) \lhd \mathrm{Gal}(E'/K)$ is solvable. Let

$$\{1\} = G_\ell \lhd G_{\ell-1} \lhd \cdots \lhd G_1 \lhd G_0 = \mathrm{Gal}(E'/K(\zeta))$$

be a composition series. The extension $(E')^{G_1}/K(\zeta)$ is radical by Proposition 6.25. Similarly, each extension $(E')^{G_{k+1}}/(E')^{G_k}$ is radical. Hence $E'/K(\zeta)$ is radical, as is $E'/K$. □

6.39. Example. The Galois group of the extension $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ is solvable.

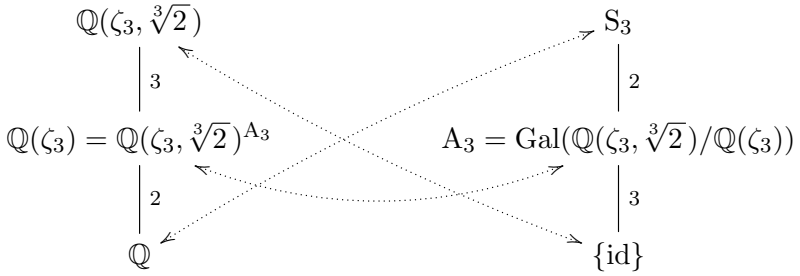
Proof. We have already studied this extension in Example 3.30 and 4.20. Clearly $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is a radical extension of $\mathbb{Q}$ and

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3)(\sqrt[3]{2}).$$

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) \cong \mathrm{S}_3$, where we identify each element of the Galois group with a permutation of the three roots of $X^3 - 2$ in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ which we list in the order

$$\sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3,\ \sqrt[3]{2}\,\zeta_3^2.$$

We have the following towers of subfields and subgroups related under the Galois Correspondence.




Here $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is itself a Galois extension and $\mathrm{A}_3 \lhd \mathrm{S}_3$. Notice that $\mathrm{A}_3 \cong \mathbb{Z}/3$ and $\mathrm{S}_3/\mathrm{A}_3 \cong \mathbb{Z}/2$, so we have the following composition series for $\mathrm{S}_3$:

$$\{\mathrm{id}\} \lhd \mathrm{A}_3 \lhd \mathrm{S}_3.$$ □

It is also interesting to reverse the question and ask whether there are extensions which are *not* solvable. This was a famous problem pursued for several hundred years. To find examples, we first recall that the smallest non-abelian simple group is $\mathrm{A}_5$ which has order 60. We should therefore expect to look for a polynomial of degree at least 5 to find a Galois group for a splitting field to be simple or occur as a composition factor of such a Galois group. Here is an explicit example over $\mathbb{Q}$.

6.40. Example. The splitting field of the polynomial $f(X) = X^5 - 35X^4 + 7 \in \mathbb{Q}[X]$ is not solvable.

Proof. Let $E \leqslant \mathbb{C}$ be the splitting field of $f(X)$ over $\mathbb{Q}$. Using the Eisenstein Test 1.38 with $p = 7$, we find that $f(X)$ is irreducible over $\mathbb{Q}$. By Theorem 4.8(iii), 5 divides the order of $\mathrm{Gal}(E/\mathbb{Q})$, so by Cauchy's Lemma this group contains an element of order 5.

Now observe that

$$f'(X) = 5X^4 - 140X^3 = 5X^3(X - 28), \quad f''(X) = 20X^4 - 420X^2 = 20X^2(X - 21).$$

There are two turning points, namely a maximum at $x = 0$ and a minimum at $x = 28$. Then

$$f(0) = 7 > 0 > f(28) = -4302585,$$

hence there are three real roots of $f(X)$ and two non-real complex ones. Then complex conjugation restricts to an element of order 2 in $\mathrm{Gal}(E/\mathbb{Q})$ which interchanges the non-real roots and fixes the others. If we list the roots of $f(X)$ as $u_1, u_2, u_3, u_4, u_5$ with $u_1, u_2$ being the non-real roots, then the transposition $(1\ 2) \in \mathrm{S}_5$ corresponds to this element. Furthermore, the only elements of $\mathrm{S}_5$ of order 5 are 5-cycles; by taking an appropriate power we can assume that there is a 5-cycle of the form $(1\ 2\ 3\ 4\ 5)$ corresponding to an element of $\mathrm{Gal}(E/\mathbb{Q})$ which we can view as a subgroup of $\mathrm{S}_5$. The next lemma shows that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{S}_5$.

6.41. Lemma. *Let $n \geqslant 1$. Suppose that $H \leqslant \mathrm{S}_n$ and $H$ contains the elements $(1\ 2)$ and $(1\ 2\ \cdots\ n)$. Then $H = \mathrm{S}_n$.*

The proof is left as an exercise. This completes the verification of Example 6.40. □

It is worth remarking that the most extreme version of this occurs when we ask for a Galois group which is *simple*. There has been a great deal of research activity on this question in the past few decades, but apparently not all simple groups are known to occur as Galois groups of extensions of $\mathbb{Q}$ or other finite subextensions of $\mathbb{C}/\mathbb{Q}$. Here is an example whose Galois group is $\mathrm{A}_5$; this is verified using Proposition 4.26.

6.42. Example. The Galois group of $f(X) = X^5 + 20X + 16$ over $\mathbb{Q}$ is $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{A}_5$, hence it is not solvable.

## 6.6. Symmetric functions

Let $k$ be a field. Consider the polynomial ring on $n$ indeterminates $\Bbbk[X_1, \ldots, X_n]$ and its field of fractions $K = \Bbbk(X_1, \ldots, X_n)$. Each permutation $\sigma \in \mathrm{S}_n$ acts on $\Bbbk[X_1, \ldots, X_n]$ by

$$\sigma \cdot f(X_1, \ldots, X_n) = f^\sigma(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Viewed as a function $\sigma\cdot\colon \Bbbk[X_1, \ldots, X_n] \longrightarrow \Bbbk[X_1, \ldots, X_n]$ is a ring isomorphism; this extends to a ring isomorphism $\sigma\cdot\colon \Bbbk(X_1, \ldots, X_n) \longrightarrow \Bbbk(X_1, \ldots, X_n)$. Varying $\sigma$ we obtain actions of the group $\mathrm{S}_n$ on $\Bbbk[X_1, \ldots, X_n]$ and $\Bbbk(X_1, \ldots, X_n)$ by ring isomorphisms fixing $\Bbbk$ and in the latter case it is by field automorphisms fixing $\Bbbk$.

6.43. Definition. The field of *symmetric functions on $n$ indeterminates* is

$$\mathrm{Sym}_n(\Bbbk) = \Bbbk(X_1, \ldots, X_n)^{\mathrm{S}_n} \leqslant \Bbbk(X_1, \ldots, X_n).$$

So if $f(X_1, \ldots, X_n) \in \Bbbk(X_1, \ldots, X_n)$, then

$$f(X_1, \ldots, X_n) \in \mathrm{Sym}_n(\Bbbk) \quad \Longleftrightarrow \quad \forall \sigma \in \mathrm{S}_n\ f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

6.44. Theorem. *The extension $\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)$ is a finite Galois extension for which $\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)) \cong \mathrm{S}_n$.*

Proof. There are elements of $\Bbbk[X_1, \ldots, X_n] \subseteq \Bbbk(X_1, \ldots, X_n)$ called *elementary symmetric functions*,

$$e_k = \sum_{i_1 < i_2 < \cdots < i_k} X_{i_1} X_{i_2} \cdots X_{i_k},$$

where $1 \leqslant k \leqslant n$. It is easy to see that for every $\sigma \in \mathrm{S}_n$, $e_k^\sigma = e_k$, so $e_k \in \mathrm{Sym}_n(\Bbbk)$. Working in the ring $\Bbbk(X_1, \ldots, X_n)[Y]$ we have

$$f_n(Y) = Y^n - e_1 Y^{n-1} + \cdots + (-1)^{n-1} e_{n-1} Y + (-1)^n e_n = 0,$$

hence the roots of this polynomial are the $X_i$. So $\Bbbk(X_1, \dots, X_n)$ is the splitting field of $f_n(Y)$ over $\operatorname{Sym}_n(\Bbbk)$. Now $\mathrm{S}_n \leqslant \operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk))$, hence

$$[\Bbbk(X_1, \dots, X_n) : \operatorname{Sym}_n(\Bbbk)] = |\operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk))| \geqslant |\mathrm{S}_n| = n!.$$

But as every element of $\operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk))$ permutes the roots of $f_n(Y)$ and is determined by this permutation, we also have

$$n! \geqslant |\operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk))|.$$

Combining these inequalities we obtain $|\operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk))| = n!$ and therefore $\operatorname{Gal}(\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk)) = \mathrm{S}_n$. □

6.45. Remark. In fact, this proof shows that the extension $\Bbbk(X_1, \dots, X_n)/\Bbbk(e_1, \dots, e_n)$ is Galois of degree $n!$. Since $\Bbbk(e_1, \dots, e_n) \leqslant \operatorname{Sym}_n(\Bbbk)$ we can also deduce that $\Bbbk(e_1, \dots, e_n) = \operatorname{Sym}_n(\Bbbk)$. Hence every element of $\operatorname{Sym}_n(\Bbbk)$ is a rational function in the $e_i$. Analogous results are true for polynomials, *i.e.*,

$$\Bbbk[X_1, \dots, X_n]^{\mathrm{S}_n} = \Bbbk[e_1, \dots, e_n].$$

6.46. Corollary. *If $n \geqslant 5$, the extension $\Bbbk(X_1, \dots, X_n)/\operatorname{Sym}_n(\Bbbk)$ is not solvable.*

## Exercises for Chapter 6

**6.1** Let $p > 0$ be a prime and $G$ a group of order $|G| = p^n$ for some $n \geqslant 1$. Show by induction on $n$ that there is a normal subgroup $N \triangleleft G$ with $|N| = p^{n-1}$. [*Hint: what do you know about the centre of $G$? Use this information to produce a quotient group of smaller order than $G$.*]

**6.2** Let $K$ be a field for which $\operatorname{char} K \neq 2$ and $n \geqslant 1$ be odd. If $K$ contains a primitive $n$-th root of unity, show that then $K$ contains a primitive $2n$-th root of unity.

**6.3** Find all values of $n \geqslant 1$ for which $\varphi(n) \mid 4$. Using this, determine which roots of unity lie in the following fields:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}\,i),\ \mathbb{Q}(\sqrt{3}\,i),\ \mathbb{Q}(\sqrt{5}\,i).$$

**6.4** (a) Describe the elements of $(\mathbb{Z}/24)^\times$ explicitly and verify that this group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. Describe the effect of each element on $\mathbb{Q}(\zeta_{24})$ and $\mathbb{Q}(\cos(\pi/12))$ under the action described in Theorem 6.2.
(b) Determine the group $(\mathbb{Z}/20)^\times$ and describe the effect of each of its elements on $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\cos(\pi/10))$ under the action described in Theorem 6.2.

**6.5** Let $n \geqslant 1$.
(a) What can you say about $\sin(2\pi/n)$ and $\operatorname{Gal}(\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q})$?
(b) Determine $\sin(\pi/12)$ and $\operatorname{Gal}(\mathbb{Q}(\sin(\pi/12))/\mathbb{Q})$.

**6.6** In this question, work in the cyclotomic field $\mathbb{Q}(\zeta_5)$ where $\zeta_5 = e^{2\pi i/5}$.
(a) Describe the Galois group $\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ and its action on $\mathbb{Q}(\zeta_5)$.
(b) Determine the minimal polynomial of $\cos(2\pi/5)$ over $\mathbb{Q}$. Hence show that

$$\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}\,.$$

For which other angles $\theta$ is $\cos\theta$ a root of this minimal polynomial? What is the value of $\sin(2\pi/5)$ ?
(c) Find the tower of subfields of $\mathbb{Q}(\zeta_5)$ and express them as fixed fields of subgroups of $\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.

**6.7** In this question, let $p$ be an odd prime and let $\zeta_p = e^{2\pi i/p} \in \mathbb{Q}(\zeta_p) \leqslant \mathbb{C}$.
(a) Consider the product

$$\xi = \prod_{r=1}^{(p-1)/2} (\zeta_p^r - \zeta_p^{-r}) \in \mathbb{Q}(\zeta_p).$$

Show that

$$\xi^2 = (-1)^{(p-1)/2} \prod_{r=1}^{p-1} (1 - \zeta_p^r).$$

(b) Deduce that

$$\xi^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod 4, \\ -p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(c) Conclude that

$$\xi = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm\sqrt{p}\, i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

and also $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$ and $\sqrt{p}\, i \in \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.

**6.8** Prove Lemma 6.41. [*Hint: show that every 2-cycle of the form* $(i\ i+1)$ *is in* $H$ *by considering elements of the form* $(1\ 2\ \cdots\ n)^r(1\ 2)(1\ 2\ \cdots\ n)^{n-r}$.]

**6.9** *This question is about an additive version of Hilbert's Theorem 90, see Theorem 6.18.* Let $E/K$ be a Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order $n$.
(a) Show that the function

$$T\colon E \longrightarrow E; \quad T(u) = u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{n-1}(u),$$

takes values in $K$ and use this to define a $K$-linear mapping $\mathrm{Tr}_{E/K}\colon E \longrightarrow K$.
(b) If $v \in E$ has $\mathrm{Tr}_{E/K}(v) = 0$, show that there is a $w \in E$ such that $v = w - \sigma(w)$.
[*Hint: Show that there is an element* $t \in E$ *for which* $\mathrm{Tr}_{E/K}\, t \neq 0$*, then consider*

$$w = \frac{1}{(\mathrm{Tr}_{E/K}\, t)}\big(v\sigma(t) + (v + \sigma(v))\sigma^2(t) + \cdots + (v + \sigma(v)\sigma^2(t) + \cdots + \sigma^{n-2}(v))\sigma^{n-1}(t)\big)$$

*and adapt the proof of Hilbert's Theorem 90 in Theorem 6.18, using* $\mathrm{Tr}_{E/K}$ *in place of* $\mathrm{N}_{E/K}$.]

**6.10** (a) For $n \geqslant 1$ and $1 \leqslant k \leqslant n$, the *$k$-th power sum* $s_k \in \Bbbk[X_1, \ldots, X_n]^{\mathrm{S}_n}$ is defined by

$$s_k = \sum_{1 \leqslant i \leqslant n} X_i^k.$$

Prove the formula

$$s_k = e_1 s_{k-1} - e_2 s_{k-2} + \cdots + (-1)^{k-1} e_{k-1} s_1 + (-1)^k k e_k.$$

(b) For $n \geqslant 1$ and $1 \leqslant k \leqslant n$, the *total symmetric function* is defined by

$$h_k = \sum_{j_1 \leqslant j_2 \leqslant \cdots \leqslant j_k} X_{j_1} X_{j_2} \cdots X_{j_k},$$

*i.e.*, the sum of all the monomials in the $X_i$ of degree $k$.

(i) For large values of $n$, express $h_1, h_2, h_3$ in terms of the elementary symmetric functions $e_1, e_2, e_3$.

(ii) Show that the power sum functions $s_k$ of the previous question satisfy

$$s_k = -(h_1 s_{k-1} + h_2 s_{k-2} + \cdots + h_{k-1} s_1) + k h_k.$$

# Bibliography


[1] E. Artin, Galois Theory, Dover Publications (1998); ISBN 0 486 62342 4.

[2] J-P. Escofier, Galois theory, Springer-Verlag, New York (2001); ISBN 0-387-98765-7. [*Highly recommended, especially for its historical notes*]

[3] J. B. Fraleigh, A First Course in Abstract Algebra, Addison Wesley (1999); ISBN 0 201 33596 4. [*Highly recommended*]

[4] T. W. Hungerford, A counterexample in Galois theory, American Mathematical Monthly **97** (1997), 54–57.

[5] S. Lang, Algebra, Addison Wesley (1993); ISBN 0 201 55540 9.

[6] R. Lidl & H. Niederreiter, Finite Fields, Cambridge University Press (1997); ISBN 0 521 39231 4.

[7] J. Rotman, Galois Theory, Springer-Verlag (1998); ISBN 0 387 98541 7.

[8] I. Stewart, Galois Theory, Chapman and Hall (1989); ISBN 0 412 34550-1. [*Very highly recommended.*]