Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/∼aknapp

Title: Basic Algebra
Cover: Construction of a regular heptadecagon, the steps shown in color sequence; see page 505.

Mathematics Subject Classification (2010): 15–01, 20–01, 13–01, 12–01, 16–01, 08–01, 18A05, 68P30.

First Edition, ISBN-13 978-0-8176-3248-9
c 2006 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
c 2016 Anthony W. Knapp
Published by the Author

CHAPTER IX

Fields and Galois Theory

Abstract. This chapter develops some general theory for field extensions and then goes on to study Galois groups and their uses. More than half the chapter illustrates by example the power and usefulness of the theory of Galois groups. Prerequisite material from Chapter VIII consists of Sections 1–6 for Sections 1–13 of the present chapter, and it consists of all of Chapter VIII for Sections 14–17 of the present chapter.

Sections 1–2 introduce field extensions. These are inclusions of a base field in a larger field. The fundamental construction is of a simple extension, algebraic or transcendental, and the next construction is of a splitting field. An algebraic simple extension is made by adjoining a root of an irreducible polynomial over the base field, and a splitting field is made by adjoining all the roots of such a polynomial. For both constructions, there are existence and uniqueness theorems.

Section 3 classifies finite fields. For each integer q that is a power of some prime number, there exists one and only one finite field of order q, up to isomorphism. One finite field is an extension of another, apart from isomorphisms, if and only if the order of the first field is a power of the order of the second field.

Section 4 concerns algebraic closure. Any field has an algebraic extension in which each nonconstant polynomial over the extension field has a root. Such a field exists and is unique up to isomorphism.

Section 5 applies the theory of Sections 1–2 to the problem of constructibility with straightedge and compass. First the problem is translated into the language of field theory. Then it is shown that three desired constructions from antiquity are impossible: "doubling a cube," trisecting an arbitrary constructible angle, and "squaring a circle." The full proof of the impossibility of squaring a circle uses the fact that π is transcendental over the rationals, and the proof of this property of π is deferred to Section 14. Section 5 concludes with a statement of the theorem of Gauss identifying integers n such that a regular n-gon is constructible and with some preliminary steps toward its proof.

Sections 6–8 introduce Galois groups and develop their theory. The theory applies to a field extension with three properties—that it is finite-dimensional, separable, and normal. Such an extension is called a "finite Galois extension." The Fundamental Theorem of Galois Theory says in this case that the intermediate extensions are in one-one correspondence with subgroups of the Galois group, and it gives formulas relating the corresponding intermediate fields and Galois subgroups.

Sections 9–11 give three standard initial applications of Galois groups. The first is to proving the theorem of Gauss about constructibility of regular n-gons, the second is to deriving the Fundamental Theorem of Algebra from the Intermediate Value Theorem, and the third is to proving the necessity of the condition of Abel and Galois for solvability of polynomial equations by radicals—that the Galois group of the splitting field of the polynomial have a composition series with abelian quotients.

Sections 12–13 begin to derive quantitative information, rather than qualitative information, from Galois groups. Section 12 shows how an appropriate Galois group points to the specific steps in the construction of a regular n-gon when the construction is possible. Section 13 introduces a tool

known as Lagrange resolvents, a precursor of modern harmonic analysis. Lagrange resolvents are used first to show that Galois extensions in characteristic 0 with cyclic Galois group of prime order p are simple extensions obtained by adjoining a p^{th} root, provided all the p^{th} roots of 1 lie in the base field. Lagrange resolvents and this theorem about cyclic Galois groups combine to yield a derivation of Cardan's formula for solving general cubic equations.

Section 14 begins the part of the chapter that depends on results in the later sections of Chapter VIII. Section 14 itself contains a proof that π is transcendental; the proof is a nice illustration of the interplay of algebra and elementary real analysis.

Section 15 introduces the field polynomial of an element in a finite-dimensional extension field. The determinant and trace of this polynomial are called the norm and trace of the element. The section gives various formulas for the norm and trace, including formulas involving Galois groups. With these formulas in hand, the section concludes by completing the proof of Theorem 8.54 about extending Dedekind domains, part of the proof having been deferred from Section VIII.11.

Section 16 discusses how prime ideals split when one passes, for example, from the integers to the algebraic integers in a number field. The topic here was broached in the motivating examples for algebraic number theory and algebraic geometry as introduced in Section VIII.7, and it was the main topic of concern in that section. The present results put matters into a wider context.

Section 17 gives two tools that sometimes help in identifying Galois groups, particularly of splitting fields of monic polynomials with integer coefficients. One tool uses the discriminant of the polynomial. The other uses reduction of the coefficients modulo various primes.

1. Algebraic Elements

If $\mathbb{K}$ and $\Bbbk$ are fields such that $\Bbbk$ is a subfield of $\mathbb{K}$, we say that $\mathbb{K}$ is a **field extension** of $\Bbbk$. When it is necessary to refer to this situation in some piece of notation, we often write $\mathbb{K}/\Bbbk$ to indicate the field extension. In this section we shall study field extensions in a general way, and in the next section we shall discuss constructions and uniqueness results involving them.

If $\mathbb{K}$ and $\mathbb{K}'$ are two fields and if φ is a ring homomorphism of $\mathbb{K}$ into $\mathbb{K}'$ with $\varphi(1) = 1$, then φ is automatically one-one since $\mathbb{K}$ has no nontrivial ideals. We refer to φ as a **field map** or **field mapping**.[1] If $\mathbb{K}$ and $\mathbb{K}'$ are both field extensions of a field $\Bbbk$ and if the restriction of a field map φ to $\Bbbk$ is the identity, then φ is called a $\Bbbk$ **field map** or a **field map fixing** $\Bbbk$. The terminology "$\Bbbk$ field map" is consistent with the view that $\mathbb{K}$ and $\mathbb{K}'$ are two R algebras for $R = \Bbbk$ in the sense of Examples 6 and 15 in Section VIII.1, and that the isomorphism in question is just an R algebra isomorphism.

If a field map $\varphi : \mathbb{K} \to \mathbb{K}'$ is onto $\mathbb{K}'$, then φ is a **field isomorphism**; it is a $\Bbbk$ **field isomorphism** if $\mathbb{K}$ and $\mathbb{K}'$ are extensions of $\Bbbk$ and φ is the identity on $\Bbbk$. When $\mathbb{K} = \mathbb{K}'$ and φ is onto $\mathbb{K}'$, φ is called an **automorphism** of $\mathbb{K}$; if also φ is the identity on a subfield $\Bbbk$, then φ is called a $\Bbbk$ **automorphism** of $\mathbb{K}$.

[1] This is the notion of morphism in the category of fields.

Throughout this section we let $\mathbb{K}/\Bbbk$ be a field extension. If $x_1, \dots, x_n$ are members of $\mathbb{K}$, we let

$$\Bbbk[x_1, \dots, x_n] = \text{subring of } \mathbb{K} \text{ generated by } 1 \text{ and } x_1, \dots, x_n,$$
$$\Bbbk(x_1, \dots, x_n) = \text{subfield of } \mathbb{K} \text{ generated by } 1 \text{ and } x_1, \dots, x_n.$$

The latter, in more detail, means the set of all quotients ab^{-1} with a and b in $\Bbbk[x_1, \dots, x_n]$ and with $b \neq 0$. It is referred to as the **field obtained by adjoining** $x_1, \dots, x_n$ to $\Bbbk$. Because of this description of the elements of $\Bbbk(x_1, \dots, x_n)$, the field $\Bbbk(x_1, \dots, x_n)$ can be regarded as the field of fractions $\mathbb{F}$ of $\Bbbk[x_1, \dots, x_n]$. In fact, we argue as follows: let $\eta : \Bbbk[x_1, \dots, x_n] \to \mathbb{F}$ be the natural ring homomorphism $a \mapsto$ class of $(a, 1)$ of $\Bbbk[x_1, \dots, x_n]$ into its field of fractions; then the universal mapping property of $\mathbb{F}$ stated in Proposition 8.6 gives a factorization of the inclusion $\iota : \Bbbk[x_1, \dots, x_n] \to \Bbbk(x_1, \dots, x_n)$ as $\iota = \widetilde{\iota}\eta$, and the field mapping $\widetilde{\iota}$ has to be onto $\Bbbk(x_1, \dots, x_n)$ since the class of (a, b) maps to the member ab^{-1} of $\Bbbk(x_1, \dots, x_n)$.

As in Chapter IV and elsewhere, we let $\Bbbk[X]$ be the ring of polynomials in the indeterminate X with coefficients in $\Bbbk$. For each x in $\mathbb{K}$, we have a unique substitution homomorphism $\varphi_x : \Bbbk[X] \to \Bbbk[x]$ carrying $\Bbbk$ to itself and carrying X to x. We say that x is **algebraic** over $\Bbbk$ if φ_x is not one-one, i.e., if x is a root of some nonzero polynomial in $\Bbbk[X]$, and that x is **transcendental** over $\Bbbk$ if φ_x is one-one.

EXAMPLES.

(1) If $\Bbbk = \mathbb{R}$, if $\mathbb{K} = \mathbb{C}$, and if x is the usual element $i = \sqrt{-1}$, then $\varphi_i(X^2 + 1) = 0$, and i is algebraic over $\mathbb{R}$.

(2) If $\Bbbk = \mathbb{Q}$, if $\mathbb{K} = \mathbb{C}$, and if θ is a complex number with the property that $\theta^n + c_{n-1}\theta^{n-1} + \cdots + c_1\theta + c_0 = 0$ for some n and for some coefficients in $\mathbb{Q}$, then θ is algebraic over $\mathbb{Q}$. This situation was the subject of Proposition 4.1, of Example 2 in Section IV.4, and of Example 10 in Section VIII.1.

(3) Let $\Bbbk = \mathbb{Q}$ and $\mathbb{K} = \mathbb{C}$. For π equal to the usual trigonometric constant, given as the least positive real such that $e^{i\pi} = -1$ when $e^z = \sum_{n=0}^{\infty} z^n/n!$, it will be proved in Section 14 that there is no polynomial $F(X)$ in $\mathbb{Q}[X]$ with $F(\pi) = 0$, and π is consequently transcendental over $\mathbb{Q}$.

(4) If $\Bbbk = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{K}$ is the 4-element field constructed in Example 3 of fields in Section IV.4, then any element of $\mathbb{K}$ is algebraic over $\Bbbk$.

(5) If $\Bbbk = \mathbb{C}(X)$ and if $\mathbb{K} = \mathbb{C}(X)[\sqrt{(X-1)X(X+1)}\,]$ as with the ring R' in Section VIII.7 and as in Example 3 of integral closures in Section VIII.9, then $\sqrt{(X-1)X(X+1)}$ is algebraic over $\mathbb{C}(X)$.

Suppose that x in $\mathbb{K}$ is algebraic over $\Bbbk$. Then

$$\ker \varphi_x = \{F(X) \in \Bbbk[X] \mid F(x) = 0\}$$

is an ideal in $\Bbbk[X]$ that is necessarily nonzero and principal. A generator is determined up to a constant factor as any nonzero polynomial in the ideal that has lowest possible degree, and we might as well take this polynomial to be monic. Thus $\ker \varphi_x$ is of the form $(F_0(X))$ for some unique monic polynomial $F_0(X)$, and this polynomial $F_0(X)$ is called the **minimal polynomial** of x over $\Bbbk$. Review of the example at the end of Section VIII.3 may help motivate the first five results below.

Proposition 9.1 If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the minimal polynomial of x over $\Bbbk$ is prime as a polynomial in $\mathbb{K}[X]$.

PROOF. Suppose that $F(X)$ factors nontrivially as $F(X) = G(X)H(X)$. Since $F(x) = 0$, either $G(x) = 0$ or $H(x) = 0$, and then we have a contradiction to the fact that F has minimal degree among all polynomials vanishing at x. □

Theorem 9.2. If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the field $\Bbbk(x)$ coincides with the ring $\Bbbk[x]$. Moreover, if the minimal polynomial of x over $\Bbbk$ has degree n, then each element of $\Bbbk(x)$ has a unique expansion as

$$c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0 \qquad \text{with all } c_i \in \Bbbk.$$

PROOF. Since the substitution ring homomorphism φ_x carries $\Bbbk[X]$ onto $\Bbbk[x]$, we have an isomorphism of rings $\Bbbk[x] \cong \Bbbk[X]/\ker \varphi_x = \Bbbk[X]/(F_0(X))$, where $F_0(X)$ is the minimal polynomial of x over $\Bbbk$. Since F_0 is prime, $(F_0(X))$ is a nonzero prime ideal and hence is maximal. Thus $\Bbbk[x]$ is a field. Consequently $\Bbbk(x) = \Bbbk[x]$.

Any element in $\Bbbk[x]$, hence in $\Bbbk(x)$, is a polynomial in x. Since $F_0(x) = 0$, we can solve $F_0(x) = 0$ for its leading term, say x^n, obtaining $x^n = G(x)$, where $G(X) = 0$ or $\deg G(X) \leq n - 1$. Thus the expansions in the statement of the theorem yield all the members of $\Bbbk[x]$. If an element has two such expansions, we subtract them and obtain a nonzero polynomial $H(X)$ of degree at most $n - 1$ with $H(x) = 0$, in contradiction to the minimality of the degree of $F_0(X)$. □

Corollary 9.3. If $x \in \mathbb{K}$ is algebraic over $\Bbbk$, then the field $\Bbbk(x)$, regarded as a vector space over $\Bbbk$, is of dimension n, where n is the degree of the minimal polynomial of x over $\Bbbk$. The elements $1, x, x^2, \ldots, x^{n-1}$ form a basis of $\Bbbk(x)$ over $\Bbbk$.

PROOF. This is just a restatement of the second conclusion of Theorem 9.2. □

We say that the field extension $\mathbb{K}/\Bbbk$ is an **algebraic extension** if every element of $\mathbb{K}$ is algebraic over $\Bbbk$.

Proposition 9.4. If the vector-space dimension of $\mathbb{K}$ over $\Bbbk$ is some finite n, then $\mathbb{K}$ is an algebraic extension of $\Bbbk$, and each element x of $\mathbb{K}$ has some nonzero polynomial $F(X)$ in $\Bbbk[X]$ of degree at most n for which $F(x) = 0$.

PROOF. This is immediate since the elements $1, x, x^2, \dots, x^n$ of $\mathbb{K}$ have to be linearly dependent over $\Bbbk$. □

When $\mathbb{K}/\Bbbk$ is a field extension, we write $[\mathbb{K} : k]$ for the vector-space dimension $\dim_{\Bbbk} \mathbb{K}$, and we call this the **degree** of $\mathbb{K}$ over $\Bbbk$. If $[\mathbb{K} : \Bbbk]$ is finite, we say that $\mathbb{K}$ is a **finite extension** of $\Bbbk$, or **finite algebraic extension** of $\Bbbk$, the condition "algebraic" being automatic by Proposition 9.4.

Corollary 9.5. If x is in $\mathbb{K}$, then x is algebraic over $\Bbbk$ if and only if $\Bbbk(x)$ is a finite algebraic extension of $\Bbbk$. In this case the minimal polynomial of x over $\Bbbk$ has degree $[\Bbbk(x) : \Bbbk]$.

PROOF. If x is algebraic over $\Bbbk$, then $[\Bbbk(x) : \Bbbk]$ is finite and is the degree of the minimal polynomial of x over $\Bbbk$, by Corollary 9.3. Proposition 9.4 shows in this case that $\Bbbk(x)$ is a finite algebraic extension. If x is transcendental over $\Bbbk$, then the substitution homomorphism φ_x is one-one, and $\dim_{\Bbbk} \Bbbk(x) \geq \dim_{\Bbbk} \Bbbk[X] = +\infty$. □

Theorem 9.6. Let $\Bbbk$, $\mathbb{K}$, and $\mathbb{L}$ be fields with $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$, and suppose that $[\mathbb{K} : \Bbbk] = n$ and $[\mathbb{L} : \mathbb{K}] = m$, finite or infinite. Let $\{\omega_1, \omega_2, \dots\}$ be a vector-space basis of $\mathbb{K}$ over $\Bbbk$, and let $\{\xi_1, \xi_2, \dots\}$ be a vector-space basis of $\mathbb{L}/\mathbb{K}$. Then the mn products $\omega_i \xi_j$ form a basis of $\mathbb{L}$ over $\Bbbk$.

PROOF OF SPANNING. If ξ is in $\mathbb{L}$, write $\xi = \sum_j a_j \xi_j$ with each a_j in $\mathbb{K}$ and with only finitely many a_j's not 0. Then expand each a_j in terms of the ω_i's, and substitute. □

PROOF OF LINEAR INDEPENDENCE. Let $\sum_{i,j} c_{ij} \omega_i \xi_j = 0$ with the c_{ij}'s in $\Bbbk$. Since the members ξ_j of $\mathbb{L}$ are linearly independent over $\mathbb{K}$, $\sum_i c_{ij} \omega_i = 0$ for each j. Since the members ω_i of $\mathbb{K}$ are linearly independent over $\Bbbk$, $c_{ij} = 0$ for all i and j. □

Corollary 9.7. If $\Bbbk$, $\mathbb{K}$, and $\mathbb{L}$ are fields with $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$, then

$$\boxed{[\mathbb{L} : \Bbbk] = [\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \Bbbk]\,.}$$

PROOF. This is immediate by counting basis elements in Theorem 9.6. □

Theorem 9.8. If $\mathbb{K}/\Bbbk$ is a field extension and if $x_1, \dots, x_n$ are members of $\mathbb{K}$ that are algebraic over $\Bbbk$, then $\Bbbk(x_1, \dots, x_n)$ is a finite algebraic extension of $\Bbbk$.

REMARK. If a finite algebraic extension of $\Bbbk$ turns out to be of the form $\Bbbk(x)$ for some x, we say that the extension is a **simple algebraic extension**.

PROOF. Since x_i is algebraic over $\Bbbk$, it is algebraic over $\Bbbk(x_1, \dots, x_{i-1})$. Hence $[\Bbbk(x_1, \dots, x_i) : \Bbbk(x_1, \dots, x_{i-1})]$ is finite. Applying Corollary 9.7 repeatedly, we see that $\Bbbk(x_1, \dots, x_n)$ is a finite extension of $\Bbbk$. Proposition 9.4 shows that it is a finite algebraic extension. □

EXAMPLE. The sum $\sqrt{2}+\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$, as a consequence of Theorem 9.8. This fact suggests Corollary 9.9 below.

Corollary 9.9 If $\mathbb{K}/\Bbbk$ is a field extension, then the elements of $\mathbb{K}$ that are algebraic over $\Bbbk$ form a field.

PROOF. If x and y in $\mathbb{K}$ are algebraic over $\Bbbk$, then $\Bbbk(x, y)$ is a finite algebraic extension of $\Bbbk$, according to Theorem 9.8. This extension contains $x \pm y$ and xy, and it contains x^{-1} if $x \neq 0$. The corollary therefore follows from Proposition 9.4. □

For the special case of Corollary 9.9 in which $\mathbb{K} = \mathbb{C}$ and $\Bbbk = \mathbb{Q}$, this subfield of $\mathbb{C}$ is called the field of **algebraic numbers**, and any finite algebraic extension of $\mathbb{Q}$ within $\mathbb{C}$ is called a **number field**, or an **algebraic number field**. The seeming discrepancy between this definition and the definition given in remarks with Proposition 4.1 (that in essence a "number field" is any simple algebraic extension of $\mathbb{Q}$) will be resolved by the Theorem of the Primitive Element (Theorem 9.34 below).

2. Construction of Field Extensions

In this section, $\Bbbk$ denotes any field. Our interest will be in constructing extension fields for $\Bbbk$ and in addressing the question of uniqueness under additional hypotheses. We begin with a kind of converse to Proposition 9.1 that generalizes the method described in Section A4 of the appendix for constructing $\mathbb{C} = \mathbb{R}(\sqrt{-1}\,)$ from $\mathbb{R}$ and the polynomial $X^2 + 1$.

Theorem 9.10 (existence theorem for simple algebraic extensions). If $F(X)$ is a monic prime polynomial in $\Bbbk[X]$, then there exists a simple algebraic extension $\mathbb{K} = \Bbbk(x)$ of $\Bbbk$ such that x is a root of $F(X)$. Moreover, $F(X)$ is the minimal polynomial of x over $\Bbbk$.

PROOF. Define $\mathbb{K} = \Bbbk[X]/(F(X))$ as a ring. Since $F(X)$ is prime, $(F(X))$ is a nonzero prime ideal, hence maximal. Therefore $\mathbb{K}$ is a field, an extension field of $\Bbbk$. Define x to be the coset $X + (F(X))$. Then $F(x) = F(X) + (F(X)) = 0 + (F(X))$, and x is therefore algebraic over $\Bbbk$. It is immediate that $\mathbb{K} = \Bbbk[x]$, and Theorem 9.2 shows that $\mathbb{K} = \Bbbk(x)$. If $G(x) = 0$ for some $G(X)$ in $\Bbbk[X]$, then $G(X)$ is in $(F(X))$. We conclude that $F(X)$ has minimal degree among all polynomials with x as a root, and $F(X)$ is therefore the minimal polynomial. □

Theorem 9.11 (uniqueness theorem for simple algebraic extensions). If $F(X)$ is a monic prime polynomial in $\Bbbk[X]$ and if $\mathbb{K} = \Bbbk(x)$ and $\mathbb{K}' = \Bbbk(y)$ are two simple algebraic extensions such that x and y are roots of $F(X)$, then there exists a field isomorphism φ of $\mathbb{K}$ onto $\mathbb{K}'$ fixing $\Bbbk$ and carrying x to y.

EXAMPLE. The monic polynomial $F(X) = X^3 - 2$ is prime in $\mathbb{Q}[X]$, and $x = \sqrt[3]{2}$ and $y = e^{2\pi i/3}\sqrt[3]{2}$ are roots of it within $\mathbb{C}$. The fields $\mathbb{Q}(x)$ and $\mathbb{Q}(y)$ are subfields of $\mathbb{C}$ and are distinct because $\mathbb{Q}(x)$ is contained in $\mathbb{R}$ and $\mathbb{Q}(y)$ is not. Nevertheless, these fields are $\mathbb{Q}$ isomorphic, according to the theorem.

PROOF. In view of the proof of Theorem 9.10, there is no loss of generality in assuming that $\mathbb{K} = \Bbbk[X]/(F(X))$. Since y is algebraic over $\Bbbk$, we can form the substitution homomorphism $\varphi_y : \Bbbk[X] \to \Bbbk(y)$. This is a $\Bbbk$ algebra homomorphism. Its kernel is the ideal $(F(X))$ since $F(X)$ is the minimal polynomial of y, and φ_y therefore descends to a one-one $\Bbbk$ algebra homomorphism $\overline{\varphi_y} : \Bbbk(x) \to \Bbbk(y)$. Since $\dim \Bbbk(x)$ and $\dim \Bbbk(y)$ both match the degree of $F(X)$, $\overline{\varphi_y}$ is onto $\Bbbk(y)$ and is therefore the required $\Bbbk$ isomorphism. □

We say that a nonconstant polynomial $F(X)$ in $\Bbbk[X]$ **splits** in a given extension field if $F(X)$ factors completely into degree-one factors over that extension field. A **splitting field** over $\Bbbk$ for a nonconstant polynomial $F(X)$ in $\Bbbk[X]$ is an extension field $\mathbb{L}$ of $\Bbbk$ such that $F(X)$ splits in $\mathbb{L}$ and such that $\mathbb{L}$ is generated by $\Bbbk$ and the roots of $F(X)$ in $\mathbb{L}$.

EXAMPLES. Let $\Bbbk = \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{-1}\,)$ is a splitting field for $X^2 + 1$, because $\pm\sqrt{-1}$ are both in $\mathbb{Q}(\sqrt{-1}\,)$ and they generate $\mathbb{Q}(\sqrt{-1}\,)$ over $\mathbb{Q}$. But $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $X^3 - 2$ because $\mathbb{Q}(\sqrt[3]{2})$ does not contain the two nonreal roots of $X^3 - 2$.

Theorem 9.12 (existence of splitting field). If $F(X)$ is a nonconstant polynomial in $\Bbbk[X]$, then there exists a splitting field of $F(X)$ over $\Bbbk$.

PROOF. We begin by constructing a certain extension field $\mathbb{K}$ of $\Bbbk$ in which $F(X)$ factors completely into degree-one factors in $\mathbb{K}[X]$. We do so by induction on $n = \deg F(X)$. For $n = 1$, there is nothing to prove. For general n, let $G(X)$

be a prime factor of $F(X)$, and apply Theorem 9.10 to obtain a simple algebraic extension $\mathbb{k}_1 = \mathbb{k}(x_1)$ over $\mathbb{k}$ such that $G(x_1) = 0$. Then $F(x_1) = 0$, and the Factor Theorem (Corollary 1.13) gives $F(X) = (X - x_1)H(X)$ for some $H(X)$ in $\mathbb{k}_1(X)$ of degree $n - 1$. Since $\deg H(X) = n - 1 < \deg F(X)$, the inductive hypothesis produces an extension $\mathbb{K}$ of $\mathbb{k}_1$ such that $H(X)$ is a constant multiple of $(X - x_2)\cdots(X - x_n)$ with all x_i in $\mathbb{K}$. Then $F(X)$ factors into degree-one factors in $\mathbb{K}[X]$, and the induction is complete.

Within the constructed field $\mathbb{K}$, let $\mathbb{L}$ be the subfield $\mathbb{L} = \mathbb{k}(x_1, \dots, x_n)$. Then $F(X)$ still factors completely into degree-one factors in $\mathbb{L}(X)$, and $\mathbb{L}$ is generated by $\mathbb{k}$ and the x_i. Hence $\mathbb{L}$ is a splitting field. □

EXAMPLES OF SPLITTING FIELDS.

(1) $\mathbb{k} = \mathbb{Q}$ and $F(X) = X^3 - 2$. The proof of Theorem 9.12 takes $\mathbb{k}_1 = \mathbb{Q}(\sqrt[3]{2})$ and writes $X^3 - 2 = (X - \sqrt[3]{2})\big(X^2 + \sqrt[3]{2}\,X + (\sqrt[3]{2})^2\big)$. Then the proof adjoins one root θ (hence both roots) of $X^2 + \sqrt[3]{2}\,X + (\sqrt[3]{2})^2$, setting $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \theta)$. With this choice of $\mathbb{K}$, the splitting field turns out to be $\mathbb{L} = \mathbb{K}$. In fact, to see that $\mathbb{L}$ is not a proper subfield of $\mathbb{K}$, we observe that $6 = [\mathbb{K} : \mathbb{k}] = [\mathbb{K} : \mathbb{L}]\,[\mathbb{L} : \mathbb{Q}]$ by Corollary 9.7 and that the proper containment $\mathbb{L} \supsetneqq \mathbb{Q}(\sqrt[3]{2})$ implies $[\mathbb{L} : \mathbb{Q}] > 3$. Since $[\mathbb{L} : \mathbb{Q}]$ is a divisor of 6 greater than 3, $[\mathbb{L} : \mathbb{Q}] = 6$. Thus $[\mathbb{K} : \mathbb{L}] = 1$, and $\mathbb{K} = \mathbb{L}$.

(2) $\mathbb{k} = \mathbb{Q}$ and $F(X) = X^3 - X - \frac{1}{3}$. Application of Corollary 8.20c to the polynomial $G(X) = -3X^2F(1/X) = X^3 + 3X^2 - 3$ shows that $G(X)$ has no degree-one factor and hence is irreducible over $\mathbb{Q}$. Then it follows that $F(X)$ is irreducible over $\mathbb{Q}$. The proof of Theorem 9.12 takes $\mathbb{k}_1 = \mathbb{Q}(r)$, where $r^3 - r - \frac{1}{3} = 0$. Then division gives

$$X^3 - X - \tfrac{1}{3} = (X - r)(X^2 + rX + (r^2 - 1)).$$

The discriminant $b^2 - 4ac$ of the quadratic factor is

$$r^2 - 4(r^2 - 1) = 4 - 3r^2 = \frac{r^2}{(1 + 2r)^2},$$

the right-hand equality following from direct computation. This discriminant is a square in $\mathbb{k}_1 = \mathbb{Q}(r)$, and hence $X^2 + rX + (r^2 - 1)$ factors into degree-one factors in $\mathbb{Q}(r)$ without passing to an extension field. Therefore $\mathbb{L} = \mathbb{Q}(r)$ with $[\mathbb{L} : \mathbb{Q}] = 3$.

Theorem 9.13 (uniqueness of splitting field). If $F(X)$ is a nonconstant polynomial in $\mathbb{k}[X]$, then any two splitting fields of $F(X)$ over $\mathbb{k}$ are $\mathbb{k}$ isomorphic.

The idea of the proof is simple enough, but carrying out the idea runs into a technical complication. The idea is to proceed by induction, using the uniqueness result for simple algebraic extensions (Theorem 9.11) repeatedly until all the roots have been addressed. The difficulty is that after one step the coefficients of the two quotient polynomials end up in two distinct but $\mathbb{k}$ isomorphic fields. Thus at the second step Theorem 9.11 does not apply directly. What is needed is the reformulated version given below as Theorem 9.11′, which lends itself to this kind of induction. In addition, as soon as the induction involves at least three steps, the above statement of Theorem 9.13 does not lend itself to a direct inductive proof. For this reason we shall instead prove a reformulated version Theorem 9.13′ of Theorem 9.13 that is ostensibly more general than Theorem 9.13.

Recall from Proposition 4.24 that a general substitution homomorphism that starts from a polynomial ring can have two ingredients. One is the substitution of some element, such as x, for the indeterminate X, and the other is a homomorphism that is made to act on the coefficients. If the homomorphism is σ, let us write $F^\sigma(X)$ to indicate the polynomial obtained by applying σ to each coefficient of $F(X)$.

Theorem 9.11′. Let $\mathbb{k}$ and $\mathbb{k}'$ be fields, and let $\sigma : \mathbb{k} \to \mathbb{k}'$ be a field isomorphism. Suppose that $F(X)$ is a monic prime polynomial in $\mathbb{k}[X]$ and that $\mathbb{K} = \mathbb{k}(x)$ and $\mathbb{K}' = \mathbb{k}'(x')$ are simple algebraic extensions such that $F(x) = 0$ and $F^\sigma(x') = 0$. Then there exists a field isomorphism $\varphi : \mathbb{k}(x) \to \mathbb{k}'(x')$ such that $\varphi\big|_{\mathbb{k}} = \sigma$ and $\varphi(x) = x'$.

PROOF. The argument is essentially unchanged from the proof of Theorem 9.11. We start from the substitution homomorphism $G(X) \mapsto G^\sigma(x')$ that replaces X by x' and that operates by σ on the coefficients. This descends to a field map of $\mathbb{k}[x]$ into $\mathbb{k}'[x']$, and the homomorphism must be onto $\mathbb{k}'[x']$ by a count of dimensions. □

Theorem 9.13′. Let $\mathbb{k}$ and $\mathbb{k}'$ be fields, and let $\sigma : \mathbb{k} \to \mathbb{k}'$ be a field isomorphism. If $F(X)$ is a nonconstant polynomial in $\mathbb{k}[X]$ and if $\mathbb{L}$ and $\mathbb{L}'$ are respective splitting fields for $F(X)$ over $\mathbb{k}$ and for $F^\sigma(X)$ over $\mathbb{k}'$, then there exists a field isomorphism $\varphi : \mathbb{L} \to \mathbb{L}'$ such that $\varphi\big|_{\mathbb{k}} = \sigma$ and such that φ sends the set of roots of $F(X)$ to the set of roots of $F^\sigma(X)$.

PROOF. We proceed by induction on $n = \deg F(X)$, the case $n = 1$ being evident. Assume the result for degree $n-1$. Let $G(X)$ be a prime factor of $F(X)$ over $\mathbb{k}$. Then $G^\sigma(X)$ is a prime factor of $F^\sigma(X)$ over $\mathbb{k}'$. The polynomials $G(X)$ and $G^\sigma(X)$ have roots in $\mathbb{L}$ and $\mathbb{L}'$, respectively. Fix one such root for each, say x_1 and x_1'. By Theorem 9.11′, there exists a field isomorphism $\sigma_1 : \mathbb{k}(x_1) \to \mathbb{k}'(x_1')$ extending σ and satisfying $\sigma_1(x_1) = x_1'$. Write $F(X) = (X - x_1)H(X)$ with coefficients in $\mathbb{k}(x_1)$, by the Factor Theorem (Corollary 1.13). Applying σ_1 to the coefficients, we obtain $F^{\sigma}(X) = (X - x'_1)H^{\sigma_1}(X)$ with coefficients in $\Bbbk'(x'_1)$. Then $\mathbb{L}$ and $\mathbb{L}'$ are splitting fields for $H(X)$ and $H^{\sigma_1}(X)$ over $\Bbbk(x_1)$ and $\Bbbk'(x'_1)$, respectively. By induction we can extend σ_1 to an isomorphism $\varphi : \mathbb{L} \to \mathbb{L}'$, and the theorem readily follows. □

3. Finite Fields

In this section we shall use the results on splitting fields in Section 2 to classify finite fields up to isomorphism. So far, the examples of finite fields that we have encountered are the prime fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p elements, p being any prime number, and the field of 4 elements in Example 3 of fields in Section IV.4. Every finite field has to contain a subfield isomorphic to one of the prime fields $\mathbb{F}_p$, and Proposition 4.33 observed as a consequence that any finite field necessarily has p^n elements for some prime number p and some integer $n > 0$.

Theorem 9.14. For each p^n with p a prime number and with n a positive integer, there exists up to isomorphism one and only one field with p^n elements. Such a field is a splitting field for $X^{p^n} - X$ over the prime field $\mathbb{F}_p$.

If $q = p^n$, it is customary to denote by $\mathbb{F}_q$ a field of order q. The theorem says that $\mathbb{F}_q$ exists and is unique up to isomorphism. Some authors refer to finite fields as **Galois fields**.

Some preparation is needed before we can come to the proof of the theorem. We need to carry over the simplest aspects of differential calculus to polynomials with coefficients in an arbitrary field $\Bbbk$. First we give an informal definition of the **derivative** of a polynomial; then we give a more precise definition. For any polynomial $F(X) = \sum_{j=0}^{n} c_j X^j$ in $\Bbbk[X]$, we informally define the derivative to be the polynomial

$$F'(X) = \sum_{j=1}^{n} j c_j X^{j-1} = \sum_{j=0}^{n-1} (j+1) c_{j+1} X^j.$$

The more precise definition uses the definition of members of $\Bbbk[X]$ as infinite sequences of members of $\Bbbk$ whose terms are 0 from some point on. In this notation if $F = (c_0, c_1, \dots, c_n, 0, \dots)$ with c_j in the j^{th} position for $j \le n$ and with 0 in the j^{th} position for $j > n$, then $F' = (c_1, 2c_2, \dots, nc_n, 0, \dots)$ with $(j+1)c_{j+1}$ in the j^{th} position for $j \le n-1$ and with 0 in the j^{th} position for $j > n-1$. In any event, the mapping $F \mapsto F'$ is $\Bbbk$ linear from $\Bbbk[X]$ to itself. The operation is called **differentiation**.

Proposition 9.15. Differentiation on $\Bbbk[X]$ satisfies the product rule: $F = GH$ implies $F' = G'H + GH'$.

PROOF. Because of the $\Bbbk$ linearity, it is enough to prove the result for monomials. Thus let $G(X) = X^m$ and $H(X) = X^n$, so that $F(X) = X^{m+n}$. Then $F'(X) = (m+n)X^{m+n-1}$, $G'(X)H(X) = mX^{m+n-1}$, and $G(X)H'(X) = nX^{m+n-1}$. Hence we indeed have $F'(X) = G'(X)H(X) + G(X)H'(X)$. □

Corollary 9.16. If n is a positive integer, if r is in $\Bbbk$, and if $F(X) = (X-r)^n$ in $\Bbbk[X]$, then $F'(X) = n(X-r)^{n-1}$.

PROOF. This is immediate by induction from Proposition 9.15 since the derivative of $X - r$ is 1. □

Corollary 9.17. Let r be in $\Bbbk$, and let $F(X)$ be in $\Bbbk[X]$. If $(X-r)^2$ divides $F(X)$, then $F(r) = F'(r) = 0$. Conversely if $F(r) = F'(r) = 0$, then $(X-r)^2$ divides $F(X)$.

PROOF. Write $F(X) = (X-r)^2G(X)$. If we substitute r for X, we see that $F(r) = 0$. If instead we differentiate, using Proposition 9.15 and Corollary 9.16, then we obtain $F'(X) = 2(X-r)G(X) + (X-r)^2G'(X)$. Substituting r for X, we obtain $F'(r) = 0 + 0 = 0$.

For the converse, let $F(r) = F'(r) = 0$. Proposition 4.28a shows that $F(X) = (X-r)G(X)$. Differentiating this identity by means of Proposition 9.15 gives $F'(X) = G(X)+(X-r)G'(X)$. Substituting r for X yields $0 = F'(r) = G(r)+0$ and shows that $G(r) = 0$. By Proposition 4.28, $G(X) = (X-r)H(X)$. Hence $F(X) = (X-r)^2H(X)$. □

Lemma 9.18. If $\Bbbk$ is a field of characteristic $p \neq 0$, then the map $\varphi : \Bbbk \to \Bbbk$ given by $\varphi(x) = x^p$ is a field mapping.

REMARK. The map $x \mapsto x^p$ is often called the **Frobenius** map. If $\Bbbk$ is a finite field, then it must carry $\Bbbk$ onto $\Bbbk$ since one-one implies onto for functions from a finite set to itself; in this case the map is an automorphism of $\Bbbk$.

PROOF. The computation $\varphi(uv) = (uv)^p = u^pv^p = \varphi(u)\varphi(v)$ shows that φ respects products. If u and v are in $\Bbbk$, then

$$\varphi(u+v) = (u+v)^p = \varphi(u) + \sum_{j=1}^{p-1} \tbinom{p}{j} u^{p-j}v^j + \varphi(v) = \varphi(u) + \varphi(v),$$

the last equality holding since the binomial coefficient $\binom{p}{j}$ has a p in the numerator for $1 \leq j \leq p-1$. Thus φ is a ring homomorphism. Since $\varphi(1) = 1$, φ is a field mapping. □

PROOF OF UNIQUENESS IN THEOREM 9.14. Let $\mathbb{k}$ be a finite field, say of characteristic p, and let $\mathbb{P}$ be the prime field of order p within $\mathbb{k}$. We know that $\mathbb{P}$ is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{k}$ is a finite-dimensional vector space over $\mathbb{P}$, we know also that $\mathbb{k}$ has order $q = p^n$ for some integer $n > 0$. The multiplicative group $\mathbb{k}^\times$ of $\mathbb{k}$ thus has order $q - 1$, and every $x \neq 0$ in $\mathbb{k}$ therefore satisfies $x^{q-1} = 1$. Taking $x = 0$ into account, we see that every member of $\mathbb{k}$ satisfies $x^q = x$. Forming the polynomial $X^q - X$ in $\mathbb{P}[X]$, we see that every member of $\mathbb{k}$ is a root of this polynomial. Iterated application q times of the Factor Theorem (Corollary 1.13) shows that $X^q - X$ factors into degree-one factors in $\mathbb{k}$. Since every member of $\mathbb{k}$ is a root of $X^q - X$, $\mathbb{k}$ is a splitting field of $X^q - X$ over $\mathbb{P}$. Then the uniqueness of the prime field up to isomorphism, in combination with the uniqueness of the splitting field of $X^q - X$ given in Theorem 9.13′, shows that $\mathbb{k}$ is uniquely determined up to isomorphism. □

PROOF OF EXISTENCE IN THEOREM 9.14. Let $q = p^n$ be given, and define $\mathbb{k}$ to be a splitting field of $X^q - X$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The field $\mathbb{k}$ exists by Theorem 9.12, and it has characteristic p. Since $X^q - X$ is monic of degree q, the definition of splitting field says that we can write

$$X^q - X = (X - u_1)(X - u_2)\cdots(X - u_q) \qquad \text{with all } u_j \in \mathbb{k}.$$

Because of Lemma 9.18, the map $\varphi(u) = u^q$, which is the n^{th} power of the map $u \mapsto u^p$, is a field mapping of $\mathbb{k}$ into itself. The members of $\mathbb{k}$ fixed by φ form a subfield of $\mathbb{k}$, and these elements of $\mathbb{k}$ are exactly the members of the set $S = \{u_1, \dots, u_q\}$. Therefore S is a subfield of $\mathbb{k}$, necessarily containing $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $X^q - X$ splits in S and since the roots of $X^q - X$ generate S, S is a splitting field of $X^q - X$ over $\mathbb{F}_p$. In other words, $S = \mathbb{k}$. To complete the proof, it is enough to show that the elements $u_1, \dots, u_q$ are distinct, and then $\mathbb{k}$ will be a field of q elements. The question is therefore whether some root of $X^q - X$ has multiplicity at least 2, i.e., whether $(X - r)^2$ divides $X^q - X$ for some r in $\mathbb{k}$. Corollary 9.17 gives a necessary condition for this divisibility, saying that the derivative of $X^q - X$ must have r as a root. However, the derivative of $X^q - X$ is $qX^{q-1} - 1 = -1$, and the constant polynomial -1 has no roots. We conclude that $\mathbb{k}$ has q elements. □

Corollary 9.19. If q and r are integers with $2 \leq q \leq r$, then the finite field $\mathbb{F}_q$ is isomorphic to a subfield of the finite field $\mathbb{F}_r$ if and only if $r = q^n$ for some integer $n \geq 1$.

PROOF. If $\mathbb{F}_q$ is isomorphic to a subfield of $\mathbb{F}_r$, then we may consider $\mathbb{F}_r$ as a vector space over $\mathbb{F}_q$, say of dimension n. In this case, $\mathbb{F}_r$ has q^n elements.

Conversely let $r = q^n$, and regard $\mathbb{F}_r$ as a splitting field of $X^{q^n} - X$ over the prime field $\mathbb{F}_p$, by Theorem 9.14. Let S be the subset of $\mathbb{F}_r$ of all roots of $X^q - X$.

Putting $a = q - 1$ and $k = \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \cdots + 1$, we have

$$X^{ka} - 1 = (X^a - 1)(X^{(k-1)a} + X^{(k-2)a} + \cdots + 1).$$

Multiplying by X, we see that $X^q - X$ is a factor of $X^{q^n} - X$. Since $X^{q^n} - X$ splits in $\mathbb{F}_r$ and has distinct roots, the same is true of $X^q - X$. Therefore $|S| = q$.

Let $q = p^m$. The m^{th} power of the homomorphism of Lemma 9.18 on $\Bbbk = \mathbb{F}_r$ is $x \mapsto x^q$, and the subset of $\mathbb{F}_r$ fixed by this homomorphism is a subfield. Thus S is a subfield, and it has q elements. □

4. Algebraic Closure

Algebraically closed fields—those for which every nonconstant polynomial with coefficients in the field has a root in the field—were introduced in Section V.1, and it was mentioned at that time that every field is a subfield of some algebraically closed field. We shall prove that existence theorem in this section in a form lending itself to a uniqueness result.

Throughout this section let $\Bbbk$ be a field. We begin by giving further descriptions of algebraically closed fields that take the theory of Sections 1–2 into account.

Proposition 9.20. The following conditions on the field $\Bbbk$ are equivalent:

(a) $\Bbbk$ has no nontrivial algebraic extensions,
(b) every irreducible polynomial in $\Bbbk[X]$ has degree 1,
(c) every polynomial in $\Bbbk[X]$ of positive degree has at least one root in $\Bbbk$,
(d) every polynomial in $\Bbbk[X]$ of positive degree factors over $\Bbbk$ into polynomials of degree 1.

PROOF. If (a) holds, then (b) holds since any irreducible polynomial of degree greater than 1 would give a nontrivial simple algebraic extension (Theorem 9.10). If (b) holds and a polynomial of positive degree is given, apply (b) to an irreducible factor to see that the given polynomial has a root; thus (c) holds. Condition (c) implies condition (d) by induction and the Factor Theorem. If (d) holds and if $\mathbb{K}$ is an algebraic extension of $\Bbbk$, let x be in $\mathbb{K}$, and let $F(X)$ be the minimal polynomial of x over $\Bbbk$. Then $F(X)$ is irreducible over $\Bbbk$, and (d) says that $F(X)$ has degree 1. Hence x is in $\Bbbk$, and we conclude that $\mathbb{K} = \Bbbk$. □

A field satisfying the equivalent conditions of Proposition 9.20 is said to be **algebraically closed**.

EXAMPLES OF ALGEBRAICALLY CLOSED FIELDS.

(1) The Fundamental Theorem of Algebra (Theorem 1.18) says that $\mathbb{C}$ is algebraically closed. This theorem was not proved in Chapter I, but a proof will be given in this chapter in Section 10.

(2) Let $\mathbb{K}$ be the subset of all members of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. By Corollary 9.9, $\mathbb{K}$ is a subfield of $\mathbb{C}$. Example 1 shows that every polynomial in $\mathbb{Q}[X]$ splits in $\mathbb{K}$, and Lemma 9.21 below then allows us to conclude that $\mathbb{K}$ is algebraically closed.

(3) Fix a prime number p, and start with $\Bbbk_0 = \mathbb{F}_p$ as the prime field $\mathbb{Z}/p\mathbb{Z}$. Enumerate the members of $\mathbb{F}_p[X]$, letting $F_n(X)$ be the n^{th} such polynomial. We construct $\Bbbk_n$ by induction on n so that $\Bbbk_n$ is a splitting field for $F_n(X)$ over $\Bbbk_{n-1}$ when $n \geq 1$. Then $\Bbbk_0 \subseteq \Bbbk_1 \subseteq \Bbbk_2 \subseteq \cdots$ is an increasing sequence of fields containing $\mathbb{F}_p$. Let $\mathbb{K}$ be the union. Any two elements of $\mathbb{K}$ lie in a single $\Bbbk_n$, and it follows that $\mathbb{K}$ is closed under the field operations. Any three elements lie in a single $\Bbbk_n$, and it follows that any of the defining properties of a field is valid in $\mathbb{K}$ because it is valid in $\Bbbk_n$. Therefore $\mathbb{K}$ is a field. This field is an extension of $\mathbb{F}_p$, and every polynomial in $\mathbb{F}_p[X]$ splits in $\mathbb{K}$. As in Example 2, Lemma 9.21 below shows that $\mathbb{K}$ is algebraically closed.

Lemma 9.21. If $\mathbb{K}/\Bbbk$ is an algebraic extension of fields and if every nonconstant polynomial in $\Bbbk[X]$ splits into degree-one factors in $\mathbb{K}$, then $\mathbb{K}$ is algebraically closed.

PROOF. Let $\mathbb{K}'$ be an algebraic extension of $\mathbb{K}$, and let x be in $\mathbb{K}'$. Let $G(X)$ be the minimal polynomial of x over $\mathbb{K}$, and write $G(X)$ as

$$G(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \qquad \text{with all } c_i \in \mathbb{K}.$$

Then x is algebraic over $\Bbbk(c_{n-1}, \ldots, c_0)$, which is a finite extension of $\Bbbk$ by Theorem 9.8. By Corollary 9.7, x lies in a finite extension of $\Bbbk$. Thus Proposition 9.4 shows that x is algebraic over $\Bbbk$. Let $F(X)$ be the minimal polynomial of x over $\Bbbk$. By assumption this splits over $\mathbb{K}$, say as

$$F(X) = (X - x_1) \cdots (X - x_m) \qquad \text{with all } x_i \in \mathbb{K}.$$

Evaluating at x and using the fact that $F(x) = 0$, we see that $x = x_j$ for some j. Therefore x is in $\mathbb{K}$, and $\mathbb{K}$ is algebraically closed. □

An extension field $\mathbb{K}/\Bbbk$ is an **algebraic closure** of $\Bbbk$ if $\mathbb{K}$ is algebraic over $\Bbbk$ and if $\mathbb{K}$ is algebraically closed. Example 2 of algebraically closed fields above gives an algebraic closure of $\mathbb{Q}$, and Example 3 gives an algebraic closure of $\mathbb{F}_p$.

Theorem 9.22 (Steinitz). Every field $\mathbb{k}$ has an algebraic closure, and this is unique up to $\mathbb{k}$ isomorphism.

REMARKS. The proof of existence is modeled on the argument for Example 3 of algebraic closures. However, we are not free in general to use a simple union of a sequence of fields and have to work harder. Because there is no evident set of possibilities within which we are forming extension fields, Zorn's Lemma is inconvenient to use and tends to result in an unintuitive construction. Instead, we use Zermelo's Well-Ordering Theorem, whose use more closely parallels the inductive construction in Example 3.

PROOF OF EXISTENCE. With $\mathbb{k}$ as the given field, let S be the set of nonconstant polynomials $s(X)$ in $\mathbb{k}[X]$, and introduce a well ordering into S by means of Zermelo's Well-Ordering Theorem (Section A5 of the appendix). Let us write $\prec$ for "strictly precedes in the ordering" and $\precsim$ for "equals or strictly precedes." For each $s \in S$, let $\bar{s}$ be the successor of s, i.e., the first element among all elements t with $s \prec t$. We write s_0 for the first element of S. Without loss of generality, we may assume that S has a last element s_∞. The idea is to construct simultaneously two kinds of things:

(i) an algebraic extension field $\mathbb{k}_s/\mathbb{k}$ for each $s \in S$ such that $\mathbb{k}_{s_0} = \mathbb{k}$ and such that $\mathbb{k}_{\bar{s}}$ is a splitting field for $s(X)$ over $\mathbb{k}_s$ whenever $s \prec s_\infty$,

(ii) a field mapping $\varphi_{ut} : \mathbb{k}_t \to \mathbb{k}_u$ for each ordered pair of elements t and u in S having $t \precsim u$, such that $\varphi_{tt} = 1$ for all t and such that $t \precsim u \precsim v$ implies $\varphi_{vt} = \varphi_{vu}\varphi_{ut}$.

These extension fields and mappings are to be such that $\mathbb{k}_s = \bigcup_{t \prec s} \varphi_{st}(\mathbb{k}_t)$ whenever s is not a successor and is not s_0. If such a system of extension fields and field homomorphisms exists, then Lemma 9.21 applies to a splitting field over $\mathbb{k}_{s_\infty}$ of the nonconstant polynomial $s_\infty(X)$ and shows that this splitting field is algebraically closed; since this splitting field is an algebraic extension of $\mathbb{k}$, it is an algebraic closure of $\mathbb{k}$.

A partial such system through t_0 means a system consisting of fields $\mathbb{k}_s$ with $s \precsim t_0$ and field homomorphisms φ_{ut} with $t \precsim u \precsim t_0$ such that the above conditions hold as far as they are applicable. A partial system exists through the first member s_0 of S because we can take $\mathbb{k}_{s_0} = \mathbb{k}$ and $\varphi_{s_0 s_0} = 1$. Arguing by contradiction, we suppose that such a system of extension fields and field homomorphisms fails to exist through some member of S. Let t_0 be the first member of S such that there is no partial system through t_0.

Suppose that t_0 is the successor of some element t_1 in S. We know that a partial system exists through t_1. If we let $\mathbb{k}_{t_0}$ be a splitting field for $t_1(X)$ over $\mathbb{k}_{t_1}$, and if we define

$$\varphi_{t_0 t} = \begin{cases} \varphi_{t_0 t_1}\varphi_{t_1 t} & \text{for } t \precsim t_1, \\ 1 & \text{for } t = t_0, \end{cases}$$

then the enlarged system is a partial system through t_0, contradiction. Thus t_0 cannot be the successor of some element of S.

When t_0 is not a successor, at least $\Bbbk_t$ is defined for $t \prec t_0$ and φ_{ut} is defined for $t \precsim u \prec t_0$. We want to form a union, but we have to keep the field operations aligned properly in the process. Define a "t-allowable tuple" to be a function $u \mapsto x_u$ defined for $t \precsim u \prec t_0$ such that x_u is in $\Bbbk_u$ and $\varphi_{vu}(x_u) = x_v$ whenever $t \precsim u \precsim v \prec t_0$. If x is in $\Bbbk_t$, then an example of a t-allowable tuple is given by $u \mapsto \varphi_{ut}(x)$ for $t \precsim u \prec t_0$.

If $t \prec t_0$ and $t' \prec t_0$, then we can apply field operations to the t-allowable tuple $u \mapsto x_u$ and to the t'-allowable tuple $u \mapsto y_u$, obtaining $\max(t, t')$-allowable tuples $u \mapsto x_u + y_u$, $u \mapsto -x_u$, $u \mapsto x_u y_u$, and $x_u \mapsto x_u^{-1}$ as long as $x_t \neq 0$. These operations are meaningful since each φ_{vu} is a field mapping.

If $t \prec t_0$ and $t' \prec t_0$, we say that the t-allowable tuple $u \mapsto x_u$ is equivalent to the t'-allowable tuple $u \mapsto y_u$ if $x_u = y_u$ for $\max(t, t') \precsim u \prec t_0$. The result is an equivalence relation, and the equivalence relation respects the field operations in the previous paragraph. We define $\Bbbk_{t_0}$ to be the set of equivalence classes of allowable tuples with the inherited field operations. The 0 element is the class of the s_0-allowable tuple $u \mapsto 0$, and the multiplicative identity is the class of the s_0-allowable tuple $u \mapsto 1$. It is a routine matter to check that $\Bbbk_{t_0}$ is a field.

If $t \prec t_0$ is given, we define the function $\varphi_{t_0t} : \Bbbk_t \to \Bbbk_{t_0}$ as follows: if x is in $\Bbbk_t$, we form the t-allowable tuple $u \mapsto \varphi_{ut}(x)$ and take its equivalence class, which is a member of $\Bbbk_{t_0}$, as $\varphi_{t_0t}(x)$. Then φ_{t_0t} is evidently a field mapping. It is evident also that $\varphi_{t_0v}\varphi_{vu} = \varphi_{t_0u}$ when $u \precsim v \prec t_0$. Defining $\varphi_{t_0t_0}$ to be the identity, we have a complete system of field mappings φ_{vu} for $\Bbbk_{t_0}$.

The final step is to check that $\Bbbk_{t_0}$ is the union of the images of the φ_{t_0t} for $t \prec t_0$. Thus choose a representative of an equivalence class in $\Bbbk_{t_0}$. Let the representative be a t-allowable tuple $u \mapsto x_u$ for $t \precsim u \prec t_0$. The element x_t is in $\Bbbk_t$, and the condition $x_u = \varphi_{ut}(x_t)$ is just the condition that the class of $u \mapsto x_u$ be the image of x_t under φ_{t_0t}. Hence every member of $\Bbbk_{t_0}$ is in the image of some φ_{t_0t} with $t \prec t_0$, and we have a contradiction to the hypothesis that a partial system through t_0 does not exist. This completes the proof of existence. □

For the uniqueness in Theorem 9.22, we again need a serious application of the Axiom of Choice, but here Zorn's Lemma can be applied fairly routinely. The proof will show a little more than is needed, and in fact the uniqueness in Theorem 9.22 will be derived as a consequence of Theorem 9.23 below.

Theorem 9.23. Let $\mathbb{K}'$ be an algebraically closed field, and let $\mathbb{K}$ be an algebraic extension of a field $\Bbbk$. If φ is a field mapping of $\Bbbk$ into $\mathbb{K}'$, then φ can be extended to a field mapping of $\mathbb{K}$ into $\mathbb{K}'$.

PROOF OF UNIQUENESS IN THEOREM 9.22 USING THEOREM 9.23. Let $\mathbb{K}$ and $\mathbb{K}'$ be algebraic closures of $\Bbbk$, and let $\varphi : \Bbbk \to \mathbb{K}'$ be the inclusion mapping. Theorem 9.23 supplies a field mapping $\Phi : \mathbb{K} \to \mathbb{K}'$ such that $\Phi\big|_{\Bbbk} = \varphi$, i.e., such that Φ fixes $\Bbbk$. Since $\mathbb{K}$ is an algebraic closure of $\Bbbk$, so is $\Phi(\mathbb{K})$. Then $\mathbb{K}'$ is an algebraic extension of the algebraically closed field $\Phi(\mathbb{K})$, and we must have $\Phi(\mathbb{K}) = \mathbb{K}'$. Thus Φ is a $\Bbbk$ isomorphism of $\mathbb{K}$ onto $\mathbb{K}'$.

PROOF OF THEOREM 9.23. Let S be the set of all triples $(\mathbb{L}, \mathbb{L}', \psi)$ such that $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ and ψ is a field mapping of $\mathbb{L}$ onto the subfield $\mathbb{L}'$ of $\mathbb{K}'$ with $\psi\big|_{\Bbbk} = \varphi$. The set S is nonempty since $(\Bbbk, \varphi(\Bbbk), \varphi)$ is a member of it. Defining $(\mathbb{L}_1, \mathbb{L}_1', \psi_1) \subseteq (\mathbb{L}_2, \mathbb{L}_2', \psi_2)$ to mean that $\mathbb{L}_1 \subseteq \mathbb{L}_2$, that $\mathbb{L}_1' \subseteq \mathbb{L}_2'$, and that ψ_1 as a set of ordered pairs is a subset of ψ_2 as a set of ordered pairs, we partially order S by inclusion upward. If $\{(\mathbb{L}_\alpha, \mathbb{L}_\alpha', \psi_\alpha)\}$ is a nonempty chain in S, form the triple $\big(\bigcup_\alpha \mathbb{L}_\alpha, \bigcup_\alpha \mathbb{L}_\alpha', \bigcup_\alpha \psi_\alpha\big)$, and put $\psi = \bigcup_\alpha \psi_\alpha$. Then $\psi\big(\bigcup_\alpha \mathbb{L}_\alpha\big) = \bigcup_\alpha \mathbb{L}_\alpha'$, and consequently $\big(\bigcup_\alpha \mathbb{L}_\alpha, \bigcup_\alpha \mathbb{L}_\alpha', \bigcup_\alpha \psi_\alpha\big)$ is an upper bound in S for the chain. By Zorn's Lemma, S has a maximal element $(\mathbb{L}_0, \mathbb{L}_0', \psi_0)$. We shall prove that $\mathbb{L}_0 = \mathbb{K}$, and the proof will be complete.

Fix x in $\mathbb{K}$, and let $F(X)$ be the minimal polynomial of x over $\mathbb{L}_0$. The minimal polynomial of $\psi_0(x)$ over $\mathbb{L}_0'$ is then $F^{\psi_0}(X)$. Since $\mathbb{K}'$ is algebraically closed, $F^{\psi_0}(X)$ has a root x' in $\mathbb{K}'$. By Theorem 9.11$'$, $\psi_0 : \mathbb{L}_0 \to \mathbb{L}'$ can be extended to an isomorphism $\Psi_0 : \mathbb{L}_0(x) \to \mathbb{L}_0'(x')$ such that $\psi_0(x) = x'$. Then $(\mathbb{L}_0(x), \mathbb{L}_0'(x'), \Psi_0)$ is in S and contains $(\mathbb{L}_0, \mathbb{L}_0', \psi_0)$. This containment, if strict, would contradict the fact that $(\mathbb{L}_0, \mathbb{L}_0', \psi_0)$ is a maximal element of S. Thus equality must hold: $\mathbb{L}_0(x) = \mathbb{L}_0$. Therefore x is in $\mathbb{L}_0$, and we conclude that $\mathbb{L}_0 = \mathbb{K}$. □

The use of algebraic closures allows us to simplify understanding of splitting fields. If we are working with a field $\Bbbk$ and is $\overline{\Bbbk}$ is a fixed algebraic closure of $\Bbbk$, then the existence and uniqueness of *the* splitting field of a polynomial $F(X)$ in $\Bbbk[X]$ becomes evident; no isomorphisms are involved. Namely let $\alpha_1, \dots, \alpha_n$ be the roots of $F(X)$ in $\overline{\Bbbk}$. Then the subfield of $\overline{\Bbbk}$ generated by $\Bbbk$ and $\alpha_1, \dots, \alpha_n$ is the splitting field of $F(X)$, and it is manifestly unique. Henceforth when we refer to *the* splitting field of a polynomial over a field $\Bbbk$, it is with an understanding of working within a fixed algebraic closure in this way.

5. Geometric Constructions by Straightedge and Compass

Classical Euclidean geometry attached a certain emphasis to constructions in the Euclidean plane that could be made by straightedge and compass. These are often referred to casually as constructions by "ruler and compass," but one is not allowed to use the markings on a ruler. Thus "straightedge and compass" is a more accurate description.

In these constructions the starting configuration may be regarded as a line with two points marked on the line. Allowable constructions are the following: to form the line through a given point different from finitely many other lines through that point, to form the line through two distinct points, to form a circle with a given center and a radius different from that of finitely many other circles through the point, and to form a circle with a given center and radius. Intersections of a line or a circle with previous lines and circles establish new points for continuing the construction.

For example a line perpendicular to a given line at a given point can be constructed by drawing any circle centered at the point, using the two intersection points as centers of new circles, drawing those circles so as to have radius larger than the first circle, and forming the line between their two points of intersection. An angle at the point P of intersection between two intersecting lines A and B may be bisected by drawing any circle centered at P, selecting one of the points of intersection on each line so that P and the two new points Q and R describe the angle, drawing circles with that same radius centered at Q and R, and forming the line between the points of intersection of the two circles. And so on.

Three notable problems remained unsolved in antiquity:

(i) how to double a cube, i.e., how to construct the side of a cube of double the volume of a given cube,

(ii) how to trisect any constructible angle, i.e., how to divide the angle into three equal parts by means of constructed lines,

(iii) how to square a circle, i.e., how to construct the side of a square whose area equals that of a given disk.

In this section we shall use the elementary field theory of Sections 1–2 to show that doubling a cube and trisecting a 60-degree angle are impossible with straightedge and compass. As to (iii), we shall reduce a proof of the impossibility of squaring the circle to a proof that π is transcendental over $\mathbb{Q}$. This latter proof we give in Section 14.

The first step is to translate the problem of geometric constructibility into a statement in algebra. Since we are given two points on a line, we can introduce Cartesian coordinates for the Euclidean plane, taking one of the points to be $(0,0)$ and the other point to be $(1,0)$. Points in the Euclidean plane are now determined by their Cartesian coordinates, which determine all distances. Distances in turn can be laid off on the x-axis from $(0,0)$. Thus the question becomes, what points on the x-axis can be constructed?

Let $\mathcal{C}$ be the set of constructible x coordinates. We are given that 0 and 1 are in $\mathcal{C}$. Closure of $\mathcal{C}$ under addition and subtraction is evident; the straightedge is not even necessary for this step. Figure 9.1 indicates why the positive elements

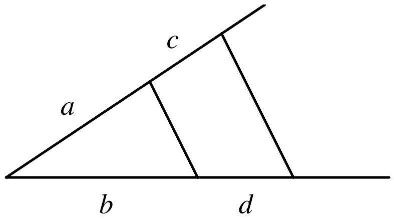

FIGURE 9.1. Closure of positive constructible x coordinates under multiplication and division.

of $\mathcal{C}$ are closed under multiplication and division. In more detail we take two intersecting lines and mark three known positive members of $\mathcal{C}$ as the distances a, b, c in the figure. Then we form the line through the two points marking a and b, and we form a line parallel to that line through the point marked off by the distance c. The intersection of this parallel line with the other original line defines a distance d. Then $a/b = c/d$, and so $d = bc/a$. By taking $a = 1$, we see that we can multiply any two members b and c in $\mathcal{C}$, obtaining a result in $\mathcal{C}$. By instead taking $c = 1$, we see that we can divide. The conclusion is that $\mathcal{C}$ is a field.

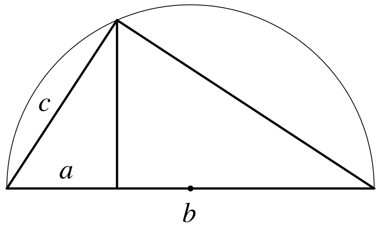

FIGURE 9.2. Closure of positive constructible x coordinates under square roots.

Figure 9.2 indicates why the positive elements of $\mathcal{C}$ are closed under taking square roots. In more detail let a and b be positive members of $\mathcal{C}$ with $a < b$. By forming a circle whose diameter is a segment of length b and by forming a line perpendicular to that line at the point marked by a, we determine the pictured right triangle with a side c satisfying $a/c = c/b$. Then $c = \sqrt{ab}$. By taking one of a and b to be 1, we see that the square root of the other of a and b is in $\mathcal{C}$. This completes the proof of the direct part of the following theorem.

Theorem 9.24. The set $\mathcal{C}$ of x coordinates that can be constructed from $x = 1$ and $x = 0$ by straightedge and compass forms a subfield of $\mathbb{R}$ such that the square root of any positive element of the field lies in the field. Conversely the members of $\mathcal{C}$ are those real numbers lying in some subfield F_n of $\mathbb{R}$ of the form

$$F_1 = \mathbb{Q}(\sqrt{a_0}\,), \quad F_2 = F_1(\sqrt{a_1}\,), \quad \dots, \quad F_n = F_{n-1}(\sqrt{a_{n-1}}\,)$$

with each a_j in F_j and with $a_0, \dots, a_{n-1}$ all ≥ 0.

PROOF OF CONVERSE. Suppose we have a subfield $F = F_n$ of $\mathbb{R}$ of the kind described in the statement of the theorem. The possibilities for obtaining a new constructible point from F by an additional construction arise from three situations: the intersection of two lines, each passing through two points of F; the intersection of a line and a circle, each determined by data from F; and the intersection of two circles, each determined by data from F.

In the case of two intersecting lines, each line is of the form $ax + by = c$ for suitable coefficients a, b, c in F, and the intersection is a point (x, y) in $F \times F$. So intersections of lines do not force us to enlarge F.

For a line and a circle, we assume that the line is given by $ax + by = c$ with a, b, c in F, that the circle has radius in F and center in $F \times F$, and that the lines and the circle actually intersect. The circle is then given by $(x-h)^2+(y-k)^2 = r^2$ with h, k, r in F. Substitution of the equation of the line into the equation of the circle gives us a quadratic equation either for x, and x then determines y, or for y, and y then determines x. The quadratic equation has real roots, and thus its discriminant is ≥ 0. The result is that x and y are in a field $F(\sqrt{l}\,)$ for some $l \geq 0$ in F.

For two circles, without loss of generality, we may take their equations to be

$$x^2 + y^2 = r^2 \qquad \text{and} \qquad (x-h)^2 + (y-h)^2 = s^2$$

with r, h, k, s in F. Subtracting gives $2xh + 2yk = h^2 + k^2 - s^2 + r^2$. With this equation and with $x^2 + y^2 = r^2$, we again have a line and circle that are being intersected. Thus the same remarks apply as in the previous paragraph.

The conclusion is that any new single construction of points of intersection by straightedge and compass leads from F to $F(\sqrt{l}\,)$ for some $l \geq 0$ in F. Thus every member of the set $\mathcal{C}$ is as described in the theorem. □

To apply the theorem to prove the impossibility of the three never-accomplished constructions that were described earlier in the section, we observe that $[F_i : F_{i-1}]$ in the theorem equals 1 or 2 for each i. Consequently every member of the constructible set $\mathcal{C}$ lies in a finite algebraic extension of $\mathbb{Q}$ of degree 2^k for some k.

For the problem of doubling a cube, the question amounts to constructing $\sqrt[3]{2}$. We argue by contradiction. If $\sqrt[3]{2}$ lies in F_n as in the theorem, then $\mathbb{Q}(\sqrt[3]{2}\,) \subseteq F_n$. With k as the integer $\leq n$ such that $[F_n : \mathbb{Q}] = 2^k$, Corollary 9.7 gives

$$2^k = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\sqrt[3]{2}\,)]\,[\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}] = 3[F_n : \mathbb{Q}(\sqrt[3]{2}\,)].$$

Thus 3 must divide a power of 2, and we have arrived at a contradiction. We conclude that it is not possible to double a cube with straightedge and compass.

For the problem of trisecting any constructible angle, let us show that a 60° angle cannot be trisected. A 60° angle is itself constructible, being the angle between two sides in an equilateral triangle. Trisecting a 60° angle amounts to constructing $\cos 20^\circ$; $\sin 20^\circ$ is then $(1-\cos^2 20^\circ)^{1/2}$. To proceed, we derive an equation satisfied by $\cos 20^\circ$, starting from

$$(\cos 20^\circ + i\sin 20^\circ)^3 = \cos 60^\circ + i\sin 60^\circ = \tfrac{1}{2} + \tfrac{i\sqrt{3}}{2}.$$

We expand the left side and extract the real part of both sides to obtain

$$\cos^3 20^\circ - 3\cos 20^\circ \sin^2 20^\circ = \tfrac{1}{2}.$$

Substituting $\sin^2 20^\circ = 1 - \cos^2 20^\circ$ and simplifying, we see that $r = \cos 20^\circ$ satisfies

$$4r^3 - 3r - \tfrac{1}{2} = 0.$$

Arguing with Corollary 8.20 as in Example 2 of splitting fields in Section 2, we readily check that $4X^3 - 3X - \frac{1}{2}$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$, and we are led to the same contradiction as for the problem of doubling the cube. Therefore it is not possible to trisect a 60° angle with straightedge and compass.

For the problem of squaring a circle, let A be the area of the circle, and let r be the radius. If the square has side x, then $x^2 = A = \pi r^2$, with r given. Thus $x = r\sqrt{\pi}$, and the essence of the matter is to construct $\sqrt{\pi}$. However, π is known to be transcendental by a theorem of F. Lindemann (1882); we give a proof in Section 14. Since π is transcendental, $\sqrt{\pi}$ is transcendental.

A fourth notable problem, which leads to further insights, concerns the construction of a regular polygon of outer radius 1 with n sides. This construction is easy with straightedge and compass when n is a power of 2 or is 3 times a power of 2, and Euclid showed that a construction is possible for $n = 5$. But a construction cannot be managed with straightedge and compass for $n = 9$, for example, because a central angle in this case is 40° and the constructibility of $\cos 40^\circ$ would imply the constructibility of $\cos 20^\circ$. Thus the question is, for what values of n can a regular n-gon be constructed with straightedge and compass?

The remarkable answer was given by Gauss. By a **Fermat number** is meant any integer of the form $2^{2^N} + 1$. A **Fermat prime** is a Fermat number that is prime. The Fermat numbers for $N = 0, 1, 2, 3, 4$ are 3, 5, 17, 257, 65537, and each is a Fermat prime. No larger Fermat primes are known.[2] The answer given

[2] Many Fermat numbers for $N \geq 5$ are known not to be prime, sometimes by the discovery of an explicit factor and sometimes by a verification that 3 to the power 2^{2^N-1} is not congruent to -1 modulo $(2^{2^N} + 1)$. (Cf. Lemma 9.46.) For example Euler discovered that 641 divides $2^{2^5} + 1$. Computer calculations have shown that 2^{2^N+1} is not prime if $5 \leq N \leq 32$.

by Gauss, which we shall prove in stages in Sections 6–9, is as follows.

Theorem 9.25 (Gauss).[3] A regular n-gon is constructible with straightedge and compass if and only if n is the product of distinct Fermat primes and a power of 2.

We can show the relevance of Fermat primes right now, and we can give an indication that if n is a prime number, then a regular n-gon can be constructed if and only if n is a Fermat prime. But a full proof even of this statement will make use of Galois groups, which we take up in the next three sections.

For the necessity let n be prime, and suppose that a regular n-gon is constructible. Returning from degrees to radians, we observe that each central angle is $2\pi/n$. Thus the constructibility implies the constructibility of $\cos 2\pi/n$, and it follows that $e^{2\pi i/n} = \cos 2\pi/n + i \sin 2\pi/n$ is in the field $\mathcal{C} + i\mathcal{C}$ of constructible points in the complex plane. We have the factorization

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

and $e^{2\pi i/n}$ is a root of the second factor. The first example of Eisenstein's criterion (Corollary 8.22) in Section VIII.5 shows that the second factor is irreducible. According to the results of Section 1, $\mathbb{Q}(e^{2\pi i/n})$ is a simple algebraic extension of $\mathbb{Q}$ of degree $n - 1$.

Applying Theorem 9.24, we see that $n - 1$ must be a power of two. Let us write $n - 1 = 2^m$. Suppose $m = a2^N$ with a odd. If $a > 1$, then the equality $n = 2^{a2^N} + 1 = (2^{2^N})^a + 1^a$ exhibits n as the sum of two a^{th} powers, necessarily divisible by $2^{2^N} + 1$. Since n is assumed prime, we conclude that $a = 1$. Therefore $n = 2^{2^N} + 1$, and n is a Fermat prime.

We do not quite succeed in proving the converse at this point. If n is the Fermat prime $2^{2^N} + 1$, then the above argument shows that the degree of $\mathbb{Q}(e^{2\pi i/n})$ over $\mathbb{Q}$ is 2^{2^N}. However, we cannot yet conclude that $\mathbb{Q}(e^{2\pi i/n})$ can be built from $\mathbb{Q}$ by successively adjoining 2^N square roots, and thus the converse part of Theorem 9.24 is not immediately applicable. Once we have the theory of Galois groups in hand, we shall see that the existence of these intermediate extensions involving square roots is ensured, and then the constructibility follows.

[3] Gauss announced both the necessity and the sufficiency in this theorem in his *Disquisitiones Arithmeticae* in 1801, but he included a proof of only the sufficiency (partly in his articles 336 and 365). A proof of the necessity appeared in a paper of Pierre-Laurent Wantzel in 1837.

6. Separable Extensions

The **Galois group** $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ of a field extension $\mathbb{K}/\Bbbk$ is defined to be the set

$$\mathrm{Gal}(\mathbb{K}/\Bbbk) = \{\Bbbk \text{ automorphisms of } \mathbb{K}\}$$

with composition as group operation. An instance of this group was introduced in the context of Example 9 of Section IV.1; in this example the field $\Bbbk$ was the field $\mathbb{Q}$ of rationals and the field $\mathbb{K}$ was a number field $\mathbb{Q}[\theta]$, where θ is algebraic over $\mathbb{Q}$. In studying $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ in this chapter, we ordinarily assume that $\dim_{\Bbbk} \mathbb{K} < \infty$, but there will be instances where we do not want to make such an assumption.

Beginning in this section, we take up a study of Galois groups in general. We shall be interested in relationships between fields $\mathbb{L}$ with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ and subgroups of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. If H is a subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then

$$\mathbb{K}^H = \big\{x \in \mathbb{K} \mid \varphi(x) = x \text{ for all } \varphi \in H\big\}$$

is a field called the **fixed field** of H; it provides an example of an intermediate field $\mathbb{L}$ and gives a hint of the relationships we shall investigate. We begin with some examples; in each case the base field $\Bbbk$ is the field $\mathbb{Q}$ of rationals.

EXAMPLES OF GALOIS GROUPS.

(1a) $\mathbb{K} = \mathbb{Q}(\sqrt{-1}\,)$. If φ is in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then we must have $\varphi\big|_{\mathbb{Q}} = 1$, and $\varphi(\sqrt{-1}\,)$ must be a root of $X^2 + 1$. Thus $\varphi(\sqrt{-1}\,) = \pm\sqrt{-1}$. Since $\mathbb{Q}$ and $\sqrt{-1}$ generate $\mathbb{Q}(\sqrt{-1}\,)$, there are at most two such φ's. On the other hand, $\mathbb{Q}(\sqrt{-1}\,)$ and $\mathbb{Q}(-\sqrt{-1}\,)$ are simple extensions of $\mathbb{Q}$ such that $\sqrt{-1}$ and $-\sqrt{-1}$ have the same minimal polynomial. Theorem 9.11 therefore produces a $\mathbb{Q}$ automorphism of $\mathbb{Q}(\sqrt{-1}\,)$ with $\varphi(\sqrt{-1}\,) = -\sqrt{-1}$, namely complex conjugation. We conclude that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 2, hence that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$.

(1b) $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$. The same argument applies as in Example 1a, and the conclusion is that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$. The nontrivial element of the Galois group carries $\sqrt{2}$ to $-\sqrt{2}$ and is different from complex conjugation.

(2) $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$. If φ is in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then $\varphi\big|_{\mathbb{Q}} = 1$, and $\varphi(\sqrt[3]{2}\,)$ has to be a root of $X^3 - 2$. But $\mathbb{K}$ is a subfield of $\mathbb{R}$, and there is only one root of $X^3 - 2$ in $\mathbb{R}$. Hence $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}$. Since $\mathbb{Q}$ and $\sqrt[3]{2}$ generate $\mathbb{Q}(\sqrt[3]{2}\,)$ as a field, we see that $\varphi = 1$. We conclude that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 1, i.e., is the trivial group.

(3) $\mathbb{K} = \mathbb{Q}(r)$, where r is a root of $X^3 - X - \frac{1}{3}$. Any φ in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ fixes $\mathbb{Q}$ and sends r to a root of $X^3 - X - \frac{1}{3}$. In Example 2 of splitting fields in Section 2, we saw that all three complex roots of $X^3 - X - \frac{1}{3}$ lie in $\mathbb{K}$. Arguing as in Example 1a, we see that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ has order 3, hence that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_3$.

(4) $\mathbb{K} = \mathbb{Q}(e^{2\pi i/17})$. According to Section 5, this is the field we need to consider in addressing the constructibility of a regular 17-gon. We saw in that section that $[\mathbb{K} : \mathbb{Q}] = 16$ and that the minimal polynomial of $e^{2\pi i/17}$ over $\mathbb{Q}$ is $X^{16} + X^{15} + \cdots + X + 1$. The other roots of the minimal polynomial in $\mathbb{C}$ are $e^{2\pi il/17}$ for $2 \leq l \leq 16$, and these all lie in $\mathbb{K}$. Theorem 9.11 therefore gives us a $\mathbb{Q}$ automorphism φ_l of $\mathbb{K}$ sending $e^{2\pi i/17}$ into $e^{2\pi il/17}$ for each l with $1 \leq l \leq 16$. Since $\mathbb{Q}$ and $e^{2\pi i/17}$ generate $\mathbb{K}$, a $\mathbb{Q}$ automorphism of $\mathbb{K}$ is completely determined by its effect on $e^{2\pi i/17}$. Thus the order of $\text{Gal}(\mathbb{K}/\mathbb{Q})$ is 16. Let us determine the group structure. Since φ_l sends $e^{2\pi i/17}$ into $e^{2\pi il/17}$, it sends $e^{2\pi ir/17} = (e^{2\pi i/17})^r$ into $(e^{2\pi il/17})^r = e^{2\pi ilr/17}$. If we drop the exponential from the notation, we can think of φ_l as defined on the integers modulo 17, the formula being $\varphi_l(r) = rl \bmod 17$. From this viewpoint φ_l is an automorphism of the additive group of $\mathbb{F}_{17}$. Lemma 4.45 shows that the group of additive automorphisms of $\mathbb{F}_{17}$ is isomorphic to $\mathbb{F}_{17}^\times$, and it follows from Corollary 4.27 that $\text{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_{16}$. For our application of constructibility of a regular 17-gon, we would like to know whether the elements of $\mathbb{K}$ are constructible. Taking Theorem 9.24 into account, we therefore seek an intermediate field $\mathbb{L}$ of which $\mathbb{K}$ is a quadratic extension. Since we know that $\text{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic, we can let $H \subseteq \text{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_{16}$ be the 2-element subgroup, and it is natural to try the fixed field $\mathbb{L} = \mathbb{K}^H$. To understand this fixed field, we need to understand the isomorphism $\mathbb{F}_{17}^\times \cong C_{16}$ better. Modulo 17, we have

$$3^2 = 9, \quad 3^4 = -2^2, \quad 3^8 = 2^4 = -1, \quad 3^{16} = 1.$$

Consequently 3 is a generator of the cyclic group $\mathbb{F}_{17}^\times$. Then $H = \{3^8,\ 1\} = \{\pm 1\}$, and $L = \{x \in \mathbb{K} \mid \varphi_{-1}(x) = \varphi_{+1}(x) = x\}$. Since $\varphi_{-1}(e^{2\pi ir/17}) = e^{-2\pi ir/17} = \overline{e^{2\pi ir/17}}$ with the overbar indicating complex conjugation, we see that

$$\mathbb{L} = \mathbb{K}^H = \{x \in \mathbb{K} \mid x = \bar{x}\}.$$

It is not hard to check that indeed $[\mathbb{K} : \mathbb{L}] = 2$. Next we need a subfield $\mathbb{L}'$ of $\mathbb{L}$ with $[\mathbb{L} : \mathbb{L}'] = 2$. We try $\mathbb{L}' = \mathbb{K}^{H'}$ with H' equal to the 4-element cyclic subgroup of $\text{Gal}(\mathbb{K}/\mathbb{Q})$. Here we have a harder time checking whether $\mathbb{L}$ is indeed a quadratic extension of $\mathbb{L}'$, but we shall see in Section 8 that it is.[4] We continue in this way, and ultimately we end up with the chain of subfields that exhibits the members of $\mathbb{K}$ as constructible.

We seek to formulate the kind of argument in the above examples as a general theorem. We have to rule out the bad behavior of $\mathbb{Q}(\sqrt[3]{2}\,)$, where one root of the

[4] Actually, Section 8 will point out how Corollary 9.36 in Section 7 already handles this step. In fact, Corollary 9.37 handles this step with no supplementary argument.

minimal polynomial lies in the field but others do not, and we shall do this by assuming that the extension field is a "normal" extension, in a sense to be defined in Section 7. In addition, our style of argument shows that we might run into trouble if our irreducible polynomials over $\mathbb{k}$ can have repeated roots in $\mathbb{K}$. We shall rule out this bad behavior by insisting that the extension be "separable," a condition that we introduce now. The extension will automatically be separable if $\mathbb{K}$ has characteristic 0.

For the remainder of this section, fix the base field $\mathbb{k}$. An irreducible polynomial $F(X)$ in $\mathbb{k}[X]$ is called **separable** if it splits into *distinct* degree-one factors in its splitting field, i.e., if

$$f(X) = a_n(X - x_1)\cdots(X - x_n) \qquad \text{with } x_i \neq x_j \text{ for } i \neq j.$$

Once this splitting into distinct degree-one factors occurs in the splitting field, it occurs in any larger field as well.

Lemma 9.26. A polynomial $F(X)$ in $\mathbb{k}[X]$ has no repeated roots in its splitting field $\mathbb{K}$ if and only if $\mathrm{GCD}(F, F') = 1$, where $F'(X)$ is the derivative of $F(X)$.

PROOF. The polynomial $F(X)$ has repeated roots in $\mathbb{K}$ if and only if $F(X)$ is divisible by $(X - r)^2$ for some $r \in \mathbb{K}$, if and only if some $r \in \mathbb{K}$ has $F(r) = F'(r) = 0$ (by Corollary 9.17), if and only if some $r \in \mathbb{K}$ has $(X - r)$ dividing $F(X)$ and also $F'(X)$ (by the Factor Theorem), if and only if some $r \in \mathbb{K}$ has $(X - r)$ dividing $\mathrm{GCD}(F, F')$ when the GCD is computed in $\mathbb{K}$, if and only if $\mathrm{GCD}(F, F') \neq 1$ when the GCD is computed in $\mathbb{K}$ (by unique factorization in $\mathbb{K}[X]$). However, the Euclidean algorithm calculates $\mathrm{GCD}(F, F')$ without reference to the field, and the GCD is therefore the same when computed in $\mathbb{K}$ as it is when computed in $\mathbb{k}$. The lemma follows. □

Proposition 9.27. An irreducible polynomial $F(X)$ in $\mathbb{k}[X]$ is separable if and only if $F'(X) \neq 0$. In particular, every irreducible (necessarily nonconstant) polynomial is separable if $\mathbb{k}$ has characteristic 0.

PROOF. Since the polynomial $F(X)$ is irreducible and $\mathrm{GCD}(F, F')$ divides $F(X)$, $\mathrm{GCD}(F, F')$ equals 1 or $F(X)$ in all cases. If $F'(X) = 0$, then $\mathrm{GCD}(F, F') = F(X)$, and Lemma 9.26 implies that $F(X)$ is not separable. Conversely if $F'(X) \neq 0$, then the facts that $\mathrm{GCD}(F, F')$ divides $F'(X)$ and that $\deg F' < \deg F$ together imply that $\mathrm{GCD}(F, F')$ cannot equal $F(X)$. So $\mathrm{GCD}(F, F') = 1$, and Lemma 9.26 implies that $F(X)$ is separable. □

Fix an algebraic extension $\mathbb{K}$ of $\mathbb{k}$. We say that an element x of $\mathbb{K}$ is **separable** over $\mathbb{k}$ if the minimal polynomial of x over $\mathbb{k}$ is separable. We say that $\mathbb{K}$ is a **separable extension** of $\mathbb{k}$ if every x in $\mathbb{K}$ is separable over $\mathbb{k}$.

EXAMPLES OF SEPARABLE EXTENSIONS AND EXTENSIONS NOT SEPARABLE.

(1) In characteristic 0, every algebraic extension $\mathbb{K}$ of $\Bbbk$ is separable, by Proposition 9.27.

(2) Every algebraic extension $\mathbb{K}$ of a finite field $\Bbbk$ is separable. In fact, if x is in $\mathbb{K}$, then $[\Bbbk(x) : \Bbbk]$ is finite. Hence $\Bbbk(x)$ is a finite field. Then we may assume that $\mathbb{K}$ is a finite field, say of order $q = p^n$ with p prime. Since the multiplicative group $\mathbb{K}^\times$ has order $q - 1$, every nonzero element of $\mathbb{K}$ is a root of $X^{q-1} - 1$, and every element of $\mathbb{K}$ is therefore a root of $X^q - X$. The minimal polynomial $F(X)$ of x over $\Bbbk$ must then divide $X^q - X$. However, we know that $X^q - X$ splits over $\mathbb{K}$ and has no repeated roots. Thus $F(X)$ splits over $\mathbb{K}$ and has no repeated roots. Then $F(X)$ is separable over $\Bbbk$, and x is separable over $\Bbbk$.

(3) Let $\Bbbk = \mathbb{F}_p(x)$ be a transcendental extension of the finite field $\mathbb{F}_p$. Because this extension is transcendental, $X^p - x$ is irreducible over $\Bbbk$. Let $\mathbb{K}$ be the simple algebraic extension $\Bbbk[X]/(X^p - x)$, which we can write more simply as $\Bbbk(x^{1/p})$. The minimal polynomial of $x^{1/p}$ over $\Bbbk$ is $X^p - x$, and its derivative is $pX^{p-1} = 0$ since the derivative of the constant x is 0. By Proposition 9.27, $x^{1/p}$ is not separable over $\Bbbk$.

The way that separability enters considerations with Galois groups is through the following theorem, explicitly or implicitly. One of the corollaries of the theorem is that if $\mathbb{K}/\Bbbk$ is an algebraic extension, then the set of elements in $\mathbb{K}$ separable over $\Bbbk$ is a subfield of $\mathbb{K}$.

Theorem 9.28. Let $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$ be an inclusion of fields such that $\mathbb{K}$ is a simple algebraic extension of $\mathbb{L}$ of the form $\mathbb{K} = \mathbb{L}(\alpha)$, let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$, and let $M(X)$ be the minimal polynomial of α over $\mathbb{L}$. Then the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ by the number of field mappings of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$.

REMARKS. An algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ exists by Theorem 9.22. Because $\overline{\mathbb{K}}$ is known to exist, the present theorem reduces to Theorem 9.11 when $\mathbb{L} = \Bbbk$.

PROOF. Any field mapping $\varphi : \mathbb{K} \to \overline{\mathbb{K}}$ is uniquely determined by $\varphi\big|_{\mathbb{L}}$ and $\varphi(\alpha)$. If $\sigma = \varphi\big|_{\mathbb{L}}$, then the equality $M(\alpha) = 0$ implies that $M^\sigma(\varphi(\alpha)) = 0$, and thus $\varphi(\alpha)$ has to be a root of $M^\sigma(X)$. The number of distinct roots of $M^\sigma(X)$ in $\overline{\mathbb{K}}$ equals the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$; hence the number of possibilities for $\varphi(\alpha)$ is at most the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$. Consequently the number of such φ's fixing $\Bbbk$ is bounded above by the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ times the number of field mappings σ of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$.

For an inequality in the reverse direction, let $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$ be any field mapping of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$, put $\mathbb{L}' = \sigma(\mathbb{L})$, let x be any root of $M^\sigma(X)$, and form the subfield $\mathbb{L}'(x)$ of $\overline{\mathbb{K}}$. Theorem 9.11′ shows that there exists a field isomorphism $\varphi : \mathbb{L}(\alpha) \to \mathbb{L}'(x)$ with $\varphi\big|_{\mathbb{L}} = \sigma$ and $\varphi(\alpha) = x$, and we can regard φ as a field mapping of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$, extending σ, and having $\varphi(\alpha) = x$. Thus the number of field mappings $\varphi : \mathbb{K} \to \overline{\Bbbk}$ fixing $\Bbbk$ is bounded below by the product of the number of distinct roots of $M(X)$ in $\overline{\mathbb{K}}$ times the number of field homomorphisms σ of $\mathbb{L}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$. □

Corollary 9.29. Let $\mathbb{K} = \Bbbk(\alpha_1, \dots, \alpha_n)$ be a finite algebraic extension of the field $\Bbbk$, and let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. Then the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is $\le [\mathbb{K} : \Bbbk]$. Moreover, the following conditions are equivalent:

(a) the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ equals $[\mathbb{K} : \Bbbk]$,
(b) each α_j is separable over $\Bbbk(\alpha_1, \dots, \alpha_{j-1})$ for $1 \le j \le n$,
(c) each α_j is separable over $\Bbbk$ for $1 \le j \le n$.

PROOF. The minimal polynomial of α_j over $\Bbbk(\alpha_1, \dots, \alpha_{j-1})$ divides the minimal polynomial of α_j over $\Bbbk$. If the second of these polynomials has distinct roots in its splitting field, so does the first. Thus (c) implies (b).

For $1 \le j \le n$, let the minimal polynomial of α_j over $\Bbbk(\alpha_1, \dots, \alpha_{j-1})$ be $M_j(X)$, let d_j be the degree of $M_j(X)$, and let s_j be the number of distinct roots of $M_j(X)$ in $\overline{\mathbb{K}}$. Then $s_j \le d_j$ with equality for a particular j if and only if α_j is separable over $\Bbbk(\alpha_1, \dots, \alpha_{j-1})$, by definition. Also, $[\mathbb{K} : \Bbbk] = \prod_{j=1}^n d_j$ by Corollary 9.7, and the number of field mappings of $\mathbb{K}$ into $\overline{\mathbb{K}}$ fixing $\Bbbk$ is $\prod_{j=1}^n s_j$ by iterated application of Theorem 9.28. From these facts, the first conclusion of the corollary is immediate, and so is the equivalence of (a) and (b).

Condition (a) is independent of the order of enumeration of $\alpha_1, \dots, \alpha_n$. Since we can always take any particular α_j to be first, we see that (a) implies (c). □

Corollary 9.30. Let $\mathbb{K} = \Bbbk(\alpha_1, \dots, \alpha_n)$ be a finite algebraic extension of the field $\Bbbk$. If each α_j for $1 \le j \le n$ is separable over $\Bbbk$, then $\mathbb{K}/\Bbbk$ is a separable extension.

PROOF. Let β be in $\mathbb{K}$, We apply the equivalence of (a) and (c) in Corollary 9.29 once to the set of generators $\{\alpha_1, \dots, \alpha_n\}$ and once to the set of generators $\{\beta, \alpha_1, \dots, \alpha_n\}$, and the result is immediate. □

Corollary 9.31. If $\mathbb{K}/\Bbbk$ is an algebraic field extension, then the subset $\mathbb{L}$ of elements of $\mathbb{K}$ that are separable over $\Bbbk$ is a subfield of $\mathbb{K}$.

PROOF. If α and β are given in $\mathbb{L}$, we apply Corollary 9.30 to the extension $\Bbbk(\alpha, \beta)$ of $\Bbbk$ to see that $\mathbb{L}$ contains the subfield generated by $\Bbbk$ and the elements α and β. □

Proposition 9.32. If $\mathbb{K}/\Bbbk$ is a separable algebraic extension and if $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, then $\mathbb{K}$ is separable over $\mathbb{L}$, and $\mathbb{L}$ is separable over $\Bbbk$.

PROOF. The separability assertion about $\mathbb{L}/\Bbbk$ says the same thing about elements of $\mathbb{L}$ that separability of $\mathbb{K}/\Bbbk$ says about those same elements, and it is therefore immediate that $\mathbb{L}/\Bbbk$ is separable.

Next let us consider $\mathbb{K}/\mathbb{L}$. If x is in $\mathbb{K}$, let $F(X)$ be its minimal polynomial over $\Bbbk$, and let $G(X)$ be its minimal polynomial over $\mathbb{L}$. Since $F(X)$ is in $\mathbb{L}[X]$ and $F(x) = G(x) = 0$, $G(X)$ divides $F(X)$. Since $\mathbb{K}/\Bbbk$ is separable, $F(X)$ splits into distinct degree-one factors in its splitting field $\mathbb{F}$. The field $\mathbb{F}$ contains the splitting field of $G(X)$, and thus the degree-one factors of $G(X)$ in $\mathbb{F}[X]$ are a subset of the degree-one factors of $F(X)$ in $\mathbb{F}[X]$. There are no repeated factors for $F(X)$, and there can be no repeated factors for $G(X)$. Thus x is separable over $\mathbb{L}$, and $\mathbb{K}/\mathbb{L}$ is a separable extension. □

In studying Galois groups, we shall be chiefly interested in the following situation in Corollary 9.29: $\mathbb{K}$ is an algebraic field extension $\mathbb{K} = \Bbbk(\alpha_1, \dots, \alpha_n)$ of $\Bbbk$ for which every field mapping of $\mathbb{K}$ into an algebraic closure that fixes $\Bbbk$ actually carries $\mathbb{K}$ into itself. We seek conditions under which this situation arises, and then we mine the consequences. As we did in the study begun in Theorem 9.28, we begin with the case of a simple algebraic extension.

Let $\mathbb{K} = \Bbbk(\gamma)$ be a simple algebraic extension of $\Bbbk$, and let $F(X)$ be the minimal polynomial of γ over $\Bbbk$. Any member φ of the Galois group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ carries γ to another root γ' of $F(X)$, and φ is uniquely determined by γ' since $\Bbbk$ and γ generate the field $\mathbb{K}$. An element φ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ carrying γ to γ' can exist only if γ' is in $\mathbb{K}$. If γ' is in $\mathbb{K}$, then $\Bbbk(\gamma) \supseteq \Bbbk(\gamma')$, and the equal finite dimensionality of $\Bbbk(\gamma)$ and $\Bbbk(\gamma')$ forces $\Bbbk(\gamma) = \Bbbk(\gamma')$. In other words, if γ' is in $\mathbb{K}$, then the unique $\Bbbk$ isomorphism $\Bbbk(\gamma) \to \Bbbk(\gamma')$ of Theorems 9.10 and 9.11 carrying γ to γ' is a member of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Making a count of what happens to all the elements γ', we see that we have proved the following.

Proposition 9.33. Let $\mathbb{K} = \Bbbk(\gamma)$ be a simple algebraic extension of $\Bbbk$, and let $F(X)$ be the minimal polynomial of γ. Then

$$|\,\mathrm{Gal}(\mathbb{K}/\Bbbk)| \leq [\mathbb{K} : \Bbbk]$$

with equality if and only if $F(X)$ is a separable polynomial and $\mathbb{K}$ is the splitting field of $F(X)$ over $\Bbbk$.

EXAMPLE. For $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$ with minimal polynomial $F(X)$, we know that $F(X)$ does not split in $\mathbb{K}$; the nonreal roots of $F(X)$ do not lie in $\mathbb{K}$. Proposition 9.33 gives us $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{Q})| < [\mathbb{K} : \mathbb{Q}] = 3$, and a glance at the argument preceding Proposition 9.33 shows that $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{Q})|$ has to be 1.

It is possible to investigate the case of several generators directly, but it is more illuminating to reduce it to the case of a single generator as in Proposition 9.33. The tool for doing so is the following important theorem.

Theorem 9.34 (Theorem of the Primitive Element). Let $\mathbb{K}/\Bbbk$ be a separable algebraic extension with $[\mathbb{K} : \Bbbk] < \infty$. Then there exists an element γ in $\mathbb{K}$ such that $\mathbb{K} = \Bbbk(\gamma)$.

PROOF. We may assume that $\Bbbk$ is infinite because Corollary 4.27 shows that the multiplicative group of a finite field is cyclic. With $\Bbbk$ infinite, we can write $\mathbb{K} = \Bbbk(x_1, \dots, x_n)$, and we proceed by induction on n, the case $n = 1$ being trivial. For general n, let $\mathbb{L} = \Bbbk(x_1, \dots, x_{n-1})$, so that $\mathbb{K} = \mathbb{L}(x_n)$. By the inductive hypothesis, $\mathbb{L}$ is of the form $\mathbb{L} = \Bbbk(\alpha)$ for some α in $\mathbb{K}$, and thus $\mathbb{K} = \Bbbk(\alpha, x_n)$. Changing notation, we see that it is enough to prove that whenever $\mathbb{K}$ is a separable algebraic extension of the form $\mathbb{K} = \Bbbk(\alpha, \beta)$, then $\mathbb{K}$ is of the form $\mathbb{K} = \Bbbk(\gamma)$ for some γ. We shall show this for γ of the form $\gamma = \beta + c\alpha$ for some c in $\Bbbk$.

Let $F(X)$ and $G(X)$ be the minimal polynomials of α and β over $\Bbbk$, and let $\mathbb{K}'$ be an extension in which $F(X)G(X)$ splits, i.e., in which $F(X)$ and $G(X)$ both split. Let $\alpha_1 = \alpha,\ \alpha_2, \dots, \alpha_m$ and $\beta_1 = \beta,\ \beta_2, \dots, \beta_n$ be the roots of $F(X)$ and $G(X)$ in $\mathbb{K}'$, In each case the roots are necessarily distinct by definition of separability of α and β. Define $\mathbb{L} = \Bbbk(\gamma)$ with $\gamma = \beta + c\alpha$, where c is a member of $\Bbbk$ yet to be specified. For suitable c, we shall show that α is in $\mathbb{L}$. Then $\beta = \gamma - c\alpha$ must be in $\mathbb{L}$, and we obtain $\mathbb{K} \subseteq \mathbb{L}$. Since γ is in $\mathbb{K}$, the reverse inclusion is built into the construction, and thus we will have $\mathbb{K} = \mathbb{L}$.

We shall compute the minimal polynomial of α over $\mathbb{L}$. We know that α is a root of $F(X)$, and we put $H(X) = G(\gamma - cX)$. Then $H(X)$ is in $\mathbb{L}[X] \subseteq \mathbb{K}'[X]$, and $G(\beta) = 0$ implies $H(\alpha) = 0$. Therefore $X - \alpha$ divides both $F(X)$ and $H(X)$ in the ring $\mathbb{K}'[X]$. Let us determine $\mathrm{GCD}(F, H)$ in $\mathbb{K}'[X]$. The separability of α says that $X - \alpha$ divides $F(X)$ only once. Since $F(X)$ splits in $\mathbb{K}'[x]$, any other prime divisor of $\mathrm{GCD}(F, H)$ in $\mathbb{K}'[X]$ has to be of the form $X - \alpha_i$ with $i \neq 1$. The definition of $H(X)$ gives $H(\alpha_i) = G(\gamma - c\alpha_i)$. If $G(\gamma - c\alpha_i) = 0$, then $\gamma - c\alpha_i = \beta_j$ for some j, with the consequence that $\beta + c\alpha - c\alpha_i = \beta_j$ and $c = (\beta_j - \beta)(\alpha - \alpha_i)^{-1}$. Since $\Bbbk$ is an infinite field, we can choose c in $\mathbb{K}$ different from all the finitely many quotients $(\beta_j - \beta)(\alpha - \alpha_i)^{-1}$. For such a choice of c, $\mathrm{GCD}(F, H) = X - \alpha$ in $\mathbb{K}'[X]$. Then $\mathrm{GCD}(F, H) = X - \alpha$, up to a scalar factor, in $\mathbb{L}[X]$ since $F(X)$ and $H(X)$ are in $\mathbb{L}[X]$ and since the GCD can be computed without reference to the field containing both elements. The ratio of the constant term to the coefficient of X has to be in $\mathbb{L}$ independently of the scalar factor multiplying $X - \alpha$, and therefore α is in $\mathbb{L}$. This completes the proof. □

7. Normal Extensions

In using Galois groups to help in understanding field extensions, an example to keep in mind is the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. In this case the Galois group is trivial and therefore gives us no information about the extension. Thus it makes sense to regard the failure of equality to hold in an inequality $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \leq [\mathbb{K} : \Bbbk]$ as an undesirable situation.[5]

Proposition 9.33 suggests that the failure of equality to hold in the inequality $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \leq [\mathbb{K} : \Bbbk]$ has something to do with two phenomena. One is the possible failure of some polynomials over $\Bbbk$ to be separable, and the other is the failure of polynomials over $\Bbbk$ to split fully in $\mathbb{K}$ once they have at least one root in $\mathbb{K}$. Having examined separability in Section 6, we turn to this question of full splitting of polynomials.

Accordingly, we make a definition, choosing among several equivalent conditions the one that is usually the easiest to check in practice. A finite[6] algebraic extension $\mathbb{K}$ of a field $\Bbbk$ is said to be **normal** over $\Bbbk$ if $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$. The following proposition gives some equivalent formulations of this condition.

Proposition 9.34A. Let $\mathbb{K}$ be a finite algebraic extension of a field $\Bbbk$, and regard $\mathbb{K}$ as contained in a fixed algebraic closure $\overline{\mathbb{K}}$. Then the following conditions on $\mathbb{K}$ are equivalent.

(a) $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$, i.e., $\mathbb{K}$ is normal over $\Bbbk$,

(b) *every* irreducible polynomial $M(X)$ in $\Bbbk[X]$ with a root in $\mathbb{K}$ splits in $\mathbb{K}$, i.e., $\mathbb{K}$ contains the splitting field for each such $M(X)$,

(c) every $\Bbbk$ isomorphism of $\mathbb{K}$ into $\overline{\mathbb{K}}$ carries $\mathbb{K}$ into itself.

REMARK. Although (a) is often the easiest of the conditions to check, (b) is often the easiest to disprove. It is therefore quite handy to know the equivalence.

PROOF. Suppose that (a) holds. Let $F(X)$ be as in (a), and let its roots be $\gamma_1, \dots, \gamma_n$. Let $M(X)$ be an irreducible polynomial in $\Bbbk[X]$ with a root α in $\mathbb{K}$, and let $\mathbb{L}$ be the splitting field of $M(X)$ over $\mathbb{K}$. Let β be any root of $M(X)$ in $\mathbb{L}$. Since $M(X)$ is irreducible over $\Bbbk$, Theorem 9.11 produces a $\Bbbk$ isomorphism σ of $\Bbbk(\alpha)$ onto $\Bbbk(\beta)$ with $\sigma(\alpha) = \beta$. The isomorphism σ leaves $F(X)$ fixed, since the coefficients of $F(X)$ are in $\Bbbk$. Now the splitting field of $F(X)$ over $\Bbbk(\alpha)$

[5] We obtained this inequality in Proposition 9.33 only when $\mathbb{K}$ has a single generator over $\Bbbk$, but we take this case as indicative of what to expect more generally.

[6] Many books do not restrict the definition to finite extensions. The additional generality of infinite algebraic extensions will not be of benefit for our current purposes, and thus we restrict to finite extensions for now. But in Section VII.6 of *Advanced Algebra*, we shall enlarge the definition of "normal" to allow infinite algebraic extensions.

is $\mathbb{K}$, since the roots of $F(X)$ are in $\mathbb{K}$ and generate $\mathbb{K}$ over $\Bbbk(\alpha)$. Similarly the splitting field of $F(X)$ over $\Bbbk(\beta)$ is $\mathbb{K}(\beta)$. Application of Theorem 9.13′ yields a field isomorphism φ of $\mathbb{K}$ onto $\mathbb{K}(\beta)$ such that $\varphi\big|_{\Bbbk(\alpha)} = \sigma$ and such that φ carries the roots of $F(X)$ to the roots of $F(X)$. We can express α as a rational expression in $\gamma_1, \dots, \gamma_n$ with coefficients in $\Bbbk$, and then $\beta = \varphi(\alpha)$ is the same rational expression in $\varphi(\gamma_1), \dots, \varphi(\gamma_n)$, which themselves are members of $\mathbb{K}$. Therefore β is in $\mathbb{K}$, and the conclusion is that $M(X)$ splits in $\mathbb{K}$.

Suppose that (b) holds. Let φ be a $\Bbbk$ isomorphism of $\mathbb{K}$ into $\overline{\mathbb{K}}$, and let α be any element of $\mathbb{K}$. The minimal polynomial $M(X)$ of α over $\Bbbk$ is irreducible and has α as a root in $\mathbb{K}$. By (b), $M(X)$ splits in $\mathbb{K}$. The element $\varphi(\alpha)$ has to be a root of $M(X)$ since φ fixes the coefficients of $M(X)$, and all the roots of $M(X)$ are assumed to lie in $\mathbb{K}$. Therefore $\varphi(\alpha)$ lies in $\mathbb{K}$, and (b) implies (c).

Suppose that (c) holds. Since $\mathbb{K}$ is a finite algebraic extension of $\Bbbk$, we can write $\mathbb{K} = \Bbbk(\alpha_1, \dots, \alpha_n)$ for suitable elements $\alpha_1, \dots, \alpha_n$ of $\mathbb{K}$. Let $P_j(X)$ be the minimal polynomial of α_j over $\Bbbk$, and put $F(X) = \prod_{j=1}^n P_j(X)$. Since the roots $\alpha_1, \dots, \alpha_n$ generate $\mathbb{K}$ over $\Bbbk$, it is enough to show that every root of $F(X)$ lies in K, i.e., each root of each $P_j(X)$ lies in $\mathbb{K}$. Let β be a root of $P_j(X)$ in $\overline{\mathbb{K}}$. We know from Theorem 9.11 that there is a $\Bbbk$ isomorphism φ of $\Bbbk(\alpha_j)$ onto $\Bbbk(\beta)$ with $\varphi(\alpha_j) = \beta$. Theorem 9.23 shows that φ extends to a field mapping of $\mathbb{K}$ into $\overline{\mathbb{K}}$, and (c) shows that the extended φ sends $\mathbb{K}$ into itself. Therefore $\beta = \varphi(\alpha_j)$ lies in $\mathbb{K}$, and all the roots of $F(X)$ in $\overline{\mathbb{K}}$ lie in $\mathbb{K}$. Thus (c) implies (a). □

Now we can put together the properties of normal and separable extensions. It will be convenient to be able to refer in this context to the equivalence of (a) and (b) that was proved in Proposition 9.34A, and thus we repeat the statement of that equivalence here.

Proposition 9.35. Let $\mathbb{K}$ be a finite separable algebraic extension of a field $\Bbbk$, so that $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| \le [\mathbb{K} : \Bbbk]$. Then the following are equivalent.

(a) $\mathbb{K}$ is the splitting field of *some* $F(X)$ in $\Bbbk[X]$, i.e., $\mathbb{K}$ is normal over $\Bbbk$,

(b) *every* irreducible polynomial $M(X)$ in $\Bbbk[X]$ with a root in $\mathbb{K}$ splits in $\mathbb{K}$, i.e., $\mathbb{K}$ contains the splitting field for each such $M(X)$,

(c) $|\operatorname{Gal}(\mathbb{K}/\Bbbk)| = [\mathbb{K} : \Bbbk]$,

(d) $\Bbbk = \mathbb{K}^G$ for $G = \operatorname{Gal}(\mathbb{K}/\Bbbk)$.

REMARKS. The equivalence of (a) and (b) is part of Proposition 9.34A, and the fact that they are equivalent with (c) follows from Proposition 9.33 and the Theorem of the Primitive Element (Theorem 9.34). We prove that the equivalent (a), (b), and (c) imply (d), and that (d) implies (b).

PROOF. Suppose that the equivalent (a), (b), and (c) hold for $\mathbb{K}/\Bbbk$. We prove (d). Write $G = \operatorname{Gal}(\mathbb{K}/\Bbbk)$, and let $\Bbbk' = \mathbb{K}^G$. Since every member of $\operatorname{Gal}(\mathbb{K}/\Bbbk)$

fixes $\Bbbk'$, $\mathrm{Gal}(\mathbb{K}/\Bbbk) \subseteq \mathrm{Gal}(\mathbb{K}/\Bbbk')$. Meanwhile, (a) for $\mathbb{K}/\Bbbk$ implies (a) for $\mathbb{K}/\Bbbk'$, and $\mathbb{K}$ is separable over $\Bbbk'$ by Proposition 9.32. Since (a) implies (c), (c) holds for both $\Bbbk'$ and $\Bbbk$, and we have

$$[\mathbb{K} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)| \le |\,\mathrm{Gal}(\mathbb{K}/\Bbbk')| = [\mathbb{K} : \Bbbk'].$$

Since $\Bbbk' \supseteq \Bbbk$, the inequality of dimensions implies that $\Bbbk' = \Bbbk$. Thus (d) holds.

Suppose (d) holds. We prove (b). Let $M(X)$ be an irreducible polynomial in $\Bbbk[X]$ having a root r in $\mathbb{K}$. The polynomial $M(X)$ is necessarily the minimal polynomial of r over $\Bbbk$. Define

$$J(X) = \prod_{\varphi \in G} (X - \varphi(r)). \tag{$*$}$$

If φ_0 is in G, then F^{φ_0} is given by replacing each $\varphi(x)$ by $\varphi_0\varphi(r)$, and the product is unchanged. Therefore $J(X) = J^{\varphi_0}(X)$, and $J(X)$ is in $\mathbb{K}^G[X]$. From the assumption in (d), $\mathbb{K}^G = \Bbbk$. Therefore $J(X)$ is in $\Bbbk[X]$. Since $J(r) = 0$ and since $M(X)$ is the minimal polynomial of r over $\Bbbk$, $M(X)$ divides $J(X)$. Over $\mathbb{K}$, $J(X)$ splits because of its definition in $(*)$. By unique factorization in $\mathbb{K}[X]$, $M(X)$ must split too. Thus $M(X)$ splits in $\mathbb{K}[X]$, and (b) holds. □

Corollary 9.36. If $\mathbb{K}$ is a finite normal separable extension of $\Bbbk$ and if $\mathbb{L}$ is a field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, then $\mathbb{K}$ is a finite normal separable extension of $\mathbb{L}$, and the subgroup $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ has

$$\boxed{|H| \cdot [\mathbb{L} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|\,.}$$

PROOF. The field $\mathbb{K}$ is a separable extension of the intermediate field $\mathbb{L}$ by Proposition 9.32, and it is a normal extension by Proposition 9.35a. Therefore Proposition 9.35c gives $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| = [\mathbb{K} : \mathbb{L}]$, and we have

$$|H| \cdot [\mathbb{L} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \cdot [\mathbb{L} : \Bbbk] = [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \Bbbk] = [\mathbb{K} : \Bbbk] = |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|,$$

the last two equalities holding by Corollary 9.7 and Proposition 9.35c. □

Corollary 9.37. Let $\mathbb{K}/\Bbbk$ be a separable algebraic extension, and suppose that H is a finite subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Then $\mathbb{K}/\mathbb{K}^H$ is a finite normal separable extension, H is the subgroup $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, and $[\mathbb{K} : \mathbb{K}^H] = |H|$.

PROOF. Proposition 9.32 shows that $\mathbb{K}$ is separable over $\mathbb{K}^H$. For an arbitrary element x of $\mathbb{K}$, form the polynomial in $\mathbb{K}[X]$ given by

$$F(X) = \prod_{\varphi \in H} (X - \varphi(x)).$$

If φ_0 is in H, then F^{φ_0} is given by replacing each $\varphi(x)$ by $\varphi_0\varphi(x)$, and the product is unchanged. Therefore $F(X) = F^{\varphi_0}(X)$, and $F(X)$ is in $\mathbb{K}^H[X]$. Thus $F(X)$ is a polynomial in $\mathbb{K}^H[X]$ that has x as a root and splits in $\mathbb{K}$. The minimal polynomial $M(X)$ of x over $\mathbb{K}^H$ must divide $F(X)$, and it too has x as a root. By unique factorization in $\mathbb{K}[X]$, $M(X)$ must split in $\mathbb{K}$. Thus $\mathbb{K}/\mathbb{K}^H$ will be a normal extension if it is shown that $[\mathbb{K} : \mathbb{K}^H] < \infty$.

The element x has $[\mathbb{K}^H(x) : \mathbb{K}^H] = \deg M(X) \leq \deg F(X) = |H|$, and the claim is that $[\mathbb{K} : \mathbb{K}^H] \leq |H|$. Assuming the contrary, we would at some point have an inequality $[\mathbb{K}^H(x_1, \dots, x_n) : \mathbb{K}^H] > |H|$ because every element of $\mathbb{K}$ is algebraic over $\Bbbk$. By the Theorem of the Primitive Element (Theorem 9.34), $\mathbb{K}^H(x_1, \dots, x_n) = \mathbb{K}^H(z)$ for some element z, and therefore $[\mathbb{K}^H(x_1, \dots, x_n) : \mathbb{K}^H] = [\mathbb{K}^H(z) : \mathbb{K}^H] \leq |H|$, contradiction. We conclude that $[\mathbb{K} : \mathbb{K}^H] \leq |H|$. From the previous paragraph, $\mathbb{K}/\mathbb{K}^H$ is a finite separable normal extension.

The definition of $\mathbb{K}^H$ shows that $H \subseteq \operatorname{Gal}(\mathbb{K}/\mathbb{K}^H)$, and Proposition 9.35c gives $|\operatorname{Gal}(\mathbb{K}/\mathbb{K}^H)| = [\mathbb{K} : \mathbb{K}^H]$. Putting these facts together with the inequality $[\mathbb{K} : \mathbb{K}^H] \leq |H|$ from the previous paragraph, we have

$$|H| \leq |\operatorname{Gal}(\mathbb{K}/\mathbb{K}^H)| = [\mathbb{K} : \mathbb{K}^H] \leq |H|$$

with equality on the left only if $H = \operatorname{Gal}(\mathbb{K}/\mathbb{K}^H)$. Equality must hold throughout the displayed line since the ends are equal, and therefore $H = \operatorname{Gal}(\mathbb{K}/\mathbb{K}^H)$. □

8. Fundamental Theorem of Galois Theory

We are now in a position to obtain the main result in Galois theory.

Theorem 9.38 (Fundamental Theorem of Galois Theory). If $\mathbb{K}$ is a finite normal separable extension of $\Bbbk$, then there is a one-one inclusion-reversing correspondence between the subgroups H of $\operatorname{Gal}(\mathbb{K}/\Bbbk)$ and the subfields $\mathbb{L}$ of $\mathbb{K}$ that contain $\Bbbk$, corresponding elements H and $\mathbb{L}$ being given by

$$\mathbb{L} = \mathbb{K}^H \qquad \text{and} \qquad H = \operatorname{Gal}(\mathbb{K}/\mathbb{L}).$$

The effect of the theorem is to take an extremely difficult problem, namely finding intermediate fields, and reduce it to a problem that is merely difficult, namely finding the Galois group. For example the finiteness of $\operatorname{Gal}(\mathbb{K}/\Bbbk)$ implies that there are only finitely many subgroups of $\operatorname{Gal}(\mathbb{K}/\Bbbk)$, and the theorem therefore implies that there are only finitely many intermediate fields; this finiteness of the number of intermediate fields is not so obvious without the theorem.

As a reminder of the availability of Theorem 9.38, Proposition 9.35, and Corollary 9.36, it is customary to refer to a finite normal separable extension as a **finite Galois extension**.

Before coming to the proof of the theorem, let us examine what the theorem says for the examples in Section 6. In each case the field $\mathbb{k}$ is the field $\mathbb{Q}$ of rationals. The extensions are separable because the characteristic is 0.

EXAMPLES.

(1a) $\mathbb{K} = \mathbb{Q}(\sqrt{-1}\,)$. This is the splitting field[7] for $X^2 + 1$. Proposition 9.33 gives $|\operatorname{Gal}(\mathbb{K}/\mathbb{Q})| = [\mathbb{K} : \mathbb{Q}] = 2$. Thus $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong C_2$. There are no nontrivial subgroups, and there are consequently no intermediate fields. We knew this already since there cannot be any intermediate $\mathbb{Q}$ vector spaces between $\mathbb{Q}$ and $\mathbb{K}$. Thus the theorem tells us nothing new.

(1b) $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$. Similar remarks apply.

(2) $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$. This extension is not normal, as a consequence of (b) in Proposition 9.34A. (Namely $X^3 - 2$ has a root in $\mathbb{K}$ but does not split in $\mathbb{K}$.) Theorem 9.38 does not apply to $\mathbb{K}$. If we adjoin r to $\mathbb{K}$ with $r^2 + (\sqrt[3]{2}\,)r + (\sqrt[3]{2}\,)^2 = 0$, we obtain the splitting field $\mathbb{K}'$ for $X^3 - 2$ over $\mathbb{Q}$. Then $\mathbb{K}'$ is a normal extension of $\mathbb{Q}$, and the theorem applies. Since each element of $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ permutes the three roots of $X^3 - 2$ and is determined by its effect on these roots, $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_3$. The Galois group $\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ has order $[\mathbb{K}' : \mathbb{Q}] = 6$ and hence is isomorphic to the whole symmetric group $\mathfrak{S}_3$. The group $\mathfrak{S}_3$ has three subgroups of order 2 and one subgroup of order 3. Therefore $\mathbb{K}'$ has three intermediate fields of degree 3 and one of degree 2. The intermediate fields of degree 3 are the three fields generated by $\mathbb{Q}$ and one of the three roots of $X^3 - 2$. The intermediate field of degree 2 corresponds to the alternating subgroup of order 3 and is the subfield generated by $\mathbb{Q}$ and the cube roots of 1. It is the splitting field for $X^2 + X + 1$ over $\mathbb{Q}$.

(3) $\mathbb{K} = \mathbb{Q}(r)$, where r is a root of $X^3 - X - \frac{1}{3}$. We know from Section 2 that $X^3 - X - \frac{1}{3}$ is irreducible over $\mathbb{Q}$ and splits in $\mathbb{K}$, and $\mathbb{K}$ by definition is therefore normal. Proposition 9.33 tells us that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ has order 3 and hence is isomorphic to C_3. There are no nontrivial subgroups, and Theorem 9.38 tells us that there are no intermediate fields. We could have seen in more elementary fashion that there are no intermediate fields by using Corollary 9.7, since the corollary tells us that the degree of an intermediate field would have to divide 3.

(4) $\mathbb{K} = \mathbb{Q}(e^{2\pi 1/17})$. We have seen that $[\mathbb{K} : \mathbb{Q}] = 16$ and that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{F}_{17}^\times \cong C_{16}$. Let c be a generator of the cyclic Galois group. Let $H_2 = \{1, c^8\}$,

[7] It is customary to regard the algebraic closure of $\mathbb{Q}$ as a subfield of $\mathbb{C}$, and thus there is no ambiguity in referring to *the* splitting field.

$H_4 = \{1, c^4, c^8, c^{12}\}$, and $H_8 = \{1, c^2, c^4, c^6, c^8, c^{10}, c^{12}, c^{14}\}$. Then put

$$\mathbb{L}_2 = \mathbb{K}^{H_2}, \qquad \mathbb{L}_4 = \mathbb{K}^{H_4}, \qquad \mathbb{L}_8 = \mathbb{K}^{H_8}.$$

The inclusions among our subgroups are

$$\{1\} \subseteq H_2 \subseteq H_4 \subseteq H_8 \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{Q}),$$

and the theorem says that the correspondence with intermediate fields reverses inclusions. Then we have

$$\mathbb{K} \supseteq \mathbb{L}_2 \supseteq \mathbb{L}_4 \supseteq \mathbb{L}_8 \supseteq \mathbb{Q}.$$

Applying Corollary 9.36, we see that each of these subfields is a quadratic extension of the next-smaller one. Theorem 9.24 says that the members of $\mathbb{K}$ are therefore constructible with straightedge and compass. Consequently a regular 17-gon is constructible with straightedge and compass. The constructibility or nonconstructibility of regular n-gons for general n will be settled in similar fashion in the next section. In Section 12 we return to the question of using Galois theory to guide us through the actual steps of the construction when it is possible.

PROOF OF THEOREM 9.38. The function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ has domain the set of all intermediate fields and range the set of all subgroups of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, since an element in $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is necessarily in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Each such extension $\mathbb{K}/\mathbb{L}$ is separable by Proposition 9.32 and is normal by Proposition 9.34A. Thus Proposition 9.35d applies to each $\mathbb{K}/\mathbb{L}$ and shows that $\mathbb{L} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{L})}$. Consequently the function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is one-one. If H is a subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then Corollary 9.37 shows that $\mathbb{L} = \mathbb{K}^H$ is an intermediate field for which $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$, and therefore the function $\mathbb{L} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is onto.

It is immediate from the definition of Galois group that $\mathbb{L}_1 \subseteq \mathbb{L}_2$ implies $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_1) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{L}_2)$, and it is immediate from the formula $\mathbb{L} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{L})}$ that $\mathrm{Gal}(\mathbb{K}/\mathbb{L}_1) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{L}_2)$ implies $\mathbb{L}_1 \subseteq \mathbb{L}_2$. This completes the proof. □

Corollary 9.39. If $\mathbb{K}$ is a finite Galois extension of $\Bbbk$ and if $\mathbb{L}$ is a subfield of $\mathbb{K}$ that contains $\Bbbk$, then $\mathbb{L}$ is a normal extension of $\Bbbk$ if and only if $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. In this case, the map $\mathrm{Gal}(\mathbb{K}/\Bbbk) \to \mathrm{Gal}(\mathbb{L}/\Bbbk)$ given by restriction from $\mathbb{K}$ to $\mathbb{L}$ is a group homomorphism that descends to a group isomorphism

$$\mathrm{Gal}(\mathbb{K}/\Bbbk) \big/ \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk).$$

PROOF. Let $\mathbb{L}$ correspond to $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ in Theorem 9.38, so that $\mathbb{L} = \mathbb{K}^H$. If φ is in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then

$$\begin{aligned} \mathbb{K}^{\varphi H \varphi^{-1}} &= \{k \in \mathbb{K} \mid \varphi h \varphi^{-1}(k) = k \text{ for all } h \in H\} \\ &= \{\varphi(k') \in \mathbb{K} \mid \varphi h(k') = \varphi(k') \text{ for all } h \in H\} \\ &= \{\varphi(k') \in \mathbb{K} \mid h(k') = k' \text{ for all } h \in H\} \\ &= \varphi(\mathbb{K}^H) = \varphi(\mathbb{L}). \end{aligned}$$

Since the correspondence of Theorem 9.38 is one-one onto, $\varphi H \varphi^{-1} = H$ if and only if $\varphi(\mathbb{L}) = \mathbb{L}$. Therefore H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ if and only if $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$.

Now suppose that H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. We have just seen that $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$. Then each φ defines by restriction a member $\overline{\varphi} = \varphi\big|_{\mathbb{L}}$ of $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and $\varphi \mapsto \overline{\varphi}$ is certainly a group homomorphism. The kernel of $\varphi \mapsto \overline{\varphi}$ is the subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ given by

$$\big\{\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk) \bigm| \varphi\big|_{\mathbb{L}} = 1\big\},$$

and this is just $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$. Thus $\varphi \mapsto \overline{\varphi}$ descends to a one-one homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)\big/\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ into $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and we have

$$|\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|/|\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \le |\,\mathrm{Gal}(\mathbb{L}/\Bbbk)|.$$

We make use of Corollary 9.7 relating degrees of extensions. Applying Proposition 9.35c to $\mathbb{K}/\Bbbk$ and $\mathbb{K}/\mathbb{L}$, as well as Proposition 9.33 to $\mathbb{L}/\Bbbk$, we obtain

$$\begin{aligned} [\mathbb{L} : \Bbbk] &= [\mathbb{K} : \Bbbk]\big/[\mathbb{K} : \mathbb{L}] \\ &= |\,\mathrm{Gal}(\mathbb{K}/\Bbbk)|/|\,\mathrm{Gal}(\mathbb{K}/\mathbb{L})| \\ &\le |\,\mathrm{Gal}(\mathbb{L}/\Bbbk)| \le [\mathbb{L} : \Bbbk], \end{aligned}$$

with equality at the first $\le$ sign only if $\varphi \mapsto \overline{\varphi}$ is onto $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ and with equality at the second $\le$ sign only if $\mathbb{L}$ is the splitting field over $\Bbbk$ of the minimal polynomial of a certain element γ of $\mathbb{L}$. Equality must hold in both cases because the end members of the display are equal, and we conclude that $\varphi \mapsto \overline{\varphi}$ is onto and that $\mathbb{L}/\Bbbk$ is a normal extension.

We are left with proving that if $\mathbb{L}/\Bbbk$ is a normal extension, then H is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. Thus let $\mathbb{L}/\Bbbk$ be normal. In view of the conclusion of the first paragraph of the proof, it is enough to prove that $\varphi(\mathbb{L}) = \mathbb{L}$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$. By definition of normal extension, $\mathbb{L}$ is the splitting field of some polynomial $F(X)$ in $\Bbbk[X]$. We may assume that $F(X)$ is monic. Let us write

$$F(X) = (X - x_1) \cdots (X - x_n) \qquad \text{with all } x_j \text{ in } \mathbb{L}.$$

Applying a given member φ of Gal($\mathbb{K}/\Bbbk$) to the coefficients, we obtain

$$F(X) = (X - \varphi(x_1)) \cdots (X - \varphi(x_n)),$$

and here the $\varphi(x_j)$'s are known only to be in $\mathbb{K}$. By unique factorization in $\mathbb{K}[X]$, $\varphi(x_i) = x_{j(i)}$ for some $j = j(i)$. Therefore $\varphi(x_i)$ is in $\mathbb{L}$ for all i. Since $\mathbb{L}$ is the splitting field of $F(X)$ over $\Bbbk$, $\mathbb{L} = \Bbbk(x_1, \dots, x_n)$. Thus φ maps $\mathbb{L}$ into $\mathbb{L}$. □

The examples of Galois groups given in Section 6 all involved fields that are finite extensions of the rationals $\mathbb{Q}$. As we shall see in Section 17, it is important for the understanding of Galois groups of finite extensions of $\mathbb{Q}$ to be able to identify Galois groups of finite extensions of *finite* fields. This matter is addressed in the following proposition.

Proposition 9.40. Let $\mathbb{K}$ be a finite extension of the finite field $\mathbb{F}_q$, where $q = p^a$ and p is prime, and suppose that $[\mathbb{K} : \mathbb{F}_q] = n$. Then $\mathbb{K}$ is a Galois extension of $\mathbb{F}_q$, the Galois group Gal($\mathbb{K}/\mathbb{F}_q$) is cyclic of order n, and a generator is the a^{th}-power Frobenius automorphism $x \mapsto x^q = x^{p^a}$.

PROOF. Theorem 9.14 shows that $\mathbb{K}$ is a splitting field for $X^{q^n} - X$ over $\mathbb{F}_p$. Hence it is a splitting field for $X^{q^n} - X$ over $\mathbb{F}_q$, and $\mathbb{K}/\mathbb{F}_q$ is a normal extension. The polynomial $X^{q^n} - X$ has no multiple roots, and it follows that $\mathbb{K}/\mathbb{F}_q$ is a separable extension.

Define φ by $\varphi(x) = x^q$. Lemma 9.18 shows that φ is an automorphism of $\mathbb{K}$. Since every member of $\mathbb{F}_q^\times$ has order dividing $q-1$, every nonzero element of $\mathbb{F}_q$ is fixed by φ. The map φ certainly carries 0 to 0, and thus φ is in Gal($\mathbb{K}/\mathbb{F}_q$). By a similar argument, φ^n fixes every element of $\mathbb{K}$, and hence $\varphi^n = 1$. Corollary 4.27 shows that $\mathbb{K}^\times$ is cyclic, hence that there exists an element y in $\mathbb{K}^\times$ such that $y^l \neq 1$ for $1 \leq l < q^n - 1$. This y has $y^l \neq y$ for $2 \leq l \leq q^n - 1$. Then $\varphi^k(y) = y^{q^k}$ cannot be 1 for $1 \leq k \leq n - 1$, and φ must have order exactly n. This shows that φ generates a cyclic subgroup of order n in Gal($\mathbb{K}/\mathbb{F}_q$). Since n is an upper bound for the order of Gal($\mathbb{K}/\mathbb{F}_q$) by Proposition 9.33, this cyclic subgroup exhausts the Galois group. □

EXAMPLE. Suppose that we are given a polynomial with coefficients in $\mathbb{F}_p$ and we want to find the Galois group of a splitting field. Since there are efficient computer programs for factoring the polynomial into irreducible polynomials, let us take that factorization as done. The Galois group will be cyclic of some order with generator the Frobenius automorphism $x \mapsto x^p$. For an irreducible polynomial of degree n, a splitting field has degree n, and the smallest power of $x \mapsto x^p$ that gives the identity is the n^{th} power. The conclusion is that the Galois group is cyclic of order equal to the least common multiple of the degrees of the irreducible constituents, a generator being the Frobenius automorphism.

9. Application to Constructibility of Regular Polygons

In this section we use Galois theory to give a proof of Theorem 9.25 concerning the constructibility of regular n-gons. Let us recall the statement.

THEOREM 9.25 (Gauss). A regular n-gon is constructible with straightedge and compass if and only if n is the product of distinct Fermat primes and a power of 2.

PROOF OF SUFFICIENCY. First suppose that n is a Fermat prime $n = 2^{2^N} + 1$. Let $\mathbb{K} = \mathbb{Q}(e^{2\pi i/n})$. We saw in Section 5 that the degree $[\mathbb{K} : \mathbb{Q}]$ is 2^{2^N}, hence is a power of 2. Furthermore we know that $\mathbb{K}$ is a separable extension of $\mathbb{Q}$, being of characteristic 0, and it is normal, being the splitting field for $X^n - 1$ over $\mathbb{Q}$. In Section 6 we saw that the Galois group $\text{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic of order 2^{2^N}. Let c be a generator of this group. For each integer k with $0 \le k \le 2^N$, let H_{2^k} be the unique cyclic subgroup of $\text{Gal}(\mathbb{K}/\mathbb{Q})$ of order 2^k. For this subgroup, $c^{2^{2^N-k}}$ is a generator. Put $\mathbb{L}_{2^k} = \mathbb{K}^{H_{2^k}}$. Then we have inclusions

$$\{1\} \subseteq H_2 \subseteq H_{2^2} \subseteq \cdots H_{2^k} \subseteq \cdots \subseteq H_{2^{2^N-1}} \subseteq H_{2^{2^N}} = \text{Gal}(\mathbb{K}/\mathbb{Q}),$$

the index being 2 at each stage. Theorem 9.38 says that the correspondence with intermediate fields reverses inclusions and that the degree of each consecutive extension of subfields matches the index of the corresponding consecutive subgroups. The intermediate fields are therefore of the form

$$\mathbb{K} \supseteq \mathbb{L}_2 \supseteq \mathbb{L}_{2^2} \supseteq \cdots \mathbb{L}_{2^k} \supseteq \cdots \supseteq \mathbb{L}_{2^{2^N-1}} \supseteq \mathbb{L}_{2^{2^N}} = \mathbb{Q},$$

and the degree in each case is 2. In view of the formula for the roots of a quadratic polynomial, each extension is obtained by adjoining some square root. By Theorem 9.24 the members of $\mathbb{K}$ are constructible with straightedge and compass. In particular, $e^{2\pi i/n}$ is constructible, and a regular n-gon is constructible.

Next suppose that $e^{2\pi i/r}$ and $e^{2\pi i/s}$ are both constructible and that $\text{GCD}(r, s) = 1$. Choose integers a and b with $ar + bs = 1$, so that $\frac{a}{s} + \frac{b}{r} = \frac{1}{rs}$. Then the equality $(e^{2\pi i/s})^a (e^{2\pi i/r})^b = e^{2\pi i/(rs)}$ shows that $e^{2\pi i/(rs)}$ is constructible. This proves the sufficiency for any product of distinct Fermat primes. Bisection of an angle is always possible with straightedge and compass, as was observed in the third paragraph of Section 5, and the proof of the sufficiency in Theorem 9.25 is therefore complete. □

REMARKS. The above proof shows that the construction is possible, but it gives little clue how to carry out the construction. We shall address this matter further in Section 12.

We turn our attention to the necessity—that n has to be the product of distinct Fermat primes and a power of 2 if a regular n-gon is constructible. For the moment let $n \geq 1$ be any integer. Let us consider the distinct n^{th} roots of 1 in $\mathbb{C}$, which are $e^{k2\pi i/n}$ for $0 \leq k < n$. The order of each of these elements divides n, and the order is exactly n if and only if $\text{GCD}(k, n) = 1$. In this case we say that $e^{k2\pi i/n}$ is a **primitive** n^{th} root of 1. Define the **cyclotomic polynomial** $\Phi_n(X)$ by

$$\Phi_n(X) = \prod_{\substack{\text{GCD}(k,n)=1, \\ 0 \leq k < n}} (X - e^{k2\pi i/n}).$$

Each such polynomial is monic by inspection. The splitting field $\mathbb{Q}(e^{2\pi i/n})$ in $\mathbb{C}$ is called a **cyclotomic field**. Since the complex roots of $X^n - 1$ are exactly the numbers $e^{k2\pi i/n}$, we have

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

the product being taken over the positive divisors d of n.

Lemma 9.41. Each cyclotomic polynomial $\Phi_n(X)$ lies in $\mathbb{Z}[X]$, and the degree of $\Phi_n(X)$ is $\varphi(n)$, where φ is the Euler φ function defined just before Corollary 1.10.

PROOF. We know that $\Phi_n(X)$ is in $\mathbb{C}[X]$, and we begin by showing by induction on n that $\Phi_n(X)$ is in $\mathbb{Q}[X]$. For $n = 1$, we have $\Phi_1[X] = X - 1$, and the assertion is true. If it is true for all d with $1 \leq d < n$, then the formula $X^n - 1 = \prod_{d|n} \Phi_d(X)$ and induction show that $X^n - 1 = \Phi_n(X)F(X)$ for some $F(X)$ in $\mathbb{Q}[X]$. By the division algorithm, $X^n - 1 = F(X)Q(X) + R(X)$ for polynomials $Q(X)$ and $R(X)$ in $\mathbb{Q}[X]$ with $R(X) = 0$ or $\deg R(X) < \deg F(X)$. Subtraction gives $F(X)\big(\Phi_n(X) - Q(X)\big) = -R(X)$ in $\mathbb{C}[X]$. If $R(X)$ is not 0, then $\deg R(X) < \deg F(X)$ gives a contradiction. Therefore $R(X) = 0$ and $F(X)\big(\Phi_n(X) - Q(X)\big) = 0$. Since $\mathbb{C}[X]$ is an integral domain, $\Phi_n(X) = Q(X)$. Thus $\Phi_n(X)$ is in $\mathbb{Q}[X]$, and the induction is complete.

To see that $\Phi_n(X)$ is in $\mathbb{Z}[X]$, we again induct, the case $n = 1$ being clear. The formula $X^n - 1 = \prod_{d|n} \Phi_d(X)$ and induction show that $X^n - 1 = \Phi_n(X)F(X)$ for some $F(X)$ in $\mathbb{Z}[X]$. Since $\Phi_n(X)$ is known to be in $\mathbb{Q}[X]$, Corollary 8.20c shows that $\Phi_n(X)$ is in $\mathbb{Z}[X]$, and the induction is complete. □

Lemma 9.42. Each cyclotomic polynomial $\Phi_n(X)$ is irreducible as a member of $\mathbb{Q}[X]$.

PROOF. Let ζ be a primitive n^{th} root of 1, let p be a prime number not dividing n, let $F(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$, and let $G(X)$ be the minimal polynomial of ζ^p. The main step is to show that $F(X) = G(X)$.

To carry out this step, we observe that $F(\zeta) = G(\zeta^p) = 0$ and that $F(X)$ and $G(X)$ must divide $\Phi_n(X)$. Arguing by contradiction, suppose that $F(X) \neq G(X)$. Then $\mathrm{GCD}(F, G) = 1$ since $F(X)$ and $G(X)$ are irreducible over $\mathbb{Q}$, and therefore $F(X)G(X)$ divides $\Phi_n(X)$. Hence we can write

$$X^n - 1 = F(X)G(X)H(X),$$

and $H(X)$ is a monic member of $\mathbb{Z}[X]$ by Lemma 9.41 and Corollary 8.20c. Since ζ is a root of $G(X^p)$, we must have $G(X^p) = F(X)M(X)$ for some monic polynomial $M(X)$ in $\mathbb{Z}[X]$. We apply the substitution homomorphism to $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ that carries X to X and reduces the coefficients modulo p; the mapping on the coefficients will be denoted by a bar. Then we have

$$X^n - \overline{1} = \overline{F}(X)\overline{G}(X)\overline{H}(X) \qquad \text{and} \qquad \overline{G}(X)^p = \overline{G}(X^p) = \overline{F}(X)\overline{M}(X),$$

the equality $\overline{G}(X)^p = \overline{G}(X^p)$ following from Lemma 9.18. If $\overline{Q}(X)$ is a prime factor of $\overline{F}(X)$, then $\overline{Q}(X)$ divides $\overline{G}(X)^p$ and therefore must divide $\overline{G}(X)$. So $\overline{Q}(X)^2$ divides $X^n - \overline{1}$. Therefore $X^n - \overline{1}$ has multiple roots in its splitting field, in contradiction to Corollary 9.17 and the fact that the derivative of $X^n - \overline{1}$ is nonzero at each nonzero member of $\mathbb{F}_p$ (since $\mathrm{GCD}(p, n) = 1$ by assumption). We conclude that $F(X) = G(X)$.

Now suppose that r is a positive integer with $\mathrm{GCD}(r, n) = 1$. Then we can write $r = p_1 \cdots p_l$ with each p_j not dividing n, and we see inductively that ζ^r has $F(X)$ as minimal polynomial. Thus $F(X)$ has at least $\varphi(n)$ roots. Since $F(X)$ divides $\Phi_n(X)$, we must have $F(X) = \Phi_n(X)$. Therefore $\Phi_n(X)$ is irreducible over $\mathbb{Q}$. □

PROOF OF NECESSITY IN THEOREM 9.25. Theorem 9.24 shows that the degree $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$ must be a power of 2 if a regular n-gon is constructible. Since $e^{2\pi i/n}$ is a root of $\Phi_n(X)$ and since Lemma 9.42 shows $\Phi_n(X)$ to be irreducible over $\mathbb{Q}$, $\Phi_n(X)$ is the minimal polynomial of $e^{2\pi i/n}$ over $\mathbb{Q}$. By Lemma 9.41 the degree in question is given by $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler φ function. Corollary 1.10 shows that if $n = p_1^{k_1} \cdots p_r^{k_r}$ is a prime factorization of n into distinct prime powers with each $k_j > 0$, then

$$\varphi(n) = \prod_{j=1}^{r} p_j^{k_j - 1}(p_j - 1).$$

For constructibility this must be a power of 2. Then each p_j dividing n must be 1 more than a power of 2, i.e., must be 2 or a Fermat prime, and the only p_j allowed to have p_j^2 dividing n is $p_j = 2$. □

10. Application to Proving the Fundamental Theorem of Algebra

In this section we use Galois theory to give a proof of the Fundamental Theorem of Algebra. Let us recall the statement.

THEOREM 1.18 (Fundamental Theorem of Algebra). Any polynomial in $\mathbb{C}[X]$ with degree ≥ 1 has at least one root.

We begin with a lemma that handles three easy special cases.

Lemma 9.43. There are no finite extensions of $\mathbb{R}$ of odd degree greater than 1, the only extension of $\mathbb{R}$ of degree 2 up to $\mathbb{R}$ isomorphism is $\mathbb{C}$, and there are no finite extensions of $\mathbb{C}$ of degree 2.

PROOF. If $\mathbb{K}$ is a finite extension of $\mathbb{R}$ of odd degree and if x is in $\mathbb{K}$, then $[\mathbb{R}(x) : \mathbb{R}]$ is odd, and consequently the minimal polynomial $F(X)$ of x over $\mathbb{R}$ is irreducible of odd degree. By Proposition 1.20, which is derived from the Intermediate Value Theorem of Section A3 of the appendix, $F(X)$ has at least one root in $\mathbb{R}$. Therefore $F(X)$ has degree 1, and x is in $\mathbb{R}$.

If $F(X)$ is an irreducible polynomial in $\mathbb{R}[X]$ of degree 2, then $F(X)$ splits in $\mathbb{C}$ by the quadratic formula, and hence the only extension of $\mathbb{R}$ of degree 2 is $\mathbb{C}$, up to $\mathbb{R}$ isomorphism, by the uniqueness of splitting fields (Theorem 9.13).

Let $G(X) = X^2 + bX + c$ be a polynomial in $\mathbb{C}[X]$ of degree 2. Then $G(X)$ has a root x in $\mathbb{C}$ given by the quadratic formula since every member of $\mathbb{C}$ has a square root[8] in $\mathbb{C}$, and $G(X)$ cannot be irreducible. Since any finite extension of $\mathbb{C}$ of degree 2 would have to be of the form $\mathbb{C}(x)$, with x equal to a root of an irreducible quadratic polynomial over $\mathbb{C}$, there can be no such extension. □

PROOF OF THEOREM 1.18. First let us show that every irreducible member $F(X)$ of $\mathbb{R}[X]$ splits over $\mathbb{C}$. Let $\mathbb{K}$ be a splitting field for $F(X)$. Say that $[\mathbb{K} : \mathbb{R}] = 2^m N$ with N odd. Then $\mathbb{K}$ is a Galois extension of $\mathbb{R}$, and $|\operatorname{Gal}(\mathbb{K}/\mathbb{R})| = 2^m N$. By the Sylow Theorems (particularly Theorem 4.59a), let H be a Sylow 2-subgroup of $\operatorname{Gal}(\mathbb{K}/\mathbb{R})$. This H has $|H| = 2^m$. The field $\mathbb{L} = \mathbb{K}^H$ that corresponds to H under Theorem 9.38 has $[\mathbb{L} : \mathbb{R}] = N$ with N odd, and the first conclusion of Lemma 9.43 shows that $N = 1$. Thus $|\operatorname{Gal}(\mathbb{K}/\mathbb{R})| = 2^m$. Corollary 4.40 shows that $\operatorname{Gal}(\mathbb{K}/\mathbb{R})$ has nested subgroups of all orders 2^{m-k} with $0 \leq k \leq m$, and Theorem 9.38 says that the corresponding fixed fields are nested and have respective degrees 2^k with $0 \leq k \leq m$. The extension field of $\mathbb{R}$ for $k = 1$ is necessarily $\mathbb{C}$ by Lemma 9.43, and Lemma 9.43 shows that there

[8] To see that every member of $\mathbb{C}$ has a square root in $\mathbb{C}$, let $c + di$ be given with c and d real and with $d \neq 0$. Let a and b be real numbers with $a^2 = \frac{1}{2}(c + \sqrt{c^2 + d^2})$, $b^2 = \frac{1}{2}(-c + \sqrt{c^2 + d^2})$, and $\operatorname{sgn}(ab) = \operatorname{sgn} d$. Then $(a + bi)^2 = c + di$.

are no quadratic extensions of $\mathbb{C}$. Therefore $m = 0$ or $m = 1$, and the possible splitting fields for $F(X)$ are $\mathbb{R}$ and $\mathbb{C}$ in the two cases.

To complete the proof, suppose that $\mathbb{K}$ is a finite algebraic extension of $\mathbb{C}$ of degree n. Then $\mathbb{K}$ is a finite algebraic extension of $\mathbb{R}$ of degree $2n$. The Theorem of the Primitive Element allows us to write $\mathbb{K} = \mathbb{R}(x)$ for some $x \in \mathbb{K}$, and the minimal polynomial of x over $\mathbb{R}$ necessarily has degree $2n$. The previous paragraph shows that this polynomial splits in $\mathbb{C}$. Thus x is in $\mathbb{C}$, and $\mathbb{K} = \mathbb{C}$. This completes the proof. □

11. Application to Unsolvability of Polynomial Equations with Nonsolvable Galois Group

The quadratic formula for finding the roots of a quadratic polynomial has in principle been known since the time of the Babylonians about 400 B.C.[9] The corresponding problem of finding roots of cubics was unsolved until the sixteenth century, and **Cardan's formula** was discovered at that time. The original formula assumes real coefficients and was in two parts, a first case corresponding to what we now view as one real root and two complex roots, the second case corresponding to what we view as three real roots.[10] There is a similar formula, but more complicated, for solving quartics. Further centuries passed with no progress on finding a corresponding formula for the roots of a polynomial of degree 5 or higher. The introduction of Galois theory in the early nineteenth century made it possible to prove a surprising negative statement about all degrees beyond 4.

Suppose that we are given a polynomial equation with coefficients in the field $\mathbb{Q}$ or a more general field $\Bbbk$ of characteristic 0. In this section we use Galois theory to address the question whether the roots of the equation in a splitting field can be expressed in terms of $\Bbbk$ and the adjunction of finitely many n^{th} roots to the field, for various values of n. For the moment let us say in this case that the roots are "expressible in terms of the members of $\Bbbk$ and radicals." We shall make this notion more precise shortly.

Recall from Section IV.8 that with a finite group G, we can find a strictly decreasing sequence of subgroups starting with G and ending with $\{1\}$ such

[9] The Babylonians did not actually have equations but had an algorithmic method that amounted to completing the square.

[10] Cardan's name was Girolamo Cardano. The solution in the first case of the cubic seems to have been discovered by Scipione dal Ferro and later by Nicolo Tartaglia. Dal Ferro died in 1526 and passed the secret method to his student Antonio Fior. In 1535 Fior engaged in a public contest with Tartaglia at solving cubics, and he lost. Cardano wheedled the solution method in the first case from Tartaglia, published it in 1539, and discovered and published the solution in the second case. Cardano's student Lodovico Ferrari discovered how to solve quartics, and Cardano published that solution as well. See "St. Andrews" in the Selected References for more information.

that each subgroup is normal in the next larger one and each quotient group is simple. Such a series was defined to be a composition series for G. The Jordan–Hölder Theorem (Corollary 4.50) says that the respective consecutive quotients are isomorphic for any two composition series, apart from the order in which they appear. We define the finite group G to be **solvable** if each of the consecutive quotients is cyclic of prime order, rather than nonabelian. It is enough that the group have a normal series for which each of the consecutive quotients is abelian.

Examples of solvable and nonsolvable groups are obtainable from the calculations in Section IV.8: abelian groups and groups of prime-power order are always solvable, the symmetric group $\mathfrak{S}_4$ and each of its subgroups are solvable, and the symmetric group $\mathfrak{S}_5$ is not solvable since a composition series is $\mathfrak{S}_5 \supseteq \mathfrak{A}_5 \supseteq \{1\}$ and the group $\mathfrak{A}_5$ is simple (Theorem 4.47).

Modulo a precise definition for a field $\Bbbk$ of the words "expressible in terms of the members of $\Bbbk$ and radicals," the answer to our main question is as follows.

Theorem 9.44 (Abel, Galois).[11] Let $\Bbbk$ be a field of characteristic 0, let $F(X)$ be in $\Bbbk[X]$, and let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$. Then the roots of $F(X)$ are expressible in terms of the members of $\Bbbk$ and radicals if and only if the group $\operatorname{Gal}(\mathbb{K}/\Bbbk)$ is solvable.

EXAMPLE. With $\Bbbk = \mathbb{Q}$, let $F(X)$ be the polynomial $F(X) = X^5 - 5X + 1$ in $\mathbb{Q}[X]$. We shall show that

(i) $F(X)$ is irreducible over $\mathbb{Q}$,
(ii) $F(X)$ has three roots in $\mathbb{R}$ and one pair of conjugate complex roots in $\mathbb{C}$,
(iii) the splitting field $\mathbb{K}$ over $\mathbb{Q}$ of any polynomial of degree 5 for which (i) and (ii) hold has Galois group with $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathfrak{S}_5$.

We know that from Theorem 4.47 that $\mathfrak{S}_5$ is not solvable, and Theorem 9.44 therefore allows us to conclude that the roots of $X^5 - 5X + 1$ are not expressible in terms of the members of $\mathbb{Q}$ and radicals.

To prove (i), we apply Eisenstein's criterion (Corollary 8.22) to the polynomial $F(X-1) = X^5 - 5X^4 + 10X^3 - 10X^2 + 5$ and to the prime $p = 5$, and the irreducibility is immediate.

To prove (ii), we observe that $F(-2) < 0$, $F(0) > 0$, $F(1) < 0$, $F(2) > 0$. Applying the Intermediate Value Theorem (Section A3 of the appendix), we see that there are at least three roots in $\mathbb{R}$. Since $F'(X) = 5(X^4 - 1)$ has exactly the two roots ± 1 in $\mathbb{R}$, $F(X)$ has at most three roots in $\mathbb{R}$ by an application of the Mean Value Theorem.

To prove (iii), label the roots $1, 2, 3, 4, 5$ with 1 and 2 denoting the nonreal roots. Each member of the Galois group permutes the roots and is determined

[11] Abel proved that there is no general solution via radicals that gives the roots of polynomials of degree 5. Galois found the present theorem, which shows how to decide the question for each individual polynomial of degree 5.

by its effect on the roots. Thus $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ may be regarded as a subgroup of $\mathfrak{S}_5$. Since $F(X)$ is irreducible over $\mathbb{Q}$, 5 divides $[\mathbb{K}:\mathbb{Q}]$ and 5 divides $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})|$. By the Sylow Theorems, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains an element of order 5, hence a 5-cycle. Some power of this 5-cycle carries root 1 to root 2. So we may assume that the 5-cycle is $(1\ 2\ 3\ 4\ 5)$. Also, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains complex conjugation, which acts as $(1\ 2)$. Then $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains

$$\begin{aligned}(1\ 2\ 3\ 4\ 5)(1\ 2)(1\ 2\ 3\ 4\ 5)^{-1} &= (2\ 3),\\ (1\ 2\ 3\ 4\ 5)(2\ 3)(1\ 2\ 3\ 4\ 5)^{-1} &= (3\ 4),\\ (1\ 2\ 3\ 4\ 5)(3\ 4)(1\ 2\ 3\ 4\ 5)^{-1} &= (4\ 5).\end{aligned}$$

Since the set $\{(1\ 2),\ (2\ 3),\ (3\ 4),\ (4\ 5)\}$ of transpositions is easily shown from Corollary 1.22 to generate $\mathfrak{S}_5$, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \mathfrak{S}_5$.

Let $\mathbb{K}'$ be a finite extension of the given field $\Bbbk$. A **root tower** for $\mathbb{K}'$ over $\Bbbk$ is a finite sequence of extensions

$$\Bbbk = \mathbb{K}'_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_{l-1} \subseteq \mathbb{K}'_l = \mathbb{K}'$$

such that for each i with $0 \le i \le l-1$, there is a prime number $n_i > 1$ and there is an element r_i in $\mathbb{K}'_{i+1}$ with $a_i = r_i^{n_i}$ in $\mathbb{K}'_i$ and r_i not in $\mathbb{K}'_i$. Then it follows that r_i^k is not in $\mathbb{K}'_i$ for any k with $0 < k < n_i$.

(If we write $a_i = r_i^{n_i}$, then we might think of writing $\mathbb{K}'_{i+1} = \mathbb{K}'_i(\sqrt[n_i]{a_i}\,)$, but this formulation is less precise at the moment since it does not specify precisely which choice of $\sqrt[n_i]{a_i}$ is to be used.)

With "root tower" now well defined, we can make a precise definition and thereby complete the precise formulation of Theorem 9.44. Let $\Bbbk$ be the given field of characteristic 0, let $F(X)$ be in $\Bbbk[X]$, and let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$. We say that the roots of $F(X)$ are **expressible in terms of members of** $\Bbbk$ **and radicals** if there exists some finite extension $\mathbb{K}'$ of $\mathbb{K}$ having a root tower over $\Bbbk$.

The statement of Theorem 9.44 is now completely precise, and the remainder of the section will be devoted to the proof of one direction of the theorem: if the roots are expressible in terms of members of $\Bbbk$ and radicals, then the Galois group is solvable. The proof of the converse direction of the theorem is postponed to Section 13. We begin with a lemma.

Lemma 9.45. Let $\Bbbk$ be a field of any characteristic, and let p be a prime number. If a is a member of $\Bbbk$ such that $X^p - a$ has no root in $\Bbbk$, then $X^p - a$ is irreducible in $\Bbbk$.

PROOF. First suppose that p is different from the characteristic. Let $\mathbb{L}$ be a splitting field for $X^p - a$. The derivative of $X^p - a$, evaluated at any root of $X^p - a$ in $\mathbb{L}$, is nonzero, and Corollary 9.17 shows that $X^p - a$ splits as the product of p distinct linear factors in $\mathbb{L}$. The quotient of any two roots of $X^p - a$ is a p^{th} root of 1. Fixing one of these two roots of $X^p - a$ and letting the other vary, we obtain p distinct p^{th} roots of 1. Thus $\mathbb{L}$ contains all p of the p^{th} roots of 1. Proposition 4.26 shows that the group of p^{th} roots of 1 is cyclic. Let ζ be a generator. If $a^{1/p}$ denotes one of the roots of $X^p - a$ in $\mathbb{L}$, then the set of all the roots is given by $\{a^{1/p}\zeta^k \mid 0 \leq k \leq p-1\}$.

Now suppose that $X^p - a$ has a nontrivial factorization $X^p - a = F(X)G(X)$ in $\Bbbk[X]$. Possibly by adjusting the leading coefficients of $F(X)$ and $G(X)$, we may assume that $F(X)$ and $G(X)$ are both monic. Unique factorization in $\mathbb{L}[X]$ then implies that there is a nonempty subset S of $\{k \mid 0 \leq k \leq p-1\}$ with a nonempty complement S^c such that

$$F(X) = \prod_{k \in S} (X - \zeta^k a^{1/p}) \qquad \text{and} \qquad G(X) = \prod_{k \in S^c} (X - \zeta^k a^{1/p}).$$

If S has m elements, then the constant term of $F(X)$ is $(-a^{1/p})^m \omega$, where ω is some p^{th} root of 1. Thus $x = (a^{1/p})^m \omega$ is in $\Bbbk$. Since $\text{GCD}(m, p) = 1$, we can choose integers c and d with $cm + dp = 1$. Since x is in $\Bbbk$, so is $x^c a^d = (a^{1/p})^{mc+dp} \omega^c = a^{1/p}\omega^c$. But $a^{1/p}\omega^c$ is a root of $X^p - a$, in contradiction to the hypothesis that no root of $X^p - a$ lies in $\Bbbk$. Hence $X^p - a$ is irreducible.

If p equals the characteristic of $\Bbbk$, then Lemma 9.18 gives the factorization $X^p - a = (X - a^{1/p})^p$, where $a^{1/p}$ is one root of $X^p - a$ in $\mathbb{K}$. Then we can argue as above except that ζ and ω are to be replaced by 1 throughout. This completes the proof of the lemma. □

PROOF OF NECESSITY IN THEOREM 9.44 THAT $\text{Gal}(\mathbb{K}/\Bbbk)$ BE SOLVABLE. We are to prove that if some finite extension $\mathbb{K}'$ of $\mathbb{K}$ has a root tower over $\Bbbk$, then $\text{Gal}(\mathbb{K}/\Bbbk)$ is solvable.

Step 1. We enlarge each field in the given root tower to obtain a root tower

$$\Bbbk \subseteq \mathbb{K}''_0 \subseteq \mathbb{K}''_1 \subseteq \cdots \subseteq \mathbb{K}''_{l-1} \subseteq \mathbb{K}''_l = \mathbb{K}''$$

of a finite extension $\mathbb{K}''$ of $\mathbb{K}'$ in such a way that $\mathbb{K}''_0$ is the normal extension of $\Bbbk$ obtained by adjoining all n^{th} roots of 1 for a suitably large n and such that each $\mathbb{K}''_{i+1}$ is the normal extension of $\mathbb{K}''_i$ for $0 \leq i \leq l-1$ obtained by adjoining all n_i^{th} roots of the member a_i of $\mathbb{K}'_i$. Using Theorem 9.22, choose an algebraic closure $\overline{\mathbb{K}'}$ of $\mathbb{K}'$. Let n be the product of the integers $n_0, n_1, \ldots, n_{l-1}$. Let $\zeta_1, \ldots, \zeta_{n-1}$ be the n^{th} roots of 1 in $\overline{\mathbb{K}'}$ other than 1 itself, define subfields of $\overline{\mathbb{K}'}$ by

$$\mathbb{K}''_i = \mathbb{K}'_i(\zeta_1, \ldots, \zeta_{n-1}) \qquad \text{for } 0 \leq i \leq l,$$

and put $\mathbb{K}'' = \mathbb{K}'_l$. The field $\mathbb{K}''_0$ is a splitting field for $X^n - 1$ over $\Bbbk$ and is therefore a normal extension. The field $\mathbb{K}''_{i+1}$ is given by $\mathbb{K}''_{i+1} = \mathbb{K}''_i(r_i)$, where r_i is a root in $\mathbb{K}''_{i+1}$ of the polynomial $X^{n_i} - a_i$ in $\mathbb{K}''_i[X]$. Here n_i is prime. Lemma 9.45 shows that either r_i is in $\mathbb{K}''_i[X]$ or $X^{n_i} - a_i$ is irreducible in $\mathbb{K}''_i[X]$. In the first case, $\mathbb{K}''_{i+1} = \mathbb{K}''_i$, and we have a normal extension. In the second case, $\mathbb{K}''_{i+1}$ is a splitting field for $X^{n_i} - a_i$ over $\mathbb{K}''_i$ because it is generated by $\mathbb{K}''_i$ and one root of $X^{n_i} - a_i$ and because all n_i^{th} roots of 1 already lie in $\mathbb{K}''_0$; thus again we have a normal extension.

Step 2. The Galois group of $\mathbb{K}''_0$ over $\Bbbk$ is abelian. In fact, Proposition 4.26 shows that the group of n^{th} roots of 1 in $\mathbb{K}''_0$ is cyclic. Let ζ be a generator, and let $U = \{\zeta^k\}_{k=0}^{n-1}$. The map of $\mathrm{Gal}(\mathbb{K}''_0/\Bbbk)$ into $\mathrm{Aut}\,U$ given by $\varphi \mapsto \varphi\big|_U$ is a one-one homomorphism, and $\mathrm{Aut}\,U$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, it follows that $\mathrm{Gal}(\mathbb{K}''_0/\Bbbk)$ is abelian.

Step 3. The Galois group of $\mathbb{K}''_{i+1}$ over $\mathbb{K}''_i$ is trivial or is cyclic of order n_i. In fact, the Galois group is trivial if $\mathbb{K}''_{i+1} = \mathbb{K}''_i$. The contrary case is that $[\mathbb{K}''_{i+1} : \mathbb{K}''_i] = n_i$, and then $\mathrm{Gal}(\mathbb{K}''_{i+1}/\mathbb{K}''_i)$ has order n_i, which is prime. Every group of order n_i is cyclic, and hence $\mathrm{Gal}(\mathbb{K}''_{i+1}/\mathbb{K}''_i)$ is cyclic.

Step 4. We extend the root tower to a larger field $\mathbb{L} \supseteq \mathbb{K}''$ that is a normal extension of $\Bbbk$. The resulting root tower of $\mathbb{L}$ will be written as

$$\begin{aligned}\Bbbk \subseteq \mathbb{L}_0 = \mathbb{K}''_0 \subseteq \mathbb{L}_1 = \mathbb{K}''_1 \subseteq \cdots \\ \subseteq \mathbb{L}_{k-1} = \mathbb{K}''_{l-1} \subseteq \mathbb{L}_l = \mathbb{K}'' \subseteq \mathbb{L}_{l+1} \subseteq \cdots \subseteq \mathbb{L}_t = \mathbb{L}.\end{aligned}$$

As it is, we cannot say that $\mathbb{K}''$ is the splitting field over $\Bbbk$ for the product of the minimal polynomials used in Step 1, because the elements a_i are not assumed to lie in $\Bbbk$. To adjust the tower to correct this problem, write $\mathbb{K}''$ as

$$\mathbb{K}'' = \Bbbk(r_0, r_1, \ldots, r_{l-1}, \zeta) = \Bbbk(x_0, \ldots, x_l),$$

with ζ as in Step 2. Here $r_0, \ldots, r_{l-1}$ are the given elements that define the original root tower, and we define $x_l = \zeta$ and $x_j = r_j$ for $0 \le j < l$. Since $\mathbb{K}''$ is a finite extension of $\Bbbk$, each x_j has a minimal polynomial $G_j(X)$ over $\Bbbk$. Define $G(X) = \prod_{j=0}^{l} G_j(X)$, and let $\mathbb{L}$ be the splitting field of $G(X)$ in the algebraic closure $\overline{\mathbb{K}'}$. The field $\mathbb{L}$ is a normal extension of $\Bbbk$. The roots of $G(X)$ are the members of $\mathbb{L}$ that are roots of some $G_j(X)$. Each x_j is a root of its own $G_j(X)$. If x'_j is another root of $G_j(X)$, then there is a $\Bbbk$ isomorphism of $\Bbbk(x_j)$ onto $\Bbbk(x'_j)$, and we know by the uniqueness of splitting fields (Theorem 9.13$'$)[12] that this

[12] The theorem is to be applied to $\sigma : \Bbbk(x_j) \to \Bbbk(x'_j)$ with $F(X) = F^\sigma(X) = G(X)$ and with $\mathbb{L}' = \mathbb{L}$.

extends to a $\Bbbk$ isomorphism of $\mathbb{L}$ onto $\mathbb{L}$. Hence to each root θ of $G(X)$ in $\mathbb{L}$ corresponds some x_j and some $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$ with $\varphi(x_j) = \theta$. Thus

$$\mathbb{L} = \Bbbk\big(\{\varphi(x_j) \mid 0 \le j \le l \text{ and } \varphi \in \mathrm{Gal}(\mathbb{L}/\Bbbk\}\big).$$

For any φ in $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ and any $j \le l-1$, the element $\varphi(x_j)$ of $\mathbb{L}$ satisfies

$$(\varphi(x_j))^{n_j} = \varphi(x_j^{n_j}) = \varphi(a_j),$$

and the element on the right is in $\varphi(K_j'')$. Any element $\varphi(\zeta)$ is an n^{th} root of 1 and hence is already in $\mathbb{K}_0''$; such elements are redundant for $\varphi \ne 1$. Enumerate $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ as $\varphi_1, \dots, \varphi_s$ with $\varphi_1 = 1$. The tower for $\mathbb{K}''$ is to be continued with the fields obtained by adjoining one at a time the elements

$$\varphi_2(r_0), \dots, \varphi_2(r_{l-1}), \varphi_3(r_0), \dots, \varphi_3(r_{l-1}), \quad \dots, \quad \varphi_s(r_0), \dots, \varphi_s(r_{l-1}).$$

The final field is $\mathbb{L}$, and then we have an enlarged tower as asserted.

Step 5. $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ is a solvable group. In fact, first we prove by induction downward on i that $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$ is solvable, the case $i = t$ being the case of the trivial group. Let $i < t$ be given. We have arranged that $\mathbb{L}_{i+1}$ is a normal extension of $\mathbb{L}_i$. Since $\mathbb{L}$ is normal over all the smaller fields by Step 4, Corollary 9.39 therefore gives $\mathrm{Gal}(\mathbb{L}_{i+1}/\mathbb{L}_i) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)\big/\mathrm{Gal}(\mathbb{L}/\mathbb{L}_{i+1})$. The group on the left side is cyclic by Step 3 or the analogous proof with some r_j replaced by a suitable $\varphi(r_j)$, and thus a normal series with abelian quotients for $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_{i+1})$ may be extended by including the term $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$, and the result is still a normal series with abelian quotients. Thus $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$ is solvable. This completes the induction and shows that $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ is solvable. To complete the proof we use the isomorphism $\mathrm{Gal}(\mathbb{L}_0/\Bbbk) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk)\big/\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ given by Corollary 9.39. The group on the left side is abelian by Step 2, and thus a normal series with abelian quotients for $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ may be extended by including the term $\mathrm{Gal}(\mathbb{L}/\Bbbk)$, and the result is still a normal series with abelian quotients. Thus $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ is solvable.

Step 6. $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is a solvable group. We have $\mathbb{L} \supseteq \mathbb{K} \supseteq \Bbbk$ with $\mathbb{L}/\Bbbk$ normal by Step 4 and with $\mathbb{K}/\Bbbk$ normal since $\mathbb{K}$ is a splitting field of $F(X)$ over $\Bbbk$. Applying Corollary 9.39, we obtain an isomorphism $\mathrm{Gal}(\mathbb{K}/\Bbbk) \cong \mathrm{Gal}(\mathbb{L}/\Bbbk)\big/\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Then Step 6 will follow from Step 5 if it is shown that any homomorphic image of a solvable group is solvable. Thus let G be a solvable group, and let $\varphi : G \to H$ be an onto homomorphism. Write $G = G_1 \supseteq \cdots \supseteq G_m = \{1\}$ with abelian quotients, and define $H_i = \varphi(G_i)$. Passage to the quotient gives us a homomorphism φ_i carrying G_i onto H_i/H_{i+1}. Since $\varphi(G_{i+1}) \subseteq H_{i+1}$, φ induces a homomorphism $\overline{\varphi}_i$ of G_i/G_{i+1} onto H_i/H_{i+1}. As the image of an abelian group under a homomorphism, H_i/H_{i+1} is abelian. Therefore H is solvable. This completes the proof. □

12. Construction of Regular Polygons

Theorem 9.25 proved the constructibility of regular n-gons when n is the product of a power of 2 and distinct Fermat primes, but it gave little clue how to carry out the construction. In this section we supply enough further detail so that one can actually carry out the construction. It is enough to handle the case that n is a Fermat prime, $n = 2^{2^N} + 1$, and we shall suppose that n is a prime of this form.

Let $\zeta = e^{2\pi i/n}$. The field of interest is $\mathbb{Q}(\zeta)$, with $[\mathbb{Q}(\zeta) : \mathbb{Q}] = n - 1$. The usual basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is $\{1, \zeta, \zeta^2, \dots, \zeta^{n-2}\}$, but we shall use the basis

$$\{\zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}\}$$

instead, in order to identify the Galois group $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ more readily with $\mathbb{F}_n^\times$, where $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ is the field of n elements. In more detail we associate the additive group of $\mathbb{F}_n$ with the additive group of exponents of the members of the cyclic group $\{1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}\}$, and members of the Galois group correspond to the various multiplications of these exponents by $\mathbb{F}_n^\times = \{1, 2, \dots, n-1\}$. The group $\mathbb{F}_n^\times$ is known to be cyclic of order $n - 1$, and thus the isomorphic Galois group is cyclic. If a generator σ of the Galois group is to correspond to multiplication by a generator g of $\mathbb{F}_n^\times$, then $\sigma(\zeta^s) = \zeta^{gs}$ for all s. With the prime n of the form $2^{2^N} + 1$, let us note for the sake of completeness why we can always take $g = 3$.

Lemma 9.46. The number 3 is a generator of $\mathbb{F}_n^\times$ when n is prime of the form $2^{2^N} + 1$ with $N > 0$.

REMARKS. We verified this assertion for $n = 17$ in Section 6, and in principle one could verify the lemma in any particular case in the same way. Here is a general argument using the law of quadratic reciprocity, whose full statement and proof will be given in Chapter I of *Advanced Algebra*. For a prime number n that is congruent to 1 modulo 4, quadratic reciprocity implies that 3 is a square modulo n if and only if n is a square modulo 3. Since

$$2^{2^N} - 1 = (2^{2^{N-1}} + 1)(2^{2^{N-2}} + 1) \cdots (2^{2^1} + 1)(2^{2^1} - 1)$$

and $2^{2^1} - 1 = 3$, 3 divides $2^{2^N} - 1$. Thus n is congruent to 2 modulo 3, n is not a square modulo 3, and 3 is not a square modulo n. The nonsquares modulo $n = 2^{2^N} + 1$ are exactly the generators of $\mathbb{F}_n^\times$, and therefore 3 is a generator.

Taking Lemma 9.46 into account, we suppose for the remainder of this section that the generator σ of the Galois group corresponds to multiplication of exponents of ζ by 3. Then $\sigma(\zeta) = \zeta^3$ and $\sigma(\zeta^s) = \zeta^{3s}$. These formulas and $\mathbb{Q}$ linearity tell us explicitly how σ operates on all of $\mathbb{Q}(\zeta)$.

The fixed fields that arise within $\mathbb{Q}(\zeta)$ correspond to subgroups of the group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \{\sigma^j \mid 0 \leq j < 2^{2^N}\}$, and there is one for each power of 2 from 2^0 to 2^{2^N}. Fix attention on the subgroup H_l of order l, and write $2^{2^N} = kl$, with k and l being powers of 2. A generator of this subgroup is σ^k, and the subgroup is $H_l = \{1, \sigma^k, \sigma^{2k}, \dots, \sigma^{(l-1)k}\}$. Let $\mathbb{K}_l$ be the fixed field of this subgroup, or equivalently of its generator σ^k; this has dimension k over $\mathbb{Q}$.

We shall determine a basis of $\mathbb{K}_l$ over $\mathbb{Q}$. Since $\sigma(\zeta^s) = \zeta^{3s}$, we have $\sigma^k(\zeta^s) = \zeta^{3^k s}$. For $0 \leq r \leq k-1$, the k elements

$$\eta_r = \zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}}$$

are linearly independent over $\mathbb{Q}$ because they involve disjoint sets of basis vectors of $\mathbb{Q}(\zeta)$ as r varies. The computation

$$\begin{aligned}\sigma^k(\eta_r) &= \sigma^k\big(\zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}}\big)\\ &= \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \zeta^{3^{r+3k}} + \cdots + \zeta^{3^{r+kl}}\\ &= \zeta^{3^r} + \zeta^{3^{r+k}} + \zeta^{3^{r+2k}} + \cdots + \zeta^{3^{r+k(l-1)}}\\ &= \eta_r\end{aligned}$$

shows that each of these vectors is in $\mathbb{K}_l$. Hence $\{\eta_0, \dots, \eta_{k-1}\}$ is a basis of $\mathbb{K}_l$ over $\mathbb{Q}$. The elements of this basis are called the **periods** of l terms of the cyclotomic field.

The extreme cases for the periods are $(k, l) = (2^{2^N}, 1)$, for which $0 \leq r \leq 2^{2^N} - 1$ with $\eta_r = \zeta^{3^r}$, and $(k, l) = (1, 2^{2^N})$, for which $r = 0$ with

$$\eta_0 = \zeta^{3^0} + \zeta^{3^1} + \zeta^{3^2} + \cdots + \zeta^{3^{2^{2^N}-1}} = \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{n-1} = -1.$$

Two facts enter into determining how to write ζ in terms of rationals and square roots. The first is that at stage k for $k \geq 2$, the sum of certain pairs of η_r's is an η for stage $k-1$. The second is that the product of two η_r's at stage k is an integer combination of η's from the same stage and that the sum formulas express this combination in terms of η's from earlier stages. The result is that at the k^{th} stage we obtain expressions for the sum and product of two η_r's in terms of η's from earlier stages. Therefore the two η_r's at stage k are the roots of a quadratic equation whose coefficients involve η's from earlier stages. Consequently we can compute the η_r's explicitly by induction on k. To proceed further, we need to know the formula for the product of two η_r's, which is due to Gauss.

To multiply two η_r's, we need to multiply various powers of ζ, and the exponents get added in the process. This addition is not readily compatible with terms like ζ^{3^r} and ζ^{3^s}, and for that reason Gauss introduced new notation. Define

$$\eta^{(t)} = \zeta^t + \zeta^{t3^k} + \zeta^{t3^{2k}} + \cdots + \zeta^{t3^{k(l-1)}} = \sum_{v \bmod l} \zeta^{t3^{kv}}$$

for $0 \le t \le n-1$. Then $\eta^{(0)} = l$, and for $0 < t \le n-1$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Gauss's product formula is given by

$$\begin{aligned}
\eta^{(s)}\eta^{(t)} &= \sum_{u \bmod l} \Big(\sum_{v \bmod l} \zeta^{s3^{ku}+t3^{kv}} \Big) \\
&= \sum_{u \bmod l} \Big(\sum_{w \bmod l} \zeta^{s3^{ku}+t3^{k(u+w)}} \Big) \qquad \text{with } v \mapsto u+w \\
&= \sum_{w \bmod l} \Big(\sum_{u \bmod l} \zeta^{(s+t3^{kw})3^{ku}} \Big) \\
&= \sum_{w \bmod l} \eta^{(s+t3^{kw})}.
\end{aligned}$$

In words, this says that to multiply two η's, we add the η's for the exponents obtained by multiplying the first term of $\eta^{(s)}$ by all the terms of $\eta^{(t)}$.

At this point it is more illuminating to work some examples than to try for a general result.

EXAMPLE 1. $n = 5$, $N = 1$, $2^{2^N} = 4$. The relevant pairs (k, l) to study in sequence are $(k, l) = (1, 4), (2, 2), (4, 1)$, and the case $(k, l) = (1, 4)$ is trivial since the only subscripted η is $\sum_{s=0}^{3} \zeta^{3^s} = -1$.

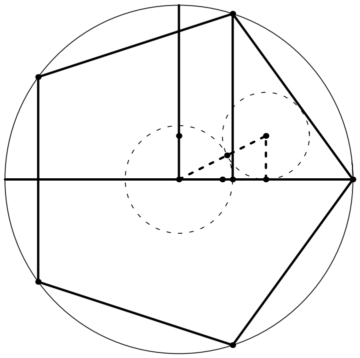

FIGURE 9.3. Construction of a regular pentagon. The circle with center $\left(\frac{1}{2}, \frac{1}{4}\right)$ and radius $\frac{1}{4}$ meets the line from $\left(\frac{1}{2}, \frac{1}{4}\right)$ to the origin at a point at distance $\cos(2\pi/5)$ from the origin.

For $k = 2$, i.e., for the case that there are 2 periods of 2 terms each, we go back to the definition of the η's and find that

$$\begin{aligned}
\eta_0 &= \zeta^{3^{0+2\cdot 0}} + \zeta^{3^{0+2\cdot 1}} = \zeta^1 + \zeta^4, \\
\eta_1 &= \zeta^{3^{1+2\cdot 0}} + \zeta^{3^{1+2\cdot 1}} = \zeta^3 + \zeta^2.
\end{aligned}$$

We form those sums of pairs of η's that yield an η from the previous step. Here there is only one pair, and the sum is given by

$$\eta_0 + \eta_1 = -1.$$

Next we form the elements $\eta^{(t)}$, remembering that for $t > 0$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Then

$$\eta^{(0)} = 2, \quad \eta^{(1)} = \eta_0, \quad \eta^{(2)} = \eta_1, \quad \eta^{(3)} = \eta_1, \quad \eta^{(4)} = \eta_0.$$

We apply Gauss's product formula to compute the product of the two η's whose sum we have identified. The formula gives

$$\eta_0\eta_1 = \eta^{(1)}\eta^{(2)} = \eta^{(4)} + \eta^{(3)} = \eta_0 + \eta_1 = -1,$$

the second equality following since the rule for the indices is to extract a power of ζ appearing in $\eta^{(1)}$ and add that index to all the powers of ζ appearing in $\eta^{(2)}$. Since η_0 and η_1 have sum -1 and product -1, they are the roots of the quadratic equation

$$x^2 + x - 1 = 0, \qquad \text{namely } \tfrac{1}{2}(-1 \pm \sqrt{5}\,).$$

Deciding which root is η_0 and which is η_1 involves looking at signs. The two roots of the quadratic equation are of opposite sign because the constant term of the quadratic equation is negative. Since $\eta_0 = \zeta + \zeta^{-1} = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos(2\pi/5)$ is positive, we obtain

$$\eta_0 = \tfrac{1}{2}(-1 + \sqrt{5}\,) \qquad \text{and} \qquad \eta_1 = \tfrac{1}{2}(-1 - \sqrt{5}\,).$$

The computation can in principle stop here, since knowing $\cos(2\pi/5)$ gives us $\sin(2\pi/5)$ and therefore $e^{2\pi i/5}$. See Figure 9.3. But it is instructive to carry out the algorithm anyway. We are thus to treat $k = 4$. The periods of 1 term are

$$\xi_0 = \zeta, \quad \xi_1 = \zeta^3, \quad \xi_2 = \zeta^4, \quad \xi_3 = \zeta^2.$$

The corresponding objects with superscripts are

$$\xi^{(0)} = 1, \quad \xi^{(1)} = \xi_0, \quad \xi^{(2)} = \xi_3, \quad \xi^{(3)} = \xi_1, \quad \xi^{(4)} = \xi_2.$$

The relevant sums of pairs are

$$\begin{aligned} \xi_0 + \xi_2 &= \eta_0, \\ \xi_1 + \xi_3 &= \xi_1. \end{aligned}$$

We again use Gauss's product formula, and this time we obtain

$$\xi_0\xi_2 = \xi^{(1)}\xi^{(4)} = \xi^{(5)} = \xi^{(0)} = 1.$$

Hence ξ_0 and ξ_2 are the roots of the quadratic equation

$$y^2 - \eta_0 y + 1 = 0, \qquad \text{namely } \frac{\frac{-1+\sqrt{5}}{2} \pm i\sqrt{4 - \big(\frac{-1+\sqrt{5}}{2}\big)^2}}{2}.$$

The root y involving the plus sign is $e^{2\pi i/5}$.

EXAMPLE 2.[13] $n = 17$, $N = 2$, $2^{2^N} = 16$. The relevant pairs (k, l) have $kl = 16$, and the case $(k, l) = (1, 16)$ is trivial since the only subscripted η is $\sum_{s=0}^{15} \zeta^{3^s} = -1$.

For $k = 2$, the 2 periods have 8 terms each, and

$$\begin{aligned}\eta_0 &= \zeta^{3^{0+2\cdot 0}} + \zeta^{3^{0+2\cdot 1}} + \zeta^{3^{0+2\cdot 2}} + \zeta^{3^{0+2\cdot 3}} + \zeta^{3^{0+2\cdot 4}} + \zeta^{3^{0+2\cdot 5}} + \zeta^{3^{0+2\cdot 6}} + \zeta^{3^{0+2\cdot 7}}\\ &= \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,\\ \eta_1 &= \zeta^{3^{1+2\cdot 0}} + \zeta^{3^{1+2\cdot 1}} + \zeta^{3^{1+2\cdot 2}} + \zeta^{3^{1+2\cdot 3}} + \zeta^{3^{1+2\cdot 4}} + \zeta^{3^{1+2\cdot 5}} + \zeta^{3^{1+2\cdot 6}} + \zeta^{3^{1+2\cdot 7}}\\ &= \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.\end{aligned}$$

We form those sums of pairs of η's that yield an η from the previous step. Here there is only one pair, and the sum is given by

$$\eta_0 + \eta_1 = -1.$$

Next we form the elements $\eta^{(t)}$, remembering that for $t > 0$, $\eta^{(t)}$ is the η_r in which ζ^t occurs. Then $\eta^{(0)} = 2$,

$$\begin{aligned}\eta^{(1)} &= \eta^{(9)} = \eta^{(13)} = \eta^{(15)} = \eta^{(16)} = \eta^{(8)} = \eta^{(4)} = \eta^{(2)} = \eta_0,\\ \eta^{(3)} &= \eta^{(10)} = \eta^{(5)} = \eta^{(11)} = \eta^{(14)} = \eta^{(7)} = \eta^{(12)} = \eta^{(6)} = \eta_1.\end{aligned}$$

To compute $\eta_0\eta_1$ by means of Gauss's product formula, we use $\eta_0 = \eta^{(1)}$ and $\eta_1 = \eta^{(3)}$. Then

$$\eta_0\eta_1 = \eta^{(1)}\eta^{(3)} = \eta^{(4)} + \eta^{(11)} + \eta^{(6)} + \eta^{(12)} + \eta^{(15)} + \eta^{(8)} + \eta^{(13)} + \eta^{(7)},$$

the indices on the right side being the indices for η_1 plus one. Resubstituting in terms of η_0 and η_1, we obtain

$$\eta_0\eta_1 = 4\eta_0 + 4\eta_1 = -4.$$

Therefore η_0 and η_1 are the roots of the quadratic equation

$$x^2 + x - 4 = 0, \qquad \text{namely } \tfrac{1}{2}(-1 \pm \sqrt{17}\,).$$

Deciding which root is η_0 and which is η_1 involves looking at signs. The two roots of the quadratic equation are of opposite sign. Since

$$\begin{aligned}\eta_0 &= (\zeta^1 + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8})\\ &= 2\big(\cos(2\pi/17) + \cos(4\pi/17) + \cos(8\pi/17) + \cos(16\pi/17)\big)\\ &> 2\big(\tfrac{1}{2} + \tfrac{1}{2} + 0 + (-1)\big) = 0,\end{aligned}$$

[13] The discussion of this example closely follows that in Van der Waerden, Vol. I, Section 54.

η_0 is the positive root, and we have

$$\eta_0 = \tfrac{1}{2}(-1+\sqrt{17}) \qquad \text{and} \qquad \eta_1 = \tfrac{1}{2}(-1-\sqrt{17}).$$

For $k = 4$, the 4 periods have 4 terms each, and

$$\begin{aligned}
\xi_0 &= \zeta^{3^{0+4\cdot0}} + \zeta^{3^{0+4\cdot1}} + \zeta^{3^{0+4\cdot2}} + \zeta^{3^{0+4\cdot3}} = \zeta^1 + \zeta^{13} + \zeta^{16} + \zeta^4,\\
\xi_1 &= \zeta^{3^{1+4\cdot0}} + \zeta^{3^{1+4\cdot1}} + \zeta^{3^{1+4\cdot2}} + \zeta^{3^{1+4\cdot3}} = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12},\\
\xi_2 &= \zeta^{3^{2+4\cdot0}} + \zeta^{3^{2+4\cdot1}} + \zeta^{3^{2+4\cdot2}} + \zeta^{3^{2+4\cdot3}} = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2,\\
\xi_3 &= \zeta^{3^{3+4\cdot0}} + \zeta^{3^{3+4\cdot1}} + \zeta^{3^{3+4\cdot2}} + \zeta^{3^{3+4\cdot3}} = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6.
\end{aligned}$$

The sums of pairs of these that yield η's are

$$\begin{aligned}
\xi_0 + \xi_2 &= \eta_0\\
\xi_1 + \xi_3 &= \eta_1.
\end{aligned}$$

We can read off superscripted ξ's from the exponents on the right sides of the formulas for $\xi_0, \dots, \xi_3$, and the results are

$$\begin{aligned}
\xi^{(1)} &= \xi^{(13)} = \xi^{(16)} = \xi^{(4)} = \xi_0,\\
\xi^{(3)} &= \xi^{(5)} = \xi^{(14)} = \xi^{(12)} = \xi_1,\\
\xi^{(9)} &= \xi^{(15)} = \xi^{(8)} = \xi^{(2)} = \xi_2,\\
\xi^{(10)} &= \xi^{(11)} = \xi^{(7)} = \xi^{(6)} = \xi_3.
\end{aligned}$$

Then the relevant products are

$$\begin{aligned}
\xi_0\xi_2 &= \xi^{(1)}\xi^{(9)} = \xi^{(10)} + \xi^{(16)} + \xi^{(9)} + \xi^{(3)} = \xi_3 + \xi_0 + \xi_2 + \xi_1 = -1,\\
\xi_1\xi_3 &= \xi^{(3)}\xi^{(6)} = \xi^{(13)} + \xi^{(14)} + \xi^{(10)} + \xi^{(9)} = \xi_0 + \xi_1 + \xi_3 + \xi_2 = -1.
\end{aligned}$$

Thus ξ_0 and ξ_2 are the roots of the quadratic equation

$$y^2 - \eta_0 y - 1 = 0,$$

while ξ_1 and ξ_3 are the roots of the quadratic equation

$$y^2 - \eta_1 y - 1 = 0.$$

Since $\xi_0\xi_2$ and $\xi_1\xi_3$ are negative, these equations each have roots of opposite sign. We observe that $\xi_0 = 2\big(\cos(2\pi/17) + \cos(8\pi/17)\big) > 0$ and that $\xi_3 = 2\big(\cos(14\pi/17) + \cos(12\pi/17)\big) < 0$, and we conclude that the signs are

$$\begin{aligned}
\xi_0 > 0 \quad &\text{and} \quad \xi_2 < 0,\\
\xi_1 > 0 \quad &\text{and} \quad \xi_3 < 0.
\end{aligned}$$

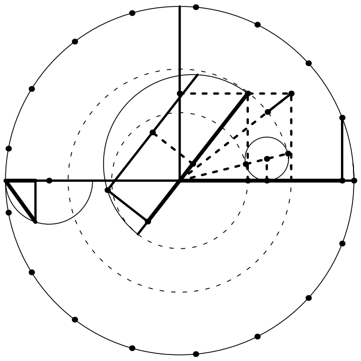

FIGURE 9.4. Construction of a regular 17-gon. The small circle has center $\left(\frac{1}{2}, \frac{1}{8}\right)$ and radius $\frac{1}{8}$. Two circles are drawn tangent to it with center $(0, 0)$; their radii are $\eta_0/4$ and $|\eta_1|/4$. Their x intercepts and height $\frac{1}{2}$ determine the dashed box. The diameter of the large solid semicircle is $\xi_0/2$, and its heavy part is $\lambda_0/2$. The separate semicircle at the left constructs $\sqrt{\xi_1/4}$ from $\xi_1/2$, and the chord in the large semicircle is at distance $\sqrt{\xi_1/4}$ from the diameter.

For $k = 8$, the 8 periods have 2 terms each, and the two with sum ξ_0 are

$$\lambda_0 = \zeta^{3^{0+8\cdot 0}} + \zeta^{3^{0+8\cdot 1}} = \zeta^1 + \zeta^{16},$$
$$\lambda_4 = \zeta^{3^{4+8\cdot 0}} + \zeta^{3^{4+8\cdot 1}} = \zeta^{13} + \zeta^4.$$

Their sum and their product are given by

$$\lambda_0 + \lambda_4 = \xi_0,$$
$$\lambda_0\lambda_4 = \zeta^{14} + \zeta^5 + \zeta^{12} + \zeta^3 = \xi_1.$$

Thus λ_0 and λ_4 are the roots of the quadratic equation

$$z^2 - \xi_0 z + \xi_1 = 0.$$

Since $\lambda_0 = 2\cos(2\pi/17) > 2\cos(8\pi/17) = \lambda_4$, λ_0 is the larger of the two roots of the equation.

In summary, we have successively defined

$$\eta_0 = \tfrac{1}{2}\big(-1 + \sqrt{17}\big) \quad \text{and} \quad \eta_1 = \tfrac{1}{2}\big(-1 - \sqrt{17}\big),$$
$$\xi_0 = \tfrac{1}{2}\big(\eta_0 + \sqrt{\eta_0^2 + 4}\big) \quad \text{and} \quad \xi_2 = \tfrac{1}{2}\big(\eta_0 - \sqrt{\eta_0^2 + 4}\big),$$
$$\xi_1 = \tfrac{1}{2}\big(\eta_1 + \sqrt{\eta_1^2 + 4}\big) \quad \text{and} \quad \xi_3 = \tfrac{1}{2}\big(\eta_1 - \sqrt{\eta_1^2 + 4}\big),$$
$$\lambda_0 = \tfrac{1}{2}\big(\xi_0 + \sqrt{\xi_0^2 - 4\xi_1}\big).$$

Since $\lambda_0 = 2\cos(2\pi/17)$, these formulas explicitly point to how to construct a regular 17-gon. See Figure 9.4.

13. Solution of Certain Polynomial Equations with Solvable Galois Group

In this section we investigate what specific information can be deduced about a finite Galois extension in characteristic 0 when the Galois group is solvable. The tool is a precursor of modern harmonic analysis[14] known as "Lagrange resolvents." The argument of the previous section could be regarded as an instance of applying the theory of Lagrange resolvents, but Lagrange resolvents give only the simpler formulas of the previous section, not the Gauss product formula.

Proposition 9.47. Let $\mathbb{K}$ be a finite normal extension of a field $\Bbbk$ of characteristic 0, suppose that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is cyclic of order n with σ as a generator, and suppose that $X^n - 1$ splits in $\Bbbk$. Fix a generator σ of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ and a primitive n^{th} root ω of 1 in $\Bbbk$. For $0 \le r < n$, define $\Bbbk$ linear maps $E_r : \mathbb{K} \to \mathbb{K}$ by

$$E_r x = n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^k x \qquad \text{for } x \in \mathbb{K}.$$

Then

(a) $E_r E_s$ equals E_s if $r = s$ and equals 0 if $r \not\equiv s \bmod n$, so that the E_r's are commuting projection operators whose images are linearly independent,

(b) $\sum_{r \bmod n} E_r = I$, so that the direct sum of the images of the E_r's is all of $\mathbb{K}$,

(c) $\sigma(x) = \omega^r x$ for all r and for all x in image E_r,

(d) image $E_0 = \Bbbk$.

REMARKS. The integers k and r depend only on their values modulo n, and the summation indices "k mod n" and "r mod n" are to be interpreted accordingly. The operators E_r are known classically as **Lagrange resolvents**, apart from the constant n^{-1}. The proposition says that the $\Bbbk$ linear map σ has a basis of eigenvectors, that the eigenvalues are a subset of the powers ω^r, and that each E_r is the projection operator on the eigenspace for the eigenvalue ω^r along the sum of the remaining eigenspaces.

[14] Lagrange resolvents give a certain specific Fourier decomposition relative to a cyclic group. Similar formulas apply whenever a cyclic group acts linearly on a vector space over $\Bbbk$ and the relevant roots of 1 lie in $\Bbbk$. For the corresponding decomposition of a vector space over $\mathbb{C}$ when a finite group G acts linearly, see Problems 47–52 at the end of Chapter VII. The decomposition in those problems can be seen to work for any field $\Bbbk$ of characteristic 0 for which the values of all irreducible characters of G lie in $\Bbbk$. The values of the characters are sums of certain roots of 1, and thus it is enough that $\Bbbk$ contain a certain finite set of roots of 1.

PROOF. For x in $\mathbb{K}$, we compute

$$\begin{aligned} E_r E_s x &= n^{-2} \sum_{k \bmod n} \omega^{-kr} \sigma^k \Big(\sum_{l \bmod n} \omega^{-ls} \sigma^l x \Big) \\ &= n^{-2} \sum_{k \bmod n} \sum_{m \bmod n} \omega^{-kr} \sigma^k \omega^{-ms+ks} \sigma^{m-k} x \\ &= n^{-2} \sum_{m \bmod n} \Big(\sum_{k \bmod n} \omega^{k(s-r)} \Big) \omega^{-ms} \sigma^m x. \end{aligned}$$

The expression in parentheses on the right side is the sum of a finite geometric series. If $s \equiv r \bmod n$, then every term in the sum is 1, and the sum is n. If $s \not\equiv r \bmod n$, then the sum is $\frac{1-\omega^{n(s-r)}}{1-\omega^{s-r}} = 0$. Thus (a) follows.

Next we calculate

$$\sum_{r \bmod n} E_r x = \sum_{r \bmod n} n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^k x = \sum_{k \bmod n} n^{-1} \Big(\sum_{r \bmod n} \omega^{-kr} \Big) \sigma^k x.$$

As in the previous paragraph, the sum in parentheses is n if $k = 0$ and it is 0 if $k \not\equiv 0 \bmod n$. Therefore only the $k = 0$ term on the right side contributes, and the right side simplifies to x. This proves (b).

The computation

$$\begin{aligned} \sigma(E_r x) &= n^{-1} \sum_{k \bmod n} \omega^{-kr} \sigma^{k+1} x \\ &= n^{-1} \sum_{l \bmod n} \omega^{(-l+1)r} \sigma^l x \\ &= \omega^r n^{-1} \sum_{l \bmod n} \omega^{-lr} \sigma^l x = \omega^r E_r x \end{aligned}$$

shows that $\sigma(y) = \omega^r y$ for every y of the form $E_r x$, and these y's are the members of the image of E_r. This proves (c).

Combining (b) and (c), we see that $\sigma(x) = x$ if and only if x is in image E_0. Since Gal($\mathbb{K}/\mathbb{k}$) is cyclic, the members of $\mathbb{K}$ fixed by σ are the members fixed by the Galois group, and these are the members of $\mathbb{k}$ by Proposition 9.35d. This proves (d). □

Corollary 9.48. Let $\mathbb{K}$ be a finite normal extension of a field $\mathbb{k}$ of characteristic 0, suppose that Gal($\mathbb{K}/\mathbb{k}$) is cyclic of prime order p, and suppose that $X^p - 1$ splits in $\mathbb{k}$. Then there exist a in $\mathbb{k}$ and x in $\mathbb{K}$ such that $x^p = a$ and $\mathbb{K} = \mathbb{k}(x)$.

REMARKS. In other words, a finite normal extension field in characteristic 0 with Galois group cyclic of prime order p is necessarily obtained by adjoining a p^{th} root of some element of the base field, provided that the base field contains all the p^{th} roots of 1. Once the extension field contains one p^{th} root of an element of the base field, it has to contain all p^{th} roots, since the base field by assumption contains a full complement of p^{th} roots of 1.

PROOF. We apply Proposition 9.47 with $n = p$. Since $[\mathbb{K} : \Bbbk] = p > 1$, (d) shows that E_0 is not the identity. By (b), some E_r with $r \neq 0$ is not the 0 operator. Let x be a nonzero element in image E_r. Since the generator σ of the Galois group is a field automorphism, $\sigma(x^p) = \sigma(x)^p = (\omega^r x)^p = \omega^{rp} x^p = x^p$. Since x^p is fixed by the Galois group, x^p lies in $\Bbbk$. Then the element $a = x^p$ has the property that $x^p = a$ and $\mathbb{K} \supseteq \Bbbk(x) \supsetneqq \Bbbk$. Since $[\mathbb{K} : \Bbbk]$ is prime, Corollary 9.7 shows that there are no intermediate fields between $\mathbb{K}$ and $\mathbb{K}$. Therefore $\mathbb{K} = \Bbbk(x)$. □

We shall apply Corollary 9.48 to prove the converse statement in Theorem 9.44—that solvability of the Galois group for a polynomial equation in characteristic 0 implies that the solutions of the equation are expressible in terms of radicals and the base field. We begin with a lemma that handles a special case.

Lemma 9.49. Let $\Bbbk$ be a field of characteristic 0, let $n > 0$ be an integer, and let $\mathbb{K}$ be a splitting field for $\prod_{r=1}^{n} (X^r - 1)$ over $\Bbbk$. Then $\mathbb{K}/\Bbbk$ is a Galois extension, the Galois group of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is abelian, and $\mathbb{K}$ has a root tower over $\Bbbk$.

PROOF. Being a splitting field in characteristic 0, $\mathbb{K}$ is a finite Galois extension of $\Bbbk$. For $1 \leq r \leq n$, let ω_r be a primitive r^{th} root of 1 in $\mathbb{K}$. The primitive r^{th} roots of 1 are parametrized by the group $(\mathbb{Z}/r\mathbb{Z})^\times$ once some ω_r is specified, the parametrization being $k \mapsto \omega_r^k$. If σ is in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, then $\sigma(\omega_r) = \omega_r^k$ for some such k. This correspondence respects multiplication in $(\mathbb{Z}/r\mathbb{Z})^\times$ since if $\sigma(\omega_r) = \omega_r^k$ and $\sigma'(\omega_r) = \omega_r^l$, then $\sigma'(\sigma(\omega_r)) = \sigma'(\omega_r^k) = \sigma'(\omega_r)^k = \omega_r^{kl}$. Thus for each r, we have a homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ into the abelian group $(\mathbb{Z}/r\mathbb{Z})^\times$. Putting these homomorphisms together as r varies and using the fact that the ω_r's generate $\mathbb{K}$ over $\Bbbk$, we obtain a one-one homomorphism of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ into the abelian group $\prod_{r=1}^{n} (\mathbb{Z}/r\mathbb{Z})^\times$. Consequently $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is isomorphic to a subgroup of an abelian group and is abelian.

It follows from Corollary 9.39 that every extension of intermediate fields is Galois and has abelian Galois group. For $1 \leq r \leq n$, we introduce the intermediate field $\mathbb{K}_r = \Bbbk(\omega_1, \omega_2, \dots, \omega_r)$. Here $\mathbb{K}_1 = \Bbbk(1) = \Bbbk$. For $1 < r < n$, $\mathbb{K}_r$ is generated as a vector space over $\mathbb{K}_{r-1}$ by $\omega_r, \omega_r^2, \dots, \omega_r^{r-1}$ since $\sum_{k=0}^{r-1} \omega_r^k = 0$ for $r > 1$, and thus $[\mathbb{K}_r : \mathbb{K}_{r-1}] \leq r - 1$. Since $\mathrm{Gal}(\mathbb{K}_r/\mathbb{K}_{r-1})$ is abelian, it has a composition series whose consecutive quotients are cyclic of prime order, the prime order necessarily being $\leq [\mathbb{K}_r : \mathbb{K}_{r-1}] \leq r - 1$. Applying Galois theory, form the chain of intermediate extensions between $\mathbb{K}_{r-1}$ and $\mathbb{K}_r$. The degree of each extension is some prime p with $p \leq r - 1$, the prime depending on the two fields in the chain. The p^{th} roots of unity are in the smaller of any two consecutive fields because they are in $\mathbb{K}_{r-1}$. By Corollary 9.48, such a degree-p extension between $\mathbb{K}_{r-1}$ and $\mathbb{K}_r$ is generated by the smaller field and the p^{th} root of an element in the smaller field. Since $\mathbb{K}_1 = \Bbbk$, we see inductively that $\mathbb{K}_r$ has a root tower over $\mathbb{K}_{r-1}$ for each r. Since $\mathbb{K} = \mathbb{K}_n$, $\mathbb{K}$ has a root tower over $\Bbbk$. □

PROOF OF SUFFICIENCY IN THEOREM 9.44 THAT $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ BE SOLVABLE. Let $F(X)$ be in $\Bbbk[X]$, and suppose that $\mathbb{K}$ is a splitting field of $F(X)$ over $\Bbbk$. Under the assumption that $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is solvable, we are to prove that there exists a finite extension $\mathbb{K}'$ of $\mathbb{K}$ having a root tower.

Since $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$ is solvable, we can find a finite sequence of subgroups of G, each normal in the next larger one, such that the quotient of any consecutive pair is cyclic of prime order. We write

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_{k-1} \supseteq H_k = \{1\}$$

with H_j/H_{j+1} cyclic of prime order p_j for $0 \leq j < k$. Let

$$\Bbbk = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_{k-1} \subseteq \mathbb{K}_k = \mathbb{K}$$

be the corresponding sequence of intermediate fields given by the Fundamental Theorem of Galois Theory (Theorem 9.38). Here $\mathbb{K}_j = \mathbb{K}^{H_j}$, and $H_j = \mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)$.

According to Corollary 9.39, $\mathbb{K}_{j+1}$ is a normal extension of $\mathbb{K}_j$ if and only if $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_{j+1})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)$, and in this case we have a group isomorphism $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_j)\big/\mathrm{Gal}(\mathbb{K}/\mathbb{K}_{j+1}) \cong \mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$. Since H_{j+1} is a normal subgroup of H_j with quotient cyclic of order p_j, it follows that $\mathbb{K}_{j+1}/\mathbb{K}_j$ is indeed normal and the Galois group is cyclic of order p_j.

Let us use Theorem 9.22 to regard $\mathbb{K}$ as lying in a fixed algebraic closure $\overline{\mathbb{K}}'$. Let n be the product of all the primes p_j, and let $\mathbb{K}'_0$ be the splitting field over $\Bbbk$ for $\prod_{r=1}^{n}(X^r - 1)$ within $\overline{\mathbb{K}}'$. For $1 \leq j \leq k$, let $\mathbb{K}'_j$ be the subfield of $\overline{\mathbb{K}}'$ generated by $\mathbb{K}_j$ and $\mathbb{K}'_0$. We define $\mathbb{K}' = \mathbb{K}'_k$. Then we have

$$\Bbbk \subseteq \mathbb{K}'_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_{k-1} \subseteq \mathbb{K}'_k = \mathbb{K}'.$$

Lemma 9.49 shows that $\mathbb{K}'_0$ has a root tower over $\mathbb{K}'$. To complete the proof, it is enough to show for each $j \geq 0$ that either $\mathbb{K}'_{j+1} = \mathbb{K}'_j$ or else $[\mathbb{K}'_{j+1} : \mathbb{K}'_j] = p_j$ and $\mathbb{K}'_{j+1}$ is generated by $\mathbb{K}'_j$ and the p_j^{th} root of some member of $\mathbb{K}'_j$.

For each $j \geq 0$, suppose that $\mathbb{K}_{j+1} = \mathbb{K}_j(x_j)$. Let $F_j(X)$ be the minimal polynomial of x_j over $\mathbb{K}_j$. Since $\mathbb{K}_{j+1}/\mathbb{K}_j$ is normal, $\mathbb{K}_{j+1}$ is the splitting field of $F_j(X)$ over $\mathbb{K}_j$. Then $\mathbb{K}'_{j+1} = \mathbb{K}'_j(x_j)$ is the splitting field of $F_j(X)\prod_{r=1}^{n}(X^r - 1)$ over $\mathbb{K}'_j$, and consequently $\mathbb{K}'_{j+1}/\mathbb{K}'_j$ is a normal extension. If g is in $\mathrm{Gal}(\mathbb{K}'_{j+1}/\mathbb{K}'_j)$, then g sends x_j into a root of $F_j(X)$ and is determined by this root. The restriction $g\big|_{\mathbb{K}_{j+1}}$ therefore carries $\mathbb{K}_{j+1}$ into itself and is in $\mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$. Since g is determined by $g(x_j)$, the group homomorphism $g \mapsto g\big|_{\mathbb{K}_{j+1}}$ is one-one. The image of this homomorphism must be a subgroup of $\mathrm{Gal}(\mathbb{K}_{j+1}/\mathbb{K}_j)$ and therefore must be trivial or have p_j elements. In the first case, $\mathbb{K}'_{j+1} = \mathbb{K}'_j$, and in the second case, $[\mathbb{K}'_{j+1} : \mathbb{K}'_j] = p_j$. In the latter case, $\mathbb{K}'_j$ contains all p_j of the p_j^{th} roots of 1 since these roots of 1 are in $\mathbb{K}'_0$; by Corollary 9.48, $\mathbb{K}'_{j+1}$ is generated by $\mathbb{K}'_j$ and a p_j^{th} root of some member of $\mathbb{K}'_j$. This completes the proof. □

We turn now to apply our methods to irreducible cubics over a field $\Bbbk$ of characteristic 0. In effect we shall derive Cardan's formula,[15] which was mentioned at the beginning of Section 11.

The Galois group of a splitting field of a cubic polynomial has to be a subgroup of the symmetric group $\mathfrak{S}_3$, and irreducibility of the cubic implies that the Galois group has to contain a 3-cycle. Therefore the Galois group has to be either $\mathfrak{S}_3$ or the alternating group $\mathfrak{A}_3 \cong C_3$.

Let the cubic be $X^3+a_2X^2+a_1X+a_0$, the coefficients being in $\Bbbk$. Substituting $X = Z - \frac{1}{3}a_2$ converts the polynomial into

$$\begin{aligned}(Z - \tfrac{1}{3}a_2)^3 + a_2(Z - \tfrac{1}{3}a_2)^2 + a_1(Z - \tfrac{1}{3}a_2) + a_0&\\ = Z^3 + (a_1 - \tfrac{1}{3}a_2^2)Z + (a_0 - \tfrac{1}{3}a_1a_2 + \tfrac{2}{27}a_2^3)&,\end{aligned}$$

and therefore we can assume whenever convenient that the given polynomial has $a_2 = 0$.

Suppose for the moment that the Galois group is $G = \mathfrak{S}_3$. A composition series is

$$G = \mathfrak{S}_3 \supseteq \mathfrak{A}_3 \supseteq \{1\},$$

and we can write the corresponding sequence of fixed fields as

$$\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K},$$

where $\mathbb{K}$ is the splitting field and $\mathbb{L}$ is $\mathbb{K}^{\mathfrak{A}_3}$. The dimensions satisfy $[\mathbb{L} : \Bbbk] = 2$ and $[\mathbb{K} : \mathbb{L}] = 3$.

Let the roots in $\mathbb{K}$ of the given cubic be r_1, r_2, r_3. Since G is solvable, Theorem 9.44 tells us that the roots are expressible in terms of radicals and members of $\Bbbk$. To derive explicit formulas for the roots, the idea is to use a two-step process with Lagrange resolvents, arguing as in the proof of Corollary 9.48 at each step.

The first step involves passing from $\Bbbk$ to $\mathbb{L}$. The square roots of 1 are already in $\Bbbk$, and $\mathbb{L}$ is to be obtained from $\Bbbk$ by adjoining one of the square roots of some element of $\Bbbk$. In Proposition 9.47 the Galois group $\operatorname{Gal}(\mathbb{L}/\Bbbk)$ is a 2-element quotient group, the sum is over members of the quotient group, and the element x is in $\mathbb{L}$. It is a little more convenient to pull the sum back to one over the 6-element symmetric group, taking ω to be the sign function on $\mathfrak{S}_3$ and taking x to be any element of $\mathbb{K}$. The formulas for the projection operators E_0 and E_1 are then

$$\begin{aligned}E_0x &= \tfrac{1}{6} \sum_{\sigma\in\mathfrak{S}_3} \sigma(x),\\ E_1x &= \tfrac{1}{6} \sum_{\sigma\in\mathfrak{S}_3} (\operatorname{sgn}\sigma)\sigma(x),\end{aligned}$$

[15] We discuss only Cardan's cubic formula, omitting any discussion of the corresponding quartic formula, which often bears Cardan's name and which can be handled with the same techniques. See Van der Waerden, Vol. I, Section 58, for details.

with x in $\mathbb{K}$, and the proof of Corollary 9.48 tells us to adjoin to $\Bbbk$ the square root of any element of image E_1, i.e., any element with $\sigma(x) = (\operatorname{sgn} x)x$ for all σ in $\mathfrak{S}_3$.

The only elements of $\mathbb{K}$ for which we have good control of the action of the Galois group, apart from the elements of $\Bbbk$, are the elements that are expressed directly in terms of the roots r_1, r_2, r_3 of the polynomial. By renumbering the roots if necessary, we may assume that the roots are permuted by $\mathfrak{S}_3$ according to their subscripts. An example of a polynomial function of r_1, r_2, r_3 that transforms according to the sign of the permutation played a role in Section I.4 in defining the sign of a permutation. It is the **difference product** of the polynomial, namely

$$\prod_{1\le i<j\le 3} (r_j - r_i).$$

This is a square root of the **discriminant** D of the polynomial, which is given by

$$D = \prod_{1\le i<j\le 3} (r_j - r_i)^2.$$

We shall compute D in terms of the coefficients of the cubic shortly. In the meantime, the proof of Corollary 9.48 thus tells us that $\mathbb{L} = \Bbbk(\sqrt{D}\,)$. Here $\sqrt{D}$ is given by

$$\begin{aligned}\sqrt{D} &= (r_3 - r_2)(r_3 - r_1)(r_2 - r_1)\\ &= (r_1r_2^2 + r_2r_3^2 + r_3r_1^2) - (r_1^2r_2 + r_2^2r_3 + r_3^2r_1).\end{aligned}$$

The second step is to pass from $\mathbb{L}$ to $\mathbb{K}$. Corollary 9.48 says to expect $\mathbb{K}$ to be obtained by adjoining the cube root of something if the cube roots of 1 are already present in $\mathbb{L}$. The proof of the second half of Theorem 9.44, which follows Corollary 9.48, indicates how we can incorporate the cube roots of 1 into the fields in order to have a root tower. What we can do is to replace $\Bbbk$ at the start by a splitting field for $\prod_{1\le r\le 3}(X^r - 1)$. Since ± 1 are already in $\Bbbk$, we are to adjoin the nontrivial cube roots of 1, i.e., the roots of $X^2 + X + 1$, if they are not already present. In other words, what we do is replace $\Bbbk$ at the start by $\Bbbk(\sqrt{-3}\,)$. Changing notation, we assume that $\sqrt{-3}$ lies in $\Bbbk$ from the outset.

We can now use Lagrange resolvents. Let σ be the generator $(1\ \ 2\ \ 3)$ of $\mathfrak{A}_3$, sending r_1 to r_2, r_2 to r_3, and r_3 to r_1. Let $\omega = \frac{1}{2}(-1 + \sqrt{-3}\,)$ be a primitive cube root of 1. Then we have

$$\begin{aligned}E_0x &= \tfrac{1}{3}(x + \sigma x + \sigma^2 x),\\ E_1x &= \tfrac{1}{3}(x + \omega^{-1}\sigma x + \omega^{-2}\sigma^2 x),\\ E_2x &= \tfrac{1}{3}(x + \omega^{-2}\sigma x + \omega^{-1}\sigma^2 x).\end{aligned}$$

Again we can use any x, but the roots of the cubic are the simplest nontrivial elements for which we know the action of σ. Corollary 9.48 shows that $\mathbb{K} = \mathbb{L}(E_1x)$ if $E_1x \neq 0$. Proposition 9.47 says that $(E_1x)^3$ is fixed by σ, and it therefore lies in $\mathbb{L}$. Hence $\mathbb{K}$ is identified as obtained from $\mathbb{L}$ by adjoining a cube root of the element $(E_1x)^3$ of $\mathbb{L}$.

Taking $x = r_1$, we have $\sigma x = r_2$ and $\sigma^2 x = r_3$. Also, $\omega^{\pm 1} = \frac{1}{2}(-1 \pm \sqrt{-3}\,)$. Using the formula for E_1x and substituting for $\sqrt{D}$ and $\omega^{\pm 1}$ then gives

$$\begin{aligned}(3E_1r_1)^3 &= r_1^3 + r_2^3 + r_3^2 + 6r_1r_2r_3 \\ &\qquad + 3\omega^{-1}(r_1^2r_2 + r_2^2r_3 + r_3^2r_1) + 3\omega(r_1r_2^2 + r_2r_3^2 + r_3r_1^2) \\ &= \sum_i r_i^3 + 6r_1r_2r_3 - \tfrac{3}{2}\sum_{i\neq j} r_i^2r_j + \tfrac{3}{2}\sqrt{-3}\sqrt{D}.\end{aligned}$$

To proceed further, we shall want to substitute expressions involving the coefficients of the cubic for the above symmetric expressions in the roots.[16] These expressions will be considerably simplified if we assume that the coefficient of X^2 in the cubic is 0. We know that this assumption involves no loss of generality. Thus we assume for the remainder of this section that the cubic is $X^3 + pX + q$. The relevant formulas relating the roots and the coefficients are

$$\begin{aligned} r_1 + r_2 + r_3 &= 0, \\ r_1r_2 + r_1r_3 + r_2r_3 &= p, \\ r_1r_2r_3 &= -q. \end{aligned}$$

Aiming for the right side of the displayed formula for $(3E_1r_1)^3$, we have

$$\begin{aligned} 0 &= (r_1 + r_2 + r_3)^3 = \sum_i r_i^3 + 3\sum_{i\neq j} r_i^2r_j + 6r_1r_2r_3, \\ 0 &= (r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) = -\tfrac{9}{2}\sum_{i\neq j} r_i^2r_j - \tfrac{27}{2}r_1r_2r_3, \\ -\tfrac{27}{2}q &= \tfrac{27}{2}r_1r_2r_3. \end{aligned}$$

Addition of these three lines and comparison with the expression for $3(E_1r_1)^3$ yields

$$-\tfrac{27}{2}q = \sum_i r_i^3 - \tfrac{3}{2}\sum_{i\neq j} r_i^2r_j + 6r_1r_2r_3 = (3E_1r_1)^3 - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

Consequently

$$(3E_1r_1)^3 = -\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

[16] Problems 36–39 at the end of Chapter VIII assure us that this rewriting is possible. For our derivation this assurance is not logically necessary, since we will be producing explicit formulas.

Similarly

$$(3E_2r_1)^3 = -\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.$$

Since $3E_0r_1 = r_1 + r_2 + r_3 = 0$, we have expressions for E_0r_1, E_1r_1, and E_2r_1, apart from the choices of the cube roots. Proposition 9.47b says that we recover r_1 by addition: $r_1 = E_0r_1 + E_1r_1 + E_2r_1$. Thus we have found a root explicitly as soon as we sort out the ambiguity in the choices of cube roots and determine the value of D in terms of the coefficients p and q.

Theorem 9.50 (Cardan's formula). Let $\Bbbk$ be a field of characteristic 0 containing $\sqrt{-3}$, and let $X^3 + pX + q$ be an irreducible cubic in $\Bbbk[X]$. For this polynomial the discriminant D is given by

$$D = -4p^3 - 27q^2.$$

The Galois group of a splitting field of the cubic is $\mathfrak{S}_3$ if D is a nonsquare in $\Bbbk$ and is $\mathfrak{A}_3$ if D is a square in $\Bbbk$. In either case, fix a square root of D, denote it by $\sqrt{D}$, and let $\omega^{\pm 1} = \tfrac{1}{2}(-1 \pm \sqrt{-3})$ be the primitive cube roots of 1. Then it is possible to determine cube roots of the form

$$3E_1r_1 = \sqrt[3]{-\tfrac{27}{2}\,q + \tfrac{3}{2}\sqrt{-3}\sqrt{D}} \quad \text{and} \quad 3E_2r_1 = \sqrt[3]{-\tfrac{27}{2}\,q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}}$$

in such a way that their product is $(3E_1r_1)(3E_1r_2) = -3p$, and in this case the three roots of $X^3 + pX + q$ are given by

$$\begin{aligned} r_1 &= E_1r_1 + E_2r_1, \\ r_2 &= \omega E_1r_1 + \omega^2 E_2r_1, \\ r_3 &= \omega^2 E_1r_1 + \omega E_2r_1. \end{aligned}$$

PROOF. Define $\sigma_k = r_1^k + r_2^k + r_3^k$ for $1 \le k \le 4$. By inspection we have

$$\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix}.$$

Taking the determinant of both sides and applying Corollary 5.3, we obtain

$$D = \det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} = 3\sigma_2\sigma_4 - \sigma_2^3 - 3\sigma_3^2.$$

The given cubic shows that $\sigma_1 = r_1 + r_2 + r_3 = 0$. For the other σ_i's, we have

$$\begin{aligned}
\sigma_2 = r_1^2 + r_2^2 + r_3^2 &= (r_1 + r_2 + r_3)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3) = -2p, \\
\sigma_3 = r_1^3 + r_2^3 + r_3^3 &= (r_1 + r_2 + r_3)(r_1^2 + r_2^2 + r_3^2) \\
&\quad - (r_1^2r_2 + r_1^2r_3 + r_2^2r_1 + r_2^2r_3 + r_3^2r_1r_3^2r_2) \\
&= -(r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3) + 3r_1r_2r_3 = -3q, \\
\sigma_4 = r_1^4 + r_2^4 + r_3^4 &= (r_1^2 + r_2^2 + r_3^2)^2 - 2(r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2) \\
&= (-2p)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3)^2 \\
&\quad + 4r_1r_2r_3(r_1 + r_2 + r_3) = (-2p)^2 - 2(p)^2 = 2p^2.
\end{aligned}$$

Substituting, we obtain $D = -12p^3 + 8p^3 - 27q^2 = -4p^3 - 27q^2$. This proves the formula for D. In particular, it confirms that D lies in $\Bbbk$.

The Galois group of the splitting field of the polynomial must be $\mathfrak{S}_3$ or $\mathfrak{A}_3$. If it is $\mathfrak{S}_3$, then we saw above that $\mathbb{L} = \Bbbk(\sqrt{D})$ and that $[\mathbb{L} : \Bbbk] = 2$. Hence D is a nonsquare in $\Bbbk$. If the Galois group is $\mathfrak{A}_3$, then $(r_3 - r_2)(r_3 - r_1)(r_2 - r_1)$ is fixed by the Galois group and lies in $\Bbbk$. The square of this element is D, and hence D is a square in $\Bbbk$.

With either Galois group the calculations with the cubic extension that precede the statement of the theorem are valid. If r_1 is one of the roots, then we know that

$$\begin{aligned}
r_1 &= E_0r_1 + E_1r_1 + E_2r_1 = E_1r_1 + E_2r_1, \\
(3E_1r_1)^3 &= -\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3}\sqrt{D}, \\
(3E_2r_1)^3 &= -\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3}\sqrt{D}.
\end{aligned}$$

The uniqueness of simple extensions (Theorem 9.11) says that we can make any choice of cube root to determine $3E_1r_1$. Then

$$\begin{aligned}
(3E_1r_1)(3E_2r_1) &= (r_1 + \omega^{-1}\sigma r_1 + \omega^{-2}\sigma^2 r_1)(r_1 + \omega^{-2}\sigma r_1 + \omega^{-1}\sigma^2 r_1) \\
&= (r_1 + \omega^{-1}r_2 + \omega r_3)(r_1 + \omega r_2 + \omega^{-1}r_3) \\
&= (r_1^2 + r_2^2 + r_3^2) + (\omega + \omega^{-1})(r_1r_2 + r_1r_3 + r_2r_3) \\
&= (r_1^2 + r_2^2 + r_3^2) - (r_1r_2 + r_1r_3 + r_2r_3).
\end{aligned}$$

The first term on the right side we calculated in the first paragraph of the proof as $\sigma_2 = -2p$, and the second term gives $-p$. Thus $(3E_1r_1)(3E_2r_1) = -3p$ as asserted. Since σ operates on image E_1 as multiplication by ω and on image E_2 as multiplication by ω^2, the fact that $r_1 = E_1r_1 + E_2r_1$ implies that

$$r_2 = \sigma(r_1) \ = \omega E_1r_1 + \omega^2 E_2r_1$$

and

$$r_3 = \sigma^2(r_1) = \omega^2 E_1r_1 + \omega E_2r_1.$$

This completes the proof. □

14. Proof That π Is Transcendental

In this section and the next three, we combine Galois theory with some of the ring theory in the second half of Chapter VIII. This combination will allow us to prove some striking theorems, see how Galois groups can be used effectively in practice, and develop some techniques for identifying Galois groups explicitly.

The present section is devoted to the proof of the following theorem.

Theorem 9.51 (Lindemann, 1882). The number π is transcendental over $\mathbb{Q}$.

The argument we give is based on that in a book by L. K. Hua.[17] For purposes of having a precise theorem, π is defined as the least positive real number such that $e^{\pi i} = -1$. In addition to Galois theory in the form of Proposition 9.35, the proof here will make use of a few facts about algebraic integers. Algebraic integers were defined in Section VIII.1 and again in Section VIII.9 (as well as in Section VII.4) as complex numbers that are roots of monic polynomials in $\mathbb{Z}[X]$. The algebraic integers form a ring by Corollary 8.38 (or alternatively by Lemma 7.30), the only algebraic integers in $\mathbb{Q}$ are the members of $\mathbb{Z}$ by Proposition 8.41 (or alternatively by Lemma 7.30), and any algebraic number x has the property that nx is an algebraic integer for some integer $n \neq 0$ by Proposition 8.42.

We begin with a lemma.

Lemma 9.52. Let $f(X)$ in $\mathbb{C}[X]$ be given by $f(X) = \sum_{k=0}^{n} a_k X^k$, and define $F(X)$ to be the sum of the derivatives of $f(X)$:

$$F(X) = \sum_{l=0}^{n} f^{(l)}(X).$$

If $Q(z)$ is defined as $Q(z) = F(0)e^z - F(z)$ for $z \in \mathbb{C}$, then $F(0) = \sum_{k=0}^{n} a_k k!$ and

$$|Q(z)| \leq e^{|z|} \sum_{k=0}^{n} |a_k||z|^k.$$

PROOF. We calculate directly that

$$F(z) = \sum_{l=0}^{n} \sum_{k=l}^{n} \frac{a_k k!}{(k-l)!} z^{k-l} = \sum_{k=0}^{n} a_k \sum_{l=0}^{k} \frac{k!}{(k-l)!} z^{k-l} = \sum_{k=0}^{n} a_k \sum_{l=0}^{k} \frac{k!}{l!} z^l.$$

[17] *Introduction to Number Theory*, pp. 484–488. In the same pages Hua establishes the earlier theorem of Hermite that e is transcendental, using a related but simpler argument.

Evaluation at $z = 0$ gives $F(0) = \sum_{k=0}^{n} a_k k!$. Then

$$\begin{aligned}
|Q(z)| &\le \Big| \sum_{k=0}^{n} a_k \sum_{l=0}^{\infty} \frac{k!}{l!} z^l - \sum_{k=0}^{n} \sum_{l=0}^{k} \frac{k!}{l!} z^l \Big| \\
&= \Big| \sum_{k=0}^{n} a_k \sum_{l=k+1}^{\infty} \frac{k!}{l!} z^l \Big| \\
&\le \sum_{k=0}^{n} |a_k| \sum_{l=k+1}^{\infty} \frac{|z|^l}{(l-k)!} \qquad \text{since } \tbinom{l}{k}^{-1} \le 1 \\
&= \sum_{k=0}^{n} |a_k| |z|^k \sum_{m=1}^{\infty} \frac{|z|^m}{m!} \\
&\le e^{|z|} \sum_{k=0}^{n} |a_k| |z|^k. \qquad \square
\end{aligned}$$

PROOF OF THEOREM 9.51. Arguing by contradiction, suppose that π is algebraic over $\mathbb{Q}$, so that $\alpha = \pi i$ is algebraic over $\mathbb{Q}$ as well. Let $M(X)$ be the minimal polynomial of α over $\mathbb{Q}$, and let $\mathbb{K}$ be the splitting field of $M(X)$ in $\mathbb{C}$. This exists since $\mathbb{C}$ is algebraically closed. We write $\alpha_1, \dots, \alpha_m$ for the roots of $M(X)$ in $\mathbb{K}$, with $\alpha_1 = \alpha$. These are distinct algebraic numbers, and they are permuted by the Galois group, $G = \operatorname{Gal}(\mathbb{K}/\mathbb{Q})$. What we shall show is that

$$R = \prod_{j=1}^{m} (1 + e^{\alpha_j}) \neq 0.$$

This will be a contradiction since $1 + e^{\alpha_1} = 0$ for $\alpha_1 = i\pi$.

We expand the product defining R, obtaining

$$R = 1 + \sum_{j} e^{\alpha_j} + \sum_{j,k} e^{\alpha_j + \alpha_k} + \cdots ,$$

Whenever one of the exponentials has total exponent 0, we lump that term with the constant 1. Otherwise we write the term as e^{β_l}, allowing repetitions among terms e^{β_l}. Thus

$$R = N + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r},$$

with N an integer ≥ 1, with each $\beta_l \neq 0$, and with $N + r = 2^m$.

Each member of $G = \operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ permutes $\alpha_1, \dots, \alpha_m$, and it therefore permutes the β_l's that are single α_j's, permutes the β_l's that are the nonzero sums of two α_j's, permutes the β_l's that are the nonzero sums of three α_j's, and so on.

Choose an integer $a > 0$ such that $a\alpha_1, \dots, a\alpha_m$ are algebraic integers, let p be a prime number large enough to satisfy some conditions to be specified shortly, and define

$$f(X) = \frac{(aX)^{p-1}}{(p-1)!} \prod_{l=1}^{r} (aX - a\beta_l)^p = \sum_{k=0}^{n} a_k X^n.$$

The members σ of G act on $f(X)$ as usual by acting on the coefficients. Each β_l that is the nonzero sum of a certain number of α_j's is sent into another $\beta_{l'}$ of the same kind, and thus σ just permutes the factors of the product defining f, leaving $f(X)$ unchanged. The coefficients of $(p-1)!f(a^{-1}X)$ are algebraic integers in $\mathbb{K}$. Being fixed by G, they are in $\mathbb{Q}$ by Proposition 9.35d, and hence they are in $\mathbb{Z}$. Therefore

$$f(X) = \frac{A_{p-1}a^{p-1}X^{p-1} + A_p a^p X^p + \cdots}{(p-1)!}$$

with $A_{p-1}, A_p, \ldots$ in $\mathbb{Z}$. Since $A_{p-1} = \prod_{l=1}^r(-a\beta_l)^p$, we can arrange that p does not divide $A_{p-1}a^{p-1}$ by choosing p greater than a and greater than $\left|\prod_{l=1}^r(a\beta_l)\right|$. If we look at the l^{th} factor in the product defining $f(X)$, we see that $(X-\beta_l)^p$ divides $f(X)$ in $\mathbb{K}[X]$. Therefore we have further formulas for $f(X)$, namely

$$f(X) = \frac{\gamma_{p,l}(X-\beta_l)^p + \gamma_{p+1,l}(X-\beta_l)^{p+1} + \cdots}{(p-1)!} \qquad \text{for } 1 \le l \le r.$$

As in Lemma 9.52, we define

$$F(X) = \sum_{l=0}^{n} f^{(l)}(X) \qquad \text{and} \qquad Q(z) = F(0)e^z - F(z).$$

Then we have $F(0) = \sum_{k=0}^n a_k k!$. For $1 \le l \le r$, the definition of $Q(z)$ gives $F(0)e^{\beta_l} = F(\beta_l) + Q(\beta_l)$. Substituting from the definition of R, we obtain

$$F(0)R = F(0)\big(N + \sum_{l=1}^r e^{\beta_l}\big) = NF(0) + \sum_{l=1}^r F(\beta_l) + \sum_{l=1}^r Q(\beta_l). \qquad (*)$$

A further condition that we impose on the size of p is that $p > N$. Then the computation

$$NF(0) = N\sum_{k=0}^n a_k k! = N(A_{p-1}a^{p-1} + pA_p a^p + p(p+1)A_{p+1}a^{p+1} + \cdots)$$

and the properties of $A_{p-1}, A_p, \ldots$ together imply that $NF(0)$ is an integer and is not divisible by p.

Let us compute $F(\beta_l)$. The derivatives through order $p-1$ of $f(X)$ are 0 at β_l. For the p^{th} derivative we have

$$p\gamma_{p,l} = f^{(p)}(\beta_l) = pA_p a^p + \sum_{j\ge1}\frac{(p+j)\cdots(j+1)}{(p-1)!}A_{p+j}a^{p+j}\beta_l^j.$$

The coefficient of $A_{p+j}a^{p+j}\beta_l^j$ inside the sum equals

$$\frac{(p+j)\cdots(j+1)j!p}{p(p-1)!j!} = p\binom{p+j}{j},$$

and thus

$$p\gamma_{p,l} = f^{(p)}(\beta_l) = a^p\big(pA_p + \sum_{j\geq 1} p\tbinom{p+j}{j}A_{p+j}(a\beta_l)^j\big).$$

The higher-order derivatives are computed and simplified similarly. For the $(p+k)^{\text{th}}$ derivative with $k \geq 1$, we find that

$$\begin{aligned}(p+k)\cdots(p+1)p\gamma_{p+k,l} &= f^{(p+k)}(\beta_l)\\ &= a^{p+k}\big((p+k)\cdots(p+1)pA_{p+k} \qquad (**)\\ &\quad + \sum_{j\geq 1}(p+k)\cdots(p+1)p\tbinom{p+j+k}{j}A_{p+j+k}(a\beta_l)^j\big).\end{aligned}$$

Put $C_{p+k} = \sum_{l=1}^r \gamma_{p+k,l}$. Summing the left and right members of $(**)$ over l gives

$$C_{p+k} = a^{p+k}\big(rA_{p+k} + \sum_{j\geq 1}\tbinom{p+j+k}{j}A_{p+j+k}\sum_{j=1}^{l}(a\beta_l)^j\big).$$

The sum $\sum_{j=1}^l (a\beta_l)^j$ is an algebraic integer fixed by G, and it is therefore an integer. Consequently each C_{p+k} is an integer. Summing the left and middle members of $(**)$ over k and l gives

$$\sum_{l=1}^r F(\beta_l) = \sum_{k\geq 0}(p+k)\cdots(p+1)pC_{p+k},$$

and this is an integer divisible by p.

Since $NF(0)$ is an integer not divisible by p, $NF(0) + \sum_{l=1}^r F(\beta_l)$ is an integer not divisible by p, and we have

$$\big|NF(0) + \sum_{l=1}^r F(\beta_l)\big| \geq 1.$$

In view of $(*)$, we will have a contradiction to $R = 0$ if we show that

$$\big|\sum_{l=1}^r Q(\beta_l)\big| < 1.$$

An easy argument by induction on m shows that if $\sum_{k=0}^m d_k z^k = \prod_{j=1}^s (z - c_j)$, then $\sum_{k=0}^m |d_k||z|^k \leq \prod_{j=1}^s(|z| + |c_j|)$. Applying this observation to the sum and product defining $f(X)$ and using Lemma 9.52, we see that

$$e^{-|z|}|Q(z)| \leq \sum_{k=0}^n |a_k||z|^k \leq \frac{(a|z|)^{p-1}\prod_{l=1}^r (a|z| + a|\beta_l|)^p}{(p-1)!}.$$

For each fixed z, the right side is the $(p-1)^{\text{st}}$ term of the convergent series for an exponential function at an appropriate point, and hence the right side is less than $r^{-1}e^{-|z|}$ for p sufficiently large, p depending on z. Choosing p large enough to make the right side less than $r^{-1}e^{-|z|}$ for $z = \beta_1, \dots, \beta_l$ and summing over these z's, we obtain $\big|\sum_{l=1}^{r} Q(\beta_l)\big| < 1$, and we have arrived at the contradiction we anticipated. □

15. Norm and Trace

This is the second of four sections in which we combine Galois theory with some of the ring theory in the second half of Chapter VIII. We shall make use of a little more linear algebra than we have used thus far in this chapter, and we shall conclude the section by completing the proof of Theorem 8.54 concerning extensions of Dedekind domains.

Let $\Bbbk$ be a field, not necessarily of characteristic 0, and let $\mathbb{K}$ be a finite algebraic extension. We take advantage of the fact that $\mathbb{K}$ is a vector space over $\Bbbk$. If a is in $\mathbb{K}$, let us write $M(a)$ for the $\Bbbk$ linear mapping from $\mathbb{K}$ to $\mathbb{K}$ given by multiplication by a. The characteristic polynomial $\det(XI - M(a))$ is called the **field polynomial** of a and is a monic polynomial in $\Bbbk[X]$ of degree $[\mathbb{K} : \Bbbk]$. The **norm** and **trace** of a relative to $\mathbb{K}/\Bbbk$ are defined to be the determinant and trace of the linear mapping $M(a)$. In symbols,

$$N_{\mathbb{K}/\Bbbk}(a) = \det(M(a)),$$
$$\operatorname{Tr}_{\mathbb{K}/\Bbbk}(a) = \operatorname{Tr}(M(a)).$$

Both $N_{\mathbb{K}/\Bbbk}$ and $\operatorname{Tr}_{\mathbb{K}/\Bbbk}$ are functions from $\mathbb{K}$ to $\Bbbk$. If $n = [\mathbb{K} : \Bbbk]$, then $N_{\mathbb{K}/\Bbbk}(a)$ is $(-1)^n$ times the constant term of $\det(XI - M(a))$, and $\operatorname{Tr}_{\mathbb{K}/\Bbbk}(a)$ is minus the coefficient of X^{n-1}. The subscript $\mathbb{K}/\Bbbk$ may be omitted when there is no chance of ambiguity.

EXAMPLE. $\Bbbk = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, $a = \sqrt{2}$. If we use $\Gamma = (1, \sqrt{2})$ as an ordered basis of $\mathbb{K}$ over $\Bbbk$, then the matrix of $M(a)$ relative to Γ is $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Since characteristic polynomials are independent of the choice of basis, the field polynomial of a can be computed in this basis and is given by

$$\det\begin{pmatrix} XI-M(a) \\ \Gamma\Gamma \end{pmatrix} = \det\begin{pmatrix} X & -2 \\ -1 & X \end{pmatrix} = X^2 - 2.$$

We can read off the norm and trace as $N(a) = -2$ and $\operatorname{Tr}(a) = 0$.

Proposition 9.53. If $\mathbb{K}/\Bbbk$ is a finite extension of fields with $n = [\mathbb{K} : \Bbbk]$, then norms and traces relative to $\mathbb{K}/\Bbbk$ have the following properties:

(a) $N(ab) = N(a)N(b)$,
(b) $N(ca) = c^n N(a)$ for $c \in \Bbbk$,
(c) $N(1) = 1$, and consequently $N(c) = c^n$ for $c \in \Bbbk$,
(c) $\operatorname{Tr}(a + b) = \operatorname{Tr}(a) + \operatorname{Tr}(b)$,
(d) $\operatorname{Tr}(ca) = c \operatorname{Tr}(a)$ for $c \in \Bbbk$,
(e) $\operatorname{Tr}(1) = n$, and consequently $\operatorname{Tr}(c) = nc$ for $c \in \Bbbk$.

PROOF. Properties (a) and (b) follow from properties of the determinant in combination with the identities $M(ab) = M(a)M(b)$ and $M(ca) = cM(a)$. Properties (c) and (d) follow from properties of the trace in combination with the identities $M(a + b) = M(a) + M(b)$ and $M(ca) = cM(a)$. Since $M(1)$ is the identity, the norm and trace of 1 are 1 and n, respectively. The other conclusions in (c) and (e) are then consequences of this fact in combination with (b) and (d). □

Proposition 9.54. Let $\mathbb{K}/\Bbbk$ and $\mathbb{L}/\mathbb{K}$ be finite extensions of fields with $[\mathbb{K} : \Bbbk] = n$ and $[\mathbb{L} : \mathbb{K}] = m$, and let a be in $\mathbb{K}$. The element a acts by multiplication on $\mathbb{K}$ and also on $\mathbb{L}$, yielding $\Bbbk$ linear maps in each case that will be denoted by $M_{\mathbb{K}/\Bbbk}(a)$ and $M_{\mathbb{L}/\Bbbk}(a)$. Then in suitable ordered vector-space bases the matrix of $M_{\mathbb{L}/\Bbbk}(a)$ is block diagonal, each block being the matrix of $M_{\mathbb{K}/\Bbbk}(a)$.

PROOF. We choose the bases as in Theorem 7.6. Thus let $\Gamma = (\omega_1, \omega_2, \dots)$ be an ordered basis of $\mathbb{K}$ over $\Bbbk$, and let $\Delta = (\xi_1, \xi_2, \dots)$ be a basis of $\mathbb{L}$ over $\mathbb{K}$. Theorem 7.6 observes that the mn products $\xi_i \omega_j$ form a basis of $\mathbb{L}$ over $\Bbbk$, and we make this set into an ordered basis Ω by saying that $(i_1, j_1) < (i_2, j_2)$ if $i_1 < i_2$ or if $i_1 = i_2$ and $j_1 < j_2$. Let $M_{\mathbb{K}/\Bbbk}(a)\omega_j = \sum_l c_{lj}\omega_l$. Then

$$M_{\mathbb{L}/\Bbbk}(a)\xi_i\omega_j = \Big(\sum_{l=1}^{n} c_{lj}\omega_l\Big)\xi_i = \sum_{k=1}^{m}\sum_{l=1}^{n} (\delta_{ki}c_{lj})\xi_k\omega_l,$$

where δ_{ki} is 1 when $k = i$ and is 0 otherwise. The matrix $\begin{pmatrix} M_{\mathbb{L}/\Bbbk}(a) \\ \Omega\Omega \end{pmatrix}$ has $((k, l), (i, j))^{\text{th}}$ entry $\delta_{ki}c_{lj}$, and this is 0 unless the primary indices k and i are equal. Thus the matrix is block diagonal, the entries of the i^{th} diagonal block being c_{lj}. □

Corollary 9.55. Let $\mathbb{K}/\Bbbk$ and $\mathbb{L}/\mathbb{K}$ be finite extensions of fields with $[\mathbb{L} : \mathbb{K}] = m$, and let a be in $\mathbb{K}$. Let $M_{\mathbb{K}/\Bbbk}(a)$ and $M_{\mathbb{L}/\Bbbk}(a)$ denote multiplication by a on $\mathbb{K}$ and on $\mathbb{L}$, and let $F_{\mathbb{K}/\Bbbk}(X)$ and $F_{\mathbb{L}/\Bbbk}(X)$ be the corresponding field polynomials. Then

$$F_{\mathbb{L}/\Bbbk}(X) = \big(F_{\mathbb{K}/\Bbbk}(X)\big)^m.$$

Consequently $N_{\mathbb{L}/\Bbbk}(a) = (N_{\mathbb{K}/\Bbbk}(a))^m$ and $\operatorname{Tr}_{\mathbb{L}/\Bbbk}(a) = m \operatorname{Tr}_{\mathbb{K}/\Bbbk}(a)$.

PROOF. Proposition 9.54 shows that the matrix of $XI - M_{\mathbb{L}/\Bbbk}(a)$ may be taken to be block diagonal with each of the m diagonal blocks equal to the matrix of $XI - M_{\mathbb{K}/\Bbbk}(a)$. The determinant of $XI - M_{\mathbb{L}/\Bbbk}(a)$ is the product of the determinants of the diagonal blocks, and the formula relating the field polynomials is proved.

The formulas for the norms and the traces are consequences of this relationship. In fact, let

$$F_{\mathbb{K}/\Bbbk}(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$$

and

$$F_{\mathbb{L}/\Bbbk}(X) = X^{mn} + d_{mn-1}X^{mn-1} + \cdots + d_0.$$

Comparing coefficients of $F_{\mathbb{L}/\Bbbk}(X)$ and $\big(F_{\mathbb{K}/\Bbbk}(X)\big)^m$, we see that $d_{mn-1} = mc_{n-1}$ and $d_0 = c_0^m$. Therefore

$$N_{\mathbb{L}/\Bbbk}(a) = (-1)^{mn}d_0 = ((-1)^n c_0)^m = (N_{\mathbb{K}/\Bbbk}(a))^m$$

and

$$\operatorname{Tr}_{\mathbb{L}/\Bbbk}(a) = -d_{mn-1} = -mc_{n-1} = m\operatorname{Tr}_{\mathbb{K}/\Bbbk}(a).$$

This completes the proof. □

Corollary 9.56. Let $\mathbb{K}/\Bbbk$ be a finite extension of fields, and let a be in $\mathbb{K}$. Then the field polynomial of a relative to $\mathbb{K}/\Bbbk$ is a power of the minimal polynomial of a over $\Bbbk$, the power being $[\mathbb{K} : \Bbbk(a)]$. In the special case $\mathbb{K} = \Bbbk(a)$, the minimal polynomial of a coincides with the field polynomial.

REMARKS. In the theory of a single linear transformation as in Chapter V, the minimal polynomial of a linear map divides the characteristic polynomial, by the Cayley–Hamilton Theorem (Theorem 5.9). For a multiplication operator in the context of fields, we get a much more precise result—that the characteristic polynomial is a power of the minimal polynomial.

PROOF. If $F(X)$ is in $\Bbbk[X]$, then the operation M of multiplication has

$$M(F(a))b = F(a)b = F(M(a))b \qquad \text{for } b \in \mathbb{K}, \tag{$*$}$$

as we see by first considering monomials and then forming $\Bbbk$ linear combinations. The minimal polynomial of a over $\Bbbk$ is the unique monic $F(X)$ of lowest degree in $\Bbbk[X]$ for which $F(a) = 0$, hence such that $M(F(a)) = 0$. Meanwhile, the minimal polynomial of the linear map $M(a)$ is the unique monic $F(X)$ of lowest degree such that $F(M(a)) = 0$. These two polynomials coincide because of $(*)$.

The degree of the minimal polynomial of $M(a)$ thus equals the degree of the minimal polynomial of a, which is $[\Bbbk(a) : \Bbbk]$. The Cayley–Hamilton Theorem (Theorem 5.9) shows that the minimal polynomial of $M(a)$ divides the characteristic polynomial of $M(a)$, i.e., the field polynomial of a. When the field $\mathbb{K}$ is $\Bbbk(a)$, the minimal polynomial of a and the field polynomial of a have the same degree; since they are monic, they are equal. This proves the second conclusion of the corollary.

For the first conclusion we know from Corollary 9.55 that the field polynomial of a relative to a general $\mathbb{K}$ is the $[\mathbb{K} : \Bbbk(a)]^{\text{th}}$ power of the field polynomial of a relative to $\Bbbk(a)$. Since we have just seen that the latter polynomial is the minimal polynomial of a, the first conclusion of the corollary follows. $\square$

EXAMPLE, CONTINUED. $\Bbbk = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2}\,)$, $a = \sqrt{2}$. We have seen that the field polynomial of a is $X^2 - 2$, that the norm and trace are $N(a) = -2$ and $\text{Tr}(a) = 0$, and that the matrix of the multiplication operator $M(a)$ in the ordered basis $\Gamma = (1, \sqrt{2}\,)$ is $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. The eigenvalues of $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix}$ are $\pm\sqrt{2}$, namely the roots of the field polynomial. These are not in the field $\Bbbk$. Indeed, they could not possibly be in the field, or we would have $M(a)x = \lambda x$ for some $x \neq 0$ in $\mathbb{K}$ and some λ in $\Bbbk$, and this would mean that $\lambda = a$. Since the roots $\pm\sqrt{2}$ of the field polynomial each have multiplicity 1 and lie in $\mathbb{K}$, the matrix $\begin{pmatrix} M(a) \\ \Gamma\Gamma \end{pmatrix}$ is similar over $\mathbb{K}$ to the diagonal matrix $\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$. Since similar matrices have the same trace and the same norm, we can compute the trace and norm of $M(a)$ from this diagonal matrix, namely by adding or multiplying its diagonal entries. The significance of the diagonal entries is that they are the images of $\sqrt{2}$ under the members of the Galois group $\text{Gal}(\mathbb{K}/\Bbbk)$. We shall now generalize these considerations. Additional complications arise when $\mathbb{K}/\Bbbk$ fails to be separable and normal.[18]

Proposition 9.57. Let $\Bbbk$ be a field, let $\Bbbk(a)$ be an algebraic extension of $\Bbbk$, and suppose that the minimal polynomial $F(X)$ of a over $\Bbbk$ is separable. Let $\mathbb{K}$ be a splitting field of $F(X)$, and factor $F(X)$ over $\mathbb{K}$ as

$$F(X) = (X - a_1)(X - a_2)\cdots(X - a_n)$$

with all $a_j \in \mathbb{K}$ and with $a_1 = a$. Then the matrix of the multiplication operator $M(a)_{\Bbbk(a)/\Bbbk}$ of a on $\Bbbk(a)$ is similar over $\mathbb{K}$ to a diagonal matrix with diagonal entries $a_1, \dots, a_n$. Consequently

$$N_{\Bbbk(a)/\Bbbk}(a) = \prod_{j=1}^{n} a_j \qquad \text{and} \qquad \text{Tr}_{\Bbbk(a)/\Bbbk}(a) = \sum_{j=1}^{n} a_j.$$

[18] The above argument used a matrix with entries in $\Bbbk$ and considered the entries as in the larger field $\mathbb{K}$. The reader may wonder what the corresponding construction is for the $\Bbbk$ linear map $M(a)$. It is *not* to treat $M(a)$ as a $\mathbb{K}$ linear map on $\mathbb{K}$, since then $M(a)$ would have just the one eigenvalue $\sqrt{2}$, which would have multiplicity 1. Instead, it is to use tensor products as in Chapter VI, knowledge of which is not being assumed at present. The idea is to extend scalars, replacing $\mathbb{K}$ by $\mathbb{K} \otimes_{\Bbbk} \mathbb{K}$ and replacing $M(a)$ by $M(a) \otimes 1$. The $\mathbb{K}$ linearity occurs in the second member of the tensor product, not the first, and the operator $M(a) \otimes 1$ is the $\mathbb{K}$ linear map with eigenvalues $\pm\sqrt{2}$.

REMARKS. The elements $a_1, \dots, a_n$ of $\mathbb{K}$, with $a_1 = a$, are called the **conjugates** of a over $\Bbbk$. The conjugates of a are the images of a under the Galois group when $\Bbbk(a)$ is Galois over $\Bbbk$, but they extend outside $\Bbbk$ when $\Bbbk(a)/\Bbbk$ is not normal.

PROOF. Corollary 9.56 shows that $F(X)$ equals the field polynomial of a relative to $\Bbbk(a)/\Bbbk$, i.e., is the characteristic polynomial of the multiplication operator $M_{\Bbbk(a)/\Bbbk}(a)$. Let A be the matrix of $M_{\Bbbk(a)/\Bbbk}(a)$ in some ordered basis of $\Bbbk(a)$ over $\Bbbk$. If we regard A as a matrix with entries in $\mathbb{K}$, then the characteristic polynomial of A splits in $\mathbb{K}$, and the roots of the characteristic polynomial have multiplicity 1, by separability. Consequently A has a basis of eigenvectors, the eigenvectors being column vectors with entries in $\mathbb{K}$ and the eigenvalues being the members $a_1, \dots, a_n$ of $\mathbb{K}$. It follows that A is similar over $\mathbb{K}$ to a diagonal matrix with diagonal entries $a_1, \dots, a_n$. The determinant and trace of this diagonal matrix equal the determinant and trace of A, and therefore the norm and trace of a are the product and sum of the members $a_1, \dots, a_n$ of $\mathbb{K}$. □

Corollary 9.58. Let $\mathbb{K}$ be a finite Galois extension of the field $\Bbbk$, let $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$, let $\mathbb{L}$ be an intermediate field with $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, and let $H = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$ as a subgroup of G. Fix an ordered basis Γ of $\mathbb{L}$ over $\Bbbk$. Then the expression "$\sigma(a)$ for $\sigma \in G/H$" is well defined for a in $\mathbb{L}$, and there exists a nonsingular matrix C of size $[\mathbb{L} : \Bbbk]$ with entries in $\mathbb{K}$ such that every a in $\mathbb{L}$ has $C^{-1}\left(\begin{smallmatrix} M_{\mathbb{L}/\Bbbk}(a) \\ \Gamma\Gamma \end{smallmatrix}\right)C$ diagonal with diagonal entries $\sigma(a)$ for $\sigma \in G/H$. In particular, every member a of $\mathbb{L}$ has norm and trace given by

$$N_{\mathbb{L}/\Bbbk}(a) = \prod_{\sigma \in G/H} \sigma(a) \qquad \text{and} \qquad \mathrm{Tr}_{\mathbb{L}/\Bbbk}(a) = \sum_{\sigma \in G/H} \sigma(a).$$

PROOF. Let a be in $\mathbb{L}$, σ be in G, and τ be in H. Then $\tau(a) = a$, and therefore $\sigma\tau(a) = \sigma(a)$. Consequently all members of the coset σH of G/H have the same value on a, and "$\sigma(a)$ for $\sigma \in G/H$" is well defined.

Let $n = [\mathbb{L} : \Bbbk] = |G/H|$. Fix an ordered basis Γ of $\mathbb{L}$ over $\Bbbk$. For each $a \in \mathbb{L}$, let $A(a)$ be the matrix of the multiplication operator $M(a)_{\mathbb{L}/\Bbbk}$ relative to Γ.

The Theorem of the Primitive Element (Theorem 9.34) shows that $\mathbb{L} = \Bbbk(x)$ for some x. Proposition 9.57 applies to this element x and to a splitting field within $\mathbb{K}$ for its minimal polynomial, showing that there is a nonsingular matrix C with entries in $\mathbb{K}$ such that $C^{-1}A(x)C$ is a diagonal matrix whose diagonal entries are the n conjugates $x_1, \dots, x_n$ of x in $\mathbb{K}$, x_1 being x; the diagonal entries are necessarily distinct by separability. For each i with $1 \le i \le n$, there exists σ_i in G with $\sigma_i(x) = x_i$ by Theorems 9.11 and 9.23. Since H fixes $\mathbb{L}$, every member of the coset $\sigma_i H$ carries x to x_i. On the other hand, every σ in G must carry x to some conjugate, hence must have $\sigma(x) = \sigma_i(x)$ for some i. Then $\sigma_i^{-1}\sigma$ fixes x

and hence $\mathbb{L}$, and it follows that $\sigma_i^{-1}\sigma$ is in H. Thus σ is in $\sigma_i H$. In other words, the conjugates $x_1, \dots, x_n$ may be regarded exactly as the images of the n cosets $\sigma_j H$.

In this terminology the diagonal entries of $C^{-1}A(x)C$ are the n elements $\sigma(x)$ for σ in G/H. For each j with $0 \le j \le n-1$, we have $A(x^j) = A(x)^j$, and hence $C^{-1}A(x^j)C = C^{-1}A(x)^jC$ is diagonal with diagonal entries $\sigma(x)^j = \sigma(x^j)$ for σ in G/H. Forming $\Bbbk$ linear combinations, we see for every polynomial $P(X)$ in $\Bbbk[X]$ of degree $\le n-1$ that $C^{-1}A(P(x))C$ is diagonal with diagonal entries $\sigma(P(x))$. Every element a of $\mathbb{K}$ is of the form $P(x)$ for some such $P(X)$, and the existence of C in the statement of the corollary is proved. The formulas for the norm and trace follow by taking the determinant and trace. □

Corollary 9.59. If $\mathbb{K}$ is a finite separable extension of the field $\Bbbk$, then the trace function $\mathrm{Tr}_{\mathbb{K}/\Bbbk}$ is not identically 0.

REMARKS. This result is trivial in characteristic 0 because $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(1) = [\mathbb{K} : \Bbbk]$ is not zero. The result is not so evident in characteristic p, and the assumption of separability is crucial. An example for which separability fails and the trace function is identically 0 has $\Bbbk = \mathbb{F}(x)$, where $\mathbb{F}$ is a finite field of characteristic p and x is transcendental, and $\mathbb{K} = \Bbbk(x^{1/p})$. The basis elements $1, x^{1/p}, x^{2/p}, \dots, x^{(p-1)/p}$ all have trace 0, and therefore the trace is identically 0.

PROOF. By the Theorem of the Primitive Element (Theorem 9.34), we can write $\mathbb{K} = \Bbbk(a)$ for some $a \ne 0$. Let $\mathbb{K}'$ be a splitting field for the minimal polynomial of a over $\Bbbk$. Then $\mathbb{K}'/\Bbbk$ is a separable extension by Corollary 9.30 and hence is a finite Galois extension. Proposition 9.57 shows that the matrix of $M_{\mathbb{K}/\Bbbk}(a)$ in any ordered basis of $\mathbb{K}$ over $\Bbbk$ is similar over $\mathbb{K}'$ to a diagonal matrix with entries $a_1, \dots, a_n$, where $a_1, \dots, a_n$ are the conjugates of a with $a_1 = a$. These conjugates are necessarily distinct by separability. For $1 \le k \le n$, the matrix of $M_{\mathbb{K}/\Bbbk}(a^k)$ is similar via the same matrix over $\mathbb{K}'$ to a diagonal matrix with entries $a_1^k, \dots, a_n^k$. If $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a^k) = 0$ for $1 \le k \le n$, then we obtain the homogeneous system of linear equations

$$\begin{aligned} a_1x_1 + a_2x_2 + \cdots + a_nx_n &= 0, \\ a_1^2x_1 + a_2^2x_2 + \cdots + a_n^2x_n &= 0, \\ &\vdots \\ a_1^nx_1 + a_2^nx_2 + \cdots + a_n^nx_n &= 0, \end{aligned}$$

with $(x_1, \dots, x_n) = (1, \dots, 1)$ as a nonzero solution. The coefficient matrix must therefore have determinant 0. This coefficient matrix, however, is a Vandermonde matrix except that the j^{th} column is multiplied by a_j for each j. Since $a_1, \dots, a_n$

are distinct, Corollary 5.3 shows that the determinant of the coefficient matrix can be 0 only if $a_1a_2\cdots a_n = 0$. Since $a \neq 0$, we have arrived at a contradiction, and we conclude that $\mathrm{Tr}_{\mathbb{K}/\Bbbk}(a^k) \neq 0$ for some k. □

With the aid of Corollary 9.59, we can complete the proof of Theorem 8.54 in Section VIII.11. Let us restate the part that still needs proof.

THEOREM 8.54. If R is a Dedekind domain with field of fractions F and if K is a finite separable extension field of F, then the integral closure T of R in K is finitely generated as an R module and consequently is a Dedekind domain.

REMARKS. What needs proof is that T is finitely generated as an R module. It was shown in Section VIII.11 how to deduce as a consequence that T is a Dedekind domain.

PROOF. Since R is Noetherian (being a Dedekind domain), Proposition 8.34 shows that it is enough to exhibit T as an R submodule of a finitely generated R module in K. Let $\{u_1, \dots, u_n\}$ be a vector-space basis of K over F. Proposition 8.42 shows that we may assume that each u_i is in T.

Define an F linear map from K into its F vector-space dual K' by $y \mapsto \ell_y$, where $\ell_y(x) = \mathrm{Tr}_{K/F}(xy)$ for $x \in K$. This map is one-one by Corollary 9.59, and the equality of dimensions of K and K' over F therefore implies that the map is onto. We can thus view every member of K' as uniquely of the form ℓ_y for some y in K. With this understanding, let $\{\ell_{v_1}, \dots, \ell_{v_n}\}$ be the dual basis of K' with $\ell_{v_j}(u_i) = \delta_{ij}$ for all i and j. Then we have

$$\mathrm{Tr}_{K/F}(u_iv_j) = \delta_{ij} \qquad \text{for all } i \text{ and } j.$$

Applying Proposition 8.42, choose $c \neq 0$ in R with cv_j in T for all j. We shall complete the proof by showing that

$$T \subseteq Rc^{-1}u_1 + \cdots + Rc^{-1}u_n. \tag{$*$}$$

Before doing so, let us observe that

$$\mathrm{Tr}_{K/F}(t) \quad \text{is in } R \text{ if } t \text{ is in } T. \tag{$**$}$$

In fact, Proposition 9.57 shows that $\mathrm{Tr}_{F(t)/F}(t)$ is the sum of all the conjugates of t, whether or not they are in K. The conjugates have the same minimal polynomial over F that t has, and hence they are integral over R. Their sum $\mathrm{Tr}_{F(t)/F}(t)$ must be integral over R by Corollary 8.38, and it must lie in F. Since R is integrally closed (being a Dedekind domain), $\mathrm{Tr}_{F(t)/F}(t)$ lies in R. This proves $(**)$.

Now we can return to the proof of $(*)$. Let x be given in T. Since T is a ring, cxv_j is in T for each j, and $\mathrm{Tr}_{K/F}(cxv_j)$ is in R by $(**)$. Since $\{u_1, \dots, u_n\}$ is a basis, we can write $x = \sum_i d_i u_i$ with each d_i in F. Since $\mathrm{Tr}(cxv_j)$ is in R, the computation

$$\mathrm{Tr}(cxv_j) = c\,\mathrm{Tr}_{K/F}(xv_j) = c\sum_{i=1}^{n} d_i\,\mathrm{Tr}(u_i v_j) = cd_j$$

shows that cd_j is in R. Then the expansion $x = \sum_i (cd_i)c^{-1}u_i$ exhibits x as in $Rc^{-1}u_1 + \cdots + Rc^{-1}u_n$ and completes the proof of $(*)$. □

16. Splitting of Prime Ideals in Extensions

Section VIII.7 was a section of motivation showing the importance for number theory and geometry of passing from factorization of elements to factorization of ideals. The later sections of Chapter VIII set the framework for this study, examining the notions of Noetherian domain, integral closure, and localization and putting them together in the notion of Dedekind domain. Only just now were we able to complete the proof of the fundamental result (Theorem 8.54) for constructing Dedekind domains out of other Dedekind domains. However, that proposition does not complete the task of extending what is in Section VIII.7 to a wider context. Much of Section VIII.7 concerned the relationship between prime ideals in one domain and prime ideals in an extension. In the present section we put that relationship in a wider context, showing how the examples of Section VIII.7 are special cases of the present theory.

In two of the examples in Section VIII.7, we worked with the ring $\mathbb{Z}$ of integers inside its field of fractions $\mathbb{Q}$ and with the ring T of algebraic integers within a quadratic extension $\mathbb{K}$ of $\mathbb{Q}$. In the third example in that section, we worked with the ring $\mathbb{C}[x]$, for transcendental x, inside its field of fractions $\mathbb{C}(x)$ and with a certain integral domain T within a quadratic extension of $\mathbb{C}(x)$. For all three examples we saw a correspondence between prime ideals P in T and prime ideals (p) in $\mathbb{Z}$ or $\mathbb{C}[x]$, and that correspondence was formalized in a more general setting in Propositions 8.43 and 8.53. The objective now is to understand that correspondence a little better.

The notation for this section is as follows: Let R be a Dedekind domain, such as $\mathbb{Z}$ or $\mathbb{C}[x]$, and let F be its field of fractions.[19] Let K be a finite separable extension of F, and let T be the integral closure of R in K. Theorem 8.54, including the part just proved in the previous section, shows that T is a Dedekind domain. We make repeated use of the fact about Dedekind domains that every nonzero prime ideal is maximal.

[19] It might seem more natural to assume that R is a principal ideal domain, as it is with $\mathbb{Z}$ and $\mathbb{C}[x]$. But that extra assumption will not help us, and it will often not be satisfied when the present results are used in the proof of the important Theorem 9.64 in the next section.

Proposition 8.43 shows that if P is any nonzero prime ideal of T, then $\mathfrak{p} = R \cap P$ is a nonzero prime ideal of R. In the reverse direction Proposition 8.53 shows that if $\mathfrak{p}$ is any nonzero prime ideal in R, then $\mathfrak{p}T \neq T$, and there exists at least one prime ideal P of T with $\mathfrak{p} = R \cap P$. The unique factorization of ideals in T (given as Theorem 8.55) explains this correspondence better. If $\mathfrak{p}$ is given, then $\mathfrak{p}T$ is a proper ideal, hence is contained in some maximal ideal P. Since "to contain is to divide" (by Theorem 8.55d), such P's (and only such P's) are factors in the decomposition of $\mathfrak{p}T$ as the product of nonzero prime ideals. Accordingly let us write

$$\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i},$$

where the P_i are the distinct prime ideals of T containing $\mathfrak{p}T$, or equivalently the distinct prime ideals of T satisfying $R \cap P_i = \mathfrak{p}$. The e_i are positive integers called the **ramification indices**.

For each P_i, we can form the composition $R \subseteq T \to T/P_i$ of inclusion followed by passage to the quotient. Since $\mathfrak{p} \subseteq P_i$, this composition descends to a ring homomorphism $R/\mathfrak{p} \to T/P_i$. The ideal $\mathfrak{p}$ is maximal in R, and the ideal P_i is maximal in T. Thus the mapping $R/\mathfrak{p} \to T/P_i$ is in fact a field map. We regard it as an inclusion. Define

$$f_i = [T/P_i : R/\mathfrak{p}],$$

allowing the dimension for the moment possibly to be $+\infty$. It will follow from Theorem 9.60, however, that f_i is finite. The integer f_i is called the **residue class degree**.

Theorem 9.60. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, then the ramification indices e_i and residue class degrees $f_i = [T/P_i : R/\mathfrak{p}]$ are related by

$$\sum_{i=1}^{g} e_i f_i = n.$$

REMARKS. Consequently each f_i is finite. The cases of interest for our earlier examples have $R = \mathbb{Z}$ or $R = \mathbb{C}[x]$. When $R = \mathbb{Z}$, each $R/\mathfrak{p}$ is a finite field. However, when $R = \mathbb{K}[x]$ for some field $\mathbb{K}$ of characteristic 0 like $\mathbb{K} = \mathbb{C}$, then each $R/\mathfrak{p}$ is a finite extension of $\mathbb{K}$, hence is an infinite field.[20]

[20] When $R = \mathbb{C}[x]$, then $T/P_i = R/\mathfrak{p} \cong \mathbb{C}$ since $\mathbb{C}$ is algebraically closed. The last example of the present section will elaborate.

PROOF. Corollary 8.63 gives a ring isomorphism

$$T/(\mathfrak{p}T) \cong T/P_1^{e_1} \times \cdots \times T/P_g^{e_g}. \qquad (*)$$

Recall from the definition of residue class degree that we have a field mapping of $R/\mathfrak{p}$ into each T/P_i. Since $\mathfrak{p} \subseteq P_i^e$ for $1 \leq e \leq e_i$ and since $\mathfrak{p} \subseteq \mathfrak{p}T$, it follows similarly that we have a one-one ring homomorphism of $R/\mathfrak{p}$ into each T/P_i^e with $1 \leq e \leq e_i$ and another one-one ring homomorphism of $R/\mathfrak{p}$ into $T/(\mathfrak{p}T)$. Consequently each T/P_i^e with $1 \leq e \leq e_i$, the product $T/P_1^{e_1} \times \cdots \times T/P_g^{e_g}$, and $T/(\mathfrak{p}T)$ may all be regarded as unital $R/\mathfrak{p}$ modules, i.e., as vector spaces over the field $R/\mathfrak{p}$. Fix i. For $1 \leq e \leq e_i$, let us prove by induction on e that

$$\dim_{R/\mathfrak{p}}(T/P_i^e) = ef_i, \qquad (**)$$

the case $e = 1$ being the base case of the induction. Assume inductively that $(**)$ holds for exponents from 1 to $e-1$. We know from Corollary 8.60 that P_i^{e-1}/P_i^e is a vector space over the field T/P_i with

$$\dim_{T/P_i}(P_i^{e-1}/P_i^e) = 1. \qquad (\dagger)$$

The First Isomorphism Theorem (as in the remark with Theorem 8.3) gives $T/P_i^{e-1} \cong (T/P_i^e)\big/(P_i^{e-1}/P_i^e)$ as vector spaces over $R/\mathfrak{p}$, and it follows that

$$\begin{aligned}\dim_{R/\mathfrak{p}}(T/P_i^e) &= \dim_{R/\mathfrak{p}}(T/P_i^{e-1}) + \dim_{R/\mathfrak{p}}(P_i^{e-1}/P_i^e)\\ &= (e-1)f_i + f_i = ef_i,\end{aligned}$$

the next-to-last equality following from $(\dagger)$ and the inductive hypothesis for the cases $e-1$ and 1. This completes the induction and the proof of $(**)$.

In view of the decomposition $(*)$ and the formula $(**)$ when $e = e_i$, the theorem will follow if it is shown that

$$\dim_{R/\mathfrak{p}}(T/(\mathfrak{p}T)) = n. \qquad (\dagger\dagger)$$

To prove $(\dagger\dagger)$ we localize. Let S be the complement of the prime ideal $\mathfrak{p}$ of R. Corollary 8.48 shows that $S^{-1}R$ is a Dedekind domain, Corollary 8.50 shows that $S^{-1}\mathfrak{p}$ is its unique maximal ideal, and Corollary 8.62 shows that $S^{-1}R$ is a principal ideal domain.

The composition $R \subseteq S^{-1}R \to S^{-1}R/S^{-1}\mathfrak{p}$ descends to a field mapping $R/\mathfrak{p} \to S^{-1}R/S^{-1}\mathfrak{p}$. Let us see that this mapping is onto. If $s_0^{-1}r_0 + S^{-1}\mathfrak{p}$ in $S^{-1}R/S^{-1}\mathfrak{p}$ is given, then s_0 is not in $\mathfrak{p}$, and the maximality of $\mathfrak{p}$ as an ideal in R implies that $(s_0) + \mathfrak{p} = R$. Therefore we can choose r in R and x in $\mathfrak{p}$ with $rs_0 + x = r_0$. Under the mapping $R/\mathfrak{p} \to S^{-1}R/S^{-1}\mathfrak{p}$, the image of $r + \mathfrak{p}$ is

$r + S^{-1}\mathfrak{p} = r + s_0^{-1}x + S^{-1}\mathfrak{p} = s_0^{-1}(rs_0 + x) + S^{-1}\mathfrak{p} = s_0^{-1}r_0 + S^{-1}\mathfrak{p}$. Thus our mapping is onto $S^{-1}R/S^{-1}\mathfrak{p}$, and we have an isomorphism of fields

$$R/\mathfrak{p} \cong S^{-1}R/S^{-1}\mathfrak{p}. \tag{‡}$$

Similarly the composition $T \subseteq S^{-1}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$ descends to a homomorphism of rings $T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$. Let us show that this map too is one-one onto.

If $t + \mathfrak{p}T$ is in the kernel, then the member t of T is in $S^{-1}\mathfrak{p}T$, and st is in $\mathfrak{p}T$ for some s in S. Hence we have $(s)(t) \subseteq P_1^{e_1} \cdots P_g^{e_g}$, and we can write $(s)(t) = P_1^{e_1} \cdots P_g^{e_g} Q$ for some ideal Q. Factoring the principal ideals (s) and (t) and using the uniqueness of factorization of ideals gives

$$(s) = P_1^{u_1} \cdots P_g^{u_g} Q_1 \qquad \text{and} \qquad (t) = P_1^{v_1} \cdots P_g^{v_g} Q_2$$

with $Q = Q_1 Q_2$ and with $u_j + v_j = e_j$ for all j. If $u_j > 0$, then we must have $(s) \subseteq P_j$ and $sR \subseteq P_j \cap R = \mathfrak{p}$. This says that s is in $\mathfrak{p}$, in contradiction to the fact that S equals the set-theoretic complement of $\mathfrak{p}$ in R. We conclude that $u_j = 0$ for all j. Therefore $(t) = P_1^{e_1} \cdots P_g^{e_g} Q_2 \subseteq P_1^{e_1} \cdots P_g^{e_g} = \mathfrak{p}T$, and t is in $\mathfrak{p}T$. Consequently the kernel consists of the 0 coset alone.

Let us show that $T/\mathfrak{p}T$ maps onto $S^{-1}T/(S^{-1}\mathfrak{p}T)$. If $s_0^{-1}t_0 + S^{-1}\mathfrak{p}T$ in $S^{-1}T/S^{-1}\mathfrak{p}T$ is given, then s_0 is not in $\mathfrak{p}$, and the maximality of $\mathfrak{p}$ as an ideal in R implies that $(s_0) + \mathfrak{p} = R$. Therefore we can choose r in R and x in $\mathfrak{p}$ with $rs_0 + x = 1$, hence with $rs_0t_0 + xt_0 = t_0$. Under the mapping $T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T)$, the image of $rt_0 + \mathfrak{p}T$ is

$$\begin{aligned} rt_0 + S^{-1}\mathfrak{p}T &= rt_0 + s_0^{-1}xt_0 + S^{-1}\mathfrak{p}T \\ &= s_0^{-1}(rs_0t_0 + xt_0) + S^{-1}\mathfrak{p}T \\ &= s_0^{-1}t_0 + S^{-1}\mathfrak{p}T. \end{aligned}$$

Thus our mapping is onto $S^{-1}T/S^{-1}\mathfrak{p}T$, and we conclude that we have an isomorphism of rings

$$T/\mathfrak{p}T \to S^{-1}T/(S^{-1}\mathfrak{p}T). \tag{‡‡}$$

Since T is finitely generated as an R module (Theorem 8.54), $S^{-1}T$ is finitely generated as an $S^{-1}R$ module with the same generators. Since $S^{-1}R$ is a principal ideal domain, Theorem 8.25c shows that $S^{-1}T$ is the direct sum of cyclic $S^{-1}R$ modules. Each of these cyclic modules must in fact be isomorphic to $S^{-1}R$ since $S^{-1}T$ has no zero divisors, and therefore $S^{-1}T$ is a free $S^{-1}R$ module of some finite rank m. If $t_1, \ldots, t_m$ are free generators, then we have

$$S^{-1}T = S^{-1}Rt_1 + \cdots + S^{-1}Rt_m. \tag{§}$$

Let us see that $\{t_1, \dots, t_m\}$ is an F vector-space basis of K. Suppose $\sum_j c_j t_j = 0$ with all c_j in F. Proposition 8.42 shows that there is an $r \neq 0$ in R with $rc_1, \dots, rc_m$ in R. Then $\sum_j (rc_j)t_j = 0$, and the independence of $t_1, \dots, t_m$ over $S^{-1}R$ implies that $rc_j = 0$ for all j. Thus $c_j = 0$ for all j, and we obtain linear independence over F. If $x \in K$ is given, we can choose $r \neq 0$ in R with rx in T by Proposition 8.42. Since $t_1, \dots, t_m$ span $S^{-1}T$ over $S^{-1}R$, we can find members $d_1, \dots, d_m$ of $S^{-1}R$ with $rx = \sum_j d_j t_j$. Then $x = \sum_j r^{-1} d_j t_j$ with each coefficient $r^{-1}d_j$ in F. This proves the spanning. Hence $\{t_1, \dots, t_m\}$ is an F vector-space basis, and $m = n$.

To complete the proof of (††) and hence the theorem, it is enough, in view of the isomorphisms (‡) and (‡‡), to prove that the cosets $t_j + S^{-1}\mathfrak{p}T$ in $S^{-1}T/(S^{-1}\mathfrak{p}T)$ form a vector-space basis over $S^{-1}R/S^{-1}\mathfrak{p}$. If t is in $S^{-1}T$, then (§) says that $t = \sum c_j t_j$ with c_j in $S^{-1}R$. Hence

$$t + S^{-1}\mathfrak{p}T = \sum (c_j + S^{-1}\mathfrak{p})(t_j + S^{-1}\mathfrak{p}T),$$

and we have spanning. If $\sum_j (c_j + S^{-1}\mathfrak{p})(t_j + S^{-1}\mathfrak{p}T) = 0 + S^{-1}\mathfrak{p}T$, then $\sum_j c_j t_j$ is in $S^{-1}\mathfrak{p}T$. Thus we can write $\sum_j c_j t_j = \sum_i a_i t_i'$ with $a_i \in \mathfrak{p}$ and $t_i' \in S^{-1}T$. Expanding each t_i' according to (§), substituting, and using the uniqueness of the expansion (§), we see for each j that c_j is a sum of products of the a_i's by members of $S^{-1}R$. Therefore each c_j is in $S^{-1}\mathfrak{p}$. This proves the linear independence and establishes (††). □

The case of greatest interest is that K is a finite Galois extension of F. In this case the statement of Theorem 9.60 simplifies and will be given in its simplified form as Theorem 9.62. We begin with a lemma.

Lemma 9.61. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F, and let T be the integral closure of R in K. Suppose that K is Galois over F. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of nonzero prime ideals in T, then $\operatorname{Gal}(K/F)$ is transitive on the set of ideals $\{P_1, \dots, P_g\}$.

PROOF. Arguing by contradiction, suppose that P_j is not of the form $\sigma(P_1)$ for some σ in $\operatorname{Gal}(K/F)$. By the Chinese Remainder Theorem we can choose an element t of T with $t \equiv 0 \bmod P_j$ and $t \equiv 1 \bmod \sigma(P_1)$ for all σ. Every σ in $\operatorname{Gal}(K/F)$ carries t to a member of T since t and $\sigma(t)$ have the same minimal polynomial over F. Corollary 9.58 shows that $N_{K/F}(t) = \prod_{\sigma \in \operatorname{Gal}(K/F)} \sigma(t)$, and consequently $N_{K/F}(t)$ is in $T \cap F = R$. Since the factor t itself is in P_j, $N_{K/F}(t)$ is in P_j. Therefore $N_{K/F}(t)$ is in $R \cap P_j = \mathfrak{p} \subseteq \prod_{i=1}^{g} P_i^{e_i}$. The right side is contained in P_1. Since P_1 is prime, some factor $\sigma_l(t)$ of $N_{K/F}(t)$ is in P_1. Then t is in $\sigma_l^{-1}(P_1)$, in contradiction to the fact that $t \equiv 1 \bmod \sigma(P_1)$ for all σ. □

Theorem 9.62. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that K is Galois over F. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ is a decomposition of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, then the ramification indices have $e_1 = \cdots = e_g$, and the residue class degrees $f_i = [T/P_i : R/\mathfrak{p}]$ have $f_1 = \cdots = f_g$. If e and f denote the common value of the e_i's and of the f_j's, then

$$\boxed{efg = n\,.}$$

PROOF. For σ in $\operatorname{Gal}(K/F)$, apply σ to the factorization $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$, obtaining

$$\mathfrak{p}T = \sigma(P_1)^{e_1} \prod_{i=2}^{g} \sigma(P_i)^{e_i}.$$

Lemma 9.61 shows that $\sigma(P_1)$ can be any P_j, and unique factorization of ideals (Theorem 8.55) therefore implies that $e_1 = e_j$. With the same σ, the fact that σ respects the field operations implies that

$$T/P_1 \cong \sigma(T)/\sigma(P_1) = T/P_j,$$

and thus $f_1 = f_j$. Substituting the values of the e_i's and the f_j's into the formula of Theorem 9.60, we obtain $efg = n$. □

EXAMPLES WITH $n = 2$ CONTINUED FROM SECTION VIII.7.

(1) $R = \mathbb{Z}$ and $T = \mathbb{Z}[\sqrt{-1}\,]$. In this case, $\mathbb{Z}$ and T are both principal ideal domains. We found three possible behaviors[21] for the prime factorization of a principal ideal $(p)T$ in T generated by a prime $p > 0$ in $\mathbb{Z}$:

(a) $(p)T$ is prime in T if $p = 4m + 3$. Here $e = g = 1$; so $f = 2$.

(b) $(p)T = (a + ib)(a - ib)$ with $p = a^2 + b^2$ if $p = 4m + 1$. Here $e = 1$ and $g = 2$; so $f = 1$.

(c) $(2)T = (1 + i)^2$. Here $e = 2$ and $g = 1$; so $f = 1$.

(2) $R = \mathbb{Z}$ and $T = \mathbb{Z}[\sqrt{-5}\,]$. In this case, T is not a unique factorization domain and is in particular not a principal ideal domain. We gave examples of three possible behaviors for the prime factorization of a principal ideal $(p)T$ in T generated by a prime $p > 0$ in $\mathbb{Z}$:

(a) $(11)T$ is prime in T. Here $e = g = 1$; so $f = 2$.

(b) $(2)T = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. Here $e = 1$ and $g = 2$; so $f = 1$.

(c) $(5)T = (\sqrt{-5}\,)^2$. Here $e = 2$ and $g = 1$; so $f = 1$.

[21] The notation here fits with the notation in Theorem 9.62 and is different from the notation in Section VIII.7.

(3) $R = \mathbb{C}[x]$ and $T = \mathbb{C}[x, \sqrt{(x-1)x(x+1)}\,]$. In this case, R is a principal ideal domain, and we saw that T is not a unique factorization domain. We found two possible behaviors for the prime factorization of a principal ideal $(p)T$ in T generated by a prime p in $\mathbb{C}[x]$:

(a) $(x - x_0)T = (x - x_0, y - y_0)(x - x_0, y + y_0)$ if the equal expressions $y_0^2 = (x_0 - 1)x_0(x_0 + 1)$ are not 0. Here $e = 1$ and $g = 2$; so $f = 1$.

(b) $(x - x_0)T = (x - x_0, y)^2$ if x_0 is in $\{-1, 0, +1\}$. Here $e = 2$ and $g = 1$; so $f = 1$.

The third type, with $(x - x_0)T$ prime in T, does not arise. It cannot arise since $f > 1$ would point to a quadratic extension of $\mathbb{C}$, yet $\mathbb{C}$ is algebraically closed.

17. Two Tools for Computing Galois Groups

In Section 8 we mentioned that the effect of the Fundamental Theorem of Galois Theory is to reduce the extremely difficult problem of finding intermediate fields to the less-difficult problem of finding a Galois group. In the intervening sections we have seen some illustrations of the power of this reduction, all in cases in which the Galois group was close at hand.

The problem of finding a Galois group in a particular situation is usually not as easy as in those cases, and it by no means can be considered as solved in general. In this section we combine Galois theory with some of the ring theory in the second half of Chapter VIII in order to develop two tools that sometimes help identify particular Galois groups.

Let us think in terms of a finite Galois extension K of the rationals $\mathbb{Q}$. The field K is the splitting field of some irreducible monic polynomial with rational coefficients, and we can scale this polynomial's indeterminate (in effect by multiplying its roots by some nonzero integer) so that the polynomial is monic and has integer coefficients. Thus let $F(X)$ be a monic irreducible polynomial in $\mathbb{Z}[X]$ of some degree d, and let K be its splitting field over $\mathbb{Q}$. The members of $\text{Gal}(K/\mathbb{Q})$ are determined by their effect on the d roots of $F(X)$, and hence $\text{Gal}(K/\mathbb{Q})$ may be regarded as a subgroup of the symmetric group $\mathfrak{S}_d$. If $r_1, \dots, r_d$ are the roots of $F(X)$, then the **discriminant** of $F(X)$ is the member of K defined by

$$D = \prod_{1 \le i < j \le d} (r_j - r_i)^2.$$

This was defined in Section 13 in the cases $d = 2$ and $d = 3$, and we computed the value of D in those cases. The discriminant is an integer under our hypotheses, and it is computable even though the roots $r_1, \dots, r_d$ of $F(X)$ are not at hand. In fact, the proof of Theorem 9.50 indicates that the discriminant D is given by the determinant

$$D = \det\begin{pmatrix} d & a_1 & a_2 & \cdots & a_{d-1} \\ a_1 & a_2 & a_3 & \cdots & a_d \\ a_2 & a_3 & a_4 & \cdots & a_{d+1} \\ & & & \vdots & \\ a_{d-1} & a_d & a_{d+1} & \cdots & a_{2d-2} \end{pmatrix},$$

where $a_j = r_1^j + r_2^j + \cdots + r_d^j$. Problems 36–39 at the end of Chapter VIII show that each of $a_1, \dots, a_{2d-1}$ can be expressed as a polynomial in the elementary symmetric polynomials in $r_1, \dots, r_d$, i.e., in the coefficients of $F(X)$, and doing so in a symbolic manipulation program is manageable for any fixed degree.[22]

The first of the two tools that sometimes help in identifying particular Galois groups directly concerns the discriminant: the discriminant is a square if and only if the Galois group is a subgroup of the alternating group. Let us state the result in the context of a general finite Galois extension even though we shall use it only for our Galois extension $K/\mathbb{Q}$.

Proposition 9.63. Let $\mathbb{K}/\Bbbk$ be a finite Galois extension, and suppose that $\mathbb{K}$ is the splitting field of a separable polynomial $F(X)$ in $\Bbbk[X]$ of degree d. Let D be the discriminant of $F(X)$, and regard $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$ as a subgroup of the symmetric group $\mathfrak{S}_d$. Then D is in $\Bbbk$, and G is a subgroup of the alternating group $\mathfrak{A}_d$ if and only if D is the square of an element of $\Bbbk$.

REMARK. The proof will use Galois theory to show that D is in $\Bbbk$, and Problems 36–39 at the end of Chapter VIII do not need to be invoked.

PROOF. Let $r_1, \dots, r_d$ be the roots of $F(X)$, and put $\Delta = \prod_{i<j}(r_j - r_i)$. Under the identification of G with a subgroup of the permutation group $\mathfrak{S}_d$ on $\{1, \dots, d\}$, each σ in G has

$$\sigma(\Delta) = \prod_{i<j}(\sigma(r_j) - \sigma(r_i)) = \prod_{i<j}(r_{\sigma(j)} - r_{\sigma(i)}) = (\operatorname{sgn}\sigma)\prod_{i<j}(r_j - r_i) = (\operatorname{sgn}\sigma)\Delta.$$

[22] For example, when $d = 3$, let $F(X) = X^3 - c_1X^2 + c_2X - c_3$. In Mathematica the following program produces a_1, a_2, a_3, a_4 as output:

```
e1={a1==r1+r2+r3, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e1,{r1,r2,r3}]
e2={a2==r1∧2+r2∧2+r3∧2, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e2,{r1,r2,r3}]
e3={a3==r1∧3+r2∧3+r3∧3, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e3,{r1,r2,r3}]
e4={a4==r1∧4+r2∧4+r3∧4, r1+r2+r3==c1, r1 r2+r2 r3+r1 r3==c2,
    r1 r2 r3==c3}
Eliminate[e4,{r1,r2,r3}]
```

In particular, the element $D = \Delta^2$ has $\sigma(D) = D$. By Proposition 9.35d, D is in $\Bbbk$.

If some σ in G has $\operatorname{sgn}\sigma = -1$, then σ does not fix Δ, and Δ is not in $\Bbbk$. Since Δ is a square root of D and since any two square roots of an element in a field differ at most by a sign, D is not the square of any element of $\Bbbk$.

Conversely if every σ in G has $\operatorname{sgn}\sigma = +1$, then every σ fixes Δ, and Proposition 9.35d shows that Δ is in $\Bbbk$. Since $D = \Delta^2$, D is the square of the member Δ of $\Bbbk$. □

The second tool is complicated to prove but simple to state. We reduce the polynomial $F(X)$ modulo p for each prime number p and form the associated finite splitting field. The Galois group for a finite extension of finite fields is cyclic by Proposition 9.40, and we thus obtain a cyclic subgroup of $\mathfrak{S}_d$. The second tool is this: if p does not divide the discriminant of $F(X)$, then this cyclic group as a permutation group is a subgroup of $\operatorname{Gal}(K/\mathbb{Q})$ as a permutation group, up to a relabeling of the symbols. In other words, the order *and cycle structure* of a generator of the cyclic group are the same as the order and cycle structure of some element of $\operatorname{Gal}(K/\mathbb{Q})$.

Let us formulate the result precisely. In the setting of Theorem 9.62, fix a prime ideal P of T lying in the factorization of $\mathfrak{p}T$. Each member σ of $G = \operatorname{Gal}(K/F)$ carries T to itself, but not every σ in G carries P to itself. Let G_P be the isotropy subgroup of G at P, i.e., let $G_P = \{\sigma \in G \mid \sigma(P) = P\}$. The subgroup G_P is called the **decomposition group** at P. Each σ in G_P descends to an automorphism of the field T/P that fixes the subfield $R/\mathfrak{p}$, since σ fixes each element of R. Thus σ defines a member $\overline{\sigma}$ of $\overline{G} = \operatorname{Gal}((T/P)/(R/\mathfrak{p}))$ by the formula

$$\overline{\sigma}(\bar{x}) = \overline{\sigma(x)}, \qquad \text{where } \bar{y} = y + P \text{ for } y \in T.$$

It is apparent that $\sigma \mapsto \overline{\sigma}$ is a homomorphism of G into $\overline{G}$. This homomorphism turns out to yield the result stated informally in the previous paragraph. It has the key property given in Theorem 9.64.

Theorem 9.64. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F with $[K : F] = n$, and let T be the integral closure of R in K. Suppose that K is Galois over F. Let $\mathfrak{p}$ be a nonzero prime ideal in R, let $P = P_1$ be a prime factor in a decomposition $\mathfrak{p}T = \prod_{i=1}^{g} P_i^{e_i}$ of $\mathfrak{p}T$ as the product of powers of distinct nonzero prime ideals in T, and suppose that T/P is a Galois extension of $R/\mathfrak{p}$. Let $G = \operatorname{Gal}(K/F)$, $G_P = \{\sigma \in G \mid \sigma(P) = P\}$, and $\overline{G} = \operatorname{Gal}((T/P)/(R/\mathfrak{p}))$. Then the group homomorphism $\sigma \mapsto \overline{\sigma}$ of G_P into $\overline{G}$ carries G_P onto $\overline{G}$.

REMARKS. In our application with $R = \mathbb{Z}$, T/P and $R/\mathfrak{p}$ are finite fields, and Proposition 9.40 shows that T/P is a Galois extension of $R/\mathfrak{p}$ with no further assumptions.

PROOF. Let K^d be the fixed field of G_P within K; Theorem 9.38 shows that $\operatorname{Gal}(K/K^d) = G_P$. Let T^d be the integral closure of R in K^d; this is a Dedekind domain, and T is the integral closure of T^d in K. We are going to apply Theorem 9.62 with R in the theorem replaced[23] by T^d.

Proposition 8.43 shows that $\mathcal{P} = T^d \cap P$ is a nonzero prime ideal of T^d. Since every member of G_P carries P to itself and since G_P is the full Galois group of K over K^d, Lemma 9.61 shows that P is the only nonzero prime ideal of T whose intersection with T^d is $\mathcal{P}$. Therefore $\mathcal{P}T^d = P^{e'}$ for some integer $e' \geq 1$.

As always, we have a field mapping $R/\mathfrak{p} \to T^d/\mathcal{P}$. Let us show that this mapping is onto $T^d/\mathcal{P}$. For any given u in T^d, we are to produce r in R with

$$r \equiv u \bmod \mathcal{P}. \tag{$*$}$$

Each σ in G that is not in G_P has $\sigma^{-1}P \neq P$, and the previous paragraph shows that the nonzero prime ideal $\mathcal{P}_\sigma = T^d \cap \sigma^{-1}P$ of T^d has $\mathcal{P}_\sigma \neq T^d \cap P$. Therefore $\mathcal{P}_\sigma + \mathcal{P} = T^d$, and the Chinese Remainder Theorem (Theorem 8.27) shows that we can find an element v of T^d with

$$v \equiv u \bmod \mathcal{P} \qquad \text{and} \qquad v \equiv 1 \bmod \mathcal{P}_\sigma$$

for all σ that lie in G but not G_P. The first congruence implies that $v - u$ is in $\mathcal{P} = T^d \cap P \subseteq P$, hence that

$$v \equiv u \bmod P, \tag{$**$}$$

while the second congruence implies that $v - 1$ is in $\mathcal{P}_\sigma = T^d \cap \sigma^{-1}P \subseteq \sigma^{-1}P$, hence that $\sigma(v-1)$ lies in P. Therefore

$$\sigma(v) \equiv 1 \bmod P \qquad \text{for all } \sigma \text{ in } G \text{ but not } G_P. \tag{$\dagger$}$$

Put $r = N_{K^d/F}(v)$. Since the splitting field of the minimal polynomial of v over F is contained in K, Corollary 9.58 shows that r is the product of the elements $\sigma(v)$ for σ in G/G_P. Each of these is in T, and hence $N_{K^d/F}(v)$ is in T. Since $N_{K^d/F}(v)$ is also in F, $r = N_{K^d/F}(v)$ is in $T \cap F = R$. If we use $\sigma = 1$ as the representative of the identity coset of G/G_P, then we have

$$r = N_{K^d/F}(v) = v\Big(\prod_{\substack{\text{some } \sigma\text{'s} \\ \text{not in } G_P}} \sigma(v)\Big).$$

[23] Consequently it would not have been sufficient to prove Theorem 9.62 when the ring R is a principal ideal domain.

The factor of v is congruent to u mod P by $(**)$, and each factor in parentheses is congruent to 1 mod P by (†). Therefore $r \equiv u$ mod P, and $r - u$ is in P. Since $r - u$ is in T^d, $r - u$ is in $T^d \cap P = \mathcal{P}$. This proves $(*)$. Consequently we can identify $\overline{G} = \mathrm{Gal}((T/P)/(R/\mathfrak{p}))$ with $\mathrm{Gal}((T/P)/(T^d/\mathcal{P}))$.

Choose $\bar{x}_1$ in T/P with $T/P = (T^d/\mathcal{P})[\bar{x}_1]$; this choice is possible by the assumed separability of $(T/P)/(R/\mathfrak{p})$. Let x_1 be a member of T with $\bar{x}_1 = x_1 + P$, and let $M(X)$ be the minimal polynomial of x_1 over K^d. Since x_1 is in T, the coefficients of $M(X)$ are in T^d. Let $\overline{M}(X)$ be the corresponding member of $(T^d/\mathcal{P})[X]$, given by the substitution homomorphism that takes T^d to $T^d/\mathcal{P}$ and takes X to X. Since K/K^d is normal, $M(X)$ splits over K. Write $x_1, \dots, x_n$ for its roots; these are in T.

Let τ be given in $\overline{G}$, and suppose that $\tau(\bar{x}_1) = \bar{x}_j$. Since $M(X)$ is irreducible over K^d, the Galois group $\mathrm{Gal}(K/K^d) = G_P$ is transitive on its roots. Choose σ in G_P with $\sigma(x_1) = x_j$. Then $\overline{\sigma}(\bar{x}_1) = \bar{x}_j$. Since $\overline{\sigma}$ and τ agree on the generator $\bar{x}_1$ of T/P over $T^d/\mathcal{P}$, they agree on T/P. Therefore τ is exhibited as the image of σ under the homomorphism of the theorem, and the proof is complete. □

A first consequence of Theorem 9.64 is that we get interpretations of the integers e, f, and g, and they will be helpful to us. Galois theory gives us $|G| = n$, and Theorem 9.62 says that $efg = n$. The transitivity in Lemma 9.61 says that G acts transitively on the set $\{P_1, \dots, P_g\}$, and the isotropy subgroup at $P = P_1$ is G_P. Hence $g|G_P| = |G|$, and $|G_P| = n/g = ef$. Galois theory gives us $|\overline{G}| = f$, and the fact that G_P maps onto $\overline{G}$ says that $G_P/\text{kernel} \cong \overline{G}$; therefore $|\text{kernel}| = |G_P|/|\overline{G}| = (ef)/f = e$. We conclude that g is the number of cosets modulo G_P, e is the order of the kernel of the homomorphism in Theorem 9.64, and f is the order of the cyclic group $\overline{G}$.

In the setting of interest for current purposes, we are taking $R = \mathbb{Z}$, $F = \mathbb{Q}$, and K equal to the splitting field of a given monic irreducible polynomial $F(X)$ of degree d in $\mathbb{Z}[X]$. We will be using Theorem 9.64 for various choices of $\mathfrak{p} = (p)$ in $\mathbb{Z}$ to make progress on identifying $\mathrm{Gal}(K/\mathbb{Q})$. In order to identify $\overline{G}$ with the subgroup G_P of G, we need the kernel of the homomorphism of G_P onto $\overline{G}$ to be trivial. From the previous paragraph we know that the condition in question is that $e = 1$. We postpone to Chapter V of *Advanced Algebra* any justification of the assertion that $e = 1$ if p does not divide the discriminant of $F(X)$.

In previous sections we have identified $\mathrm{Gal}(K/\mathbb{Q})$ in some cases when the Galois group is relatively small compared with the degree d of the polynomial. The method now is helpful when the Galois group is relatively large compared with d.

Let us be sure when $e = 1$ that the theorem is telling us not only that G_P is isomorphic to $\overline{G}$ as an abstract group, but also that the cycle structure of the elements of $\overline{G}$ is the same as the cycle structure of the elements of G_P. For this purpose we ignore the proof of the theorem and concentrate only on the statement. Assuming that p does not divide the discriminant, let $\overline{F}(X)$ be the reduction of $F(X)$ modulo p, let $r_1, \dots, r_d$ be the roots of $F(X)$ in T, and let $\bar{r}_1, \dots, \bar{r}_d$ be the images of $r_1, \dots, r_d$ under the quotient homomorphism $T \to T/P$. The elements $\bar{r}_1, \dots, \bar{r}_d$ are distinct since p does not divide the discriminant of $F(X)$. Any member σ of $G = \mathrm{Gal}(K/\mathbb{Q})$ permutes $r_1, \dots, r_d$ and is determined by the resulting permutation since K is assumed to be generated by $r_1, \dots, r_d$. Under the assumption that σ is in G_P, σ descends to an automorphism $\overline{\sigma}$ of T/P. This automorphism $\overline{\sigma}$ acts on the set of elements $\bar{r}_1, \dots, \bar{r}_d$, permuting them. Since the mapping of the r_j's to the $\bar{r}_j$'s is one-one, the resulting permutation of the subscripts $1, \dots, d$ is the same.

When p varies, we cannot match the elements $\bar{r}_1, \dots, \bar{r}_d$ for one value of p with those for another value of p, because we have no direct knowledge of $r_1, \dots, r_d$. Thus we cannot directly compare the permutation groups $\overline{G}$ that we obtain for different p's. But at least we know their cycle structure.

To apply the theory, we factor $\overline{F}(X)$ quickly with a symbolic manipulation program, and we obtain the Galois group of a splitting field of $\overline{F}(X)$ by inspection, together with the cycle structure of its elements. Specifically an irreducible factor of degree m contributes an m-cycle for the element, and the cycles corresponding to distinct irreducible factors are disjoint. Then we put together the information from various p's and see what elements must be in $\mathrm{Gal}(K/\mathbb{Q})$, up to a relabeling of indices.

EXAMPLE 1. $F(X) = X^5 - X - 1$. The discriminant is $D = 2869 = 19 \cdot 151$. Thus the method may be used with any prime number other than 19 and 151. Here is the factorization for a few primes, together with the cycle structure within $\mathfrak{S}_5$ for a generator of $\overline{G}$:

p	$\overline{F}(X)$	Cycle lengths
2	$(X^2 + X + 1)(X^3 + X + 1)$	$2, 3$
3	$X^5 + 2X + 2$	5
17	$(X + 9)(X + 11)(X^3 + 14X^2 + 12X + 6)$	$1, 1, 3$
23	$(X + 9)(X^4 + 14X^3 + 12X^2 + 7X + 5)$	$1, 4$

For comparison, $p = 19$ gives $\overline{F}(X) = (X + 6)^2(X^2 + 7X^2 + 13X + 10)$, but we cannot use this prime since it divides the discriminant. It is enough to use the information from $p = 2$ and $p = 3$. The irreducibility modulo 3 implies irreducibility over $\mathbb{Q}$. From $p = 3$, we obtain a 5-cycle in $\mathrm{Gal}(K/\mathbb{Q})$. From $p = 2$, we obtain the product of a 2-cycle and a 3-cycle, and the cube of this element is a 2-cycle. In the example in Section 11 following the statement of Theorem 9.44, we saw in effect that the only subgroup of $\mathfrak{S}_5$ containing a 5-cycle and a 2-cycle is $\mathfrak{S}_5$ itself. Therefore $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_5$.

EXAMPLE 2. $F(X) = X^5 + 10X^3 - 10X^2 + 35X - 18$. The discriminant is $D = 3025000000 = 2^6 5^8 11^2$, a perfect square. Thus the Galois group is a subgroup of the alternating group $\mathfrak{A}_5$. The method using reduction modulo p may be used with any prime other than 2, 5, and 11. Here is the factorization for a few primes, together with the cycle structure within $\mathfrak{S}_5$ for a generator of $\overline{G}$:

p	$\overline{F}(X)$	Cycle lengths
3	$X(X+2)(X^3+X^2+2X+1)$	$1, 1, 3$
7	$X^5+3X^3+4X^2+3$	5
17	$(X+14)(X^2+5X+14)(X^2+15X+15)$	$1, 2, 2$

It is enough to use the information from $p = 3$ and $p = 7$. The irreducibility modulo 7 implies irreducibility over $\mathbb{Q}$. From $p = 7$, we obtain a 5-cycle in $\mathrm{Gal}(K/\mathbb{Q})$. From $p = 3$, we obtain a 3-cycle. Any 5-cycle and any 3-cycle together generate all of $\mathfrak{A}_5$. In fact, the generated subgroup must have order divisible by 15, hence must have order 15, 30, or 60. It cannot be of order 15 because every group of order 15 is cyclic and $\mathfrak{A}_5$ has no elements of order 15. It cannot be of order 30 because $\mathfrak{A}_5$ is simple and subgroups of index 2 have to be normal. Hence it is all of $\mathfrak{A}_5$.

EXAMPLE 3. Galois group $\mathfrak{S}_d$. Given $d \geq 4$, let us see how to form an irreducible $F(X)$ for which $\mathrm{Gal}(K/\mathbb{Q})$ is all of $\mathfrak{S}_d$. For any degree d and any prime number ℓ, there exists at least one irreducible monic polynomial of degree d in $\mathbb{F}_\ell[X]$; the reason is that the finite field $\mathbb{F}_{\ell^d}$ is a simple extension of $\mathbb{F}_\ell$ by Corollary 9.19. Let $H_{d,2}(X)$ be such a polynomial of degree d for $\ell = 2$, and let $H_{d-1,3}(X)$ be such a polynomial of degree $d-1$ for $\ell = 3$. Then let p be a prime greater than d, and let $H_{2,p}(X)$ be an irreducible monic polynomial of degree 2 in $\mathbb{F}_p[X]$. We can regard each of $H_{d,2}(X)$, $H_{d-1,3}(X)$, and $H_{2,p}(X)$ as in $\mathbb{Z}[X]$ by reinterpreting their coefficients as integers. Consider the congruences

$$\begin{aligned} F[X] &\equiv H_{d,2}(X) && \mod (2), \\ F[X] &\equiv XH_{d-1,3}(X) && \mod (3), \\ F[X] &\equiv \Big(\prod_{k=0}^{d-3}(X-k)\Big)H_{2,p}(X) && \mod (p), \end{aligned}$$

in $\mathbb{Z}[X]$. Since the sum of any two of the three ideals (2), (3), and (p) of $\mathbb{Z}[X]$ is $\mathbb{Z}[X]$, the Chinese Remainder Theorem (Theorem 8.27) implies that there exists a simultaneous solution $F[X]$ to these congruences in $\mathbb{Z}[X]$, and we may take $F[X]$ to be monic of degree d. Let K be a splitting field for $F[X]$ over $\mathbb{Q}$. Our method applies to the primes 2, 3, and p since none of the three polynomials has any repeated factors. The result of applying the method is that $\mathrm{Gal}(K/\mathbb{Q})$ contains a d-cycle, a $(d-1)$-cycle, and a 2-cycle. Let us see that the subgroup generated by these three elements is all of $\mathfrak{S}_d$. We may assume that the $(d-1)$-cycle is $(1\ 2\ \cdots\ d-1)$. Without loss of generality, the 2-cycle is either $(1\ \ j)$ with $j<d$ or is $(k\ \ d)$ with $k<d$. In the first case some power of the d-cycle is a permutation τ with $\tau(1)=d$; if σ denotes the 2-cycle $(1\ \ j)$, then Lemma 4.41 shows that $\tau\sigma\tau^{-1}$ is the 2-cycle $(d\ \ \tau(j))$, and this is of the form $(k\ \ d)$ with $k<d$. Thus we may assume in any event that $\mathrm{Gal}(K/\mathbb{Q})$ contains $(1\ 2\ \cdots\ d-1)$ and some 2-cycle $(k\ \ d)$ with $k<d$. Conjugating $(k\ \ d)$ by powers of $(1\ 2\ \cdots\ d-1)$, we see that $\mathrm{Gal}(K/\mathbb{Q})$ contains *every* 2-cycle $(k\ \ d)$ with $k<d$. For $1\leq k<d-1$, we then find that $\mathrm{Gal}(K/\mathbb{Q})$ contains

$$(k\ \ d)(k+1\ \ d)(k\ \ d)=(k\ \ k+1).$$

So $\mathrm{Gal}(K/\mathbb{Q})$ contains $(1\ 2), (2\ 3), \dots, (d-2\ \ d-1)$, and we have already seen that it contains $(d-1\ \ d)$. These $d-1$ transpositions generate the full symmetric group, and therefore $\mathrm{Gal}(K/\mathbb{Q})=\mathfrak{S}_d$.

18. Problems

1. Take as known that the polynomial X^3-3X+4 is irreducible over $\mathbb{Q}$, and let r be a complex root of it. In the field $\mathbb{Q}(r)$, find a multiplicative inverse for r^2+r+1 and express it in the form ar^2+br+c with a, b, c in $\mathbb{Q}$.
2. Suppose that R is an integral domain and that F is a subring that is a field, so that R can be considered as a vector space over F. Prove that if $\dim_F R$ is finite, then R is a field.
3. Let $\mathbb{K}$ be a subfield of $\mathbb{C}$ that is not a subfield of $\mathbb{R}$. Prove that $\mathbb{K}$ is topologically dense in $\mathbb{C}$.
4. Let $\mathbb{K}=\Bbbk(x)$ be a transcendental extension of the field $\Bbbk$, and let y be a member of $\mathbb{K}$ that is not in $\Bbbk$. Prove that $\Bbbk(x)$ is an algebraic extension of $\Bbbk(y)$.
5. What is a necessary and sufficient condition on an integer $N>0$ for the positive square root of N to be in the subfield $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}$?
6. The polynomials $F(X)=X^3+X+1$ and $G(Y)=Y^3+Y^2+1$ are irreducible over $\mathbb{F}_2$. Let $\mathbb{K}$ be the field $\mathbb{K}=\mathbb{F}_2[X]/(F(X))$, and let $\mathbb{L}$ be the field $\mathbb{L}=\mathbb{F}_2[Y]/(G(Y))$. Since $\mathbb{K}$ and $\mathbb{L}$ are two fields of order 8, they must be isomorphic. Find an explicit isomorphism.
7. Can a field of order 8 have a subfield of order 4? Why or why not?
8. If $\mathbb{K}$ is a finite field, prove that the product of the nonzero elements of $\mathbb{K}$ is -1. (Educational note: When $\mathbb{K}$ is $\mathbb{F}_p$, this result reduces to Wilson's Theorem, given as Problem 8 at the end of Chapter IV.)
9. Suppose that $\mathbb{K}/\Bbbk$ is a finite extension of the form $\mathbb{K}=\Bbbk(r)$ with $[\mathbb{K}:\Bbbk]$ odd. Prove that $\mathbb{K}=\Bbbk(r^2)$.

10. Suppose that $\mathbb{K}/\Bbbk$ is a finite extension of fields and that $\mathbb{K} = \Bbbk[r, s]$. Prove that if $[\Bbbk(r) : \Bbbk]$ is relatively prime to $[\Bbbk(s), \Bbbk]$, then
   (a) the minimal polynomial of r over $\Bbbk$ is irreducible over $\Bbbk(s)$,
   (b) $[\mathbb{K} : \Bbbk] = [\Bbbk(r) : \Bbbk]\,[\Bbbk(s) : \Bbbk]$.

11. In $\mathbb{C}$, let $\beta = \sqrt[3]{2}$, $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, and $\alpha = \omega\beta$.
   (a) Prove for all c in $\mathbb{Q}$ that $\gamma = \beta + c\alpha$ is a root of some sixth-degree polynomial of the form $X^6 + aX^3 + b$.
   (b) Prove that the minimal polynomial of $\beta + \alpha$ over $\mathbb{Q}$ has degree 3.
   (c) Prove that the minimal polynomial of $\beta - \alpha$ over $\mathbb{Q}$ has degree 6.

12. Suppose that $\Bbbk$ is a finite field and that $F(X)$ is a member of $\Bbbk[X]$ whose derivative is the 0 polynomial. Prove that $F(X)$ is reducible over $\Bbbk$.

13. Let $\Bbbk$ be a field, let $F(X)$ be a separable polynomial in $\Bbbk[X]$, let $\mathbb{K}$ be a splitting field of $F(X)$ over $\Bbbk$, and let $r_1, \dots, r_n$ be the roots of $F(X)$ in $\mathbb{K}$. Regard $\text{Gal}(\mathbb{K}/\Bbbk)$ as a subgroup of the symmetric group $\mathfrak{S}_n$.
   (a) Prove that $\text{Gal}(\mathbb{K}/\Bbbk)$ is transitive on $\{r_1, \dots, r_n\}$ if and only if $F(X)$ is irreducible over $\Bbbk$.
   (b) Show that the cyclotomic polynomial $\Phi_8(X)$ is an example with $\Bbbk = \mathbb{Q}$ and $n = 4$ for which $\text{Gal}(\mathbb{K}/\Bbbk)$ is transitive but $\text{Gal}(\mathbb{K}/\Bbbk)$ contains no 4-cycle.
   (c) Prove that if n is prime and $F(X)$ is irreducible over $\Bbbk$, then $\text{Gal}(\mathbb{K}/\Bbbk)$ contains an n-cycle.

14. Let $a_1, \dots, a_n$ be relatively prime square-free integers ≥ 2, and define $\mathbb{L}_k = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_k})$ for $0 \leq k \leq n$.
   (a) Show for each k that $[\mathbb{L}_k : \mathbb{Q}] = 2^l$ with $0 \leq l \leq k$.
   (b) Suppose for a particular k that $[\mathbb{L}_k : \mathbb{Q}] = 2^k$. Exhibit a vector-space basis of $\mathbb{L}_k$ over $\mathbb{Q}$, and describe the members of $\text{Gal}(\mathbb{L}_k/\mathbb{Q})$ by telling the effect of each member on all basis vectors of $\mathbb{L}_k$ over $\mathbb{Q}$.
   (c) Suppose for a particular $k < n$ that $[\mathbb{L}_k : \mathbb{Q}] = 2^k$. Assume that $\sqrt{a_{k+1}}$ lies in $\mathbb{L}_k$, and let $\sqrt{a_{k+1}}$ be expanded in terms of the basis of (b). Show that application of the members of $\text{Gal}(\mathbb{L}_k/\mathbb{Q})$ leads to a contradiction.
   (d) Deduce that $[\mathbb{L}_n : \mathbb{Q}] = 2^n$.

15. Let p be a prime number, and suppose that a is a member of $\mathbb{Q}$ such that $X^p - a$ has no root in $\mathbb{Q}$. If r is a member of $\mathbb{C}$ with $r^p = a$, prove that
   (a) the cyclotomic polynomial $\Phi_p(X)$ is irreducible in $\mathbb{Q}(r)$,
   (b) the splitting field $\mathbb{K}$ of $X^p - a$ over $\mathbb{Q}$ has degree $[\mathbb{K} : \mathbb{Q}] = p(p-1)$,
   (c) the Galois group $\text{Gal}(\mathbb{K}/\mathbb{Q})$ is isomorphic to a semidirect product of the multiplicative group of $\mathbb{F}_p$ and the additive group of $\mathbb{F}_p$, with the action of a member m of the multiplicative group on the members n of the additive group being given by $m(n) = mn$.

16. Let $F(X)$ be a polynomial in $\Bbbk[X]$ of degree n, where $\Bbbk$ is a field of characteristic 0, and let $\mathbb{K}$ be a splitting field for $F(X)$ over $\Bbbk$. Prove that $[\mathbb{K} : \Bbbk]$ divides $n!$.

17. Let $\Bbbk$ be a field, and let $\mathbb{K}$ be a quadratic extension $\Bbbk(r)$, where $r^2 = a$ is a member of $\Bbbk$.
    (a) If $\Bbbk$ has characteristic 0, determine all elements of $\mathbb{K}$ whose squares are in $\Bbbk$.
    (b) What happens differently if the characteristic is different from 0?

18. Let G be a finite group. Show that there exist two finite extensions $\Bbbk$ and $\mathbb{K}$ of $\mathbb{Q}$ such that $\mathbb{K}$ is a Galois extension of $\Bbbk$ and the Galois group $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ is isomorphic to G.

19. Let $\mathbb{K}/\Bbbk$ be a finite normal extension. For $F(X)$ in $\mathbb{K}[X]$ and σ in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, let $F^\sigma(X)$ be the result of the substitution homomorphism $\mathbb{K}[X] \to \mathbb{K}[X]$ carrying X to X and extending the action of σ on $\mathbb{K}$, i.e., let $F^\sigma(X)$ be obtained by applying σ to the coefficients of $F(X)$. Prove that $\prod_{\sigma \in \mathrm{Gal}(\mathbb{K}/\Bbbk)} F^\sigma(X)$ is in $\Bbbk[X]$.

20. Corollary 9.37 concerns a separable algebraic extension $\mathbb{K}/\Bbbk$ and a finite subgroup H of $\mathrm{Gal}(\mathbb{K}/\Bbbk)$, showing that $\mathbb{K}/\mathbb{K}^H$ is a finite Galois extension with $H = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^H)$ and $[\mathbb{K} : \mathbb{K}^H] = |H|$. By going over its proof, obtain the conclusion that if $\{x_1, \dots, x_n\}$ is the H orbit of x_1 in $\mathbb{K}$, then
    (a) the minimal polynomial of x_1 over $\mathbb{K}^H$ is $\prod_{j=1}^n (X - x_j)$.
    (b) n divides $|H|$.
    (c) $\mathbb{K} = \mathbb{K}^H(x_1)$ if the isotropy subgroup of H at x_1 is trivial.

21. Let $\mathbb{K}$ be the transcendental extension $\mathbb{C}(z)$ of $\mathbb{C}$.
    (a) Prove that any linear fractional transformation $\varphi(z) = \frac{az+b}{cz+d}$ with $ad-bc \neq 0$ in $\mathbb{C}$ extends uniquely to a $\mathbb{C}$ automorphism of $\mathbb{K}$.
    (b) Let H be the 4-element subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{C})$ generated by the extensions of $\sigma(z) = -z$ and $\tau(z) = 1/z$. Show that $w = z^2 + z^{-2}$ is invariant under H, and conclude that every member of $\mathbb{C}(w)$ lies in $\mathbb{K}^H$.
    (c) Applying the previous problem to the element $x_1 = z$ of $\mathbb{K}$, show that the minimal polynomial of z over $\mathbb{C}(w)$ has degree 4.
    (d) Conclude that $\mathbb{K}^H = \mathbb{C}(z^2 + z^{-2})$.

22. In characteristic 0, let $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\Bbbk$ be quadratic extensions.
    (a) Show that there exists an irreducible polynomial $F(X) = X^4 + bX^2 + c$ in $\Bbbk[X]$ such that $F(r) = 0$ for some r in $\mathbb{L}$.
    (b) Show that the element r in (a) has $\mathbb{L} = \Bbbk(r)$.
    (c) Show that $\mathbb{L}$ is a normal extension of $\Bbbk$ with Galois group $C_2 \times C_2$ if and only if c is a square in $\Bbbk$ for some polynomial as in (a), if and only if c is a square in $\Bbbk$ for every polynomial as in (a).

(d) Show that $\mathbb{L}$ is a normal extension of $\Bbbk$ with Galois group C_4 if and only if $c^{-1}(b^2-4c)$ is a square in $\Bbbk$ for some polynomial as in (a), if and only if $c^{-1}(b^2-4c)$ is a square in $\Bbbk$ for every polynomial as in (a).

(e) Give an example of quadratic extensions $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\Bbbk$ in characteristic 0 such that $\mathbb{L}/\Bbbk$ is not normal.

23. Determine Galois groups for splitting fields over $\mathbb{Q}$ for the two polynomials X^3-3X+1 and X^3+X+1.

24. Suppose that $F(X)$ is an irreducible cubic polynomial in $\mathbb{Q}[X]$ whose splitting field $\mathbb{K}$ has $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ isomorphic to $\mathfrak{S}_3$. What are the possibilities, up to isomorphism, for the Galois group of a splitting field of $(X^3-1)F(X)$ over $\mathbb{Q}$?

25. Let $\mathbb{K}/\Bbbk$ be a finite Galois extension whose Galois group is isomorphic to $\mathfrak{S}_3$. Is $\mathbb{K}$ necessarily a splitting field of some irreducible cubic polynomial in $\Bbbk[X]$? Why or why not?

26. Is Cardan's cubic formula valid for finding roots of reducible cubics X^3+pX+q in characteristic 0?

27. Prove that the discriminant of a real cubic with distinct roots is positive if all the roots are real, and is negative if two of the roots are complex.

28. Let $F(X)=X^3+pX+q$ be irreducible in $\mathbb{Q}[X]$, and suppose that $X-r$ is a factor for some r in $\mathbb{C}$.

(a) Show that $F(X)$ factors in $\mathbb{Q}(r)[X]$ as $F(X)=(X-r)(X^2+rX+(r^2+p))$.

(b) We know that $\mathbb{Q}(r)$ is a splitting field for $F(X)$ over $\mathbb{Q}$ if and only if the discriminant $-4p^3-27q^2$ is a square in $\mathbb{Q}$. On the other hand, it is evident from the factorization of $F(X)$ that it splits is $\mathbb{Q}(r)$ if and only if the discriminant $r^2-4(r^2+p)$ is a square in $\mathbb{Q}(r)$. Show by a direct calculation that these two conditions are equivalent.

29. Let $\mathbb{K}$ be a splitting field of an irreducible cubic polynomial $F(X)$ in $\mathbb{Q}[X]$. If $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is $\mathfrak{S}_3$, does it follow that $\mathbb{K}$ contains all three cube roots of 1? Why or why not?

30. In characteristic 0, let $\mathbb{K}$ be the splitting field over $\Bbbk$ of an irreducible polynomial in $\Bbbk[X]$ of degree 5. Assuming that the discriminant of the polynomial is a square in $\Bbbk$, what are the possibilities for $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ up to a relabeling of the indices?

31. Determine the Galois group of a splitting field over $\mathbb{Q}$ for the polynomial $X^5+6X^3-12X^2+5X-4$. Use of a computer may be helpful for this problem.

32. The proof of Theorem 9.64 introduced a positive integer e' in its second paragraph. Prove that e' equals the integer e_1 in the statement of the theorem.

33. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite separable extension of F, and let L be a finite separable extension of K. Let T be the integral closure of R in K, and let U be the integral closure of R in L. Let $\mathfrak{p}$, P, and Q be nonzero prime ideals in R, T, and U, respectively, and let the ramification indices and decomposition degrees for the extensions L/K, L/F, and K/F be

$$e(Q|P), e(P|\mathfrak{p}), e(Q|\mathfrak{p}) \qquad \text{and} \qquad f(Q|P), f(P|\mathfrak{p}), f(Q|\mathfrak{p}).$$

Prove that

$$e(Q|\mathfrak{p}) = e(Q|P)e(P|\mathfrak{p}) \qquad \text{and} \qquad f(Q|\mathfrak{p}) = f(Q|P)f(P|\mathfrak{p}).$$

Problems 34–40 concern norms and traces.

34. Let m be a square-free integer, and let N and Tr denote the norm and trace from $\mathbb{Q}(\sqrt{m}\,)$ to $\mathbb{Q}$.
  (a) Show that $N(a + b\sqrt{m}\,) = a^2 - mb^2$ and $\mathrm{Tr}(a + b\sqrt{m}\,) = 2a$.
  (b) Let T be the ring of algebraic integers in $\mathbb{Q}(\sqrt{m}\,)$. It was shown in Section VIII.9 that T consists of all $a + b\sqrt{m}$ with a, b in $\mathbb{Z}$ if $m \equiv 2 \bmod 4$ or $m \equiv 3 \bmod 4$, and of all $a + b\sqrt{m}$ with a, b in $\mathbb{Z}$ or a, b in $\mathbb{Z} + \frac{1}{2}$ if $m \equiv 1 \bmod 4$. Prove for $a + b\sqrt{m}$ in $\mathbb{Q}(\sqrt{m}\,)$ that $a + b\sqrt{m}$ is in T if and only if $N(a + b\sqrt{m}\,)$ and $\mathrm{Tr}(a + b\sqrt{m}\,)$ are both in $\mathbb{Z}$.
  (c) Assume that $a + b\sqrt{m}$ is in T. Prove that $N(a + b\sqrt{m}\,)$ is in $\mathbb{Z}^\times$ if and only if $a + b\sqrt{m}$ is in $T^\times$.
  (d) For $m = 2$, give an example of a member of $T^\times$ other than ± 1.

35. For the extension $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$, find the value of the norm N and the trace Tr on a general element $a + b\sqrt[3]{2} + c(\sqrt[3]{2}\,)^2$ of $\mathbb{Q}(\sqrt[3]{2}\,)$; here a, b, c are in $\mathbb{Q}$.

36. Let $N(\,\cdot\,)$ be the norm relative to the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, where ζ is a primitive n^{th} root of 1.
  (a) Show that $N(1-\zeta) = \Phi_n(1)$, where $\Phi_n(X)$ is the n^{th} cyclotomic polynomial.
  (b) Using the formula $\prod_{d|n,\ d>1} \Phi_d(X) = X^{n-1} + X^{n-2} + \cdots + 1$, show that $N(1 - \zeta) = \Phi_n(1)$ equals p if n is a power of the positive prime p and equals 1 if n is divisible by more than one positive prime.

37. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $4n + 1$. It was shown in Problem 31 at the end of Chapter VIII that such a prime is the sum of two squares. This problem gives a shorter proof. Take as known from Section VIII.4 that the ring $\mathbb{Z}[\sqrt{-1}\,]$ of Gaussian integers is a Euclidean domain, and from Problem 30 at the end of Chapter VIII that $x^2 \equiv -1 \bmod p$ has an integer solution x. Carry out the following steps:

(a) Write

$$\frac{x \pm \sqrt{-1}}{p} = \frac{1}{p}x \pm \frac{1}{p}\sqrt{-1}.$$

If p were prime in $\mathbb{Z}[\sqrt{-1}\,]$, then it would follow from the divisibility of x^2+1 by p that p divides $x+\sqrt{-1}$ or p divides $x-\sqrt{-1}$. Deduce from the displayed equation that neither alternative is viable, and conclude that p cannot be prime in $\mathbb{Z}[\sqrt{-1}\,]$.

(b) Using the conclusion of (a) to write p as a nontrivial product in $\mathbb{Z}[\sqrt{-1}]$ and applying the norm function, prove that there exist integers a and b such that $p = a^2+b^2$.

38. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $8n+1$. Take as known from Problem 13 at the end of Chapter VIII that $\mathbb{Z}[\sqrt{-2}\,]$ is a Euclidean domain, and from the law of quadratic reciprocity (to be proved in Chapter I of *Advanced Algebra*) that $x^2 \equiv -2 \bmod p$ has an integer solution x. Guided by the argument for the previous problem, prove that there exist integers a and b such that $p = a^2+2b^2$.

39. Let $p > 0$ be a prime in $\mathbb{Z}$ of the form $6n+1$. Take as known from Problem 26 at the end of Chapter VIII that $\mathbb{Z}\big[\frac{1}{2}(1+\sqrt{-3}\,)\big]$ is a Euclidean domain, and from the law of quadratic reciprocity (to be proved in *Advanced Algebra*) that $x^2 \equiv -3 \bmod p$ has an integer solution x. Guided by the argument for the previous problem, prove that there exist integers a and b such that $p = a^2+3b^2$.

40. Let $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{L}'$ be fields such that $\mathbb{L}'/\Bbbk$ is a finite separable extension. Using Corollary 9.58, prove that the norm and trace satisfy

$$N_{\mathbb{L}'/\Bbbk} = N_{\mathbb{L}/\Bbbk} \circ N_{\mathbb{L}'/\mathbb{L}} \qquad \text{and} \qquad \mathrm{Tr}_{\mathbb{L}'/\Bbbk} = \mathrm{Tr}_{\mathbb{L}/\Bbbk} \circ \mathrm{Tr}_{\mathbb{L}'/\mathbb{L}}\,.$$

Problems 41–45 make use of the theory of symmetric polynomials, which was introduced in Problems 36–39 at the end of Chapter VIII.

41. Let $\Bbbk$ be a field, let $F(X)$ be a polynomial in $\Bbbk[X]$, let $\mathbb{K}$ be an extension field in which $F(X)$ splits, and let $r_1, \dots, r_n$ be the roots of $F(X)$ in $\mathbb{K}$, repeated according to their multiplicities. If $P(X_1, \dots, X_n)$ is a symmetric polynomial in $\Bbbk[X_1, \dots, X_n]$, prove that $P(r_1, \dots, r_n)$ is a member of $\Bbbk$.

42. Let $\Bbbk$ be a field, let $F(X)$ and $G(X)$ be polynomials over $\Bbbk$, let $\mathbb{K}$ be an extension field in which $F(X)$ and $G(X)$ both split, and let $r_1, \dots, r_m$ and $s_1, \dots, s_n$ be the respective roots of $F(X)$ and $G(X)$ in $\mathbb{K}$, repeated according to their multiplicities. Deduce from the previous problem that the polynomials

$$H_1(X) = \prod_{i=1}^{m}\prod_{j=1}^{n}(X - r_i - s_j) \qquad \text{and} \qquad H_2(X) = \prod_{i=1}^{m}\prod_{j=1}^{n}(X - r_i s_j)$$

lie in $\Bbbk[X]$.

43. (a) Find a nonzero polynomial with rational coefficients having $\sqrt{2}+\sqrt{3}$ as a root. What is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$?
    (b) Find a nonzero polynomial with rational coefficients having $\sqrt{2}+\sqrt[3]{2}$ as a root. What is the minimal polynomial of $\sqrt{2}+\sqrt[3]{2}$ over $\mathbb{Q}$?

44. Let $\mathbb{k}$ be a field of characteristic 0, and let $\mathbb{K}=\mathbb{k}(r_1,\dots,r_n)$ be the field of fractions of the polynomial ring $\mathbb{k}[r_1,\dots,r_n]$ in n indeterminates. Show that any σ in the symmetric group $\mathfrak{S}_n$ defines a member of $\mathrm{Gal}(\mathbb{K}/\mathbb{k})$ such that $\sigma(r_j)=r_{\sigma(j)}$ for all σ in $\mathfrak{S}_n$. Then define $F(X)$ to be the polynomial

$$F(X)=(X-r_1)\cdots(X-r_n)$$

in $\mathbb{K}[X]$, and show that
    (a) $F(X)$ is irreducible over the fixed field $\mathbb{K}^{\mathfrak{S}_n}$,
    (b) $\mathbb{K}$ is a splitting field for $F(X)$ over $\mathbb{K}^{\mathfrak{S}_n}$,
    (c) $\mathbb{K}^{\mathfrak{S}_n}=\mathbb{k}(u_1,\dots,u_n)$, where $u_1,\dots,u_n$ are given by

$$u_1=\sum_i r_I,\qquad u_2=\sum_{i<j} r_ir_j,\qquad \dots,\qquad u_n=\prod_i r_i,$$

    (d) the Galois group of the splitting field of $F(X)$ over $\mathbb{k}(u_1,\dots,u_n)$ is $\mathfrak{S}_n$.

45. **(Cubic resolvent)** This problem carries out one step in finding the roots of an arbitrary quartic polynomial. Let $\mathbb{k}$ be a field of characteristic 0, let $\mathbb{K}=\mathbb{k}(p,q,r)$ be the field of fractions of the polynomial ring $\mathbb{k}[p,q,r]$ in n indeterminates, and let $\mathbb{L}$ be a splitting field of the polynomial

$$F(X)=X^4+pX^2+qX+r$$

in $\mathbb{K}[X]$. The Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is $\mathfrak{S}_4$ by the previous problem. Let $B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$. In the composition series $\mathfrak{S}_4\supseteq\mathfrak{A}_4\supseteq B_4\supseteq\{(1),(1\ 2)\}(3\ 4)\}\supseteq\{1\}$, Proposition 9.63 shows that the fixed field of $\mathfrak{A}_4$ is $\mathbb{K}(\sqrt{D})$, where D is the discriminant. To obtain the fixed field of B_4, we adjoin to $\mathbb{K}(\sqrt{D})$ an element of $\mathbb{L}$ invariant under B_4 but not under $\mathfrak{A}_4$. If s_1,s_2,s_3,s_4 denote the roots of $F(X)$ in $\mathbb{L}$, then such an element is $(s_1+s_2)(s_3+s_4)$. Its three conjugates under $\mathfrak{A}_4/B_4$ are

$$\begin{aligned}\theta_1&=(s_1+s_2)(s_3+s_4),\\ \theta_2&=(s_1+s_3)(s_2+s_4),\\ \theta_3&=(s_1+s_4)(s_2+s_3),\end{aligned}$$

which are the three roots of the "cubic resolvent" polynomial

$$\theta^3-c_1\theta^2+c_2\theta-c_3,$$

where c_1,c_2,c_3 are the elementary symmetric polynomials in $\theta_1,\theta_2,\theta_3$ given by

$$c_1 = \sum_i \theta_i, \qquad c_2 = \sum_{i<j} \theta_i\theta_j, \qquad c_3 = \prod_i \theta_i.$$

(a) Show that c_1, c_2, c_3 are symmetric polynomials in s_1, s_2, s_3, s_4, hence are polynomials in the coefficients p, q, r.

(b) Verify that $c_1 = 2p$, $c_2 = p^2 - 4r$, and $c_3 = q^2$.

(c) Show that the discriminant of the cubic resolvent equals the discriminant of the original quartic polynomial.

Problems 46–50 concern Galois groups of splitting fields of quartic polynomials. Take as known that the discriminant of a quartic polynomial $F(X) = X^4 + pX^2 + qX + r$ is given by

$$-4p^3q^2 - 27q^4 + 16p^4r + 144pq^2r - 128p^2r^2 + 256r^3.$$

Let $\mathbb{K}$ be a splitting field for $F(X)$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Regard G as a subgroup of the symmetric group $\mathfrak{S}_4$.

46. (a) Identify all transitive subgroups of the alternating group $\mathfrak{A}_4$, up to a relabeling of the four indices.

    (b) Identify all transitive subgroups of the symmetric group $\mathfrak{S}_4$ other than those in (a), up to a relabeling of the four indices.

47. Suppose $q = 0$.

    (a) Show that G is a subgroup of $\mathfrak{A}_4$ if and only if r is a square in $\mathbb{Q}$.

    (b) Show by solving $F(X) = 0$ explicitly that $[\mathbb{K} : \mathbb{Q}]$ is a power of 2, and conclude that G has no element of order 3.

    (c) Deduce when r is a square that $G = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ if $F(X)$ is irreducible over $\mathbb{Q}$.

    (d) Deduce when r is a nonsquare that G is cyclic of order 4 or is dihedral of order 8 if $F(x)$ is irreducible over $\mathbb{Q}$; in the dihedral case, G is generated by a 4-cycle and the group listed in (c). (Problem 22 shows how to distinguish between the two cases.)

48. For $F(X) = X^4 + X + 1$, show by considering reduction modulo 2 and modulo 3 that $G = \mathfrak{S}_4$.

49. Let $F(X) = X^4 + 8X + 12$.

    (a) Compute the discriminant of $F(X)$, and verify that it is a square.

    (b) Show that $F(X) \equiv (1 + X)(2 + X + 4X^2 + X^3)$ mod 5 with the two factors on the right side irreducible in $\mathbb{F}_5$.

    (c) Show from (a) and (b) that if $F(X)$ is reducible over $\mathbb{Q}$, then it must have a root that is an integer. Check that there is no such root.

    (d) Conclude that $G = \mathfrak{A}_4$.

50. For each transitive group G as in Problem 46, find a polynomial $F(X)$ of degree 4 over $\mathbb{Q}$ whose splitting field $\mathbb{K}$ over $\mathbb{Q}$ has $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ isomorphic to G.

Problems 51–56 continue the introduction to error-correcting codes begun in Problems 63–73 at the end of Chapter IV and continued in Problems 25–28 at the end of Chapter VII. The current problems will not make use of the problems in Chapter VII. As in the problems in Chapter IV, we work with the field $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, with Hamming space $\mathbb{F}^n$, and with linear codes C in $\mathbb{F}^n$. The minimal distance of C is denoted by $\delta(C)$. Problem 72 in Chapter IV introduced cyclic redundancy codes, which are determined by a generating polynomial $G(X)$ of some degree g suitably less than n. Such a code C is built from all polynomials $G(X)B(X)$ with $B(X) = 0$ or $\deg B(X) \leq n - g - 1$. A given polynomial $c_0 + c_1X + \cdots$ becomes the n-tuple $(c_0, c_1, \dots)$ of C; the code C has dimension $n - g$. This set of problems will discuss a special class of cyclic redundancy codes called cyclic codes, and then a special subclass called BCH codes.

51. A linear code C in $\mathbb{F}^n$ is called a **cyclic code** if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C, then so is $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$.
    (a) Prove that a linear code C is cyclic if and only if the set of all polynomials $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ corresponding to members $(c_0, c_1, \dots, c_{n-1})$ of C is an ideal in the ring $\mathbb{F}[X]/(X^n - 1)$. (In this case the members of C will be identified with the set of such polynomials.)
    (b) Prove that if C is cyclic and nonzero, then there exists a unique $G(X)$ in C of lowest possible degree. Moreover, $G(X)$ divides $X^n - 1$ in $\mathbb{F}[X]$, and C consists exactly of the polynomials $G(X)F(X) \bmod (X^n - 1)$ such that $F(X) = 0$ or $\deg F(X) \leq n - \deg G(X) - 1$, and C has dimension $n - \deg G(X)$. (The polynomial $G(X)$ is called the **generating polynomial** of C. A cyclic code C over the field $\mathbb{Z}/2\mathbb{Z}$ having block length n and dimension k is called a **binary cyclic** (n, k) **code**.)
    (c) Prove that if $G(X)$ has degree $n - k$, then a basis of C consists of the polynomials $G(X), XG(X), X^2G(X), \dots, X^{k-1}G(X)$.
    (d) Under the assumption that C is cyclic and nonzero, (b) says that it is possible to write $X^n - 1 = G(X)H(X)$ for some $H(X)$ in $\mathbb{F}[X]$. Prove that a member $B(X)$ of $\mathbb{F}[X]/(X^n - 1)$ lies in C if and only if $H(X)B(X) \equiv 0 \bmod (X^n - 1)$.

52. (a) Show that the row space C of the matrix $\mathcal{G} = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix}$ is a cyclic $(7, 3)$ code with generating polynomial $G(X) = 1 + X^2 + X^3 + X^4$.
    (b) Show directly from $\mathcal{G}$ that C has minimal distance $\delta = 4$.
    (c) The polynomial $H(X) = 1 + X^2 + X^3$ has the property that $G(X)H(X) = X^7 - 1$ in $\mathbb{F}[X]$. Find a 4-by-7 matrix $\mathcal{H}$ such that the column vectors $v \in \mathbb{F}^7$ that lie in C are exactly the ones with $\mathcal{H}v = 0$.

(d) The matrix $\mathcal{H}$ in (c) is called the **check matrix** for the code. Describe a procedure for constructing the check matrix when starting from a general binary cyclic (n, k) code whose generating polynomial $G(X)$ is known and whose polynomial $H(X)$ with $G(X)H(X) = X^n - 1$ is known. Prove that the procedure works.

53. Show that $X^n - 1$ is a separable polynomial over $\mathbb{F}$ if n is odd but not if n is even.

54. Let C be a binary cyclic (n, k) code with generating polynomial $G(X)$, and suppose that n is odd. Let $\mathbb{K}$ be a finite extension field of $\mathbb{F}$ in which $X^n - 1$ splits, and let α be a primitive n^{th} root of 1, i.e., a root of $X^n - 1$ in $\mathbb{K}$ such that $\alpha^m \neq 1$ for $0 < m < n$. Suppose that r and s are integers with $0 \leq s < n$ and

$$G(\alpha^r) = G(\alpha^{r+1}) = \cdots = G(\alpha^{r+s}) = 0.$$

(a) Let $P(X) = G(X)F(X)$ with $F(X) \neq 0$ and $\deg F < k$ be an arbitrary nonzero member of C, so that $P(\alpha^r) = P(\alpha^{r+1}) = \cdots = P(\alpha^{r+s}) = 0$. Write $P(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, and use the values of $P(\alpha^j)$ for $r \leq j \leq r + s$ to set up a homogeneous system of $s + 1$ linear equations with n unknowns $c_0, \ldots, c_{n-1}$.

(b) Using an argument with Vandermonde determinants, show that every $(s+1)$-by-$(s+1)$ submatrix of the coefficient matrix of the system in (a) is invertible.

(c) Obtain a contradiction from (b) if $s + 1$ or fewer of the coefficients of $P(X)$ are nonzero.

(d) Conclude that the minimal distance $\delta(C)$ is $\geq s + 2$.

55. **(BCH codes, or Bose–Chaudhuri–Hocquenghem codes)** Let n be an odd positive integer, let e be a positive integer $< n/2$, let $\mathbb{K}$ be a finite extension field of $\mathbb{F}$ in which $X^n - 1$ splits, and let α be a primitive n^{th} root of 1 in $\mathbb{K}$. For $1 \leq j \leq 2e$, let $F_j(X)$ be the minimal polynomial of α^j over $\mathbb{F}$, and define $G(X) = (1 + X)\,\mathrm{LCM}(F_1(X), \ldots, F_{2e}(X))$. Prove that $G(X)$ divides $X^n - 1$ and that $G(X)$ is the generating polynomial for a cyclic code C in $\mathbb{F}^n$ with minimal distance $\delta(C) \geq 2e + 2$. (Educational note: Therefore C has the built-in capability of correcting at least e errors.)

56. In the setting of the previous problem, let $n = 2^m - 1$ for a positive integer m, and let $\mathbb{K}$ be a field of order 2^m.

(a) Prove that any irreducible polynomial in $\mathbb{F}[X]$ with a root in $\mathbb{K}$ has order dividing m, and conclude that the order of the generating polynomial $G(X)$ in the previous problem is at most $2em + 1$.

(b) Prove that there exists a sequence C_r of binary cyclic (n_r, k_r) codes of BCH type such that k_r/n_r tends to 1 and the minimal distance $\delta(C_r)$ tends to infinity. (Educational note: The fraction k_r/n_r tells the fraction of message bits to total bits in each transmitted block. Thus the problem says that there are linear codes capable of correcting as large a number of errors as we please while having as large a percentage of message bits as we please.)

57. Take as known that $F_1(X) = 1 + X + X^4$ is irreducible over $\mathbb{F}$. Let $\mathbb{K}$ be the field $\mathbb{F}[X]/(F_1(X))$ of order 16, and let α be the coset $X + (F_1(X))$ in $\mathbb{K}$.
   (a) Explain why $F_1(X)$ factors as $F_1(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)$ over $\mathbb{K}$.
   (b) Find the minimal polynomial $F_3(X)$ of α^3.
   (c) Show in $\mathbb{F}^{15}$ that the binary cyclic code C with generating polynomial $G(X) = (1 + X)F_1(X)F_3(X)$ has $\dim C = 6$ and $\delta(C) \geq 6$.

Problems 58-63 combine Problems 12–13 in Chapter V with the notion of extension of scalars from Chapter VI and some Galois theory from Chapter IX to prove the general **Jordan–Chevalley decomposition**. Let $\Bbbk$ be a field, and let V be a finite-dimensional vector space over $\Bbbk$. A linear map $N : V \to V$ is called **nilpotent** if $N^k = 0$ for some k. A linear map $S : V \to V$ is called **semisimple** if there is some finite extension $\mathbb{K}$ of $\Bbbk$ for which the linear map $S^{\mathbb{K}} : V^{\mathbb{K}} \to V^{\mathbb{K}}$ obtained by extension of scalars has a basis of eigenvectors. The theorem is that if $L : V \to V$ is a linear map with the property that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable, then L has a unique decomposition $L = S + N$ with S semisimple, N nilpotent, and $SN = NS$. The theorem applies without restriction to a linear $L : V \to V$ if $\Bbbk$ is finite or has characteristic 0 because the separability condition is automatically satisfied in these cases.

58. Let $\Bbbk$ be a field, let V be a vector space over $\Bbbk$, and let $\mathbb{K}$ be an extension field of $\Bbbk$. Extend scalars to form the $\mathbb{K}$ vector space given by $V^{\mathbb{K}} = V \otimes_{\Bbbk} \mathbb{K}$, and let $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ act on $V^{\mathbb{K}}$ by saying that $\varphi(v \otimes c) = v \otimes \varphi(c)$ for φ in $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ and $v \otimes c$ in $V^{\mathbb{K}}$. Explain for $V = \Bbbk^n$ that $V^{\mathbb{K}}$ may be interpreted as $\mathbb{K}^n$ and that the action by φ reduces to $(\varphi(u))_j = \varphi(u_j)$.

59. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be a linear map. Suppose that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable. Prove the existence of a Jordan–Chevalley decomposition of L by following these steps:
   (a) Let $\mathbb{K}$ be a splitting field of $\Bbbk$, so that $\mathbb{K}$ is a finite Galois extension of $\Bbbk$. Use Problems 12–13 of Chapter V to show that $L \otimes 1 : V^{\mathbb{K}} \to V^{\mathbb{K}}$ has a unique decomposition as a sum $\mathcal{S} + \mathcal{N}$ of $\mathbb{K}$ linear maps of $V^{\mathbb{K}}$ to itself such that $\mathcal{S}\mathcal{N} = \mathcal{N}\mathcal{S}$, $\mathcal{N}$ is nilpotent, and $\mathcal{S}$ has a basis of eigenvectors.
   (b) Prove that any $\mathbb{K}$ linear $\mathcal{T}$: $V^{\mathbb{K}} \to V^{\mathbb{K}}$ such that $(1 \otimes \varphi)\mathcal{T} = \mathcal{T}(1 \otimes \varphi)$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$ is of the form $\mathcal{T} = T \otimes 1$ for a unique $\Bbbk$ linear $T : V \to V$.
   (c) Show that the $\mathbb{K}$ linear maps $\mathcal{S}$ and $\mathcal{N}$ of (a) satisfy $(1 \otimes \varphi)\mathcal{S} = \mathcal{S}(1 \otimes \varphi)$ and $(1 \otimes \varphi)\mathcal{N} = \mathcal{N}(1 \otimes \varphi)$ for all $\varphi \in \mathrm{Gal}(\mathbb{K}/\Bbbk)$, and deduce from (b) that $\mathcal{S}$ and $\mathcal{N}$ may be written as $\mathcal{S} = S \otimes 1$ and $\mathcal{N} = N \otimes 1$ for uniquely defined $\Bbbk$ linear maps S and N of V into itself.
   (d) Show that S is semisimple, N is nilpotent, and $SN = NS$, and conclude that $L = S + N$ is a Jordan–Chevalley decomposition of L.

(e) Show that S and N are polynomials in L.

60. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be a linear map. Prove the uniqueness result that there is at most one decomposition $L = S + N$ with S semisimple, N nilpotent, and $SN = NS$.

61. Let $\Bbbk = \mathbb{R}$, and let $L : \mathbb{R}^4 \to \mathbb{R}^4$ be the linear map defined by the matrix

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The minimal polynomial of L or A is $(X^2+1)^2$. Calculate the Jordan–Chevalley decomposition of L in matrix form.

62. Let $\mathbb{F}_2$ be a field of two elements, and let $\Bbbk = \mathbb{F}_2(x)$, where x is transcendental over $\mathbb{F}_2$. Let $L : \Bbbk^2 \to \Bbbk^2$ be the linear map defined by the matrix $A = \left(\begin{smallmatrix} 0 & x \\ 1 & 0 \end{smallmatrix}\right)$. The characteristic polynomial of L or A is $M(X) = X^2 - x$. This is irreducible over $\Bbbk$ and hence is also the minimal polynomial. The quadratic extension $\mathbb{K} = \Bbbk[x^{1/2}]$ of $\Bbbk$ is a splitting field for $M(X)$, and $M(X)$ has a double root in $\Bbbk[x^{1/2}]$.
    (a) Show that A, regarded as a matrix in $M_2(\mathbb{K})$, does not have a basis of eigenvectors. Conclude that L is not semisimple.
    (b) Calculate the most general 2-by-2 matrix commuting with A, and show that it cannot have characteristic polynomial X^2 unless it is the 0 matrix.
    (c) Conclude that L cannot have a Jordan–Chevalley decomposition.

63. Let $\Bbbk$ be a field, let V be a finite-dimensional vector space over $\Bbbk$, and let $L : V \to V$ be an *invertible* linear map. Suppose that every irreducible factor of the minimal polynomial of L over $\Bbbk$ is separable. A linear map $U : V \to V$ is called **unipotent** if $(U - I)^k = 0$ for some k. By suitably adjusting the proof of the Jordan–Chevalley decomposition, prove that there exist linear maps S and U of V into itself such that S is semisimple, U is unipotent, and $L = SU = US$.

Problems 64–73 introduce ordered fields, formally real fields, and real closed fields. An **ordered field** $\Bbbk$ is a field with a specified subset P of "positive" elements that is closed under addition and multiplication and is such that each nonzero element of $\Bbbk$ is in exactly one of P and $-P$. The fields $\mathbb{Q}$ and $\mathbb{R}$ are examples. A **formally real field** $\Bbbk$ is a field in which -1 is not the sum of squares. A **real closed field** $\Bbbk$ is a formally real field such that no proper algebraic extension of $\Bbbk$ is formally real. The problems together prove the existence part of the **Artin–Schreier Theorem**: If $\Bbbk$ is an ordered field with P as its set of positive elements and if $\overline{\Bbbk}$ is an algebraic closure, then there exists a real closed field $\mathbb{K}$ between $\Bbbk$ and $\overline{\Bbbk}$ that is an ordered field with P contained in its set of positive elements. Moreover, $\mathbb{K}$ is unique up to $\Bbbk$ isomorphism, and $\overline{\Bbbk}$ is of the form $\mathbb{K}(\sqrt{-1}\,)$.

64. Verify the following properties of an ordered field $\Bbbk$ when P is the set of positive elements:
    (a) 1 is in P,
    (b) every nonzero square is in P,
    (c) whenever a is in P, then so is a^{-1},
    (d) $\Bbbk$ is formally real,
    (e) $\Bbbk$ has characteristic 0.

65. In an ordered field $\Bbbk$ whose set of positive elements is P, define $x > y$ and $y < x$ to mean $x - y$ is in P. Let a, b, c, d be in $\Bbbk$. Check the following:
    (a) exactly one the relations $a > b$, $a = b$, and $a < b$ holds,
    (b) if $a > b$ and $b > c$, then $a > c$,
    (c) if $a > b$, then $a + c > b + c$,
    (d) if $a > b$ and $c > 0$, then $ac > bc$,
    (e) if $a > b > 0$, then $b^{-1} > a^{-1}$,
    (f) if $a > b > 0$ and $c > d > 0$, then $ac > bd$,
    (g) if $a > b$ and $c > d$, then $ac + bd > ad + bc$.

66. Let $\Bbbk$ be an ordered field with P as its set of positive elements, let $\Bbbk(x)$ be a transcendental extension, and define the positive elements of $\Bbbk(x)$ to be those for which the quotient of the leading coefficient of the numerator by the leading coefficient of the denominator is in P. Show that with this definition of the set of positive elements, $\Bbbk(x)$ becomes an ordered field in which $x > n$ for every positive integer n. (Then also $1/n > 1/x$ for every positive integer n by Problem 65e.)

67. (a) Show that $\mathbb{Q}(\sqrt{2}\,)$ becomes an ordered field in two distinct ways.
    (b) If $\Bbbk$ is an ordered field with P as its set of positive elements and if c is a member of P that is not a square, show that there are two ways of defining the set of positive elements P' of $\mathbb{K} = \Bbbk(\sqrt{c}\,)$ so that $\mathbb{K}$ becomes an ordered field with $P \subseteq P'$.

68. Let $\Bbbk$ be an ordered field, and let $\mathbb{K}$ be the extension that arises by adjoining the square roots of all the positive elements of $\mathbb{K}$. Prove that $\mathbb{K}$ is a formally real field by carrying out the following steps:
    (a) Show that if n is chosen as small as possible so that an equation $-1 = \sum_{j=1}^{k} p_j \xi_j^2$ holds in $\mathbb{K}$ with all p_j positive in $\Bbbk$ and all ξ_j in an extension $\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_n}\,)$ of $\Bbbk$ with all c_j positive in $\Bbbk$, then writing

$$\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_n}\,) = \Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_{n-1}}\,)(\sqrt{c_n}\,)$$

leads to an equation

$$-1 = \sum_{j=1}^{k} p_j a_j^2 + \sum_{j=1}^{k} p_j c_n b_j^2 + 2\sqrt{c_n} \sum_{j=1}^{k} p_j a_j b_j \qquad (*)$$

in which a_j and b_j are in $\Bbbk(\sqrt{c_1}\,, \dots, \sqrt{c_{n-1}}\,)$.

(b) Consider the third term on the right side of $(*)$, and show that a contradiction results if this term is 0 and a different contradiction arises if this term is not 0.

69. Let $\Bbbk$ be a formally real field, and let $\overline{\Bbbk}$ be an algebraic closure. Show that there exist maximal formally real subfields of $\overline{\Bbbk}$ containing $\Bbbk$, and show that any such is a real closed field.

70. Carry out the following steps to show that a real closed field $\Bbbk$ becomes an ordered field in one and only one way:
   (a) Suppose that $c \neq 0$ is not a square, hence that $\Bbbk(\sqrt{c}\,)$ is a quadratic extension of $\Bbbk$. Why is $-1 = \sum_{j=1}^{n}(a_j + b_j\sqrt{c}\,)^2$ for suitable members a_j and b_j of $\Bbbk$?
   (b) By expanding the identity in (a), show that c is not a sum of squares. In other words, every sum of squares in $\Bbbk$ is a square in $\Bbbk$.
   (c) Solve for c in the expansion in (b), and conclude that $-c$ is a square.
   (d) Conclude from the previous steps that the choice of P as the set of nonzero squares makes $\Bbbk$ into an ordered field and that there no other possible definition for the set P of positive elements that makes $\Bbbk$ into an ordered field.

71. Carry out the following steps to show that in any real closed field $\Bbbk$, every polynomial of odd degree has a root:
   (a) Show by induction that it is enough to handle irreducible polynomials of odd degree.
   (b) For an irreducible polynomial $Q(X)$ of odd degree n, let $\Bbbk(\alpha)$ be a simple algebraic extension of $\Bbbk$ such that $Q(\alpha) = 0$. Show that an expression of -1 as a sum of squares in $\Bbbk(\alpha)$ forces an identity $\sum_{j=1}^{k} R_j(X)^2 + Q(X)A(X) = -1$ for suitable polynomials $R_j(X)$ in $\Bbbk[X]$ of degree $\leq n-1$ and some polynomial $A(X)$ in $\Bbbk[X]$ of odd degree $\leq n-2$.
   (c) If r is a root of the polynomial $A(X)$ in (b), show that $\sum_{j=1}^{k} R_j(r)^2 = -1$, and deduce a contradiction.

72. By using the results of Problems 70–71 and taking into account the proof of Theorem 1.18 that appears in Section IX.10, prove that if $\Bbbk$ is a real closed field, then $\Bbbk(\sqrt{-1}\,)$ is algebraically closed.

73. Put the above results together to give a proof of the existence in the Artin–Schreier Theorem: if an ordered field $\Bbbk$ has P as its set of positive elements and $\overline{\Bbbk}$ as an algebraic closure, then there exists a real closed field $\mathbb{K}$ with $\Bbbk \subseteq \mathbb{K} \subset \overline{\Bbbk}$ such that $\overline{\Bbbk} = \mathbb{K}(\sqrt{-1}\,)$ and such that P is contained in the set of squares in $\overline{\Bbbk}$, i.e., such that the set of positive elements in the natural ordered-field structure on $\overline{\Bbbk}$ contains P.