MT5836 Galois Theory

MRQ

May 10, 2019

Contents

Introduction

The subject of Galois Theory traces back to Évariste Galois (1811–1832). He was a French mathematician whose work involved understanding the solution of polynomial equations. The standard formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

for the roots of the quadratic equation

$$ax^2 + bx + c = 0$$

is well-known. It turns out that analogous formulae exist for the roots of cubic and quartic polynomial equations. For example, the method to solve the general cubic equation was considered by mathematicians based in Bologna in the early 16th century (e.g., Scipione dal Ferro (1465–1526) and those who followed him).

What Galois did was to show that, in general, a quintic equation could not be solved by a similar formula. What he did not do was succeed in explaining it to anyone in a comprehensible way. For example, in 1830 he submitted his work to the Paris Academy of Sciences, but the final report states:

> We have made every effort to understand Galois's proof. His reasoning is not sufficiently clear, sufficiently developed, for us to judge its correctness, and we can give no idea of it in this report. The author announces that the proposition which is the special object of this memoir is part of a general theory susceptible of many applications. Perhaps it will transpire that the different parts of a theory are mutually clarifying, are easier to grasp together rather than in isolation. We would then suggest that the author should publish the whole of his work in order to form a definitive opinion. But in the state which the part he has submitted to the Academy now is, we cannot propose to give it approval.
>
> [from Stewart, *Galois Theory, Second edition*, p.xxi]

Galois's ideas were eventually understood, via the letter that he wrote to Chevalier on the eve of the duel which killed him. This theory is basically what is presented in this lecture course. As we now understand it, what Galois observed is the following:

- To every polynomial equation, $f(x) = 0$, we can associate a group, the *Galois group*, consisting of certain permutations of the roots.
- If the Galois group is *soluble*, then the polynomial equation can be solved *by radicals* (that is, by a formula of the type we are interested in).
- We can construct a polynomial whose Galois group is the symmetric group S_5, which is not soluble since it contains the non-abelian simple group A_5, and therefore we cannot solve the corresponding polynomial equation by radicals.

In fact, what we do is more general. We shall actually consider a pair of fields one inside the other ($F \subseteq K$) and then associate to this a *Galois group* $\mathrm{Gal}(K/F)$. Our work in this module will be to understand the link between the two concepts of the field extension $F \subseteq K$ and its Galois group. As a consequence of understanding these we can then establish Galois's above observations by specialising to the case when K is the field obtained by adjoining the roots of our polynomial $f(x)$ to the field F.

Structure of the lecture course

The following topics will be covered in the lectures:

- **Basic facts about fields and polynomial rings:** Mostly a review of material from MT3503, but some new information about irreducible polynomials.
- **Field extensions:** Terminology and basic properties about the situation of two fields with $F \subseteq K$.
- **Splitting fields and normal extensions:** Field extensions constructed by adjoining the roots of a polynomial, constructed so that the polynomial factorizes into linear factors over the larger field.
- **Basic facts about finite fields:** Existence and uniqueness of field of order p^n, together with the fact that the multiplicative group of a finite field is cyclic.
- **Separable extensions and the Theorem of the Primitive Element:** Separability is a technical condition to avoid repeated roots of irreducible polynomials. The Theorem of the Primitive Element applies in this circumstance and allows us to assume that our field extensions have a specific form and hence to simplify various proofs.
- **Galois groups and the Fundamental Theorem of Galois Theory:** The definition of the Galois group as the collection of invertible structure preserving maps of a field extension (this will be made more precise later). The Fundamental Theorem of Galois Theory states that the structure of the Galois group corresponds to the structure of the field extension.
- **Examples and Applications:** Including the link between solution of a polynomial equation by radicals and the solubity of the Galois groups.

Recommended texts

- Ian Stewart, *Galois Theory*, Chapman & Hall; 3rd Edition, 2004 in the library; 4th Edition, 2015.
- John M. Howie, *Fields and Galois Theory*, Springer Undergraduate Mathematics Series, Springer, 2006.
- P. M. Cohn, *Algebra, Vol. 2*, Wiley, 1977, Chapter 3. [Out of print, but available in the library.]

Chapter 1

Rings, Fields and Polynomials

This first chapter contains a review of the background material required to study Galois Theory. The majority comes from the module *MT3505 Rings and Fields* and consequently many proofs in this chapter are omitted or greatly abbreviated. The last part of this chapter is concerned with polynomials and polynomial rings. One important concept that we shall use throughout the module is what it means for a polynomial to be *irreducible*. We shall devote some time to methods for establishing that a polynomial is irreducible.

Rings

We start with properties of rings before specialise to fields and to polynomial rings.

Definition 1.1 A *commutative ring with a* 1 is a set R endowed with two binary operations denoted as addition and multiplication such that the following conditions hold:

(i) R forms an abelian group with respect to addition (with additive identity 0, called *zero*);

(ii) multiplication is *associative*: $a(bc) = (ab)c$ for all $a, b, c \in R$;

(iii) multiplication is *commutative*: $ab = ba$ for all $a, b \in R$;

(iv) the *distributive laws* hold:

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

for all $a, b, c \in R$;

(v) there is a *multiplicative identity* 1 in R satisfying $a1 = 1a = a$ for all $a \in R$.

Comment: There is also a definition of a "ring", without the assumption of the multiplication being commutative or it having a multiplicative identity 1. One simply drops conditions (iii) and (v) from the definition above. Since we are interested in studying fields in this module, we shall not need to consider non-commutative rings as there will be no examples of such rings occurring in these notes. This is why we only give the more restricted definition of a *commutative* ring *with a* 1 above as this is sufficient for our needs. In addition, note that in a commutative ring one needs only assume one of the two distributive laws since the other may be deduced from that one via commutativity.

Definition 1.2 Let R be a commutative ring with a 1. An *ideal* I in R is a non-empty subset of R that is both an additive subgroup of R and satisfies the property that if $a \in I$ and $r \in R$, then $ar \in I$.

Thus a subset I of R is an ideal if it satisfies the following four conditions:

(i) I is non-empty (or $0 \in I$);

(ii) $a + b \in I$ for all $a, b \in I$;

(iii) $-a \in I$ for all $a \in I$;

(iv) $ar \in I$ for all $a \in I$ and $r \in R$.

(In a non-commutative ring, one needs to assume both ar and ra belong to I, but R being commutative ensures these products are equal.)

It follows from the definition that an ideal I of R is closed under multiplication: $ab \in I$ for all $a, b \in I$ (since an element $b \in I$ is, in particular, an element of the larger set R). This means that an ideal I is, in particular, a *subring*. Note that, in general, I does not contain the multiplicative identity 1, since if it did $r = 1r \in I$ for all $r \in R$. Thus, the only ideal of R that contains the multiplicative identity 1 is the ring R itself.

The reason for being interested in ideals is that one can form quotient rings, as we shall now describe. Let R be a commutative ring and let I be an ideal of R. Then I is, in particular, a subgroup of the additive group of R and the latter is an abelian group. We can therefore form the additive cosets of I; that is, define

$$I + r = \{\, a + r \mid a \in I \,\}$$

for each $r \in R$. We know from group theory (covered in both *MT2505* and *MT4003*) when two such cosets are equal,

$$I + r = I + s \qquad \text{if and only if} \qquad r - s \in I,$$

and that the set of all cosets forms a group via addition of the representatives:

$$(I + r) + (I + s) = I + (r + s) \qquad \text{for } r, s \in R.$$

(In arbitrary group, one requires that the subgroup is *normal*, but this holds because R is an *abelian* group under addition.) As is observed in *MT3505*, the assumption that I is an ideal then ensures that there is a well-defined multiplication on the set of cosets, given by

$$(I + r)(I + s) = I + rs \qquad \text{for } r, s \in R,$$

with respect to which the set of cosets $I + r$ forms a ring, called the *quotient ring* and denoted by R/I.

Theorem 1.3 *Let R be a commutative ring with a 1 and I be an ideal of R. Then the quotient ring R/I is a commutative ring with a 1.*

Proof: The fact that R/I is a ring is omitted, since verifying the above operations are well-defined is relatively technical and this was all established in *MT3505*. That the multiplication is commutative follows from the fact that the multiplication in R is commutative:

$$(I + r)(I + s) = I + rs = I + sr = (I + s)(I + r) \qquad \text{for all } r, s \in R.$$

The multiplication identity is $I + 1$:

$$(I + r)(I + 1) = I + r1 = I + r \qquad \text{for all } r \in R.$$

□

The other standard bit of terminology that we shall require relating to rings is, of course, the definition of a homomorphism. In the following, I shall use the common habit in algebra of writing maps on the right, so the image of an element a under a map ϕ is written $a\phi$ (rather than $\phi(a)$, as would be common in some other branches of mathematics).

Definition 1.4 Let R and S be commutative rings with 1. A *homomorphism* $\phi\colon R \to S$ is a map such that

(i) $(a+b)\phi = a\phi + b\phi$

(ii) $(ab)\phi = (a\phi)(b\phi)$

for all $a, b \in R$.

Definition 1.5 Let R and S be commutative rings with 1 and $\phi\colon R \to S$ be a homomorphism.

(i) The *kernel* of ϕ is
$$\ker\phi = \{\, a \in R \mid a\phi = 0 \,\}.$$

(ii) The *image* of ϕ is
$$\operatorname{im}\phi = R\phi = \{\, a\phi \mid a \in R \,\}.$$

Theorem 1.6 (First Isomorphism Theorem) *Let R and S be commutative rings with 1 and $\phi\colon R \to S$ be a homomorphism. Then the kernel of ϕ is an ideal of R, the image of ϕ is a subring of S and*
$$R/\ker\phi \cong \operatorname{im}\phi.$$

PROOF: This is a standard result established in *MT3505* (via a proof very similar to that used for groups). The isomorphism is the map given by
$$\theta\colon (\ker\phi) + a \mapsto a\phi$$
for $a \in R$. One must, amongst other things, establish that this is well-defined, in the sense that the image of a coset under θ does not depend upon the choice of representative a for the coset in the quotient ring. □

A final set of ring-theoretic definitions are the following, to which we return at the end of this chapter.

Definition 1.7 Let R be a commutative ring with a 1.

(i) A *zero divisor* in R is a non-zero element a such that $ab = 0$ for some non-zero $b \in R$.

(ii) An *integral domain* is a commutative ring with a 1 containing no zero divisors.

Fields

Galois Theory can be viewed as the study of fields and their subfields. We shall now present the basic facts about such structures.

Definition 1.8 A *field* F is a commutative ring with a 1 such that $0 \neq 1$ and every non-zero element is a *unit*, that is, has a multiplicative inverse.

Thus a field F is a commutative ring with a 1 such that (i) there are non-zero elements and (ii) if $a \in F$ with $a \neq 0$, then there exists some $b \in F$ with $ab = 1$. We shall write a^{-1} or $1/a$ for the multiplicative inverse of a.

Example 1.9 (i) Standard examples of fields familiar from, for example, linear algebra are the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of rational numbers, real numbers and complex numbers, respectively.

(ii) If p is a prime number, the set $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ forms a field under addition and multiplication modulo p. To see that every non-zero element has a multiplicative inverse, note that if $1 \leqslant x \leqslant p-1$, then x and p are coprime, so there exists $u, v \in \mathbb{Z}$ with $ux + vp = 1$ (exploiting the fact that $\mathbb{Z}$ is a *Euclidean domain*). Hence, $ux \equiv 1 \pmod{p}$ and so, modulo p, u is a multiplicative inverse for x in $\mathbb{F}_p$.

Proposition 1.10 (i) *Every field is an integral domain.*

(ii) *The set of non-zero elements in a field forms an abelian group under multiplication.*

We write F^* for the multiplicative group of non-zero elements in a field.

PROOF: [Omitted in lectures. These facts were observed in *MT3505*.]

Let F be a field.

(i) If $a, b \in F$ with $a \neq 0$ and $ab = 0$, then $b = a^{-1}(ab) = 0$. Hence if $ab = 0$, either $a = 0$ or $b = 0$, so F contains no zero divisors.

(ii) Write $F^* = F \setminus \{0\}$. Part (i) tells us that F^* is closed under multiplication. The remaining conditions to be an abelian group under this binary operation follow immediately from the definition of a field (multiplication is associative in any ring, it is commutative in any commutative ring, there is a multiplicative identity in any ring with a 1, and in a field every non-zero element has a multiplicative inverse). □

If F is any field, with multiplicative identity denoted by 1, and n is a positive integer, let us define

$$\overline{n} = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

By the distributive law,

$$\overline{mn} = \overline{m}\,\overline{n}$$

for all positive integers m and n. Since F is, in particular, an integral domain, it follows that if there exists a positive integer n such that $\overline{n} = 0$ then necessarily the smallest such positive integer n is a prime number.

Definition 1.11 Let F be a field with multiplicative identity 1.

(i) If it exists, the smallest positive integer p such that $\overline{p} = 0$ is called the *characteristic* of F.

(ii) If no such positive integer exists, we say that F has *characteristic zero*.

Our observation is therefore that every field F either has characteristic zero or has characteristic p for some prime number p. We shall say that K is a *subfield* of F when $K \subseteq F$ and that K forms a field itself under the addition and multiplication induced from F; that is, when the following conditions hold:

(i) K is non-empty and contains non-zero elements (or, equivalently when taken with the other two conditions, $0, 1 \in K$);

(ii) $a + b, -a, ab \in K$ for all $a, b \in K$;

(iii) $1/a \in K$ for all non-zero $a \in K$.

Theorem 1.12 *Let F be a field.*

(i) *If F has characteristic zero, then F has a unique subfield isomorphic to the rationals $\mathbb{Q}$ and this is contained in every subfield of F.*

(ii) *If F has characteristic p (prime), then F has a unique subfield isomorphic to the field $\mathbb{F}_p$ of integers modulo p and this is contained in every subfield of F.*

Definition 1.13 This unique minimal subfield in F is called the *prime subfield* of F.

PROOF: This was proved in *MT3505*. One proves it as follows:

(i) Suppose F has characteristic zero. Extend the notation $\overline{n}$ to all $n \in \mathbb{Z}$ by defining

$$\overline{0} = 0 \qquad \text{and} \qquad \overline{-n} = -\overline{n}$$

for all positive integers n. If K is any subfield of F then K contains 0, 1 and all sums involving 1, so $\overline{n} \in K$ for all $n \in \mathbb{Z}$. Hence

$$Q = \{\, \overline{m}/\overline{n} \mid m, n \in \mathbb{Z},\ n \neq 0 \,\}$$

is a subset of the subfield K.

One now verifies, from the field axioms and the assumption that $\overline{n} \neq 0$ when $n \neq 0$, that the map $n \mapsto \overline{n}$ is a ring homomorphism $\mathbb{Z} \to F$ and then extend this to a ring homomorphism $\mathbb{Q} \to F$ given by $m/n \mapsto \overline{m}/\overline{n}$. We conclude that Q is a subfield of F that is isomorphic to the field $\mathbb{Q}$ of rational numbers and is contained in every subfield K of F.

Finally, uniqueness of Q follows from the minimality condition: if Q_1 and Q_2 were subfields contained in every subfield of F then, in particular, $Q_1 \subseteq Q_2$ and $Q_2 \subseteq Q_1$, from which we deduce $Q_1 = Q_2$.

(ii) Use a similar argument to part (i). If F has characteristic p (prime) and K is any subfield of F, then K contains all the elements $\overline{n}$; that is,

$$P = \{0, 1, \overline{2}, \overline{3}, \ldots, \overline{p-1}\} \subseteq K.$$

Now observe that P is closed under addition and multiplication and the map $n \mapsto \overline{n}$ is an isomorphism from the field $\mathbb{F}_p$ of p elements to P. □

Polynomials

Polynomials arise in a number of places within Galois Theory. The motivation of the subject arises in the problem of solving polynomial equations. More significantly, algebraic elements, those arising as roots of polynomial equations, will be of great importance in our field extensions as discussed in Chapter 2.

Definition 1.14 Let F be a field. A *polynomial* over F in the indeterminate X is an expression of the form

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

where n is a non-negative integer and the coefficients a_0, a_1, …, a_n are elements of F.

We shall often substitute elements of a field for the indeterminate in a polynomial. Thus if α is an element of the field F, or indeed of any field that contains F as a subfield, and $f(X) = a_0 + a_1X + \cdots + a_nX^n$ where the coefficients are also elements in F, we write $f(\alpha)$ for the expression

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n.$$

We shall write $F[X]$ for the set of all polynomials in the indeterminate X with coefficients taken from the field F. We add two such polynomials by simply adding the coefficients,

$$\sum a_iX^i + \sum b_iX^i = \sum (a_i + b_i)X^i,$$

and we multiply two polynomials by exploiting the distributive law:

$$\Big(\sum a_i X^i\Big)\Big(\sum b_i X^i\Big) = \sum c_i X^i$$

where $c_k = \sum_{i=1}^{k} a_i b_{k-i}$. With these definitions, one deduces in a straightforward way that $F[X]$ forms a commutative ring with a 1, namely the multiplicative identity is the constant polynomial 1. If $f(X)$ has a non-zero term $a_n X^n$ of highest degree (that is, all other terms in $f(X)$ has the form $a_i X^i$ with $i < n$) and $g(X)$ has a non-zero term $b_m X^m$ of highest degree, then the term of highest degree in $f(X)g(X)$ is $a_n b_m X^{n+m}$ and this is non-zero since F is a field so $a_n b_m \neq 0$. Therefore $F[X]$ is actually an integral domain since $f(X), g(X) \neq 0$ implies $f(X)g(X) \neq 0$.

Proposition 1.15 *If F is a field, the polynomial ring $F[X]$ is a* Euclidean domain.

The Euclidean function associated to $F[X]$ is the degree of a polynomial. Recall that if $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ is a *non-zero* polynomial with leading term having non-zero coefficient, that is, $a_n \neq 0$, the *degree* of $f(X)$ is

$$\deg f(X) = n.$$

The properties of the degree are:

(i) if $f(X)$ and $g(X)$ are non-zero, then $\deg f(X)g(X) = \deg f(X) + \deg g(X)$;

(ii) if $f(X)$ and $g(X)$ are polynomials with $f(X) \neq 0$, then there exist unique polynomials $q(X)$ and $r(X)$ satisfying

$$g(X) = q(X)\, f(X) + r(X) \qquad \text{with either } r(X) = 0 \text{ or } \deg r(X) < \deg f(X).$$

These properties were established in *MT3505*. They are not verified in this module, but will be assumed, and are what is claimed within Proposition 1.15.

As a consequence, all the properties of Euclidean domains established in *MT3505* apply to a polynomial ring $F[X]$ over a field F. For example:

Proposition 1.16 *If F is a field, the polynomial ring $F[X]$ is a principal ideal domain; that is, every ideal I in $F[X]$ has the form $I = \big(f(X)\big) = \{\, f(X)g(X) \mid g(X) \in F[X] \,\}$ for some polynomial $f(X)$.*

Proof: Let I be an ideal of $F[X]$. If $I = \{0\}$, then $I = (0)$. Suppose that $I \neq \{0\}$. Let $f(X)$ be a polynomial in I such that $\deg f(X)$ is as small as possible among the degrees of non-zero polynomials in I. Certainly $\big(f(X)\big) \subseteq I$, since I is closed under multiplication by any polynomial.

Now if $g(X) \in I$, divide $f(X)$ to obtain a quotient and remainder:

$$g(X) = q(X)\, f(X) + r(X)$$

where either $r(X) = 0$ or $\deg r(X) < \deg f(X)$. Then $r(X) = g(X) - q(X)\, f(X)$ belongs to I, since I is an ideal. By the assumption about $f(X)$ having smallest degree amongst non-zero polynomials in I, we conclude $r(X) = 0$. Hence $g(X)$ is indeed a multiple of $f(X)$. This establishes $I = \big(f(X)\big)$, as claimed. □

Another fact that holds as a consequence of Proposition 1.15 concerns the greatest common divisor of a pair (or more) of polynomials.

Definition 1.17 Suppose $f(X)$ and $g(X)$ are polynomials over the field F. A *greatest common divisor* of $f(X)$ and $g(X)$ is a polynomial $h(X)$ of greatest degree such that $h(X)$ divides both $f(X)$ and $g(X)$.

To say that $h(X)$ *divides* $f(X)$ means that $f(X)$ is a multiple of $h(X)$; that is, $f(X) = h(X)\,q(X)$ for some $q(X) \in F[X]$. In a general Euclidean domain, the greatest common divisor is defined uniquely up to multiplication by a unit. In the polynomial ring $F[X]$, the units are constant polynomials (that is, elements of the base field F viewed as elements of $F[X]$). This follows from the first property of degrees listed: $\deg f(X)g(X) = \deg f(X) + \deg g(X)$, so the only way that $f(X)g(X) = 1$ can hold is if $\deg f(X) = 0$. As a consequence, the greatest common divisor of a pair of polynomials is defined uniquely up to multiplication by a scalar from the field F.

We shall need at times the following fact about the form of the greatest common divisor in a Euclidean domain. This result is often accompanied with a practical algorithm for computing the greatest common divisor, but that will not be as important in this module. The proof of the result can be found in *MT3505*.

Theorem 1.18 *Let F be a field and $f(X)$ and $g(X)$ be two non-zero polynomials over F. Then there exist $u(X), v(X) \in F[X]$ such that the greatest common divisor of $f(X)$ and $g(X)$ is given by*

$$h(X) = u(X)\,f(X) + v(X)\,g(X).$$

Another standard fact about a Euclidean domain is that it is necessarily a unique factorization domain. Consequently, every polynomial over F can be factorized as a product of irreducible polynomials and these irreducible factors are determined uniquely up to multiplication by scalars (as the units are the constant polynomials) and reordering of the factors (of course, since multiplication is commutative). In view of this, we record the definition of what it means for a polynomial to be irreducible, since that will be a particularly significant concept in terms of what follows.

Definition 1.19 Let $f(X)$ be a polynomial over a field F of degree at least 1. We say that $f(X)$ is *irreducible* over F if it cannot be factorized as $f(X) = g_1(X)\,g_2(X)$ where $g_1(X)$ and $g_2(X)$ are polynomials in $F[X]$ of degree smaller than $f(X)$.

Thus, a polynomial $f(X)$ is irreducible if the only polynomials of degree smaller than $f(X)$ that divide it are the constant polynomials (i.e., the units). The term *reducible* is used for a polynomial that is not irreducible; that is, that can be factorized as a product of two polynomials of smaller degree. It will be important to be able to show that certain polynomials are irreducible. In general, this is rather difficult to achieve and one generally needs to rely upon *ad hoc* methods, particularly over fields of characteristic $p > 0$.

We first make the observation that the concept of irreducibility depends heavily upon the field over which we are working. After that we shall consider various examples of methods for showing polynomials are irreducible.

Example 1.20 Consider the polynomial $f(X) = X^2 + 1$. If we view $f(X)$ as a polynomial over the real numbers $\mathbb{R}$, then it is irreducible: if it were to factorize then it would be a product of two linear factors. However, the roots of this polynomial do not exist in the real numbers, so $f(X)$ has no roots in $\mathbb{R}$ and hence is irreducible over $\mathbb{R}$. However, when viewed as a polynomial over $\mathbb{C}$, it is reducible:

$$X^2 + 1 = (X - i)(X + i)$$

Similary $g(X) = X^2 - 2$ is irreducible over $\mathbb{Q}$ (since it has no roots in $\mathbb{Q}$, so can have no linear factors), but is reducible over $\mathbb{R}$ (since it factorizes over this field as $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.

Example 1.21 *Show that the following polynomials are irreducible over the given fields:*

(i) $f(X) = X^2 + X + 1$ *over* $\mathbb{F}_2$*;*

(ii) $g(X) = X^3 + 2X + 1$ *over* $\mathbb{F}_3$*;*

(iii) $h(X) = X^4 + X + 1$ *over* $\mathbb{F}_2$.

SOLUTION: (i) If $f(X) = X^2 + X + 1$ factorizes into two polynomials of smaller degree over $\mathbb{F}_2$, then it is a product of two linear factors and hence would have a root in $\mathbb{F}_2$. Observe $f(0) = f(1) = 1$. Hence $f(X)$ has no roots in $\mathbb{F}_2$ and is therefore irreducible.

(ii) If $g(X) = X^3 + 2X + 1$ factorizes into two polynomials of smaller degree over $\mathbb{F}_3$, then one of these factors would be linear and hence $g(X)$ would have a root in $\mathbb{F}_3$. Observe $g(0) = g(1) = g(2) = 1$. Hence $g(X)$ has no roots in $\mathbb{F}_3$ and is therefore irreducible.

(iii) First note that $h(0) = h(1) = 1$, so $h(X)$ has no roots in $\mathbb{F}_2$ and hence has no linear factors. As a consequence, if $h(X)$ is reducible, then it is a product of two irreducible quadratic factors. There are four quadratic polynomials over $\mathbb{F}_2$:

$$X^2, \quad X^2 + 1, \quad X^2 + X, \qquad X^2 + X + 1.$$

The first three are reducible, having either 0 or 1 (or both in the case of the third) as roots. We conclude that $X^2 + X + 1$ is the only irreducible quadratic polynomial over $\mathbb{F}_2$. Note that

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1$$

(since $\mathbb{F}_2$ has characteristic 2) and therefore $h(X) = X^4 + X + 1$ is not a product of $X^2 + X + 1$ with itself.

We conclude that $h(X)$ is indeed irreducible over $\mathbb{F}_2$. □

If one works over the field $\mathbb{Q}$ of rational numbers, then there are several methods that are useful for determining that a polynomial $f(X)$ is irreducible. First note that we can multiply by the lowest common multiple of the denominators of the coefficients in $f(X)$ and obtain a scalar multiple of $f(X)$ that happens to have all its coefficients being integers. In view of this, we shall discuss polynomials with integer coefficients and ask whether they are irreducible as polynomials over $\mathbb{Q}$. The first step is to note that it is sufficient to show that such a polynomial cannot be factorized into two polynomials with integer coefficients.

Theorem 1.22 (Gauss's Lemma) *Let $f(X)$ be a polynomial with integer coefficients. Then $f(X)$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.*

PROOF: Let $f(X) \in \mathbb{Z}[X]$. Note that if $f(X) = g_1(X)\, g_2(X)$ where $g_1(X), g_2(X) \in \mathbb{Z}[X]$ and $\deg g_1(X), \deg g_2(X) < \deg f(X)$, then this is also a factorization over $\mathbb{Q}$ (essentially because $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$). Hence, taking the contrapositive, if $f(X)$ is irreducible over $\mathbb{Q}$ then it is irreducible over $\mathbb{Z}$.

Conversely, suppose $f(X) = g_1(X)\, g_2(X)$ where $g_1(X), g_2(X) \in \mathbb{Q}[X]$ with degrees satisfying $\deg g_1(X), \deg g_2(X) < \deg f(X)$. Consider the denominators of the coefficients appearing in the polynomials $g_1(X)$ and $g_2(X)$. Multiply through by the lowest common multiple of the denominators of the coefficients of $g_1(X)$ and by that for $g_2(X)$. Hence we find a positive integer n such that the expression

$$n\, f(X) = \bar{g}_1(X)\, \bar{g}_2(X) \tag{1.1}$$

holds, where $\bar{g}_1(X), \bar{g}_2(X) \in \mathbb{Z}[X]$, $\deg \bar{g}_1(X) = \deg g_1(X) < \deg f(X)$ and $\deg \bar{g}_2(X) = \deg g_2(X) < \deg f(X)$. Among all such expressions, choose n to be the smallest positive integer such that we can factorize $n\, f(X)$ as in Equation (1.1).

We claim that $n = 1$. If not, choose a prime number p that divides n. Then p divides the product $\bar{g}_1(X)\,\bar{g}_2(X)$. Suppose

$$\bar{g}_1(X) = a_0 + a_1X + \cdots + a_\ell X^\ell \qquad \text{and} \qquad \bar{g}_2(X) = b_0 + b_1X + \cdots + b_mX^m$$

for some coefficients $a_i, b_i \in \mathbb{Z}$. We claim that p either divides all the a_i or divides all the b_i. If not, we can assume that p divides a_0, a_1, …, a_{j-1} but does not divide a_j and that p divides b_0, b_1, …, b_{k-1} but does not divide b_k. Consider the coefficient c_{j+k} of X^{j+k} in the product $\bar{g}_1(X)\,\bar{g}_2(X)$:

$$c_{j+k} = a_0b_{j+k} + \cdots + a_{j-1}b_{k+1} + a_jb_k + a_{j+1}b_{k-1} + \cdots + a_{j+k}b_0.$$

We know that p divides c_{j+k} and that it divides a_0, a_1, …, a_{j-1}, b_0, …, b_{k-1}. Hence p divides the product a_jb_k and therefore p divides either a_j or b_k (since p is a prime number). This contradicts our assumption.

We conclude that either p divides all the coefficients of $\bar{g}_1(X)$ or of $\bar{g}_2(X)$. Let us assume the former. Define $\tilde{g}_1(X)$ to equal $\frac{1}{p}\bar{g}_1(X)$, which we now know is a polynomial with integer coefficients. We may therefore divide Equation (1.1) by p to obtain

$$\tfrac{n}{p}\, f(X) = \tilde{g}_1(X)\,\bar{g}_2(X).$$

This contradicts the choice of n to be minimal. We conclude therefore that $n = 1$ and hence that $f(X)$ is factorizable as a product of two polynomials of smaller degree over $\mathbb{Z}$. This completes the proof of Gauss's Lemma. □

Theorem 1.23 (Eisenstein's Irreducibility Criterion) *Let*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

be a polynomial over $\mathbb{Z}$. Suppose there exists a prime number p such that

(i) *p does not divide a_n;*

(ii) *p divides a_0, a_1, …, a_{n-1};*

(iii) *p^2 does not divide a_0.*

Then $f(X)$ is irreducible over $\mathbb{Q}$.

Proof: In view of Gauss's Lemma, it is sufficient to show that $f(X)$ cannot be factorized into two polynomials of smaller degree over $\mathbb{Z}$. Suppose that $f(X) = g_1(X)\,g_2(X)$, where

$$g_1(X) = b_0 + b_1X + \cdots + b_kX^k \qquad \text{and} \qquad g_2(X) = c_0 + c_1X + \cdots + c_\ell X^\ell$$

and where $b_0, b_1, \ldots, b_k, c_0, c_1, \ldots, c_\ell \in \mathbb{Z}$. Note $a_0 = b_0c_0$, so by hypotheses (ii) and (iii), p divides one of b_0 or c_0, but not both. Let us suppose, without loss of generality, that p divides b_0 but not c_0. Now since p does not divides a_n, it cannot be the case that p divides all the coefficients of $g_1(X)$. Hence there exists some coefficient b_i such that p divides b_0, b_1, …, b_{i-1}, but p does not divide b_i. Note $i \leqslant k = \deg g_1(X) < n$. Then, by hypothesis (ii),

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0$$

is divisible by p and it follows that p divides the last term b_ic_0 (as p divides b_0, b_1, …, b_{i-1}). However, p divides neither of b_i or c_0, so this is impossible.

This contradiction establishes that $f(X)$ is indeed irreducible over $\mathbb{Q}$. □

Example 1.24 *Show that the following polynomials are irreducible over $\mathbb{Q}$:*

(i) $X^n - p$, *for any prime number* p;

(ii) $\frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$;

(iii) $X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1$, *for any prime number* p.

SOLUTION: (i) $X^n - p$ is irreducible by Eisenstein's Criterion: it is of the form to apply Theorem 1.23.

(ii) If $f(X) = \frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$, then

$$9f(X) = 2X^5 + 15X^4 + 9X^3 + 3.$$

Thus $9f(X)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (using the prime $p = 3$), so cannot be factorized as a product of polynomials of smaller degree over $\mathbb{Q}$. The same therefore applies to $f(X)$. (Note that 9 is a unit in $\mathbb{Q}[X]$.)

(iii) Write $\Phi(X) = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1$. Suppose $\Phi(X)$ can be factorized as a product of polynomials of smaller degree over $\mathbb{Q}$; say, $\Phi(X) = g(X)\,h(X)$. Note

$$(X-1)\cdot\Phi(X) = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1) = X^p - 1.$$

Substitute $Y = X - 1$:

$$Y \cdot \Phi(Y+1) = (Y+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} Y^i.$$

Hence

$$\begin{aligned}\Phi(Y+1) &= \sum_{i=1}^{p} \binom{p}{i} Y^{i-1} \\ &= Y^{p-1} + \binom{p}{p-1} Y^{p-2} + \binom{p}{p-2} Y^{p-3} + \cdots + \binom{p}{2} Y + \binom{p}{1}.\end{aligned}$$

The constant coefficient in $\Phi(Y+1)$ is $\binom{p}{1} = p$, which is divisible by p but not p^2. Note that, for $i = 1, 2, \ldots, p-1$,

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!} = \frac{p(p-1)(p-2)\ldots(p-i+1)}{i!}$$

and we know this is an integer. Note that the prime p is bigger than all the factors in $i!$ (by assumption on i), so

$$\textit{the binomial coefficient } \binom{p}{i} \textit{ is divisible by the prime } p \textit{ for } i = 1, 2, \ldots, p-1. \tag{1.2}$$

Hence we may apply Eisenstein's Criterion to $\Phi(Y+1)$ to conclude that $\Phi(Y+1)$ is irreducible as a polynomial in Y. Our original assumption, however, implies that $\Phi(Y+1) = g(Y+1)\,h(Y+1)$, which is a contradiction.

Hence $\Phi(X)$ is indeed irreducible over $\mathbb{Q}$. □

There is one final method that we mention for showing a polynomial (with integer coefficients) is irreducible is to reduce the coefficients modulo some prime p. The choice of prime p is usually delicate: when the type of argument presented here applies, it typically does so for some choices of prime but not others.

Example 1.25 *Show that the polynomial* $f(X) = X^4 + 8X^3 + 9X^2 + 6X + 5$ *is irreducible over* $\mathbb{Q}$.

SOLUTION: Suppose that $f(X)$ is reducible over $\mathbb{Q}$. Then $f(X)$ is reducible over $\mathbb{Z}$, by Gauss's Lemma, so factorizes as a product of polynomials with integer coefficients of smaller degree.

We shall reduce all the coefficients modulo 3. To be more precise, there is a ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{F}_3$ that arises by reducing an integer modulo 3. The kernel of ϕ is the ideal (3) of all multiples of 3. We induce a map $\bar{\phi}\colon \mathbb{Z}[X] \to \mathbb{F}_3[X]$ by applying ϕ to the coefficients in a polynomial; that is, reducing the coefficients modulo 3. Since the coefficients of sums of polynomials and products of polynomials are determined by operations in the base ring/field, it follows, from the fact that ϕ is a homomorphism, the induced map $\bar{\phi}$ is a ring homomorphism $\mathbb{Z}[X] \to \mathbb{F}_3[X]$. Applying $\bar{\phi}$ to the factorization of $f(X)$ as a product of two polynomials from $\mathbb{Z}[X]$, we conclude that

$$\bar{f}(X) = f(X)\bar{\phi} = X^4 + 2X^3 + 2$$

factorizes; that is, $\bar{f}(X)$ is reducible over $\mathbb{F}_3$. We shall show this is impossible.

First note

$$\bar{f}(0) = 2, \qquad \bar{f}(1) = 2, \qquad \bar{f}(2) = 2^4 + 2^4 + 2 = 1,$$

so that $\bar{f}(X)$ does not have any roots in $\mathbb{F}_3$ and hence has no linear factors. Therefore $\bar{f}(X)$ must be a product of quadratic factors:

$$X^4 + 2X^3 + 2 = (X^2 + aX + b)(X^2 + cX + d)$$

for some coefficients $a, b, c, d \in \mathbb{F}_3$. Equating coefficients:

$$\begin{aligned} a + c &= 2, & ac + b + d &= 0, \\ ad + bc &= 0, & bd &= 2 \end{aligned}$$

The constant coefficient tells us that either $b = 1$ and $d = 2$, or $b = 2$ and $d = 1$. Thus $b + d = 0$. The degree 2 coefficient then tells us $ac = 0$, so either $a = 0$ or $c = 0$. The degree 1 coefficient then tells us that the other of a or c is also zero. Then $a + c = 0$, so the degree 3 coefficient equation fails.

In conclusion, $\bar{f}(X)$ is irreducible over $\mathbb{F}_3$ and we then deduce the original assumption about $f(X)$ was incorrect. Hence $f(X)$ is indeed irreducible over $\mathbb{Q}$. □

The final fact about integral domains, that we shall apply to the polynomial ring $F[X]$, is that every integral domain has a field of fractions. To be precise, if R is an integral domain, the field of fractions of R is the set of all expressions of the form r/s where (i) $r, s \in R$ with $s \neq 0$, and (ii) we define $r_1/s_1 = r_2/s_2$ if and only if $r_1 s_2 = r_2 s_1$. (The latter condition defines an equivalence relation on ordered pairs (r, s) with $s \neq 0$ and we write r/s for the equivalence containing the ordered pair (r, s) under this equivalence relation.) Mirroring the definition of addition and multiplication on the rational numbers, we define

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \qquad \text{and} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

for such fractions r_1/s_1 and r_2/s_2. One verifies that the set of all such fractions forms a commutative ring under this operation and that every non-zero fraction r/s (that is, when both r and s are non-zero) has a multiplicative inverse, namely s/r, because

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{rs} = \frac{1}{1}$$

from the definition of when two fractions are equal. The latter is the multiplicative identity in the field of fractions. Notice finally that R embeds in the field of fractions via the map $r \mapsto r/1$; that is, the set $\{\, r/1 \mid r \in R \,\}$ is a subring isomorphic to the original integral domain R.

Let us apply this construction in the case when $R = F[X]$, the integral domain of polynomials with coefficients from the field F. We consequently construct the following object:

Definition 1.26 Let F be a field. The *field of rational functions* with coefficients in F is denoted by $F(X)$ and is the field of fractions of the polynomial ring $F[X]$.

The elements of $F(X)$ are expressions of the form

$$\frac{f(X)}{g(X)}$$

where $f(X)$ and $g(X)$ are polynomials with coefficients from F. Equality of two such expressions is given by

$$\frac{f_1(X)}{g_1(X)} = \frac{f_2(X)}{g_2(X)} \qquad \text{if and only if} \qquad f_1(X)\, g_2(X) = f_2(X)\, g_1(X).$$

If one exploits the fact that $F[X]$ is a unique factorization domain, one can deduce from this that $f_2(X)$ and $g_2(X)$ are obtained from $f_1(X)$ and $g_1(X)$ via cancelling and then multiplying by some common factors. Addition in $F(X)$ is achieved by placing a pair of fractions over a common denominator. The polynomial $f(X)$ is identified with its image $f(X)/1$ in the field $F(X)$. Thus, we view the polynomial ring $F[X]$ as a subring of the field $F(X)$ of rational functions. In particular, since the constant polynomials form a copy of F, we observe:

Proposition 1.27 *The field F occurs as a subfield of the field $F(X)$ of rational functions with coefficients in F.*

Chapter 2

Field Extensions

This chapter introduces the primary terminology that will be used throughout the module. Galois Theory is essentially the study of fields satisfying $F \subseteq K$; that is, what we call a field extension. We shall present here the basic technology required to work with such extensions.

Definition 2.1 Let F and K be fields such that F is a subfield of K. We then say that K is an *extension* of F. We also call F the *base field* of the extension.

In particular, note that every field is an extension of its prime subfield. The point of this definition, though, is a change of perspective. We are not viewing a field extension $F \subseteq K$ as being the situation where we start with a field K and then pass to a subfield F. Instead, the philosophy here will be much more starting with a base field F and then creating a bigger field K containing F that is the extension. We shall flesh out this viewpoint initially over the course of the chapter and subsequently over the whole module.

The degree of an extension

The first observation to make in this setting is that if the field K is an extension of the field F, then K, in particular, satisfies the following conditions:

- K forms an abelian group under addition;
- we can multiply elements of K by elements of F;
- $a(x + y) = ax + ay$ for all $a \in F$ and $x, y \in K$;
- $(a + b)x = ax + bx$ for all $a, b \in F$ and $x \in K$;
- $(ab)x = a(bx)$ for all $a, b \in F$ and $x \in K$;
- $1x = x$ for all $x \in K$.

Thus, we can view K as a *vector space* over the field F.

Definition 2.2 Let the field K be an extension of the field F.

(i) The *degree* of K over F is the dimension of K when viewed as a vector space over F. We denote this by $|K : F|$. Thus

$$|K : F| = \dim_F K.$$

(ii) If the degree $|K : F|$ is finite, we say that K is a *finite extension* of F.

Warning: Note that saying K is a finite extension of F does *not* mean that K is a finite field. There are many situations where both fields have infinitely many elements in them. It refers precisely to the *dimension* of the bigger field over the smaller field.

Example 2.3 (i) The field $\mathbb{C}$ of complex numbers is an extension of the field $\mathbb{R}$ of real numbers. Every complex number can be written as $x + iy$ where $x, y \in \mathbb{R}$ and it follows that $\{1, i\}$ is a basis for the set of complex numbers when viewed as a real vector space. Hence

$$|\mathbb{C} : \mathbb{R}| = 2;$$

that is, this is a degree 2 extension.

(ii) The field $\mathbb{R}$ of real numbers is an extension of the field $\mathbb{Q}$ of rational numbers. Any finite dimensional vector space V over $\mathbb{Q}$ is countable, since if $\{v_1, v_2, \ldots, v_n\}$ is a basis for V over $\mathbb{Q}$, then there are countably many elements of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

with $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}$. Since $\mathbb{R}$ is uncountable, we conclude that $\mathbb{R}$ is not a finite extension of $\mathbb{Q}$; it has infinite degree over $\mathbb{Q}$.

Theorem 2.4 (Tower Law) *Let $F \subseteq K \subseteq L$ be field extensions. Then L is a finite extension of F if and only if L is a finite extension of K and K is a finite extension of F. In such a case,*

$$|L : F| = |L : K| \cdot |K : F|.$$

PROOF: First suppose that L is a finite extension of F. This means that, when viewed as a vector space over F, L is finite-dimensional. Now $K \subseteq L$ and K is closed under addition and by multiplication by elements of F (since it is a field). Hence K is a subspace of L, when viewed as a vector space over F, and so is also finite-dimensional over F.

Let $\mathscr{B} = \{x_1, x_2, \ldots, x_k\}$ be a basis for L over F. Then every element of L can be written in the form

$$a_1 x_1 + a_2 x_2 + \cdots + a_k x_k \tag{2.1}$$

where $a_1, a_2, \ldots, a_k \in F$. Therefore, every element of L can also be written in the form (2.1) where we choose the coefficients a_i from the field K. (We certainly get all the linear combinations built using scalars from F and cannot produce elements outside L since K is a subfield of L.) Hence $\mathscr{B}$ spans L when viewed as vector space over K and so we conclude $|L : K| < \infty$.

Conversely, suppose that both $|L : K|$ and $|K : F|$ are finite. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis for L over K and let $\{w_1, w_2, \ldots, w_n\}$ be a basis for K over F. We claim that the set of products $\mathscr{B} = \{\, v_i w_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \,\}$ is a basis for L over F.

First note that if $x \in L$, then we can express x in terms of the basis for L over K, to deduce that there exist $a_1, a_2, \ldots, a_m \in K$ such that

$$x = \sum_{i=1}^{m} a_i v_i.$$

Now, for each i, express a_i in terms of the basis for K over F to find $b_{i1}, b_{i2}, \ldots, b_{in} \in F$ such that

$$a_i = \sum_{j=1}^{n} b_{ij} w_j.$$

Substitute this into the previous sum to conclude

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} v_i w_j$$

and we conclude that $\mathscr{B}$ does indeed span L as a vector space over F.

Now suppose that for some coefficients $c_{ij} \in F$ such that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} v_i w_j = 0.$$

First express this as

$$\sum_{i=1}^{m} \Big(\sum_{j=1}^{n} c_{ij} w_j \Big) v_i = 0$$

and use the fact that $\{v_1, v_2, \ldots, v_m\}$ is a basis for L over K to conclude that, for $i = 1, 2, \ldots, m$, the elements

$$\sum_{j=1}^{n} c_{ij} w_j$$

in K are all equal to 0. Now use the fact that $\{w_1, w_2, \ldots, w_n\}$ is a basis for K over F to deduce

$$c_{ij} = 0 \qquad \text{for all } i \text{ and } j.$$

We therefore conclude that $\mathscr{B}$ is indeed a basis for L over F. In conclusion, L is a finite extension of F and

$$|L : F| = |\mathscr{B}| = mn = |L : K| \cdot |K : F|.$$

□

Comment: We shall need the observation made in the course of the proof later, so we make this explicit: In the setting of the theorem, if $\{v_1, v_2, \ldots, v_m\}$ is a basis for L over K and $\{w_1, w_2, \ldots, w_n\}$ is a basis for K over F, then $\{ v_i w_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \}$ is a basis for L over F.

Algebraic elements and algebraic extensions

The central results presented in this module will concern finite extensions and accordingly we seek to establish detailed information about such extensions. The first step is understand the concept of algebraic elements and their link to polynomial equations. Later in this chapter we shall show that we can characterize finite extensions in terms of algebraic elements.

Definition 2.5 Let the field K be an extension of the field F.

(i) An element $\alpha \in K$ is said to be *algebraic* over F if there exists a non-zero polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$. When this holds, we shall say that α satisfies the polynomial equation $f(X) = 0$.

(ii) We say that K is an *algebraic extension* of F if every element of K is algebraic over F.

Thus to say that an element $\alpha \in K$ is algebraic over the subfield F is to say that there are coefficients b_0, b_1, …, b_n in F such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

The first observation to make is that every element α of the base field F is algebraic over F since it is a root of the linear (i.e., degree 1) polynomial $X - \alpha$. The interesting question is then which other elements of K also happen to be algebraic over F. Indeed in the context of finite extensions, our first, and important, observation is the following.

Lemma 2.6 *Every finite extension is an algebraic extension.*

PROOF: Let K be an extension of F of degree n. Let $\alpha \in K$. Then the $n+1$ elements

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

are linearly dependent over F, so there exist coefficients b_0, b_1, ..., b_n in F, not all of which are zero, such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

Hence α satisfies a non-zero polynomial over F (namely $f(X) = b_0 + b_1X + \cdots + b_nX^n$), so is algebraic over F. □

Simple extensions

To continue our investigation of finite extensions, we introduce the following notation to describe how a field extension is formed. It enables us to view an extension as formed from a base field by introducing further elements.

Definition 2.7 Let the field K be an extension of the field F and α_1, α_2, ..., α_n be elements of K. We write

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

for the smallest subfield of K that contains both F and the elements α_1, α_2, ..., α_n.

It is straightforward to verify that the intersection of a collection of subfields of K is again a subfield (see Problem Sheet I, Question 2; one just needs to verify the conditions listed in Chapter 1 on page 8). Consequently, the "smallest subfield" containing F and the elements α_1, α_2, ..., α_n makes sense: it is the intersection of all the subfields of K that contain this collection of elements. It is possible to describe more explicitly the elements of the field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ in general, but we shall mainly concentrate on a special case.

Definition 2.8 We say that the field K is a *simple extension* of the field F if $K = F(\alpha)$ for some $\alpha \in K$. We then also say that K is obtained by *adjoining the element* α to F.

Simple extensions will be of great importance. In the case that α is algebraic over F, we shall have a precise description of elements in the simple extension $F(\alpha)$ and good knowledge of the degree $|F(\alpha) : F|$ (see Theorem 2.14 below). For a general extension $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ obtained by adjoining a finite collection of elements to a base field F, we can view this as a chain of simple extensions,

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

since at each stage $F(\alpha_1, \ldots, \alpha_i)$ is the simple extension obtained by adjoining the element α_i to the previous subfield $F(\alpha_1, \ldots, \alpha_{i-1})$.

Example 2.9 Let F be a field and X be an indeterminate. The field $F(X)$ of rational functions is a simple extension of F.

Indeed, in Proposition 1.27 we observed that F occurs as a subfield of $F(X)$, so $F(X)$ is indeed an extension of F. The elements of $F(X)$ has the form $f(X)/g(X)$ where $f(X)$ and $g(X)$

are polynomials with coefficients from F. Now if L is any subfield of $F(X)$ that contains the subfield F and the element X, then it first contains all polynomials in X, since L is closed under multiplication and addition. It is also closed under quotients and hence contains all quotients $f(X)/g(X)$ where $f(X)$ and $g(X)$ are polynomials. Therefore $L = F(X)$. We conclude that $F(X)$ indeed equals its smallest subfield containing F and the indeterminate X.

Thus the field $F(X)$ of rational functions is the simple extension of F obtained by adjoining the indeterminate X. In particular, the notation $F(X)$ as introduced in Definition 1.26 is consistent with that in Definition 2.8. Moreover, X is not an algebraic element over F: if b_0, b_1, $\ldots$, b_n are elements of F, not all of which are zero, then

$$b_0 + b_1X + b_2X^2 + \cdots + b_nX^n$$

is some non-zero polynomial $f(X)$ and so non-zero in the field $F(X)$ of rational functions. The term *transcendental* is used for an element that is not algebraic over the base field. Thus the indeterminate X as used in $F(X)$ is transcendental over the base field F. In fact, it turns out — though not so significant for this module — that if α is any transcendental element over the base field F, then the simple extension $F(\alpha)$ is isomorphic to the field $F(X)$ of rational functions.

Minimum polynomials

We shall be most interested in simple extensions $F(\alpha)$ where α is algebraic over the base field F. The most important definition we need in this context is the following:

Definition 2.10 Let F be a field and α be an element in some field extension of F such that α is algebraic over F. The *minimum polynomial* of α over F is the monic polynomial $f(X)$ of least degree in $F[X]$ such that $f(\alpha) = 0$.

Recall that a polynomial is *monic* if its leading term has coefficient 1. (The minimum polynomial is also sometimes called the "minimal polynomial" in some sources.)

One can apply very similar arguments to those used in linear algebra to establish quite directly that the minimum polynomial of an algebraic element exists and is unique. We shall, however, use a more ring-theoretic flavour of argument since that will also set up the technology we shall use to understand the structure of a simple extension.

Let α be an element in some extension of the field F that is algebraic over F. Define a map $\phi\colon F[X] \to F(\alpha)$ by evaluating a polynomial at α:

$$\phi\colon g(X) \mapsto g(\alpha).$$

We shall first observe that ϕ is a ring homomorphism. This is actually quite straightforward and depends upon only the ring axioms holding in the field $F(\alpha)$, but we shall check it explicitly.

Consider two polynomial $g(X), h(X) \in F[X]$, say

$$g(X) = \sum a_iX^i \qquad \text{and} \qquad h(X) = \sum b_iX^i$$

(where we understand that these are finite sums: all but finitely many a_i and b_i are zero). Then

$$\begin{aligned} g(X)\phi + h(X)\phi &= g(\alpha) + h(\alpha) \\ &= \sum a_i\alpha^i + \sum b_i\alpha^i \\ &= \sum (a_i + b_i)\alpha^i \\ &= (g + h)(\alpha) \\ &= \big(g(X) + h(X)\big)\phi \end{aligned}$$

and

$$\begin{aligned} g(X)\phi \cdot h(X)\phi &= g(\alpha)\, h(\alpha) \\ &= \Big(\sum a_i \alpha^i\Big)\Big(\sum b_i \alpha^i\Big) \\ &= \sum c_i \alpha^i, \end{aligned}$$

where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, by the distributive laws. Note $g(X)\, h(X) = \sum c_i X^i$, by definition, so

$$g(X)\phi \cdot h(X)\phi = \big(g(X)\, h(X)\big)\phi.$$

Hence ϕ is a ring homomorphism. The First Isomorphism Theorem (Theorem 1.6) tells us that

$$\frac{F[X]}{\ker \phi} \cong \operatorname{im} \phi$$

and $\operatorname{im} \phi$ is some subring of $F(\alpha)$. (The latter field contains F, α and is closed, in particular, under products and sums, so necessarily contains all $g(\alpha)$.) The assumption that α is algebraic ensures there exist some non-zero polynomials $g(X)$ satisfying $g(\alpha) = 0$; that is, $\ker \phi \neq \mathbf{0}$. The fact that $F[X]$ is a principal ideal domain tells us that

$$\ker \phi = \big(f(X)\big)$$

for some polynomial $f(X)$. Moreover, the proof of Proposition 1.16 tells us that $\deg f(X)$ is minimal amongst all non-zero polynomials $g(X)$ in $\ker \phi$; that is, amongst all non-zero polynomials $g(X)$ satisfying $g(\alpha) = 0$. Finally, note that the scalars are units in $F[X]$, so we may divide by the coefficient of the leading terms of $f(X)$, without changing the ideal generated by $f(X)$, and hence assume $f(X)$ is monic; that is, $f(X)$ is the *minimum polynomial* of α over F.

We have therefore established the first two parts of the following result that describes the main properties of the minimum polynomial. The others can be deduced quickly, as we now demonstrate, from what we have done.

Theorem 2.11 *Let F be a field and α be an element in some field extension of F such that α is algebraic over F. Then*

(i) *the minimum polynomial $f(X)$ of α over F exists;*

(ii) *the map $\phi\colon F[X] \to F(\alpha)$ given by $g(X) \mapsto g(\alpha)$ (that is, evaluating each polynomial at α) is a ring homomorphism with kernel $\ker \phi = \big(f(X)\big)$;*

(iii) *the minimum polynomial $f(X)$ of α over F is irreducible over F;*

(iv) *if $g(X) \in F[X]$, then $g(\alpha) = 0$ if and only if the minimum polynomial $f(X)$ of α over F divides $g(X)$;*

(v) *the minimum polynomial $f(X)$ of α over F is unique;*

(vi) *if $g(X)$ is any monic polynomial over F such that $g(\alpha) = 0$, then $g(X)$ is the minimum polynomial of α over F if and only if $g(X)$ is irreducible over F.*

Proof: (iii) Suppose $f(X)$ is reducible over F. Then $f(X) = g_1(X)\, g_2(X)$ for some (necessarily non-zero) polynomials $g_1(X)$ and $g_2(X)$ of smaller degree than $f(X)$. Then

$$0 = f(\alpha) = g_1(\alpha)\, g_2(\alpha).$$

Since $F(\alpha)$ is a field, either $g_1(\alpha) = 0$ or $g_2(\alpha) = 0$. However, this then contradicts the assumption that $f(X)$ has smallest degree among polynomials satisfied by α.

We conclude that $f(X)$ is indeed irreducible.

(iv) This follows from (ii):

$$\begin{aligned} g(\alpha) = 0 \qquad & \text{if and only if} \qquad g(X) \in \ker \phi = \big(f(X)\big) \\ & \text{if and only if} \qquad f(X) \text{ divides } g(X). \end{aligned}$$

(v) Suppose that $g(X)$ is a polynomial of the same smallest degree as $f(X)$ such that $g(\alpha) = 0$. Then, by (iv), $g(X)$ is a multiple of $f(X)$; say, $g(X) = f(X)\,h(X)$ for some polynomial $h(X)$. However, $\deg g(X) = \deg f(X)$, so we conclude $h(X)$ must be a constant polynomial. Thus $g(X) = c\,f(X)$ for some scalar $c \in F$. Consequently, if $f(X)$ and $g(X)$ are both *monic*, then $c = 1$. Hence the monic polynomial $f(X)$ of least degree such that $f(\alpha) = 0$ is unique.

(vi) This is essentially a corollary of (iii) and (iv).

$\Rightarrow$: If $g(X)$ is not irreducible, then it cannot be the minimum polynomial of α by part (iii).

$\Leftarrow$: Conversely suppose $g(X)$ is irreducible. By (iv), $g(X) = f(X)\,h(X)$ for some polynomial $h(X)$. Since $g(X)$ is irreducible and $f(X)$ is not constant, we conclude that $h(X)$ is constant. Hence $g(X) = c\,f(X)$ for some scalar c and the fact that both polynomials are monic forces $c = 1$. Therefore $g(X) = f(X)$ is the minimum polynomial of α over F. □

We now have enough of the basic theory of minimum polynomials that we can find them in some of the more straightforward examples. Other examples can be quite difficult, but some of the theory that we develop later in this section will be useful for the problem of determining the degree of a simple extension.

Example 2.12 *Show that the following complex numbers are algebraic over $\mathbb{Q}$ and determine their minimum polynomials over $\mathbb{Q}$:*

(i) $\sqrt{m}$*, where m is an integer such that $p \mid m$, for some prime p, but $p^2 \nmid m$;*

(ii) $\sqrt[3]{2}$*;* (iii) $\mathrm{e}^{2\pi i/3}$.

Solution: (i) First observe that $\sqrt{m}$ is a root of the polynomial $f(X) = X^2 - m$. Hence $\sqrt{m}$ is algebraic over $\mathbb{Q}$ as it satisfies some polynomial with rational coefficients. Moreover, $X^2 - m$ is irreducible (since our choice of m together with the property of the prime p ensures that Eisenstein's Criterion (Theorem 1.23) applies to $f(X)$. Hence $X^2 - m$ is the minimum polynomial of $\sqrt{m}$ over $\mathbb{Q}$.

Note that it also follows from this that $\sqrt{m} \notin \mathbb{Q}$, since otherwise we would be able to factorize $f(X)$ into two linear factors: $X^2 - m = (X - \sqrt{m})(X + \sqrt{m})$, contrary to the quadratic polynomial being irreducible over $\mathbb{Q}$.

(ii) The cube root $\sqrt[3]{2}$ is a root of the polynomial $g(X) = X^3 - 2$. Hence $\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$. Moreover, $X^3 - 2$ is irreducible by Eisenstein's Criterion. Therefore $X^3 - 2$ is the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

(iii) Let $\omega = \mathrm{e}^{2\pi i/3}$. Note that $\omega^3 = 1$, so ω is a root of $X^3 - 1$. Hence ω is indeed algebraic over $\mathbb{Q}$. However, $X^3 - 1$ is not irreducible: for a start, $1 \in \mathbb{Q}$ is also a root of that polynomial. Instead, observe

$$\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1),$$

so, since $\omega \neq 1$, we deduce $\omega^2 + \omega + 1 = 0$; that is, ω is also a root of the polynomial $h(X) = X^2 + X + 1$. The latter must be irreducible, since if it were not then it would be a product of two linear factors, one of which would have to be $X - \omega$, yet $\omega \notin \mathbb{Q}$ so this is not possible. Hence $X^2 + X + 1$ is the minimum polynomial of $\omega = \mathrm{e}^{2\pi i/3}$ over $\mathbb{Q}$. □

Comment: Note that the minimum polynomial of an algebraic element α depends upon the particular base field. For example, a special case of Example 2.12(i) is that $\sqrt{2}$ has minimum polynomial over $X^2 - 2$ over $\mathbb{Q}$, whereas its minimum polynomial over $\mathbb{R}$ is $X - \sqrt{2}$.

If we concentrate our efforts on simple extensions $F(\alpha)$ with α algebraic over the base field F, there are two questions that naturally arise and whose answers will enable us to make progress:

(i) Given an irreducible polynomial $f(X)$ over the field F, can we construct a simple extension $F(\alpha)$ such that the minimum polynomial of α over F is $f(X)$?

(ii) If α is algebraic over F, what is the structure of the simple extension $F(\alpha)$ and in what way is this determined by the minimum polynomial of α over F?

These questions essentially boil down to the existence of simple extensions and to then investigating their properties (and essentially establishing uniqueness as a consequence). Note that in answering the first question in the affirmative, as we do in the following theorem, we are showing that we can always *adjoin a root α of an irreducible polynomial to a field F* to construct some simple extension $F(\alpha)$.

Theorem 2.13 *Let F be a field and $f(X)$ be a monic irreducible polynomial over F. Then there exists a simple extension $F(\alpha)$ of F such that α is algebraic over F with minimum polynomial $f(X)$.*

The ideas discussed when establishing Theorem 2.11 give us a hint as to how to construct the simple extension. We shall construct it using the quotient ring $F[X]/\big(f(X)\big)$ of the polynomial ring $F[X]$ by the ideal generated by $f(X)$.

Proof: Let $I = \big(f(X)\big)$, the ideal of the polynomial ring $F[X]$ generated by $f(X)$, and let $K = F[X]/I$, the quotient ring of $F[X]$ by the ideal I. Certainly K is a commutative ring with a 1. Note that the multiplicative identity is $I + 1$. Since $f(X)$ is irreducible, non-zero constant polynomials are not divisible by $f(X)$ (irreducibles are not units) and so $1 \notin I$; that is, the multiplicative identity in K is non-zero.

Now if $g(X)$ is any polynomial such that $I + g(X)$ is non-zero (that is, $g(X) \notin I$), consider the greatest common divisor $h(X)$ of $f(X)$ and $g(X)$. Since $f(X)$ is irreducible, $h(X)$ is either a constant polynomial or a scalar multiple of $f(X)$. However, $f(X)$ does not divide $g(X)$, by assumption, so we conclude that $h(X)$ a constant. It follows therefore by the Euclidean Algorithm (Theorem 1.18) that there are polynomials $u(X), v(X) \in F[X]$ such that

$$1 = u(X)\, g(X) + v(X)\, f(X).$$

Hence, in the quotient ring,

$$I + 1 = \big(I + u(X)\big)\big(I + g(X)\big).$$

We conclude that every non-zero element of K has a multiplicative inverse and thus K is indeed a field.

Define the map $\iota\colon F \to K$ by

$$\iota\colon c \mapsto I + c.$$

The definition of addition and multiplication in the quotient ring K ensures that ι is a homomorphism. It is injective, since if $c\iota = d\iota$ (for some $c, d \in F$), then $c - d \in I$, which forces $c = d$ (as the only constant polynomial in $I = \big(f(X)\big)$ is 0). Hence $\operatorname{im}\iota = \{\, I + c \mid c \in F \,\}$ is a subring of K isomorphic to F; that is, K is a field extension of a subfield isomorphic to F. Identifying F with this isomorphic copy via ι, we view K as a field extension of F.

Finally, write $\alpha = I + X \in K$. Since every element of K has the form $I + g(X)$, where $g(X) \in F[X]$, we see, using the definition of addition and multiplication in K, that every element of K is expressible as a sum $b_0 + b_1\alpha + \cdots + b_n\alpha^n$ for some non-negative integer n and some $b_0, b_1, \ldots, b_n \in F$. Thus, the smallest subfield of K containing the subfield F and the element α is the whole field K; that is, $K = F(\alpha)$. Moreover, applying this to the polynomial $f(X)$, we calculate

$$f(\alpha) = f(I + X) = I + f(X) = I + 0;$$

that is, α satisfies the polynomial $f(X)$, so α is algebraic and, by Theorem 2.11(vi), the minimum polynomial of α is $f(X)$. □

Comments: There are two comments to make placing the above existence result for simple extensions in context.

(i) Although not stated in Chapter 1, the Correspondence Theorem for rings tells us that there is a one-one correspondence between ideals in the quotient ring $F[X]/I$, where $I = \big(f(X)\big)$, and ideals in the polynomial ring $F[X]$ that contain I. We have shown that when $f(X)$ is irreducible, the quotient $K = F[X]/I$ is a field; that is, it has only two ideals $\mathbf{0}$ and K itself. Therefore, via the correspondence, $I = \big(f(X)\big)$ is a maximal ideal of the polynomial ring: there are no ideals J satisfying $I < J < F[X]$. Consequently, we are observing above that $\big(f(X)\big)$ is a maximal ideal when $f(X)$ is irreducible. (The implication also reverses, as follows quite easily, but we omit the proof.)

(ii) Recall that the prime subfields are constructed from the ring of integers $\mathbb{Z}$. We observed, in Theorem 1.12, that the prime subfield of any field is either isomorphic to $\mathbb{Q}$ (which is the field of fractions of the Euclidean domain $\mathbb{Z}$) or to a finite field $\mathbb{F}_p$ (which occurs as the quotient $\mathbb{Z}/(p)$ by the ideal generated by some prime p, the primes being the irreducible elements in $\mathbb{Z}$). An analogous observation is being made here. If F is a field, the simple extensions of F are constructed from the Euclidean domain $F[X]$ as follows:

- If α is transcendental, then $F(\alpha)$ is isomorphic to the field of fractions, $F(X)$, of $F[X]$.
- If α is algebraic, then $F(\alpha)$ can be constructed as the quotient $F[X]/\big(f(X)\big)$ by an ideal generated by an irreducible polynomial $f(X)$.

Having established the existence of simple extensions with any specified minimum polynomial, we now establish the main result concerning the structure of such simple extensions $F(\alpha)$ with α algebraic. We determine the degree of the extension and establish a uniqueness result showing that $F(\alpha)$ is always constructed as in Theorem 2.13.

Theorem 2.14 *Let F be a field and α be an element in some extension of F. The simple extension $F(\alpha)$ over F is a finite extension if and only if α is algebraic over F. Moreover, in this case,*

$$|F(\alpha) : F| = \deg f(X),$$

the degree of the minimum polynomial $f(X)$ of α over F. Furthermore,

$$F(\alpha) \cong \frac{F[X]}{\big(f(X)\big)}$$

(as rings).

We shall use the various parts of Theorem 2.14, particularly the first two, throughout the module. The final conclusion of the theorem will be particularly significant as a technical tool in a number of proofs.

PROOF: If $F(\alpha)$ is a finite extension of F, then all its elements, in particular α, are algebraic over F by Lemma 2.6.

Conversely, suppose α is algebraic over F. Let $f(X)$ be the minimum polynomial of α over F and let n be the degree of $f(X)$. We make use of the technology developed when proving Theorem 2.11. Recall the ring homomorphism $\phi\colon F[X] \to F(\alpha)$ is defined by evaluating polynomials at α:

$$\phi\colon g(X) \mapsto g(\alpha).$$

The kernel of ϕ is $\ker\phi = \big(f(X)\big)$. Let $L = \operatorname{im}\phi$. This is a subring of $F(\alpha)$ and it contains all the elements of F (as the images of the constant polynomials under ϕ) and α (as the image of X). We shall show that L is a field.

If $g(\alpha) \neq 0$, then $g(X)$ is not a multiple of $f(X)$ by Theorem 2.11(iv). Since $f(X)$ is irreducible, the greatest common divisor of $f(X)$ and $g(X)$ must be a constant. (It cannot be $f(X)$ as $f(X)$ does not divide $g(X)$.) Hence by Theorem 1.18 there exist polynomials $u(X), v(X) \in F[X]$ such that

$$1 = u(X)\, g(X) + v(X)\, f(X).$$

We now substitute α to conclude

$$1 = u(\alpha)\, g(\alpha).$$

Hence $g(\alpha)$ has a multiplicative inverse in L and we conclude that L is indeed a field. We then conclude $F(\alpha) = L$ from the definition of $F(\alpha)$ as the smallest field containing F and α. The last part of the theorem is now established

$$F(\alpha) = \operatorname{im}\phi \cong \frac{F[X]}{\ker\phi} = \frac{F[X]}{(f(X))}$$

by the First Isomorphism Theorem.

It remains to establish $F(\alpha)$ is a finite extension of F and to determine the degree of the extension. If $b \in F(\alpha)$, then $b = g(\alpha)$ for some polynomial $g(X) \in F[X]$. Since $F[X]$ is a Euclidean domain, we can write

$$g(X) = q(X)\, f(X) + r(X)$$

where either $r(X) = 0$ or $\deg r(X) < \deg f(X) = n$. Then

$$b = g(\alpha) = q(\alpha)\, f(\alpha) + r(\alpha) = r(\alpha).$$

Hence every element of $F(\alpha)$ is the image of a polynomial of degree at most $n-1$ under ϕ and we conclude that $F(\alpha)$ is spanned by the set $\mathscr{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ as a vector space over F. In fact, $\mathscr{B}$ is linearly independent, for if we had a linear dependence relation

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$$

then $g(X) = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1}$ would be a polynomial of degree smaller than $f(X)$ satisfying $g(\alpha) = 0$. The definition of the minimum polynomial forces

$$b_0 = b_1 = \cdots = b_{n-1} = 0.$$

Hence $\mathscr{B}$ is a basis for $F(\alpha)$ over F. We conclude that $F(\alpha)$ is indeed a finite extension of F and that the degree is

$$|F(\alpha) : F| = |\mathscr{B}| = n = \deg f(X).$$

This completes the proof of the theorem. □

We record the following observation that was made towards the end of the proof:

Corollary 2.15 *Suppose that α is algebraic over F with minimum polynomial of degree n. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for the simple extension $F(\alpha)$ over F.* □

It will be important to interpret the isomorphism appearing in the proof of Theorem 2.14 in various proofs that follow. When observing that $F[X]/\big(f(X)\big)$ is isomorphic to the simple extension $F(\alpha)$, we applied the First Isomorphism Theorem. Recall that the specific isomorphism $\bar{\phi}$ establishing the two rings are isomorphic is given by

$$\bar{\phi}\colon (\ker\phi) + g(X) \mapsto g(X)\phi = g(\alpha)$$

for any $g(X) \in F[X]$. (See the sketch proof of Theorem 1.6 above.) In particular, the effect on specific elements in the quotient ring are as follows:

$$\bar{\phi}\colon \big(f(X)\big) + a \mapsto a$$

for any element a in the base field F, and

$$\bar{\phi}\colon \big(f(X)\big) + X \mapsto \alpha.$$

We shall now use the Theorem, and its corollary, to give a description of a variety of fields that we can construct. We shall make use of the minimum polynomials calculated in Example 2.12.

Example 2.16 (i) The field $\mathbb{Q}(\sqrt{2})$ is the extension of $\mathbb{Q}$ obtained by adjoining $\sqrt{2}$. We know from Example 2.12 that the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $f(X) = X^2 - 2$. Since this has degree 2, we conclude

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2.$$

Moreover, as noted in Corollary 2.15, $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Thus every element of $\mathbb{Q}(\sqrt{2})$ can be expressed *uniquely* in the form

$$a + b\sqrt{2}$$

where $a, b \in \mathbb{Q}$. The addition, subtraction, multiplication and division can now be explicitly determined in terms of this form. Addition can be performed simply by adding the coefficients in front of each basis element (after all, the addition is part of the vector space structure). To multiply use the distributive laws:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

for any $a, b, c, d \in \mathbb{Q}$. Division can be obtained by a process similar to "complex conjugation":

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\end{aligned}$$

for any $a, b \in \mathbb{Q}$. We know that the denominator is non-zero if a and b are not both 0, since $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Note here that if $a, b \neq 0$, then $a^2 - 2b^2 \neq 0$ since otherwise $\sqrt{2} = |a/b|$, which would be a contradiction as $\sqrt{2} \notin \mathbb{Q}$.

(ii) The previous example has much in common to the behaviour of the complex numbers. Indeed, note that $\mathbb{C} = \mathbb{R}(i)$, the field obtained by adjoining the imaginary number i to the real numbers and the minimum polynomial of i over $\mathbb{R}$ is $X^2 + 1$. This is consistent, via the Theorem, with the fact that $|\mathbb{C} : \mathbb{R}| = 2$ (the degree of the minimum polynomial) and $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

(iii) Similarly, we know that the minimum polynomial of $\alpha = \sqrt[3]{2}$ is $X^3 - 2$, which has degree 3. Hence

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$$

and $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$. Consequently, elements of $\mathbb{Q}(\alpha)$ can be uniquely expressed in the form

$$a + b\alpha + c\alpha^2,$$

where $a, b, c \in \mathbb{Q}$, and multiplication of two such elements can be achieved by exploiting the fact that $\alpha^3 = 2$.

(iv) Finally, turning to the final part of Example 2.12, recall that the minimum polynomial of $\omega = \mathrm{e}^{2\pi i/3}$ over $\mathbb{Q}$ is $X^2 + X + 1$. Hence

$$|\mathbb{Q}(\omega) : \mathbb{Q}| = 2,$$

$\{1, \omega\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, and consequently every element of $\mathbb{Q}(\omega)$ is uniquely expressed in the form

$$a + b\omega$$

where $a, b \in \mathbb{Q}$. We multiply two such expression by exploiting the fact that $\omega^2 = -(\omega+1)$. Thus

$$\begin{aligned}(a + b\omega)(c + d\omega) &= ac + (ad + bc)\omega + bd\omega^2 \\ &= (ac - bd) + (ad + bc - bd)\omega.\end{aligned}$$

The theory we have developed so far enables us to give a good description of finite extensions of a base field.

Theorem 2.17 *Let K be an extension of a field F. Then K is a finite extension of F if and only if $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some finite collection α_1, α_2, …, α_n of elements of K each of which is algebraic over F.*

Proof: First suppose that K is a finite extension of F. Then K has some finite basis, say $\mathscr{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, over F. Necessarily then $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ since the smallest field containing F and the elements α_i necessarily contains all *F-linear combinations* of the α_i (that is, all expression $b_1\alpha_1 + \cdots + b_n\alpha_n$ where the b_i are selected from F). Lemma 2.6 tells us that every element of K is algebraic over F, so in particular each of the α_i is algebraic over F.

Conversely, suppose $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where each α_i is algebraic over the base field F. We shall show, by induction on n, that $|K : F|$ is finite. The base case is $n = 0$, when $K = F$ and then $|K : F| = 1$ since $\{1\}$ is a basis for F as a vector space over itself F.

Assume then that $n \geqslant 1$ and, by induction, that the subfield $L = F(\alpha_1, \ldots, \alpha_{n-1})$ is a finite extension of F. Note that $L(\alpha_n) = K$, since the smallest subfield of K containing L and the element α_n necessarily contains F and all the α_i. Now the minimum polynomial of α_n over F has coefficients in F, so these coefficients also belong L. Hence α_n is algebraic over L and Theorem 2.14 tells us that $|L(\alpha_n) : L|$ is finite. Therefore, by the Tower Law (Theorem 2.4),

$$|K : F| = |L(\alpha_n) : F| = |L(\alpha_n) : L| \cdot |L : F|$$

is finite. This completes the induction and establishes the theorem. □

Example 2.18 *Determine the degree of* $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *over* $\mathbb{Q}$.

SOLUTION: We shall first make use of the Tower Law (Theorem 2.4) in the form

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}):\mathbb{Q}|.$$

Now $\sqrt{2}$ has minimum polynomial X^2-2 over $\mathbb{Q}$ (note this polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion), so

$$|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2.$$

The element $\sqrt{3}$ is algebraic over $\mathbb{Q}(\sqrt{2})$ since it is a root of the polynomial X^2-3. Hence

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| \leqslant 2.$$

(Note at this stage, we do not know for certain that the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is X^2-3. This polynomial is irreducible over $\mathbb{Q}$, but we need more work to determine whether or not it is irreducible over $\mathbb{Q}(\sqrt{2})$.) If it were the case that $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| = 1$, then these two fields would be equal and $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Thus we would be able to write

$$\sqrt{3} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Q}$ (since Corollary 2.15 tells us that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$). Note that both a and b must be non-zero, as if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$ while if $a = 0$ then $\sqrt{6} = 2b \in \mathbb{Q}$, both of which are false as $\sqrt{3}$ and $\sqrt{6}$ are irrational. Upon squaring this equation, we conclude that

$$3 = a^2 + 2ab\sqrt{2} + 2b^2;$$

that is,

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}.$$

This is again a contradiction. We conclude that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and hence $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})| = 2$. We conclude, therefore, from the Tower Law, that

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = 4.$$

Note also that the Tower Law tells us that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ (see the comment after the proof of Theorem 2.4).

Now apply the Tower Law to the inclusions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ (note that $\sqrt{2}+\sqrt{3}$ is an element of the larger field, so these inclusions hold):

$$4 = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})| \cdot |\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|,$$

so $|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|$ divides 4.

Note $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$ because $\{1, \sqrt{2}, \sqrt{3}\}$ is linearly independent over $\mathbb{Q}$. Hence $|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}| = 2$ or 4. Suppose the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{3}$ is quadratic, say $X^2 + bX + c$ for some $b, c \in \mathbb{Q}$. Thus

$$\begin{aligned} 0 = \alpha^2 + b\alpha + c &= (\sqrt{2}+\sqrt{3})^2 + b(\sqrt{2}+\sqrt{3}) + c \\ &= 2 + 2\sqrt{6} + 3 + b\sqrt{2} + b\sqrt{3} + c \\ &= (5+c) + b\sqrt{2} + b\sqrt{3} + 2\sqrt{6}. \end{aligned}$$

This contradicts the fact that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent. Hence α is not a root of a quadratic polynomial over $\mathbb{Q}$. We conclude therefore

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

□

Example 2.19 Let us write $\mathbb{A}$ for the set of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. We call $\mathbb{A}$ the *field of algebraic numbers* over $\mathbb{Q}$. In this example, we show that $\mathbb{A}$ is indeed a subfield of $\mathbb{C}$ and determine the degree $|\mathbb{A} : \mathbb{Q}|$.

Certainly $\mathbb{A}$ is non-empty since it contains $\mathbb{Q}$ (these are the roots of linear equations $X - a$ for $a \in \mathbb{Q}$) together with lots of elements considered already, e.g., $\sqrt{2}$, $\sqrt{3}$, i, etc. Let $\alpha, \beta \in \mathbb{A}$. Note that

$$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = |\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}|$$

and here $|\mathbb{Q}(\alpha) : \mathbb{Q}|$ is finite because α is algebraic over $\mathbb{Q}$ and $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)|$ is finite because β is algebraic over $\mathbb{Q}$, so also algebraic over $\mathbb{Q}(\alpha)$. Hence $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}|$ is finite, so every element of $\mathbb{Q}(\alpha, \beta)$ is algebraic over $\mathbb{Q}$ by Lemma 2.6. Now $\mathbb{Q}(\alpha, \beta)$ is a field, so it contains $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and, provided $\alpha \neq 0$, also $1/\alpha$. Therefore the elements $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and $1/\alpha$ are algebraic over $\mathbb{Q}$, so belong to $\mathbb{A}$. This establishes that $\mathbb{A}$ is a subfield of $\mathbb{C}$.

Finally, note also that $\sqrt[n]{2} \in \mathbb{A}$ and this has minimum polynomial $X^n - 2$ over $\mathbb{Q}$ (the latter polynomial being irreducible by Eisenstein's Criterion). Hence $|\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}| = n$ and applying the Tower Law to the inclusion $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{A}$, we conclude that $|\mathbb{A} : \mathbb{Q}| \geqslant n$ for all positive integers n. Therefore $\mathbb{A}$ is an infinite degree extension of $\mathbb{Q}$ consisting entirely of algebraic elements. (As a consequence, this tells us that the converse of Lemma 2.6 is false: there are algebraic extensions that are not finite extensions.)

Chapter 3

Splitting Fields and Normal Extensions

The purpose of this chapter is to show how we can use the methods of Chapter 2 to construct, given a polynomial $f(X)$ over some base field, an extension in which the polynomial $f(X)$ can be factorized as a product of linear (that is, degree 1) factors.

Splitting fields

Let F be a field and consider a polynomial $f(X)$ over the field F. Suppose that there is an extension L of F such that, when $f(X)$ is viewed as a polynomial over L, we can factorize it as a product of linear factors:

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n).$$

We shall then say that $f(X)$ *splits* over L. Necessarily, in such a situation, then the roots α_1, α_2, …, α_n of $f(X)$ are elements of the field L. Note then that $f(X)$ might split in some such extension L, because it contains all the roots of $f(X)$, but not in some particular subfield of L because one or more of those roots do not belong to that subfield.

In this context, we make the following definition:

Definition 3.1 Let $f(X)$ be a polynomial over some field F. We say that a field K is a *splitting field* for $f(X)$ over F if K is an extension of F satisfying the following properties:

(i) $f(X)$ splits into a product of linear factors over K, and

(ii) if $F \subseteq L \subseteq K$ and $f(X)$ splits over L, then $L = K$.

Thus, a splitting field for a polynomial $f(X)$ over a field F is an extension K of F in which $f(X)$ splits over K but such that $f(X)$ does not split over any proper subfield of K; that is, K is a minimal field over which $f(X)$ splits.

The form of a splitting field is quite naturally expressed using the roots of our polynomial:

Lemma 3.2 *Let $f(X)$ be a polynomial over a field F and suppose there is some extension L of F such that $f(X)$ splits over L with roots α_1, α_2, …, α_n. Then*

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

is a splitting field for $f(X)$ over F.

In particular, in the case of a polynomial $f(X)$ over $F = \mathbb{Q}$, we know that $L = \mathbb{C}$ is a suitable extension to use in the lemma since we know from the Fundamental Theorem of Algebra (proved in *Complex Analysis*) that every polynomial over $\mathbb{Q}$ has roots in $\mathbb{C}$ and hence splits over $\mathbb{C}$. We then obtain a splitting field for $f(X)$ over $\mathbb{Q}$ as $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where α_1, α_2, $\ldots$, α_n are the roots of $f(X)$ in $\mathbb{C}$.

We now prove the lemma:

PROOF: By assumption, over the field L, we can factorize $f(X)$ as

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n).$$

where $c \in F$ (since it is a coefficient of the original polynomial $f(X)$). Write

$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

the smallest subfield of L containing α_1, α_2, $\ldots$, α_n. Certainly $f(X)$ splits over the field K.

Suppose $F \subseteq K' \subseteq K$ such that $f(X)$ splits over K'. This means that we have a decomposition of $f(X)$ as a product of linear factors with coefficients from K', say

$$f(X) = c(X - \beta_1)(X - \beta_2)\ldots(X - \beta_n)$$

where $\beta_1, \beta_2, \ldots, \beta_n \in K'$. As $K' \subseteq K$, we now have two factorizations in $K[X]$ for $f(X)$ as a product of linear factors. Since the polynomial ring $K[X]$ is a unique factorization domain, these factorizations into irreducible polynomials must be the same; that is, the α_i and the β_i are the same. We conclude that $\alpha_1, \alpha_2, \ldots, \alpha_n \in K'$ and the definition of $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ as the smallest field containing F and the α_i, then forces $K' = K$.

This establishes that K is indeed a splitting field for F. □

We now apply the method of Lemma 3.2 to find some splitting fields of relatively straightforward polynomials.

Example 3.3 Find splitting fields for the following polynomials over $\mathbb{Q}$:

(i) $f(X) = X^2 - 2$;

(ii) $g(X) = X^3 - 1$;

(iii) $h(X) = X^3 - 2$.

SOLUTION: (i) The factorization of $f(X)$ over $\mathbb{C}$ is

$$f(X) = (X - \sqrt{2})(X + \sqrt{2}).$$

Hence a splitting field for $f(X)$ over $\mathbb{Q}$ is, by our argument above,

$$K = \mathbb{Q}(\sqrt{2}).$$

(Note that $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, as the latter is a field, so closed under subtraction.)

(ii) The factorization of $g(X)$ over $\mathbb{Q}$ is

$$g(X) = (X - 1)(X^2 + X + 1).$$

We can further factorize it over $\mathbb{Q}$ as

$$g(X) = (X - 1)(X - \omega)(X - \omega^2)$$

where $\omega = e^{2\pi i/3}$ (and note $\omega^2 = e^{4\pi i/3}$ is the other cube root of 1 in $\mathbb{C}$). Hence a splitting field for $g(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\omega).$$

(iii) The factorization of $h(X)$ over $\mathbb{C}$ is

$$h(X) = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2})$$

where $\omega = e^{2\pi i/3}$. Our method tells us a splitting field for $h(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}).$$

However, note that ω belongs to this field K, since K is closed under division, and we now observe that this field K equals

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

The latter description would be helpful if we wished to use the methods of Chapter 2 to determine the degree of K over $\mathbb{Q}$ and even to find a basis for this splitting field over the base field $\mathbb{Q}$. □

Existence of splitting fields

Using the method described above depends upon us being able to find some extension L in which $f(X)$ splits and then finding a splitting field inside it. Over the rational numbers $\mathbb{Q}$, this is no problem since we can use the complex numbers $\mathbb{C}$, but even then it gives little restriction upon the degree of the splitting extension. In fact, using the theory developed in Chapter 2 we can construct a splitting field for a polynomial $f(X)$ irrespective of what the base field is and to also obtain decent bounds on the degree of the extension in terms of the polynomial, as we shall now show.

Theorem 3.4 (Existence of Splitting Fields) *Let $f(X)$ be a polynomial of degree n over a field F. Then there is a splitting field K for $f(X)$ over F with degree $|K : F|$ dividing $n!$.*

Proof: We proceed by induction on n. If $n = 1$, then $f(X)$ is already a linear polynomial, so F itself is a splitting field for $f(X)$ over F and, of course, $|F : F| = 1$.

We now assume that the claimed result holds for all polynomials of degree less than n. We consider two cases:

Case 1: $f(X)$ is irreducible over F.

Let us apply Theorem 2.13 to adjoin a root α of $f(X)$ to F. Then $|F(\alpha) : F| = n$, by Theorem 2.14 and we can write

$$f(X) = (X - \alpha)\, g(X)$$

for some polynomial $g(X)$ of degree $n-1$ with coefficients in $F(\alpha)$. Now by induction, $g(X)$ has a splitting field K over $F(\alpha)$ and the degree $|K : F(\alpha)|$ divides $(n-1)!$. Note that $K = F(\alpha, \alpha_2, \ldots, \alpha_n)$ where $\alpha_2, \ldots, \alpha_n$ are the roots of $g(X)$; that is, K is obtained by adjoining the roots of $f(X)$ to F. Hence, using Lemma 3.2, K is a splitting field for $f(X)$ over F and, by the Tower Law (Theorem 2.4),

$$|K : F| = |K : F(\alpha)| \cdot |F(\alpha) : F| = |K : F(\alpha)| \cdot n,$$

which divides $n!$.

Case 2: $f(X)$ is reducible over F.

We can then write $f(X) = g(X)\,h(X)$ where $g(X)$ and $h(X)$ are polynomials over F of degree k and $n-k$, respectively (where $1 \leqslant k \leqslant n-1$). By induction, there is a splitting field

$$L = F(\beta_1, \ldots, \beta_k)$$

for $g(X)$ over F where $|L : F|$ divides $k!$ and $\beta_1, \ldots, \beta_k$ are the roots of $g(X)$ in L. Equally, there is a splitting field

$$K = L(\gamma_{k+1}, \ldots, \gamma_n)$$

for $h(X)$ over L where $|K : L|$ divides $(n-k)!$ and $\gamma_{k+1}, \ldots, \gamma_n$ are the roots of $h(X)$ in K.

Now in the field K, $f(X)$ splits as a product of linear factors with roots β_1, …, β_k, γ_{k+1}, …, γ_n. We conclude that

$$K = F(\beta_1, \ldots, \beta_k, \gamma_{k+1}, \ldots, \gamma_n)$$

is a splitting field for $f(X)$ over F and the degree

$$|K : F| = |K : L| \cdot |L : F|$$

divides $k!\,(n-k)!$, and hence divides $n!$ (since the binomial coefficient $\binom{n}{k}$ is an integer). □

Uniqueness of splitting fields and related isomorphisms

We now know that splitting fields always exist, have some constraint about their degree over the base field, and have a method to construct them in a nice case (for example, splitting fields over any subfield of $\mathbb{C}$). We now turn to establishing that splitting fields are unique and in doing so will also develop some key tools for the main theorem of the course.

We begin with the following first step.

Lemma 3.5 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be an irreducible polynomial in $F_1[X]$ and write $f^\phi(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let α be a root of $f(X)$ and β be a root of $f^\phi(X)$ in some extensions of F_1 and F_2, respectively. Then there exists an isomorphism $\psi\colon F_1(\alpha) \to F_2(\beta)$ which extends ϕ and maps α to β.*

To say that ψ *extends* ϕ means that $a\psi = a\phi$ for all $a \in F_1$; that is, the restriction $\psi|_{F_1}$ of ψ to F_1 is the isomorphism ϕ we started with.

Proof: First note that the isomorphism $\phi\colon F_1 \to F_2$ induces an isomorphism $\phi^*\colon F_1[X] \to F_2[X]$ between the corresponding polynomial rings, namely

$$\phi^*\colon a_0 + a_1X + \cdots + a_mX^m \mapsto (a_0\phi) + (a_1\phi)X + \cdots + (a_m\phi)X^m.$$

So, in this notation, $f^\phi(X) = f(X)\phi^*$. This map ϕ^* is indeed an isomorphism of rings because addition and multiplication in polynomial rings is determined by operations on the coefficients within the polynomials and ϕ preserves these operations. Since $f(X)$ is irreducible in $F_1[X]$, we conclude that $f^\phi(X) = f(X)\phi^*$ is irreducible in $F_2[X]$. The isomorphism ϕ^* maps the ideal $\big(f(X)\big)$ to the ideal $\big(f^\phi(X)\big)$ and hence we have an induced isomorphism

$$\bar{\phi}\colon \frac{F_1[X]}{\big(f(X)\big)} \to \frac{F_2[X]}{\big(f^\phi(X)\big)}$$

given by

$$\bar{\phi}\colon \big(f(X)\big) + g(X) \mapsto \big(f^\phi(X)\big) + g(X)\phi^*.$$

In particular,

$$\Big(\big(f(X)\big)+X\Big)\bar{\phi}=\big(f^{\phi}(X)\big)+X \qquad \text{and} \qquad \Big(\big(f(X)\big)+a\Big)\bar{\phi}=\big(f^{\phi}(X)\big)+a\phi$$

for $a \in F_1$.

We link these quotients to the field extensions $F_1(\alpha)$ and $F_2(\beta)$. Recall from Theorem 2.14 that these field extensions are isomorphic to the quotient rings appearing above. To be specific, there are isomorphisms

$$\psi_1 \colon \frac{F_1[X]}{\big(f(X)\big)} \to F_1(\alpha)$$

$$\psi_2 \colon \frac{F_2[X]}{\big(f^{\phi}(X)\big)} \to F_2(\beta)$$

and these satisfy

$$\Big(\big(f(X)\big)+a\Big)\psi_1 = a \qquad \Big(\big(f(X)\big)+X\Big)\psi_1 = \alpha$$

$$\Big(\big(f^{\phi}(X)\big)+b\Big)\psi_2 = b \qquad \Big(\big(f^{\phi}(X)\big)+X\Big)\psi_2 = \beta$$

for any $a \in F_1$ and $b \in F_2$. We now compose these isomorphisms: $\psi_1^{-1}\bar{\phi}\psi_2$ is an isomorphism from $F_1(\alpha)$ to $F_2(\beta)$ satisfying

$$a\,\psi_1^{-1}\bar{\phi}\psi_2 = \Big(\big(f(X)\big)+a\Big)\bar{\phi}\psi_2 = \Big(\big(f^{\phi}(X)\big)+a\phi\Big)\psi_2 = a\phi,$$

for all $a \in F_1$, and

$$\alpha\,\psi_1^{-1}\bar{\phi}\psi_2 = \Big(\big(f(X)\big)+X\Big)\bar{\phi}\psi_2 = \Big(\big(f^{\phi}(X)\big)+X\Big)\psi_2 = \beta.$$

This establishes the result. □

We use this as the base step in an induction to establish the uniqueness of splitting fields. The most important theorem in this chapter is the following:

Theorem 3.6 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be any polynomial in $F_1[X]$ and write $f^{\phi}(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let K_1 be a splitting field for $f(X)$ over F_1 and K_2 be a splitting field for $f^{\phi}(X)$ over F_2. Then there exists an isomorphism $\theta\colon K_1 \to K_2$ which extends ϕ.*

To establish uniqueness of splitting fields, we take $F_1 = F_2$ and ϕ to be the identity map in the above theorem. This tells us that two splitting fields for a polynomial over F_1 are isomorphic via an isomorphism that restricts to the identity on F_1.

We accordingly make the following definition:

Definition 3.7 Let F be a field and let K_1 and K_2 be extensions of F. An *F-isomorphism* from K_1 to K_2 is a field isomorphism $\psi\colon K_1 \to K_2$ such that

$$a\psi = a \qquad \text{for all } a \in F.$$

We then say K_1 and K_2 are *F-isomorphic*.

Thus taking $F_1 = F_2 = F$ in Theorem 3.6 and ϕ to be the identity, we conclude:

Corollary 3.8 (Uniqueness of Splitting Fields) *Let $f(X)$ be a polynomial over a field F. Any two splitting fields for $f(X)$ over F are F-isomorphic.* □

It remains then to establish the above theorem.

PROOF OF THEOREM 3.6: Let $n = \deg f(X)$ and proceed by induction on n. If $n = 1$, then $K_1 = F_1$ and $K_2 = F_2$, so we may take $\theta = \phi$.

Now we assume the result holds for all polynomials of degree smaller than n. We shall consider two cases:

Case 1: $f(X)$ is irreducible over F_1.

Let α be any root of $f(X)$ in the field K_1 and β be any root of $f^\phi(X)$ in K_2. (We know these exist because K_1 and K_2 are splitting fields for $f(X)$ and $f^\phi(X)$ over F_1 and F_2 respectively.) By Lemma 3.5, there is an isomorphism $\psi\colon F_1(\alpha) \to F_2(\beta)$ such that $\psi|_{F_1} = \phi$ and $\alpha\psi = \beta$. Now

$$f(X) = (X - \alpha)\, g(X),$$

for some polynomial $g(X)$ of degree $n-1$ with coefficients from $F_1(\alpha)$, and, applying ψ to the coefficients, we observe

$$f^\phi(X) = (X - \beta)\, g^\psi(X)$$

(where $g^\psi(X)$ is the polynomial with coefficients in $F_2(\beta)$ obtained by applying ψ to the coefficients of $g(X)$). Now K_1 is a splitting field for $g(X)$ over $F_1(\alpha)$ (since K_1 is obtained by adjoining α and all the roots of $g(X)$ to F_1) and K_2 is a splitting field for $g^\psi(X)$ over $F_2(\beta)$. Hence, by induction, there is an isomorphism $\theta\colon K_1 \to K_2$ such that $\theta|_{F_1(\alpha)} = \psi$. In particular,

$$\theta|_{F_1} = \psi|_{F_1} = \phi,$$

as required.

Case 2: $f(X)$ is reducible over F_1.

Let us write $f(X) = g(X)\, h(X)$ in $F_1[X]$ where $g(X)$ and $h(X)$ are non-constant polynomials. Applying ϕ to the coefficients, we obtain

$$f^\phi(X) = g^\phi(X)\, h^\phi(X)$$

in $F_2[X]$ (using the notation introduced in the statement of the Theorem). Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be the roots of $g(X)$ in K_1 and $\beta_1, \beta_2, \ldots, \beta_k$ be the roots of $g^\phi(X)$ in K_2. Put

$$L_1 = F_1(\alpha_1, \alpha_2, \ldots, \alpha_k) \qquad \text{and} \qquad L_2 = F_2(\beta_1, \beta_2, \ldots, \beta_k).$$

Then L_1 is a splitting field for $g(X)$ over F_1 and L_2 is a splitting field for $g^\phi(X)$ over F_2. By induction, there is an isomorphism $\psi\colon L_1 \to L_2$ such that $\psi|_{F_1} = \phi$.

Finally, note that K_1 is obtained from F_1 by adjoining all the roots of $f(X)$, so it is obtained from L_1 by adjoining all the roots of $h(X)$; that is, K_1 is a splitting field for $h(X)$ over L_1. Similarly K_2 is a splitting field for $h^\phi(X) = h^\psi(X)$ over L_2. Hence, by induction, there is an isomorphism $\theta\colon K_1 \to K_2$ such that $\theta|_{L_1} = \psi$. In particular,

$$\theta|_{F_1} = \psi|_{F_1} = \phi.$$

This completes the inductive step and establishes the theorem. □

Before turning to the final topic of this chapter, we shall give an example illustrating how the results established so far will appear within the later theory.

Definition 3.9 (i) An *automorphism* of a field F is an isomorphism from F to itself.

(ii) Let K be an extension of the field F. An *F-automorphism* of K is an F-isomorphism from K to itself.

Thus an F-automorphism of the extension K is an isomorphism $\phi\colon K \to K$ such that $a\phi = a$ for all a in the base field F.

Example 3.10 *Determine all $\mathbb{Q}$-automorphisms of the simple extension $\mathbb{Q}(i)$.*

To fit this example in context, note that the roots of the polynomial $X^2 + 1$ in $\mathbb{C}$ are $\pm i$. Hence $\mathbb{Q}(i)$ is the splitting field for $X^2 + 1$ over $\mathbb{Q}$. (In view of the uniqueness in Corollary 3.8, we are also now justified in referring to "the splitting field" rather than "a splitting field" of a polynomial.)

SOLUTION: As noted, i is a root of the polynomial $X^2 + 1$. The latter polynomial is irreducible over $\mathbb{Q}$, so it is the minimum polynomial of i over $\mathbb{Q}$, the degree $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ and $\{1, i\}$ is a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$. Let ψ be a $\mathbb{Q}$-automorphism of $\mathbb{Q}(i)$. Then

$$(a + bi)\psi = a + b(i\psi),$$

for $a, b \in \mathbb{Q}$, and we conclude that ψ is determined by its effect on i. Now $i^2 + 1 = 0$, so applying the automorphism ψ we see that

$$(i\psi)^2 + 1 = 0.$$

Hence ψ must map i to a root of $X^2 + 1$; that is, $i\psi = \pm i$. Thus, there are at most two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$.

Conversely, if β is any root of $X^2 + 1$, applying Lemma 3.5 (taking $F_1 = F_2 = \mathbb{Q}$ and ϕ to be the identity map), there is a $\mathbb{Q}$-isomorphism $\mathbb{Q}(i) \to \mathbb{Q}(\beta)$ which maps i to β. However, $\beta = \pm i$, so $\mathbb{Q}(\beta) = \mathbb{Q}(i)$ and ψ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(i)$.

We conclude that there are precisely two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$. □

Normal Extensions

Definition 3.11 An extension K of a field F is a *normal extension* if every irreducible polynomial over F that has at least one zero in K splits over K.

Note that saying K is a normal extension of F only tells us about irreducible polynomials over F that have a root in the larger field K. It tells us nothing about reducible polynomials nor does it guarantee that a particular polynomial has any roots in the larger field K.

Example 3.12 (i) The field $\mathbb{C}$ of complex numbers is a normal extension of $\mathbb{R}$, since every polynomial over $\mathbb{R}$ splits over $\mathbb{C}$.

(ii) Consider the simple extension $\mathbb{Q}(\sqrt[3]{2})$ obtained by adjoining the cube root of 2 to $\mathbb{Q}$. This is *not* a normal extension of $\mathbb{Q}$ since the irreducible polynomial $X^3 - 2$ (over $\mathbb{Q}$) has a root in $\mathbb{Q}(\sqrt[3]{2})$ but does not split over this field as the other two roots are complex numbers.

It would seem on the face of it rather complicated to show that an extension is normal. The definition asks us to show check that every irreducible polynomial with a root in the bigger field actually splits. The following theorem characterizes finite normal extensions (and hence gives essentially all examples) as the splitting fields of polynomials.

Theorem 3.13 *A finite extension K of a field F is a normal extensions if and only if K is the splitting field of some polynomial over F.*

So we know that an extension is normal if we can recognize it as a splitting field of some polynomial (which does not need itself to be an irreducible polynomial). On the other hand, to show an extension is not normal, we should find an irreducible polynomial over the base field which has a root but does not split in the larger field and then by definition the extension is not normal.

PROOF: Suppose K is a finite normal extension of F. By Theorem 2.17, we know that K is an algebraic extension of F of the form

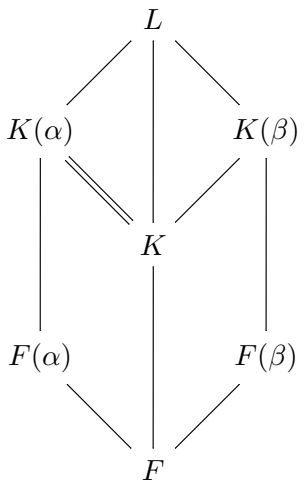
$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$. Let $f_i(X)$ be the minimum polynomial of α_i over F and let

$$g(X) = f_1(X)\, f_2(X) \ldots f_m(X) \in F[X].$$

Now $f_i(X)$ is an irreducible polynomial over F and has a root α_i in K, Hence, by normality, $f_i(X)$ splits over K. It follows that $g(X)$ splits over K. On the other hand, K is constructed from F by adjoining (some of) the roots of $g(X)$, so K is the splitting field of $g(X)$ over F.

Conversely, suppose K is the splitting field of some polynomial $g(X)$ over F. Let $f(X)$ be any irreducible polynomial over F and suppose that $f(X)$ has some root α in K. We must show that $f(X)$ splits over K. First let L be the splitting field for $f(X)$ over K. (Our goal is essentially to show, in fact, that $L = K$.) Let β be any root of $f(X)$ in L and consider the following diagram (where an upward sloping line indicates inclusion):



We shall show that $K(\beta) = K$ to conclude $\beta \in K$. It will then follow that all the roots of $f(X)$ in L actually belong to K.

By the Tower Law (Theorem 2.4):

$$\begin{aligned} |K(\beta) : K| \cdot |K : F| &= |K(\beta) : F| = |K(\beta) : F(\beta)| \cdot |F(\beta) : F| \\ |K(\alpha) : K| \cdot |K : F| &= |K(\alpha) : F| = |K(\alpha) : F(\alpha)| \cdot |F(\alpha) : F| \end{aligned} \tag{3.1}$$

Since $f(X)$ is irreducible over F and α and β are roots of $f(X)$ in some extension, we know

$$|F(\alpha) : F| = |F(\beta) : F| = \deg f(X)$$

and

$$F(\alpha) \cong \frac{F[X]}{\big(f(X)\big)} \cong F(\beta)$$

by Theorem 2.14. Let $\phi\colon F(\alpha) \to F(\beta)$ be this isomorphism. Note, from the form of the isomorphism from $F[X]/\big(f(X)\big)$ to $F(\alpha)$ and $F(\beta)$ in Theorem 2.14, that ϕ is an F-isomorphism (that is, $a\phi = a$ for all $a \in F$).

Observe that $K(\alpha)$ can be obtained from $F(\alpha)$ by adjoining the roots of $g(X)$ to $F(\alpha)$, since we build K from F by adjoining these roots, and hence $K(\alpha)$ is the splitting field for $g(X)$

over $F(\alpha)$. Similarly, $K(\beta)$ is the splitting field for $g(X)$ over $F(\beta)$. We now make use of Theorem 3.6 to produce an isomorphism $\theta\colon K(\alpha) \to K(\beta)$ such that $\theta|_{F(\alpha)} = \phi$. This isomorphism then maps the subfield $F(\alpha)$ to the subfield $F(\beta)$. Consequently, θ will map a basis for $K(\alpha)$ over $F(\alpha)$ to a basis for $K(\beta)$ over $F(\beta)$. Therefore these bases have the same cardinality; that is,

$$|K(\alpha) : F(\alpha)| = |K(\beta) : F(\beta)|.$$

From this we conclude that the right-hand sides appearing in the Equations 3.1 are equal, and therefore the left-hand sides are equal. Hence

$$|K(\alpha) : K| = |K(\beta) : K|.$$

However, $\alpha \in K$, so we conclude $|K(\beta) : K| = 1$; that is, $\beta \in K$.

We have now shown that every root of $f(X)$ does indeed belong to K and hence $f(X)$ splits over K. It follows that K is indeed a normal extension of F. □

Chapter 4

Separability

The purpose of this chapter is to introduce a technical condition that appears within our main theorem. We shall observe that all extensions of a field of characteristic zero satisfy this condition (see Corollary 4.9 below), so the main purpose of introducing this condition is to ensure that the theory can be applied both in characteristic zero and in positive characteristic. The main result of this chapter is the Theorem of the Primitive Element that tells us that we can assume, under the technical condition provided, that a finite extension is actually a simple extension. This will enable us to establish later results more easily.

Separable polynomials

Definition 4.1 Let $f(X)$ be an irreducible polynomial over a field F. We say that $f(X)$ is *separable* over F if it has no multiple roots in a splitting field.

So this means that if $f(X)$ is a separable polynomial over a field F, then firstly it is irreducible over F and secondly, if K is a splitting field for $f(X)$ over F, then over K

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$$

where the elements α_1, α_2, $\dots$, α_n in K are distinct.

In order to interpret and make use of this definition, we introduce the concept of formal differentiation:

Definition 4.2 Let $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial over some field F. The *formal derivative* of $f(X)$ is the polynomial

$$Df(X) = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Example 4.3 (i) When dealing with a polynomial over $\mathbb{C}$ (or indeed over any subfield of $\mathbb{C}$), the formal derivative D is simply the usual derivative of a complex-valued function.

(ii) If $f(X) = X^p + 1$ over some field of characteristic p, then

$$Df(X) = pX^{p-1} = 0.$$

Thus the formal derivative can behave somewhat unexpectedly when we work over a field of positive characteristic.

Despite the unusual behaviour just observed, formal differentiation does satisfy some familiar properties, namely it is linear and satisfies the usual product rule for differentiation.

Lemma 4.4 (Basic properties of formal differentiation) *Let $f(X)$ and $g(X)$ be polynomials in $F[X]$ and α and β be scalars in F. Then*

$$D\big(\alpha\, f(X) + \beta\, g(X)\big) = \alpha\, Df(X) + \beta\, Dg(X)$$
$$D\big(f(X)\, g(X)\big) = f(X) \cdot Dg(X) + Df(X) \cdot g(X)$$

PROOF: Suppose first that $f(X) = \sum a_i X^i$ and $g(X) = \sum b_i X^i$. Then

$$\alpha\, f(X) + \beta\, g(X) = \sum (\alpha a_i + \beta b_i) X^i,$$

so

$$\begin{aligned} D\big(\alpha\, f(X) + \beta\, g(X)\big) &= \sum_{i \geqslant 1} i(\alpha a_i + \beta b_i) X^{i-1} \\ &= \alpha \sum_{i \geqslant 1} i a_i X^{i-1} + \beta \sum_{i \geqslant 1} i b_i X^{i-1} \\ &= \alpha\, Df(X) + \beta\, Dg(X), \end{aligned}$$

as required.

Having shown that formal differentiation is linear, we shall now turn to the product rule. Consider first the case when $f(X) = X^m$ and $g(X) = X^n$ are powers of X. Then

$$D\big(f(X)\, g(X)\big) = D(X^{m+n}) = (m+n) X^{m+n-1},$$

while

$$\begin{aligned} f(X) \cdot Dg(X) + Df(X) \cdot g(X) &= X^m \cdot n X^{n-1} + m X^{m-1} \cdot X^n \\ &= n X^{m+n-1} + m X^{m+n-1} \\ &= (m+n) X^{m+n-1} \\ &= D\big(f(X)\, g(X)\big), \end{aligned}$$

in this special case.

We now use linearity to deal with arbitrary polynomials: for $f(X) = \sum a_i X^i$ and $g(X) = \sum b_i X^i$, observe

$$\begin{aligned} D\big(f(X)\, g(X)\big) &= D\bigg(\Big(\sum a_i X^i\Big)\Big(\sum b_j X^j\Big)\bigg) \\ &= D\bigg(\sum_{i,j} a_i b_j X^i X^j\bigg) \\ &= \sum_{i,j} a_i b_j D(X^i X^j) \\ &= \sum_{i,j} a_i b_j (X^i \cdot D(X^j) + D(X^i) \cdot X^j) \\ &= \Big(\sum_i a_i X^i\Big)\Big(\sum_j b_j D(X^j)\Big) + \Big(\sum_i a_i D(X^i)\Big)\Big(\sum_j b_j X^j\Big) \\ &= \Big(\sum_i a_i X^i\Big) \cdot D\Big(\sum_j b_j X^j\Big) + D\Big(\sum_i a_i X^i\Big) \cdot \Big(\sum_j b_j X^j\Big) \\ &= f(X) \cdot Dg(X) + Df(X) \cdot g(X), \end{aligned}$$

as claimed. □

We have now shown that formal differentiation satisfies familiar properties of "normal" differentiation. We are also only using it with polynomials, which were the easiest functions that we first learnt to differentiate anyway. One just simply needs to be careful with polynomials over fields of positive characteristic, where some unusual things happen (as observed in Example 4.3(ii) above). The crucial link between formal differentiation and the concept of separability is the following:

Lemma 4.5 *Let $f(X)$ be a polynomial over a field F. Then $f(X)$ has a repeated root in a splitting field if and only if $f(X)$ and the formal derivative $Df(X)$ have a common factor of degree at least one in the polynomial ring $F[X]$.*

These lecture notes now contain two proofs of this lemma. The second was the original found in the notes, but the first is a clarified version of the proof presented during the lectures. The first half of the proof is the same for both versions; it is the second half that is updated in the new version.

PROOF: [New proof] Suppose first that $f(X)$ has a repeated root in a splitting field K for $f(X)$. Then

$$f(X) = (X - \alpha)^2 \, g(X)$$

where $\alpha \in K$ and $g(X) \in K[X]$ is some polynomial. Hence, using the basic properties of formal differentiation,

$$Df(X) = (X - \alpha)^2 \, Dg(X) + 2(X - \alpha) \, g(X)$$

over K. In particular, $f(\alpha) = Df(\alpha) = 0$; that is, $f(X)$ and $Df(X)$ are polynomials over F which vanish when evaluated at α in K. Therefore, by Theorem 2.11(iv), they are both divisible by the minimum polynomial of α. Consequently they have a common factor in $F[X]$ of degree at least one.

Conversely suppose $f(X)$ and $Df(X)$ have a common factor in $F[X]$ of degree at least one. Passing to the splitting field, we conclude that these two polynomials have a common factor in $K[X]$ of degree at least one and that this common factor is a product of linear factors (since it divides $f(X)$ and this splits over K). In particular, there is a linear factor $X - \alpha$ (for some $\alpha \in K$) that divides both $f(X)$ and $Df(X)$ in $K[X]$. Write

$$f(X) = (X - \alpha) \, h(X)$$

for some $h(X) \in K[X]$. Then

$$Df(X) = (X - \alpha) \, Dh(X) + h(X)$$

by our properties of formal differentiation. By assumption, $X - \alpha$ divides $Df(X)$, so it also divides $h(X) = Df(X) - (X - \alpha) \, Dh(X)$. Hence we can write

$$h(X) = (X - \alpha) \, g(X)$$

for some polynomial $g(X) \in K[X]$. Thus

$$f(X) = (X - \alpha)^2 \, g(X)$$

over K and we conclude that $f(X)$ has a repeated root α in K. This completes the proof of the lemma. □

PROOF: [Original proof in lecture notes] Suppose first that $f(X)$ has a repeated root in a splitting field K for $f(X)$. Then

$$f(X) = (X - \alpha)^2 g(X)$$

where $\alpha \in K$ and $g(X) \in K[X]$ is some polynomial. Hence, using the basic properties of formal differentiation,

$$Df(X) = (X - \alpha)^2 \cdot Dg(X) + 2(X - \alpha)\, g(X)$$

over K. In particular, $f(\alpha) = Df(\alpha) = 0$; that is, $f(X)$ and $Df(X)$ are polynomials over F which vanish when evaluated at α in K. Therefore, by Theorem 2.11(iv), they are both divisible by the minimum polynomial of α. Thus they have a common factor of degree at least one.

Conversely, suppose $f(X)$ has no repeated root in a splitting field K. Over the next stage of the proof, we work over the splitting field K and temporarily forget about the original field F.

Claim: $f(X)$ and $Df(X)$ are coprime in $K[X]$.

We proceed by induction on the degree n of $f(X)$. If $n = 1$, then $Df(X)$ is a non-zero constant (even over a field of positive characteristic), so the highest common factor is also a constant (that is, a unit in $F[X]$) and hence $f(X)$ and $Df(X)$ are indeed coprime in this case.

Suppose that $n > 1$ and, over the splitting field K, write

$$f(X) = (X - \alpha)\, g(X)$$

where $\alpha \in K$ and $g(X) \in K[X]$. Our original hypothesis tells us that $g(X)$ has no repeated roots in K, so by induction we can assume that $g(X)$ and $Dg(X)$ are coprime in $K[X]$. In addition, $X - \alpha$ does not divide $g(X)$. Now, by the basic properties of formal differentiation,

$$Df(X) = (X - \alpha) \cdot Dg(X) + g(X). \tag{4.1}$$

Suppose that $f(X)$ and $Df(X)$ are not coprime over K. As K is a splitting field for $f(X)$ over F, any polynomial that divides $f(X)$ in $K[X]$ can be factorized into linear factors and we conclude that there exists some linear factor of $f(X)$ in $K[X]$ that also divides $Df(X)$. Since $X - \alpha$ does not divide $g(X)$, use of Equation (4.1) shows that it does not divide $Df(X)$ either. Thus any linear factor dividing both $f(X)$ and $Df(X)$ is not $X - \alpha$. Hence there is a linear factor of $g(X)$ that divides $Df(X)$ and, from Equation (4.1), this linear factor divides $Dg(X)$. This contradicts the induction hypothesis and we have therefore established the claim.

We now return to the base field F. If $f(X)$ and $Df(X)$ have a common factor $h(X)$ in $F[X]$, then it also divides these two polynomials in $K[X]$, so it is constant by what we have just established. This shows that, under the assumption that $f(X)$ has no repeated root in K, we can conclude $f(X)$ and $Df(X)$ have only constants as factors. This establishes the required converse. □

Proposition 4.6 *Let $f(X)$ be an irreducible polynomial over a field F of characteristic zero. Then $f(X)$ is separable.*

PROOF: Let $f(X)$ be an irreducible polynomial over a field F. Necessarily $f(X)$ is not constant, so using the fact that F has characteristic zero,

$$Df(X) \neq 0.$$

(If the leading term of $f(X)$ is $a_n X^n$ with $a_n \neq 0$, then the leading term of $Df(X)$ is $na_n X^{n-1}$ and $na_n \neq 0$ in F.) Suppose that $f(X)$ is not separable. Then, by Lemma 4.5, $f(X)$ and $Df(X)$ have a common factor $g(X)$ of degree at least one. Now

$$\deg g(X) \leqslant \deg Df(X) = \deg f(X) - 1,$$

yet $f(X)$ is irreducible so has no non-constant divisors of degree less than $\deg f(X)$. This is a contradiction and we conclude that $f(X)$ is indeed separable. □

The same result is not true over a field of characteristic p. The proof above breaks down since possible $Df(X) = 0$ even when $f(X)$ is an irreducible polynomial over a field of characteristic p. To construct a counterexample requires a bit of work. We shall state the construction here, but defer the details to Problem Sheet IV, Question 5, since this is not central to the theory we develop.

Example 4.7 Let t be an indeterminate and consider the field $F = \mathbb{F}_p(t)$ of rational functions over the finite field $\mathbb{F}_p$ in the indeterminate t. Define

$$f(X) = X^p - t,$$

a polynomial in the indeterminate X with coefficients in the field F. One can establish the following facts:

(i) $f(X) = 0$ has no roots in F;

(ii) if α is any root of $f(X)$ in a splitting field, then $f(X) = (X - \alpha)^p$;

(iii) $f(X)$ is irreducible over F.

Hence $f(X)$ is an inseparable polynomial over the field F.

Separable extensions and the Theorem of the Primitive Element

We shall now extend the concept of separability to extensions. Since it relates to the minimum polynomials of elements in the extension, this definition applies to algebraic extensions.

Definition 4.8 Let K be an algebraic extension of a field F. We say that K is a *separable extension* of F if the minimum polynomial of every element of K over F is separable over F.

In view of Proposition 4.6, we conclude:

Corollary 4.9 *Every algebraic extension of a field of characteristic zero is a separable extension.* □

We now turn to establish the Theorem of the Primitive Element concerning finite separable extensions. This will enable us to assume that we are working with a simple extension; that is, an extension of the form $F(\alpha)$ for some algebraic element α.

Lemma 4.10 *Let L be a separable extension of an infinite field F and let $\beta, \gamma \in L$. Then there exists some $\alpha \in F(\beta, \gamma)$ such that*

$$F(\beta, \gamma) = F(\alpha).$$

Proof: Recall that a separable extension is, in particular, an algebraic extension. Let $f(X)$ be the minimum polynomial of β over F and $g(X)$ be the minimum polynomial of γ over F. Let K be a splitting field for the polynomial $f(X)\,g(X)$ over F. Let

$$\beta_1, \beta_2, \ldots, \beta_m \qquad \text{and} \qquad \gamma_1, \gamma_2, \ldots, \gamma_n$$

be the roots of $f(X)$ and $g(X)$, respectively, in K, where $\beta_1 = \beta$ and $\gamma_1 = \gamma$, without loss of generality. The assumption that L is a separable extension ensures that the β_i are distinct and the γ_i are distinct.

Since F is an infinite field, we can choose $c \in F$ such that $c \neq 0$ and

$$c \neq \frac{\beta_1 - \beta_i}{\gamma_1 - \gamma_j}$$

for all $i \geqslant 2$ and $j \geqslant 2$. Put $\alpha = \beta_1 - c\gamma_1$. The purpose of our choice of c is to achieve the following claim:

Claim:

$$\beta_i - c\gamma_j = \alpha \qquad \text{if and only if} \qquad i = j = 1. \tag{4.2}$$

Certainly if $i = j = 1$, then $\beta_i - c\gamma_i = \beta_1 - c\gamma_1 = \alpha$. Conversely, suppose $\beta_i - c\gamma_j = \beta_1 - c\gamma_1$. Then $c(\gamma_1 - \gamma_j) = \beta_1 - \beta_i$. If $j \neq 1$, then $c = (\beta_1 - \beta_i)/(\gamma_1 - \gamma_j)$ which is impossible since if $i = 1$, it says $c = 0$, and if $i \geqslant 2$ then we have contradicted the definition of c. Hence $j = 1$ and now $\beta_1 - \beta_i = 0$, which gives $i = 1$ since the roots of $f(X)$ are distinct.

Let $E = F(\alpha)$, which is some subfield of $F(\beta, \gamma)$ since $\alpha = \beta_1 - c\gamma_1 \in F(\beta, \gamma)$. We must establish the reverse inclusion.

Consider the two polynomials

$$h(X) = f(cX + \alpha) \qquad \text{and} \qquad g(X),$$

which are polynomials over E. Observe that

$$h(\gamma_1) = f(c\gamma_1 + \alpha) = f(\beta_1) = 0,$$

while $g(\gamma_1) = 0$. Our goal is to determine the greatest common divisor of these two polynomials in $E[X]$. However, we first work over the larger field K. Indeed, over K, we know

$$g(X) = (X - \gamma_1)(X - \gamma_2) \dots (X - \gamma_n)$$

and so the greatest common divisor $k(X)$ of $h(X)$ and $g(X)$ in $K[X]$ is a product of some of these factors $X - \gamma_j$. If $X - \gamma_j$ is a divisor of $h(X)$, then $h(\gamma_j) = 0$; that is,

$$f(c\gamma_j + \alpha) = 0.$$

This $c\gamma_j + \alpha = \beta_i$ for some i and, as noted above in Equation (4.2), this forces $i = j = 1$. Hence any such common factor of $h(X)$ and $g(X)$ could only be $X - \gamma_1$ and this is indeed a factor since $h(\gamma_1) = g(\gamma_1) = 0$. Hence

$$\text{the greatest common divisor of } h(X) \text{ and } g(X) \text{ in } K[X] \text{ is } k(X) = X - \gamma_1.$$

Now consider the highest common factor of $h(X)$ and $g(X)$ in $E[X]$. It is certainly a factor of $h(X)$ and $g(X)$ in the larger ring $K[X]$, so divides $k(X) = X - \gamma_1$. However, if $h(X)$ and $g(X)$ were coprime in $E[X]$, we would be able to find $u(X), v(X) \in E[X]$ such that

$$1 = u(X)\, h(X) + v(X)\, g(X),$$

but this would give a contradiction since the right-hand side evaluates to 0 when we substite the element γ_1 for X. We conclude that the highest common factor of $h(X)$ and $g(X)$ in $E[X]$ must also be $X - \gamma_1$ and hence the coefficient $\gamma = \gamma_1 \in E$. Finally

$$\beta = \beta_1 = \alpha + c\gamma_1 \in E$$

and we deduce $F(\beta, \gamma) \subseteq E = F(\alpha)$.

From this we conclude the claimed equality: $F(\alpha) = F(\beta, \gamma)$. □

Theorem 4.11 (Theorem of the Primitive Element) *Let K be a finite separable extension of an infinite field F. Then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof: By Theorem 2.17, we know that $K = F(\beta_1, \beta_2, \dots, \beta_n)$ for some $\beta_1, \beta_2, \dots, \beta_n \in K$. If $n = 1$, then certainly the claim holds.

If $n > 1$, we now apply induction. Since every element of K has separable minimum polynomial over F, we conclude that $F(\beta_1, \dots, \beta_{n-1})$ is also a finite separable extension of F. Hence, by induction,

$$F(\beta_1, \dots, \beta_{n-1}) = F(\gamma)$$

for some γ. Now $K = F(\gamma, \beta_n)$ and, by Lemma 4.10, we now conclude $K = F(\alpha)$ for some $\alpha \in K$, as required. □

Corollary 4.12 *Every finite extension of a field of characteristic zero can be expressed as a simple extension.*

As we mentioned at the start of the chapter, separable extensions will appear in our main theorem. We still need to understand finite separable extensions of finite fields, since Theorem 4.11 does not apply. Accordingly, we study finite fields in the next chapter to establish, in particular, an analogous result upon which we can rely in that case.

Chapter 5

Finite Fields

Many courses on Galois Theory finish with a final chapter which discusses the properties of finite fields and how the study of Galois Theory applies to them. In these lecture notes, however, I have chosen to place at this point in the notes the information about the structure of finite fields (in particular, their construction) since the methods developed in the previous two chapters are sufficient. It is also my plan to exploit the Theorem of the Primitive Element during our investigation of the main theory. This theorem essentially applies to infinite fields and consequently we need alternative methods for finite fields. Hence it will be important to establish that the multiplicative group of a finite field is cyclic, as we shall do in this chapter.

Construction of finite fields

Let F be a finite field. Then F has characteristic p for some prime number p and it has a subfield isomorphic to the finite field $\mathbb{F}_p$ (that is, the prime subfield of F). Let $n = |F : \mathbb{F}_p|$ be the degree of the extension. (As F is finite, it is certainly finite dimensional as a vector space over $\mathbb{F}_p$.) If $\{x_1, x_2, \ldots, x_n\}$ is a basis for F over $\mathbb{F}_p$, then every element of F can be expressed uniquely in the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

where $a_1, a_2, \ldots, a_n \in \mathbb{F}_p$. Hence

$$|F| = p^n.$$

Thus, we can make our first observation:

Proposition 5.1 *A finite field F has order p^n where p is a prime number equal to the characteristic of F and where n is the degree of F over its prime subfield $\mathbb{F}_p$.* □

Note, in particular, this argument shows that a finite extension of the field $\mathbb{F}_p$ (or indeed of any finite field) is still a finite field.

Of course, Proposition 5.1 provides us with a restriction which finite fields could exists, namely that they must all have prime-power order, but we need to do more to show that fields of each such order do indeed exist. We shall need two observations in our argument.

Lemma 5.2 *Let F be a finite field of order $q = p^n$ and characteristic p. Then*

(i) $a^{q-1} = 1$ *for all* $a \in F \setminus \{0\}$;

(ii) ***("Freshman's Exponentiation")***

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}$$

for all $a, b \in F$ and non-negative integers k.

PROOF: (i) The set of non-zero elements of F forms the multiplicative group F^*, which is a group of order $q-1$, so $a^{q-1}=1$ for all $a \in F^*$ by Lagrange's Theorem.

(ii) We proceed by induction on k. When $k=0$, the result is immediate since both sides equal $a+b$. Now if $c, d \in F$, note that

$$(c+d)^p = \sum_{i=0}^{p} \binom{p}{i} c^i d^{p-i}. \tag{5.1}$$

We already observed (back in Example 1.24(iii)) that each binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, 2, \ldots, p-1$. Hence, in our field F of characteristic p,

$$(c+d)^p = c^p + d^p.$$

Returning to the inductive step,

$$\begin{aligned}
(a+b)^{p^{k+1}} &= \left((a+b)^{p^k}\right)^p \\
&= (a^{p^k} + b^{p^k})^p && \text{by induction} \\
&= (a^{p^k})^p + (b^{p^k})^p && \text{by Equation (5.1)} \\
&= a^{p^{k+1}} + b^{p^{k+1}},
\end{aligned}$$

completing the induction. □

We can now establish that there exists a finite field of each prime-power order and, moreover, it is unique.

Theorem 5.3 *Let p be a prime number and n be a positive integer. Then there is precisely one field of order p^n up to isomorphism.*

PROOF: We start by establishing existence. Let $f(X) = X^{p^n} - X$ and let F be the splitting field of $f(X)$ over $\mathbb{F}_p$ (which exists by Theorem 3.4). Let S be the set of roots of $f(X)$ in F. Note certainly $0, 1 \in S$. If $a, b \in S$, then $a^{p^n} = a$, $b^{p^n} = b$, so

$$\begin{aligned}
(ab)^{p^n} &= a^{p^n} b^{p^n} = ab \\
(a+b)^{p^n} &= a^{p^n} + b^{p^n} = a+b \\
(-a)^{p^n} &= (-1)^{p^n} a^{p^n} = -a \\
(1/a)^{p^n} &= 1/a^{p^n} = 1/a
\end{aligned}$$

(if $a \neq 0$ in the last). Note here that in the second equation we use Freshman's Exponentiation (Lemma 5.2(ii)), while in the third note that $(-1)^{p^n} = -1$ when p is odd, while $(-1)^{p^n} = 1 = -1$ when $p = 2$. The conclusion is that S is a subfield of F. In particular, S must contain the prime subfield, so $\mathbb{F}_p \subseteq S$. However, we now recall that F is the splitting field of $f(X)$ over $\mathbb{F}_p$ and so is the smallest field containing $\mathbb{F}_p$ and all the roots of $f(X)$; that is, $F = S$, so we record:

Every element of F is a root of $f(X)$.

To determine the order of the splitting field F, we shall determine the number of roots of $f(X)$ in F. Observe the formal derivative of $f(X)$ is

$$Df(X) = p^n X^{p^n - 1} - 1 = -1$$

and we conclude that $f(X)$ and $Df(X)$ have no common factor of degree one or more. Hence, by Lemma 4.5, the polynomial $f(X)$ has no repeated roots in the splitting field F; that is, $f(X)$ has precisely p^n roots in F. We conclude:

The splitting field F is a finite field of order p^n.

To establish uniqueness, consider any field K of order p^n, so that K is an extension of the prime subfield $\mathbb{F}_p$ of degree n. The multiplicative group of K has order $p^n - 1$, so

$$a^{p^n-1} = 1 \qquad \text{for all } a \in K \setminus \{0\}$$

and therefore

$$a^{p^n} = a \qquad \text{for all } a \in K.$$

We conclude that our polynomial $f(X)$ has p^n distinct roots in K and therefore this polynomial splits in K; that is, K is a splitting field for $f(X)$ over $\mathbb{F}_p$. We now use the fact that splitting fields are unique (Corollary 3.8) to conclude that K is $\mathbb{F}_p$-isomorphic to the field F constructed previously. This completes the proof. □

Definition 5.4 The (unique) field of order p^n is denoted $\mathbb{F}_{p^n}$ and is often called the *Galois field* of order p^n.

Although the theorem establishes that the Galois field $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, this is not necessarily a convenient description to construct the field. It is often easier to go back to Theorem 2.13 which describes how to construct a simple extension with a specified minimum polynomial.

Example 5.5 *Construct the Galois field $\mathbb{F}_4$ of order 4 and give its multiplication table.*

Solution: Let $f(X) = X^2 + X + 1$ over $\mathbb{F}_2$. Note that this polynomial is irreducible over $\mathbb{F}_2$ since

$$f(0) = f(1) = 1$$

so $f(X)$ has no linear factors. Adjoin a root α of $f(X)$ over $\mathbb{F}_2$ to construct the simple extension $\mathbb{F}_2(\alpha)$. Thus we have a degree 2 extension of $\mathbb{F}_2$ with basis $\{1, \alpha\}$. The elements of $\mathbb{F}_2(\alpha)$ are

$$0, \quad 1, \quad \alpha, \quad \alpha + 1$$

so $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$ (using the uniqueness of finite fields that we have established in Theorem 5.3). Addition is straightforward: we just use the vector space structure. The multiplication is achieved by exploiting the fact that $f(\alpha) = 0$, so $\alpha^2 = \alpha + 1$. Hence the multiplication table of $\mathbb{F}_4$ is:

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Indeed, observe for example

$$\alpha(\alpha + 1) = \alpha^2 + \alpha = 1.$$

□

The multiplicative group of a finite field

In this section, we shall show that the multiplicative group of a finite field is always a cyclic group. In some examples that we know, this can be seen straightaway. For example, $\mathbb{F}_4^*$ is a group of order 3, so is cyclic generated by any non-identity element and indeed, in the notation of the solution for Example 5.5,

$$\alpha, \qquad \alpha^2 = \alpha + 1, \qquad \alpha^3 = \alpha^2 + \alpha = 1$$

are the three non-zero elements of $\mathbb{F}_4$. Equally, if we calculate the powers of 3 in $\mathbb{F}_7$, we observe they are

$$3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

This example does illustrate the need for care though, since 3 is a generator for $\mathbb{F}_7^*$, but 2 does not generate this multiplicative group.

To work towards showing that the multiplicative group of a finite field is indeed cyclic, we begin by introducing the following terminology:

Definition 5.6 The *exponent* of a finite group is the least common multiple of the orders of elements of G.

Note that Lagrange's Theorem tells us that the order of every element of a finite group G divides the order of G and hence the exponent of G also divides $|G|$.

Lemma 5.7 *Let G be a finite abelian group with exponent ν. Then there exists some $g \in G$ of order ν.*

This could be established relatively quickly from the Classification of Finite Abelian Groups as direct products of cyclic groups. The proof presented here will be direct without requiring explicit use of that result. (Some aspects of the proof will be in common with the proof of said Classification.)

PROOF: First factorize ν into its product of primes,

$$\nu = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

and let $q = p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Consider an element $x_1 \in G$ such that the order of x is a power of p_1 and that $o(x_1) = p_1^{\beta}$ with β as large as possible.

Claim: $\beta = \alpha_1$.

Since ν is the lowest common multiple of the element orders, certainly p_1^{β} divides ν and so $\beta \leqslant \alpha_1$. Suppose $\beta < \alpha_1$. Then if $h \in G$, we note, from the fact that $o(h)$ divides ν, that

$$1 = h^{\nu} = (h^q)^{p_1^{\alpha_1}},$$

so h^q is an element of p_1-power order. From our assumption on x as having the largest p_1-power order in G, we conclude then that $(h^q)^{p_1^{\beta}} = 1$; that is,

$$h^{p_1^{\beta} q} = 1$$

so the order of h divides $p_1^{\beta} q$. This is true for all elements h in G and we conclude that the lowest common multiple of the orders of elements in G divides

$$p_1^{\beta} q = p_1^{\beta} p_2^{\alpha_2} \dots p_k^{\alpha_k} < \nu,$$

contrary to the assumption that ν is the exponent of G.

In conclusion, $\beta = \alpha_1$ and we observe that there is an element x_1 in G of order $p_1^{\alpha_1}$.

Similarly, we now conclude that there are elements x_1, x_2, …, x_k in G with $o(x_i) = p_i^{\alpha_i}$. Finally, as x_1, x_2, …, x_k commute and have coprime orders, we conclude

$$o(x_1 x_2 \dots x_k) = o(x_1)\, o(x_2) \dots o(x_k) = \nu,$$

as required. □

Theorem 5.8 *The multiplicative group of a finite field is cyclic.*

PROOF: Let F be a finite field of order p^n. Let ν be the exponent of the multiplicative group. Since ν is divisible by the order of any element $a \in F^*$, we conclude

$$a^\nu = 1 \qquad \text{for all } a \in F \setminus \{0\}.$$

Hence

$$a^{\nu+1} - a = 0 \qquad \text{for all } a \in F.$$

We conclude that the polynomial $X^{\nu+1} - X$ has p^n roots in F, so its degree $\nu + 1 \geqslant p^n$. On the other hand, we know that the exponent ν divides the group order $|F^*|$ by Lagrange's Theorem (as noted before), so $\nu \leqslant p^n - 1$. We conclude therefore that

$$\nu = p^n - 1.$$

Now Lemma 5.7 tells us that F^* contains an element g of order $p^n - 1$, so $F^* = \langle g \rangle$, as required. □

We can use the fact that the multiplicative group is cyclic to provide an alternative to the Theorem of the Primitive Element for finite fields.

Corollary 5.9 *Let $F \subseteq K$ be an extension of finite fields. Then $K = F(\alpha)$ for some $\alpha \in K$.*

PROOF: Indeed, choose α to be the generator for K^*. Then the smallest subfield containing α must be the whole of K, so $K = F(\alpha)$. □

Putting Theorem 4.11 together with Corollary 5.9, we conclude that if K is a finite separable extension of F, then $K = F(\alpha)$ for some $\alpha \in K$ irrespective of whether F is an infinite field or a finite field.

Chapter 6

Galois Groups and the Fundamental Theorem of Galois Theory

We now turn to the key idea of Galois Theory, namely that to every extension K of a field F we can associate a group, the Galois group of K over F, and that properties of the field extension are determined by the structure of the group. This latter fact is encoded within the Fundamental Theorem of Galois Theory and we prove this theorem, the main result of the course, in this chapter.

Galois groups

The primary object that we are interested in when studying Galois theory is the following:

Definition 6.1 Let K be an extension of the field F. The *Galois group* $\mathrm{Gal}(K/F)$ of K over F is the set of all F-automorphisms of K with binary operation being composition of automorphisms.

Recall that an F-automorphism of K is an isomorphism $\phi\colon K \to K$ such that $a\phi = a$ for all $a \in F$. Certainly the identity map is an F-automorphism, while if ϕ and ψ are F-automorphisms of K then so are the composite $\phi\psi$ and the inverse ϕ^{-1}. Of course, composition of maps is an associative binary operation and we can therefore conclude that the Galois group $\mathrm{Gal}(K/F)$ is indeed a group.

Example 6.2 Recall from Example 3.10 that there are precisely two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$, namely those given, respectively, by

$$a + bi \mapsto a + bi \qquad \text{and} \qquad a + bi \mapsto a - bi$$

for $a, b \in \mathbb{Q}$; that is, a $\mathbb{Q}$-automorphism is determined by to which of the two roots of $X^2 + 1$ it maps i. Hence $|\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})| = 2$; that is, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$.

We shall observe in our main theorem that it is no coincidence that this group order equals the degree $|\mathbb{Q}(i) : \mathbb{Q}|$ of the extension.

The sets $\mathscr{F}$ and $\mathscr{G}$

Definition 6.3 Let K be an extension of the field F and let $G = \mathrm{Gal}(K/F)$ be the Galois group of K over F.

(i) Define $\mathscr{G}$ to be the set of subgroups of G.

(ii) Define $\mathscr{F}$ to be the set of *intermediate fields*; that is,

$$\mathscr{F} = \{\, L \mid L \text{ is a field with } F \subseteq L \subseteq K \,\}.$$

(iii) If $H \in \mathscr{G}$, define

$$H^* = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in H \,\},$$

the set of points in K fixed by all F-automorphisms in H.

(iv) If $L \in \mathscr{F}$, define

$$L^* = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\},$$

the set of all F-automorphisms that fix all points in L.

We shall show that (iii) and (iv) in this definition provide us with maps $^*\colon \mathscr{G} \to \mathscr{F}$ and $^*\colon \mathscr{F} \to \mathscr{G}$ and then investigate properties of these maps.

We also use the notation $\mathrm{Fix}_K(H)$ for the elements of the field K that are fixed by all automorphisms in the subgroup $H \in \mathscr{G}$; that is,

$$H^* = \mathrm{Fix}_K(H).$$

Equally, note that automorphisms in L^* consists of automorphisms of K that are the identity when applied to elements of L, so

$$L^* = \mathrm{Gal}(K/L)$$

for any $L \in \mathscr{F}$.

Comment: Stewart's book denotes the above maps by † and * to distinguish between them. I choose to follow the notation in Cohn's chapter on field theory, namely to denote both maps by the same symbol. My reason for this is that it is usually clear which one we are actually using, some of the notation becomes a little more transparent (at least, in my opinion) and it certainly gives me one less thing of which to keep track.

Lemma 6.4 *Let K be an extension of the field F and $G = \mathrm{Gal}(K/F)$.*

(i) *If $H \in \mathscr{G}$, then $H^* \in \mathscr{F}$;*

(ii) *If $L \in \mathscr{F}$, then $L^* \in \mathscr{G}$;*

(iii) *If $H_1, H_2 \in \mathscr{G}$ with $H_1 \leqslant H_2$, then $H_1^* \supseteq H_2^*$;*

(iv) *If $L_1, L_2 \in \mathscr{F}$ with $L_1 \subseteq L_2$, then $L_1^* \geqslant L_2^*$.*

Thus our definitions of * provide us with maps $\mathscr{G} \to \mathscr{F}$ and $\mathscr{F} \to \mathscr{G}$ that *reverse inclusions.*

Proof: (i) All elements of the Galois group, by definition, fix all points in the base field F, so we certainly observe

$$F \subseteq H^* \subseteq K.$$

In particular, H^* is non-empty and contains non-zero elements since it contains the field F. Suppose $x, y \in H^*$. Then, since each $\phi \in H$ is a field isomorphism,

$$\begin{aligned}(x+y)\phi &= x\phi + y\phi = x + y\\ (xy)\phi &= (x\phi)(y\phi) = xy\\ (-x)\phi &= -(x\phi) = -x\\ (1/x)\phi &= 1/(x\phi) = 1/x\end{aligned}$$

for all $\phi \in H$ (and where $x \neq 0$ in the fourth equation). This shows that $x + y, xy, -x \in H^*$ and, if $x \neq 0$, that $1/x \in H^*$. Hence H^* is closed under the field operations, so we conclude that H^* is indeed an intermediate field.

(ii) First note that the identity map certainly fixes all points in the intermediate field L, so L^* is non-empty. Let $\phi, \psi \in L^*$. Then

$$x(\phi\psi) = (x\phi)\psi = x\psi = x \qquad \text{for all } x \in L,$$

using the fact that $x\phi = x\psi = x$ for all $x \in L$, and hence $\phi\psi \in L^*$. Similarly

$$x = x\phi\phi^{-1} = (x\phi)\phi^{-1} = x\phi^{-1} \qquad \text{for all } x \in L,$$

so $\phi^{-1} \in L^*$. We conclude that L^* is a subgroup of G.

(iii) Suppose $H_1 \leqslant H_2$. If $x \in H_2^*$, then $x\phi = x$ for all $\phi \in H_2$, so $x\phi = x$ for all $\phi \in H_1$. Hence $x \in H_1^*$.

(iv) Suppose $L_1 \subseteq L_2$. If $\phi \in L_2^*$, then $x\phi = x$ for all $x \in L_2$, so $x\phi = x$ for all $x \in L_1$. Hence $\phi \in L_1^*$. □

The Fundamental Theorem of Galois Theory

In the Fundamental Theorem of Galois Theory, we shall actually observe that $^*\colon \mathscr{G} \to \mathscr{F}$ and $^*\colon \mathscr{F} \to \mathscr{G}$ are inverses of each other under sufficient assumptions concerning the field extension K of F. We shall define the term that encodes these conditions.

Definition 6.5 A finite extension of fields is called a *Galois extension* if it is normal and separable.

Lemma 6.6 *Let K be a finite Galois extension of a field F and L be an intermediate field ($F \subseteq L \subseteq K$). Then K is a Galois extension of L.*

Proof: First K is a finite normal extension of F, so by Theorem 3.13, it is the splitting field of some polynomial $g(X) \in F[X]$. Now $g(X)$ can also be viewed as a polynomial over L and K is still the splitting field for $g(X)$ over L (it is obtained by adjoining the roots of $g(X)$ to the subfield L). Hence K is a finite normal extension of L.

Second K is a separable extension of F. If $\gamma \in K$, then the minimum polynomial $m(X)$ of γ over F has distinct roots in a splitting field (that is, distinct roots in K). Now the minimum polynomial $m'(X)$ of γ over L must divide $m(X)$ (by Theorem 2.11(iv)) and so $m'(X)$ also has distinct roots in K where it splits. It follows that K is also a separable extension of L.

Thus the extension K of L satisfies the two required conditions so is a Galois extension. □

Theorem 6.7 (Fundamental Theorem of Galois Theory) *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. Then:*

(i) $|G| = |K : F|$.

(ii) *The maps $H \mapsto H^*$ and $L \mapsto L^*$ are mutual inverses and give a one-one inclusion-reversing correspondence between $\mathscr{G}$ and $\mathscr{F}$.*

(iii) *If L is an intermediate field, then*

$$|K : L| = |L^*| \qquad \text{and} \qquad |L : F| = |G|/|L^*|.$$

(iv) *An intermediate field L is a normal extension of F if and only if L^* is a normal subgroup of G. Moreover, in this situation,*

$$\mathrm{Gal}(L/F) \cong G/L^*.$$

PROOF: (i) Let $n = |K : F|$. Since K is a finite separable extension of F, use the Theorem of the Primitive Element (Theorem 4.11), or Corollary 5.9 when F is a finite field, to write

$$K = F(\alpha)$$

for some $\alpha \in K$. Let $f(X)$ be the minimum polynomial of α over F. Then

$$\deg f(X) = |F(\alpha) : F| = n.$$

Note that the elements of $F(\alpha)$ are linear combinations of powers of α,

$$x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

with $a_0, a_1, \ldots, a_{n-1} \in F$, and the effect of applying any F-automorphism $\phi \in G$ is then determined by the value of $\alpha\phi$:

$$\begin{aligned} x\phi &= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1})\phi \\ &= a_0 + a_1(\alpha\phi) + a_2(\alpha\phi)^2 + \cdots + a_{n-1}(\alpha\phi)^{n-1}. \end{aligned}$$

Furthermore, if we apply ϕ to the equation $f(\alpha) = 0$ we obtain

$$f(\alpha\phi) = 0,$$

so $\alpha\phi$ must be one of the roots of $f(X)$. Since $f(X)$ has degree n, we conclude that there are at most n F-automorphisms of K; that is,

$$|G| \leqslant n.$$

Finally, recall that since K is a separable extension of F, the minimum polynomial $f(X)$ of α has distinct roots in its splitting field. It splits over K, because $f(X)$ is irreducible over F, has at least one root in K and K is a normal extension of F. We conclude that $f(X)$ has n distinct roots in K. Let β be any root of $f(X)$ in K. Now

$$|F(\beta) : F| = \deg f(X) = |F(\alpha) : F| = |K : F|,$$

by Theorem 2.14, so $F(\beta) = K = F(\alpha)$. We now apply Lemma 3.5 to conclude there is an isomorphism $\psi\colon F(\alpha) \to F(\beta)$ such that ψ extends the identity map $F \to F$ and satisfies $\alpha\psi = \beta$. Hence there is an F-automorphism $\psi \in G$ which maps α to β. This establishes the reverse inequality, there are at least n F-automorphisms in G, and we have established part (i) of the Fundamental Theorem:

$$|G| = n = |K : F|.$$

(iii) We can deduce the third part of the Fundamental Theorem from (i). Let L be an intermediate field: $F \subseteq L \subseteq K$. Then, by definition,

$$\begin{aligned} L^* &= \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} \\ &= \mathrm{Gal}(K/L), \end{aligned}$$

since L^* consists of all automorphisms of K that fix all points of L. By Lemma 6.6, K is a finite Galois extension of L, so we can apply part (i) to conclude

$$|L^*| = |\mathrm{Gal}(K/L)| = |K : L|.$$

Finally, we complete the proof of (iii) by use of the Tower Law (Theorem 2.4):

$$|L : F| = \frac{|K : F|}{|K : L|} = \frac{|G|}{|L^*|}.$$

(ii) We have observed that for an intermediate field $L \in \mathscr{F}$,

$$L^* = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} = \mathrm{Gal}(K/L),$$

while, by definition, for a subgroup $H \in \mathscr{G}$,

$$H^* = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in H \,\} = \mathrm{Fix}_K(H),$$

the set of points of K fixed by the maps in H. Lemma 6.4 tells us that

$$L^* \in \mathscr{G}, \qquad H^* \in \mathscr{F}$$

and that the $*$-operations reverse inclusions. To complete the proof of (ii), namely to show each operation is the inverse of the other, we must prove that

$$H^{**} = H \qquad \text{for all } H \in \mathscr{G}$$

$$L^{**} = L \qquad \text{for all } L \in \mathscr{F}.$$

This will require us to make use of two further lemmas.

Lemma 6.8 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The fixed field of G,*

$$G^* = \mathrm{Fix}_K(G) = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in G \,\},$$

is precisely the base field of F.

Proof: Let us write $F_1 = G^*$. It follows from Lemma 6.4(i) that F_1 is some intermediate field: $F \subseteq F_1 \subseteq K$.

Let us apply the Theorem of the Primitive Element (Theorem 4.11, or use Corollary 5.9 if F is finite) to observe $K = F(\alpha)$ for some $\alpha \in K$. Let $f(X)$ be the minimum polynomial of α over F and let $g(X)$ be the minimum polynomial of α over F_1. Since $f(X)$ is a polynomial with coefficients from F_1 (as $F \subseteq F_1$) with $f(\alpha) = 0$, we conclude that $g(X)$ divides $f(X)$ in $F_1[X]$.

Now $f(X)$ is an irreducible polynomial over F with the root α in the normal separable extension K. Hence $f(X)$ splits over K and the roots of $f(X)$ in K are distinct. Let β be one of these roots of $f(X)$ in K. In the proof of part (i) of the Fundamental Theorem of Galois Theory, we observed there is an element $\psi \in G$ mapping α to β. Apply ψ to the equation

$$g(\alpha) = 0.$$

The coefficients of $g(X)$ are elements of F_1, so they are fixed by ψ (by definition of F_1). Hence, upon applying ψ, we conclude

$$g(\beta) = g(\alpha\psi) = \big(g(\alpha)\big)\psi = 0.$$

Hence each of the roots of $f(X)$ is also a root of $g(X)$. As these roots are distinct, we conclude that $g(X)$ is not a proper divisor of $f(X)$ but must have the same degree. Thus

$$\begin{aligned} |K : F_1| = |F_1(\alpha) : F_1| &= \deg g(X) \\ &= \deg f(X) = |F(\alpha) : F| = |K : F| = |K : F_1| \cdot |F_1 : F| \end{aligned}$$

Hence $|F_1 : F| = 1$ and $F_1 = F$, as required. □

Lemma 6.9 *Let K be a finite separable extension of a field F and let H be a finite group of F-automorphisms of K (that is, H is some subgroup of $\mathrm{Gal}(K/F)$). Then*

$$|K : H^*| = |H|$$

(where $H^* = \mathrm{Fix}_K(H)$).

PROOF: Write $L = H^*$. By the Theorem of the Primitive Element (Theorem 4.11, or Corollary 5.9 if F is finite), write $K = F(\alpha)$ for some $\alpha \in K$. Put

$$g(X) = \prod_{\phi \in H} (X - \alpha\phi),$$

which is some polynomial with coefficients from K; that is, $g(X) \in K[X]$. If $\psi \in H$, write $\bar{\psi}$ for the automorphism of the ring $K[X]$ obtained by applying ψ to the coefficients of polynomials. If we apply $\bar{\psi}$ to one of the linear factors $X - \alpha\phi$ of $g(X)$, we produce $X - \alpha\phi\psi$, which is again one of the linear factors of $g(X)$ since the product $\phi\psi$ is again an element of the group H. Indeed, the map $\phi \mapsto \phi\psi$ is a bijection $H \to H$ and so $\bar{\psi}$ permutes the linear factors of $g(X)$; that is,

$$g(X)\bar{\psi} = \prod_{\phi \in H} (X - \alpha\phi\psi) = g(X)$$

for all $\psi \in H$. Thus the coefficients appearing in $g(X)$ are fixed by all elements of H; that is, these coefficients belong to $\mathrm{Fix}_K(H) = H^* = L$ and we conclude that

$$g(X) \in L[X].$$

The definition of $g(X)$ says that it splits in K and, since $K = F(\alpha)$, we certainly build K by adjoining the roots of K to the subfield L. Thus K is the splitting field of $g(X)$ over L and hence, by Theorem 3.13, K is a normal extension of L.

The field K is also a separable extension of L, since K is a separable extension of F. (This was observed in the second half of the proof of Lemma 6.6; also see Question 3(b) on Problem Sheet IV.) In conclusion, K is a finite Galois extension of L and we can apply part (i) of the Fundamental Theorem of Galois Theory to conclude

$$|K : L| = |\mathrm{Gal}(K/L)| \geqslant |H|.$$

(Note every element of H is an L-automorphism of K, so H is a subgroup of $\mathrm{Gal}(K/L)$.)

On the other hand, $\deg g(X) = |H|$, so the degree of the minimum polynomial of α over L is at most $|H|$. Hence

$$|K : L| = |L(\alpha) : L| \leqslant |H|.$$

We have therefore shown

$$|K : H^*| = |K : L| = |H|,$$

as required. □

We now return to the proof of part (ii) of the Fundamental Theorem of Galois Theory. Let $L \in \mathscr{F}$. It follows from Lemma 6.6 that K is also a Galois extension of L. We have observed $L^* = \mathrm{Gal}(K/L)$ in part (iii). Now

$$L^{**} = \mathrm{Fix}_K(L^*) = L,$$

by Lemma 6.8 applied to the extension K of L.

Now let $H \in \mathscr{G}$. Let $H_1 = H^{**}$. Certainly H fixes all the points in H^* (by definition of H^*), so $H \leqslant H_1$. Take $L = H^*$ in the previous step to conclude

$$H_1^* = H^{***} = (H^*)^{**} = H^*.$$

Now by Lemma 6.9 applied to each of the subgroups H and H_1,

$$|K : H^*| = |H| \qquad \text{and} \qquad |K : H_1^*| = |H_1|,$$

so we conclude $|H| = |H_1|$. It follows that

$$H = H_1 = H^{**},$$

as required. The completes the proof of part (ii) of the Fundamental Theorem of Galois Theory.

(iv) We turn to the last part of the Fundamental Theorem. Let $L \in \mathscr{F}$ and consider what it means for L^* to be a normal subgroup of G. Observe

$$\begin{array}{lll} L^* \trianglelefteq G & \text{if and only if} & \phi\theta\phi^{-1} \in L^* \quad \text{for } \theta \in L^*,\ \phi \in G \\ & \text{if and only if} & x(\phi\theta\phi^{-1}) = x \quad \text{for } x \in L,\ \theta \in L^*,\ \phi \in G \\ & \text{if and only if} & x\phi\theta = x\phi \quad \text{for } x \in L,\ \theta \in L^*,\ \phi \in G \\ & \text{if and only if} & x\phi \in L^{**} \quad \text{for } x \in L,\ \phi \in G \\ & \text{if and only if} & x\phi \in L \quad \text{for } x \in L,\ \phi \in G, \end{array}$$

using part (ii). Hence

$$L^* \trianglelefteq G \qquad \text{if and only if} \qquad L\phi \subseteq L \quad \text{for all } \phi \in G.$$

Now suppose $L\phi \subseteq L$ for all $\phi \in G$. Let $g(X)$ be an irreducible polynomial over F and suppose that $g(X)$ has some root β which lies in L. We may assume that $g(X)$ is monic, by dividing by a scalar if necessary, so that $g(X)$ is the minimum polynomial of β over F. Put

$$h(X) = \prod_{\phi \in G} (X - \beta\phi).$$

If $\psi \in G$, the induced automorphism $\bar{\psi}$ of $K[X]$ permutes the linear factors of $h(X)$ when we apply it, so $\bar{\psi}$ fixes the coefficients of $h(X)$; that is, $h(X)$ is actually a polynomial with coefficients in $G^* = \mathrm{Fix}_K(G) = F$ (using Lemma 6.8). Since β is a root of $h(X)$ by construction, the minimum polynomial $g(X)$ of β over F divides $h(X)$. By assumption, $L\phi \subseteq L$ for all $\phi \in G$, and hence all the roots of $h(X)$ belong to L. Since $g(X)$ divides $h(X)$, we conclude that $g(X)$ splits in L. We have shown that if $L\phi \subseteq L$ for all $\phi \in G$, then L is a normal extension of F.

Conversely, suppose L is a normal extension of F. Let $\alpha \in L$ and $\phi \in G$. Let $f(X)$ be the minimum polynomial of α over F. Now $f(\alpha) = 0$, so applying ϕ, we conclude $f(\alpha\phi) = 0$. Thus $\alpha\phi$ is a root of $f(X)$. However, since L is a normal extension of F, all the roots of $f(X)$ belong to L. We thus conclude $\alpha\phi \in L$. It follows that if L is a normal extension of F then $L\phi \subseteq L$ for all $\phi \in G$.

We have then proved the following lemma which will be key in establishing part (iv) of the Fundamental Theorem:

Lemma 6.10 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The following conditions on an intermediate field L are equivalent:*

(i) *L^* is a normal subgroup of G;*

(ii) *$L\phi \subseteq L$ for all $\phi \in G$;*

(iii) *L is a normal extension of F.* □

The equivalence of (i) and (iii) in the lemma establish the first step of part (iv) of the Fundamental Theorem. Finally, let us assume L is a normal extension of F. First this means that L is a Galois extenson of F (since L inherits separability from the bigger field K). The lemma also tells us that $L^* \trianglelefteq G$ and $L\phi \subseteq L$ for all $\phi \in G$. Hence each F-automorphism ϕ

of K induces a F-automorphism $\phi|_L$ of L. (The restriction is certainly a map $\phi|_L \colon L \to L$ that preserves the field operations, while it is an automorphism since $\phi^{-1}|_L$ is the inverse.) Hence we can define a map $\Phi \colon G \to \mathrm{Gal}(L/F)$ by

$$\phi \mapsto \phi|_L.$$

Now

$$\ker \Phi = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\} = L^*,$$

by definition, so

$$\begin{aligned}
|\mathrm{im}\,\Phi| &= \frac{|G|}{|L^*|} && \text{(by the First Isomorphism Theorem for groups)} \\
&= \frac{|K:F|}{|K:L|} && \text{(by parts (i) and (iii))} \\
&= |L:F| && \text{(by the Tower Law)} \\
&= |\mathrm{Gal}(L/F)| && \text{(by (i) applied to the Galois extension } L \text{ of } F).
\end{aligned}$$

Hence Φ is surjective and so, by the First Isomorphism Theorem,

$$\mathrm{Gal}(L/F) \cong G/L^*.$$

This completes the proof of the Fundamental Theorem of Galois Theory. □

In light of the fact that we have established part (ii) of the Fundamental Theorem, we can make the following definition.

Definition 6.11 When K is a finite Galois extension of the field F, the maps $H \mapsto H^*$ and $L \mapsto L^*$ are called the *Galois correspondence* between the set $\mathscr{G}$ of subgroups of the Galois group and the set $\mathscr{F}$ of intermediate fields.

Examples of Galois groups

Let us now turn to illustrating the use of the Fundamental Theorem of Galois Theory and the calculation of Galois groups. We make a further definition of what we mean by a Galois group.

Definition 6.12 Let $f(X)$ be a polynomial over a field F. The *Galois group* $\mathrm{Gal}_F(f(X))$ of $f(X)$ is the Galois group $\mathrm{Gal}(K/F)$ of the splitting field K of $f(X)$ over F.

If F is a field of characteristic zero, then the splitting field K of a polynomial $f(X)$ over F is a normal extension, by Theorem 3.13, and is separable by Corollary 4.9. Hence we may apply the Fundamental Theorem of Galois Theory in such a situation.

Example 6.13 Let $f(X) = X^4 - 2$ over $\mathbb{Q}$. The roots of this polynomial in $\mathbb{C}$ are

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}.$$

Hence the splitting field of $f(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt[4]{2}, i).$$

Now $f(X)$ is the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ (since it is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion), so

$$|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = \deg f(X) = 4.$$

As $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, the minimum polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$ is X^2+1 (the latter cannot factorize into linear polynomials over a subfield of $\mathbb{R}$). Hence

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

Hence, by the Tower Law,

$$|K : \mathbb{Q}| = |K : \mathbb{Q}(\sqrt[4]{2})| \cdot |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 8.$$

Part (i) of the Fundamental Theorem of Galois Theory tells us that

$$|\mathrm{Gal}(K/\mathbb{Q})| = 8.$$

On the other hand, any $\mathbb{Q}$-automorphism of K is determined by its effect on $\sqrt[4]{2}$ and i, but must map $\sqrt[4]{2}$ to one of the four roots of $f(X)$ and must map i to $\pm i$. These choices would give us at most eight $\mathbb{Q}$-automorphisms, so they must all *be* $\mathbb{Q}$-automorphisms of K. Hence the members of $\mathrm{Gal}(K/\mathbb{Q})$ are as follows:

$$\begin{array}{rll}
\sigma\colon & \sqrt[4]{2} \mapsto i\sqrt[4]{2}, & i \mapsto i \\
\sigma^2\colon & \sqrt[4]{2} \mapsto -\sqrt[4]{2}, & i \mapsto i \\
\sigma^3\colon & \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, & i \mapsto i \\
\sigma^4 = \mathrm{id}\colon & \sqrt[4]{2} \mapsto \sqrt[4]{2}, & i \mapsto i \\
\tau\colon & \sqrt[4]{2} \mapsto \sqrt[4]{2}, & i \mapsto -i \\
\sigma\tau\colon & \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, & i \mapsto -i \\
\sigma^2\tau\colon & \sqrt[4]{2} \mapsto -\sqrt[4]{2}, & i \mapsto -i \\
\sigma^3\tau\colon & \sqrt[4]{2} \mapsto i\sqrt[4]{2}, & i \mapsto -i
\end{array}$$

The formulae for these automorphisms are calculated as follows. Write σ and τ for the maps labelled as such above. Then

$$(\sqrt[4]{2})\sigma^2 = (i\sqrt[4]{2})\sigma = (i\sigma)(\sqrt[4]{2}\sigma) = i \cdot i\sqrt[4]{2} = -\sqrt[4]{2}$$

and

$$i\sigma^2 = i$$

since $i\sigma = i$. Hence, if the first map is σ, the second map is indeed σ^2. Similar calculations apply for the other $\mathbb{Q}$-automorphisms.

Our conclusion is that $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 8 possessing an element σ of order 4 and an element τ of order 2. We also calculate that

$$\tau^{-1}\sigma\tau\colon \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, \quad i \mapsto i,$$

so

$$\tau^{-1}\sigma\tau = \sigma^3 = \sigma^{-1}.$$

Hence

$$\mathrm{Gal}(K/\mathbb{Q}) \cong D_8,$$

the dihedral group of order 8.

The Galois correspondence is a one-one inclusion-reversing correspondence between the subgroups of D_8 and the intermediate fields between $\mathbb{Q}$ and K.

For example, $\langle\sigma\rangle$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order 4, so $\langle\sigma\rangle^*$ is an intermediate field such that $|K : \langle\sigma\rangle^*| = 4$ (take $L = \langle\sigma\rangle^*$ in part (iii) of the Fundamental Theorem of Galois Theory); that is,

$$|\langle\sigma\rangle^* : \mathbb{Q}| = 2.$$

Note that i is certainly fixed by σ, so $i \in \langle\sigma\rangle^*$ and we conclude

$$\langle\sigma\rangle^* = \mathbb{Q}(i).$$

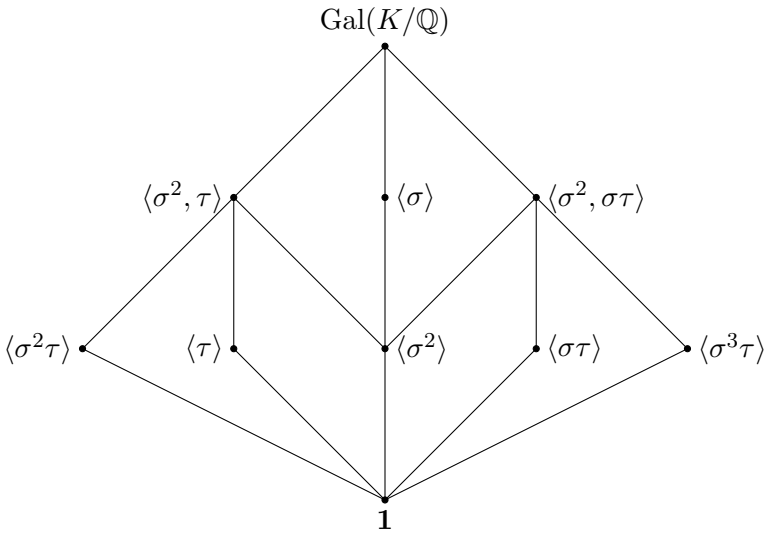
Furthermore, $\langle\sigma\rangle \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$, while $\mathbb{Q}(i)$ is the splitting field of X^2+1 over $\mathbb{Q}$, so is a normal extension of $\mathbb{Q}$ (consistent with part (iv) of the Fundamental Theorem of Galois Theory).

Similarly, $\langle\tau\rangle$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order 2, so $|\langle\tau\rangle^* : \mathbb{Q}| = 4$. Note that $\sqrt[4]{2} \in \langle\tau\rangle^*$, so

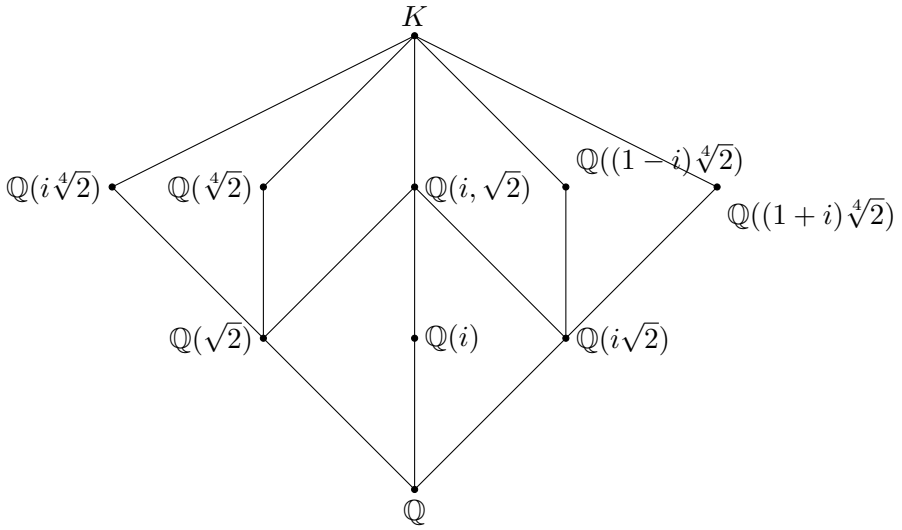
$$\langle\tau\rangle^* = \mathbb{Q}(\sqrt[4]{2}).$$

In this case, $\langle\tau\rangle$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and neither is $\mathbb{Q}(\sqrt[4]{2})$ a normal extension of $\mathbb{Q}$ (since the irreducible polynomial X^4-2 has a root in the field but does not split over $\mathbb{Q}(\sqrt[4]{2})$).

With further analysis, we can work out the subgroup lattice of $D_8 \cong \mathrm{Gal}(K/\mathbb{Q})$:



The corresponding lattice of intermediate fields is obtained by inverting the above diagram:



A general result which will help us calculate Galois groups is the following:

Lemma 6.14 *Let $f(X)$ be a polynomial over the field F, let K be the splitting field of $f(X)$ over F and let Ω be the set of roots of $f(X)$ in K. Then* $\mathrm{Gal}(K/F)$ *is isomorphic to the group of permutations that it induces on Ω.*

Since a polynomial of degree n has at most n roots in a splitting field, the above lemma has the following consequence as an immediate corollary.

Corollary 6.15 *Let $f(X)$ be a polynomial of degree n over a field F. The Galois group of $f(X)$ over F is isomorphic to a subgroup of the symmetric group S_n of degree n.* □

PROOF OF LEMMA 6.14: Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$. Any F-automorphism ϕ of K fixes the coefficients of $f(X)$ and hence, upon applying ϕ to the equation $f(\omega_i) = 0$, we conclude that ϕ must map a root of $f(X)$ to another root. Since ϕ is bijective, we conclude that ϕ induces a permutation of the finite set Ω. Hence we have a map

$$\begin{aligned} \rho\colon G &\to \mathrm{Sym}(\Omega) \\ \phi &\mapsto \phi|_\Omega. \end{aligned}$$

Since the group operation in both groups is composition, it follows that ρ is a group homomomorphism. Let $\phi \in \ker\rho$. Then $\omega_i\phi = \omega_i$ for $i = 1, 2, \ldots, n$. However, $K = F(\omega_1, \omega_2, \ldots, \omega_n)$; that is, every element of K is a sum of products involving elements from F and powers of the ω_i, so ϕ must then act as the identity on K; that is, $\phi = 1$. Thus $\ker\rho = \mathbf{1}$, ρ is injective and

$$G \cong \mathrm{im}\,\rho,$$

which is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$. □

Example 6.16 (Cubic polynomials) If $f(X)$ is a polynomial of degree 3 over $\mathbb{Q}$, then the Galois group of $f(X)$ over $\mathbb{Q}$ is isomorphic to a subgroup of the symmetric group S_3 of degree 3. We shall show that all possibilities can occur.

(i) Take $f(X) = X^3$. Then $f(X)$ splits over $\mathbb{Q}$, so the splitting field is $K = \mathbb{Q}$ and the Galois group is trivial:

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathbf{1}.$$

(ii) Take $f(X) = X^3 + X = X(X^2 + 1)$. The splitting field of $f(X)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(i)$. The Fundamental Theorem of Galois Theory tells us that

$$|\mathrm{Gal}(K/\mathbb{Q})| = |\mathbb{Q}(i) : \mathbb{Q}| = 2,$$

so

$$\mathrm{Gal}(K/\mathbb{Q}) \cong C_2,$$

a cyclic group of order 2.

(iii) Take $f(X) = X^3 - 3X - 1$. Note

$$\begin{aligned} f(X+1) &= (X+1)^3 - 3(X+1) - 1 \\ &= X^3 + 3X^2 - 3, \end{aligned}$$

which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Hence $f(X)$ is irreducible over $\mathbb{Q}$. To find the roots of the polynomial, recall the trigonometric formula

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Now if $\alpha = 2\cos\theta$ for some θ, then

$$\alpha^3 - 3\alpha = 8\cos^3\theta - 6\cos\theta = 2\cos 3\theta.$$

Hence

$$f(\alpha) = 0 \qquad \text{if and only if} \qquad \cos 3\theta = \tfrac{1}{2}.$$

It follows that the three roots of $f(X)$ in $\mathbb{C}$ are

$$\alpha = 2\cos\tfrac{\pi}{9}, \qquad \beta = 2\cos\tfrac{7\pi}{9}, \qquad \gamma = 2\cos\tfrac{13\pi}{9}.$$

Now

$$\begin{aligned}\beta = 2\cos\tfrac{7\pi}{9} &= -2\cos\tfrac{2\pi}{9}\\ &= -2\left(2\cos^2\tfrac{\pi}{9} - 1\right)\\ &= 2 - \alpha^2,\end{aligned}$$

while $\alpha+\beta+\gamma = 0$ (from the X^2 coefficient in $f(X)$). Hence $\gamma = \alpha^2 - \alpha - 2$. We conclude that the splitting field of $X^3 - 3X - 1$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\alpha)$. Then, by the Fundamental Theorem of Galois Theory,

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 3,$$

so

$$\mathrm{Gal}(K/\mathbb{Q}) \cong C_3,$$

a cyclic group of order 3.

(iv) Take $f(X) = X^3 - 2$. The splitting field of $f(X)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = \mathrm{e}^{2\pi i/3}$. Then

$$|K : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| \cdot |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 6,$$

since the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $f(X)$ and the minimum polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is $X^2 + X + 1$. Hence, combining the Fundamental Theorem of Galois Theory with Corollary 6.15, we conclude that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of order 6 inside the symmetric group S_3 of degree 3; that is,

$$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3.$$

Galois groups of finite fields

We finish this chapter by considering the Galois group of a finite field $\mathbb{F}_{p^n}$ over its prime subfield $\mathbb{F}_p$. Recall that $\mathbb{F}_{p^n}$ occurs as the splitting field of the polynomial $f(X) = X^{p^n} - X$ over $\mathbb{F}_p$, so $\mathbb{F}_{p^n}$ is a normal extension of $\mathbb{F}_p$. Also if $\alpha \in \mathbb{F}_{p^n}$, then α is a root of $f(X)$, so the minimum polynomial of α divides $X^{p^n} - X$ and hence has distinct roots. Consequently, $\mathbb{F}_{p^n}$ is also a separable extension of $\mathbb{F}_p$. We conclude that $\mathbb{F}_{p^n}$ is a finite Galois extension of $\mathbb{F}_p$ and the Fundamental Theorem of Galois Theory applies. In particular, it tells us

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = |\mathbb{F}_{p^n} : \mathbb{F}_p| = n.$$

We will construct the $\mathbb{F}_p$-automorphisms of $\mathbb{F}_{p^n}$ using the following:

Definition 6.17 The *Frobenius automorphism* γ of the finite field $\mathbb{F}_{p^n}$ of order p^n is the map $\gamma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by

$$\gamma\colon a \mapsto a^p$$

for all $a \in \mathbb{F}_{p^n}$.

First note that

$$(ab)\gamma = (ab)^p = a^p\, b^p = (a\gamma)(b\gamma)$$

and, by "Freshman's Exponentiation",

$$(a+b)\gamma = (a+b)^p = a^p + b^p = a\gamma + b\gamma$$

for all $a, b \in \mathbb{F}_{p^n}$. Hence γ is a homomorphism $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Note

$$a \in \ker \gamma \qquad \text{if and only if} \qquad a^p = 0 \qquad \text{if and only if} \qquad a = 0,$$

using the fact that a field has no zero divisors. This tells us $\ker \gamma = \mathbf{0}$ and therefore γ is an injective map. The fact that $\mathbb{F}_{p^n}$ is finite then tells us that γ is necessarily also surjective. In conclusion, γ is an automorphism of the finite field $\mathbb{F}_{p^n}$.

Furthermore, the multiplicative group $\mathbb{F}_p^*$ of the prime subfield $\mathbb{F}_p$ is cyclic of order $p-1$, so

$$a^{p-1} = 1 \qquad \text{for all } a \in \mathbb{F}_p \setminus \{0\}$$

and hence

$$a^p = a \qquad \text{for all } a \in \mathbb{F}_p;$$

that is,

$$a\gamma = a \qquad \text{for all } a \in \mathbb{F}_p.$$

In summary, we have established the following fact about the Frobenius automorphism:

Lemma 6.18 *The Frobenius automorphism γ of $\mathbb{F}_{p^n}$, given by $a\gamma = a^p$ for all $a \in \mathbb{F}_{p^n}$, is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_{p^n}$ (that is, an element of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$).* □

Note further that, for any positive integer k,

$$a\gamma^k = a^{p^k} \qquad \text{for each } a \in \mathbb{F}_{p^n}.$$

We know that every element of $\mathbb{F}_{p^n}$ satisfies $a^{p^n} = a$; that is, $a\gamma^n = a$. Hence $\gamma^n = 1$, the identity element of the Galois group. Now suppose $\gamma^k = 1$ for some positive integer k; that is,

$$a^{p^k} = a \qquad \text{for all } a \in \mathbb{F}_{p^n}.$$

Thus every element of $\mathbb{F}_{p^n}$ is a root of the polynomial $X^{p^k} - X$. Since a polynomial cannot have more roots than its degree, we conclude that $k \geqslant n$.

Hence the smallest positive integer k such that $\gamma^k = 1$ is $k = n$; that is, the order of γ, as an element of the Galois group, is precisely n. It follows that $\langle\gamma\rangle$ is a subgroup of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of order n and since the Galois group has order n, we conclude

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\gamma\rangle.$$

Thus we have established:

Theorem 6.19 *Let p be a prime number and n a positive integer. Then the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of the Galois field of order p^n over its prime subfield is cyclic of order n generated by the Frobenius automorphism γ.* □

Example 6.20 *Let α be a root of the irreducible polynomial $f(X) = X^3 + X + 1$ in some extension of the field $\mathbb{F}_2$. Express the roots of $f(X)$ in $\mathbb{F}_2(\alpha)$ in terms of the basis $\{1, \alpha, \alpha^2\}$.*

SOLUTION: Note that $f(X)$ is indeed irreducible over $\mathbb{F}_2$, since $f(0) = f(1) = 1$, so $f(X)$ has no roots and hence no linear factors over $\mathbb{F}_2$. The simple extension $\mathbb{F}_2(\alpha)$ then has degree 3 over $\mathbb{F}_2$ and consequently $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$.

The field $\mathbb{F}_2(\alpha) \cong \mathbb{F}_8$, so the Galois group $\mathrm{Gal}(\mathbb{F}_2(\alpha)/\mathbb{F}_2)$ is cyclic of order 3 generated by the Frobenius automorphism $\gamma\colon a \mapsto a^2$. The Galois group permutes the roots of the polynomial $f(X)$ and hence the roots of $f(X)$ are α, $\alpha^2 = \alpha\gamma$ and $\alpha^4 = \alpha\gamma^2$. Observe

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha.$$

Hence the roots of $X^3 + X + 1$ in $\mathbb{F}_2(\alpha)$, expressed in terms of the basis $\{1, \alpha, \alpha^2\}$, are α, α^2 and $\alpha^2 + \alpha$. □

Chapter 7

Solution of Equations by Radicals

We now establish the fact that we cannot always express the roots of a polynomial by formulae of the form similar to that of the quadratic formula. To be precise, we shall show that the splitting field of a polynomial is what is known as a radical extension if and only if the Galois group is soluble. In Example 7.14, we give an example of a polynomial whose Galois group is not soluble and hence it is not soluble by radicals.

Radical extensions

In this chapter, we consider the question of when there is a formula for the solutions of a polynomial equation analogous to the standard formula for roots of a quadratic polynomial. By a "formula" for the solution, we mean an expression of form similar, for example, to

$$\alpha = \frac{1 + \sqrt[7]{\frac{-2+\sqrt{-3}}{4+\sqrt[5]{5}}}}{2 - \sqrt[3]{17}};$$

that is, formed by repeated use of field operations and taking (various types of) roots. In order to formalize what we mean by these formulae and to make precise what we mean by "solution by radicals," we make the following definition.

Definition 7.1 (i) An extension K of a field F is said to be a *simple radical extension* if $K = F(\alpha)$ for some element $\alpha \in K$ satisfying $\alpha^p \in F$ for some prime number p.

(ii) An extension K of a field F is called a *radical extension* if there is a sequence of intermediate fields

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$

such that K_i is a simple radical extension of K_{i-1} for $i = 1, 2, \ldots, n$.

Consequently, if K is a radical extenson of F, then

$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

where, for each i, some prime power of α_i belongs in the subfield $F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$. We can therefore view α_i as being a root of an element of $F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, so every element of K can be written as a formula involving field operations and pth roots (for a variety of prime numbers p).

We make the following basic observations about radical extensions. The second part notes that there is no restriction in only permitting pth roots for prime values p in the definition of a simple radical extension.

Lemma 7.2 (i) *Suppose that K is a radical extension of F and that L is a radical extension of K. Then L is a radical extension of F.*

(ii) *Suppose $K = F(\alpha)$ where $\alpha^m \in F$ for some positive integer $m > 1$. Then K is a radical extension of F.*

(iii) *A radical extension is a finite extension.*

PROOF: (i) By assumption we have a chain of simple radical extensions from F to K and from K to L. Putting these together we get a chain of intermediate fields:

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = L$$

where each K_i is a simple radical extension of K_{i-1} and each L_j is a simple radical extension of L_{j-1}. This has the right form for us to conclude that L is a radical extension of F.

(ii) We proceed by induction on m. If m is prime, then by definition K is a simple radical extension of F and there is nothing to prove.

Otherwise $m = kp$ for some positive integer $k > 1$ and some prime p. Put $\beta = \alpha^p$ and consider the chain of subfields

$$F \subseteq F(\beta) \subseteq F(\alpha).$$

(Note $\beta \in F(\alpha)$ as $\beta = \alpha^p$, so $F(\beta) \subseteq F(\alpha)$.) Now $\beta^k = \alpha^{kp} = \alpha^m \in F$, so by induction $F(\beta)$ is a radical extension of F, while $F(\alpha)$ is a (simple) radical extension of $F(\beta)$ since $\alpha^p = \beta \in F(\beta)$. Hence, by (i), $F(\alpha)$ is a radical extension of F. This completes the induction step.

(iii) If $F(\alpha)$ is a *simple* radical extension of F, then α is a root of the polynomial $X^p - \lambda$ over F (where $\lambda = \alpha^p \in F$ and p is some prime). In particular, α is algebraic over F, so $F(\alpha)$ is of finite degree over F. Now if K is a radical extension of F, say

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$

where each K_i is a simple radical extension of K_{i-1}, then K is of finite degree over F by repeated use of the Tower Law. □

Definition 7.3 Let $f(X)$ be a polynomial over a field F of characteristic zero. We say that $f(X)$ is *soluble by radicals* if there exists a radical extension of F over which $f(X)$ splits.

Thus, $f(X)$ is soluble by radicals when the splitting field K of $f(X)$ over F is contained in some radical extension L of F. This is then consistent with what we referred to previously as a "formula for a root of a polynomial equation." If $f(X)$ is soluble by radicals, then every root is some element of a radical extension of the base field and hence can be expressed as a formula involving repeated use of field operations and pth roots (for a variety of prime numbers p).

We wish to make use of Galois groups and the Fundamental Theorem of Galois Theory in the context of solution by radicals. Accordingly we shall need to be considering normal extensions and so shall make use of the following lemma. Note that separability comes for free since we are now exclusively working over a field of characteristic zero and so can use Corollary 4.9.

Lemma 7.4 *Let K be a radical extension of a field F of characteristic zero. Then there exists an extension L of K such that L is a normal radical extension of F.*

PROOF: Let

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K \tag{7.1}$$

be a sequence of intermediate fields such that each K_i is a simple radical extension of K_{i-1}. Then there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ and prime numbers $p_1, p_2, \ldots, p_n$ such that

$$K_i = F(\alpha_1, \alpha_2, \ldots, \alpha_i) \qquad \text{and} \qquad \alpha_i^{p_i} = \lambda_i \in K_{i-1}.$$

For each i, let $f_i(X)$ be the minimum polynomial of α_i over F. We construct a chain of fields L_i as follows. Define $L_0 = F$ and then, having defined L_{i-1}, set L_i to be the splitting field of $f_i(X)$ over L_{i-1}.

Claim: Each L_i contains a subfield K_i' such that the chain of fields

$$F = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_n'$$

is the image of the chain (7.1) under an F-isomorphism $K_n \to K_n'$.

We take $K_0' = F$. Suppose that we have shown that, for some value m, each L_i with $0 \leqslant i \leqslant m-1$ contains a subfield K_i' such that

$$F = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_{m-1}'$$

is the image of the first m terms of (7.1) under some F-isomorphism $K_{m-1} \to K_{m-1}'$. Let $g(X)$ be the minimum polynomial of α_m over K_{m-1}. Then $g(X)$ divides $f_m(X)$ in the polynomial ring $K_{m-1}(X)$. Hence when we apply the F-isomorphism ϕ to the coefficients, we deduce that $g^\phi(X)$ divides $f_m(X)$ over the field K_{m-1}'. In particular, $g^\phi(X)$ splits over the field L_m. Let γ be any root of $g^\phi(X)$ in L_m. Now apply Lemma 3.5 to conclude there is an isomorphism $\psi\colon K_{m-1}(\alpha_m) \to K_{m-1}'(\gamma)$ that extends ϕ. In particular, ψ is an F-isomorphism $K_m \to K_m' = K_{m-1}'(\gamma)$ that maps the first $m+1$ terms of (7.1) to the subfields K_i' for $0 \leqslant i \leqslant m$.

By induction, the claim now follows. Furthermore, we identify each K_i with its image under the F-isomorphism $K_n \to K_n'$; that is, we may assume that we have constructed a chain of fields

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n$$

with $K_i \subseteq L_i$ for each i and such that L_i is obtained by adjoining the roots of $f_i(X)$ to L_{i-1}. As a consequence, each L_i is the splitting field of $f_1(X)\, f_2(X) \ldots f_i(X)$ over F, so is a normal extension of F (via Theorem 3.13).

Claim: Each L_i is a radical extension of F.

Again we proceed by induction on i, noting that the result is trivial for $i = 0$ since $L_0 = F$. Therefore assume L_{i-1} is a radical extension of F for some $i \geqslant 1$. We shall prove that L_i is a radical extension of F by constructing the necessary intermediate fields between L_{i-1} and L_i.

Let $\beta_1, \beta_2, \ldots, \beta_k$ be the roots of $f_i(X)$ in L_i, where $\beta_1 = \alpha_i$ without loss of generality. (This is where we use the identification made above of $K_i = K_{i-1}(\alpha_i)$ with the corresponding subfield of L_i.) Then by definition

$$L_i = L_{i-1}(\beta_1, \beta_2, \ldots, \beta_k).$$

Consider any root β_j. Since $f_i(X)$ is an irreducible polynomial over F, by Lemma 3.5, there is an isomorphism $\psi\colon F(\beta_1) \to F(\beta_j)$ such that $\psi|_F$ is the identity map $F \to F$ and $\beta_1\psi = \beta_j$. Now L_i is the splitting field for $f_1(X)\, f_2(X) \ldots f_i(X)$ over both $F(\beta_1)$ and $F(\beta_j)$ (one obtains L_i from these fields by adjoining the other roots of this product). Hence, by Theorem 3.6, there exists an isomorphism $\theta\colon L_i \to L_i$ such that $\theta|_{F(\beta_1)} = \psi$. Thus θ is an element of the Galois group $\mathrm{Gal}(L_i/F)$ and

$$\alpha_i\theta = \beta_1\theta = \beta_1\psi = \beta_j.$$

Recall that $\alpha_i^{p_i} = \lambda_i \in L_{i-1}$. Now as L_{i-1} is a normal extension of F, by Lemma 6.10 applied to the Galois group $\mathrm{Gal}(L_i/F)$,

$$L_{i-1}\theta \subseteq L_{i-1}.$$

Hence

$$\beta_j^{p_i} = (\alpha_i\theta)^{p_i} = (\alpha_i^{p_i})\theta = \lambda_i\theta \in L_{i-1}.$$

Therefore we have a chain of simple radical extensions:

$$L_{i-1} \subseteq L_{i-1}(\beta_1) \subseteq L_{i-1}(\beta_1, \beta_2) \subseteq \cdots \subseteq L_{i-1}(\beta_1, \beta_2, \ldots, \beta_k) = L_i.$$

It follows that L_i is a radical extension of L_{i-1} and, by our inductive hypothesis, also then a radical extension of F. Taking $L = L_n$, we now have the required normal radical extension of F that contains $K = K_n$. □

Soluble groups and other group theory

The key theorem of the chapter links radical extensions to what are called soluble groups. Accordingly, we need to introduce enough group theory to work with such groups. We shall omit the proofs, since they belong most naturally in a course on group theory (for example, they appear in the version of *MT5824 Topics in Groups* that I taught in some years and for which the lecture notes can be found on my webpages).

The definition we require is the following:

Definition 7.5 A group G is called *soluble* (*solvable* in the U.S.) if there are subgroups

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_d = \mathbf{1} \tag{7.2}$$

such that, for each $i = 1, 2, \ldots, d$, the subgroup G_i is normal in G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

There are multiple equivalent possible definitions for the concept of a soluble group. For example, an equivalent definition is that the derived series of G (see *MT4003*) reaches the trivial subgroup $\mathbf{1}$ after finitely many steps. The concept of commutators and derived subgroups is not essential for the Galois Theory context and we shall stick to soluble groups as given by Definition 7.5. The following observations are straightforward from the above definition:

- An abelian group is soluble: If G is abelian take $G_0 = G$ and $G_1 = \mathbf{1}$ in the definition.
- A non-abelian simple group is not soluble: If G is simple, then the only proper normal subgroup is $G_1 = \mathbf{1}$ and G is only soluble if it is abelian.

The basic properties of soluble groups that we need are the following:

Proposition 7.6 (i) *If G is soluble, then every subgroup of G is soluble.*

(ii) *If G is soluble, then every quotient group of G is soluble.*

(iii) *If N is a normal subgroup of G such that G/N and N are both soluble, then G is soluble.*

The proofs of these facts are omitted since they belong most naturally in a course on group theory. If H is a subgroup of a soluble group G with a chain of subgroups as in Equation (7.2), then the corresponding chain for H has quotients isomorphic to subgroups of the G_{i-1}/G_i, so are abelian. If N is a normal subgroup of G, then the quotients in the corresponding chain for G/N are quotients of the G_{i-1}/G_i, so are abelian. Finally, for (iii), the quotients for the chain for G are those of G/N together with those for N. (More details are found on the Problem Sheet VII.)

In the context of soluble groups, we shall also need the following observation:

Proposition 7.7 *Let G be a finite soluble group. Then G has a chain of subgroups*

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

such that, for $i = 1, 2, \ldots, n$, H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is cyclic of prime order.

PROOF: [Slightly sketched] We start with the chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_d = \mathbf{1}$$

provided by the definition of a soluble group. Suppose some quotient G_{i-1}/G_i is not simple. This means that there is a non-trivial proper normal subgroup and this corresponds to some normal subgroup N of G_{i-1} containing G_i. We then produce a new chain of subgroups

$$G = G_0 > \cdots > G_{i-1} > N > G_i > \cdots > G_d = \mathbf{1}$$

and here N/G_i is a subgroup of G_{i-1}/G_i so is abelian and, by the Third Isomorphism Theorem,

$$G_{i-1}/N \cong \frac{G_{i-1}/G_i}{N/G_i}$$

which is abelian as a quotient of an abelian group.

We repeat this process until we cannot proceed any further. (This must eventually stop since G is finite so has only finitely many subgroups.) Our final product is a chain of subgroups

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

such that each H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is both abelian and simple; that is, they are all cyclic of prime order. □

We also state one further fact from group theory that we need. For those that have covered Sylow's Theorem in a previous course can deduce it from that theorem. (It is basically an easier first case of that theorem.)

Theorem 7.8 (Cauchy's Theorem) *Let G be a finite group and p be a prime number that divides the order of G. Then G contains an element of order p.*

DEDUCTION FROM SYLOW'S THEOREM: Let P be a Sylow p-subgroup of G. The hypothesis ensures $P \neq \mathbf{1}$ and then if g is a non-identity element of P it has order p^k for some $k > 0$. Now $g^{p^{k-1}}$ has order p. □

Examples of polynomials with abelian Galois groups

When considering radical extensions of a field, we involve a number of intermediate fields, each of which is a simple radical extension of the previous one. Consequently, we shall first consider the special case of a simple radical extension $F(\alpha)$ of a field F. Here we know that $\alpha^p = \lambda$ for some $\lambda \in F$ and some prime number p. Accordingly the following two lemmas provide us with the detailed information that we need and in both cases we observe that the resulting Galois group is abelian (and hence link with our definition of soluble group above).

Lemma 7.9 *Let F be a field of characteristic zero and let K be the splitting field of $X^p - 1$ over F, where p is a prime number. Then the Galois group* $\mathrm{Gal}(K/F)$ *is abelian.*

PROOF: Let $f(X) = X^p - 1$. The formal derivative is $Df(X) = pX^{p-1}$, so $f(X)$ and $Df(X)$ has no common factors of degree $\geqslant 1$. Hence the roots of $f(X)$ in K are distinct. Consider the set Z of roots of $f(X)$ in K. If $\alpha, \beta \in Z$, then

$$(\alpha\beta)^p = \alpha^p\beta^p = 1 \qquad \text{and} \qquad (1/\alpha)^p = 1/\alpha^p = 1,$$

so Z is closed under multiplication and division. Hence Z is a subgroup of K^* of order p. As a group of prime order, it is therefore cyclic, so there is a generator ε for Z. The roots of $f(X)$ are then ε, ε^2, ..., ε^{p-1} and 1, so

$$K = F(\varepsilon).$$

Any $\phi \in \mathrm{Gal}(K/F)$ is then determined by its effect on ε and it must map ε to a root of $f(X)$; that is, to a power of ε. Let $\phi, \psi \in \mathrm{Gal}(K/F)$, say

$$\phi\colon \varepsilon \mapsto \varepsilon^i \qquad \text{and} \qquad \psi\colon \varepsilon \mapsto \varepsilon^j,$$

for some i and j. Then

$$\varepsilon\phi\psi = (\varepsilon^i)\psi = (\varepsilon\psi)^i = (\varepsilon^j)^i = \varepsilon^{ij}$$

and $\varepsilon\psi\phi = \varepsilon^{ij}$ similarly. Since these automorphisms are determined by their effect on ε, we conclude $\phi\psi = \psi\phi$, as required. □

Lemma 7.10 *Let F be a field of characteristic zero in which $X^n - 1$ splits. Let $\lambda \in F$ and let K be the splitting field for $X^n - \lambda$ over F. Then the Galois group* $\mathrm{Gal}(K/F)$ *is abelian.*

PROOF: Fix one root α of $X^n - \lambda$ in K. Since $X^n - 1$ splits over F, any other root of $X^n - \lambda$ in K has the form $\varepsilon\alpha$ where $\varepsilon \in F$ is a root of $X^n - 1$. Thus $K = F(\alpha)$.

Now any $\phi \in \mathrm{Gal}(K/F)$ is determined by its effect on α and must map α to a root of $X^n - \lambda$. Hence if $\phi, \psi \in \mathrm{Gal}(K/F)$, they have the form

$$\phi\colon \alpha \mapsto \varepsilon\alpha \qquad \text{and} \qquad \psi\colon \alpha \mapsto \eta\alpha$$

where $\varepsilon, \eta \in F$ are roots of $X^n - 1$. Now

$$\alpha\phi\psi = (\varepsilon\alpha)\psi = \varepsilon\eta\alpha,$$

since ψ fixes ε (as $\varepsilon \in F$). Similarly $\alpha\psi\phi = \varepsilon\eta\alpha$. Hence $\phi\psi = \psi\phi$, as required. □

Galois groups of normal radical extensions

We now have the ingredients needed to prove our first result about the Galois group of a normal radical extension.

Theorem 7.11 *Let F be a field of characteristic zero and K be a normal radical extension of F. Then the Galois group* $\mathrm{Gal}(K/F)$ *is soluble.*

Corollary 7.12 (Galois) *Let $f(X)$ be a polynomial over a field F of characteristic zero. If $f(X)$ is soluble by radicals then the Galois group of $f(X)$ over F is soluble.*

PROOF: By assumption, the splitting field L for $f(X)$ over F is contained in some radical extension of F. By applying Lemma 7.4, we pass to the situation where

$$F \subseteq L \subseteq K$$

and K is a *normal* radical extension of F. Theorem 7.11 then tells us that $\mathrm{Gal}(K/F)$ is a soluble group. However, L is a normal extension of F, so part (iv) of the Fundamental Theorem of Galois Theory (Theorem 6.7) tells us that

$$\mathrm{Gal}_F(f(X)) = \mathrm{Gal}(L/F) \cong \frac{\mathrm{Gal}(K/F)}{L^*},$$

which is a quotient of a soluble group, hence soluble by Proposition 7.6(ii). This establishes the corollary. □

Proof of Theorem 7.11: We proceed by induction on the degree $|K : F|$. Note that if $|K : F| = 1$, then $\mathrm{Gal}(K/F) = \mathbf{1}$, so is certainly soluble. Assume $|K : F| > 1$ and let

$$F = K_0 \subset K_1 \subset \cdots \subset K_n = K$$

be a chain of intermediate fields such that K_i is a simple radical extension of K_{i-1}, say $K_i = K_{i-1}(\alpha_i)$. We may assume that $K_i \neq K_{i-1}$ for all i. We shall now construct some normal extensions of F inside K from the element α_1 with $K_1 = F(\alpha_1)$. This will enable us to apply induction.

Suppose $\alpha_1^p = \lambda \in F$ for some prime number p and let $g(X)$ be the minimum polynomial of α_1 over F. Note that $g(X)$ divides $X^p - \lambda$. Since $g(X)$ has a root in K and K is a normal extension of F, $g(X)$ must split in K. Now $\alpha_1 \notin F$, so $\deg g(X) \geqslant 2$ and, moreover by use of Proposition 4.6, $g(X)$ is separable and so has distinct roots. Let β be a root of $g(X)$ in K with $\beta \neq \alpha_1$. Put $\varepsilon = \beta/\alpha_1$. Then $\varepsilon \neq 1$ and

$$\varepsilon^p = \beta^p/\alpha_1^p = \lambda/\lambda = 1.$$

Thus ε is an element of order p in the multiplicative group of K, so the polynomial $X^p - 1$ splits in K with roots 1, ε, ε^2, $\ldots$, ε^{p-1}. Let $L = F(\varepsilon)$, which is then the splitting field of $X^p - 1$ over F.

Then let $M = L(\alpha_1) \subseteq K$. Now the roots of $X^p - \lambda$ in K are α_1, $\varepsilon\alpha_1$, $\ldots$, $\varepsilon^{p-1}\alpha_1$, all of which belong to M. Consequently, $M = L(\alpha_1)$ is the splitting field for $X^p - \lambda$ over L (and also over F).

Now consider the chain of fields

$$F \subseteq L \subseteq M \subseteq K. \tag{7.3}$$

We first apply Lemma 7.9 to the extension $L = F(\varepsilon)$ of F and conclude that $\mathrm{Gal}(L/F)$ *is abelian.* We also apply Lemma 7.10 to the extension $M = L(\alpha_1)$ of L and conclude that $\mathrm{Gal}(M/L)$ *is abelian.* We also know that $\alpha_1 \in M$, so $M \neq F$. Hence the degree $|K : M|$ is strictly smaller than $|K : F|$. Now K is a normal extension of F, so it is a normal extension of M. Also we have

$$M = M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = K$$

where $M_i = M_{i-1}(\alpha_i)$ and some prime power of α_i lies in $K_{i-1} \subseteq M_{i-1}$. Hence K is a radical extension of M. We now apply induction to conclude that $\mathrm{Gal}(K/M)$ *is soluble.*

Now let us turn to the Galois group $G = \mathrm{Gal}(K/F)$. We shall apply the Fundamental Theorem of Galois Theory (Theorem 6.7). Applying the Galois correspondence to the fields appearing in Equation (7.3) yields subgroups of G:

$$\mathbf{1} \leqslant M^* \leqslant L^* \leqslant G,$$

where $M^* = \mathrm{Gal}(K/M)$ and $L^* = \mathrm{Gal}(K/L)$ occurring as subgroups of G. We have observed M^* is soluble. Now M is a normal extension of L (as the splitting field of $X^p - \lambda$), so by part (iv) of the Fundamental Theorem of Galois Theory, $M^* \trianglelefteqslant L^* = \mathrm{Gal}(K/L)$ and

$$L^*/M^* \cong \mathrm{Gal}(M/L),$$

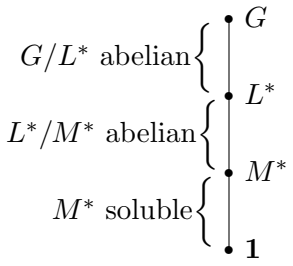


Figure 7.1: Structure of the Galois group G in Theorem 7.11

which is abelian, so soluble. Finally, L is a normal extension of F (as the splitting field of X^p-1), so $L^* \trianglelefteq G$ and

$$G/L^* \cong \mathrm{Gal}(L/F),$$

which is abelian, so soluble. The structure of the group G is illustrated in Figure 7.1. Now applying Proposition 7.6(iii) twice, we conclude that $G = \mathrm{Gal}(K/F)$ is soluble, completing the induction. □

A polynomial which is insoluble by radicals

In the example below we give an example of a polynomial that is not soluble by radicals. We do this by demonstrating that its Galois group is not soluble, with use of the following lemma, and then making use of Corollary 7.12.

Lemma 7.13 *Let p be a prime and $f(X)$ be an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose that $f(X)$ has precisely two non-real roots in $\mathbb{C}$. Then the Galois group of $f(X)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p of degree p.*

Proof: By adjoining the roots of $f(X)$ found in $\mathbb{C}$, we can construct a splitting field K for $f(X)$ contained in $\mathbb{C}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$, the Galois group of $f(X)$ over $\mathbb{Q}$. By Lemma 6.14, we may regard G as a subgroup of the symmetric group on Ω, the set of roots of $f(X)$ in K. We know $|\Omega| = p$, so the symmetric group on Ω is (isomorphic to) S_p.

Now by part (i) of the Fundamental Theorem of Galois Theory (Theorem 6.7),

$$|G| = |K : \mathbb{Q}|.$$

Let α be one of the roots of $f(X)$. Then $|K : \mathbb{Q}|$ is divisible by $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f(X) = p$. Hence, by Cauchy's Theorem, G possesses an element of order p. However, an element of order p in S_p must be a p-cycle, so G contains a p-cycle σ. By taking a suitable power of σ, we can assume that $\sigma = (\alpha_1\ \alpha_2 \ldots \alpha_p)$ where α_1 and α_2 are the two non-real roots of $f(X)$.

Observe, in addition, that complex conjugation must permute the roots of $f(X)$, so induces some $\mathbb{Q}$-automorphism τ in G. This must fix the $p-2$ real roots of $f(X)$ and hence must swap the two non-real roots. Thus τ is the transposition $(\alpha_1\ \alpha_2)$.

Now we know that $(\alpha_1\ \alpha_2)$ and $(\alpha_1\ \alpha_2 \ldots \alpha_p)$ generate the symmetric group S_p and hence we conclude $G = S_p$. □

Example 7.14 *The quintic polynomial $f(X) = X^5 - 9X + 3$ over $\mathbb{Q}$ is not soluble by radicals.*

Proof: By Eisenstein's Criterion (with $p = 3$), $f(X)$ is irreducible over $\mathbb{Q}$. Now

$$f(-2) = -11, \qquad f(-1) = 11, \qquad f(1) = -5, \qquad f(2) = 17.$$

Hence, by the Intermediate Value Theorem, $f(X)$ has at least three real roots (one between -2 and -1, one between -1 and 1 and one between 1 and 2). The derivative of $f(X)$ is

$$f'(X) = 5X^4 - 9,$$

so $f'(X)$ has exactly two real roots, so $f(X)$ has two turning points. There must be a turning point between every pair of real roots (Rolle's Theorem), so $f(X)$ has *exactly* three real roots and therefore two non-real roots. Now Lemma 7.13 tells us that

$$\mathrm{Gal}_F(f(X)) \cong S_5,$$

the symmetric group of degree 5. Now the alternating group A_5 is a non-abelian simple group and is therefore not soluble. Hence, using Proposition 7.6(i), the Galois group of $f(X)$ over $\mathbb{Q}$ is not soluble and, by Corollary 7.12, $f(X)$ is not soluble by radicals. □

Thus for this particular quintic polynomial, we cannot express the roots using formulae involving field operations and pth roots.

Galois's Great Theorem

We finish the chapter by establish the converse of Corollary 7.12; that is, we shall show that if the Galois group of a polynomial is soluble then the polynomial is soluble by radicals. We begin with a special case in Lemma 7.16, which can be viewed as a base step of an induction argument, but we first need a technical result in the middle.

Lemma 7.15 *Let K be a finite normal extension of a field F of characteristic zero, let $\varepsilon \in F$ and suppose that $\mathrm{Gal}(K/F)$ is cyclic of order p generated by some F-automorphism ϕ. Then there exists some $x \in K$ such that*

$$x + \varepsilon(x\phi) + \varepsilon^2(x\phi^2) + \cdots + \varepsilon^{p-1}(x\phi^{p-1}) \neq 0.$$

Proof: We actually prove a stronger assertion: Namely we claim that there does not exist non-zero scalars $\lambda_0, \lambda_1, \ldots, \lambda_{p-1}$ in K such that

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_{p-1}(x\phi^{p-1}) = 0$$

for all $x \in K$. Suppose for a contraduction that such non-zero scalars λ_i exist. Choose n to be as small as possible such that there exist non-zero $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ with

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_n(x\phi^n) = 0 \tag{7.4}$$

for all $x \in K$. Our assumption ensures $n \leqslant p-1$, while $n \geqslant 1$ since K is a field.

Since $n \leqslant p-1$, the automorphism ϕ^n is not the identity and so we can choose $y \in K$ with $y\phi^n \neq y$. Note that successive application of ϕ permutes the elements of $\{y, y\phi, y\phi^2, \ldots, y\phi^{p-1}\}$ in a cycle of length p. In particular, since p is prime, these elements must be distinct.

Substitute yx for x in the above equation (7.4). We use the fact that ϕ and all its powers are automorphisms to conclude

$$\lambda_0 yx + \lambda_1(y\phi)(x\phi) + \cdots + \lambda_n(y\phi^n)(x\phi^n) = 0 \tag{7.5}$$

for all $x \in K$. Now multiply Equation (7.4) by $y\phi^n$ and subtract Equation (7.5) to deduce

$$\lambda_0(y\phi^n - y)x + \lambda_1(y\phi^n - y\phi)(x\phi) + \cdots + \lambda_{n-1}(y\phi^n - y\phi^{n-1})(x\phi^n) = 0$$

for all $x \in K$. Since the images of y under the powers of ϕ are distinct, the coefficients $\mu_i = \lambda_i(y\phi^n - y\phi^i)$ are non-zero and we now have an equation

$$\mu_0 x + \mu_1(x\phi) + \cdots + \mu_{n-1}(x\phi^n) = 0$$

for all $x \in K$. This contradicts our minimality choice of n.

In conclusion, there does not exist non-zero scalars λ_i satisfying

$$\lambda_0 x + \lambda_1(x\phi) + \cdots + \lambda_{p-1}(x\phi^{p-1}) = 0$$

for all $x \in K$. In particular, taking $\lambda_i = \varepsilon^i$, there exists some $x \in K$ such that

$$x + \varepsilon(x\phi) + \cdots + \varepsilon^{p-1}(x\phi^{p-1}) \neq 0.$$

□

Lemma 7.16 *Let K be a finite normal extension of a field F of characteristic zero and suppose that $X^p - 1$ splits in F (for some prime p). If $\mathrm{Gal}(K/F)$ is cyclic of order p then $K = F(\alpha)$ for some α satisfying $\alpha^p \in F$.*

Thus the lemma shows that, under the given hypotheses, K is a simple radical extension of F.

PROOF: By the Theorem of the Primitive Element (Theorem 4.11), $K = F(\beta)$ for some $\beta \in F$. We know that the roots of $X^p - 1$ in K are 1, ε, ε^2, $\ldots$, ε^{p-1} for some $\varepsilon \in F$. Let ϕ be a generator for $G = \mathrm{Gal}(K/F)$. Use Lemma 7.15 to produce $x \in K$ such that

$$\alpha = x + \varepsilon(x\phi) + \varepsilon^2(x\phi^2) + \cdots + \varepsilon^{p-1}(x\phi^{p-1}) \neq 0.$$

Then, noting $\varepsilon\phi = \varepsilon$ since ϕ is an F-automorphism and $\varepsilon \in F$,

$$\alpha\phi = x\phi + \varepsilon(x\phi^2) + \varepsilon^2(x\phi^3) + \cdots + \varepsilon^{p-1}x = \varepsilon^{-1}\alpha,$$

so

$$(\alpha^p)\phi = (\alpha\phi)^p = (\varepsilon^{-1}\alpha)^p = \alpha^p.$$

Hence $\alpha^p \in \mathrm{Fix}_K(G) = F$ (by Lemma 6.8).

Since $\varepsilon \neq 1$ and $\alpha \neq 0$, we have $\alpha\phi \neq \alpha$, so $\alpha \notin F$. Thus

$$F \subsetneq F(\alpha) \subseteq K.$$

Now by part (i) of the Fundamental Theorem of Galois Theory (Theorem 6.7),

$$|K : F| = |G| = p$$

so, using the Tower Law, $F(\alpha) = K$, as required. □

Theorem 7.17 (Galois's Great Theorem) *Let $f(X)$ be a polynomial over a field F of characteristic zero. Then $f(X)$ is soluble by radicals if and only if the Galois group of $f(X)$ over F is soluble.*

PROOF: One direction of this theorem is, of course, already established as Corollary 7.12. It remains to establish the converse.

Let K be the splitting field of $f(X)$ over F and assume that $G = \mathrm{Gal}(K/F)$ is a soluble group. We shall establish the existence of a radical extension of F that contains the splitting field K. We proceed by induction on the order of G. If $G = \mathbf{1}$, then $K = F$ (by part (i) of

the Fundamental Theorem of Galois Theory (Theorem 6.7)) and certainly then K is a radical extension of F.

Assume then that G is non-trivial and let

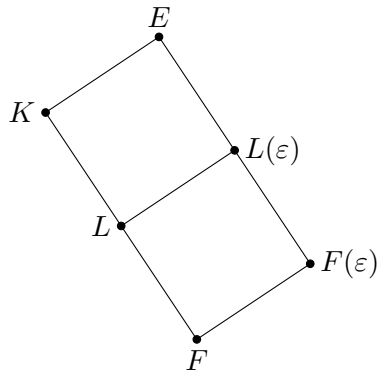
$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

be a chain of subgroups as provided by Proposition 7.7. Thus we are assuming, in particular, G_1 is a normal subgroup of G and G/G_1 is a cyclic group of order p for some prime p. Let

$$L = G_1^* = \mathrm{Fix}_K(G_1).$$

Now $G_1 = G_1^{**} = L^* = \mathrm{Gal}(K/L)$, by the Galois Correspondence (part (ii) of the Fundamental Theorem). Since G_1 is a proper subgroup of G, we may apply induction to conclude that there is a radical extension E of L containing K. By adjoining an element $\varepsilon \neq 1$ such that $\varepsilon^p = 1$ to E, if necessary, we may also assume that $X^p - 1$ splits in E.

The situation now is that we have various fields as shown in the following diagram:



We shall complete the proof by showing that E is a radical extension of F.

Now E is a radical extension of L, so it is certainly a radical extension of $L(\varepsilon)$ (by adjoining the same elements to $L(\varepsilon)$ as were adjoined to L to construct the intermediate fields). By construction, $F(\varepsilon)$ is a simple radical extension of F, so we need to show $L(\varepsilon)$ is a radical extension of $F(\varepsilon)$.

As G_1 is a normal subgroup of G, we know L is a normal extension of F (by part (iv) of the Fundamental Theorem of Galois Theory (Theorem 6.7)), so it is the splitting field for some polynomial $g(X)$ over F. Hence $L(\varepsilon)$ is the splitting field for $g(X)$ over $F(\varepsilon)$, so $L(\varepsilon)$ is a normal extension of $F(\varepsilon)$. Now

$$|L(\varepsilon) : F| = |L(\varepsilon) : F(\varepsilon)| \cdot |F(\varepsilon) : F| = |L(\varepsilon) : L| \cdot |L : F|,$$

by two applications of the Tower Law (Theorem 2.4), and so $p = |G|/|L^*| = |L : F|$ divides $|L(\varepsilon) : F(\varepsilon)| \cdot |F(\varepsilon) : F|$. Now, since $\varepsilon^p = 1$ and $\varepsilon \neq 1$, the minimum polynomial of ε over F divides

$$X^{p-1} + X^{p-2} + \cdots + X + 1,$$

so $|F(\varepsilon) : F| \leqslant p - 1$. We deduce that p divides $|L(\varepsilon) : F(\varepsilon)|$.

On the other hand, by use of the Theorem of the Primitive Element (Theorem 4.11), $L = F(\alpha)$ for some α and then $L(\varepsilon) = F(\varepsilon, \alpha)$. The minimum polynomial of α over $F(\varepsilon)$ divides that over F, so $|L(\varepsilon) : F(\varepsilon)| \leqslant |L : F| = p$.

Hence $|L(\varepsilon) : F(\varepsilon)| = p$ and we see that $\mathrm{Gal}(L(\varepsilon)/F(\varepsilon))$ is cyclic of order p (using part (i) of the Fundamental Theorem of Galois Theory). Now Lemma 7.16 shows $L(\varepsilon)$ is a simple radical extension of $F(\varepsilon)$, which completes the proof of the theorem. □