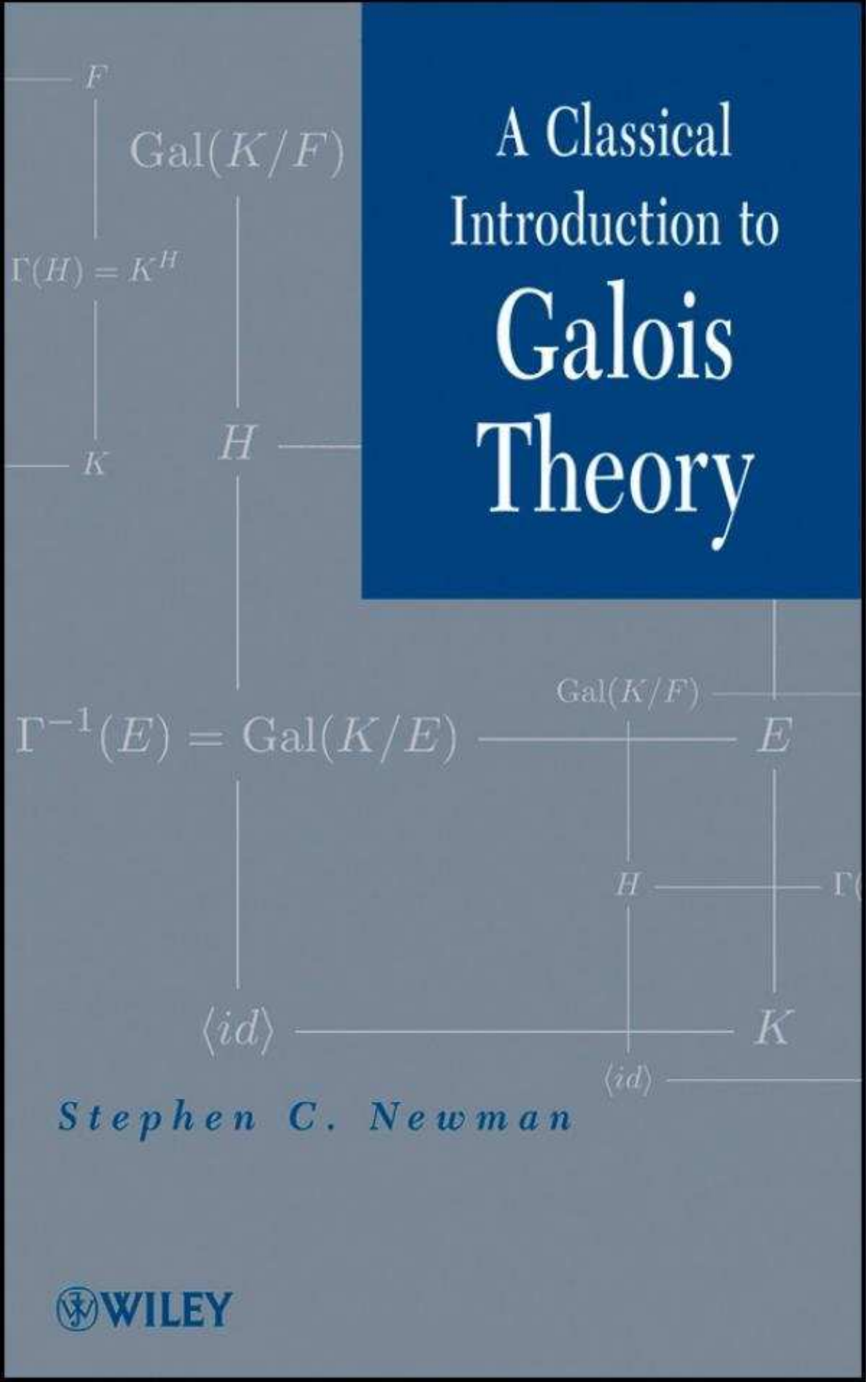


A Classical Introduction to Galois Theory

Stephen C. Newman

WILEY

A CLASSICAL INTRODUCTION TO GALOIS THEORY

This page intentionally left blank

A CLASSICAL INTRODUCTION TO GALOIS THEORY

STEPHEN C. NEWMAN
University of Alberta,
Edmonton, Alberta, Canada

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data:

Newman, Stephen C., 1952–
A classical introduction to Galois theory / Stephen C. Newman.
p. cm.
Includes index.
ISBN 978-1-118-09139-5 (hardback)
1. Galois theory. I. Title.
QA214.N49 2012
512′.32–dc23

2011053469

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To Sandra

This page intentionally left blank

CONTENTS

This page intentionally left blank

PREFACE

The quadratic formula for solving polynomials of degree 2 has been known for centuries, and it is still an important part of mathematics education. Less familiar are the corresponding formulas for solving polynomials of degrees 3 and 4. These expressions are more complicated than their quadratic counterpart, but the fact that they exist comes as no surprise. It is therefore altogether unexpected that no such formulas are available for solving polynomials of degrees 5 and higher. Why should this be so? A complete answer to this intriguing problem is provided by Galois theory. In fact, Galois theory was created precisely to address this and related questions about polynomials, a feature that might not be apparent from a survey of current textbooks on university level algebra. The reason for this change in focus is that Galois theory long ago outgrew its origin as a method of studying the algebraic properties of polynomials. The elegance of the modern approach to Galois theory is undeniable, but the attendant abstraction tends to obscure the satisfying concreteness of the ideas that underlie and motivate this profoundly beautiful area of mathematics.

This book develops Galois theory from a historical perspective. Throughout, the emphasis is on issues related to the solvability of polynomials by radicals. This gives the book a sense of purpose, and far from narrowing the scope, it provides a platform on which to develop much of the core curriculum of Galois theory. Classical results by Abel, Gauss, Kronecker, Lagrange, Ruffini, and, of course, Galois are presented as background and motivation leading up to a modern treatment of Galois theory. The celebrated criterion due to Galois for the solvability of polynomials by radicals is presented in detail. The power of Galois theory as both a theoretical and computational tool is illustrated by a study of the solvability of polynomials of prime degree, by developing the theory of

periods of roots of unity (due to Gauss), by determining conditions for a type of denesting of radicals, and by deriving the classical formulas for solving general quadratic, cubic, and quartic polynomials by radicals.

The reader is expected to have a basic knowledge of linear algebra, but other than that the book is largely self-contained. In particular, most of what is needed from the elementary theory of polynomials and fields is presented in the early chapters of the book, and much of the necessary group theory is provided in a series of appendices. When planning and writing this book, I had in mind that it might be used as a resource by mathematics students interested in understanding the origins of Galois theory and the reason it was created in the first place. To this end, proofs are quite detailed and there are numerous worked examples, while on the other hand, exercises have not been included.

Several acknowledgements are in order. It is my pleasure to thank Professor David Cox of Amherst College, Professor Jean-Pierre Tignol of the Université catholique de Louvain, and Professor Al Weiss of the University of Alberta for their valuable comments on drafts of the manuscript. I am further indebted to Professors Cox and Tignol for their exceptional books on Galois theory from which I benefitted greatly (see the References section). The commutative diagrams were prepared using the program *diagrams.sty* developed by Paul Taylor, who kindly answered technical questions on its use.

Needless to say, any errors or other shortcomings in the book are solely the responsibility of the author. I am most interested in receiving your comments, which can be e-mailed to me at *stephennewman@telus.net*. The inevitable corrections to follow will be posted and periodically updated on the websites *http://www.stephennewman.net* and *ftp://ftp.wiley.com/public/sci_tech_med/galois_theory*.

Finally, and most importantly, I want to thank my wife, Sandra, for her steadfast support and encouragement throughout the writing of the manuscript. It is to her, with love, that this book is dedicated.

CHAPTER 1

CLASSICAL FORMULAS

The historical backdrop to this book is the search for methods of solving polynomial equations by radicals, a challenge embraced by many of the greatest mathematicians of the past. There are polynomial equations of any given degree n that can be solved in this way. For example, $x^n - 2 = 0$ has such a solution, usually denoted by the symbol $\sqrt[n]{2}$. The question that arises is whether there is a solution by radicals of the so-called *general equation* of degree n,

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where the coefficients $a_0, a_1, \ldots, a_n$ are indeterminates. When a solution exists, it provides a "formula" into which numeric coefficients can be substituted for specific cases. The *quadratic formula* for second degree equations is no doubt familiar to the reader (see the following discussion).

In fact, methods of solving quadratic equations were known to the Babylonians as long ago as 2000 B.C. The book *Al Kitab Al Jabr Wa'al Muqabelah* by the Persian mathematician Mohammad ibn Musa al-Khwarizmi appeared around 830 A.D. In this work, the title of which gives us the word "algebra," techniques available at that time for solving quadratic equations were systematized. Around 1079, the Persian mathematician and poet Omar Khayyam (of *Rubaiyat* fame) presented a geometric method for solving certain cubic (third degree) equations.

An algebraic solution of a particular type of cubic equation was discovered by the Italian mathematician Scipione del Ferro (1465–1526) around 1515, but

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

this accomplishment was not published in his lifetime. About 1535, a more complete set of solutions was developed by the Italian mathematician Niccolo Fontana (*ca* 1500–1557), nicknamed "Tartaglia" (the "Stammerer"). These results were further developed by another Italian mathematician, Girolamo Cardano (1501–1576), who published them in his book *Artis Magnae, Sive de Regulis Algebraicis* (*The Great Art, or the Rules of Algebra*), which appeared in 1545. The solution of the quartic (fourth degree) equation was discovered by yet another Italian mathematician, Ludovico Ferrari (1522–1565), a pupil of Cardano.

The next challenge faced by the mathematical scholars of the Renaissance was to find the solution of the quintic (fifth degree) equation. Since the quadratic, cubic, and quartic equations had given up their secrets, there was every reason to believe that with sufficient effort and ingenuity the same would be true of the quintic. Yet, despite the efforts of some of the greatest mathematicians of Europe over the ensuing two centuries, the quintic equation remained stubbornly resistant. In 1770, the Italian mathematician Joseph-Louis Lagrange (1736–1813, born Giussepe Lodovico Lagrangia) published his influential *Réflexions sur la résolution algébrique des équations.* In this journal article of over 200 pages, Lagrange methodically analyzed the known techniques of solving polynomial equations. The principles uncovered by Lagrange, along with his introduction of what would ultimately become group theory, opened up an entirely new approach to the problem of solving polynomial equations by radicals.

Nevertheless, the methods developed by Lagrange did not lead to a solution of the general quintic. In 1801, the eminent German mathematician and scientist Carl Friedrich Gauss (1777–1855) published *Disquisitiones Arithmeticae* (*Number Research*), a landmark in which he demonstrated, among other things, that for any degree n, the roots of the polynomial equation $x^n - 1 = 0$ can be expressed in terms of radicals. Despite this success, it seems that Gauss was of the opinion that the general quintic equation could not be solved by radicals.

This was certainly the view held by the Italian mathematician and physician Paolo Ruffini (1765–1822), who published a treatise of over 500 pages on the topic in 1799. An important feature of his work was the extensive use of group theory, albeit in what would now be considered rudimentary form. Although specific objections to the proofs Ruffini presented were not forthcoming, there seems to have been a reluctance on the part of the mathematical community to accept his claims. Perhaps this was related to the novelty of his approach, or maybe it was simply because his proofs were excessively complex, and therefore suspect. Over the years, Ruffini greatly simplified his methods, but his arguments never seemed to achieve widespread approval, at least not during his lifetime. A notable exception was the French mathematician Augustin-Louis Cauchy (1789–1857), who was supportive of Ruffini and an early contributor to the development of group theory.

In any event, the matter was definitively settled by the Norwegian mathematician Niels Henrik Abel (1802–1829) with the publication in 1824 of a succinct and accessible proof showing that it is impossible to solve the general quintic

equation by radicals. This result, along with its various generalizations, will be referred to here as the *Impossibility Theorem*. As remarkable as this achievement was, the methods used by Abel shed relatively little light on *why* the quintic equation is insolvable.

This question was answered in a spectacular manner by the French mathematician Évariste Galois (1811–1832). In fact, his approach encompasses not only general polynomial equations but also the more complicated case where the coefficients of the polynomial are numeric. In the manuscript *Mémoire sur les conditions de résolubilité des équations par radicaux,* submitted to the Paris Academy of Sciences when he was just 18 years of age, and published posthumously 14 years after his tragic death, Galois provides the foundations for what would become the mathematical discipline with which his name has become synonymous.

This book presents an introduction to Galois theory along both classical and modern lines, with a focus on questions related to the solvability of polynomial equations by radicals. The classical content includes theorems on polynomials, fields, and groups due to such luminaries as Gauss, Kronecker, Lagrange, Ruffini, and, of course, Galois. These results figured prominently in earlier expositions of Galois theory but seem to have gone out of fashion. This is unfortunate because, aside from being of intrinsic mathematical interest, such material provides powerful motivation for the more modern treatment of Galois theory presented later in this book.

Over the course of the book, three versions of the Impossibility Theorem are presented. The first relies entirely on polynomials and fields, the second incorporates a limited amount of group theory, and the third takes full advantage of modern Galois theory. This progression through methods that involve more and more group theory characterizes the first part of the book. The latter part of the book is devoted to topics that illustrate the power of Galois theory as a theoretical and computational tool, but again in the context of solvability of polynomial equations by radicals.

In this chapter, we derive the classical formulas for solving quadratic, cubic, and quartic polynomial equations by radicals. It is assumed that the polynomials have coefficients in $\mathbb{Q}$, the field of rational numbers. This choice of underlying field is made for the sake of concreteness, but the arguments to follow apply equally to "general" polynomials as defined in Chapter 7. The discussion presented here is somewhat informal. In Chapter 2 and later in the book, we introduce concepts that allow the material given below to be made more rigorous. Suggestions for further reading on the material in this chapter, and other portions of the book devoted to classical topics, can be found in Appendix F.

1.1 QUADRATIC POLYNOMIALS

Let

$$f(x) = x^2 - ax + b \tag{1.1}$$

be a quadratic polynomial with coefficients in $\mathbb{Q}$. A *root* of $f(x)$ is an element α (in some field) such that $f(\alpha) = 0$. It is a fundamental result that, since $f(x)$ has degree 2, there are precisely two such roots, which we denote by α_1 and α_2. Consequently, $f(x)$ can be expressed as

$$f(x) = (x - \alpha_1)(x - \alpha_2). \tag{1.2}$$

The roots of $f(x)$ are given by the *quadratic formula*:

$$\alpha_1, \alpha_2 = \frac{a \pm \sqrt{a^2 - 4b}}{2}. \tag{1.3}$$

Here and throughout, the notation $\pm$ is to be interpreted as follows: α_1 corresponds to the $+$ sign and α_2 to the $-$ sign. Accordingly, (1.3) is equivalent to

$$\alpha_1 = \frac{a + \sqrt{a^2 - 4b}}{2} \quad \text{and} \quad \alpha_2 = \frac{a - \sqrt{a^2 - 4b}}{2}.$$

A corresponding interpretation is given to the notation $\mp$.

To derive (1.3), we substitute $x = y + a/2$ into (1.1), producing the so-called *reduced quadratic polynomial*

$$g(y) = y^2 + p$$

where

$$p = -\frac{a^2}{4} + b.$$

The roots of $g(y)$ are

$$\beta_1, \beta_2 = \pm\sqrt{-p} = \frac{\pm\sqrt{a^2 - 4b}}{2}.$$

Setting $\beta_i = \alpha_i - a/2$ for $i = 1, 2$, gives (1.3). It is readily verified that (1.2) holds:

$$f(x) = \left(x - \frac{a + \sqrt{a^2 - 4b}}{2}\right)\left(x - \frac{a - \sqrt{a^2 - 4b}}{2}\right). \tag{1.4}$$

When $\alpha_1 = \alpha_2$, we say that $f(x)$ has a *repeated root*. The preceding statement that $f(x)$ has two roots remains true, provided that we take the repetition of roots into account.

The quantity $a^2 - 4b$ is referred to as the *discriminant* of $f(x)$ and is denoted by $\text{disc}(f)$. We have from (1.3) that

$$\text{disc}(f) = a^2 - 4b = (\alpha_1 - \alpha_2)^2. \tag{1.5}$$

Thus, $f(x)$ has a repeated root if and only if $\text{disc}(f) = 0$. In this case, the repeated root is $\alpha_1 = \alpha_2 = a/2$, and (1.4) becomes

$$f(x) = \left(x - \frac{a}{2}\right)^2. \tag{1.6}$$

This gives us a way of deciding whether a quadratic polynomial has a repeated root based solely on its coefficients. We will see a significant generalization of this finding in Chapter 3.

The symbol $\sqrt{a^2 - 4b}$ deserves a comment. In the absence of further conditions, $\sqrt{a^2 - 4b}$ represents either of the two roots of $x^2 - (a^2 - 4b)$. When $a^2 - 4b > 0$, $\sqrt{a^2 - 4b}$ is a real number, and it is common practice to take $\sqrt{a^2 - 4b}$ to be the positive square root of $a^2 - 4b$. To take a simpler example, $\sqrt{2}$ is typically regarded as the positive square root of 2, that is, $\sqrt{2} = 1.414\ldots$ The negative square root of 2 is then $-\sqrt{2} = -1.414\ldots$ The distinction between the positive and negative square roots of 2 rests on metric properties of real numbers. In this book, we are focused almost exclusively on algebraic matters. Accordingly, unless otherwise indicated, $\sqrt{2}$ stands for either the positive or negative square root of 2. Expressed differently but more algebraically, $\sqrt{2}$ represents either of the roots of $x^2 - 2$. As such, we are not obligated to specify whether $\sqrt{2}$ equals $1.414\ldots$ or $-1.414\ldots$, only that it is one of these two quantities; by default, $-\sqrt{2}$ is the other. Returning to $\sqrt{a^2 - 4b}$, we observe that switching from one root of $x^2 - (a^2 - 4b)$ to the other merely interchanges the values of α_1 and α_2, leaving us with the same two roots of $f(x)$.

1.2 CUBIC POLYNOMIALS

Let

$$f(x) = x^3 - ax^2 + bx - c \tag{1.7}$$

be a cubic polynomial with coefficients in $\mathbb{Q}$. Consistent with the quadratic case, $f(x)$ has three roots, which we denote by α_1, α_2, and α_3. To find formulas for these roots, we resort to a series of *ad hoc* devices. First, we eliminate the quadratic term in (1.7) by making the substitution $x = y + a/3$. This produces the *reduced cubic polynomial*

$$g(y) = y^3 + py + q \tag{1.8}$$

where

$$p = \frac{-a^2}{3} + b \quad \text{and} \quad q = \frac{-2a^3}{27} + \frac{ab}{3} - c.$$

Denote the roots of $g(y)$ by β_1, β_2, and β_3, where $\beta_i = \alpha_i - a/3$ for $i = 1, 2, 3$. Next, substitute

$$y = \frac{1}{3}\left(z - \frac{3p}{z}\right) \tag{1.9}$$

into (1.8) and obtain

$$\frac{z^6 + 27qz^3 - 27p^3}{z^6}$$

where z is assumed to be nonzero. The roots of $g(y)$ can be determined by first finding the roots of

$$r(z) = z^6 + 27qz^3 - 27p^3 \tag{1.10}$$

and then reversing the substitution (1.9). Observing that $r(z)$ is a quadratic polynomial in z^3, it follows that the roots of $r(z)$ are the same as the roots of

$$z^3 - 27\left(-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}\right).$$

Let

$$\lambda_1, \lambda_2 = 3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \tag{1.11}$$

where, in keeping with (1.9), λ_1 and λ_2 are chosen so that

$$\lambda_1\lambda_2 = -3p. \tag{1.12}$$

By definition, the *cube roots of unity* are the roots of the polynomial

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

In particular, the roots of $x^2 + x + 1$ are

$$\omega, \omega^2 = \frac{-1 \pm i\sqrt{3}}{2} \tag{1.13}$$

where, as usual, $i = \sqrt{-1}$. In (1.13), we take $\sqrt{3}$ to be the positive square root of 3. The notation ω will be reserved for $(-1 + i\sqrt{3})/2$ for the rest of the book. We note in passing that

$$\omega^2 + \omega + 1 = 0. \tag{1.14}$$

It follows that the roots of $r(z)$ are

$$\lambda_1 \quad \omega\lambda_1 \quad \omega^2\lambda_1 \quad \lambda_2 \quad \omega\lambda_2 \quad \text{and} \quad \omega^2\lambda_2.$$

At first glance, it appears that the cubic polynomial $g(y)$ also has six roots, which is impossible. However, because of (1.12), the following identities hold:

$$\begin{aligned}
\frac{1}{3}\left(\lambda_1 - \frac{3p}{\lambda_1}\right) &= \frac{\lambda_1 + \lambda_2}{3} = \frac{1}{3}\left(\lambda_2 - \frac{3p}{\lambda_2}\right) \\
\frac{1}{3}\left(\omega^2\lambda_1 - \frac{3p}{\omega^2\lambda_1}\right) &= \frac{\omega^2\lambda_1 + \omega\lambda_2}{3} = \frac{1}{3}\left(\omega\lambda_2 - \frac{3p}{\omega\lambda_2}\right) \\
\frac{1}{3}\left(\omega\lambda_1 - \frac{3p}{\omega\lambda_1}\right) &= \frac{\omega\lambda_1 + \omega^2\lambda_2}{3} = \frac{1}{3}\left(\omega^2\lambda_2 - \frac{3p}{\omega^2\lambda_2}\right).
\end{aligned}$$

The three roots of $g(x)$ are therefore

$$\begin{aligned}
\beta_1 &= \frac{\lambda_1 + \lambda_2}{3} \\
\beta_2 &= \frac{\omega^2\lambda_1 + \omega\lambda_2}{3} \\
\beta_3 &= \frac{\omega\lambda_1 + \omega^2\lambda_2}{3}.
\end{aligned} \tag{1.15}$$

Substituting from (1.11), we obtain

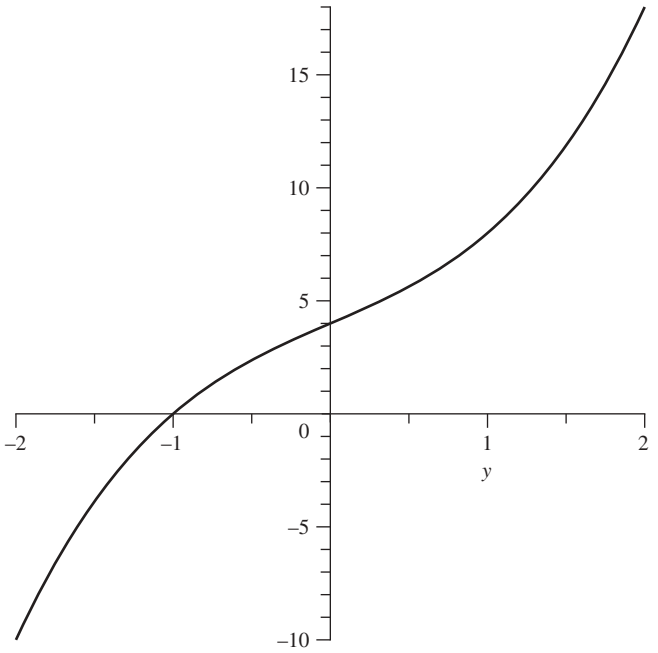
$$\begin{aligned}
\beta_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \\
\beta_2 &= \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \\
\beta_3 &= \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}
\end{aligned} \tag{1.16}$$

which are known as *Cardan's formulas*.

Example 1.1. Setting $p = 3$ and $q = 4$, we have

$$g(y) = y^3 + 3y + 4.$$

The graph of $g(y)$ is shown below.



Clearly, $g(y)$ has one real root, hence two nonreal complex roots. As suggested by the graph, the real root is -1. We have from (1.16) that

$$\begin{aligned}
\beta_1 &= \sqrt[3]{-2+\sqrt{5}} + \sqrt[3]{-2-\sqrt{5}} \\
\beta_2 &= \omega^2\sqrt[3]{-2+\sqrt{5}} + \omega\sqrt[3]{-2-\sqrt{5}} \\
\beta_3 &= \omega\sqrt[3]{-2+\sqrt{5}} + \omega^2\sqrt[3]{-2-\sqrt{5}}.
\end{aligned} \tag{1.17}$$

The roots of $x^2 - 5$ are $\sqrt{5}$ and $-\sqrt{5}$, and the three roots of $x^3 + 2 - \sqrt{5}$ are

$$\sqrt[3]{-2+\sqrt{5}} \qquad \omega\sqrt[3]{-2+\sqrt{5}} \quad \text{and} \quad \omega^2\sqrt[3]{-2+\sqrt{5}}.$$

We now take $\sqrt{5}$ and $\sqrt[3]{-2+\sqrt{5}}$ to be positive real numbers. For (1.12) to be satisfied, $\sqrt[3]{-2-\sqrt{5}} = -\sqrt[3]{2+\sqrt{5}}$ must be a negative real number. It can be

shown that

$$\sqrt[3]{-2+\sqrt{5}} = \frac{-1+\sqrt{5}}{2} \quad \text{and} \quad \sqrt[3]{2+\sqrt{5}} = \frac{1+\sqrt{5}}{2}.$$

Using (1.13) and (1.14), we can simplify (1.17) to

$$\beta_1 = -1 \quad \text{and} \quad \beta_2, \beta_3 = \frac{1 \mp i\sqrt{15}}{2}. \tag{1.18}$$

Alternatively, since -1 is a root of $g(y)$, we have

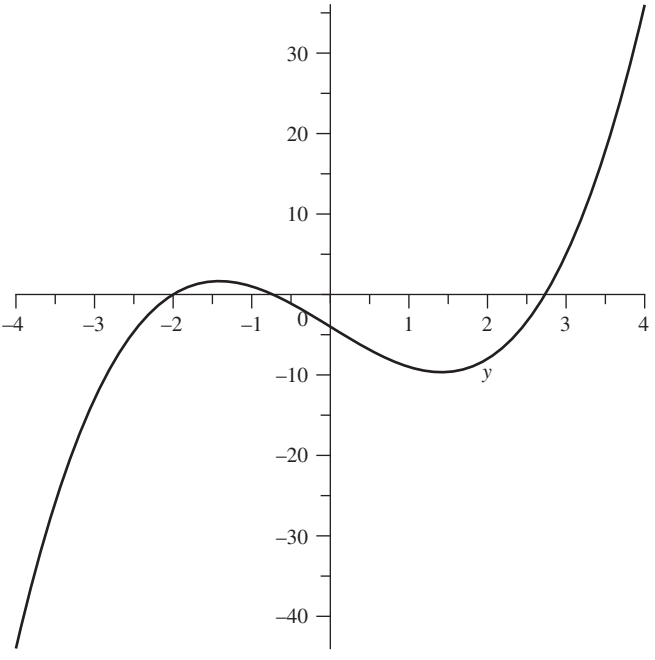
$$g(y) = (y+1)(y^2 - y + 4)$$

which again leads to (1.18). ◊

Example 1.2. Setting $p = -6$ and $q = -4$, we have

$$g(y) = y^3 - 6y - 4.$$

The graph of $g(y)$ is shown below.



Evidently, $g(y)$ has three real roots, and as suggested by the graph, one of them is -2. Then (1.16) yields

$$\begin{aligned}\beta_1 &= \sqrt[3]{2+2i} + \sqrt[3]{2-2i}\\ \beta_2 &= \omega^2\sqrt[3]{2+2i} + \omega\sqrt[3]{2-2i}\\ \beta_3 &= \omega\sqrt[3]{2+2i} + \omega^2\sqrt[3]{2-2i}.\end{aligned} \tag{1.19}$$

The appearance of (1.19) is surprising, given that each of β_1, β_2, and β_3 is a real number. However, it can be shown that

$$\sqrt[3]{2+2i} = -1+i \quad \text{and} \quad \sqrt[3]{2-2i} = -1-i.$$

This makes it possible to simplify (1.19) to

$$\beta_1 = -2 \quad \text{and} \quad \beta_2, \beta_3 = 1 \pm \sqrt{3}. \tag{1.20}$$

Alternatively, since -2 is a root of $g(y)$, we have

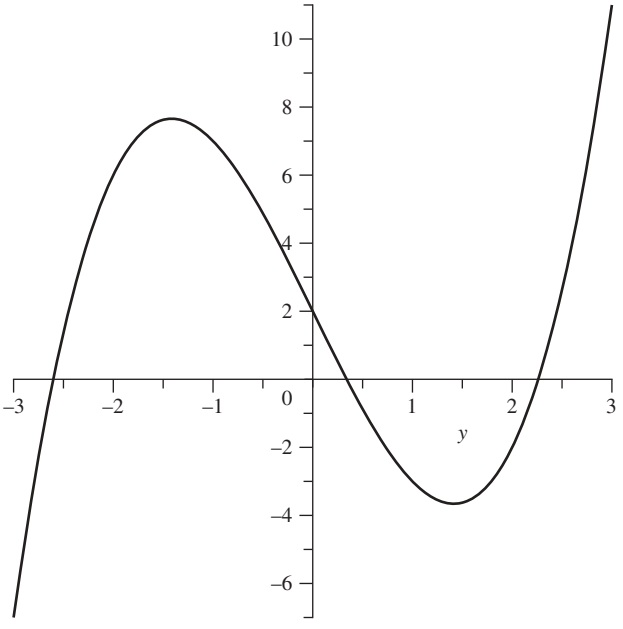
$$g(y) = (y+2)(y^2 - 2y - 2)$$

from which (1.20) results. ◊

Example 1.3. Setting $p = -6$ and $q = 2$, we have

$$g(y) = y^3 - 6y + 2.$$

The graph of $g(y)$ is shown below.



We see that $g(y)$ has three real roots, but this time the numerical value of a root is not empirically obvious. According to (1.16),

$$\beta_1 = \sqrt[3]{-1+i\sqrt{7}} + \sqrt[3]{-1-i\sqrt{7}}$$

$$\beta_2 = \omega^2\sqrt[3]{-1+i\sqrt{7}} + \omega\sqrt[3]{-1-i\sqrt{7}}$$

$$\beta_3 = \omega\sqrt[3]{-1+i\sqrt{7}} + \omega^2\sqrt[3]{-1-i\sqrt{7}}.$$

It is reasonable to expect that, just as in Example 1.2, we should be able to express β_1, β_2, and β_3 entirely in terms of real numbers. Surprisingly, it is *not* possible to do so, as will follow from Theorem 6.21. This counterintuitive result is an example of a classical problem called the *Casus Irreducibilis* (Irreducible Case). ♢

1.3 QUARTIC POLYNOMIALS

Let

$$f(x) = x^4 - ax^3 + bx^2 - cx + d \tag{1.21}$$

be a quartic polynomial with coefficients in $\mathbb{Q}$, and denote its roots by α_1, α_2, α_3, and α_4. Analogous to the approach used to solve the quadratic and cubic polynomials, we begin by substituting $x = y + a/4$ into (1.21) and obtain the *reduced quartic polynomial*

$$g(y) = y^4 + py^2 + qy + r$$

where

$$p = \frac{-3a^2}{8} + b \qquad q = \frac{-a^3}{8} + \frac{ab}{2} - c$$

and

$$r = \frac{-3a^4}{256} + \frac{a^2b}{16} - \frac{ac}{4} + d.$$

Denote the roots of $g(y)$ by β_1, β_2, β_3, and β_4, where $\beta_i = \alpha_i - a/4$ for $i = 1, 2, 3, 4$. To find the roots of $g(y)$, we again resort to a series of contrivances. First, rewrite $g(y) = 0$ as

$$y^4 = -py^2 - qy - r. \tag{1.22}$$

Let θ_1 be a "quantity," as yet unspecified, and add $\theta_1 y^2 + \theta_1^2/4$ to both sides of (1.22) to obtain

$$\left(y^2 + \frac{\theta_1}{2}\right)^2 = (\theta_1 - p)\left[y^2 - \left(\frac{q}{\theta_1 - p}\right)y + \frac{\theta_1^2 - 4r}{4(\theta_1 - p)}\right]. \tag{1.23}$$

We assume for the moment that $\theta_1 \neq p$ and view the expression in square brackets in (1.23) as a polynomial in y. As remarked in Section 1.1, this polynomial will be a square if its discriminant

$$\left(\frac{q}{\theta_1 - p}\right)^2 - 4\left[\frac{\theta_1^2 - 4r}{4(\theta_1 - p)}\right] = \frac{-(\theta_1^3 - p\theta_1^2 - 4r\theta_1 + 4pr - q^2)}{(\theta_1 - p)^2}$$

equals 0. Accordingly, we now require θ_1 to be an arbitrary but fixed root of

$$s(z) = z^3 - pz^2 - 4rz + 4pr - q^2. \tag{1.24}$$

Cardan's formulas can be used to find an explicit expression for θ_1. In view of (1.6), we can now rewrite (1.23) as

$$\left(y^2 + \frac{\theta_1}{2}\right)^2 = (\theta_1 - p)\left[y - \frac{q}{2(\theta_1 - p)}\right]^2. \tag{1.25}$$

Define ϕ_1 by setting

$$\phi_1^2 = 4(\theta_1 - p). \tag{1.26}$$

Then (1.25) becomes

$$\left[y^2 + \left(\frac{\phi_1^2}{8} + \frac{p}{2}\right)\right]^2 = \left[\left(\frac{\phi_1}{2}\right)y - \frac{q}{\phi_1}\right]^2.$$

This is equivalent to the pair of quadratic equations

$$\begin{aligned} y^2 + \left(\frac{\phi_1^2}{8} + \frac{p}{2}\right) &= \left(\frac{\phi_1}{2}\right)y - \frac{q}{\phi_1} \\ y^2 + \left(\frac{\phi_1^2}{8} + \frac{p}{2}\right) &= -\left(\frac{\phi_1}{2}\right)y + \frac{q}{\phi_1} \end{aligned}$$

which we rewrite as

$$\begin{aligned} y^2 - \left(\frac{\phi_1}{2}\right)y + \left(\frac{\phi_1^2}{8} + \frac{p}{2} + \frac{q}{\phi_1}\right) &= 0 \\ y^2 + \left(\frac{\phi_1}{2}\right)y + \left(\frac{\phi_1^2}{8} + \frac{p}{2} - \frac{q}{\phi_1}\right) &= 0 \end{aligned} \tag{1.27}$$

respectively.

Denote the roots of the first equation in (1.27) by β_1 and β_2, and those of the second by β_3 and β_4. We then have

$$\begin{aligned}\beta_1, \beta_2 &= \frac{\phi_1}{4} \pm \frac{1}{2}\sqrt{-\frac{\phi_1^2}{4} - 2p - \frac{4q}{\phi_1}} \\ \beta_3, \beta_4 &= -\frac{\phi_1}{4} \pm \frac{1}{2}\sqrt{-\frac{\phi_1^2}{4} - 2p + \frac{4q}{\phi_1}}\end{aligned} \tag{1.28}$$

which will be referred to as *Ferrari's formulas*. Note that if we replace ϕ_1 with $-\phi_1$ in (1.28), we obtain the same roots for $g(y)$ but with the rows of (1.28) reversed.

It remains to consider the case $\theta_1 = p$. In this situation, (1.24) becomes

$$s(z) = z^3 - \theta_1 z^2 - 4rz + 4\theta_1 r - q^2.$$

Then $s(\theta_1) = 0$ implies that $q = 0$, hence $g(y) = y^4 + py^2 + r$. This is a quadratic polynomial in y^2, the roots of which are easily found.

Example 1.4 (5th root of unity). Consider the polynomial

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

The reason for the choice of notation will be made clear in Chapter 5. We return to $\Phi_5(x)$ several times later in the book. To give $\Phi_5(x)$ a more familiar interpretation, observe that

$$x^5 - 1 = (x - 1)\Phi_5(x).$$

In the terminology of Chapter 5, the roots of $x^5 - 1$ are the 5th roots of unity. More specifically, the roots of $\Phi_5(x)$ are ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4, where

$$\zeta_5 = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right).$$

The reduced polynomial corresponding to $\Phi_5(x)$ is

$$g(y) = y^4 + \left(\frac{5}{8}\right)y^2 + \left(\frac{5}{8}\right)y + \frac{205}{256}.$$

In the above notation,

$$s(z) = z^3 - \left(\frac{5}{8}\right)z^2 - \left(\frac{205}{64}\right)z + \frac{825}{512}.$$

The reduced polynomial corresponding to $s(z)$ is

$$h(y) = y^3 - \left(\frac{10}{3}\right)y + \frac{25}{27}.$$

Using Cardan's formulas, we find that $h(y)$ has the roots

$$\frac{5}{3} \quad \text{and} \quad -\frac{5}{6} \pm \frac{\sqrt{5}}{2}.$$

It follows that the roots of $s(z)$ are

$$\frac{15}{8} \quad \text{and} \quad -\frac{5}{8} \pm \frac{\sqrt{5}}{2}.$$

The respective values of ϕ_1 are

$$\sqrt{5} \quad \text{and} \quad \sqrt{-5 \pm 2\sqrt{5}}.$$

Choosing $\phi_1 = \sqrt{5}$ and taking all square roots to be positive, we find from Ferrari's formulas that the roots of $\Phi_5(x)$ are

$$\begin{aligned} \zeta_5, \zeta_5^4 &= \frac{-1 + \sqrt{5} \pm i\sqrt{10 + 2\sqrt{5}}}{4} \\ \zeta_5^2, \zeta_5^3 &= \frac{-1 - \sqrt{5} \pm i\sqrt{10 - 2\sqrt{5}}}{4}. \end{aligned} \tag{1.29}$$

In (1.29), the assignment of the powers of ζ_5 to their expressions in terms of radicals was made on the basis of their respective numerical values. ◊

CHAPTER 2

POLYNOMIALS AND FIELD THEORY

This chapter provides the background material on polynomials and fields needed as a foundation for the remainder of the book. We begin with a few remarks on notation. The ring of integers will be denoted by $\mathbb{Z}$, and the fields of rational, real, and complex numbers by $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. The letters E, F, K, and L will always denote fields; x, y, and z will always denote indeterminates; and m and n will always denote integers, usually natural numbers.

Recall that a field F has *characteristic* 0 if for all natural numbers n,

$$1 + 1 + \cdots + 1 \neq 0. \qquad [n \text{ terms}]$$

Otherwise F is said to have nonzero characteristic. Any field of characteristic 0 contains an isomorphic copy of $\mathbb{Q}$. If F has nonzero characteristic, then the smallest natural number n violating the characteristic 0 property is a prime, say p. In this case, F is said to have *characteristic* p. Up to isomorphism, there is a unique field $\mathbb{F}_p$ of p elements, and it has characteristic p. We adopt the following convention:

With the exception of $\mathcal{F}$ in Theorem E.3, all fields other than $\mathbb{F}_p$ are assumed to have characteristic 0.

Most of the results to follow do not require such a strong assumption, but we proceed on this basis as a matter of convenience, and because it is the classical case.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

2.1 DIVISIBILITY

We denote by $F[x]$ the ring of polynomials in x with coefficients in the field F. An element $f(x)$ of $F[x]$ is said to be a polynomial *over* F. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

For convenience of notation, we sometimes denote $f(x)$ by f. *By writing* $f(x)$ *in this manner, it is implicit, here and throughout, that* $a_n \neq 0$*, except when* $n = 0$ *and* $a_0 = 0$. We refer to a_n as the *leading coefficient* of $f(x)$. If $a_n = 1$, $f(x)$ is said to be a *monic polynomial*. When $n = 0$, in which case $f(x) = a_0$, we say that $f(x)$ is a *constant polynomial*. If $f(x)$ is a constant polynomial and $a_0 = 0$, that is, $f(x) = 0$, we refer to $f(x)$ as the *zero polynomial*. (It will be clear from the context when the expression $f(x) = 0$ is meant to indicate that $f(x)$ is the zero polynomial, and when it represents a nonzero polynomial equation to be "solved" for x.)

If $f(x)$ is a nonzero polynomial, its *degree* is defined to be $\deg(f) = n$. In particular, the degree of a nonzero constant polynomial is 0. *The degree of the zero polynomial is not defined*. Let $g(x)$ be a nonzero polynomial in $F[x]$. We say that $g(x)$ *divides* $f(x)$, or that $g(x)$ is a *divisor* of $f(x)$, if there is a polynomial $h(x)$ in $F[x]$ such that $f(x) = g(x)h(x)$.

Theorem 2.1 (Division Algorithm). Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r) < \deg(g)$ or $r(x) = 0$. If $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ and $g(x)$ is monic, then $q(x)$ and $r(x)$ are also in $\mathbb{Z}[x]$.

Proof. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Recall the convention that $a_n, b_m \neq 0$. If $m > n$, we set $q(x) = 0$ and $r(x) = f(x)$. For $m \leq n$, the proof is by induction on n. Suppose that $n = 0$. Then $m = 0$, hence $f(x) = a_0 \neq 0$ and $g(x) = b_0 \neq 0$. In this case, we set $q(x) = a_0/b_0$ and $r(x) = 0$. Now, assume that $n \geq 1$ and let

$$h(x) = f(x) - \left(\frac{a_n}{b_m}\right) x^{n-m} g(x).$$

Clearly, $\deg(h) < n$. By the induction hypothesis, there are polynomials $s(x)$ and $r(x)$ in $F[x]$ such that $h(x) = s(x)g(x) + r(x)$, with $\deg(r) < \deg(g)$ or $r(x) = 0$. Setting

$$q(x) = s(x) + \left(\frac{a_n}{b_m}\right) x^{n-m}$$

we have $f(x) = q(x)g(x) + r(x)$, with $\deg(r) < \deg(g)$ or $r(x) = 0$. It is clear that $q(x)$ is in $F[x]$.

To show uniqueness, suppose that $q'(x)$ and $r'(x)$ satisfy the above conditions. It follows from $f(x) = q'(x)g(x) + r'(x)$ that

$$r(x) - r'(x) = [q'(x) - q(x)]g(x).$$

Suppose that $q(x) - q'(x) \neq 0$. Using well-known properties of the degree of a polynomial, we find that

$$\deg(g) \leq \deg(q' - q) + \deg(g) = \deg(r - r') \leq \max\{\deg(r), \deg(r')\}.$$

This contradiction shows that $q(x) = q'(x)$, hence $r(x) = r'(x)$.

The second assertion is demonstrated similarly using an inductive argument. Briefly, suppose that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ and that $g(x)$ is monic. Then $h(x)$ is in $\mathbb{Z}[x]$, and by the induction hypothesis, so are $s(x)$ and $r(x)$. Therefore, so is $q(x)$. □

We refer to $q(x)$ and $r(x)$ in the Division Algorithm as the *quotient* and *remainder*, respectively, of the division of $f(x)$ by $g(x)$. In the above definition of what it means for a polynomial $f(x)$ in $F[x]$ to have a polynomial $g(x)$ in $F[x]$ as a divisor, we required the existence of a polynomial $h(x)$ in $F[x]$ such that $f(x) = g(x)h(x)$. In light of the Division Algorithm, we see that specifying that $h(x)$ is a polynomial in $F[x]$ is unnecessary.

Let $f(x)$ and $g(x)$ be polynomials in $F[x]$. We say that a polynomial $h(x)$ in $F[x]$ is a *greatest common divisor* of $f(x)$ and $g(x)$ if $h(x)$ divides $f(x)$ and $g(x)$ and if, in addition, $h(x)$ is divisible by every polynomial in $F[x]$ that divides $f(x)$ and $g(x)$. In the trivial case where $g(x) = 0$, $f(x)$ itself is a greatest common divisor of $f(x)$ and $g(x)$. Suppose that $h'(x)$ is another greatest common divisor of $f(x)$ and $g(x)$. Then $h(x)$ and $h'(x)$ divide each other, which means that $h(x)$ equals $h'(x)$ multiplied by some element of F. It follows that if $f(x)$ and $g(x)$ have a greatest common divisor, then there is a unique greatest common divisor that is monic. We refer to this polynomial as *the* greatest common divisor of $f(x)$ and $g(x)$, and denote it by $\gcd(f, g)$.

Theorem 2.2 (Euclidean Algorithm). Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$. Then $\gcd(f, g)$ exists, and there are polynomials $s(x)$ and $t(x)$ in

$F[x]$ such that

$$\gcd(f, g) = s(x)f(x) + t(x)g(x).$$

Proof. The Euclidean Algorithm relies on repeated applications of the Division Algorithm. Without loss of generality, we may assume that $\deg(g) \leq \deg(f)$. For step 1, divide $f(x)$ by $g(x)$ and obtain the remainder $r_1(x)$. If $r_1(x) = 0$, the process stops. Otherwise, for step 2, divide $g(x)$ by $r_1(x)$ and obtain the remainder $r_2(x)$. If $r_2(x) = 0$, the process stops. Otherwise, for step 3, divide $r_1(x)$ by $r_2(x)$ and obtain the remainder $r_3(x)$, and so on. Since the degrees of successive remainders are strictly decreasing, after a finite number of steps the process produces a zero remainder. The steps involved are as follows:

$$\begin{array}{lll}
f = q_1 g + r_1 & \deg(r_1) < \deg(g) & [\text{step } 1] \\
g = q_2 r_1 + r_2 & \deg(r_2) < \deg(r_1) & [\text{step } 2] \\
r_1 = q_3 r_2 + r_3 & \deg(r_3) < \deg(r_2) & [\text{step } 3] \\
\vdots & \vdots & \vdots \\
r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} & \deg(r_{n-1}) < \deg(r_{n-2}) & [\text{step } n-1] \\
r_{n-2} = q_n r_{n-1} + r_n & \deg(r_n) < \deg(r_{n-1}) & [\text{step } n] \\
r_{n-1} = q_{n+1} r_n & & [\text{step } n+1]
\end{array}$$

We see from step $n + 1$ that $r_n(x)$ divides $r_{n-1}(x)$, and then from step n that $r_n(x)$ divides $r_{n-2}(x)$, and so on, until from steps 2 and 1 that $r_n(x)$ divides $g(x)$ and $f(x)$. Now, suppose that $h(x)$ is a polynomial in $F[x]$ that divides $f(x)$ and $g(x)$. We have from step 1 that $h(x)$ divides $r_1(x)$, and then from step 2 that $h(x)$ divides $r_2(x)$, and so on, until from step n, that $h(x)$ divides $r_n(x)$. Let c be the leading coefficient of $r_n(x)$. Then $\gcd(f, g) = r_n(x)/c$.

To show that $\gcd(f, g) = s(x)f(x) + t(x)g(x)$ for certain polynomials $s(x)$ and $t(x)$ in $F[x]$, rewrite the equations in steps 1 to n as follows:

$$\begin{aligned}
f - q_1 g &= r_1 \\
g &= q_2 r_1 + r_2 \\
0 &= r_1 - q_3 r_2 - r_3 \\
&\vdots \\
0 &= r_{n-4} - q_{n-2} r_{n-3} - r_{n-2} \\
0 &= r_{n-3} - q_{n-1} r_{n-2} - r_{n-1} \\
0 &= r_{n-2} - q_n r_{n-1} - r_n.
\end{aligned}$$

In matrix notation, this becomes

$$\begin{pmatrix} f - q_1 g \\ g \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 0 & 0 & \cdots & 0 & 0 & 0 \\ q_2 & \mathbf{1} & 0 & \cdots & 0 & 0 & 0 \\ 1 & -q_3 & \mathbf{-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{-1} & 0 & 0 \\ 0 & 0 & 0 & \cdots & -q_{n-1} & \mathbf{-1} & 0 \\ 0 & 0 & 0 & \cdots & 1 & -q_n & \mathbf{-1} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_{n-2} \\ r_{n-1} \\ r_n \end{pmatrix}$$

where the elements along the main diagonal are shown in bold. Using Cramer's rule, we have

$$r_n = \frac{\begin{vmatrix} \mathbf{1} & 0 & 0 & \cdots & 0 & 0 & f - q_1 g \\ q_2 & \mathbf{1} & 0 & \cdots & 0 & 0 & g \\ 1 & -q_3 & \mathbf{-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{-1} & 0 & 0 \\ 0 & 0 & 0 & \cdots & -q_{n-1} & \mathbf{-1} & 0 \\ 0 & 0 & 0 & \cdots & 1 & -q_n & \mathbf{0} \end{vmatrix}}{\begin{vmatrix} \mathbf{1} & 0 & 0 & \cdots & 0 & 0 & 0 \\ q_2 & \mathbf{1} & 0 & \cdots & 0 & 0 & 0 \\ 1 & -q_3 & \mathbf{-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{-1} & 0 & 0 \\ 0 & 0 & 0 & \cdots & -q_{n-1} & \mathbf{-1} & 0 \\ 0 & 0 & 0 & \cdots & 1 & -q_n & \mathbf{-1} \end{vmatrix}}$$

where again the elements along the main diagonals are shown in bold. Since the matrix in the denominator is lower triangular, its determinant is simply the product of the elements along the main diagonal, that is, $(-1)^{n-2}$. Expanding the determinant in the numerator along the last column gives

$$r_n(x) = s'(x)f(x) + t'(x)g(x)$$

where $s'(x)$ and $t'(x)$ are polynomials in $F[x]$. Let $s(x) = s'(x)/c$ and $t(x) = t'(x)/c$. Then

$$\gcd(f, g) = s(x)f(x) + t(x)g(x).$$

□

In the notation of Theorem 2.2, when $\gcd(f, g) = 1$, we say that $f(x)$ and $g(x)$ are *relatively prime*. In this important case, there are polynomials $s(x)$ and $t(x)$ in $F[x]$ such that

$$s(x)f(x) + t(x)g(x) = 1.$$

Example 2.3. Consider the polynomials

$$f(x) = (x - 1)(x^3 - 2) = x^4 - x^3 - 2x + 2$$

and

$$g(x) = (x - 1)(x - 3) = x^2 - 4x + 3$$

in $\mathbb{Q}[x]$. We use the Euclidean Algorithm to verify what is apparent from the definitions of $f(x)$ and $g(x)$, namely, that $\gcd(f, g) = x - 1$. Dividing $f(x)$ by $g(x)$ gives $f(x) = q_1(x)g(x) + r_1(x)$, where

$$q_1(x) = x^2 + 3x + 9 \quad \text{and} \quad r_1(x) = 25x - 25.$$

Next, dividing $g(x)$ by $r_1(x)$ yields $g(x) = q_2(x)r_1(x) + r_2(x)$, where

$$q_2(x) = (x - 3)/25 \quad \text{and} \quad r_2(x) = 0.$$

According to the Euclidean Algorithm, $\gcd(f, g)$ equals $r_1(x)$ divided by its leading coefficient, that is, $\gcd(f, g) = x - 1$, as expected. We have from $r_1(x) = f(x) - q_1(x)g(x)$ that

$$\gcd(f, g) = \left(\frac{1}{25}\right) f(x) + \left(\frac{-x^2 - 3x - 9}{25}\right) g(x).$$

◊

When a field F is contained in another field E, we say that F is a *subfield* of E and that E is an *extension* of F. According to these definitions, F is both a subfield and an extension of itself. If K is an extension of E, we say that E is *between* F and K. Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$. Observe that when $f(x)$ and $g(x)$ are viewed as polynomials in $E[x]$, the Division Algorithm produces the same quotient and remainder as when $f(x)$ and $g(x)$ are regarded as polynomials in $F[x]$. Similarly, the Euclidean Algorithm produces the same greatest common divisor. This shows that the Division Algorithm and Euclidean Algorithm are independent of ambient fields.

Let $f(x)$ be a nonconstant polynomial in $F[x]$. An element α in some extension of F is said to be a *root* of $f(x)$ if $f(\alpha) = 0$. *The root of a constant polynomial, including the zero polynomial, is not defined*. At this point, we have no guarantee that there is an extension of F that contains a root of $f(x)$. However, as we show

in Section 2.6, it is a fundamental result that such an extension always exists. In what follows, when we say that an element α "is a root of $f(x)$," it is implicit that α is an element in some (possibly unspecified) extension of F.

Theorem 2.4. Let $f(x)$ be a nonconstant polynomial in $F[x]$, and let α be a root of $f(x)$. Then $x - \alpha$ divides $f(x)$.

Proof. Let E be an extension of F that contains α. By the Division Algorithm, there are polynomials $q(x)$ and $r(x)$ in $E[x]$ such that

$$f(x) = q(x)(x - \alpha) + r(x) \tag{2.1}$$

with $\deg(r) < 1$ or $r(x) = 0$. Therefore, $r(x)$ is a constant polynomial, say, $r(x) = a_0$. Substituting $x = \alpha$ into (2.1) shows that $a_0 = 0$, hence $f(x) = q(x)(x - \alpha)$. □

A nonconstant polynomial $f(x)$ in $F[x]$ is said to be *irreducible* over F if it cannot be written as the product of two polynomials in $F[x]$, each of smaller degree than $f(x)$; otherwise $f(x)$ is said to be *reducible* over F. The requirement that both polynomials in the product have degree less than $\deg(f)$ is crucial because, for any nonzero c in F, we can trivially express $f(x)$ as the product $c[f(x)/c]$. The definition of irreducibility is restricted to nonconstant polynomials in order to have "unique factorization" (Theorem 2.8). Without this requirement, any constant polynomial in $F[x]$ would be irreducible over F, in which case, for example, x and $1x$ would be distinct factorizations of x into polynomials that are "irreducible" over $F[x]$. Unlike the situation with the Division Algorithm and Euclidean Algorithm, irreducibility is intimately connected with the ambient field. For example, $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Q}(\sqrt{2})$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Theorem 2.5. Let $f(x)$ be a nonconstant polynomial in $F[x]$. Then $f(x)$ is irreducible over F if and only if the following property holds: If $f(x)$ divides the product of a finite number of polynomials in $F[x]$, then $f(x)$ divides at least one of them.

Proof. ($\Rightarrow$): Suppose that $f(x)$ divides $g_1(x)g_2(x)\cdots g_n(x)$, where $n \geq 2$ and $g_i(x)$ is a polynomial in $F[x]$ for $i = 1, 2, \ldots, n$. The proof is by induction on n. Let $n = 2$ and suppose that $f(x)$ does not divide $g_1(x)$. Since $\gcd(f, g_1)$ divides $f(x)$, and $f(x)$ is irreducible over F, either $\gcd(f, g_1) = 1$ or $\gcd(f, g_1)$ equals $f(x)$ divided by its leading coefficient. The latter possibility is excluded because $g_1(x)$ is not divisible by $f(x)$. By the Euclidean Algorithm, there are polynomials $s(x)$ and $t(x)$ in $F[x]$ such that $s(x)f(x) + t(x)g_1(x) = 1$, hence

$$s(x)f(x)g_2(x) + t(x)g_1(x)g_2(x) = g_2(x). \tag{2.2}$$

Since $f(x)$ divides both terms on the left-hand side of (2.2), it divides the right-hand side, that is, $f(x)$ divides $g_2(x)$. Now, let $n > 2$, and suppose as before that $f(x)$ does not divide $g_1(x)$. The case $n = 2$ shows that $f(x)$ divides $g_2(x)g_3(x)\cdots g_n(x)$. By the induction hypothesis, $f(x)$ divides $g_i(x)$ for some $2 \le i \le n$.

($\Leftarrow$): Suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $F[x]$. Since $f(x)$ trivially divides $g(x)h(x)$, by assumption, $f(x)$ divides $g(x)$ or $h(x)$. This is impossible unless either $g(x)$ or $h(x)$ has the same degree as $f(x)$. □

Theorem 2.6. Let $f(x)$ be a nonconstant polynomial in $F[x]$, and let α be a root of $f(x)$. Then the following are equivalent:
(a) $f(x)$ is irreducible over F.
(b) $f(x)$ has the smallest degree of any polynomial in $F[x]$ that has α as a root.
(c) $f(x)$ divides any polynomial in $F[x]$ that has α as a root.

Proof. (a)$\Rightarrow$(b): Since $f(x)$ is a nonconstant polynomial in $F[x]$ that has α as a root, there is such a polynomial of minimal degree. Let us denote it by $g(x)$. By the Division Algorithm, there are polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \tag{2.3}$$

with $\deg(r) < \deg(g)$ or $r(x) = 0$. Substituting $x = \alpha$ into (2.3) shows that $r(\alpha) = 0$. The minimal property of $g(x)$ implies that $r(x) = 0$, hence $f(x) = q(x)g(x)$. Since $f(x)$ is irreducible over $F[x]$, and $g(x)$ is a nonconstant polynomial, $q(x)$ must be a constant polynomial. Therefore, $\deg(f) = \deg(g)$.

(b)$\Rightarrow$(c): Let $g(x)$ be a polynomial in $F[x]$ that has α as a root. By the Division Algorithm, there are polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$g(x) = q(x)f(x) + r(x) \tag{2.4}$$

with $\deg(r) < \deg(f)$ or $r(x) = 0$. Substituting $x = \alpha$ into (2.4), we find that $r(\alpha) = 0$. The minimal property of $f(x)$ implies that $r(x) = 0$, hence $g(x) = q(x)f(x)$.

(c)$\Rightarrow$(a): Suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $F[x]$. Since $f(\alpha) = 0$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. Suppose that $g(\alpha) = 0$. By assumption, $f(x)$ divides $g(x)$. Since $f(x)$ and $g(x)$ divide each other, they have the same degree. □

In the notation of Theorem 2.6, if there is a (nonconstant) polynomial in $F[x]$ that has α as a root, then there is a unique (nonconstant) polynomial in $F[x]$ that is monic and of minimal degree among such polynomials in $F[x]$. We denote this polynomial by $\min(\alpha, F)$ and refer to it as the *minimal polynomial* of α over F. The crucial properties of $\min(\alpha, F)$ are that it is irreducible over F and it divides precisely those polynomials in $F[x]$ that have α as a root.

Theorem 2.7. Let $f(x)$ and $g(x)$ be nonconstant monic polynomials in $F[x]$ that are irreducible over F. If $f(x)$ and $g(x)$ have a root in common, then they are equal.

Proof. By Theorem 2.6, $f(x)$ and $g(x)$ divide each other. Since both polynomials are monic, they are equal. □

Let $f(x)$ be a polynomial in $F[x]$, and let

$$f(x) = f_1(x)f_2(x)\cdots f_n(x) \tag{2.5}$$

where $f_i(x)$ is a polynomial in $F[x]$ for $i = 1, 2, \ldots, n$. The product in (2.5) is referred to as a *factorization* of $f(x)$ over F, and each $f_i(x)$ is said to be a *factor*. Observe that this definition permits the trivial factorization where $f(x)$ is the only factor, as well as factorizations where at least some of the $f_i(x)$ are constant polynomials. Even if we exclude these cases, a factorization may not be unique. For example,

$$\begin{aligned} x^3 - 6x^2 + 11x - 6 &= (x-1)(x-2)(x-3) \\ &= (x-1)(x^2 - 5x + 6) \\ &= (x^2 - 3x + 2)(x-3). \end{aligned}$$

As the next result shows, uniqueness of factorization (up to order of factors) can be ensured by requiring the factors to be irreducible.

Theorem 2.8. Let $f(x)$ be a nonconstant polynomial in $F[x]$. Then $f(x)$ has a factorization over F of the form

$$f(x) = ag_1(x)^{d_1}g_2(x)^{d_2}\cdots g_m(x)^{d_m} \tag{2.6}$$

where a is the leading coefficient of $f(x)$, the d_j are natural numbers, and the $g_j(x)$ are distinct (nonconstant) monic polynomials in $F[x]$ that are irreducible over F for $j = 1, 2, \ldots, m$. This factorization is unique up to order of factors.

Proof. If $f(x)$ is irreducible over F, then $a[f(x)/a]$ is the desired factorization. On the other hand, if $f(x)$ is reducible over F, it factors into two nonconstant polynomials in $F[x]$, each of degree less than $\deg(f)$. We repeat the process with each of the constituent polynomials, and so on. Since the factors have progressively smaller degrees, the process terminates in a factorization of the form

$$f(x) = [b_1 s_1(x)][b_2 s_2(x)]\cdots[b_n s_n(x)]$$

where $b_1, b_2, \ldots, b_n$ are in F and $s_1(x), s_2(x), \ldots, s_n(x)$ are (nonconstant) monic polynomials in $F[x]$ that are irreducible over F. Then $a = b_1 b_2 \cdots b_n$, and we have the factorization

$$f(x) = a s_1(x) s_2(x) \cdots s_n(x).$$

We claim that this factorization is unique up to order of factors. The proof is by induction on n. Suppose that

$$f(x) = c t_1(x) t_2(x) \cdots t_l(x)$$

is another such factorization. Clearly, $a = c$. Suppose that $n = 1$. Then

$$s_1(x) = t_1(x) t_2(x) \cdots t_l(x)$$

and by Theorem 2.5, $s_1(x)$ divides one of $t_1(x), t_2(x), \ldots, t_l(x)$, say $t_1(x)$. Since $s_1(x)$ and $t_1(x)$ are both monic and irreducible over F, they are equal. We cannot have $l > 1$, otherwise $t_2(x) t_3(x) \cdots t_l(x) = 1$, which is impossible because each of $t_2(x), t_3(x), \ldots, t_l(x)$ is a nonconstant polynomial. Thus, $l = 1$.

Now, suppose that $n > 1$. Then

$$s_1(x) s_2(x) \cdots s_n(x) = t_1(x) t_2(x) \cdots t_l(x).$$

Again by Theorem 2.5, $s_1(x)$ divides one of $t_1(x), t_2(x), \ldots, t_l(x)$, say $t_1(x)$, and as before, $s_1(x)$ and $t_1(x)$ are equal. We then have

$$s_2(x) s_3(x) \cdots s_n(x) = t_2(x) t_3(x) \cdots t_l(x). \tag{2.7}$$

By the induction hypothesis, the left- and right-hand sides of (2.7) are the same except possibly for the order of factors. This proves the claim.

To complete the proof, we simply collect together identical factors in either of the above factorizations of $f(x)$, which produces a factorization of the form of (2.6). □

2.2 ALGEBRAIC EXTENSIONS

Let α be an element in an extension E of F, and define

$$F[\alpha] = \{f(\alpha) : f(x) \in F[x]\}$$

and

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in F[x]; g(\alpha) \neq 0 \right\}.$$

It is easily verified that $F[\alpha]$ is a ring and $F(\alpha)$ is a field. We say that $F[\alpha]$ and $F(\alpha)$ are *generated* over F by α. Evidently, $F[\alpha]$ is the smallest ring in E that contains F and α; similarly, $F(\alpha)$ is the smallest such field.

We say that α is *algebraic* over F if there is a (nonconstant) polynomial in $F[x]$ that has α as a root; otherwise α is said to be *transcendental* over F. For example, since $\sqrt{2}$ is a root of $x^2 - 2$, it is algebraic over $\mathbb{Q}$. On the other hand, it is well known (but difficult to prove) that the mathematical constants π and e are transcendental over $\mathbb{Q}$. We say that an extension E of F is an *algebraic extension* if every element of E is algebraic over F. Observe that in this case, every element of E has a minimal polynomial over F. In what follows, when we say that an element α "is algebraic over F," it is to be understood that α is an element in some (possibly unspecified) extension of F.

Theorem 2.9. If α is algebraic over F, then $F(\alpha) = F[\alpha]$.

Proof. Clearly, $F[\alpha] \subseteq F(\alpha)$. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$, with $g(\alpha) \neq 0$, and let $h(x) = \min(\alpha, F)$. Then $h(x)$ does not divide $g(x)$, so $\gcd(g, h) = 1$. By the Euclidean Algorithm, there are polynomials $s(x)$ and $t(x)$ in $F[x]$ such that

$$s(x)g(x) + t(x)h(x) = 1. \tag{2.8}$$

Substituting $x = \alpha$ into (2.8) gives $s(\alpha)g(\alpha) = 1$, hence

$$\frac{f(\alpha)}{g(\alpha)} = f(\alpha)s(\alpha).$$

Since $f(x)$ and $g(x)$ were arbitrary, $F(\alpha) \subseteq F[\alpha]$. Therefore, $F(\alpha) = F[\alpha]$. □

2.3 DEGREE OF EXTENSIONS

Let E be an extension of F. An important observation, and one that puts the power of linear algebra at our disposal, is that E can be viewed as a vector space over F. Accordingly, the *degree* of E over F, denoted by $[E : F]$, is defined to be the dimension of E as a vector space over F. We say that E is a *finite extension* of F if $[E : F]$ is finite; otherwise E is said to be an *infinite extension*.

Theorem 2.10. If E is a finite extension of F, then E is an algebraic extension of F.

Proof. Take α in E, and let $n = [E : F]$. Since the $n + 1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over F, there are $b_0, b_1, \ldots, b_n$ in F, not all of which are 0, such that

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

Then

$$f(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

is a nonzero polynomial in $F[x]$ that has α as a root. □

Let α be algebraic over F. We define the *degree* of α over F, denoted by $\deg(\alpha, F)$, to be the degree of $\min(\alpha, F)$, that is,

$$\deg(\alpha, F) = \deg(\min(\alpha, F)).$$

Theorem 2.11. Let α be algebraic over F and let $n = \deg(\alpha, F)$. Then:
(a) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F.
(b) $[F(\alpha) : F] = n$.
(c) $F(\alpha)$ is a finite algebraic extension of F.

Proof. The result is trivial for $n = 1$. Suppose that $n > 1$.

(a): Let $\mathcal{A} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. By Theorem 2.9, each element of $F(\alpha)$ is of the form $f(\alpha)$ for some polynomial $f(x)$ in $F[x]$. Let $g(x) = \min(\alpha, F)$ and note that $\deg(g) = n$. By the Division Algorithm, there are polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \tag{2.9}$$

with $\deg(r) \leq n - 1$ or $r(x) = 0$. Substituting $x = \alpha$ into (2.9) shows that $f(\alpha) = r(\alpha)$. Therefore, $\mathcal{A}$ spans $F(\alpha)$ over F.

Suppose that $b_0, b_1, \ldots, b_{n-1}$ are elements in F, not all of which are 0, such that

$$b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_1\alpha + b_0 = 0.$$

Then at least one of $b_1, b_2, \ldots, b_{n-1}$ must be nonzero, so

$$h(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$$

is a (nonconstant) polynomial in $F[x]$ of degree less than n that has α as a root. This contradicts the minimal property of $g(x)$. Thus, the elements of $\mathcal{A}$ are linearly independent over F.

(b): The basis $\mathcal{A}$ has n elements, so $[F(\alpha) : F] = n$.

(c): This follows from part (b) and Theorem 2.10. □

Theorem 2.12. Let α be algebraic over F, and let $f(x)$ be a polynomial in $F[x]$ that has α as a root. Then:
(a) $[F(\alpha) : F] \leq \deg(f)$.
(b) $[F(\alpha) : F] = \deg(f)$ if and only if $f(x)$ is irreducible over F.

(c) If E is an extension of F, then $[E(\alpha) : E] \leq [F(\alpha) : F]$.

Proof. Let $g(x) = \min(\alpha, F)$ and observe that, by Theorem 2.11(b), $[F(\alpha) : F] = \deg(g)$.

(a): By Theorem 2.6, $g(x)$ divides $f(x)$, so

$$[F(\alpha) : F] = \deg(g) \leq \deg(f).$$

(b): Since $g(x)$ divides $f(x)$, it follows that $\deg(g) = \deg(f)$ if and only if $g(x)$ equals $f(x)$ divided by its leading coefficient.

(c): Let $h(x) = \min(\alpha, E)$. Viewing $g(x)$ as a polynomial in $E[x]$, we have from Theorem 2.6 that $h(x)$ divides $g(x)$. Then part (b) implies that

$$[E(\alpha) : E] = \deg(h) \leq \deg(g) = [F(\alpha) : F].$$

□

Theorem 2.13. Let E be an extension of F. Then $[E : F] = 1$ if and only if $E = F$.

Proof. Straightforward. □

We define a *tower of fields* over F to be a series of extensions of F of the form

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n.$$

Theorem 2.14 (Tower Theorem). Let K be an extension of F, and let

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = K$$

be a tower of fields over F. Then $[K : F]$ is finite if and only if $[E_i : E_{i-1}]$ is finite for $i = 1, 2, \ldots, n$. In this case,

$$[K : F] = [E_n : E_{n-1}][E_{n-1} : E_{n-2}] \cdots [E_1 : E_0].$$

Proof. We prove the assertion for $n = 2$. The general case follows by induction. Consider the tower $F \subseteq E \subseteq K$. If $[K : F]$ is finite, then we have from linear algebra that $[K : E]$ and $[E : F]$ are finite. Conversely, if $[K : E]$ and $[E : F]$ are finite, let $\mathcal{A} = \{\alpha_j : j = 1, 2, \ldots, m\}$ be a basis for E over F, where $m = [E : F]$, and let $\mathcal{B} = \{\beta_k : k = 1, 2, \ldots, l\}$ be a basis for K over E, where $l = [K : E]$.

We claim that

$$\mathcal{C} = \{\alpha_j \beta_k : j = 1, 2, \ldots, m; k = 1, 2, \ldots, l\}$$

is a basis for K over F. Take γ in K. Since $\mathcal{B}$ spans K over E,

$$\gamma = \sum_{k=1}^{l} c_k \beta_k \tag{2.10}$$

for some c_k in E, and since $\mathcal{A}$ spans E over F,

$$c_k = \sum_{j=1}^{m} b_{jk} \alpha_j \tag{2.11}$$

for some b_{jk} in F. Substituting (2.11) into (2.10) gives

$$\gamma = \sum_{j=1}^{m} \sum_{k=1}^{l} b_{jk} \alpha_j \beta_k.$$

Therefore, $\mathcal{C}$ spans K over F.

Suppose that

$$\sum_{j=1}^{m} \sum_{k=1}^{l} b_{jk} \alpha_j \beta_k = \sum_{k=1}^{l} \left(\sum_{j=1}^{m} b_{jk} \alpha_j \right) \beta_k = 0.$$

Since $\mathcal{B}$ is a basis for K over E, $\sum_{j=1}^{m} b_{jk} \alpha_j = 0$ for each k, and since $\mathcal{A}$ is a basis for E over F, $b_{jk} = 0$ for each j and k. Therefore, the elements of $\mathcal{C}$ are linearly independent over F. This proves the claim.

It follows that

$$[K : F] = lm = [K : E][E : F].$$

Thus, if $[K : E]$ and $[E : F]$ are finite, then so is $[K : F]$. □

Theorem 2.15. If K is an extension of F of prime degree, and E is a field between F and K, then either $E = F$ or $E = K$.

Proof. By the Tower Theorem, $[K : F] = [K : E][E : F]$, so either $[K : E] = 1$ or $[E : F] = 1$. The result now follows from Theorem 2.13. □

There are a handful of theorems in this book that will be called on so frequently that to reference them each and every time would be repetitive. Accordingly, we will cite such results the first few times they are used but not necessarily thereafter. Theorems 2.6, 2.9, 2.12(b), 2.13, and 2.14 fall in this category, as does Theorem 2.23 below.

2.4 DERIVATIVES

Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

be a nonconstant polynomial in $F[x]$. The (formal) *derivative* of $f(x)$ with respect to x is defined to be

$$D_x(f) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

If $f(x)$ is a constant polynomial (including the zero polynomial), we define $D_x(f) = 0$. Observe that

$$\deg(D_x(f)) = \deg(f) - 1 \tag{2.12}$$

whenever $f(x)$ is a nonconstant polynomial. Here is an instance where F having characteristic 0 is important. As an illustration, if the characteristic of F were a prime p, then

$$D_x(x^p - 1) = px^{p-1} = 0$$

and this clearly violates (2.12).

The formal derivative has certain properties that are familiar from differential calculus.

Theorem 2.16. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$. Then

$$D_x(f + g) = D_x(f) + D_x(g)$$

and

$$D_x(fg) = fD_x(g) + D_x(f)g.$$

Proof. The first identity follows immediately from the definition of D_x. The second identity can be demonstrated using

$$\begin{aligned} D_x(x^{m+n}) &= x^m(nx^{n-1}) + (mx^{m-1})x^n \\ &= x^m D_x(x^n) + D_x(x^m)x^n \end{aligned}$$

for arbitrary nonnegative integers m and n. □

Let $f(x)$ be a nonconstant polynomial in $F[x]$, and let α be a root of $f(x)$. We know from Theorem 2.4 that $x - \alpha$ divides $f(x)$. If $(x-\alpha)^d$ divides $f(x)$ for some $d > 1$, we say that α is a *repeated root* of $f(x)$; otherwise α is referred to

as a *simple root*. If all the roots of $f(x)$ are simple, we say that $f(x)$ has simple roots.

Theorem 2.17. Let $f(x)$ be a nonconstant polynomial in $F[x]$. Then $f(x)$ has simple roots if and only if $\gcd(f, D_x(f)) = 1$.

Proof. Let α be a root of $f(x)$, and let $g(x) = f(x)/(x - \alpha)$. Then

$$D_x(f) = (x - \alpha)D_x(g) + g(x)$$

hence

$$\begin{aligned} \alpha \text{ is a repeated root of } f(x) &\Leftrightarrow \alpha \text{ is a root of } g(x) \\ &\Leftrightarrow \alpha \text{ is a root of } D_x(f) \\ &\Leftrightarrow \alpha \text{ is a root of } \gcd(f, D_x(f)). \end{aligned}$$

□

As an illustration, let $h(x) = x^n - 1$, where $n \geq 1$. Since $D_x(h) = nx^n$, and $h(x)$ does not have 0 as a root, it follows from Theorem 2.17 that $h(x)$ has simple roots. This is consistent with Example 1.4.

Theorem 2.18. Let $f(x)$ be a nonconstant polynomial in $F[x]$. If $f(x)$ is irreducible over F, then $f(x)$ has simple roots.

Proof. Since $f(x)$ is irreducible over F, either $\gcd(f, D_x(f)) = 1$ or $\gcd(f, D_x(f))$ equals $f(x)$ divided by its leading coefficient. The latter possibility is excluded by (2.12). The result now follows from Theorem 2.17. □

If α is algebraic over F, we refer to the roots of $\min(\alpha, F)$ as the *conjugates* of α over F. Evidently, the conjugates of α over F are the same as the conjugates over F of any other root of $\min(\alpha, F)$. It follows from Theorem 2.18 that $\min(\alpha, F)$ has simple roots, that is, the conjugates of α are distinct.

2.5 PRIMITIVE ELEMENT THEOREM

We denote the ring of polynomials over F in the n indeterminates $x_1, x_2, \ldots, x_n$ by $F[x_1, x_2, \ldots, x_n]$, and denote a typical element of $F[x_1, x_2, \ldots, x_n]$ by $p(x_1, x_2, \ldots, x_n)$ or, for brevity, by p. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements in an extension E of F, and define

$$F[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{p(\alpha_1, \alpha_2, \ldots, \alpha_n) : p \in F[x_1, x_2, \ldots, x_n]\}$$

and

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \frac{p(\alpha_1, \alpha_2, \ldots, \alpha_n)}{q(\alpha_1, \alpha_2, \ldots, \alpha_n)} : p, q \in F[x_1, x_2, \ldots, x_n]; q(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0 \right\}.$$

Let $\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, and let β be an arbitrary element of E. We sometimes denote $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ by $F(\mathcal{A})$ and $F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta)$ by $F(\mathcal{A}, \beta)$.

Consistent with the case $n = 1$ discussed in Section 2.2, $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a ring and $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a field. We say that $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ and $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are generated over F by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Clearly, $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is the smallest ring in E that contains F and the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$; similarly, $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest such field. It is usual to refer to $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ as the *field of fractions* of $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

As an illustration, we have the ring

$$\begin{aligned} \mathbb{Q}[\sqrt{2}, \sqrt{3}] &= \{p(\sqrt{2}, \sqrt{3}) : p \in F[x_1, x_2]\} \\ &= \{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} : a_1, a_2, a_3, a_4 \in \mathbb{Q}\} \end{aligned}$$

and the field

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \left\{ \frac{p(\sqrt{2}, \sqrt{3})}{q(\sqrt{2}, \sqrt{3})} : p, q \in F[x_1, x_2], q(\sqrt{2}, \sqrt{3}) \neq 0 \right\} \\ &= \left\{ \frac{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6}}{b_1 + b_2\sqrt{2} + b_3\sqrt{3} + b_4\sqrt{6}} : a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Q}; \right. \\ &\qquad \left. b_1 + b_2\sqrt{2} + b_3\sqrt{3} + b_4\sqrt{6} \neq 0 \right\}. \end{aligned} \tag{2.13}$$

Theorem 2.19. For $n > 1$, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements in some extension of F. Then

$$F[\alpha_1, \alpha_2, \ldots, \alpha_n] = F[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$$

and

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n).$$

Proof. Observe that we have not assumed that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are necessarily algebraic over F. We prove the assertion for $n = 2$. The general case follows by induction. Let α and β be elements in some extension of F.

By definition,

$$F[\alpha,\beta] = \{p(\alpha,\beta) : p(x,y) \in F[x,y]\}$$

and

$$F[\alpha][\beta] = \{f(\beta) : f(y) \in F[\alpha](y)\}.$$

Each $p(x,y)$ in $F[x,y]$ can be expressed in the form

$$p(x,y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x)$$

where $a_i(x)$ is a polynomial in $F[x]$ for $i = 1,2,\ldots,n$. It follows that $p(\alpha,y)$ is in $F[\alpha][y]$, hence $p(\alpha,\beta)$ is in $F[\alpha][\beta]$. Therefore, $F[\alpha,\beta] \subseteq F[\alpha][\beta]$. The reverse inclusion is demonstrated similarly.

By definition,

$$F(\alpha,\beta) = \left\{\frac{p(\alpha,\beta)}{q(\alpha,\beta)} : p(x,y), q(x,y) \in F[x,y]; q(\alpha,\beta) \neq 0\right\}$$

and

$$F(\alpha)(\beta) = \left\{\frac{f(\beta)}{g(\beta)} : f(y), g(y) \in F(\alpha)[y]; g(\beta) \neq 0\right\}.$$

Each $f(y)$ and $g(y)$ in $F(\alpha)[y]$ can be expressed in the form

$$f(y) = \sum_{j=0}^{m} \frac{b_j(\alpha)}{c_j(\alpha)} y^j \quad \text{and} \quad g(y) = \sum_{k=0}^{l} \frac{d_k(\alpha)}{e_k(\alpha)} y^k$$

where $b_j(x)$ and $c_j(x)$ are polynomials in $F[x]$ with $c_j(\alpha) \neq 0$ for $j = 1,2,\ldots,m$, and similarly for the $d_k(x)$ and $e_k(x)$. Clearing denominators in $f(y)$ and $g(y)$, we see that $f(\beta)/g(\beta)$ is in $F(\alpha,\beta)$. Therefore, $F(\alpha)(\beta) \subseteq F(\alpha,\beta)$. The reverse inclusion is demonstrated similarly. □

The next two results generalize Theorems 2.9 and 2.11(c).

Theorem 2.20. If $\alpha_1,\alpha_2,\ldots,\alpha_n$ are algebraic over F, then

$$F(\alpha_1,\alpha_2,\ldots,\alpha_n) = F[\alpha_1,\alpha_2,\ldots,\alpha_n].$$

Proof. The case $n = 1$ follows from Theorem 2.9. Suppose that $n = 2$, and let α and β be algebraic over F. Then β is algebraic over $F(\alpha)$, and it follows from Theorems 2.9 and 2.19 that

$$F(\alpha,\beta) = F(\alpha)(\beta) = F(\alpha)[\beta] = F[\alpha][\beta] = F[\alpha,\beta].$$

The general case follows by induction. □

As an illustration, we have from Theorem 2.20 that (2.13) can be expressed as

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} : a_1, a_2, a_3, a_4 \in \mathbb{Q}\}.$$

Thus, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ spans $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$. Since $\min(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, by Theorem 2.11(b), $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. It is easily demonstrated that $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$, hence $\min(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$. Again by Theorem 2.11(b),

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

The Tower Theorem implies that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4. \tag{2.14}$$

Therefore, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

Theorem 2.21. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over F, then $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a finite algebraic extension of F.

Proof. Let $E_0 = F$, and let $E_i = E_{i-1}(\alpha_i)$ for $i = 1, 2, \ldots, n$. By Theorem 2.19, $E_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Since α_i is algebraic over F, it is algebraic over E_{i-1}. It follows from Theorem 2.11(b) that $[E_i : E_{i-1}]$ is finite for each i. By the Tower Theorem,

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] = [E_n : E_{n-1}][E_{n-1} : E_{n-2}] \cdots [E_1 : E_0].$$

Therefore, $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a finite extension of F, and by Theorem 2.10, it is an algebraic extension of F. □

If an extension K of F is generated over F by a single element, that is, if $K = F(\theta)$ for some θ in K, we say that K is a *simple extension* of F and that θ is a *primitive element* for K over F.

Theorem 2.22 (Primitive Element Theorem). Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraic over F. Then there are elements $c_2, \ldots, c_n$ in F such that $\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$ is a primitive element for $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ over F, that is,

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n).$$

Proof. The result is trivial for $n = 1$. Suppose that $n = 2$, and let β and γ be algebraic over F. Let

$$f(x) = \min(\beta, F) \qquad g(x) = \min(\gamma, F)$$
$$h(x) = \min(\gamma, F(\beta + c\gamma)) \quad \text{and} \quad r(x) = f(\beta + c\gamma - cx).$$

Let us denote the roots of $f(x)$ by $\beta = \beta_1, \beta_2, \ldots, \beta_s$ and those of $g(x)$ by $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_t$. By Theorem 2.18, $\beta_1, \beta_2, \ldots, \beta_s$ are distinct, as are $\gamma_1, \gamma_2, \ldots, \gamma_t$. Since F is infinite, there is c in F such that

$$c \neq \frac{\beta_i - \beta_k}{\gamma_j - \gamma_l} \tag{2.15}$$

for $i \neq k = 1, 2, \ldots, s$ and $j \neq l = 1, 2, \ldots, t$. Thus, the $\beta_i + c\gamma_j$ are distinct.

Observe that $g(x)$, $h(x)$, and $r(x)$ have the root γ in common. Since $g(x)$ and $r(x)$ are in $F(\beta + c\gamma)[x]$, they are divisible by $h(x)$. Therefore, $h(x)$ divides $\gcd(g, r)$, from which it follows that the roots of $h(x)$ are among $\gamma_1, \gamma_2, \ldots, \gamma_t$. Let γ_j be such a root for some $1 \leq j \leq t$. Then γ_j is a root of $r(x)$, so $\beta + c\gamma - c\gamma_j = \beta_i$ for some $1 \leq i \leq s$. Given the choice of c, we have $i = j = 1$. This means that γ is the only root of $h(x)$, hence $h(x) = x - \gamma$. It follows that γ is in $F(\beta + c\gamma)$, and therefore, so is β. Thus, $F(\beta, \gamma) \subseteq F(\beta + c\gamma)$. Clearly, the reverse inclusion holds, so $F(\beta, \gamma) = F(\beta + c\gamma)$.

Now, suppose that $n = 3$. With β and γ as above, let δ be algebraic over F. By Theorem 2.19,

$$F(\beta, \gamma, \delta) = F(\beta, \gamma)(\delta) = F(\beta + c\gamma)(\delta) = F(\beta + c\gamma, \delta).$$

Casting $\beta + c\gamma$ and δ in the former roles of β and γ, respectively, we have from the case $n = 2$ that there is d in F such that

$$F(\beta + c\gamma, \delta) = F(\beta + c\gamma + d\delta).$$

Therefore,

$$F(\beta, \gamma, \delta) = F(\beta + c\gamma + d\delta).$$

The general case follows by induction. □

As an illustration, consider the increasingly familiar field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. In the notation of the Primitive Element Theorem,

$$\beta_1, \beta_2 = \pm\sqrt{2} \quad \text{and} \quad \gamma_1, \gamma_2 = \pm\sqrt{3}.$$

Then (2.15) is satisfied provided that

$$c \neq \frac{(\pm\sqrt{2}) - (\mp\sqrt{2})}{(\pm\sqrt{3}) - (\mp\sqrt{3})} = \pm\frac{\sqrt{2}}{\sqrt{3}}.$$

In particular, for $c = 1$, we have

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}). \tag{2.16}$$

An extension K of F is said to be *finitely generated* over F if there are finitely many elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in K that generate K over F, that is, $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. According to this definition, $\alpha_1, \alpha_2, \ldots, \alpha_n$ could consist entirely of elements that are algebraic over F, entirely of elements that are transcendental over F, or some combination of each.

Theorem 2.23. Let K be an extension of F. Then the following are equivalent:
(a) K is a finitely generated algebraic extension of F.
(b) K is a simple algebraic extension of F.
(c) K is a finite extension of F.

Proof. The result is trivial if $K = F$, so assume that $K \neq F$.

(a)⇒(b): This follows from the Primitive Element Theorem.

(b)⇒(c): This follows from Theorem 2.11(b).

(c)⇒(a): Since K is a finite extension of F, there is a finite basis for K over F. Evidently, K is generated over F by the elements of this basis. By Theorem 2.10, K is an algebraic extension of F. □

2.6 ISOMORPHISM EXTENSION THEOREM AND SPLITTING FIELDS

We now turn to the matter of proving that for an arbitrary nonconstant polynomial over a field, there is an extension of the field that contains a root of the polynomial. Let

$$\begin{aligned} \phi\colon F &\longrightarrow F' \\ a &\longmapsto a' \end{aligned}$$

be a (field) isomorphism, and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be an arbitrary polynomial in $F[x]$. We extend ϕ to a ring isomorphism $\overline{\phi}$ by defining

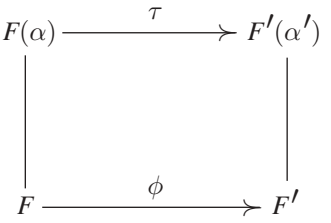
$$\begin{aligned} \overline{\phi}\colon F[x] &\longrightarrow F'[x] \\ f(x) &\longmapsto f'(x) \end{aligned} \tag{2.17}$$

where

$$f'(x) = a'_n x^n + a'_{n-1} x^{n-1} + \cdots + a'_1 x + a'_0.$$

The following result is the key to constructing the desired extension of F.

Theorem 2.24 (Isomorphism Extension Theorem). Let $\phi\colon F \longrightarrow F'$ be an isomorphism, let $f(x)$ be a polynomial in $F[x]$ that is irreducible over F, and let $f'(x)$ be as defined in (2.17). Let α be a root of $f(x)$ and let α' be a root of $f'(x)$. Then ϕ extends uniquely to an isomorphism $\tau\colon F(\alpha) \longrightarrow F'(\alpha')$ such that $\tau(\alpha) = \alpha'$.



Proof. We may assume without loss of generality that $f(x)$ is monic, hence $f(x) = \min(\alpha, F)$ and $f'(x) = \min(\alpha', F')$. By Theorem 2.9, each element of $F(\alpha)$ is of the form $g(\alpha)$ for some polynomial $g(x)$ in $F[x]$. We extend $\phi\colon F \longrightarrow F'$ to a map $\tau\colon F(\alpha) \longrightarrow F'(\alpha')$ by defining $\tau(g(\alpha)) = g'(\alpha')$. Suppose that $h(x)$ is a polynomial in $F[x]$ such that $g(\alpha) = h(\alpha)$. Then α is a root of $g(x) - h(x)$, so $g(x) - h(x) = s(x)f(x)$, where $s(x)$ is in $F[x]$. Thus, $g'(x) - h'(x) = s'(x)f'(x)$, hence $g'(\alpha') = h'(\alpha')$. Therefore, τ is well defined. Clearly, τ is additive, multiplicative, and surjective. Suppose that $g'(\alpha') = 0$. Then $f'(x)$ divides $g'(x)$, hence $f(x)$ divides $g(x)$, so $g(\alpha) = 0$. Therefore, τ is injective. Lastly, τ is unique because it is completely determined by its value at α. □

The identity isomorphism on an arbitrary field will be denoted by id. (This same symbol will be used to denote the identity element of an arbitrary group.)

To illustrate the Isomorphism Extension Theorem, let $F = F' = \mathbb{Q}$, $\phi = id$, and $f(x) = x^2 + x + 1$. Then $f'(x) = f(x)$. Let $\alpha = \omega$ and $\alpha' = \omega^2$, where ω and ω^2, as defined in (1.13), are the roots of $f(x)$. We note that $f(x)$ is irreducible over $\mathbb{Q}$, otherwise it would factor into two linear terms, and then ω and ω^2 would be in $\mathbb{Q}$. By the Isomorphism Extension Theorem, $id\colon \mathbb{Q} \longrightarrow \mathbb{Q}$ extends uniquely to an isomorphism $\tau\colon \mathbb{Q}(\omega) \longrightarrow \mathbb{Q}(\omega^2)$ such that $\tau(\omega) = \omega^2$. Since $\mathbb{Q}(\omega^2) = \mathbb{Q}(\omega)$, τ is an automorphism of $\mathbb{Q}(\omega)$ that fixes $\mathbb{Q}$ pointwise.

Theorem 2.25 (Kronecker[1]). Let $f(x)$ be a polynomial in $F[x]$ that is irreducible over F. Then there is an extension $F(\alpha)$ of F, unique up to isomorphism, such that α is a root of $f(x)$.

[1]Leopold Kronecker (1823–1891) was a German mathematician and one of the early contributors to the development of Galois theory.

Proof. Let us denote by $(f(x))$ the principal ideal generated by $f(x)$ in the ring $F[x]$, and consider the projection homomorphism

$$\begin{aligned} \iota\colon F[x] &\longrightarrow F[x]/(f(x)) \\ h(x) &\longmapsto h(x) + (f(x)). \end{aligned}$$

It is convenient to denote $h(x) + (f(x))$ by $[h(x)]$. Then $[f(x)] = [0]$. Let $[g(x)]$ be a nonzero element of $F[x]/(f(x))$; that is, assume that $g(x)$ is not in $(f(x))$. Since $f(x)$ is irreducible over F, and $g(x)$ is not divisible by $f(x)$, we have $\gcd(f, g) = 1$. By the Euclidean Algorithm, there are polynomials $s(x)$ and $t(x)$ in $F[x]$ such that

$$s(x)f(x) + t(x)g(x) = 1.$$

Then

$$[1] = [s(x)][f(x)] + [t(x)][g(x)] = [t(x)][g(x)]$$

so $[g(x)]$ has a multiplicative inverse. Therefore, $F[x]/(f(x))$ is a field.

We denote by $\iota_{|F}$ the field homomorphism obtained by restricting ι to F. Clearly, $\iota_{|F}$ is injective. Identifying F with $\mathrm{im}(\iota_{|F})$, the *image* of F under ι_F, and denoting $[x]$ by α, we have $[h(x)] = h([x]) = h(\alpha)$ for arbitrary $h(x)$ in $F[x]$. With these conventions, $F(\alpha) = F[x]/(f(x))$, and we can express $[f(x)] = [0]$ as $f(\alpha) = 0$. Thus, $F(\alpha)$ is the desired extension of F. The assertion regarding uniqueness up to isomorphism follows from the Isomorphism Extension Theorem. □

It is clear from the construction in Theorem 2.25 that there is nothing of an algebraic nature to distinguish one root of $f(x)$ from another. We therefore have the important observation that the roots of a polynomial that is irreducible over a field are algebraically indistinguishable over that field. Recalling the discussion around $\sqrt{2}$ and $-\sqrt{2}$ in Section 1.1, we now note that those remarks are consistent with $x^2 - 2$ being irreducible over $\mathbb{Q}$.

Let $f(x)$ be a polynomial in $F[x]$, and let L be an extension of F. If $f(x)$ has a factorization over L consisting of linear factors, that is, factors of degree 1, we say that $f(x)$ *splits* over F. Then

$$f(x) = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \tag{2.18}$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_n$ in L, where c is in F. Clearly, each of $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a root of $f(x)$, and it follows from Theorems 2.4 and 2.5 that these are all of them. Thus, $f(x)$ has $n = \deg(f)$ roots, where repeated roots are counted according to their multiplicity. Throughout the rest of the book, whenever we say that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are (all) the roots of a polynomial, it is implicit that certain roots in the list might be repeated.

Renumbering the roots if necessary, let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the distinct roots of $f(x)$, and suppose that α_j appears d_j times in (2.18) for $j = 1, 2, \ldots, m$. Then

$$f(x) = c(x - \alpha_1)^{d_1}(x - \alpha_2)^{d_2} \cdots (x - \alpha_m)^{d_m}. \tag{2.19}$$

Since each of the $x - \alpha_j$ is irreducible over L, (2.19) is the unique factorization of $f(x)$ over L guaranteed by Theorem 2.8.

With $f(x)$ as in (2.18), consider the subfield $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of L generated over F by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Evidently, K contains all the roots of $f(x)$, and it is clear that no proper subfield of K has this property. A field satisfying these conditions is said to be a *splitting field* of $f(x)$ over F. Since K is a splitting field of $bf(x)$ over F for all nonzero b in F, K is a splitting over F for an infinity of polynomials in $F[x]$. When it is not important to specify a particular polynomial in $F[x]$ that gives rise to K as a splitting field over F, we will simply say that K is a splitting field over F. It follows from Theorem 2.21 that K is a finite algebraic extension of F.

Theorem 2.26. Every nonconstant polynomial in $F[x]$ has a splitting field over F.

Proof. Let $f(x)$ be a nonconstant polynomial in $F[x]$. The proof is by induction on $n = \deg(f)$. For $n = 1$, F itself is the desired splitting field. Suppose that $n > 1$. According to Theorem 2.8, $f(x)$ factors over F into a product of polynomials, each of which is irreducible over F. By Theorem 2.25, there is an extension of F that contains a root α_1 of an arbitrarily chosen factor. Consider $g(x) = f(x)/(x - \alpha_1)$, which is a polynomial in $F(\alpha_1)[x]$ of degree $n - 1$. By the induction hypothesis, $g(x)$ has a splitting field

$$F(\alpha_1)(\alpha_2, \alpha_3, \ldots, \alpha_n) = F(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$$

over $F(\alpha_1)$, where $\alpha_2, \alpha_3, \ldots, \alpha_n$ are the $n - 1$ roots of $g(x)$. Then $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the n roots of $f(x)$, so $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a splitting field of $f(x)$ over F. □

Despite the almost trivial nature of the next theorem, in the context of later results, it turns out to be surprisingly powerful.

Theorem 2.27. If K is a splitting field over F, and E is a field between F and K, then K is a splitting field over E.

Proof. Since K is a splitting field over F of a polynomial in $F[x]$, it is also a splitting field over E of that same polynomial now viewed as a polynomial in $E[x]$. □

The reason for referring to K in Theorem 2.26 as "a" splitting field of $f(x)$ over F rather than "the" splitting field is illustrated by the following example. Consistent with the construction in Theorem 2.25, $\mathbb{R}[x]/(x^2+1)$ is a splitting field of x^2+1 over $\mathbb{R}$. If we identify $\mathbb{R}$ with $\mathbb{R}+(x^2+1)$ and denote $[x] = x+(x^2+1)$ by i, we obtain the complex numbers:

$$\mathbb{C} = \{a+ib : a, b \in \mathbb{R}\}.$$

Alternatively, consider $\mathbb{R}^2$ endowed with the following addition and multiplication:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1).$$

Then

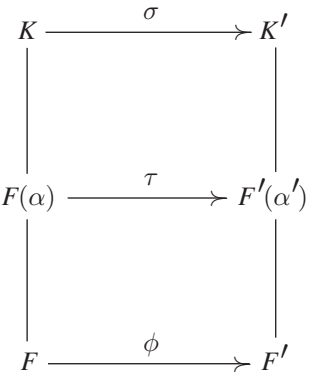
$$\mathbb{C} \longrightarrow \mathbb{R}^2$$
$$a + bi \longmapsto (a, b)$$

is a field isomorphism that maps i to $(0, 1)$.

Intuitively, it seems that there should be only one splitting field for a given polynomial over a given field, at least up to isomorphism. We now show that this instinct is correct.

Theorem 2.28. Let $\phi: F \longrightarrow F'$ be an isomorphism, let $f(x)$ be a polynomial in $F[x]$, and let $f'(x)$ be as defined in (2.17). Let K be a splitting field of $f(x)$ over F, and let K' be a splitting field of $f'(x)$ over F'. Then ϕ extends to an isomorphism $\sigma: K \longrightarrow K'$.

Proof. The proof is by induction on $n = [K : F]$. Suppose that $n = 1$. By Theorem 2.13, $K = F$ and $K' = F'$, so we take $\sigma = \phi$. Now, suppose that $n > 1$. By Theorem 2.8, $f(x)$ has a factorization into a product of polynomials in $F[x]$ that are irreducible over F. Every factor cannot be linear, otherwise we would have $[K : F] = 1$. Let $g(x)$ be a factor of degree at least 2, and let $g'(x)$ be the corresponding factor of $f'(x)$. Let α be a root of $g(x)$ and let α' be a root of $g'(x)$. By the Isomorphism Extension Theorem, ϕ extends (uniquely) to an isomorphism $\tau: F(\alpha) \longrightarrow F'(\alpha')$ such that $\tau(\alpha) = \alpha'$.



Since $[K : F] = n$ and $[F(\alpha) : F] \geq 2$, we have $[K : F(\alpha)] \leq n - 1$. The argument used in Theorem 2.27 shows that K is a splitting field of $f(x)$ over $F(\alpha)$ and that K' is a splitting field of $f'(x)$ over $F(\alpha')$. By the induction hypothesis, τ extends to an isomorphism $\sigma : K \longrightarrow K'$. □

Theorem 2.29. Let $f(x)$ be a polynomial in $F[x]$. Then all splitting fields of $f(x)$ over F are isomorphic.

Proof. Set $F = F'$ and $\phi = id$ in Theorem 2.28, and let K and K' be any two splitting fields of $f(x)$ over F. □

In light of Theorem 2.29, we now speak of *the* splitting field of $f(x)$ over F.

Theorem 2.30. Let $f(x)$ be a polynomial in $F[x]$ of degree n, and let K be the splitting field of $f(x)$ over F. Then $[K : F] \leq n!$.

Proof. Denoting the roots of $f(x)$ by $\alpha_1, \alpha_2, \ldots, \alpha_n$, we have $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. The proof is by induction on n. Suppose that $n = 1$. Then $f(x) = x - \alpha_1$, so α_1 is in F and $[K : F] = 1$. Now, suppose that $n > 1$. By Theorem 2.12(a), $[F(\alpha_1) : F] \leq n$. Since K is the splitting field of

$$\frac{f(x)}{x - \alpha_1} = (x - \alpha_2)(x - \alpha_3) \cdots (x - \alpha_n)$$

over $F(\alpha_1)$, by the induction hypothesis, $[K : F(\alpha_1)] \leq (n - 1)!$. Therefore,

$$[K : F] = [K : F(\alpha_1)][F(\alpha_1) : F] \leq n!.$$

□

The Fundamental Theorem of Algebra states that any polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$. Those readers wishing to avoid the abstraction inherent in the above discussion on the existence and uniqueness of splitting fields may prefer to think more concretely in terms of polynomials in $\mathbb{Q}[x]$ or $\mathbb{R}[x]$, in which case splitting fields will automatically be subfields of $\mathbb{C}$. Relatively little will be sacrificed by this change in perspective. Indeed, this is the classical case.

CHAPTER 3

FUNDAMENTAL THEOREM ON SYMMETRIC POLYNOMIALS AND DISCRIMINANTS

This chapter is primarily devoted to a classical result called the Fundamental Theorem on Symmetric Polynomials (FTSP), and some of its consequences. The FTSP is well named because of the central role it played in the early study of the algebraic properties of the roots of polynomials. Our first application of the FTSP will be to develop some results on discriminants, a simple example of which was provided in Section 1.1.

3.1 FUNDAMENTAL THEOREM ON SYMMETRIC POLYNOMIALS

Let E be a field, and let $E[x_1, x_2, \ldots, x_n]$ be the ring of polynomials over E in the n indeterminates $x_1, x_2, \ldots, x_n$. A *monomial* in $E[x_1, x_2, \ldots, x_n]$ is a polynomial consisting of a single term, that is, an expression of the form $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, where c is in E. We refer to c as the *coefficient* of the monomial. When $k_1 = k_2 = \cdots = k_n = 0$, we have a *constant monomial*, and when $c = 0$, we have the *zero monomial*. Any nonzero polynomial in $E[x_1, x_2, \ldots, x_n]$ is the sum of a finite number of nonzero monomials. If $c \neq 0$, the *degree* of $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ is defined to be the n-tuple

$$\deg(cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}) = (k_1, k_2, \ldots, k_n).$$

In particular, the degree of a nonzero constant monomial is $(0, 0, \ldots, 0)$. *The degree of the zero monomial is not defined*.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Let $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ and $x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ be distinct monomials, and consider the n differences $k_1 - l_1, k_2 - l_2, \ldots, k_n - l_n$. If the first nonzero difference in the sequence is positive, we write

$$(k_1, k_2, \ldots, k_n) > (l_1, l_2, \ldots, l_n)$$

and if it is negative, we write

$$(k_1, k_2, \ldots, k_n) < (l_1, l_2, \ldots, l_n).$$

This is referred to as the *lexicographic ordering* of monomials because it is akin to the familiar method of ordering words in a dictionary. With this ordering, we can express each nonzero polynomial $p = p(x_1, x_2, \ldots, x_n)$ in $E[x_1, x_2, \ldots, x_n]$ as a sum of nonzero monomials of strictly decreasing degree:

$$\begin{aligned} p = {} & c_{(k_1,k_2,\ldots,k_n)}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} + c_{(k_1,k_2,\ldots,k_n-1)}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n-1} \\ & + \cdots + c_{(0,0,\ldots,1)}x_n + c_{(0,0,\ldots,0)}. \end{aligned} \tag{3.1}$$

We refer to

$$c_{(k_1,k_2,\ldots,k_n)}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$$

as the *leading term* of p, and to $c_{(k_1,k_2,\ldots,k_n)}$ as the *leading coefficient*. The *degree* of p is defined to be the degree of its leading term:

$$\deg(p) = (k_1, k_2, \ldots, k_n).$$

The degree of the zero polynomial is not defined. As we now show, this definition of degree has properties that are similar to those encountered with polynomials in one indeterminate.

Theorem 3.1. Let p and q be nonzero polynomials in $E[x_1, x_2, \ldots, x_n]$. Then

$$\deg(p + q) \leq \max\{\deg(p), \deg(q)\} \tag{3.2}$$

and

$$\deg(pq) = \deg(p) + \deg(q). \tag{3.3}$$

Proof. If p and q have the same degree, the leading term of $p + q$ is the sum of the respective leading terms, except when the leading coefficients are the negative of each other, which accounts for the $\leq$ sign in (3.2). If p and q have different degrees, the leading term of $p + q$ is the leading term of the polynomial with the

larger degree. In either case, (3.2) holds. The leading term of pq is the product of the leading terms of p and q, from which (3.3) follows. □

Theorem 3.2. Every sequence of polynomials in $E[x_1, x_2, \ldots, x_n]$ of strictly decreasing degree is finite.

Proof. Let $\mathcal{T}$ denote the corresponding sequence of strictly decreasing n-tuples of degrees. The proof is by induction on n. The result is clear for $n = 1$. Suppose that $n > 1$. Let us denote the first (largest) member of the sequence by $(k_1, k_2, \ldots, k_n)$. For $i = 0, 1, \ldots, k_1$, let $\mathcal{T}_i$ be the subsequence of $\mathcal{T}$, possibly empty, consisting of n-tuples that have i in the first position. Evidently, $\mathcal{T}$ equals the union of the $\mathcal{T}_i$. In fact, $\mathcal{T}$ equals the subsequence $\mathcal{T}_{k_1}$, followed by the subsequence $\mathcal{T}_{k_1-1}$, and so on, until $\mathcal{T}_0$. Since each $\mathcal{T}_i$ is effectively a strictly decreasing sequence of $(n-1)$-tuples, each prefixed by i, by the induction hypothesis, the $\mathcal{T}_i$ are finite. Therefore, so is $\mathcal{T}$. □

The *symmetric group* on n "letters," denoted by S_n, is discussed in Appendix D. The particular set of letters used to define S_n is a matter of convenience, and we will make different choices at various points in this book. Here, we choose $\{x_1, x_2, \ldots, x_n\}$ or sometimes $\{1, 2, \ldots, n\}$. When $n = 1$, the symmetric group consists solely of the identity. We exclude this trivial case and assume that $n > 1$.

For each σ in S_n, we define a map

$$\begin{aligned} \sigma : E[x_1, x_2, \ldots, x_n] &\longrightarrow E[x_1, x_2, \ldots, x_n] \\ p(x_1, x_2, \ldots, x_n) &\longmapsto p(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)) \end{aligned} \tag{3.4}$$

that is,

$$\sigma(p) = \sigma(p(x_1, x_2, \ldots, x_n)) = p(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)). \tag{3.5}$$

An alternative method of writing (3.5) is

$$\sigma(p) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Let q be the zero polynomial in $E[x_1, x_2, \ldots, x_n]$. Regardless of how q is expressed as the sum of monomials, since $x_1, x_2, \ldots, x_n$ are indeterminates over E, $\sigma(q)$ is again the zero polynomial. Therefore,

$$q(x_1, x_2, \ldots, x_n) = 0 \quad \Leftrightarrow \quad q(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)) = 0 \tag{3.6}$$

for all σ in S_n. Suppose that p and p' are polynomials in $E[x_1, x_2, \ldots, x_n]$ such that $p = p'$. Setting $q = p - p'$, we have from (3.6) that $\sigma(p) = \sigma(p')$, which shows that σ is well defined. It is easily demonstrated that σ is a ring automorphism of

$E[x_1, x_2, \ldots, x_n]$ that fixes the elements of E pointwise. In fact, S_n has a group structure.

Theorem 3.3. S_n is a group of ring automorphisms of $E[x_1, x_2, \ldots, x_n]$ that fix the elements of E pointwise (where multiplication is defined to be composition of automorphisms).

Proof. Straightforward. □

Despite having just defined S_n to be a group of automorphisms, it is sometimes convenient to revert to the original formulation and think of S_n as a group of permutations on $\{x_1, x_2, \ldots, x_n\}$ or $\{1, 2, \ldots, n\}$. This has the advantage of providing access to the definitions and results of Appendix D.

We say that p in $E[x_1, x_2, \ldots, x_n]$ is *symmetric* in $x_1, x_2, \ldots, x_n$ over E if $\sigma(p) = p$ for all σ in S_n. For example, take $p = x_1x_3 + 3x_2 + 1$ in $\mathbb{Q}[x_1, x_2, x_3]$, and in cycle notation, let $\sigma = (x_1\ x_2)$ in S_3. Then $\sigma(p) = x_2x_3 + 3x_1 + 1 \neq p$, demonstrating that p is not symmetric in x_1, x_2, x_3 over $\mathbb{Q}$. By contrast, $x_1 + x_2 + x_3$ and $[(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2$ are symmetric.

The *elementary symmetric polynomials* in $x_1, x_2, \ldots, x_n$ over E are defined as follows:

$$\begin{aligned}
s_1 &= \sum_{1 \le j_1 \le n} x_{j_1} \\
s_2 &= \sum_{1 \le j_1 < j_2 \le n} x_{j_1}x_{j_2} \\
&\vdots \\
s_i &= \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} x_{j_1}x_{j_2}\cdots x_{j_i} \\
&\vdots \\
s_n &= \sum_{1 \le j_1 < j_2 < \cdots < j_n \le n} x_{j_1}x_{j_2}\cdots x_{j_n}.
\end{aligned} \tag{3.7}$$

For example,

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
s_n &= x_1x_2\cdots x_n.
\end{aligned}$$

It is easy to see that, true to their name, the elementary symmetric polynomials are in fact symmetric in $x_1, x_2, \ldots, x_n$ over E. The importance of these

polynomials stems from the following observation. Let x be another indeterminate over E. Then

$$(x - x_1)(x - x_2)\cdots(x - x_n) = \\ x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^i s_i x^{n-i} + \cdots + (-1)^n s_n. \tag{3.8}$$

For example, taking $n = 2$, we have

$$s_1 = x_1 + x_2 \qquad s_2 = x_1x_2$$

and

$$(x - x_1)(x - x_2) = x^2 - s_1x + s_2.$$

With $n = 3$,

$$s_1 = x_1 + x_2 + x_3 \qquad s_2 = x_1x_2 + x_1x_3 + x_2x_3 \qquad s_3 = x_1x_2x_3$$

and

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3.$$

And with $n = 4$,

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3 + x_4 \\ s_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ s_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ s_4 &= x_1x_2x_3x_4 \end{aligned}$$

and

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4.$$

The degrees of the elementary symmetric polynomials have a distinctive form:

$$\begin{aligned} \deg(s_1) &= (1, 0, 0, \ldots, 0) \\ \deg(s_2) &= (1, 1, 0, \ldots, 0) \\ &\vdots \\ \deg(s_n) &= (1, 1, 1, \ldots, 1). \end{aligned}$$

Let $k_1, k_2, \ldots, k_n$ be nonnegative integers. It follows from (3.3) that

$$\begin{aligned}
&\deg(s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n}) \\
&\quad = k_1 \deg(s_1) + k_2 \deg(s_2) + \cdots + k_n \deg(s_n) \\
&\quad = (k_1, 0, \ldots, 0) + (k_2, k_2, 0, \ldots, 0) + \cdots + (k_n, k_n, \ldots, k_n) \\
&\quad = (k_1 + k_2 + k_3 + \cdots + k_n, k_2 + k_3 + \cdots + k_n, \ldots, k_n). \qquad (3.9)
\end{aligned}$$

For example, the leading term of

$$p = x_1^3 x_2 + 2x_1^2 x_2^2 + x_1 x_2^3$$

in $E[x_1, x_2]$ is $x_1^3 x_2$, so $\deg(p) = (3, 1)$. Alternatively, observing that

$$p = (x_1 + x_2)^2 x_1 x_2 = s_1^2 s_2$$

we have from (3.9) that

$$\deg(p) = (2 + 1, 1) = (3, 1).$$

Given a polynomial p in $E[y_1, y_2, \ldots, y_n]$, where $y_1, y_2, \ldots, y_n$ are indeterminates over E, we denote by $p(s_1, s_2, \ldots, s_n)$ the element in $E[s_1, s_2, \ldots, s_n]$ obtained by substituting $y_i = s_i$ into p for $i = 1, 2, \ldots, n$. For example, let $p(y_1, y_2, y_3) = y_1 y_3 + 3y_2 + 1$ in $\mathbb{Q}[y_1, y_2, y_3]$. Then

$$\begin{aligned}
p(s_1, s_2, s_3) &= s_1 s_3 + 3s_2 + 1 \\
&= (x_1 + x_2 + x_3)(x_1 x_2 x_3) + 3(x_1 x_2 + x_1 x_3 + x_2 x_3) + 1 \\
&= x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 + 3x_1 x_2 + 3x_1 x_3 + 3x_2 x 3_3 + 1.
\end{aligned}$$

Let $E[s_1, s_2, \ldots, s_n]$ be the subring of $E[x_1, x_2, \ldots, x_n]$ generated over E by $s_1, s_2, \ldots, s_n$. Then

$$E[s_1, s_2, \ldots, s_n] = \{p(s_1, s_2, \ldots, s_n) : p \in E[y_1, y_2, \ldots, y_n]\}.$$

It is important to remember that even though the elements of $E[s_1, s_2, \ldots, s_n]$ are formally polynomials in $s_1, s_2, \ldots, s_n$ with coefficients in E, they are ultimately polynomials in $x_1, x_2, \ldots, x_n$ with coefficients in E.

Let us denote by $E[x_1, x_2, \ldots, x_n]^{S_n}$ the set of elements in $E[x_1, x_2, \ldots, x_n]$ that are symmetric in $x_1, x_2, \ldots, x_n$ over E, that is,

$$E[x_1, x_2, \ldots, x_n]^{S_n} = \{p \in E[x_1, x_2, \ldots, x_n] : \sigma(p) = p \text{ for all } \sigma \in S_n\}.$$

Evidently,

$$E[s_1, s_2, \ldots, s_n] \subseteq E[x_1, x_2, \ldots, x_n]^{S_n}.$$

The following result, known as the *Fundamental Theorem on Symmetric Polynomials* (FTSP), asserts that the reverse inclusion also holds.

Theorem 3.4 (Fundamental Theorem on Symmetric Polynomials).

$$E[s_1, s_2, \ldots, s_n] = E[x_1, x_2, \ldots, x_n]^{S_n}.$$

Proof. One inclusion was demonstrated above. To show the reverse inclusion, take p in $E[x_1, x_2, \ldots, x_n]^{S_n}$ and let $c_1 x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ be its leading term. Then $\deg(p) = (k_1, k_2, \ldots, k_n)$. Since p is symmetric in $x_1, x_2, \ldots, x_n$, it has $c_1 x_{\sigma(1)}^{k_1} x_{\sigma(2)}^{k_2} \cdots x_{\sigma(n)}^{k_n}$ as a term for all σ in S_n. It follows that $k_1 \geq k_2 \geq \cdots \geq k_n$. For if not, with the appropriate choice of σ, we could produce a monomial term of degree greater than $(k_1, k_2, \ldots, k_n)$. Let

$$q_1 = s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_{n-1}^{k_{n-1} - k_n} s_n^{k_n}.$$

Clearly, q_1 is symmetric in $x_1, x_2, \ldots, x_n$ over E, and we have from (3.9) that

$$\deg(q_1) = (k_1, k_2, \ldots, k_n).$$

The leading coefficient of q_1, that is, the coefficient of $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, is the product of the leading coefficients of the $s_i^{k_i - k_{i+1}}$, so it equals 1. Thus,

$$p_1 = p - c_1 q_1$$

is symmetric in $x_1, x_2, \ldots, x_n$ over E, with $\deg(p) > \deg(p_1)$.

We repeat the process starting with p_1 and obtain

$$p_2 = p_1 - c_2 q_2 = p - c_1 q_1 - c_2 q_2$$

which is symmetric in $x_1, x_2, \ldots, x_n$ over E, with $\deg(p_1) > \deg(p_2)$, and so on. By Theorem 3.2, the process ends after, say, m steps. Then $p_m = c_m$ is in E, otherwise the process could continue. Thus,

$$p = c_1 q_1 + c_2 q_2 + \cdots + c_{m-1} q_{m-1} + c_m$$

is in $E[s_1, s_2, \ldots, s_n]$, hence

$$E[x_1, x_2, \ldots, x_n]^{S_n} \subseteq E[s_1, s_2, \ldots, s_n].$$

□

By definition, $E[s_1, s_2, \ldots, s_n]$ is a subring of $E[x_1, x_2, \ldots, x_n]$. As the next theorem shows, the rings $E[s_1, s_2, \ldots, s_n]$ and $E[y_1, y_2, \ldots, y_n]$ are isomorphic, and therefore, so are $E[s_1, s_2, \ldots, s_n]$ and $E[x_1, x_2, \ldots, x_n]$.

Theorem 3.5. The map

$$\begin{aligned} \iota\colon E[y_1, y_2, \ldots, y_n] &\longrightarrow E[s_1, s_2, \ldots, s_n] \\ p(y_1, y_2, \ldots, y_n) &\longmapsto p(s_1, s_2, \ldots, s_n) \end{aligned}$$

is a ring isomorphism.

Proof. An argument similar to that used in connection with (3.4) shows that ι is well defined. It is straightforward to verify that ι is additive, multiplicative, and surjective. We need to show that ι is injective. Let p be a nonzero polynomial in $E[y_1, y_2, \ldots, y_n]$. With p expressed in the form (3.1), we have

$$\deg(p) = (k_1, k_2, \ldots, k_n).$$

Suppose that all zero monomials have been suppressed from the expression for p. It follows from (3.2) and (3.9) that

$$\deg(\iota(p)) = (k_1 + k_2 + k_3 + \cdots + k_n, k_2 + k_3 + \cdots + k_n, \ldots, k_n).$$

Thus, the leading term of the image of p under ι is the image under ι of the leading term of p. A similar remark applies to leading coefficients. It follows that since p is a nonzero polynomial, so is $\iota(p)$. Therefore, $\ker(\iota) = \{0\}$, hence ι is injective. □

We know from the FTSP that every element in $E[x_1, x_2, \ldots, x_n]$ that is symmetric in $x_1, x_2, \ldots, x_n$ over E can be expressed as a polynomial in $s_1, s_2, \ldots, s_n$ with coefficients in E. In view of the isomorphism in Theorem 3.5, we now see that this polynomial expression is unique.

3.2 FUNDAMENTAL THEOREM ON SYMMETRIC RATIONAL FUNCTIONS

The ring $E[x_1, x_2, \ldots, x_n]$ has the field of fractions

$$E(x_1, x_2, \ldots, x_n) = \left\{ \frac{p}{q} : p, q \in E[x_1, x_2, \ldots, x_n];\, q(x_1, x_2, \ldots, x_n) \neq 0 \right\}.$$

The elements of $E(x_1, x_2, \ldots, x_n)$ are classically referred to as *rational functions* over E. We extend the map σ defined in (3.4) to $E(x_1, x_2, \ldots, x_n)$ in the following way:

$$\begin{aligned} \sigma : E(x_1, x_2, \ldots, x_n) &\longrightarrow E(x_1, x_2, \ldots, x_n) \\ \frac{p}{q} &\longmapsto \frac{\sigma(p)}{\sigma(q)} \end{aligned} \tag{3.10}$$

that is,

$$\sigma\left(\frac{p}{q}\right) = \frac{\sigma(p)}{\sigma(q)}.$$

It follows from (3.6) that if $q \neq 0$, then $\sigma(q) \neq 0$, so the quotient $\sigma(p)/\sigma(q)$ in (3.10) makes sense. Suppose that p' and q' are polynomials in $E[x_1, x_2, \ldots, x_n]$ such that $p/q = p'/q'$. Then $pq' = p'q$ implies that $\sigma(p)\sigma(q') = \sigma(p')\sigma(q)$, hence $\sigma(p)/\sigma(q) = \sigma(p')/\sigma(q')$, so σ is well defined.

We say that p/q in $E(x_1, x_2, \ldots, x_n)$ is *symmetric* in $x_1, x_2, \ldots, x_n$ over E if $\sigma(p/q) = p/q$ for all σ in S_n. The ring $E[s_1, s_2, \ldots, s_n]$ has the field of fractions

$$E(s_1, s_2, \ldots, s_n) = \left\{ \frac{p(s_1, s_2, \ldots, s_n)}{q(s_1, s_2, \ldots, s_n)} : p, q \in E[y_1, y_2, \ldots, y_n]; q(s_1, s_2, \ldots, s_n) \neq 0 \right\}.$$

Let us denote by $E(x_1, x_2, \ldots, x_n)^{S_n}$ the set of elements in $E(x_1, x_2, \ldots, x_n)$ that are symmetric over E, that is,

$$E(x_1, x_2, \ldots, x_n)^{S_n} = \left\{ \frac{p}{q} \in E(x_1, x_2, \ldots, x_n) : \sigma\left(\frac{p}{q}\right) = \frac{p}{q} \text{ for all } \sigma \in S_n \right\}.$$

Clearly,

$$E(s_1, s_2, \ldots, s_n) \subseteq E(x_1, x_2, \ldots, x_n)^{S_n}.$$

According to the following result, referred to here as the *Fundamental Theorem on Symmetric Rational Functions* (FTSRF), the reverse inclusion also holds.

Theorem 3.6 (Fundamental Theorem on Symmetric Rational Functions).

$$E(s_1, s_2, \ldots, s_n) = E(x_1, x_2, \ldots, x_n)^{S_n}.$$

Proof. One inclusion was argued above. To show the reverse inclusion, take p/q in $E(x_1, x_2, \ldots, x_n)^{S_n}$ and let

$$\theta = p \prod_{\sigma \in S_n \setminus \langle id \rangle} \sigma(q) \quad \text{and} \quad \psi = \prod_{\sigma \in S_n} \sigma(q).$$

Then $p/q = \theta/\psi$. By the FTSP, ψ is in $E[s_1, s_2, \ldots, s_n]$, so

$$\frac{\sigma(\theta)}{\psi} = \frac{\sigma(\theta)}{\sigma(\psi)} = \sigma\left(\frac{\theta}{\psi}\right) = \sigma\left(\frac{p}{q}\right) = \frac{p}{q} = \frac{\theta}{\psi}.$$

It follows that $\sigma(\theta) = \theta$ for all σ in S_n. Again by the FTSP, θ is in $E[s_1, s_2, \ldots, s_n]$, hence θ/ψ is in $E(s_1, s_2, \ldots, s_n)$. Therefore,

$$E(x_1, x_2, \ldots, x_n)^{S_n} \subseteq E(s_1, s_2, \ldots, s_n).$$

□

The next result is the counterpart to Theorem 3.5 for the present setting. A key observation is that, by Theorem 3.5,

$$\begin{aligned} &E(s_1, s_2, \ldots, s_n) \\ &\quad = \left\{ \frac{p(s_1, s_2, \ldots, s_n)}{q(s_1, s_2, \ldots, s_n)} : p, q \in E[y_1, y_2, \ldots, y_n]; q(y_1, y_2, \ldots, y_n) \neq 0 \right\} \\ &\quad = \left\{ \frac{p(s_1, s_2, \ldots, s_n)}{q(s_1, s_2, \ldots, s_n)} : \frac{p}{q} \in E(y_1, y_2, \ldots, y_n) \right\}. \end{aligned}$$

Theorem 3.7. The map

$$\begin{aligned} \iota : E(y_1, y_2, \ldots, y_n) &\longrightarrow E(s_1, s_2, \ldots, s_n) \\ \frac{p(y_1, y_2, \ldots, y_n)}{q(y_1, y_2, \ldots, y_n)} &\longmapsto \frac{p(s_1, s_2, \ldots, s_n)}{q(s_1, s_2, \ldots, s_n)} \end{aligned}$$

is a field isomorphism.

Proof. This follows from Theorem 3.5 and the preceding remarks. □

3.3 SOME IDENTITIES BASED ON ELEMENTARY SYMMETRIC POLYNOMIALS

The elementary symmetric polynomials satisfy a number of identities that will be useful later on. We motivate the discussion with the case $n = 3$. As defined above,

$$x^3 - s_1 x^2 + s_2 x - s_3 = (x - x_1)(x - x_2)(x - x_3).$$

Let $s_{1[1]}$ and $s_{2[1]}$ be the elementary symmetric polynomials in x_2 and x_3, that is,

$$s_{1[1]} = x_2 + x_3 \quad \text{and} \quad s_{2[1]} = x_2 x_3.$$

Then

$$\begin{aligned} & x^3 - s_1 x^2 + s_2 x - s_3 \\ & \quad = (x - x_1)(x^2 - s_{1[1]} x + s_{2[1]}) \\ & \quad = x^3 - (x_1 + s_{1[1]}) x^2 + (x_1 s_{1[1]} + s_{2[1]}) x - x_1 s_{2[1]} \end{aligned}$$

hence

$$s_1 = x_1 + s_{1[1]} \quad s_2 = x_1 s_{1[1]} + s_{2[1]} \quad \text{and} \quad s_3 = x_1 s_{2[1]}.$$

Solving for $s_{1[1]}$ and $s_{2[1]}$ gives

$$s_{1[1]} = s_1 - x_1 \quad \text{and} \quad s_{2[1]} = s_2 - x_1 s_1 + x_1^2.$$

We have from the above identities that

$$E[x_1, s_{1[1]}, s_{2[1]}] = E[x_1, s_1, s_2, s_3].$$

Similarly, let $s_{1[2]}$ and $s_{2[2]}$ be the elementary symmetric polynomials in x_1 and x_3, that is,

$$s_{1[2]} = x_1 + x_3 \quad \text{and} \quad s_{2[2]} = x_1 x_3$$

and let $s_{1[3]}$ and $s_{2[3]}$ be the elementary symmetric polynomials in x_1 and x_2, that is,

$$s_{1[3]} = x_1 + x_2 \quad \text{and} \quad s_{2[3]} = x_1 x_2.$$

Then

$$s_{1[1]} + s_{1[2]} + s_{1[3]} = (x_2 + x_3) + (x_1 + x_3) + (x_1 + x_2) = 2s_1$$

and

$$s_{2[1]} + s_{2[2]} + s_{2[3]} = x_2 x_3 + x_1 x_3 + x_1 x_2 = s_2.$$

The above identities generalize to arbitrary n, as we now show. Let $s_{k[i]}$ be the kth elementary symmetric polynomial in the $n-1$ indeterminates $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ for $i = 1, 2, \ldots, n$ and $k = 1, 2, \ldots, n-1$. Consistent with (3.7), we have

$$s_{1[i]} = \sum_{\substack{1 \le j_1 \le n \\ j_1 \ne i}} x_{j_1}$$

$$
\begin{aligned}
s_{2[i]} &= \sum_{\substack{1\le j_1<j_2\le n\\ j_1,j_2\neq i}} x_{j_1}x_{j_2}\\
&\vdots\\
s_{k[i]} &= \sum_{\substack{1\le j_1<j_2<\cdots<j_k\le n\\ j_1,j_2,\ldots,j_k\neq i}} x_{j_1}x_{j_2}\cdots x_{j_k}\\
&\vdots\\
s_{n-1[i]} &= \sum_{\substack{1\le j_1<j_2<\cdots<j_{n-1}\le n\\ j_1,j_2,\ldots,j_{n-1}\neq i}} x_{j_1}x_{j_2}\cdots x_{j_{n-1}}.
\end{aligned}
\tag{3.11}
$$

So, for example,

$$s_{1[i]} = x_1 + x_2 + \cdots + x_{i-1} + x_i + \cdots + x_n$$

and

$$s_{n-1[i]} = x_1x_2\cdots x_{i-1}x_i\cdots x_n.$$

Another way of expressing $s_{k[i]}$ is

$$s_{k[i]} = s_k(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n).$$

Analogous to the case $n = 3$, we have

$$
\begin{aligned}
s_1 &= x_i + s_{1[i]}\\
s_2 &= x_i s_{1[i]} + s_{2[i]}\\
&\vdots\\
s_k &= x_i s_{k-1[i]} + s_{k[i]}\\
&\vdots\\
s_{n-1} &= x_i s_{n-2[i]} + s_{n-1[i]}\\
s_n &= x_i s_{n-1[i]}
\end{aligned}
\tag{3.12}
$$

and

$$
\begin{aligned}
s_{1[i]} &= s_1 - x_i\\
s_{2[i]} &= s_2 - x_i s_1 + x_i^2
\end{aligned}
$$

$$
\begin{aligned}
s_{3[i]} &= s_3 - x_i s_2 + x_i^2 s_1 - x_i^3 \\
&\vdots \\
s_{k[i]} &= \sum_{j=0}^{k-1} (-1)^j x_i^j s_{k-j} + (-1)^k x_i^k \\
&\vdots \\
s_{n-1[i]} &= \sum_{j=0}^{n-2} (-1)^j x_i^j s_{n-1-j} + (-1)^{n-1} x_i^{n-1}.
\end{aligned} \tag{3.13}
$$

Theorem 3.8. For $n > 1$,

$$E[x_i, s_{1[i]}, s_{2[i]}, \ldots, s_{n-1[i]}] = E[x_i, s_1, s_2, \ldots, s_n]$$

for $i = 1, 2, \ldots, n$.

Proof. It follows from (3.13) that

$$E[x_i, s_{1[i]}, s_{2[i]}, \ldots, s_{n-1[i]}] \subseteq E[x_i, s_1, s_2, \ldots, s_{n-1}]$$

and from (3.12) that

$$E[x_i, s_1, s_2, \ldots, s_n] \subseteq E[x_i, s_{1[i]}, s_{2[i]}, \ldots, s_{n-1[i]}].$$

□

Theorem 3.9. For $n > 1$,

$$\sum_{i=1}^{n} s_{k[i]} = (n-k)s_k$$

for $k = 1, 2, \ldots, n-1$.

Proof. The product $x_{j_1} x_{j_2} \cdots x_{j_k}$, where $1 \le j_1 < j_2 < \cdots < j_k \le n$, appears once as a term in s_k. It also appears once as a term in $s_{k[i]}$, except when $j_1 = i$, or $j_2 = i$, …, or $j_k = i$. □

3.4 DISCRIMINANTS

Assume that $n > 1$. The *alternating polynomial*, also classically called the *alternating function*, in $E[x_1, x_2, \ldots, x_n]$ is

$$\Delta_n = \Delta_n(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j). \tag{3.14}$$

For convenience of notation, we sometimes abbreviate Δ_n to Δ. Closely related to Δ_n is the *Vandermonde matrix*:

$$V_n = V_n(x_1, x_2, \ldots, x_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}.$$

Theorem 3.10. For $n \geq 2$,

$$\det(V_n) = (-1)^{n(n-1)/2}\Delta_n.$$

Proof. The proof is by induction on n. The result is straightforward for $n = 2$. Suppose that $n > 2$ and consider the polynomial

$$g(x) = \det[V_n(x_1, x_2, \ldots, x_{n-1}, x)]$$

in $\mathbb{Q}(x_1, x_2, \ldots, x_{n-1})[x]$. Expanding the determinant along its nth column, we find that $g(x)$ has degree $n-1$ with leading coefficient $\det(V_{n-1})$. Since each of $x_1, x_2, \ldots, x_{n-1}$ is a root of $g(x)$, it follows from remarks made in connection with (2.18) that these are all the roots. By the induction hypothesis,

$$\begin{aligned} g(x) &= \det(V_{n-1})(x - x_1)(x - x_2)\cdots(x - x_{n-1}) \\ &= (-1)^{n-1}\det(V_{n-1})(x_1 - x)(x_2 - x)\cdots(x_{n-1} - x) \\ &= (-1)^{n(n-1)/2}\Delta_{n-1}(x_1 - x)(x_2 - x)\cdots(x_{n-1} - x) \end{aligned}$$

hence

$$\det(V_n) = g(x_n) = (-1)^{n(n-1)/2}\Delta_n.$$

□

Since

$$(x_i - x_j)^2 = -(x_i - x_j)(x_j - x_i)$$

and since there are $\binom{n}{2} = n(n-1)/2$ terms in (3.14), we have

$$\Delta_n^2 = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} (x_i - x_j). \tag{3.15}$$

It is clear from (3.15) that Δ_n^2 is symmetric in $x_1, x_2, \ldots, x_n$ over E. By the FTSP, Δ_n^2 is in $E[s_1, s_2, \ldots, s_n]$. We could use the algorithm developed in the proof of the FTSP to find an explicit expression for Δ_n^2, but the calculations are onerous even for relatively small n. As an alternative, we present a technique based on *Newton's identities* that relieves at least some of the computational burden.

For each nonnegative integer k, let

$$v_k = x_1^k + x_2^k + \cdots + x_n^k.$$

Note that $v_0 = n$ and $v_1 = s_1$. Evidently, the v_k are symmetric in $x_1, x_2, \ldots, x_n$ over E.

Theorem 3.11 (Newton's Identities). For $2 \leq k \leq n$,

$$v_k = \sum_{i=1}^{k-1} (-1)^{i+1} s_i v_{k-i} + (-1)^{k+1} k s_k. \tag{3.16}$$

For $k \geq n$,

$$v_k = \sum_{i=1}^{n} (-1)^{i+1} s_i v_{k-i}. \tag{3.17}$$

Proof. Take $2 \leq k \leq n-1$. According to (3.13),

$$s_{k[j]} = \sum_{i=0}^{k-1} (-1)^i x_j^i s_{k-i} + (-1)^k x_j^k$$

for $j = 1, 2, \ldots, n$. Summing both sides of this identity over j and invoking Theorem 3.9, we find that

$$\begin{aligned}(n-k)s_k &= \sum_{i=0}^{k-1} (-1)^i s_{k-i} v_i + (-1)^k v_k \\ &= \sum_{i=1}^{k} (-1)^{k-i} s_i v_{k-i} + (-1)^k v_k\end{aligned}$$

which is equivalent to (3.16). Now, take $k \geq n$. It follows from (3.8) that

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n + \sum_{i=1}^{n} (-1)^i s_i x^{n-i}$$

hence

$$x^{k-n}(x-x_1)(x-x_2)\cdots(x-x_n) = x^k + \sum_{i=1}^{n}(-1)^i s_i x^{k-i}. \tag{3.18}$$

Substituting $x = x_j$ into (3.18) gives

$$x_j^k = \sum_{i=1}^{n}(-1)^{i+1} s_i x_j^{k-i}$$

for $j = 1, 2, \ldots, n$. Summing both sides of this identity over j gives (3.17). Finally, we observe that the right-hand sides of (3.16) and (3.17) are identical when $k = n$. □

Theorem 3.12. For $n \geq 2$,

$$\Delta_n^2 = \begin{vmatrix} \nu_0 & \nu_1 & \nu_2 & \cdots & \nu_{n-1} \\ \nu_1 & \nu_2 & \nu_3 & \cdots & \nu_n \\ \nu_2 & \nu_3 & \nu_4 & \cdots & \nu_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{n-1} & \nu_n & \nu_{n+1} & \cdots & \nu_{2n-2} \end{vmatrix}.$$

Proof. It follows from Theorem 3.10 and the properties of determinants that

$$\Delta_n^2 = [\det(V_n)]^2 = \det(V_n V_n^{\mathrm{t}}) = \begin{vmatrix} \nu_0 & \nu_1 & \nu_2 & \cdots & \nu_{n-1} \\ \nu_1 & \nu_2 & \nu_3 & \cdots & \nu_n \\ \nu_2 & \nu_3 & \nu_4 & \cdots & \nu_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{n-1} & \nu_n & \nu_{n+1} & \cdots & \nu_{2n-2} \end{vmatrix}$$

where t denotes matrix transposition. □

Example 3.13. For $n = 3$ and $k = 0, 1, \ldots, 4$, Newton's identities are as follows:

$$\begin{aligned} \nu_0 &= 3 \\ \nu_1 &= s_1 \\ \nu_2 &= s_1\nu_1 - 2s_2 \\ &= s_1^2 - 2s_2 \\ \nu_3 &= s_1\nu_2 - s_2\nu_1 + 3s_3 \end{aligned}$$

$$
\begin{aligned}
&= s_1^3 - 3s_1s_2 + 3s_3 \\
\nu_4 &= s_1\nu_3 - s_2\nu_2 + s_3\nu_1 \\
&= s_1^4 - 4s_1^2s_2 + 4s_1s_3 + 2s_2^2.
\end{aligned}
$$

Then

$$
\begin{aligned}
\Delta_3^2 &= \begin{vmatrix} \nu_0 & \nu_1 & \nu_2 \\ \nu_1 & \nu_2 & \nu_3 \\ \nu_2 & \nu_3 & \nu_4 \end{vmatrix} \\
&= -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2. \qquad (3.19)
\end{aligned}
$$

◊

Example 3.14. For $n = 4$ and $k = 0, 1, \ldots, 6$, Newton's identities are as follows:

$$
\begin{aligned}
\nu_0 &= 4 \\
\nu_1 &= s_1 \\
\nu_2 &= s_1\nu_1 - 2s_2 \\
&= s_1^2 - 2s_2 \\
\nu_3 &= s_1\nu_2 - s_2\nu_1 + 3s_3 \\
&= s_1^3 - 3s_1s_2 + 3s_3 \\
\nu_4 &= s_1\nu_3 - s_2\nu_2 + s_3\nu_1 - 4s_4 \\
&= s_1^4 - 4s_1^2s_2 + 4s_1s_3 + 2s_2^2 - 4s_4 \\
\nu_5 &= s_1\nu_4 - s_2\nu_3 + s_3\nu_2 - s_4\nu_1 \\
&= s_1^5 - 5s_1^3s_2 + 5s_1^2s_3 + 5s_1s_2^2 - 5s_1s_4 - 5s_2s_3 \\
\nu_6 &= s_1\nu_5 - s_2\nu_4 + s_3\nu_3 - s_4\nu_2 \\
&= s_1^6 - 6s_1^4s_2 + 6s_1^3s_3 + 9s_1^2s_2^2 - 6s_1^2s_4 \\
&\quad - 12s_1s_2s_3 - 2s_2^3 + 6s_2s_4 + 3s_3^2.
\end{aligned}
$$

Then

$$
\begin{aligned}
\Delta_4^2 &= \begin{vmatrix} \nu_0 & \nu_1 & \nu_2 & \nu_3 \\ \nu_1 & \nu_2 & \nu_3 & \nu_4 \\ \nu_2 & \nu_3 & \nu_4 & \nu_5 \\ \nu_3 & \nu_4 & \nu_5 & \nu_6 \end{vmatrix} \\
&= -27s_1^4s_4^2 + 18s_1^3s_2s_3s_4 - 4s_1^3s_3^3 - 4s_1^2s_2^3s_4 \\
&\quad + s_1^2s_2^2s_3^2 + 144s_1^2s_2s_4^2 - 6s_1^2s_3^2s_4 - 80s_1s_2^2s_3s_4 \\
&\quad + 18s_1s_2s_3^3 + 16s_2^4s_4 - 4s_2^3s_3^2 - 192s_1s_3s_4^2 \\
&\quad - 128s_2^2s_4^2 + 144s_2s_3^2s_4 - 27s_3^4 + 256s_4^3. \qquad (3.20)
\end{aligned}
$$

◊

Let $E = \mathbb{Q}$, let F be an arbitrary field, and let $f(x)$ be a polynomial in $F[x]$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. The *discriminant* of $f(x)$ is defined to be

$$\operatorname{disc}(f) = [\Delta_n(\alpha_1, \alpha_2, \ldots, \alpha_n)]^2 = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2. \tag{3.21}$$

The notion of a discriminant was introduced in Section 1.1 in the context of quadratic polynomials in $\mathbb{Q}[x]$. Note that since $[\Delta_n(x_1, x_2, \ldots, x_n)]^2$ is symmetric in $x_1, x_2, \ldots, x_n$ over $\mathbb{Q}$, $\operatorname{disc}(f)$ is independent of the numbering of the roots of $f(x)$.

For any nonzero element c in F, $f(x)$ and $cf(x)$ have the same roots, hence $\operatorname{disc}(f) = \operatorname{disc}(cf)$. We assume for convenience in what follows that $f(x)$ is monic. Let

$$\begin{aligned} f(x) &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \\ &= x^n - b_1 x^{n-1} + b_2 x^{n-2} + \cdots + (-1)^{n-1} b_{n-1} x + (-1)^n b_n. \end{aligned}$$

The coefficients of $f(x)$ can be thought of as the "elementary symmetric polynomials" in $\alpha_1, \alpha_2, \ldots, \alpha_n$. More formally,

$$\begin{aligned} b_1 &= s_1(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ b_2 &= s_2(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &\vdots \\ b_{n-1} &= s_{n-1}(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ b_n &= s_n(\alpha_1, \alpha_2, \ldots, \alpha_n). \end{aligned}$$

Since $[\Delta_n(x_1, x_2, \ldots, x_n)]^2$ is in $F[s_1, s_2, \ldots, s_n]$, once we are given a "formula" for $[\Delta_n(x_1, x_2, \ldots, x_n)]^2$, as exemplified by (3.19) and (3.20), we can compute $\operatorname{disc}(f)$ by making the substitution $s_i = b_i$ for $i = 1, 2, \ldots, n$. Thus, $\operatorname{disc}(f)$ can be calculated directly from the coefficients of $f(x)$.

Theorem 3.15. Let F be an arbitrary field, and let $f(x)$ be a polynomial in $F[x]$. Then $\operatorname{disc}(f)$ is in F.

Proof. This follows from the preceding remarks. □

We have from (3.21) that $f(x)$ has a repeated root if and only if $\operatorname{disc}(f) = 0$. So, we now have a test for the presence of a repeated root based solely on the coefficients of $f(x)$. Making the substitution $x = y + b_1/n$ in $f(x)$ produces the reduced polynomial $g(y)$, which has the roots $\beta_i = \alpha_i - b_1/n$ for $i = 1, 2, \ldots, n$. It is clear that $\operatorname{disc}(f) = \operatorname{disc}(g)$. Recall the reduced cubic polynomial $g(y) = y^3 + py + q$ of Section 1.2. Substituting $s_1 = 0$, $s_2 = p$, and $s_3 = -q$ into (3.19) gives

$$\operatorname{disc}(g) = -4p^3 - 27q^2. \tag{3.22}$$

We now describe an approach to computing discriminants based on derivatives.

Theorem 3.16. With $n \geq 2$, let $f(x)$ be a nonconstant monic polynomial in $F[x]$ of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} D_x(f)(\alpha_i)$$

where $D_x(f)(\alpha_i)$ is $D_x(f)$ evaluated at α_i.

Proof. Since

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

we have from Theorem 2.16 that

$$D_x(f)(x) = \sum_{i=1}^{n} \Bigg[\prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x - \alpha_j) \Bigg].$$

Then

$$D_x(f)(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j)$$

for each i, hence

$$\prod_{i=1}^{n} D_x(f)(\alpha_i) = \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} (\alpha_i - \alpha_j).$$

The result now follows from (3.15). □

Theorem 3.17. With $n \geq 2$, let $f(x) = x^n + ax + b$ be a polynomial in $F[x]$. Then

$$\operatorname{disc}(f) = (-1)^{(n-1)(n-2)/2}(n-1)^{n-1}a^n + (-1)^{n(n-1)/2}n^n b^{n-1}. \tag{3.23}$$

Proof. Let us denote the roots of $f(x)$ by $\gamma_1, \gamma_2, \ldots, \gamma_n$. There are three cases to consider.

Case I. $a = 0$.
Then $f(x) = x^n + b$. Since $\gamma_j^n = -b$ for $j = 1, 2, \ldots, n$ and $\gamma_1 \gamma_2 \cdots \gamma_n = (-1)^n b$, we have

$$\prod_{j=1}^{n} D_x(f)(\gamma_j) = \prod_{j=1}^{n} n\gamma_j^{n-1} = n^n(-1)^{n(n-1)}b^{n-1} = n^n b^{n-1}.$$

By Theorem 3.16,

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2} n^n b^{n-1}.$$

Case II. $b = 0$.
Then $f(x) = x^n + ax$. Let $\gamma_1 = 0$. Since $\gamma_j^{n-1} = -a$ for $j = 2, 3, \ldots, n$, we have

$$\prod_{j=1}^{n} D_x(f)(\gamma_j) = a \prod_{j=2}^{n} (n\gamma_j^{n-1} + a) = (-1)^{n-1}(n-1)^{n-1}a^n.$$

By Theorem 3.16,

$$\operatorname{disc}(f) = (-1)^{(n-1)(n-2)/2}(n-1)^{n-1}a^n.$$

Case III. $a, b \neq 0$.
Note that $b \neq 0$ implies that $\gamma_j \neq 0$ for each j. Since γ_j is a root of $f(x)$, we have $\gamma_j^{n-1} = -(a\gamma_j + b)/\gamma_j$, hence

$$\begin{aligned}
\prod_{j=1}^{n} D_x(f)(\gamma_j) &= \prod_{j=1}^{n} (n\gamma_j^{n-1} + a) \\
&= \prod_{j=1}^{n} \left\{ \frac{(n-1)a}{\gamma_j} \left[\frac{-nb}{(n-1)a} - \gamma_j \right] \right\} \\
&= \frac{(n-1)^n a^n}{(-1)^n b} f\left(\frac{-nb}{(n-1)a} \right) \\
&= \frac{(n-1)^n a^n}{(-1)^n b} \left\{ \left[\frac{-nb}{(n-1)a} \right]^n + a \left[\frac{-nb}{(n-1)a} \right] + b \right\} \\
&= (-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}.
\end{aligned}$$

The result now follows from Theorem 3.16. □

When $n = 3$, (3.23) becomes $\operatorname{disc}(f) = -4a^3 - 27b^2$. Thus, Theorem 3.17 generalizes (3.22).

3.5 DISCRIMINANTS AND SUBFIELDS OF THE REAL NUMBERS

We recall a few basics about complex numbers. Let $\gamma = a + ib$ be an arbitrary complex number, where a and b are real numbers. We denote by $\operatorname{Re}(\gamma) = a$

and $\mathrm{Im}(\gamma) = b$ the real and imaginary parts of γ, respectively, and let $\|\gamma\| = \sqrt{a^2 + b^2}$ be the norm of γ. In what follows, we denote complex conjugation by an overline, that is,

$$\overline{\gamma} = \overline{a + bi} = a - bi.$$

Then

$$\gamma + \overline{\gamma} = 2\,\mathrm{Re}(\gamma) \qquad \gamma - \overline{\gamma} = 2i\,\mathrm{Im}(\gamma) \tag{3.24}$$

and

$$\gamma\overline{\gamma} = \|\gamma\|^2. \tag{3.25}$$

Note that $\overline{\gamma} = \gamma$ if and only if γ is in $\mathbb{R}$.

An important observation is that complex conjugation is a field automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$ pointwise. This has several consequences. The image of a subfield L of $\mathbb{C}$ under complex conjugation, denoted by $\overline{L}$, is again a subfield of $\mathbb{C}$. Let $f(x)$ be a polynomial in $\mathbb{R}[x]$. Then $\overline{f(\gamma)} = f(\overline{\gamma})$ for all γ in $\mathbb{C}$. Therefore, if γ is a root of $f(x)$, then so is $\overline{\gamma}$. Suppose that $f(x)$ is of degree n and has simple roots. The preceding remark implies that the nonreal roots of $f(x)$ come in complex conjugate pairs. Let $f(x)$ have r real roots and c pairs of nonreal roots. Then

$$n = r + 2c. \tag{3.26}$$

Theorem 3.18. Let F be a subfield of $\mathbb{R}$, and let $f(x)$ be a polynomial in $F[x]$ that has simple roots. Then $\mathrm{disc}(f) > 0$ if and only if c is even.

Proof. By Theorem 3.15, $\mathrm{disc}(f)$ is in $\mathbb{R}$, so the inequality $\mathrm{disc}(f) > 0$ makes sense. The real roots of $f(x)$ will be denoted by $\alpha_1, \alpha_2, \ldots, \alpha_r$ and referred to as being of type I. The conjugate pairs of nonreal roots will be denoted by $(\beta_1, \overline{\beta_1}), \ldots, (\beta_c, \overline{\beta_c})$, with $\beta_1, \beta_2, \ldots, \beta_c$ said to be of type II, and $\overline{\beta_1}, \overline{\beta_2}, \ldots, \overline{\beta_c}$ of type III. If all the roots are real numbers, that is, if $c = 0$, then it is clear that $\mathrm{disc}(f) > 0$. Suppose that $c \geq 1$. Let $\gamma = a + ib$ be an arbitrary nonzero complex number, where a and b are real numbers. Then $\gamma\overline{\gamma} = a^2 + b^2 > 0$, and if $b \neq 0$, then $(\gamma - \overline{\gamma})^2 = -4b^2 < 0$. In light of these inequalities, the terms comprising $\mathrm{disc}(f)$ can be partitioned as follows, where we take $i \neq j$.
(i) Both roots appearing in the term are of type I:

$$(\alpha_i - \alpha_j)^2 > 0.$$

(ii) One root appearing in the term is of type I and the other is of type II or type III:

$$(\alpha_i - \beta_j)^2(\alpha_i - \overline{\beta_j})^2 = [(\alpha_i - \beta_j)(\overline{\alpha_i - \beta_j})]^2 > 0.$$

(iii) Both roots appearing in the term are of type II or type III:

$$(\beta_i - \beta_j)^2(\overline{\beta_i} - \overline{\beta_j})^2 = [(\beta_i - \beta_j)(\overline{\beta_i - \beta_j})]^2 > 0.$$

(iv) One root appearing in the term is of type II and the other—not its conjugate—is of type III:

$$(\beta_i - \overline{\beta_j})^2(\overline{\beta_i} - \beta_j)^2 = [(\beta_i - \overline{\beta_j})(\overline{\beta_i - \overline{\beta_j}})]^2 > 0.$$

(v) One root appearing in the term is of type II and the other—its conjugate—is of type III:

$$(\beta_i - \overline{\beta_i})^2 < 0.$$

The above partitioning of the roots of $f(x)$ shows that the sign of $\operatorname{disc}(f)$ is determined by the number of terms appearing in category (v), of which there are c, one for each pair of nonreal complex conjugate roots. Thus,

$$\operatorname{disc}(f) = (-1)^c |\operatorname{disc}(f)|.$$

Since the roots of $f(x)$ are simple, $\operatorname{disc}(f) \neq 0$. Therefore, $\operatorname{disc}(f) > 0$ if and only if c is even. □

It is instructive to consider a special case of Theorem 3.18.

Theorem 3.19. Let F be a subfield of $\mathbb{R}$, and let $f(x)$ be a cubic polynomial in $F[x]$ that has simple roots. If $\operatorname{disc}(f) > 0$, then $f(x)$ has three real roots, and if $\operatorname{disc}(f) < 0$, then $f(x)$ has one real root (and two nonreal complex conjugate roots).

Proof. In the present case, (3.26) becomes $3 = r + 2c$. According to Theorem 3.18, if $\operatorname{disc}(f) > 0$, then $c = 0$, hence $r = 3$, and if $\operatorname{disc}(f) < 0$, then $c = 1$, hence $r = 1$.

An alternative proof offers further insights into the role played by $\operatorname{disc}(f)$ in the cubic case. For convenience, we return to the notation of Section 1.2 and observe that although $f(x)$ was assumed to be in $\mathbb{Q}[x]$, the arguments used there apply equally for $f(x)$ in $F[x]$, where F is an arbitrary field. Let $g(y)$ be the corresponding reduced polynomial. As was remarked before (3.22), $\operatorname{disc}(f) = \operatorname{disc}(g)$, so it is sufficient to prove the assertion for $g(y)$.

Let $\delta = \operatorname{disc}(g)$ as shown in (3.22). Since

$$\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} = \frac{1}{2}\sqrt{\frac{-\delta}{27}} \tag{3.27}$$

we can rewrite (1.11) as

$$\lambda_1, \lambda_2 = \sqrt[3]{\frac{1}{2}\left(-q \pm \sqrt{\frac{-\delta}{27}}\right)}. \tag{3.28}$$

Recall from (1.12) that $\lambda_1\lambda_2 = -3p$, and from (1.15) that the roots of $g(y)$ are

$$\begin{aligned} \beta_1 &= \frac{\lambda_1 + \lambda_2}{3} \\ \beta_2 &= \frac{\omega^2\lambda_1 + \omega\lambda_2}{3} \\ \beta_3 &= \frac{\omega\lambda_1 + \omega^2\lambda_2}{3}. \end{aligned} \tag{3.29}$$

Since ω and ω^2 are complex conjugates, we have $\overline{\omega} = \omega^2$ and $\overline{\omega^2} = \omega$.

Suppose that $\delta < 0$. Then (3.27) is a real number, and we are at liberty to take λ_1 to be the unique real cube root of λ_1^3. It follows from $\lambda_1\lambda_2 = -3p$ that λ_2 is the unique real cube root of λ_2^3. Thus, β_1 is a real root expressed in terms of real radicals. Since λ_1 and λ_2 are real numbers, we have

$$\overline{\beta_2} = \frac{\overline{\omega^2}\,\overline{\lambda_1} + \overline{\omega}\,\overline{\lambda_2}}{3} = \frac{\omega\lambda_1 + \omega^2\lambda_2}{3} = \beta_3. \tag{3.30}$$

Suppose that either β_2 or β_3 is a real number. Then (3.30) implies that they are equal, which contradicts the assumption that $f(x)$ has simple roots. Thus, β_2 and β_3 are nonreal complex conjugates, hence $r = 1$ (and $c = 1$). This is seen even more clearly by using (1.13) to rewrite (3.29) as

$$\begin{aligned} \beta_1 &= \frac{\lambda_1 + \lambda_2}{3} \\ \beta_2, \beta_3 &= \frac{-(\lambda_1 + \lambda_2)}{6} \mp i\,\frac{\sqrt{3}(\lambda_1 - \lambda_2)}{6}. \end{aligned}$$

Now, suppose that $\delta > 0$. Then (3.27) is a nonreal complex number, and we can express (3.28) as

$$\lambda_1, \lambda_2 = \sqrt[3]{\frac{1}{2}\left(-q \pm i\sqrt{\frac{\delta}{27}}\right)}.$$

It follows from $\lambda_1\lambda_2 = -3p$ that λ_1 and λ_2 are nonreal complex conjugates. We can now express (3.29) as

$$\beta_1 = \frac{\overline{\lambda_2} + \lambda_2}{3}$$
$$\beta_2 = \frac{\overline{\omega\lambda_2} + \omega\lambda_2}{3}$$
$$\beta_3 = \frac{\overline{\omega^2\lambda_2} + \omega^2\lambda_2}{3}.$$

Then (3.24) implies that β_1, β_2, and β_3 are real numbers, hence $r = 3$ (and $c = 0$). The striking observation to make here is that the three real roots have been expressed in terms of nonreal complex numbers. This relates to the Casus Irreducibilis mentioned in Section 1.2, a phenomenon to be explored further in Theorem 6.21. □

To illustrate the above considerations, in Examples 1.1, 1.2, and 1.3, $g(y)$ has 1, 3, and 3 real roots, respectively, and from (3.22), $\text{disc}(g) = -540$, 432, and 756, respectively. These results are consistent with Theorems 3.18 and 3.19.

CHAPTER 4

IRREDUCIBILITY AND FACTORIZATION

In this chapter, we cover some of the classical results on irreducibility and factorization of polynomials. Section 4.1 considers irreducibility over the rational numbers and culminates in Eisenstein's criterion. Section 4.2 presents some results on irreducibility of polynomials in relation to splitting fields. In Section 4.3, we examine the manner in which polynomials factor (or not) when an element is adjoined to a field.

4.1 IRREDUCIBILITY OVER THE RATIONAL NUMBERS

Any nonzero polynomial $f(x)$ in $\mathbb{Q}[x]$ can be expressed in the form

$$f(x) = \frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}{b} \tag{4.1}$$

where $a_0, a_1, \ldots, a_n$ are integers and b is a natural number. The *greatest common divisor* of $a_0, a_1, \ldots, a_n$, denoted by $\gcd(a_0, a_1, \ldots, a_n)$, is the largest natural number that divides each of $a_0, a_1, \ldots, a_n$ (Appendix E). We define the *content* of $f(x)$ to be the positive rational number

$$\mathrm{c}(f) = \frac{\gcd(a_0, a_1, \ldots, a_n)}{b}.$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Let

$$f(x) = \frac{d_n x^n + d_{n-1}x^{n-1} + \cdots + d_1 x + d_0}{e}$$

be another way of expressing $f(x)$, where $d_0, d_1, \ldots, d_n$ are integers and e is a natural number. Simplifying the numerator and denominator of (4.1), we may assume that $\gcd(a_0, a_1, \ldots, a_n)$ and b are relatively prime; likewise for $\gcd(d_0, d_1, \ldots, d_n)$ and e. Then $ea_i = bd_i$ for $i = 0, 1, \ldots, n$, hence

$$e \gcd(a_0, a_1, \ldots, a_n) = b \gcd(d_0, d_1, \ldots, d_n).$$

Since b is relatively prime to $\gcd(a_0, a_1, \ldots, a_n)$, b divides e; similarly, e divides b. Thus, $b = e$ and $a_i = d_i$ for $i = 0, 1, \ldots, n$. This shows that no matter what the original expression for $f(x)$, the simplified version is unique. Therefore, any expression for $f(x)$ equals the simplified version multiplied numerator and denominator by a given natural number. Thus, $\mathrm{c}(f)$ is well defined.

Theorem 4.1. Let $f(x)$ be a nonzero polynomial in $\mathbb{Q}[x]$. Then:
(a) $f(x)$ is in $\mathbb{Z}[x]$ if and only if $\mathrm{c}(f)$ is a natural number.
(b) $\mathrm{c}(rf) = r\mathrm{c}(f)$ for any positive rational number r.

Proof. We continue with the above notation.

(a): Evidently, if $f(x)$ is in $\mathbb{Z}[x]$, then $\mathrm{c}(f)$ is a natural number. To prove the converse, suppose that (4.1) expresses $f(x)$ in simplified form. For $\mathrm{c}(f)$ to be a natural number, we must have $b = 1$, which means that $f(x)$ is in $\mathbb{Z}[x]$.

(b): Let $r = s/t$. Then

$$\mathrm{c}(rf) = \frac{\gcd(sa_0, sa_1, \ldots, sa_n)}{tb} = \frac{s \gcd(a_0, a_1, \ldots, a_n)}{tb} = r\mathrm{c}(f).$$

□

We say that a polynomial $g(x)$ in $\mathbb{Q}[x]$ is *primitive* if $\mathrm{c}(g) = 1$. In view of Theorem 4.1(a), this is equivalent to $g(x)$ being in $\mathbb{Z}[x]$ and its coefficients being relatively prime. For each nonzero polynomial $f(x)$ in $\mathbb{Q}[x]$, let

$$f^*(x) = \frac{f(x)}{\mathrm{c}(f)}.$$

Note that $\deg(f^*) = \deg(f)$.

Theorem 4.2. Let $f(x)$ be a nonzero polynomial in $\mathbb{Q}[x]$. Then $f^*(x)$ is a primitive polynomial, hence an element of $\mathbb{Z}[x]$. Furthermore, $f(x) = \mathrm{c}(f)f^*(x)$ expresses $f(x)$ uniquely as the product of a positive rational number and a primitive polynomial.

Proof. By Theorem 4.1(b), $c(f^*) = 1$, so $f^*(x)$ is primitive. Suppose that $f(x) = rg(x)$ for some positive rational number r and some primitive polynomial $g(x)$. Again by Theorem 4.1(b), $c(f) = rc(g) = r$, which implies that $f^*(x) = g(x)$. □

Theorem 4.3 (Gauss's Lemma). If $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ are primitive polynomials, then so is $f(x)g(x)$.

Proof. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

and

$$f(x)g(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \cdots + c_1 x + c_0.$$

Suppose, for a contradiction, that $f(x)g(x)$ is not primitive. Then there is a prime p that divides each of the coefficients of $f(x)g(x)$. Since $f(x)$ and $g(x)$ are primitive, each has a coefficient that is not divisible by p. Let i and j be the smallest values of the indices such that a_i and b_j are not divisible by p. Then p divides each term on the right-hand side of

$$a_i b_j = c_{i+j} - (a_{i+j}b_0 + \cdots + a_{i+1}b_{j-1} + a_{i-1}b_{j+1} + \cdots + a_0 b_{i+j})$$

so p divides a_i or b_j. This contradiction shows that $f(x)g(x)$ is primitive. □

Theorem 4.4. Let $f(x)$ and $g(x)$ be nonzero polynomials in $\mathbb{Q}[x]$. Then

$$c(fg) = c(f)c(g) \quad \text{and} \quad (fg)^*(x) = f^*(x)g^*(x).$$

Proof. We have from $f(x) = c(f)f^*(x)$ and $g(x) = c(g)g^*(x)$ that

$$f(x)g(x) = c(f)c(g)f^*(x)g^*(x).$$

By Theorem 4.3, $f^*(x)g^*(x)$ is primitive, and since $c(f)$ and $c(g)$ are positive rational numbers, so is $c(f)c(g)$. It follows from the uniqueness property of Theorem 4.2 that $c(fg) = c(f)c(g)$ and $(fg)^*(x) = f^*(x)g^*(x)$. □

We say that a nonconstant polynomial $f(x)$ in $\mathbb{Z}[x]$ is *irreducible* over $\mathbb{Z}$ if it cannot be written as the product of two polynomials in $\mathbb{Z}[x]$, each of degree less than $\deg(f)$; otherwise $f(x)$ is said to be *reducible* over $\mathbb{Z}$.

Theorem 4.5. Let $f(x)$ be a nonconstant polynomial in $\mathbb{Z}[x]$. If $f(x)$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x) = g(x)h(x)$ for some polynomials $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$, each of degree less than $\deg(f)$. By Theorem 4.4, $f(x) = c(g)c(h)g^*(x)h^*(x)$. Since $f(x)$ is in $\mathbb{Z}[x]$, $c(f) = c(g)c(h)$ is a natural number. By Theorem 4.2, $g^*(x)$ and $h^*(x)$ are in $\mathbb{Z}[x]$. Therefore, $f(x)$ is reducible over $\mathbb{Z}$. □

Theorem 4.6 (Eisenstein's Criterion[1]). Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a nonconstant polynomial in $\mathbb{Z}[x]$. If there is a prime p such that (i) p divides $a_0, a_1, \ldots, a_{n-1}$, (ii) p does not divide a_n, and (iii) p^2 does not divide a_0, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. In view of Theorem 4.5, it is sufficient to show that $f(x)$ is irreducible over $\mathbb{Z}$. Suppose, for a contradiction, that $f(x)$ is reducible over $\mathbb{Z}$. Let $g(x)$ and $h(x)$ be nonconstant polynomials in $\mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$, where

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

and

$$h(x) = c_l x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + c_0.$$

By properties (i) and (iii), $a_0 = b_0 c_0$ is divisible by p but not by p^2. Therefore, p divides b_0 or c_0, but not both. Suppose that p divides b_0 (and not c_0). By property (ii), p does not divide $a_n = b_m c_l$, so p does not divide b_m. Let j be the smallest value of the index such that p does not divide b_j. Since $m < n$, we have $1 \le j \le m - 1 < n - 1$. By property (i), a_j is divisible by p. Then p divides each term on the right-hand side of

$$b_j c_0 = a_j - (b_{j-1}c_1 + b_{j-2}c_2 + \cdots + b_1 c_{j-1} + b_0 c_j)$$

so p divides b_j or c_0. This contradiction shows that $f(x)$ is irreducible over $\mathbb{Z}$. □

Example 4.7. By Eisenstein's criterion with $p = 2$, the polynomial $g(y) = y^3 - 6y + 2$ in Example 1.3 is irreducible over $\mathbb{Q}$. ◊

[1]Ferdinand Gotthold Max Eisenstein (1823–1852) was a prolific German mathematician who made significant contributions to number theory.

Example 4.8. Let p be an odd prime and let

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Substituting $x = y + 1$ into $\Phi_p(x)$ and using the binomial formula (E.1), we obtain

$$\Phi_p(y + 1) = \frac{(y + 1)^p - 1}{y} = \sum_{i=1}^{p} \binom{p}{i} y^{i-1}.$$

Condition (i) of Eisenstein's criterion is satisfied because, as pointed out in the proof of Theorem E.7, $\binom{p}{i}$ is divisible by p for $i = 1, 2, \ldots, p - 1$. Since $\binom{p}{p} = 1$ and $\binom{p}{1} = p$, conditions (ii) and (iii) are also met. Thus, $\Phi_p(y + 1)$ is irreducible over $\mathbb{Q}$, and therefore, so is $\Phi_p(x)$. ◊

4.2 IRREDUCIBILITY AND SPLITTING FIELDS

We have defined a splitting field over a field F to be an extension K that is generated over F by (all) the roots of some polynomial in $F[x]$. As will become evident in subsequent chapters, splitting fields are central to discussions of solvability by radicals. They have a range of interesting properties, one of the most important of which is captured by the next result.

Theorem 4.9. If K is a splitting field over F, then every polynomial in $F[x]$ that is irreducible over F and has a root in K splits over K; equivalently, $\min(\alpha, F)$ splits over K for every α in K.

Proof. Let K be the splitting field over F of the polynomial $f(x)$ in $F[x]$, and let $f(x)$ have the roots $\beta_1, \beta_2, \ldots, \beta_n$. Let

$$f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} + \cdots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n$$

and let $s_1, s_2, \ldots, s_n$ be the elementary symmetric polynomials in $x_1, x_2, \ldots, x_n$ over F. Then $s_i(\beta_1, \beta_2, \ldots, \beta_n) = a_i$ for $i = 1, 2, \ldots, n$. Take α in K. By Theorem 2.20, there is a polynomial p in $F[x_1, x_2, \ldots, x_n]$ such that $\alpha = p(\beta_1, \beta_2, \ldots, \beta_n)$. Let

$$\begin{aligned} g(x) &= \prod_{\sigma \in S_n} [x - p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})] \\ &= \sum_{j=0}^{n!} q_j(x_1, x_2, \ldots, x_n) x^j \end{aligned} \tag{4.2}$$

where each q_j is a polynomial in $F[x_1, x_2, \ldots, x_n]$. Since the coefficients of $g(x)$ are the "elementary symmetric polynomials" in the $p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$, they are symmetric in $x_1, x_2, \ldots, x_n$ over F. It follows from the FTSP that for each j,

$$q_j(x_1, x_2, \ldots, x_n) = q_j'(s_1, s_2, \ldots, s_n)$$

for some polynomial q_j' in $F[y_1, y_2, \ldots, y_n]$. Thus,

$$g(x) = \sum_{j=0}^{n!} q_j'(s_1, s_2, \ldots, s_n)x^j. \tag{4.3}$$

Substituting $x_i = \beta_i$ into (4.2) is the same as substituting $s_i = a_i$ into (4.3). Therefore,

$$h(x) = \sum_{j=0}^{n!} q_j'(b_1, b_2, \ldots, b_n)x^j$$

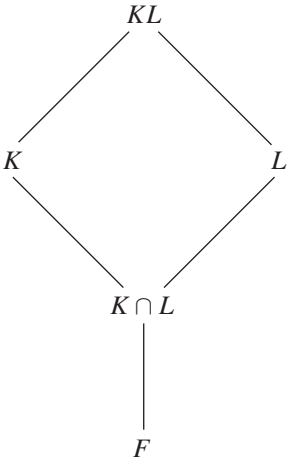
is a polynomial in $F[x]$ that has α as a root. By construction, $h(x)$ splits over K, and since $\min(\alpha, F)$ divides $h(x)$, it too splits over K. □

Let K and L be extensions of F that are contained in a common extension M. We define the *compositum* KL of K and L to be the smallest field in M that contains both K and L. *Whenever a compositum is being formed, it will be assumed (if it is not explicitly stated) that the fields involved are contained in some larger extension*. Stopping to prove the existence of such "closures" would take us beyond the scope of this book. When K and L are finite extensions of F, their compositum is readily characterized. In this case, by Theorem 2.23, $K = F(\theta)$ and $L = F(\psi)$ for some θ in K and some ψ in L. Let M be the splitting field of $\min(\theta, F) \cdot \min(\psi, F)$. Then $KL = F(\theta, \psi)$.

Continuing with F, K, and L as above, let α in K be algebraic over L, and let $g(x) = \min(\alpha, L)$. Then $g(x)$ is irreducible over any subfield E of L such that $g(x)$ is in $E[x]$. In this case, $g(x) = \min(\alpha, E)$. The next result shows that if K is a splitting field over F, then $K \cap L$ is an instance of such an E. We note in passing that the smallest field between F and L with this property is the one generated over F by the coefficients of $g(x)$.

Theorem 4.10. Let K be a splitting field over F, and let L be a finite extension of F. Then:

(a) KL is a splitting field over L.
(b) $\min(\alpha, L) = \min(\alpha, K \cap L)$ for all α in K.
(c) $[KL : L] = [K : K \cap L]$.
(d) $[KL : F] = \dfrac{[K : F][L : F]}{[K \cap L : F]}$.



Proof. (a): Suppose that K is the splitting field over F of some polynomial $h(x)$ in $F[x]$, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $h(x)$. Then $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, hence $KL = L(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Viewing $h(x)$ as a polynomial in $L[x]$, we see that KL is the splitting field of $h(x)$ over L.

(b): We have from Theorem 2.21 that α is algebraic over F, hence algebraic over $K \cap L$; and we have from Theorem 2.21 and part (a) that α is algebraic over L. Let $f(x) = \min(\alpha, K \cap L)$ and $g(x) = \min(\alpha, L)$. Since K is a splitting field over F, by Theorem 2.27, it is a splitting field over $K \cap L$. It follows from Theorem 4.9 that $f(x)$ splits over K. Since $f(x)$ is in $L[x]$, it is divisible by $g(x)$, so $g(x)$ splits over K. The coefficients of $g(x)$ are, up to a sign, the "elementary symmetric polynomials" in its roots, hence $g(x)$ is in $K[x]$. Thus, $g(x)$ is in $(K \cap L)[x]$, and it is therefore divisible by $f(x)$. Since $f(x)$ and $g(x)$ are monic polynomials that divide each other, they are equal.

(c): By Theorem 2.23, $K = F(\theta)$ for some θ in K. Then $KL = L(\theta)$ and $K = (K \cap L)(\theta)$. It follows from part (b) and Theorem 2.12(b) that

$$\begin{aligned}[KL : L] &= [L(\theta) : L] = \deg(\theta, L) = \deg(\theta, K \cap L) \\ &= [(K \cap L)(\theta) : K \cap L] = [K : K \cap L].\end{aligned}$$

(d): We have from part (c) that

$$[KL : F] = [KL : L][L : F] = [K : K \cap L][L : F] = \frac{[K : F][L : F]}{[K \cap L : F]}.$$

□

As an illustration, Theorem 4.10(c) implies that

$$\begin{aligned}[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] &= [\mathbb{Q}(\sqrt{3})\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \\ &= [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{2})] \\ &= [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2. \qquad (4.4)\end{aligned}$$

4.3 FACTORIZATION AND ADJUNCTION

Let $f(x)$ be a polynomial in $F[x]$ that is irreducible over F. We are interested in exploring the manner in which $f(x)$ factors (or not) when F is extended by the adjunction of an element β that is algebraic over F. Suppose that $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x)$ and $h(x)$ in $F(\beta)[x]$. We claim that both $g(x)$ and $h(x)$ have at least one coefficient in $F(\beta)\backslash F$, the set of elements in $F(\beta)$ that are not in F. Certainly one of them does, otherwise $g(x)h(x)$ would be a factorization of $f(x)$ over F. Suppose that $g(x)$ has a coefficient in $F(\beta)\backslash F$. Then $h(x)$ must also have a coefficient in $F(\beta)\backslash F$, otherwise, by the Division Algorithm, $f(x) = q(x)h(x) + r(x)$ for $q(x)$ and $r(x)$ in $F[x]$, with $\deg(r) < \deg(h)$ or $r(x) = 0$. Then $r(x) = h(x)[g(x) - q(x)]$, which contradicts the properties of $r(x)$. So, there are polynomials $g'(x, y)$ and $h'(x, y)$ in $F[x, y]\backslash F[x]$ such that $g(x) = g'(x, \beta)$ and $h(x) = h'(x, \beta)$. In this way, we can express the factorization of $f(x)$ over $F(\beta)$ as $f(x) = g'(x, \beta)h'(x, \beta)$.

We now examine in greater detail certain algebraic properties of $p(x, \beta)$, where $p(x, y)$ is an arbitrary polynomial in $F[x, y]$. Note that $p(x, y)$ can be expressed in the form

$$p(x, y) = c_n(y)x^n + c_{n-1}(y)x^{n-1} + \cdots + c_1(y)x + c_0(y)$$

where $c_i(y)$ is a polynomial in $F[y]$ for $i = 0, 1, \ldots, n$.

Let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the conjugates of β over F. We will have occasion to consider

$$p(x, \beta_j) = c_n(\beta_j)x^n + c_{n-1}(\beta_j)x^{n-1} + \cdots + c_1(\beta_j)x + c_0(\beta_j)$$

for $j = 1, 2, \ldots, m$.

Evidently, $p(x, \beta_j)$ is a polynomial in $F(\beta_j)[x]$, and if $p(x, \beta)$ is monic, then so is $p(x, \beta_j)$. An important observation is that, for each i, $c_i(\beta) = 0$ if and only if $c_i(\beta_j) = 0$ for each j. This has a number of implications: the $p(x, \beta_j)$ all have the same degree; $p(x, \beta)$ is a constant polynomial in $F(\beta)[x]$ if and only if $p(x, \beta_j)$ is a constant polynomial in $F(\beta_j)[x]$ for each j; and $p(x, \beta)$ is the zero polynomial in $F(\beta)[x]$ if and only if $p(x, \beta_j)$ is the zero polynomial in $F(\beta_j)[x]$ for each j.

Theorem 4.11. In the above notation, if $p(x, \beta) = r(x, \beta)s(x, \beta)$ for some polynomials $r(x, y)$ and $s(x, y)$ in $F[x, y]$, then $p(x, \beta_j) = r(x, \beta_j)s(x, \beta_j)$ for $j = 1, 2, \ldots, m$.

Proof. Since $p(x, \beta) - r(x, \beta)s(x, \beta)$ is the zero polynomial in $F(\beta)[x]$, it follows from the above remarks that $p(x, \beta_j) - r(x, \beta_j)s(x, \beta_j)$ is the zero polynomial in $F(\beta_j)[x]$ for each j. □

Theorem 4.12. In the above notation, if $p(x,\beta)$ is irreducible over $F(\beta)$, then $p(x,\beta_j)$ is irreducible over $F(\beta_j)$ for $j = 1, 2, \ldots, m$.

Proof. Suppose that $p(x,\beta_j)$ is reducible over $F(\beta_j)$ for some $1 \le j \le m$. Then there are polynomials $r(x,y)$ and $s(x,y)$ in $F[x,y]$ such that $p(x,\beta_j) = r(x,\beta_j)s(x,\beta_j)$, where $r(x,\beta_j)$ and $s(x,\beta_j)$ both have degree less than that of $p(x,\beta_j)$. With the roles of β and β_j reversed, it follows from Theorem 4.11 and earlier remarks that $p(x,\beta) = r(x,\beta)s(x,\beta)$, where $r(x,\beta)$ and $s(x,\beta)$ both have degree less than $p(x,\beta)$. Thus, $p(x,\beta)$ is reducible over $F(\beta)$. □

Theorem 4.13. Let α and β be algebraic over F, let

$$f(x) = \min(\alpha, F) \quad r(x,\beta) = \min(\alpha, F(\beta)) \quad \text{and} \quad h(x) = \min(\beta, F)$$

and let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the roots of $h(x)$. Then:

(a)
$$[f(x)]^e = r(x,\beta_1)r(x,\beta_2)\cdots r(x,\beta_m) \tag{4.5}$$

where
$$e = [F(\alpha,\beta) : F(\alpha)].$$

(b) If $F(\alpha)$ is a splitting field over F, then $\deg(r)$ divides $\deg(f)$, and $\deg(f)/\deg(r)$ divides $\deg(h)$.

Proof. (a): We have $\deg(h) = m$. Since $r(x,\beta)$ divides $f(x)$, there is a polynomial $s(x,y)$ in $F[x,y]$ such that $f(x) = r(x,\beta)s(x,\beta)$. Given that $f(x)$ and $r(x,\beta)$ are monic, so is $s(x,\beta)$. By Theorem 4.11,

$$f(x) = r(x,\beta_j)s(x,\beta_j) \tag{4.6}$$

for $j = 1, 2, \ldots, m$. Taking the product of both sides of (4.6) over j gives

$$[f(x)]^m = R(x)S(x) \tag{4.7}$$

where
$$R(x) = r(x,\beta_1)r(x,\beta_2)\cdots r(x,\beta_m)$$

and
$$S(x) = s(x,\beta_1)s(x,\beta_2)\cdots s(x,\beta_m).$$

Since the coefficients of $R(x)$ and $S(x)$ are symmetric in $\beta_1, \beta_2, \ldots, \beta_m$, by the FTSP, $R(x)$ and $S(x)$ are in $F[x]$. Furthermore, since $r(x,\beta)$ and $s(x,\beta)$ are monic, so are $R(x)$ and $S(x)$. By Theorem 2.8, $R(x)$ and $S(x)$ each have a

factorization into polynomials in $F[x]$ that are monic and irreducible over F. The product of these factorizations is a factorization of $R(x)S(x)$. Since the left-hand side of (4.7) is such a factorization, the uniqueness of factorization of $R(x)$ implies that $R(x) = [f(x)]^e$ for some e, that is,

$$[f(x)]^e = r(x, \beta_1)r(x, \beta_2) \cdots r(x, \beta_m). \tag{4.8}$$

Comparing degrees in (4.8), we find that

$$e \deg(f) = m \deg(r) = \deg(r) \deg(h) \tag{4.9}$$

or equivalently,

$$e = \frac{\deg(\alpha, F(\beta)) \deg(\beta, F)}{\deg(\alpha, F)}.$$

It follows from Theorem 2.12(b) that

$$e = \frac{[F(\alpha, \beta) : F(\beta)][F(\beta) : F]}{[F(\alpha) : F]} = [F(\alpha, \beta) : F(\alpha)].$$

(b): Since $F(\alpha)$ is a splitting field over F, setting $K = F(\alpha)$ and $L = F(\beta)$ in Theorem 4.10(c) yields

$$\deg(r) = [F(\alpha, \beta) : F(\beta)] = [F(\alpha) : F(\alpha) \cap F(\beta)].$$

As in part (a), we have

$$\deg(f) = [F(\alpha) : F] \quad \text{and} \quad \deg(h) = [F(\beta) : F].$$

It is now easily verified that $\deg(r)$ divides $\deg(f)$ and that $\deg(f)/\deg(r)$ divides $\deg(h)$. □

The factorization (4.5) is of interest, but it is not all that could be hoped for. First, it is factorization of a power of $f(x)$, not of $f(x)$ itself (except when $e = 1$). Second, and more disappointing, the terms in the factorization are polynomials that are irreducible over different fields. Obviously, what we would like to have is a factorization of $f(x)$ into polynomials over the same field that are irreducible over that field, in particular the field $F(\beta)$. Recall that such a factorization is provided by Theorem 2.8. We now show that when $F(\beta)$ is a splitting field over F, this factorization has an especially appealing form.

Theorem 4.14. Let α and β be algebraic over F, let

$$f(x) = \min(\alpha, F) \quad r(x, \beta) = \min(\alpha, F(\beta)) \quad \text{and} \quad h(x) = \min(\beta, F)$$

and let $\beta = \beta_1, \beta_2, \ldots, \beta_m$ be the roots of $h(x)$. Suppose that $F(\beta)$ is a splitting field over F. Then:

(a) Renumbering $\beta_2, \beta_3, \ldots, \beta_m$ if necessary,

$$f(x) = r(x, \beta_1) r(x, \beta_2) \cdots r(x, \beta_l)$$

is a factorization of $f(x)$ over $F(\beta)$, where $r(x, \beta_1), r(x, \beta_2), \ldots, r(x, \beta_l)$ are distinct monic polynomials in $F(\beta)[x]$ that are irreducible over $F(\beta)$, and where

$$l = [F(\alpha) \cap F(\beta) : F].$$

(b) If β is in $F(\alpha)$, then $l = m$.
(c) If $F(\alpha) \cap F(\beta) = F$, then $f(x) = r(x, \beta)$.
(d) $\deg(r)$ divides $\deg(f)$, and $\deg(f)/\deg(r)$ divides $\deg(h)$.

Proof. (a): We have $\deg(h) = m$. Since $h(x)$ is irreducible over F, and since $F(\beta)$ is a splitting field over F, by Theorem 4.9, $h(x)$ splits over $F(\beta)$. Therefore, $F(\beta_j) \subseteq F(\beta)$ for $j = 1, 2, \ldots, m$. The reverse inclusion holds by symmetry, so $F(\beta_j) = F(\beta)$ for each j. By Theorems 4.12 and 4.13(a), and in the notation of Theorem 4.13, (4.5) is a factorization of $[f(x)]^e$ into polynomials $r(x, \beta_1), r(x, \beta_2), \ldots, r(x, \beta_m)$ in $F(\beta)[x]$ that are irreducible over $F(\beta)$ and all of the same degree. It follows from Theorem 2.18 that each $r(x, \beta_j)$ has simple roots, and from Theorem 2.7 that any of the $r(x, \beta_j)$ that have a root in common are equal. Again by Theorem 2.18, $f(x)$ has simple roots, so each root of $[f(x)]^e$ is repeated e times. Renumbering $\beta_2, \beta_3, \ldots, \beta_m$ if necessary, it follows that (4.5) can be expressed as

$$[f(x)]^e = [r(x, \beta_1) r(x, \beta_2) \cdots r(x, \beta_l)]^e$$

where

$$l = \frac{m}{e}. \tag{4.10}$$

So,

$$f(x) = \xi r(x, \beta_1) r(x, \beta_2) \cdots r(x, \beta_l)$$

for some eth root of unity ξ. Since $f(x)$ and the $r(x, \beta_j)$ are monic, $\xi = 1$. Therefore,

$$f(x) = r(x, \beta_1) r(x, \beta_2) \cdots r(x, \beta_l). \tag{4.11}$$

Comparing degrees in (4.11) shows that

$$l = \frac{\deg(f)}{\deg(r)} = \frac{[F(\alpha) : F]}{[F(\alpha, \beta) : F(\beta)]} = \frac{[F(\beta) : F]}{[F(\alpha, \beta) : F(\alpha)]}. \tag{4.12}$$

Since $F(\beta)$ is a splitting field over F, setting $K = F(\beta)$ and $L = F(\alpha)$ in Theorem 4.10(c) gives

$$[F(\alpha, \beta) : F(\alpha)] = [F(\beta) : F(\alpha) \cap F(\beta)].$$

Therefore,

$$l = [F(\alpha) \cap F(\beta) : F]. \tag{4.13}$$

(b), (c): This follows from (4.13).

(d): That $\deg(r)$ divides $\deg(f)$ follows from the first identity in (4.12). That $\deg(f)/\deg(r)$ divides $\deg(h)$ follows from (4.10) and (4.12). □

Example 4.15 (5th root of unity). Continuing with Example 1.4, recall that the roots of

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

are ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4, where

$$\zeta_5 = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right).$$

According to Example 4.8, $\Phi_5(x)$ is irreducible over $\mathbb{Q}$, so $\Phi_5(x) = \min(\zeta_5, \mathbb{Q})$. We illustrate Theorem 4.14(a) with $F = \mathbb{Q}$, $\alpha = \zeta_5$, and $\beta = \sqrt{5}$. Directly from (1.29), we have

$$\zeta_5 + \zeta_5^4 = \frac{-1 + \sqrt{5}}{2} \quad \text{and} \quad \zeta_5^2 + \zeta_5^3 = \frac{-1 - \sqrt{5}}{2} \tag{4.14}$$

hence

$$\begin{aligned}\Phi_5(x) &= [(x - \zeta_5)(x - \zeta_5^4)][(x - \zeta_5^2)(x - \zeta_5^3)] \\ &= \left[x^2 + \left(\frac{1 - \sqrt{5}}{2}\right)x + 1\right]\left[x^2 + \left(\frac{1 + \sqrt{5}}{2}\right)x + 1\right].\end{aligned}$$

Let

$$r(x, y) = \frac{2x^2 + x\ - xy + 2}{2}.$$

Then

$$\Phi_5(x) = r(x, \sqrt{5})\, r(x, -\sqrt{5})$$

is a factorization of $\Phi_5(x)$ over $\mathbb{Q}(\sqrt{5})$. Note that $r(x, \sqrt{5})$ is irreducible over $\mathbb{Q}(\sqrt{5})$, otherwise the nonreal complex number ζ_5 would be in $\mathbb{Q}(\sqrt{5})$. We have from (4.14) that $\sqrt{5}$ is in $\mathbb{Q}(\zeta_5)$, hence

$$[\mathbb{Q}(\zeta_5) \cap \mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2.$$

These observations are consistent with Theorem 4.14(a). ◊

Theorem 4.16. Let $f(x)$ and $h(x)$ be polynomials in $F[x]$ that are irreducible over F, let $f(x)$ be of prime degree p, and let β be a root of $h(x)$. Then:
(a) If $f(x)$ is reducible over $F(\beta)$, then p divides $\deg(h)$.
(b) If $f(x)$ is reducible over $F(\beta)$, and $F(\beta)$ is a splitting field over F, then $f(x)$ splits over $F(\beta)$.

Proof. (a): Let α be a root of $f(x)$. Without loss of generality, we may assume that $f(x)$ and $h(x)$ are monic. Then $f(x) = \min(\alpha, F)$ and $h(x) = \min(\beta, F)$. In the notation of Theorems 4.13 and 4.14, $r(x, \beta) = \min(\alpha, F(\beta))$ and (4.9) becomes $ep = \deg(r)\deg(h)$. Since $f(x)$ is reducible over $F(\beta)$, we have $\deg(r) < \deg(f) = p$. Therefore, p cannot divide $\deg(r)$, so it divides $\deg(h)$.

(b): By assumption, $F(\beta)$ is a splitting field over F, so Theorem 4.14 applies, and (4.12) gives $p = l\deg(r)$. Arguing as in part (a), we find that $l = p$ and $\deg(r) = 1$, which means that $f(x)$ splits over $F(\beta)$. □

Theorem 4.17. Let α and β be algebraic over F, let c be an element in F such that $F(\alpha + c\beta) = F(\alpha, \beta)$ (as in the Primitive Element Theorem), and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of α over F. Then

$$\min(\alpha + c\beta, F) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i - c\beta_{ij}) \tag{4.15}$$

where $\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}$ are m distinct conjugates of β over F for $i = 1, 2, \ldots, n$, and where

$$m = [F(\alpha, \beta) : F(\alpha)].$$

Proof. Let

$$f(x) = \min(\alpha + c\beta, F) \quad \text{and} \quad r(x, \alpha) = \min(\alpha + c\beta, F(\alpha)).$$

By Theorem 4.13(a),

$$[f(x)]^e = r(x, \alpha_1) r(x, \alpha_2) \cdots r(x, \alpha_n) \tag{4.16}$$

where

$$e = [F(\alpha + c\beta, \alpha) : F(\alpha + c\beta)] = 1.$$

The determination of e in Theorem 4.13 relied on the Tower Theorem. We now show that $e = 1$ using a different approach. Let $m = \deg(r)$ and $t(x, y) = c^{-m} r(y + cx, y)$. Then

$$t(x, \alpha) = c^{-m} r(\alpha + cx, \alpha)$$

is a (nonconstant) monic polynomial in $F(\alpha)[x]$ of degree m that has β as a root. Furthermore, $t(x, \alpha)$ is irreducible over $F(\alpha)$, otherwise $r(x, \alpha)$ would be reducible over $F(\alpha)$. Therefore, $t(x, \alpha) = \min(\beta, F(\alpha))$. Let $h(x) = \min(\beta, F)$. By Theorem 4.13(a),

$$[h(x)]^d = t(x, \alpha_1) t(x, \alpha_2) \cdots t(x, \alpha_n) \tag{4.17}$$

for some $d \leq n$. We have from Theorem 4.12 that $t(x, \alpha_i)$ is irreducible over $F(\alpha_i)$. It then follows from (4.17) and Theorem 2.18 that the roots of $t(x, \alpha_i)$ are m distinct conjugates of β, which we denote by $\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}$ for each i. Then

$$t(x, \alpha_i) = \prod_{j=1}^{m} (x - \beta_{ij})$$

hence

$$r(x, \alpha_i) = c^m t\left(\frac{x - \alpha_i}{c}, \alpha_i\right) = \prod_{j=1}^{m} (x - \alpha_i - c\beta_{ij}).$$

Since the roots of $t(x, \alpha_i)$ are distinct, so are those of $r(x, \alpha_i)$. Furthermore, the defining property of c ensures that the $r(x, \alpha_i)$ have no roots in common. It follows from (4.16) that $e = 1$ and that

$$f(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i - c\beta_{ij}).$$

Finally, by the Primitive Element Theorem,

$$m = \deg(r) = [F(\alpha + c\beta) : F(\alpha)] = [F(\alpha, \beta) : F(\alpha)].$$

□

Example 4.18. To illustrate Theorem 4.17, let $F = \mathbb{Q}$, $\alpha = \sqrt{2}$, and $\beta = \sqrt{3}$. Recall from (2.16) that

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

and from (4.4) that

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

Thus, in the notation of Theorem 4.17, $m = n = 2$. According to (4.15),

$$\begin{aligned}\min(\sqrt{2}+\sqrt{3},\mathbb{Q}) &= (x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})] \\ &\quad \times (x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}) \\ &= x^4 - 10x^2 + 1.\end{aligned}$$

$\Diamond$

We observe from (4.15) that

$$[F(\alpha,\beta):F] = [F(\alpha+c\beta):F] = mn = [F(\alpha,\beta):F(\alpha)][F(\alpha):F].$$

Thus, during the course of proving Theorem 4.17, we have incidentally proved a version of the Tower Theorem, but using properties of polynomials as opposed to the earlier proof that relied on linear algebra. In a way, this places the Tower Theorem within the classical realm, and to that extent "justifies" its use in this chapter, as well as in Chapters 5–8, where the focus is also on classical results.

CHAPTER 5

ROOTS OF UNITY AND CYCLOTOMIC POLYNOMIALS

5.1 ROOTS OF UNITY

Roots of unity play a central role in the solution of polynomial equations by radicals. In this chapter, some of the basic results on roots of unity are presented in the context of polynomials. We return to the topic in Chapter 10 from the perspective of Galois theory.

The *phi-function* is well known from number theory (Appendix E). For each natural number n, $\varphi(n)$ is defined to be the number of natural numbers less than or equal to n that are relatively prime to n, that is,

$$\varphi(n) = |\{k : 1 \leq k \leq n; \gcd(k, n) = 1\}|.$$

For example, 1, 3, 7, and 9 are the natural numbers between 1 and 10 that are relatively prime to 10, so $\varphi(10) = 4$. By Theorem E.2, if m and n are relatively prime, then

$$\varphi(mn) = \varphi(m)\varphi(n) \tag{5.1}$$

and if $n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ is the factorization of n into distinct primes, then

$$\varphi(n) = p_1^{d_1-1}(p_1 - 1)p_2^{d_2-1}(p_2 - 1) \cdots p_m^{d_m-1}(p_m - 1). \tag{5.2}$$

Note that for a prime p, we have $\varphi(p) = p - 1$.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Let F be a field, and let n be a natural number. Each root of $x^n - 1$ (in the splitting field of $x^n - 1$ over F) is called an nth *root of unity*. The set of all such roots of unity will be denoted by μ_n. Since $D_x(x^n - 1) = nx^{n-1}$, and F has characteristic 0, the remarks following Theorem 2.17 demonstrate that there are n distinct nth roots of unity. Thus, $|\mu_n| = n$. It is readily verified that μ_n is a group under multiplication. In fact, by Theorem E.3, μ_n is cyclic with $\varphi(n)$ generators. Each generator is called a *primitive* nth *root of unity*. The set of all such generators will be denoted by π_n. Thus, $|\pi_n| = \varphi(n)$.

Let ϱ be an element of μ_n. As discussed in Appendix B, the order of ϱ, denoted by $\text{ord}(\varrho)$, is the smallest natural number k such that $\varrho^k = 1$. Since μ_n is cyclic, ϱ generates μ_n if and only if $\text{ord}(\varrho) = n$. Therefore,

$$\pi_n = \{\zeta \in \mu_n : \text{ord}(\zeta) = n\}.$$

Let ζ be an element of π_n in what follows. Since ζ is a generator of μ_n, in the notation of Appendix B, we have

$$\mu_n = \langle \zeta \rangle = \{\zeta^k : 1 \leq k \leq n\}. \tag{5.3}$$

Another characterization of π_n follows from Theorem B.6(a):

$$\pi_n = \{\zeta^k : 1 \leq k \leq n; \gcd(k, n) = 1\}. \tag{5.4}$$

Note that the splitting field of $x^n - 1$ over F is $F(\zeta)$. Let m be a natural number, and let ξ be in π_m. In keeping with the notation established at the beginning of Section 2.5, we have

$$F(\zeta) = F(\mu_n) \qquad F(\xi) = F(\mu_m)$$

and

$$F(\xi, \zeta) = F(\mu_m, \mu_n) = F(\mu_m, \zeta).$$

When the focus is on ζ as an element that has been adjoined to $F(\xi)$, our tendency will be to use the notation $F(\mu_m, \zeta)$ in preference to $F(\xi, \zeta)$ or $F(\mu_m, \mu_n)$.

Theorem 5.1. Let n be a natural number. Then:
(a) d divides n if and only if $\mu_d \subseteq \mu_n$.
(b) $\mu_n = \bigcup_{d|n} \pi_d$, and the union is disjoint.
(c) If ζ is a primitive nth root of unity and d divides n, then $\zeta^{n/d}$ is a primitive dth root of unity.

Proof. Part (a) follows from Theorems B.5 and B.7(a), part (b) from Theorem B.9, and part (c) from Theorem B.7(b). □

For natural numbers m and n, let

$$\mu_m \mu_n = \{\xi\zeta : \xi \in \mu_m, \zeta \in \mu_n\} \quad \text{and} \quad \pi_m \pi_n = \{\xi\zeta : \xi \in \pi_m, \zeta \in \pi_n\}.$$

Theorem 5.2. Let m and n be relatively prime natural numbers. Then:
(a) $\mu_{mn} = \mu_m \mu_n$, and each element of μ_{mn} has a unique expression as an element of $\mu_m \mu_n$.
(b) $\pi_{mn} = \pi_m \pi_n$, and each element of π_{mn} has a unique expression as an element of $\pi_m \pi_n$.

Proof. (a): Take ξ in μ_m and ζ in μ_n. Then $(\xi\zeta)^{mn} = (\xi^m)^n(\zeta^n)^m = 1$, so $\xi\zeta$ is in μ_{mn}, hence $\mu_m\mu_n \subseteq \mu_{mn}$. Conversely, take η in μ_{mn}. Since m and n are relatively prime, by Theorem E.1, there are integers a and b such that $am + bn = 1$. We have from $(\eta^{am})^n = 1$ that η^{am} is in μ_n; likewise η^{bn} is in μ_m. Thus, $\eta = \eta^{am}\eta^{bn}$ is in $\mu_m\mu_n$, hence $\mu_{mn} \subseteq \mu_m\mu_n$. Therefore, $\mu_{mn} = \mu_m\mu_n$. Since $|\mu_{mn}| = mn$ and $|\mu_m\mu_n| \leq mn$, we see that each $\xi\zeta$, with ξ in μ_m and ζ in μ_n, is a unique element of $\mu_m\mu_n$.

(b): Take ξ in π_m and ζ in π_n. By Theorem B.4, $\text{ord}(\xi\zeta) = mn$, so $\xi\zeta$ is in π_{mn}, hence $\pi_m\pi_n \subseteq \pi_{mn}$. Conversely, take η in π_{mn}. Since $am + bn = 1$, we have $\gcd(a, n) = 1$, thus $\gcd(am, mn) = m$. By Theorem B.3, $\text{ord}(\eta^{am}) = n$, so η^{am} is in π_n; likewise η^{bn} is in π_m. Thus, $\eta = \eta^{am}\eta^{bn}$ is in $\pi_m\pi_n$, hence $\pi_{mn} \subseteq \pi_m\pi_n$. Therefore, $\pi_{mn} = \pi_m\pi_n$. The uniqueness property follows from part (a). □

5.2 CYCLOTOMIC POLYNOMIALS

For the remainder of the chapter, we assume that $F = \mathbb{Q}$. This is not much of a restriction, as in this book we are focused almost exclusively on fields of characteristic 0, and all such fields contain an isomorphic copy of $\mathbb{Q}$. For each natural number n, let

$$\zeta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

In particular, $\zeta_4 = i$, and with ω as defined in (1.13), $\zeta_3 = \omega$. Evidently, ζ_n is a primitive nth root of unity, so

$$\mu_n = \langle\zeta_n\rangle = \{\zeta_n^k : 1 \leq k \leq n\}$$

and

$$\pi_n = \{\zeta_n^k : 1 \leq k \leq n; \gcd(k, n) = 1\}.$$

We refer to $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$ as the nth *cyclotomic field*. The nth *cyclotomic polynomial* is

$$\Phi_n(x) = \prod_{\zeta\in\pi_n}(x - \zeta). \tag{5.5}$$

We see in Theorem 5.6(a) that the notation $\Phi_n(x)$ is consistent with Examples 1.4 and 4.8.

Theorem 5.3. For all natural numbers n, $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$ and

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{5.6}$$

Proof. It is clear from (5.5) that $\Phi_n(x)$ is monic and has degree $\varphi(n)$. The proof that $\Phi_n(x)$ is in $\mathbb{Z}[x]$ proceeds by induction on n. The result is trivial for $n = 1$. Suppose that $n > 1$. It follows from Theorem 5.1(b) that

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d|n} \left[\prod_{\zeta \in \pi_d} (x - \zeta) \right] = \prod_{d|n} \Phi_d(x).$$

By the induction hypothesis, $\Phi_d(x)$ is in $\mathbb{Z}[x]$ for each $1 \le d < n$. Therefore,

$$h(x) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$$

is in $\mathbb{Z}[x]$ and $\Phi_n(x) = (x^n - 1)/h(x)$. Since $x^n - 1$ and $h(x)$ are in $\mathbb{Z}[x]$, and $h(x)$ is monic, it follows from the Division Algorithm that $\Phi_n(x)$ is in $\mathbb{Z}[x]$. □

The factorization in (5.6) makes it possible to compute $\Phi_n(x)$ recursively. For example, from $\Phi_1(x) = x - 1$ and $\Phi_1(x)\Phi_3(x) = x^3 - 1$, we have

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

The following table gives explicit expressions for $\Phi_n(x)$ for $n = 1, 2, \ldots, 10$.

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

It is possible to draw certain inferences about primitive roots of unity directly from the $\Phi_n(x)$. For example, since ω is a root of $\Phi_3(x)$, $-\omega$ is a root of $\Phi_6(x)$, so $-\omega$ is a primitive 6th root of unity.

Theorem 5.4. Let n be a natural number, and let ζ be a primitive nth root of unity. Then:
(a) $\Phi_n(x) = \min(\zeta, \mathbb{Q})$.
(b) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Proof. (a): Let $f(x) = \min(\zeta, \mathbb{Q})$ and $h(x) = x^n - 1$. Since $h(x)$ has simple roots, by Theorem 2.8,

$$h(x) = g_1(x)g_2(x)\cdots g_m(x)$$

where $g_1(x), g_2(x), \ldots, g_m(x)$ are distinct monic polynomials in $\mathbb{Q}[x]$ that are irreducible over $\mathbb{Q}$. Since $c(h) = 1$, it follows from Theorem 4.4 that

$$h(x) = h^*(x) = g_1^*(x)g_2^*(x)\cdots g_m^*(x)$$

where $g_1^*(x), g_2^*(x), \ldots, g_n^*(x)$ are distinct monic, primitive polynomials that are irreducible over $\mathbb{Q}$. Therefore, $f(x) = g_j^*(x)$ for some $1 \le j \le m$, hence $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ that is irreducible over $\mathbb{Q}$.

For each natural number k, let $f_k(x) = f(x^k)$. Since $f(x)$ and $f_k(x)$ are in $\mathbb{Z}[x]$, and $f(x)$ is monic, it follows from the Division Algorithm that there are polynomials $q_k(x)$ and $r_k(x)$ in $\mathbb{Z}[x]$ such that

$$f_k(x) = q_k(x)f(x) + r_k(x)$$

with $\deg(r_k) < \deg(f)$ or $r_k(x) = 0$.

Claim I. $\{r_k(x) : k = 1, 2, 3, \ldots\} = \{r_1(x), r_2(x), \ldots, r_n(x)\}$.
Since $\zeta^{k+n} = \zeta^k$, ζ is a root of $f_{k+n}(x) - f_k(x)$, so $f(x)$ divides $f_{k+n}(x) - f_k(x)$. It follows from

$$f_{k+n}(x) - f_k(x) = [q_{k+n}(x) - q_k(x)]\, f(x) + r_{k+n}(x) - r_k(x)$$

that $f(x)$ divides $r_{k+n}(x) - r_k(x)$. Since $\deg(f) > \deg(r_{k+n} - r_k)$, we have $r_{k+n}(x) - r_k(x) = 0$. This proves the claim.

Claim II. Let $C = \max\{c(r_1), c(r_2), \ldots, c(r_n)\}$. If p is a prime greater than C, then $f(x)$ divides $f_p(x)$.
We have from Theorem E.7 that

$$[f(x)]^p = f_p(x) - pg_p(x)$$

where $g_p(x)$ is a polynomial in $\mathbb{Z}[x]$. Since $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$, by the Division Algorithm, there are polynomials $q_p'(x)$ and $r_p'(x)$ in $\mathbb{Z}[x]$ such that

$$g_p(x) = q_p'(x)f(x) + r_p'(x)$$

with $\deg(r'_p) < \deg(f)$ or $r'_p(x) = 0$. We now have two expressions for $f_p(x)$:

$$f_p(x) = q_p(x)f(x) + r_p(x)$$

with $\deg(r_p) < \deg(f)$ or $r_p(x) = 0$, and

$$\begin{aligned} f_p(x) &= [f(x)]^p + pg_p(x) \\ &= \{[f(x)]^{p-1} + pq'_p(x)\}f(x) + pr'_p(x) \end{aligned}$$

with $\deg(pr'_p) = \deg(r'_p) < \deg(f)$ or $pr'_p(x) = 0$. It follows from the uniqueness property of the Division Algorithm that $r_p(x) = pr'_p(x)$, hence $c(r_p) = pc(r'_p)$. Suppose that $r_p(x) \neq 0$. Then $c(r_p) \geq p > C$, but according to Claim I, $c(r_p) \leq C$. Thus, $r_p(x) = 0$, hence $f(x)$ divides $f_p(x)$. This proves the claim.

Claim III. If k is a natural number less than n and $\gcd(k, n) = 1$, then ζ^k is a root of $f(x)$.

With C as in Claim II, let P be the product of all primes less than or equal to C that do not divide k, and let $N = k + nP$. Since $\zeta^N = \zeta^k$, it is sufficient to show that ζ^N is a root of $f(x)$. It follows from the definitions that k and nP are relatively prime. Therefore, any prime less than or equal to C divides k or nP, but not both. Thus, any prime dividing N must be greater than C. It follows that the prime factorization of N (into not necessarily distinct primes) is of the form $N = p_1 p_2 \cdots p_s$, where $p_j > C$ for $j = 1, 2, \ldots, s$. By Claim II, $f(x)$ divides $f_{p_1}(x)$, so ζ is a root of $f_{p_1}(x)$, hence ζ^{p_1} is a root of $f(x)$. Similarly, $f(x)$ divides $f_{p_2}(x)$, so ζ^{p_1} is a root of $f_{p_2}(x)$, hence $\zeta^{p_1 p_2}$ is a root of $f(x)$. Proceeding in this way, we find that $\zeta^N = \zeta^{p_1 p_2 \cdots p_s}$ is a root of $f(x)$. This proves the claim.

Since ζ is a root of $\Phi_n(x)$, $f(x) = \min(\zeta, \mathbb{Q})$ divides $\Phi_n(x)$. By Theorem 5.3, $\deg(f) \leq \varphi(n)$. On the other hand, we have from Claim III that $\deg(f) \geq \varphi(n)$. Therefore, $\deg(f) = \varphi(n)$. Since $f(x)$ and $\Phi_n(x)$ are monic, it follows that $f(x) = \Phi_n(x)$.

(b): By part (a), and Theorems 2.12(b) and 5.3,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n).$$

□

Theorem 5.4 is another of those theorems that will be used repeatedly, often without being specifically referenced.

It follows from Theorems 5.3 and 5.4(a) that (5.6) is a factorization of $x^n - 1$ into polynomials in $\mathbb{Q}[x]$ that are irreducible over $\mathbb{Q}$. In fact, it is the factorization guaranteed by Theorem 2.8.

Let $\mathcal{R}$ be a commutative ring with multiplicative identity. The set of elements in $\mathcal{R}$ that have a multiplicative inverse in $\mathcal{R}$ (that is, the units) will be denoted by $\mathcal{R}^\times$. It is easily verified that $\mathcal{R}^\times$ is a group under multiplication. For a field F, we have $F^\times = F\backslash\{0\}$.

For each natural number n, let $n\mathbb{Z}$ be the principal ideal generated by n in the ring $\mathbb{Z}$, and let us denote by $\mathbb{Z}/n\mathbb{Z}$ the corresponding quotient ring, that is,

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \{k + n\mathbb{Z} : k \in \mathbb{Z}\} \\ &= \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}.\end{aligned}$$

We are interested in characterizing $(\mathbb{Z}/n\mathbb{Z})^\times$. If $k + n\mathbb{Z}$ is in $(\mathbb{Z}/n\mathbb{Z})^\times$, then $ak \equiv 1 \pmod{n}$ for some a in $\mathbb{Z}$. Then $ak + bn = 1$ for some b in $\mathbb{Z}$, hence k and n are relatively prime. Conversely, if k in $\mathbb{Z}$ is relatively prime to n, then, by Theorem E.1, there are c and d in $\mathbb{Z}$ such that $ck + dn = 1$. Thus, $ck \equiv 1 \pmod{n}$, hence $k + n\mathbb{Z}$ is in $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{k + n\mathbb{Z} : k \in \mathbb{Z}; \gcd(k, n) = 1\}.$$

For convenience of exposition, we will usually drop $n\mathbb{Z}$ from the notation for $k + n\mathbb{Z}$ and restrict k to lie between 0 and $n - 1$ inclusive. Accordingly, we have

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n - 1\}. \tag{5.7}$$

and

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{k : 1 \le k \le n; \gcd(k, n) = 1\}. \tag{5.8}$$

We adopt the convention that any calculation taking place in $\mathbb{Z}/n\mathbb{Z}$ or $(\mathbb{Z}/n\mathbb{Z})^\times$ is to be performed modulo n and in such a way that the result is an element of (5.7) or (5.8), respectively. In certain situations, to avoid ambiguity, we will employ the notation "$\equiv$" and "$(\mathrm{mod}\, n)$." Note from (5.8) that $(\mathbb{Z}/n\mathbb{Z})^\times$ is of order $\varphi(n)$. For example, $\varphi(10) = 4$ and $(\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$.

Let p be a prime. In this case, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, and we denote it by $\mathbb{F}_p$. So,

$$\mathbb{F}_p = \{0, 1, \ldots, p - 1\}$$

and

$$\mathbb{F}_p^\times = \{1, 2, \ldots, p - 1\}.$$

By Theorem E.4, $\mathbb{F}_p^\times$ is cyclic with $\varphi(p - 1)$ generators. Each such generator g is referred to as a *primitive congruence root modulo* p. So, we have

$$\mathbb{F}_p^\times = \{g^i \pmod{p} : i = 0, 1, \ldots, p - 2\}. \tag{5.9}$$

Expressed another way: $1, g, g^2, \ldots, g^{p-2} \pmod{p}$ are $1, 2, 3, \ldots, p - 1$ in some order. By Theorem E.5, $g^{p-1} \equiv 1 \pmod{p}$, so the sequence

$$1, g, g^2, g^3, \ldots \pmod{p}$$

repeats cyclically every $p - 1$ terms.

Let ζ be a primitive pth root of unity. Then (5.3) and (5.4) become

$$\mu_p = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$$

and

$$\pi_p = \{\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{p-1}\} = \{\zeta, \zeta^g, \zeta^{g^2}, \ldots, \zeta^{g^{p-2}}\}. \tag{5.10}$$

Theorem 5.5. Let m and n be relatively prime natural numbers, and let ζ be a primitive nth root of unity. Then:
(a) $\mathbb{Q}(\mu_m, \mu_n) = \mathbb{Q}(\mu_{mn})$.
(b) $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.
(c) $[\mathbb{Q}(\mu_m, \mu_n) : \mathbb{Q}(\mu_m)] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$.
(d) $\Phi_n(x) = \min(\zeta, \mathbb{Q}(\mu_m))$.

Proof. Theorem 5.4(b) will be used repeatedly.

(a): We have from Theorem 5.1(a) that $\mu_m, \mu_n \subseteq \mu_{mn}$, hence $\mathbb{Q}(\mu_m, \mu_n) \subseteq \mathbb{Q}(\mu_{mn})$. The reverse inclusion follows from Theorem 5.2(a).

(b): It follows from (5.1) and part (a) that

$$[\mathbb{Q}(\mu_m, \mu_n) : \mathbb{Q}] = [\mathbb{Q}(\mu_{mn}) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n).$$

Since $\mathbb{Q}(\mu_m)$ is the splitting field of $\Phi_m(x)$ over $\mathbb{Q}$, by Theorem 4.10(d),

$$[\mathbb{Q}(\mu_m, \mu_n) : \mathbb{Q}] = \frac{[\mathbb{Q}(\mu_m) : \mathbb{Q}][\mathbb{Q}(\mu_n) : \mathbb{Q}]}{[\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} = \frac{\varphi(m)\varphi(n)}{[\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]}.$$

Therefore, $[\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) : \mathbb{Q}] = 1$, hence $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.

(c): We have from (5.1) and part (a) that

$$\begin{aligned}[\mathbb{Q}(\mu_m, \mu_n) : \mathbb{Q}(\mu_m)] = [\mathbb{Q}(\mu_{mn}) : \mathbb{Q}(\mu_m)] &= \frac{[\mathbb{Q}(\mu_{mn}) : \mathbb{Q}]}{[\mathbb{Q}(\mu_m) : \mathbb{Q}]} \\ &= \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].\end{aligned}$$

(d): Let $h(x) = \min(\zeta, \mathbb{Q}(\mu_m))$. Since $\mathbb{Q}(\mu_m, \zeta) = \mathbb{Q}(\mu_m, \mu_n)$, we have from part (c) and Theorem 2.12(b) that

$$\deg(h) = [\mathbb{Q}(\mu_m, \zeta) : \mathbb{Q}(\mu_m)] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \deg(\Phi_n).$$

Since $h(x)$ divides $\Phi_n(x)$ and both polynomials are monic, it follows that $h(x) = \Phi_m(x)$. □

As an illustration, recall that $\omega = \zeta_3$ and $i = \zeta_4$. Then

$$\mathbb{Q}(\omega, i) = \mathbb{Q}(\mu_3, \mu_4) = \mathbb{Q}(\mu_{12}) = \mathbb{Q}(\zeta_{12})$$

and $\mathbb{Q}(\omega) \cap \mathbb{Q}(i) = \mathbb{Q}$.

Theorem 5.6. Let p be a prime, and let ζ be a primitive pth root of unity. Then:
(a) $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.
(b) $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$ for every natural number k.
(c) $x^{p^{k-1}} - \zeta$ is irreducible over $\mathbb{Q}(\mu_{p-1}, \zeta)$ for every natural number k.

Proof. (a): By Theorem 5.3, $x^p - 1 = (x-1)\Phi_p(x)$, hence

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \tag{5.11}$$

(b): Again by Theorem 5.3,

$$x^{p^k} - 1 = \left[\prod_{j=0}^{k-1} \Phi_{p^j}(x)\right]\Phi_{p^k}(x) = (x^{p^{k-1}} - 1)\Phi_{p^k}(x).$$

It follows from (5.11) that

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \Phi_p(x^{p^{k-1}}).$$

(c): Let η be a root of $h(x) = x^{p^{k-1}} - \zeta$. Then $\eta^{p^{k-1}} = \zeta$, and since $\operatorname{ord}(\zeta) = p$, it follows that $\operatorname{ord}(\eta) = p^k$. That is, η is a primitive p^k root of unity. By Theorems 5.4(b) and 5.5(c),

$$[\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$$

and

$$[\mathbb{Q}(\mu_{p-1}, \eta) : \mathbb{Q}(\mu_{p-1})] = [\mathbb{Q}(\eta) : \mathbb{Q}] = p^{k-1}(p-1).$$

Therefore,

$$[\mathbb{Q}(\mu_{p-1}, \eta) : \mathbb{Q}(\mu_{p-1}, \zeta)] = \frac{[\mathbb{Q}(\mu_{p-1}, \eta) : \mathbb{Q}(\mu_{p-1})]}{[\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})]} = p^{k-1}.$$

Since $h(x)$ is a polynomial in $\mathbb{Q}(\mu_{p-1}, \zeta)[x]$ of degree p^{k-1} that has η as a root, by Theorem 2.12(b), $h(x)$ is irreducible over $\mathbb{Q}(\mu_{p-1}, \zeta)$. □

CHAPTER 6

RADICAL EXTENSIONS AND SOLVABILITY BY RADICALS

In this chapter, we present initial results on the solvability of polynomial equations by radicals, culminating in the first of three versions of the Impossibility Theorem. Other than invoking certain theorems that depend on the FTSP (by virtue of which the symmetric group is involved), the findings presented here are based entirely on methods developed in terms of polynomials and fields. Starting in Chapter 7, we gradually introduce group theory into the discussion of solvability.

6.1 BASIC RESULTS ON RADICAL EXTENSIONS

Let F be a field. A polynomial in $F[x]$ of the form $x^m - a$, where m is a natural number, is classically referred to as a *binomial polynomial* over F. An extension E of F is said to be a *binomial extension* of F if $E = F(\beta)$, where β is the root of a binomial polynomial in $F[x]$. Since $x - 1$ is considered to be a binomial polynomial, F is a binomial extension of itself. For $m > 1$, let $\sqrt[m]{a}$ denote an arbitrary root of $x^m - a$. We say that $\sqrt[m]{a}$ is an mth *root* of a, and in general refer to an expression such as $\sqrt[m]{a}$ as a *radical*. In this notation, $F(\sqrt[m]{a})$ is a binomial extension of F.

Recall that a tower of fields over F is a series of extensions of the form

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_i \subseteq \cdots \subseteq E_n.$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

When $E_i = E_{i+1}$, we say that E_i (or E_{i+1}) is *redundant*. By removing one member of each pair of redundant fields, we create a tower of fields with proper inclusions. An extension R of F is called a *radical extension* of F if there is a tower of fields

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_i \subseteq \cdots \subseteq R_n = R \tag{6.1}$$

where R_i is a binomial extension of R_{i-1} for $i = 1, 2, \ldots, n$. By definition, $R_i = R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{m_i}$ is in R_{i-1} for some natural number m_i for each i. The notion of radical extension is an abstraction of what we observed in Cardan's and Ferrari's formulas, where successive radicals are built up in a step-wise "nested" manner.

Since β_i is a root of the polynomial $x^{m_i} - \beta_i^{m_i}$ in $R_{i-1}[x]$, it follows from Theorem 2.12 that $[R_i : R_{i-1}] \leq m_i$, with equality if and only if $x^{m_i} - \beta_i^{m_i}$ is irreducible over R_{i-1}. So, we have

$$[R : F] \leq [R_n : R_{n-1}][R_{n-1} : R_{n-2}] \cdots [R_1 : R_0] = m_n m_{n-1} \cdots m_1.$$

Thus, R is a finite extension of F, and it follows from Theorem 2.10 that R is an algebraic extension of F. Trivially, a binomial extension of F is a radical extension of F, hence F is a radical extension of itself.

Theorem 6.1. If M_1 is a radical extension of F, and M_2 is a radical extension of M_1, then M_2 is a radical extension of F.

Proof. Straightforward. □

Recall the convention established in Section 4.2 that whenever a compositum is being formed, it is assumed that the fields involved are contained in some larger extension. Let E be an extension of F. Forming the compositum of E and each field in the tower (6.1), we obtain

$$E = ER_0 \subseteq ER_1 \subseteq \cdots \subseteq ER_i \subseteq \cdots \subseteq ER_n = ER \tag{6.2}$$

where $ER_i = ER_{i-1}(\beta_i)$ and $\beta_i^{m_i}$ is in ER_{i-1} for $i = 1, 2, \ldots, n$.

Theorem 6.2. If R is a radical extension of F, and E is an extension of F, then ER is a radical extension of E.

Proof. This follows from the preceding remarks. □

We now come to one of the central themes of this book. Let $f(x)$ be a polynomial in $F[x]$, and let K be the splitting field of $f(x)$ over F. If K is contained in a radical extension of F, we say that $f(x)$ is *solvable by radicals* over F, or that

the roots of $f(x)$ can be expressed in terms of radicals over F. Strictly speaking, we should refer to the polynomial equation $f(x) = 0$ as being solvable by radicals, but the present terminology is standard. It is important to note that the definition of solvability by radicals does not require K to be a radical extension of F, only that K be contained in one.

A "good" definition of solvability should ensure that if a polynomial is solvable by radicals over a given field, it is automatically solvable by radicals over any extension of that field. The next result shows that our definition of solvability meets this requirement.

Theorem 6.3. If $f(x)$ in $F[x]$ is solvable by radicals over F, then $f(x)$ is solvable by radicals over any extension of F.

Proof. Let K be the splitting field of $f(x)$ over F, let R be a radical extension of F that contains K, and let E be an extension of F. The argument used in the proof of Theorem 4.10(a) shows that EK is the splitting field of $f(x)$ over E. By Theorem 6.2, ER is a radical extension of E, and clearly, $EK \subseteq ER$. □

As will become evident shortly, binomial polynomials of prime degree are important in discussions of solvability by radicals. Accordingly, we make the following definitions. An extension E of F is said to be a *prime binomial extension* of F if $E = F(\beta)$, where β is the root of a binomial polynomial in $F[x]$ of prime degree. We say that R is a *prime radical extension* of F if there is a tower of fields of the form (6.1), where R_i is a prime binomial extension of R_{i-1} for $i = 1, 2, \ldots, n$.

The next result shows that prime radical extensions are as plentiful as radical extensions. The essential idea for the proof is straightforward. If a is in F and p and q are primes, then

$$\sqrt[pq]{a} = \sqrt[p]{\sqrt[q]{a}}.$$

It then follows from

$$F \subseteq F(\sqrt[q]{a}) \subseteq F\left(\sqrt[p]{\sqrt[q]{a}}\right)$$

that $F(\sqrt[pq]{a})$ is a prime radical extension of F.

Theorem 6.4. If R is a radical extension of F with $[R : F] > 1$, then R is a prime radical extension of F.

Proof. It is sufficient to prove the assertion for the case where R is a binomial extension of F. Let $R = F(\beta)$, where β^m is in F for some m. Since $[R : F] > 1$,

by Theorem 2.12(a), $m > 1$. Let $m = p_1 p_2 \cdots p_n$ be the factorization of m into not necessarily distinct primes, and let

$$\gamma_0 = \beta^m \quad \text{and} \quad \gamma_i = \beta^{m/m_i} = \sqrt[m_i]{\beta^m}$$

where $m_i = p_1 p_2 \cdots p_i$ for $i = 1, 2, \ldots, n$. Then $\gamma_i^{p_i} = \gamma_{i-1}$ for each i. Let

$$R_0 = F \quad \text{and} \quad R_i = R_{i-1}(\gamma_i) = F(\gamma_i)$$

for each i. Then R_i is a prime binomial extension of R_{i-1} for each i, and we have the tower of fields

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_i \subseteq \cdots \subseteq R_n = R. \tag{6.3}$$

Thus, R is a prime radical extension of F. □

Consider $\sqrt[m]{1}$ for $m > 1$. By definition, $\sqrt[m]{1}$ is an arbitrary but fixed root of $x^m - 1$. According to the above definition of solvability, $\sqrt[m]{1}$ expresses a root of $x^m - 1$ in terms of radicals over $\mathbb{Q}$. We would like to express all the roots of $x^m - 1$ in this way. If we knew that $\sqrt[m]{1}$ is a primitive mth root of unity, then

$$1, \sqrt[m]{1}, (\sqrt[m]{1})^2, \ldots, (\sqrt[m]{1})^{m-1}$$

would be the desired expressions. However, all we can say about $\sqrt[m]{1}$ is that it is one of the m roots of $x^m - 1$, but cannot say which one. It was remarked in connection with Theorem 2.25 that if a polynomial over a field is irreducible over that field, then its roots are algebraically indistinguishable over the field. The fact that $x^m - 1$ is reducible over $\mathbb{Q}$ (as is clear from Theorem 5.3) explains why its roots do not all have the same algebraic properties over $\mathbb{Q}$. These observations suggest that we focus on binomial polynomials that are irreducible over a given field. For this reason, we need to introduce another type of solvability.

An extension E of F is said to be an *irreducible binomial extension* of F if $E = F(\beta)$, where β is the root of a binomial polynomial in $F[x]$ that is irreducible over F. It follows from earlier remarks that if $x^m - \beta^m$ is such an irreducible binomial polynomial, then $m = [F(\beta) : F]$. We say that R is an *irreducible radical extension* of F if there is a tower of fields of the form (6.1), where R_i is an irreducible binomial extension of R_{i-1} for $i = 1, 2, \ldots n$. The revised definition of solvability is as follows. A polynomial $f(x)$ in $F[x]$ is said to be *solvable by irreducible radicals* over F if the splitting field of $f(x)$ over F is contained in an irreducible radical extension of F. Despite the apparent difference between the two definitions of solvability, it will be demonstrated below that they are equivalent. That is, we will show that $f(x)$ is solvable by radicals over F if and only if $f(x)$ is solvable by irreducible radicals over F.

For the remainder of this chapter—indeed, for the rest of the book—our focus will be on solvability by irreducible radicals, and there will be a corresponding emphasis on irreducible radical extensions. This is consistent with the approach taken, for example, by Tignol (2001) and van der Waerden (1991), but the reader is advised that not all authors adopt this perspective.

In what follows, we will have occasion to consider binomial extensions and radical extensions that are both prime and irreducible. Thus, we are led to the following hybrid definition. An extension E of F is said to be a *prime-irreducible binomial extension* of F if $E = F(\beta)$, where β is the root of a binomial polynomial in $F[x]$ that is of prime degree and also irreducible over F. We say that R is a *prime-irreducible radical extension* of F if there is a tower of fields of the form (6.1), where R_i is a prime-irreducible binomial extension of R_{i-1} for $i = 1, 2, \ldots n$.

Theorem 6.5. If R is an irreducible radical extension of F with $[R : F] > 1$, then R is a prime-irreducible radical extension of F.

Proof. It is sufficient to prove the assertion for the case where R is a binomial extension of F. We continue with the notation in the proof of Theorem 6.4. Suppose that $x^m - \beta^m$ is irreducible over F, and let $g_i(x) = x^{p_i} - \gamma_i^{p_i}$ for $i = 1, 2, \ldots, n$. By Theorem 2.12(b), $[R : F] = m$. Since γ_i is a root of $g_i(x)$, we have from Theorem 2.12(a) that $[R_i : R_{i-1}] \leq p_i$ for each i. It follows that

$$m = [R_n : R_{n-1}][R_{n-1} : R_{n-2}] \cdots [R_1 : R_0] \leq p_n p_{n-1} \cdots p_1 = m.$$

So, $[R_i : R_{i-1}] = p_i$, and by Theorem 2.12(b), $g_i(x)$ is irreducible over R_{i-1} for each i. Therefore, R is a prime-irreducible radical extension of F. Note that in the present setting, the inclusions in (6.3) are proper. □

6.2 GAUSS'S THEOREM ON CYCLOTOMIC POLYNOMIALS

The goal of this section is to prove, along with Gauss, that the cyclotomic polynomials are solvable by (irreducible) radicals over $\mathbb{Q}$. In fact, we prove somewhat more.

Recall the remarks on complex numbers made before Theorem 3.18. Let n be a natural number, let ζ be an nth root of unity (not necessarily primitive), and take $1 \leq k \leq n$. Since $\|\zeta^k\| = 1$, we have from (3.25) that

$$\overline{\zeta^k} = \zeta^{-k} = \zeta^{n-k}. \tag{6.4}$$

It follows from (3.24) and (6.4) that

$$\zeta^k + \zeta^{-k} = 2\,\mathrm{Re}(\zeta^k) \tag{6.5}$$

for $k = 0, 1, \ldots, n-1$. In particular,

$$\zeta_n^k + \zeta_n^{-k} = 2\,\mathrm{Re}(\zeta_n^k) = 2\cos\left(\frac{2k\pi}{n}\right)$$

for $k = 0, 1, \ldots, n-1$, where $\zeta_n = e^{2\pi i/n}$.

Example 6.6 (5th root of unity). We encountered the polynomial $\Phi_5(x)$ in Example 1.4, where it was solved by radicals over $\mathbb{Q}$ using Cardan's and Ferrari's formulas. Here we describe another approach that places the problem within the purview of the quadratic formula. Note that

$$\begin{aligned}\frac{\Phi_5(x)}{x^2} &= \frac{(x^4+1)+(x^3+x)+x^2}{x^2} \\ &= \left(x^2+\frac{1}{x^2}\right)+\left(x+\frac{1}{x}\right)+1 \end{aligned} \tag{6.6}$$

and

$$\left(x+\frac{1}{x}\right)^2 = \left(x^2+\frac{1}{x^2}\right)+2.$$

Substituting $y = x + x^{-1}$ into the right-hand side of (6.6) gives

$$g(y) = y^2 + y - 1 \tag{6.7}$$

which has the roots

$$\gamma_1, \gamma_2 = \frac{-1 \pm \sqrt{5}}{2}.$$

We know that $g(y)$ is irreducible over $\mathbb{Q}$, otherwise $\Phi_5(x)$ would be reducible over $\mathbb{Q}$, contradicting Example 4.8 and Theorem 5.4(a). Since $y = (x^2+1)/x$, each of the roots of

$$x^2 - \gamma_1 x + 1 = x^2 + \left(\frac{1-\sqrt{5}}{2}\right)x + 1$$

and

$$x^2 - \gamma_2 x + 1 = x^2 + \left(\frac{1+\sqrt{5}}{2}\right)x + 1$$

is a root of $\Phi_5(x)$. Thus,

$$\begin{aligned} \zeta_5, \zeta_5^4 &= \frac{-1+\sqrt{5} \pm i\sqrt{10+2\sqrt{5}}}{4} \\ \zeta_5^2, \zeta_5^3 &= \frac{-1-\sqrt{5} \pm i\sqrt{10-2\sqrt{5}}}{4} \end{aligned} \tag{6.8}$$

where all square roots are taken to be positive real numbers. These are precisely the expressions for the roots of $\Phi_5(x)$ that were obtained in Example 1.4. Note that

$$\gamma_1 = \zeta_5 + \zeta_5^{-1} = \zeta_5 + \zeta_5^4$$

and

$$\gamma_2 = \zeta_5^2 + \zeta_5^{-2} = \zeta_5^2 + \zeta_5^3.$$

In light of (6.5) and our choice of substitution, it is not surprising that γ_1 and γ_2 are real numbers.

We have from (6.8) that

$$\mathbb{Q}(\zeta_5) = \mathbb{Q}\Big(\sqrt{5}, \sqrt{-10-2\sqrt{5}}\Big) = \mathbb{Q}\Big(\sqrt{-10-2\sqrt{5}}\Big).$$

Consider the tower of binomial extensions from $\mathbb{Q}$ to $\mathbb{Q}(\zeta_5)$,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}\Big(\sqrt{-10-2\sqrt{5}}\Big) = \mathbb{Q}(\zeta_5).$$

Since $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$, it follows that $\mathbb{Q}(\zeta_5)$ is an irreducible radical extension of $\mathbb{Q}$. ◊

Theorem 6.7. Let p be a prime, and let k be a natural number. Let ζ be a primitive pth root of unity, and let η be a primitive p^kth root of unity. Then:

(a) $\mathbb{Q}(\mu_{p-1}, \zeta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1})$ of degree $p-1$.
(b) $\mathbb{Q}(\mu_{p-1}, \eta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1}, \zeta)$ of degree p^{k-1}.
(c) $\mathbb{Q}(\mu_{p-1}, \eta)$ is an irreducible radical extension of $\mathbb{Q}(\mu_{p-1})$ of degree $p^{k-1} \times (p-1)$.

Proof. (a): Since the primitive quadratic root of unity is -1, the result is trivial for $p = 2$. Suppose that $p > 2$. Let ξ be a primitive $(p-1)$th root of unity, and note that $\mathbb{Q}(\mu_{p-1}) = \mathbb{Q}(\xi)$. Let g be a primitive congruence root modulo p. It follows

from (5.10) that the primitive pth roots of unity are ζ^{g^i} for $i = 0, 1, \ldots p-2$. Let

$$\lambda = \sum_{i=0}^{p-2} \xi^i \zeta^{g^i} = \zeta + \xi\zeta^g + \xi^2\zeta^{g^2} + \cdots + \xi^{p-2}\zeta^{g^{p-2}} \tag{6.9}$$

and let $h(x) = \min(\lambda, \mathbb{Q}(\mu_{p-1}))$. It follows from Theorem 5.5(d) that $\Phi_p(x) = \min(\zeta, \mathbb{Q}(\mu_{p-1}))$. By Theorem 2.11(a), $\{1, \zeta, \zeta^2 \ldots, \zeta^{p-2}\}$ is a basis for $\mathbb{Q}(\mu_{p-1}, \zeta)$ over $\mathbb{Q}(\mu_{p-1})$. Since each of the powers of ζ in (6.9) is greater than or equal to 1, we can factor out ζ and use the basis property to conclude that $\lambda \neq 0$.

Since

$$h\left(\sum_{j=0}^{p-2} \xi^j x^{g^j}\right) \tag{6.10}$$

is a polynomial in $\mathbb{Q}(\mu_{p-1})[x]$ that has ζ as a root, it is divisible by $\Phi_p(x)$. The ζ^{g^i} are the roots of $\Phi_p(x)$, so they are roots of (6.10). Therefore,

$$\lambda_i = \sum_{j=0}^{p-2} \xi^j \zeta^{g^{i+j}} = \xi^{-i}\lambda \tag{6.11}$$

is a root of $h(x)$ for each i.

By Theorem 5.5(c),

$$[\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1.$$

Since $\lambda \neq 0$, the λ_i are distinct, hence $\deg(h) \geq p - 1$. It follows from $\mathbb{Q}(\mu_{p-1}, \lambda) \subseteq \mathbb{Q}(\mu_{p-1}, \zeta)$ and Theorem 2.12(b) that

$$p - 1 = [\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})] \geq [\mathbb{Q}(\mu_{p-1}, \lambda) : \mathbb{Q}(\mu_{p-1})] = \deg(h) \geq p - 1.$$

Therefore,

$$[\mathbb{Q}(\mu_{p-1}, \lambda) : \mathbb{Q}(\mu_{p-1})] = \deg(h) = p - 1$$

and

$$\mathbb{Q}(\mu_{p-1}, \zeta) = \mathbb{Q}(\mu_{p-1}, \lambda).$$

Since $\deg(h) = p - 1$, the λ_i comprise all the roots of $h(x)$. We have from (6.11) that the constant term of $h(x)$, which is an element of $\mathbb{Q}(\mu_{p-1})$, is

$$(-1)^{p-1}\lambda_0\lambda_1\cdots\lambda_{p-2} = (-1)^{p-1}\xi^{-(p-1)(p-2)/2}\lambda^{p-1}.$$

Thus, λ^{p-1} is in $\mathbb{Q}(\mu_{p-1})$, and by Theorem 2.12(b), $h(x) = x^{p-1} - \lambda^{p-1}$. Therefore, $\mathbb{Q}(\mu_{p-1}, \zeta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1})$ of degree $p - 1$.

(b): By Theorem 5.1(c), $\eta^{p^{k-1}}$ is a primitive pth root of unity. We may assume without loss of generality that $\eta^{p^{k-1}} = \zeta$. By Theorem 5.6(c), $g(x) = x^{p^{k-1}} - \zeta$ is irreducible over $\mathbb{Q}(\mu_{p-1}, \zeta)$, hence $g(x) = \min(\eta, \mathbb{Q}(\mu_{p-1}, \zeta))$. Thus, $\mathbb{Q}(\mu_{p-1}, \zeta, \eta) = \mathbb{Q}(\mu_{p-1}, \eta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1}, \zeta)$ of degree p^{k-1}.

(c): This follows from parts (a) and (b) and

$$[\mathbb{Q}(\mu_{p-1}, \eta) : \mathbb{Q}(\mu_{p-1})] = [\mathbb{Q}(\mu_{p-1}, \eta) : \mathbb{Q}(\mu_{p-1}, \zeta)][\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})].$$

□

We make a few remarks on explicit computations related to the constructions in Theorem 6.7. For part (a), let $p - 1 = q_1 q_2 \cdots q_n$ be a factorization of $p - 1$ into not necessarily distinct primes. Since λ^{p-1} is in $\mathbb{Q}(\mu_{p-1})$, a tower of irreducible binomial extensions from $\mathbb{Q}(\mu_{p-1})$ to $\mathbb{Q}(\mu_{p-1}, \zeta)$ can be constructed along the lines of Theorems 6.4 and 6.5:

$$\begin{aligned}\mathbb{Q}(\mu_{p-1}) \subset \mathbb{Q}(\mu_{p-1}, \sqrt[q_1]{\lambda^{p-1}}) \subset \mathbb{Q}(\mu_{p-1}, \sqrt[q_1 q_2]{\lambda^{p-1}}) \\ \subset \cdots \subset \mathbb{Q}(\mu_{p-1}, \sqrt[p-1]{\lambda^{p-1}}) = \mathbb{Q}(\mu_{p-1}, \zeta). \qquad (6.12)\end{aligned}$$

For part (b), a tower of irreducible binomial extensions from $\mathbb{Q}(\mu_{p-1}, \zeta)$ to $\mathbb{Q}(\mu_{p-1}, \eta)$ is obtained similarly:

$$\begin{aligned}\mathbb{Q}(\mu_{p-1}, \zeta) \subset \mathbb{Q}(\mu_{p-1}, \sqrt[p]{\zeta}) \subset \mathbb{Q}(\mu_{p-1}, \sqrt[p^2]{\zeta}) \\ \subset \cdots \subset \mathbb{Q}(\mu_{p-1}, \sqrt[p^{k-1}]{\zeta}) = \mathbb{Q}(\mu_{p-1}, \eta). \qquad (6.13)\end{aligned}$$

We note for later use that by Theorem 5.1(c), each field in (6.12) contains the primitive q_ith root of unity $\xi^{(p-1)/q_i}$ for $i = 1, 2, \ldots n$, and each field in (6.13) contains the primitive pth root of unity ζ.

It has likely been observed by now that the calculations underlying some of our worked examples, although potentially illuminating, are time-consuming and laborious to do by hand. An alternative is available. *Maple* is a sophisticated programming language developed by Maplesoft (2011) designed to handle a range of symbolic and numerical calculations. We will often rely on *Maple* to carry out extensive algebraic manipulations that would be infeasible otherwise.

See Cox (2012) and especially Swallow (2004) for a discussion of how *Maple* can be used to perform such tasks.

Example 6.8 (5th root of unity). We illustrate aspects of Theorem 6.7 for the case $p = 5$. Since i is a primitive 4th root of unity, $\mathbb{Q}(\mu_4) = \mathbb{Q}(i)$. The primitive congruence roots modulo 5 are 2 and 3. Taking $g = 2$, we have

j	0	1	2	3
$2^j \pmod 5$	1	2	4	3

Setting $\xi = i$ and $\zeta = \zeta_5$, (6.9) becomes

$$\lambda = \zeta_5 + i\zeta_5^2 - \zeta_5^4 - i\zeta_5^3.$$

We will demonstrate that, consistent with the proof of Theorem 6.7, $\mathbb{Q}(\mu_4, \zeta_5) = \mathbb{Q}(\mu_4, \lambda)$ and λ^4 is in $\mathbb{Q}(\mu_4)$. In what follows, all square roots are taken to be positive real numbers.

Using *Maple*, we find that $\lambda^4 = -15 + 20i$, which is in $\mathbb{Q}(\mu_4)$, as claimed. We show in Example 14.4 that

$$\lambda^2 = -\sqrt{5}(1 + 2i)$$

and

$$\lambda = \frac{-\sqrt{10 - 2\sqrt{5}}}{2} + i\frac{\sqrt{10 + 2\sqrt{5}}}{2}.$$

Employing the method described in the proof of Theorem 10.2(b), and with some help from *Maple*, we obtain

$$\zeta_5 = \left(-\frac{1}{4}\right) + \left(\frac{1}{4}\right)\lambda + \left(\frac{-1 + 2i}{20}\right)\lambda^2 + \left(\frac{3 + 4i}{100}\right)\lambda^3$$

which confirms that $\mathbb{Q}(\mu_4, \zeta_5) = \mathbb{Q}(\mu_4, \lambda)$. It can be shown that this expression does indeed equal ζ_5 as presented in (6.8).

Evidently, $\mathbb{Q}(\mu_4, \lambda^2) = \mathbb{Q}(\mu_4, \sqrt{5})$. Since

$$\sqrt{10 + 2\sqrt{5}}\,\sqrt{10 - 2\sqrt{5}} = 4\sqrt{5}$$

we have

$$\mathbb{Q}(\mu_4, \zeta_5) = \mathbb{Q}(\mu_4, \lambda) = \mathbb{Q}\Big(\mu_4, \sqrt{10 + 2\sqrt{5}}\Big).$$

Thus, the tower of irreducible binomial extensions

$$\mathbb{Q}(\mu_4) \subset \mathbb{Q}(\mu_4, \lambda^2) \subset \mathbb{Q}(\mu_4, \lambda) = \mathbb{Q}(\mu_4, \zeta_5)$$

can be expressed as

$$\mathbb{Q}(\mu_4) \subset \mathbb{Q}(\mu_4, \sqrt{5}) \subset \mathbb{Q}\left(\mu_4, \sqrt{10 + 2\sqrt{5}}\right) = \mathbb{Q}(\mu_4, \zeta_5). \tag{6.14}$$

We will see in Example 13.11 that this is the only such tower from $\mathbb{Q}(\mu_4)$ to $\mathbb{Q}(\mu_4, \zeta_5)$. ◊

Example 6.9 (7th root of unity). We remarked subsequent to Theorem 5.3 that $-\omega$ is a primitive 6th root of unity. It follows from $\omega = (-1 + \sqrt{-3})/2$ that

$$\mathbb{Q}(\mu_6) = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3}).$$

The primitive congruence roots modulo 7 are 3 and 5. Taking $g = 3$, we have

j	0	1	2	3	4	5
$3^j \pmod 7$	1	3	2	6	4	5

Setting $\xi = -\omega$ and $\zeta = \zeta_7$, (6.9) becomes

$$\lambda = \zeta_7 - \omega\zeta_7^3 + \omega^2\zeta_7^2 - \zeta_7^6 + \omega\zeta_7^4 - \omega^2\zeta_7^5.$$

Using *Maple*, we find that

$$\lambda^6 = \frac{-7(71 - 39\sqrt{-3})}{2}$$

which is in $\mathbb{Q}(\mu_6)$, as expected. We know from the proof of Theorem 6.7 that $\mathbb{Q}(\mu_6, \zeta_7) = \mathbb{Q}(\mu_6, \lambda)$.

Consider the following towers of irreducible binomial extensions from $\mathbb{Q}(\mu_6)$ to $\mathbb{Q}(\mu_6, \zeta_7)$:

$$\mathbb{Q}(\mu_6) \subset \mathbb{Q}(\mu_6, \lambda^2) \subset \mathbb{Q}(\mu_6, \lambda) = \mathbb{Q}(\mu_6, \zeta_7) \tag{6.15}$$

$$\mathbb{Q}(\mu_6) \subset \mathbb{Q}(\mu_6, \lambda^3) \subset \mathbb{Q}(\mu_6, \lambda) = \mathbb{Q}(\mu_6, \zeta_7). \tag{6.16}$$

We will see in Chapter 13 that these are the only such towers.

From (6.15), we obtain the tower

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{-3}) \subset \mathbb{Q}(\sqrt{-3}, \lambda^2) \subset \mathbb{Q}(\sqrt{-3}, \lambda) = \mathbb{Q}(\sqrt{-3}, \zeta_7).$$

Thus, $\mathbb{Q}(\zeta_7)$ is contained in an irreducible radical extension of $\mathbb{Q}$. This raises the question of whether $\mathbb{Q}(\zeta_7)$ itself, like $\mathbb{Q}(\zeta_5)$ in Example 6.6, is an irreducible

radical extension of $\mathbb{Q}$. More generally, for p prime, we now ask for conditions under which $\mathbb{Q}(\zeta_p)$ is an irreducible radical extension of $\mathbb{Q}$. An answer is provided in Theorem 10.16. ◊

The next theorem is the reason why binomial polynomials of prime degree figure so prominently in discussions of solvability by radicals.

Theorem 6.10 (Abel's Lemma). Let p be a prime, and let $h(x) = x^p - a$ be a polynomial in $F[x]$, where $a \neq 0$. Then the following are equivalent:
(a) $h(x)$ is reducible over F.
(b) a is a pth power of an element in F.
(c) $h(x)$ has a root in F.

Suppose that F contains a primitive pth root of unity. If $h(x)$ is reducible over F, then $h(x)$ splits over F.

Proof. (a)⇒(b): Let β be a root of $h(x)$, and let ζ be a primitive pth root of unity. The roots of $h(x)$ are $\zeta^i\beta$ for $i = 0, 1, \ldots, p-1$. Since $h(x)$ is reducible over F, there are nonconstant polynomials $f(x)$ and $g(x)$ in $F[x]$, of degrees $m < p$ and $n < p$, respectively, such that $h(x) = f(x)g(x)$. The constant terms of $f(x)$ and $g(x)$, which are elements of F, are $\zeta^M\beta^m$ and $\zeta^N\beta^n$, respectively, for some M and N. It follows from $m + n = p$ that m and n are relatively prime. By Theorem E.1, there are integers r and s such that $rm + sn = 1$. Let

$$\gamma = (\zeta^M\beta^m)^r(\zeta^N\beta^n)^s = \zeta^{rM+sN}\beta.$$

Then γ is in F and $\gamma^p = a$.

(b)⇒(c): If β in F is such that $a = \beta^p$, then β is a root of $h(x)$.

(c)⇒(a): If β in F is a root of $h(x)$, then

$$h(x) = (x - \beta)(x^{p-1} + \beta x^{p-2} + \cdots + \beta^{p-1})$$

is a factorization over F.

The second assertion follows immediately from the first. □

Let R be an irreducible radical extension of F, and let E be an extension of F. By Theorem 6.2, ER is a radical extension of E, but without further assumptions it does not necessarily follow that ER is an irreducible radical extension of F. We know from Theorem 6.4 that ER is a prime radical extension of E. Thus, if certain roots of unity were available, we could use Theorem 6.10 to refashion the tower of prime binomial extensions from E to ER into a tower of prime-irreducible binomial extensions. Before proceeding with this construction, we need a definition relating to the existence of certain roots of unity.

We say that a radical extension R of F has the *root of unity property* over F if there is a tower of fields of the form (6.1) such that R_{i-1} contains a primitive m_ith root of unity for $i = 1, 2, \ldots, n$. As we show next, in this case, R is automatically

both a prime and an irreducible radical extension of F, and all this takes place in the context of a single tower of fields. Thus, we are led to the following composite definition. We say that a prime-irreducible radical extension R of F has the root of unity property over F if there is a tower of fields of the form (6.1) such that R_i is a prime-irreducible radical extension of R_{i-1}, and R_{i-1} contains a primitive m_ith root of unity for $i = 1, 2, \ldots, n$.

Theorem 6.11. Let R be a radical extension of F with $[R : F] > 1$. If R has the root of unity property over F, then R is a prime-irreducible radical extension of F with the root of unity property over F.

Proof. It is sufficient to consider the case where R is a binomial extension of F with the root of unity property over F. Let $R = F(\beta)$, where β^m is in F for some m, and where F contains a primitive mth root of unity ξ. Let $m = p_1 p_2 \cdots p_n$ be the factorization of m into not necessarily distinct primes. As in Theorem 6.4, we construct a tower of fields such that $R_i = R_{i-1}(\gamma_i)$, where $\gamma_i^{p_i}$ is in R_{i-1} for $i = 1, 2, \ldots, n$. By Theorem 5.1(c), F contains the primitive p_ith root of unity ξ^{m/p_i} for each i. It follows from Theorem 6.10 that either $x^{p_i} - \gamma_i^{p_i}$ is irreducible over R_{i-1} or it splits over R_{i-1}. In the latter situation, R_i is redundant. After deleting redundancies from the tower, we find that R is a prime-irreducible radical extension of F with the root of unity property over F. □

The next three results are straightforward technical pieces that are needed in preparation for Gauss's theorem.

Theorem 6.12. If M_1 is a radical extension of F with the root of unity property over F, and M_2 is a radical extension of M_1 with the root of unity property over M_1, then M_2 is a radical extension of F with the root of unity property over F.

Proof. Straightforward. □

Theorem 6.13. If R is a radical extension of F with the root of unity property over F, and E is an extension of F, then ER is a radical extension of E with the root of unity property over E.

Proof. We adopt the notation of (6.1) and (6.2). By Theorem 6.2, ER is a radical extension of E, with $ER_i = ER_{i-1}(\beta_i)$ and $\beta_i^{m_i}$ in ER_{i-1} for $i = 1, 2, \ldots, n$. Since R_{i-1} contains a primitive m_ith root of unity for each i, so does ER_{i-1}. Therefore, ER has the root of unity property over E. □

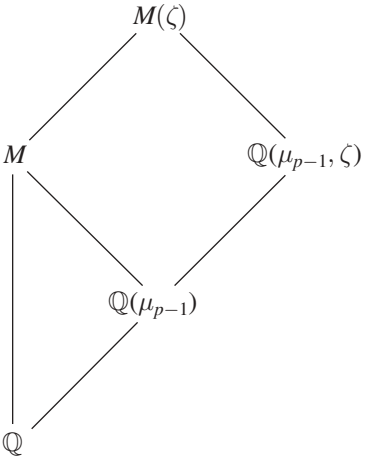
Theorem 6.14. If L_1 and L_2 are radical extensions of F that have the root of unity property over F, then $L_1 L_2$ is a radical extension of F with the root of unity property over F.

Proof. By Theorem 6.13, $L_1 L_2$ is a radical extension of L_1 with the root of unity property over L_1. The result now follows from Theorem 6.12. □

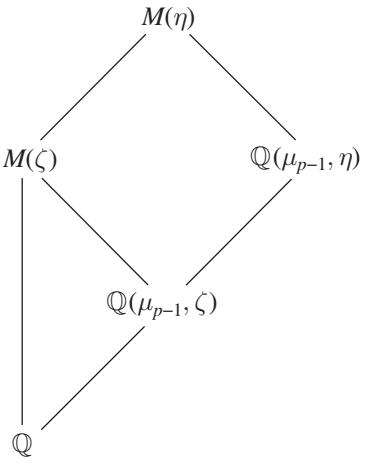
Theorem 6.15 (Gauss). Let F be a field. For all natural numbers n, $\mathbb{Q}(\mu_n)$ is contained in a prime-irreducible radical extension of F that has the root of unity property over F.

Proof. We first consider the case $F = \mathbb{Q}$. The proof is by induction on n. The result is trivial for $n = 1$. Suppose that $n > 1$. Let $n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ be the factorization of n into distinct primes. There are three cases to consider.

Case I. $m = 1$ and $d_1 = 1$.
Let $p_1 = p$, and let ζ be a primitive pth root of unity. Since $p - 1 < p = n$, by the induction hypothesis, $\mathbb{Q}(\mu_{p-1})$ is contained in a radical extension M of $\mathbb{Q}$ that has the root of unity property over $\mathbb{Q}$. It follows from Theorem 6.7(a) and remarks made in connection with (6.12) that $\mathbb{Q}(\mu_{p-1}, \zeta)$ is a radical extension of $\mathbb{Q}(\mu_{p-1})$ with the root of unity property over $\mathbb{Q}(\mu_{p-1})$. By Theorem 6.13, $M\mathbb{Q}(\mu_{p-1}, \zeta) = M(\zeta)$ is a radical extension of M with the root of unity property over M. Then Theorem 6.12 implies that $M(\zeta)$ is a radical extension of $\mathbb{Q}$ with the root of unity property over $\mathbb{Q}$.



Case II. $m = 1$ and $d_1 > 1$.
Let $p_1 = p$ and $d_1 = d$, and let η be a primitive p^dth root of unity. We have from Case I that $\mathbb{Q}(\mu_{p-1}, \zeta)$ is contained in the radical extension $M(\zeta)$ of $\mathbb{Q}$, which has the root of unity property over $\mathbb{Q}$. It follows from Theorem 6.7(b) and remarks made in connection with (6.13) that $\mathbb{Q}(\mu_{p-1}, \eta)$ is a radical extension of $\mathbb{Q}(\mu_{p-1}, \zeta)$ with the root of unity property over $\mathbb{Q}(\mu_{p-1}, \zeta)$. By Theorem 6.13, $M(\zeta)\mathbb{Q}(\mu_{p-1}, \eta) = M(\eta)$ is a radical extension of $M(\zeta)$ with the root of unity property over $M(\zeta)$. Then Theorem 6.12 implies that $M(\eta)$ is a radical extension of $\mathbb{Q}$ with the root of unity property over $\mathbb{Q}$.



Case III. $m > 1$.
Let $n_j = p_j^{d_j}$ for $j = 1, 2, \ldots, m$. Since $n_j < n$, by the induction hypothesis, $\mathbb{Q}(\mu_{n_j})$ is contained in a radical extension L_j of $\mathbb{Q}$ that has the root of unity property over $\mathbb{Q}$. Let $L = L_1 L_2 \cdots L_m$. A straightforward induction based on Theorem 5.5(a) shows that

$$\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n_1})\mathbb{Q}(\mu_{n_2}) \cdots \mathbb{Q}(\mu_{n_m}).$$

Clearly, $\mathbb{Q}(\mu_n)$ is contained in L. An equally straightforward induction based on Theorem 6.14 shows that L is a radical extension of $\mathbb{Q}$ with the root of unity property over $\mathbb{Q}$.

Thus, for each n, $\mathbb{Q}(\mu_n)$ is contained in a radical extension T_n of $\mathbb{Q}$ that has the root of unity property over $\mathbb{Q}$. Now, let F be an arbitrary field. By Theorem 6.13, FT_n is a radical extension of F that has the root of unity property over F. The result now follows from Theorem 6.11. □

We are now able to show that the two definitions of solvability are equivalent.

Theorem 6.16. If R is a radical extension of F, then R is contained in a prime-irreducible radical extension of F with the root of unity property over F.

Proof. We adopt the notation of (6.1) and (6.2), and let $N = m_1 m_2 \cdots m_n$. It follows from Theorem 6.15 that there is a radical extension E of F with the root of unity property over F that contains a primitive Nth root of unity. According to Theorem 6.2, ER is a radical extension of E. By Theorem 5.1(c), E contains a primitive m_ith root of unity for each i, so ER has the root of unity property over E. Then Theorem 6.12 implies that ER is a radical extension of F with the root of unity property over F. The result now follows from Theorem 6.11. □

Theorem 6.17. A polynomial $f(x)$ in $F[x]$ is solvable by radicals over F if and only if it is solvable by irreducible radicals over F.

Proof. This follows from Theorem 6.16. □

We remark that the statement in Theorem 6.15 regarding the root of unity property was not part of the original formulation by Gauss. It has been introduced here primarily for the role it plays in Theorem 6.23.

6.3 ABEL'S THEOREM ON RADICAL EXTENSIONS

In Section 1.1, we defined the polynomial $f(x) = x^2 - ax + b$ in $\mathbb{Q}[x]$ and showed that its roots are given by the quadratic formula

$$\alpha_1, \alpha_2 = \frac{a \pm \sqrt{a^2 - 4b}}{2}.$$

Therefore,

$$\sqrt{a^2 - 4b} = \alpha_1 - \alpha_2.$$

Since $\alpha_1 + \alpha_2 = a$ is in $\mathbb{Q}$, we have

$$\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt{a^2 - 4b}).$$

Thus, the radical appearing in the quadratic formula is a polynomial expression in the roots of $f(x)$ with coefficients in $\mathbb{Q}$. Furthermore, the splitting field of $f(x)$ over $\mathbb{Q}$ is not just contained in an irreducible radical extension of $\mathbb{Q}$, it *is* an irreducible radical extension of $\mathbb{Q}$.

In Section 1.2, we defined the polynomial $g(y) = y^3 + py + q$ in $\mathbb{Q}[x]$ and demonstrated that its roots are given by Cardan's formulas

$$\beta_1 = \frac{\lambda_1 + \lambda_2}{3}$$

$$\beta_2 = \frac{\omega^2\lambda_1 + \omega\lambda_2}{3}$$

$$\beta_3 = \frac{\omega\lambda_1 + \omega^2\lambda_2}{3}$$

where

$$\lambda_1, \lambda_2 = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

with $\lambda_1\lambda_2 = -3p$. It follows that

$$\begin{aligned}\beta_1 &= \frac{\lambda_1 + \lambda_2}{3}\\ \omega\beta_2 &= \frac{\lambda_1 + \omega^2\lambda_2}{3}\\ \omega^2\beta_3 &= \frac{\lambda_1 + \omega\lambda_2}{3}.\end{aligned} \tag{6.17}$$

Summing over both sides of (6.17) and using (1.14), we find that

$$\lambda_1 = 3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} = \beta_1 + \omega\beta_2 + \omega^2\beta_3. \tag{6.18}$$

Similarly,

$$\lambda_2 = 3\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} = \beta_1 + \omega^2\beta_2 + \omega\beta_3.$$

We have from (3.22) that

$$-4p^3 - 27q^2 = [(\beta_1 - \beta_2)(\beta_1 - \beta_3)(\beta_2 - \beta_3)]^2$$

hence

$$6i\sqrt{3}\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} = (\beta_1 - \beta_2)(\beta_1 - \beta_3)(\beta_2 - \beta_3)$$

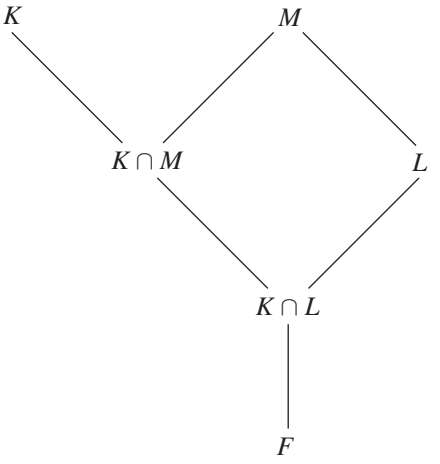
where we note that $i\sqrt{3}$ is in $\mathbb{Q}(\omega)$. Therefore,

$$\mathbb{Q}(\omega, \beta_1, \beta_2, \beta_3) = \mathbb{Q}\left(\omega, \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}\right).$$

So, analogous to the quadratic case, the radicals appearing in Cardan's formulas are polynomial expressions in β_1, β_2, and β_3 with coefficients in $\mathbb{Q}(\omega)$, and the splitting field of $g(y)$ over $\mathbb{Q}(\omega)$ is an irreducible radical extension of $\mathbb{Q}(\omega)$.

Our goal in the remainder of this section is to prove, along with Abel, that these findings for quadratic and cubic polynomials are instances of a more general phenomenon. Historically, it was Lagrange who first commented on the special cases we have just considered.

Theorem 6.18. Let K be a splitting field over F, let L be an extension of F, and let M be an irreducible binomial extension of L of prime degree p. Suppose that F contains a primitive pth root of unity. If $K \cap L \neq K \cap M$, then $K \cap M$ is an irreducible binomial extension of $K \cap L$ of degree p.



Proof. Let $K \cap M = (K \cap L)(\theta)$ for some θ in $K \cap M$. Then θ is not in L, otherwise θ would be in $K \cap L$, which contradicts $K \cap L \neq K \cap M$. We have from $L \subset L(\theta) \subseteq M$ and Theorem 2.15 that $L(\theta) = M$. Since M is an irreducible binomial extension of L of degree p, there is β in $M \backslash L$ such that $M = L(\beta)$, where β^p is in L. By Theorem 2.11(a), $\{1, \beta, \ldots, \beta^{p-1}\}$ is a basis for M over L, so

$$\theta = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{p-1}\beta^{p-1} \tag{6.19}$$

for some $a_0, a_1, \ldots, a_{p-1}$ in L. There is $a_k \neq 0$ for some $1 \leq k \leq p-1$, otherwise θ would be in L. Furthermore, β^k is in $M \backslash L$, otherwise we would have from Theorem 2.12(a) that $[M : L] \leq k < p$. Let $\gamma = a_k\beta^k$. Then γ is in $M \backslash L$ and $\gamma^p = (a_k)^p(\beta^p)^k$ is in L.

We claim that γ is in K. By Theorem 2.15, $M = L(\gamma)$. Therefore, $\{1, \gamma, \ldots, \gamma^{p-1}\}$ is also a basis for M over L, hence

$$\theta = b_0 + b_1\gamma + b_2\gamma^2 + \cdots + b_{p-1}\gamma^{p-1} \tag{6.20}$$

for some $b_0, b_1, \ldots, b_{p-1}$ in L. Since $k\mathbb{F}_p^\times = \mathbb{F}_p^\times$, substituting $\gamma = a_k\beta^k$ into (6.20) produces (6.19). Therefore, $b_1 = 1$.

Let $g(x) = \min(\theta, L)$ and $h(x) = \min(\gamma, L)$. Since γ^p is in L and $[L(\gamma) : L] = p$, it follows from Theorem 2.12(b) that $h(x) = x^p - \gamma^p$. By assumption,

F contains a primitive pth root of unity ζ, so the roots of $h(x)$ are $\zeta^i\gamma$ for $i = 0, 1, \ldots, p-1$. Since

$$g\left(\sum_{j=0}^{p-1} b_j x^j\right) \tag{6.21}$$

is a polynomial in $L[x]$ that has γ as a root, it is divisible by $h(x)$. Therefore, $\zeta^i\gamma$ is a root of (6.21) for each i. It follows that

$$\theta_i = \sum_{j=0}^{p-1} b_j \zeta^{ij} \gamma^j$$

is a root of $g(x)$ for each i, where we note that $\theta = \theta_0$.

Consider

$$\sum_{i=0}^{p-1} \zeta^{-i}\theta_i = \sum_{j=0}^{p-1} b_j \gamma^j \left[\sum_{i=0}^{p-1} (\zeta^{j-1})^i\right].$$

Since ζ is a pth root of unity, ζ^{j-1} is a root of

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

for each j, where $\zeta^{-1} = \zeta^{p-1}$. Furthermore, since ζ is a primitive pth root of unity, $\zeta^{j-1} = 1$ if and only if $j = 1$. Therefore,

$$\sum_{i=0}^{p-1} (\zeta^{j-1})^i = \begin{cases} 0 & \text{if } j = 0 \\ p & \text{if } j = 1 \\ 0 & \text{if } 2 \le j \le p-1 \end{cases}$$

hence

$$\sum_{i=0}^{p-1} \zeta^{-i}\theta_i = pb_1\gamma = p\gamma.$$

By Theorem 2.27, K is a splitting field over $K \cap L$, and by Theorem 4.10(b), $g(x) = \min(\theta, K \cap L)$. Since θ is in K, we have from Theorem 4.9 that $g(x)$ splits over K. Therefore, the θ_i are in K, hence γ is in K. This proves the claim.

We observed above that γ is in $M \backslash L$ and γ^p is in L. Thus, γ is in $(K \cap M) \backslash (K \cap L)$ and γ^p is in $K \cap L$. It follows from Theorem 2.12(b) that

$$\begin{aligned}[K \cap M : K \cap L] &= [(K \cap L)(\theta) : K \cap L] = \deg(g) \\ &= [L(\theta) : L] = [M : L] = p.\end{aligned}$$

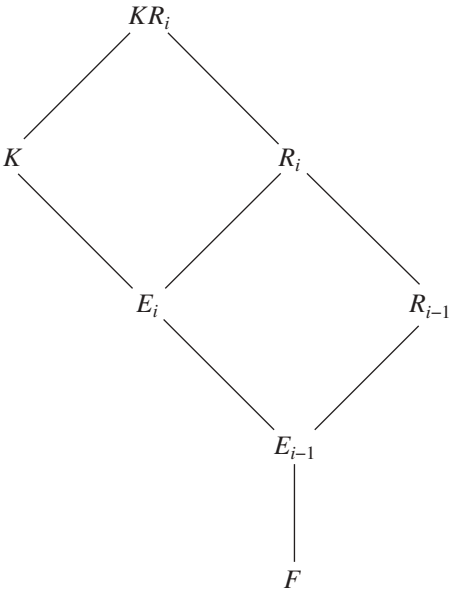
By Theorem 2.15, $K \cap M = (K \cap L)(\gamma)$. Invoking Theorem 2.12(b) yet again, we see that $\min(\gamma, K \cap L) = x^p - \gamma^p$. This shows that $K \cap M$ is an irreducible binomial extension of $K \cap L$ of degree p. □

Theorem 6.19 (Abel). Let K be a splitting field over F, and suppose that F contains a primitive pth root of unity for every prime p dividing $[K : F]$. If K is contained in an irreducible radical extension R of F, then K itself is an irreducible radical extension of F.

Proof. Since R is an irreducible radical extension of F, by Theorem 6.5, there is a tower of fields

$$F = R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

where R_i is an irreducible binomial extension of R_{i-1} of prime degree p_i for $i = 1, 2, \ldots, n$. Let $E_i = K \cap R_i$ for $i = 0, 1, \ldots, n$, and note that $E_0 = F$ and $E_n = K$.



Since K is a splitting field over F, by Theorem 4.10(c),

$$[KR_i : R_i] = [K : K \cap R_i] = [K : E_i]$$

for each i. Therefore,

$$[E_i : E_{i-1}] = \frac{[K : E_{i-1}]}{[K : E_i]} = \frac{[KR_{i-1} : R_{i-1}]}{[KR_i : R_i]} = \frac{[R_i : R_{i-1}]}{[KR_i : KR_{i-1}]}.$$

Since $[R_i : R_{i-1}] = p_i$ is prime, either $[E_i : E_{i-1}] = p_i$ or $[E_i : E_{i-1}] = 1$. In the latter case, E_i is redundant. For the moment, suppose that there are no redundancies. We then have the tower of fields

$$F = E_0 \subset \cdots \subset E_i \subset \cdots \subset E_n = K.$$

Since $p_i = [E_i : E_{i-1}]$ divides $[K : F]$, F contains a primitive p_ith root of unity. Setting $p = p_i$, $L = R_{i-1}$, and $M = R_i$ in Theorem 6.18, we find that E_i is an irreducible binomial extension of E_{i-1} of degree p_i for each i. Thus, K is an irreducible radical extension of F. In the case of redundant fields, the redundancies can be dropped and the preceding argument used. □

6.4 POLYNOMIALS OF PRIME DEGREE

Irreducible polynomials of prime degree have unique properties, as we already encountered in Theorem 4.16. In this section, we explore the solvability by radicals of such polynomials, returning to the topic in Chapter 12 from the perspective of Galois theory. We begin by addressing the classical "Irreducible Case" mentioned in connection with Example 1.3.

Theorem 6.20. Let F be a subfield of $\mathbb{R}$, and let β be an element in $\mathbb{R}\backslash F$ such that β^p is in F for some prime p. Then $x^p - \beta^p$ is irreducible over F.

Proof. By Theorem 6.10, it is sufficient to show that $h(x) = x^p - \beta^p$ has no roots in F. Suppose that γ in F is a root of $h(x)$. Then $\gamma^p = \beta^p$ implies that $\beta = \zeta\gamma$ for some pth root of unity ζ. Since β and γ are in $\mathbb{R}$, so is $\zeta = \beta/\gamma$. Thus, if $p = 2$, then $\zeta = 1$ or -1, and if $p > 2$, then $\zeta = 1$. In either case, β is in F. This contradiction shows that no such γ exists. □

Theorem 6.21 (Casus Irreducibilis). Let F be a subfield of $\mathbb{R}$, let $f(x)$ be a cubic polynomial in $F[x]$ that is irreducible over F, and suppose that the roots of $f(x)$ are real numbers. Then any radical extension of F containing the roots of $f(x)$ is not a subfield of $\mathbb{R}$.

Proof. Let K be the splitting field of $f(x)$ over F, and let R be a radical extension of F that contains K. Suppose, for a contradiction, that R is a subfield of $\mathbb{R}$. Let us denote the roots of $f(x)$ by $\alpha_1, \alpha_2, \alpha_3$ and let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

Evidently, δ is in K, and it follows from Theorem 3.15 that $\delta^2 = \text{disc}(f)$ is in F.

There are two cases to consider.

Case I. δ is in F.
By Theorem 6.4, R is a prime radical extension of F. After deleting redundancies, we have a tower of fields

$$F = R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

where R_i is a binomial extension of R_{i-1} of prime degree p_i for $i = 1, 2, \ldots, n$. Then $R_i = R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{p_i}$ is in R_{i-1} for each i. Let $h_i(x) = x^{p_i} - \beta_i^{p_i}$. Having assumed that R is a subfield of $\mathbb{R}$, it follows from Theorem 6.20 that $h_i(x)$ is irreducible over R_{i-1} for each i. By Theorem 2.12(b), $[R_i : R_{i-1}] = p_i$ for each i.

Since $f(x)$ is irreducible over F, the Division Algorithm and Theorem 2.4 imply that $f(x)$ has no roots in F. On the other hand, $f(x)$ splits over $K \subseteq R$. So there is $1 \leq k \leq n$ such that $f(x)$ has a root in R_k but not in R_{k-1}. Taking α_1 to be such a root, we have $R_{k-1} \subset R_{k-1}(\alpha_1) \subseteq R_k$. Since $[R_k : R_{k-1}] = p_k$, Theorem 2.15 implies that $R_{k-1}(\alpha_1) = R_k$. Furthermore, $f(x)$ is irreducible over R_{k-1}. For if not, since $f(x)$ has degree 3, at least one of its factors over R_{k-1} would be linear, and then R_{k-1} would contain a root of $f(x)$. By Theorem 2.12(b), $p_k = 3$.

Since $f(x)$ and $x - \alpha_1$ are in $R_{k-1}(\alpha_1)[x]$, so is

$$g(x) = \frac{f(x)}{x - \alpha_1} = (x - \alpha_2)(x - \alpha_3) = x^2 - (\alpha_2 + \alpha_3)x + \alpha_2\alpha_3.$$

It follows that $\alpha_2 + \alpha_3$ and $\delta/g(\alpha_1) = \alpha_2 - \alpha_3$ are in $R_{k-1}(\alpha_1)$, and therefore, so are α_2 and α_3. Thus, R_k is the splitting field of $f(x)$ over R_{k-1}. The roots of $h_k(x)$ are β_k, $\omega\beta_k$, and $\omega^2\beta_k$, where, as usual, ω is a primitive cube root of unity. Since $h_k(x)$ is irreducible over R_{k-1}, and β_k is in R_k, by Theorem 4.9, $h_k(x)$ splits over R_k. Thus, ω is in $R_k \subseteq \mathbb{R}$. This contradiction shows that R is not a subfield of $\mathbb{R}$.

Case II. δ is not in F.
Let $E = F(\delta)$. By Theorem 6.2, $R = ER$ is a radical extension of E. Furthermore, $f(x)$ is irreducible over E. For if not, since $f(x)$ has degree 3, at least one of its factors over E would be linear, and then E would contain a root of $f(x)$, say α_1. By Theorem 2.12(b), $[F(\alpha_1) : F] = 3$, hence

$$2 = [E : F] = [E : F(\alpha_1)][F(\alpha_1) : F] \geq 3.$$

This contradiction shows that $f(x)$ is irreducible over E. Thus, we are back to Case I with E in the former role of F. □

In Example 1.2, we showed that the three real roots of $y^3 - 6y - 4$ can be expressed in terms of radicals over $\mathbb{Q}$ without the use of nonreal complex numbers. This would appear to violate Theorem 6.21, except that we also showed

that $y^3 - 6y - 4$ is reducible over $\mathbb{Q}$. In Example 1.3, we asked whether the roots of $y^3 - 6y + 2$, all of which are real numbers, can be expressed in terms of radicals over $\mathbb{Q}$ without using nonreal complex numbers. As shown in Example 4.7, $y^3 - 6y + 2$ is irreducible over $\mathbb{Q}$. It follows from Theorem 6.21 that, even though the roots of $y^3 - 6y + 2$ are real, in order to express them in terms of radicals (not to mention irreducible radicals) over $\mathbb{Q}$, we must employ nonreal complex numbers.

Theorem 6.22. Let $f(x)$ be a polynomial in $F[x]$ of prime degree p that is irreducible over F. Suppose that $f(x)$ splits over a prime-irreducible radical extension R of F,

$$F = R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

where R_i is an irreducible binomial extension of R_{i-1} of prime degree p_i for $i = 1, 2, \ldots, n$. Suppose further that R_i is a splitting field over R_{i-1} for each i, and that R is the only field in the tower over which $f(x)$ splits. Then:
(a) $f(x)$ is irreducible over R_i for $i = 1, 2, \ldots, n-1$.
(b) $p_n = p$.

Proof. We have that $R_i = R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{p_i}$ is in R_{i-1}, and $h_i(x) = x^{p_i} - \beta_i^{p_i}$ is irreducible over R_{i-1} for $i = 1, 2, \ldots, n$. Suppose that $n = 1$. By assumption, $f(x)$ is irreducible over $R_0 = F$ and splits over $R_1 = R$. Let α be an arbitrary root of $f(x)$. Since $F(\alpha) \subseteq R_1$, we have from Theorem 2.12(b) that $p = [F(\alpha) : F]$ divides $p_1 = [R_1 : F]$, hence $p_1 = p$. This proves the assertion for $n = 1$. Now, suppose that $n > 1$. By assumption, $R_1 = F(\beta_1)$ is the splitting field of $h_1(x)$ over $R_0 = F$ and $f(x)$ does not split over R_1. It follows from Theorem 4.16(b) that $f(x)$ is irreducible over R_1. An analogous argument shows that $f(x)$ is irreducible over R_2, and so on, until finally, $f(x)$ splits over $R_n = R$. By Theorem 4.16(a), p divides $\deg(h_n) = p_n$, hence $p_n = p$. □

It is interesting to observe that Theorem 6.22 provides an explanation for why Cardan's formulas (1.16) have a cube root as the last step in the sequence of radicals.

Let $f(x)$ be a polynomial in $\mathbb{R}[x]$ of degree n. Recall that in connection with (3.26), we defined r to be the number of real roots of $f(x)$, and c to be the number of conjugate pairs of nonreal complex roots.

The following remarkable result leads directly to our first version of the Impossibility Theorem.

Theorem 6.23 (Kronecker). Let F be a subfield of $\mathbb{R}$, and let $f(x)$ be a polynomial in $F[x]$ of prime degree $p \geq 5$ that is irreducible over F. If $f(x)$ is solvable by irreducible radicals over F, then $r = 1$ or $r = p$.

Proof. Let K be the splitting field of $f(x)$ over F. By assumption, K is contained in an irreducible radical extension R of F. In view of Theorem 6.16, we may

assume that R is a prime-irreducible radical extension of F with the root of unity property over F. So, there is a tower of fields

$$F = R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

where R_i is an irreducible binomial extension of R_{i-1} of prime degree p_i, and R_{i-1} contains a primitive p_ith root of unity for $i = 1, 2, \ldots, n$. Then $R_i = R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{p_i}$ is in R_{i-1}, and $h_i(x) = x^{p_i} - \beta_i^{p_i}$ is irreducible over R_{i-1} for each i. We can express R_i as

$$R_i = R_{i-1}(\beta_i) = F(\beta_1, \beta_2, \ldots, \beta_i)$$

for each i. According to remarks made in connection with (6.1), R is an algebraic extension of F. It follows from the Fundamental Theorem of Algebra that R is a subfield of $\mathbb{C}$.

Let $L_0 = F$ and let

$$L_i = L_{i-1}(\beta_i, \overline{\beta_i}) = F(\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \ldots, \beta_i, \overline{\beta_i})$$

for $i = 1, 2, \ldots, n$. Evidently, $\beta_i^{p_i}$ and $\overline{\beta_i}^{p_i}$ are in L_{i-1}, and since F is a subfield of $\mathbb{R}$, we have $\overline{L_i} = L_i$ for each i. Since $f(x)$ is irreducible over L_0 and splits over L_n, there is $1 \leq m \leq n$ such that $f(x)$ is irreducible over L_{m-1} but reducible over L_m. Let

$$L = L_{m-1} \quad \beta = \beta_m \quad \text{and} \quad q = p_m.$$

We seek a subfield E of L_n and an element γ in L_n with the following properties:

(a) $f(x)$ is irreducible over E.
(b) $f(x)$ is reducible over $E(\gamma)$.
(c) γ^q is in E.
(d) γ is not in E.
(e) $\overline{E} = E$.
(f) If γ is a nonreal complex number, then $\gamma\overline{\gamma}$ is in E.

There are two cases to consider.

Case I. $f(x)$ is irreducible over $L(\beta\overline{\beta})$.
Let $E = L(\beta\overline{\beta})$ and $\gamma = \beta$.
(a) By definition of Case I, $f(x)$ is irreducible over $L(\beta\overline{\beta}) = E$.
(b) By definition of L_m, $f(x)$ is reducible over

$$L_m = L(\beta, \overline{\beta}) = L(\beta\overline{\beta}, \beta) = E(\gamma).$$

(c) $\gamma^q = \beta^q$ is in $L \subseteq E$.

(d) Suppose that $\gamma = \beta$ is in $E = L(\beta\overline{\beta})$. Then $L(\beta\overline{\beta}) = L(\beta, \overline{\beta}) = L_m$, hence $f(x)$ is reducible over $L(\beta\overline{\beta})$, which contradicts the definition of Case I.
(e) Since $\beta\overline{\beta}$ is a real number and $\overline{L} = L$, we have

$$\overline{E} = \overline{L(\beta\overline{\beta})} = L(\beta\overline{\beta}) = E.$$

(f) $\gamma\overline{\gamma} = \beta\overline{\beta}$ is in $E = L(\beta\overline{\beta})$ whether $\gamma = \beta$ is a nonreal complex number or not.

Case II. $f(x)$ is reducible over $L(\beta\overline{\beta})$.
Let $E = L$ and $\gamma = \beta\overline{\beta}$.
(a) By definition of L_{m-1}, $f(x)$ is irreducible over $L_{m-1} = L = E$.
(b) By definition of Case II, $f(x)$ is reducible over $L(\beta\overline{\beta}) = E(\gamma)$.
(c) Since β^q and $\overline{\beta}^q$ are in L, so is $\gamma^q = \beta^q\overline{\beta}^q$.
(d) Suppose that $\gamma = \beta\overline{\beta}$ is in $E = L$. Then $L = L(\beta\overline{\beta})$, and by definition of Case II, $f(x)$ is reducible over L, which contradicts the defining property of $L_{m-1} = L$.
(e) $\overline{L} = L$, hence $\overline{E} = E$.
(f) Since $\gamma = \beta\overline{\beta}$ is a real number, the condition is met by default.

Thus, we have at our disposal the desired E and γ. According to properties (a) and (b), $f(x)$ is a polynomial in $E[x]$ of prime degree p that is irreducible over E and reducible over $E(\gamma)$. We have from property (c) that $h(x) = x^q - \gamma^q$ is in $E[x]$. Since R_{m-1} contains a primitive p_mth root of unity, it follows from $R_{m-1} \subseteq L \subseteq E$ and $q = p_m$ that E contains a primitive qth root of unity ζ. This has two implications: (i) $E(\gamma)$ is the splitting field of $h(x)$ over E, and (ii) by Theorem 6.10 and property (d), $h(x)$ is irreducible over E. It follows from Theorem 4.16 that

$$p = q \quad \text{and} \quad f(x) \text{ splits over } E(\gamma).$$

Therefore, ζ is a primitive pth root of unity, and

$$h(x) = x^p - \gamma^p = \min(\gamma, E)$$

hence $[E(\gamma) : E] = p$. So, the roots of $h(x)$ are $\gamma_i = \zeta^i\gamma$ for $i = 0, 1, \ldots, p-1$.

By assumption, p is odd and $f(x)$ is in $\mathbb{R}[x]$. It can be shown using differential calculus that $f(x)$ has at least one real root α. Since $f(x)$ splits over $E(\gamma)$, α is in $E(\gamma)$. By Theorem 2.11(a), $\{1, \gamma, \ldots, \gamma^{p-1}\}$ is a basis for $E(\gamma)$ over E. Therefore,

$$\alpha = \sum_{j=0}^{p-1} b_j \gamma^j \tag{6.22}$$

for some $b_0, b_1, \ldots, b_{p-1}$ in E. There must be $b_k \neq 0$ for some $1 \leq k \leq p-1$, otherwise α would be in E, and then $x - \alpha$ would divide $f(x)$, contradicting the irreducibility of $f(x)$ over E.

Since

$$f\left(\sum_{j=0}^{p-1} b_j x^j\right)$$

is a polynomial in $E[x]$ that has γ as a root, it is divisible by $h(x)$, so each γ_i is a root. Therefore,

$$\alpha_i = \sum_{j=0}^{p-1} b_j \gamma_i^j = \sum_{j=0}^{p-1} b_j \zeta^{ij} \gamma^j \tag{6.23}$$

is a root of $f(x)$ for $i = 0, 1, \ldots p-1$, where we note that $\alpha_0 = \alpha$. Suppose that $\alpha_r = \alpha_s$ for some $0 \le r \le s \le p-1$. Since $\{1, \gamma, \ldots, \gamma^{p-1}\}$ is a basis for $E(\gamma)$ over E, with k as above, we have $\zeta^{rk} = \zeta^{sk}$, hence $\zeta^{(s-r)k} = 1$. But ζ is a primitive pth root of unity, so either $s - r = 0$ or it equals a multiple of p. The constraints on r and s exclude the second possibility, so $r = s$. Therefore, the α_i are distinct. Since $f(x)$ has degree p, the α_i comprise all the roots of $f(x)$.

We make a few observations of the effects of complex conjugation. Since α is a real number, $\alpha = \overline{\alpha}$. It follows from (6.22) that

$$\alpha = \sum_{j=0}^{p-1} b_j \gamma^j = \sum_{j=0}^{p-1} \overline{b_j}\, \overline{\gamma}^j = \overline{\alpha}. \tag{6.24}$$

Since the b_j are in E, property (e) implies that the $\overline{b_j}$ are also in E. We have from (6.23) that

$$\overline{\alpha_i} = \sum_{j=0}^{p-1} \overline{b_j}\, \overline{\gamma_i}^j \tag{6.25}$$

and from (6.4) that

$$\overline{\gamma_i} = \zeta^{p-i}\, \overline{\gamma}. \tag{6.26}$$

To complete the proof, we need to consider two cases.

Case A. γ is a real number.
Then (6.24) becomes

$$\sum_{j=0}^{p-1} b_j \gamma^j = \sum_{j=0}^{p-1} \overline{b_j} \gamma^j.$$

Since $\{1, \gamma, \ldots, \gamma^{p-1}\}$ is a basis for $E(\gamma)$ over E, and both the b_j and $\overline{b_j}$ are in E, it follows that $b_j = \overline{b_j}$ for each j. So, the b_j are real numbers. We have from (6.26) that

$$\overline{\gamma_i} = \zeta^{p-i}\gamma = \gamma_{p-i}.$$

Then (6.25) becomes

$$\overline{\alpha_i} = \sum_{j=0}^{p-1} b_j \gamma_{p-i}^j = \alpha_{p-i}.$$

Suppose that α_r is a real number for some $1 \le r \le p-1$. Then $\alpha_r = \overline{\alpha_r} = \alpha_{p-r}$. Since the α_i are distinct, we have $r = p - r$, which is impossible because p is odd. Therefore, when γ is a real number, α is the only real root of $f(x)$. That is, $r = 1$.

Case B. γ is a nonreal complex number.
Let $\phi = \gamma\overline{\gamma}$. According to property (f), ϕ is in E. We have from (6.24) that

$$\sum_{j=0}^{p-1} b_j \gamma^j - \sum_{j=0}^{p-1} \overline{b_j} \left(\frac{\phi}{\gamma}\right)^j = 0.$$

Then

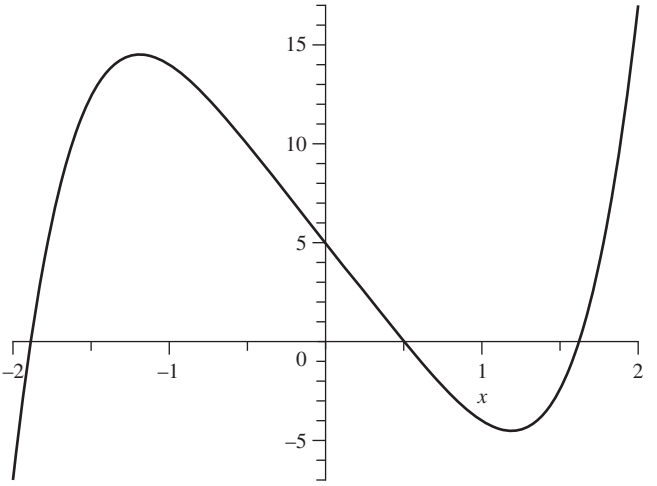
$$x^{p-1}\left[\sum_{j=0}^{p-1} b_j x^j - \sum_{j=0}^{p-1} \overline{b_j} \left(\frac{\phi}{x}\right)^j\right]$$

is a polynomial in $E[x]$ that has γ as a root. It is therefore divisible by $h(x)$, so each γ_i is a root. Thus,

$$\sum_{j=0}^{p-1} b_j \gamma_i^j = \sum_{j=0}^{p-1} \overline{b_j} \left(\frac{\phi}{\gamma_i}\right)^j \tag{6.27}$$

for each i. We have from (6.26) that $\phi = \gamma_i\overline{\gamma_i}$. Substituting into (6.27), it follows from (6.23) and (6.25) that $\alpha_i = \overline{\alpha_i}$ for $i = 0, 1, \ldots, p-1$. Therefore, when γ is a nonreal complex number, all the roots of $f(x)$ are real. That is, $r = p$. □

Example 6.24. Let $f(x) = x^5 - 10x + 5$ in $\mathbb{Q}[x]$. By Eisenstein's criterion with $p = 5$, $f(x)$ is irreducible over $\mathbb{Q}$. The graph of $f(x)$ is shown below.



As can be seen, $f(x)$ has three real roots. It follows from Theorem 6.23 that $f(x)$ is not solvable by irreducible radicals over $\mathbb{Q}$. ◊

We are now able to present the first of three versions of the Impossibility Theorem.

Theorem 6.25 (Impossibility Theorem). For all $n \geq 5$, there is a polynomial in $\mathbb{Q}[x]$ of degree n that is not solvable by irreducible radicals over $\mathbb{Q}$.

Proof. With $f(x)$ as in Example 6.24, let $g(x) = x^{n-5}f(x)$. Then $g(x)$ is a polynomial in $\mathbb{Q}[x]$ that is not solvable by irreducible radicals over $\mathbb{Q}$. □

CHAPTER 7

GENERAL POLYNOMIALS AND THE BEGINNINGS OF GALOIS THEORY

This chapter begins with a discussion of general polynomials and some of their basic properties. Having established this as background, we go on to develop aspects of the classical Galois theory of general polynomials, including a second version of the Impossibility Theorem.

7.1 GENERAL POLYNOMIALS

Let E be a field, and let $t_1, t_2, \ldots, t_n$ be elements in some extension of E. We say that $t_1, t_2, \ldots, t_n$ are *algebraically independent* over E if there does not exist a nonzero polynomial p in $E[x_1, x_2, \ldots, x_n]$ such that $p(t_1, t_2, \ldots, t_n) = 0$. Evidently, if $t_1, t_2, \ldots, t_n$ are algebraically independent over E, then t_i is transcendental over E for $i = 1, 2, \ldots, n$.

Theorem 7.1. If $t_1, t_2, \ldots, t_n$ are algebraically independent over E, then $t_{i+1}, t_{i+2}, \ldots, t_n$ are algebraically independent over $E(t_1, t_2, \ldots, t_i)$ for $i = 1, 2, \ldots, n-1$.

Proof. Suppose that $t_{i+1}, t_{i+2}, \ldots, t_n$ are not algebraically independent over $E(t_1, t_2, \ldots, t_i)$. Then there is a nonzero polynomial r in

$$E(t_1, t_2, \ldots, t_i)[x_{i+1}, x_{i+2}, \ldots, x_n]$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

such that $r(t_{i+1}, t_{i+2}, \ldots, t_n) = 0$. Let q be a polynomial in $E[x_1, x_2, \ldots, x_i]$ such that $q(t_1, t_2, \ldots, t_i)$ equals the product of the denominators of the nonzero coefficients of r. Then $p = qr$ is a nonzero polynomial in $E[x_1, x_2, \ldots, x_n]$ such that $p(t_1, t_2, \ldots, t_n) = 0$. Therefore, $t_1, t_2, \ldots, t_n$ are not algebraically independent over E. □

Let L be an extension of E. We say that the subset $\{t_1, t_2, \ldots, t_n\}$ of L is a *transcendence basis* for L over E if $t_1, t_2, \ldots, t_n$ are algebraically independent over E and $[L : E(t_1, t_2, \ldots, t_n)]$ is finite.

Theorem 7.2. Let L be a finitely generated extension of E such that $[L : E]$ is infinite. Then:
(a) L has a transcendence basis over E.
(b) All transcendence bases for L over E have the same number of elements.

Proof. (a): Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ generate L over E, that is, $L = E(\alpha_1, \alpha_2, \ldots, \alpha_n)$. At least one of $\alpha_1, \alpha_2, \ldots, \alpha_n$ is transcendental over E, say α_1, otherwise, by Theorem 2.21, $[L : E]$ would be finite. If $[L : E(\alpha_1)]$ is infinite, then at least one of $\alpha_2, \alpha_3, \ldots, \alpha_n$ is transcendental over $E(\alpha_1)$, say α_2. Continuing this process for $m \leq n$ steps produces a field $E(\alpha_1, \alpha_2, \ldots, \alpha_m)$ such that α_j is transcendental over $E(\alpha_1, \alpha_2, \ldots, \alpha_{j-1})$ for $j = 1, 2, \ldots, m$, with $[L : E(\alpha_1, \alpha_2, \ldots, \alpha_m)]$ finite. To show that $\alpha_1, \alpha_2, \ldots, \alpha_m$ are algebraically independent over E, suppose that p is a nonzero polynomial in $E[x_1, x_2, \ldots, x_m]$ such that $p(\alpha_1, \alpha_2 \ldots, \alpha_m) = 0$. Let k be the largest value of the index such that x_k appears in p. Then α_k is algebraic over $E(\alpha_1, \alpha_2 \ldots, \alpha_{k-1})$. This contradiction shows that $\{\alpha_1, \ldots, \alpha_m\}$ is a transcendence basis for L over E.

(b): In what follows, semicolons are sometimes used in place of commas to increase readability. Let $\{\beta_1, \beta_2, \ldots, \beta_l\}$ be another transcendence basis for L over E. Without loss of generality, we may assume that $m \leq l$. By Theorem 2.10, L is an algebraic extension of $E(\alpha_1, \alpha_2, \ldots, \alpha_m)$, hence β_1 is algebraic over $E(\alpha_1, \alpha_2, \ldots, \alpha_m)$. So, there is a nonzero polynomial q_1 in $E[y_1; x_1, x_2, \ldots, x_m]$ such that $q_1(\beta_1; \alpha_1, \alpha_2, \ldots, \alpha_m) = 0$. Since β_1 is transcendental over E, at least one of $x_1, x_2, \ldots, x_m$, say x_1, appears in q_1. Then α_1 is algebraic over $E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)$. By Theorem 2.11(b),

$$[E(\beta_1; \alpha_1, \alpha_2, \ldots, \alpha_m) : E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)]$$

is finite, and since $[L : E(\alpha_1, \alpha_2, \ldots, \alpha_m)]$ is finite, so is $[L : E(\beta_1; \alpha_1, \alpha_2, \ldots, \alpha_m)]$. Therefore, $[L : E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)]$ is finite.

We repeat the preceding process. By Theorem 2.10, L is an algebraic extension of $E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)$, hence β_2 is algebraic over $E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)$. So, there is a nonzero polynomial q_2 in $E[y_1, y_2; x_2, x_3, \ldots, x_m]$ such that $q_2(\beta_1, \beta_2; \alpha_2, \alpha_3, \ldots, \alpha_m) = 0$. Since β_1 and β_2 are algebraically independent

over E, at least one of $x_2, x_3, \ldots, x_m$, say x_2, appears in q_2. Then α_2 is algebraic over $E(\beta_1, \beta_2; \alpha_3, \ldots, \alpha_m)$. By Theorem 2.11(b),

$$[E(\beta_1, \beta_2; \alpha_2, \alpha_3, \ldots, \alpha_m) : E(\beta_1, \beta_2; \alpha_3, \ldots, \alpha_m)]$$

is finite, and since $[L : E(\beta_1; \alpha_2, \alpha_3, \ldots, \alpha_m)]$ is finite, so is $[L : E(\beta_1, \beta_2; \alpha_2, \alpha_3, \ldots, \alpha_m)]$. Therefore, $[L : E(\beta_1, \beta_2; \alpha_3, \ldots, \alpha_m)]$ is finite.

Continuing in this way for a total of m steps, we arrive at a field $E(\beta_1, \beta_2, \ldots, \beta_m)$ such that $[L : E(\beta_1, \beta_2, \ldots, \beta_m)]$ is finite. Evidently, $\beta_1, \beta_2, \ldots, \beta_m$ are algebraically independent over E, so $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is a transcendence basis for L over E. Suppose that $m < l$. Since $\beta_1, \beta_2, \ldots, \beta_m, \beta_{m+1}$ are algebraically independent over E, by Theorem 7.1, β_{m+1} is transcendental over $E(\beta_1, \beta_2, \ldots, \beta_m)$. Thus,

$$[E(\beta_1, \beta_2, \ldots, \beta_m, \beta_{m+1}) : E(\beta_1, \beta_2, \ldots, \beta_m)]$$

is infinite, and therefore, so is $[L : E(\beta_1, \beta_2, \ldots, \beta_m)]$. This contradiction shows that $m = l$. □

Let L be a finitely generated extension of E. If $[L : E]$ is infinite, we denote by $\mathrm{tr}[L : E]$ the uniquely defined number of elements in a transcendence basis for L over E guaranteed by Theorem 7.2. If $[L : E]$ is finite, we set $\mathrm{tr}[L : E] = 0$. We refer to $\mathrm{tr}[L : E]$ as the *transcendence degree* of L over E. For example, suppose that t_1 and t_2 are algebraically independent over E, and consider

$$E \subset E(t_1^2, t_2^2) \subset E(t_1, t_2).$$

Then

$$\mathrm{tr}[E(t_1^2, t_2^2) : E] = 2 = \mathrm{tr}[E(t_1, t_2) : E].$$

Since $E(t_1^2, t_2^2, t_1, t_2)$ is an algebraic extension of $E(t_1^2, t_2^2)$,

$$\mathrm{tr}[E(t_1^2, t_2^2, t_1, t_2) : E(t_1^2, t_2^2)] = 0.$$

Theorem 7.3. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements in some extension of E. Then $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraically independent over E if and only if

$$\mathrm{tr}[E(\alpha_1, \alpha_2, \ldots, \alpha_n) : E] = n.$$

Proof. Let $L = E(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

($\Rightarrow$): Clearly, $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ satisfies the two requirements to be a transcendence basis for L over E. By Theorem 7.2(b), $\mathrm{tr}[L : E] = n$.

($\Leftarrow$): Since $\mathrm{tr}[L : E] \neq 0$, the construction used in Theorem 7.2 applies. Thus, $\mathrm{tr}[L : E]$ equals the number of elements in $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ that are needed for

a transcendence basis for L over E. But $\text{tr}[L : E] = n$, so we need all of them. Therefore, $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraically independent over E. □

Theorem 7.4. Let

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} + \cdots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n$$

be a polynomial in $E(a_1, a_2, \ldots, a_n)[x]$ with roots $\beta_1, \beta_2, \ldots, \beta_n$. Then a_1, $a_2, \ldots, a_n$ are algebraically independent over E if and only if $\beta_1, \beta_2, \ldots, \beta_n$ are algebraically independent over E.

Proof. Let

$$L = E(a_1, a_2, \ldots, a_n) \quad \text{and} \quad M = E(\beta_1, \beta_2, \ldots, \beta_n).$$

We claim that $\text{tr}[M : E] = \text{tr}[L : E]$. If $\text{tr}[M : E] = 0$, then, by definition, $[M : E]$ is finite. Since $a_1, a_2, \ldots, a_n$ are the "elementary symmetric polynomials" in $\beta_1, \beta_2, \ldots, \beta_n$, we have $L \subseteq M$. Therefore, $[L : E]$ is finite, hence $\text{tr}[L : E] = 0$. On the other hand, if $\text{tr}[M : E] \neq 0$, then the construction used in Theorem 7.2 can be applied to $a_1, a_2, \ldots, a_n, \beta_1, \beta_2, \ldots, \beta_n$. Since

$$M = E(a_1, a_2, \ldots, a_n, \beta_1, \beta_2, \ldots, \beta_n)$$

and $\beta_1, \beta_2, \ldots, \beta_n$ are algebraic over L, it follows that $\text{tr}[M : E] = \text{tr}[L : E]$. This proves the claim. The result now follows from Theorem 7.3. □

We refer to any polynomial in $E[x]$ that satisfies either of the equivalent conditions of Theorem 7.4 as a *general polynomial* of degree n over E. As usual, let $x_1, x_2, \ldots, x_n$ be indeterminates over E, and in the above notation, let $t_1, t_2, \ldots, t_n$ be algebraically independent over E. Although we have not developed the notion of indeterminates in a formal way, it is clear that $x_1, x_2, \ldots, x_n$ are algebraically independent over E. On the other hand, for our purposes, $t_1, t_2, \ldots, t_n$ behave essentially like indeterminates over E. More formally, it can be demonstrated that the rings $E[x_1, x_2, \ldots, x_n]$ and $E[t_1, t_2, \ldots, t_n]$ are isomorphic. With this as justification, in what follows, we will intentionally blur the modest distinction between $x_1, x_2, \ldots, x_n$ and $t_1, t_2, \ldots, t_n$. Importantly, this permits us to adapt the results in Chapter 3 on symmetric polynomials to the present setting merely by replacing xs with ts.

Accordingly, let $s_1, s_2, \ldots, s_n$ be the elementary symmetric polynomials in $t_1, t_2, \ldots, t_n$. Then

$$\begin{aligned} f(x) &= (x - t_1)(x - t_2) \cdots (x - t_n) \\ &= x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n \end{aligned} \tag{7.1}$$

is a general polynomial over E. In light of the above-mentioned isomorphism, all general polynomials over E are indistinguishable algebraically, so we refer to $f(x)$ as *the* general polynomial of degree n over E.

The ring $E[t_1, t_2, \ldots, t_n]$ has the field of fractions

$$K = E(t_1, t_2, \ldots, t_n). \tag{7.2}$$

As remarked before Theorem 3.7, the subring $E[s_1, s_2, \ldots, s_n]$ of $E[t_1, t_2, \ldots, t_n]$ has the field of fractions

$$\begin{aligned} F &= E(s_1, s_2, \ldots, s_n) \\ &= \left\{ \frac{g(s_1, s_2, \ldots, s_n)}{h(s_1, s_2, \ldots, s_n)} : g, h \in E[x_1, x_2, \ldots, x_n]; h(x_1, x_2, \ldots, x_n) \neq 0 \right\}. \end{aligned} \tag{7.3}$$

Clearly,

$$K = F(t_1, t_2, \ldots, t_n). \tag{7.4}$$

In view of (7.2) and (7.3), the FTSRF can now be expressed as

$$K^{S_n} = F. \tag{7.5}$$

With $f(x)$ as in (7.1), we have the important observations that $f(x)$ is a polynomial in $F[x]$, and K is its splitting field over F. By Theorem 2.20,

$$K = F[t_1, t_2, \ldots, t_n]. \tag{7.6}$$

It follows from (7.6) that each element of K is of the form $p(t_1, t_2, \ldots, t_n)$ for some polynomial p in $F[x_1, x_2, \ldots, x_n]$.

Consistent with (3.4), for each σ in S_n, we define a map

$$\begin{aligned} \sigma : K &\longrightarrow K \\ p(t_1, t_2, \ldots, t_n) &\longmapsto p(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)) \end{aligned} \tag{7.7}$$

that is,

$$\sigma(p(t_1, t_2, \ldots, t_n)) = p(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)).$$

Let $q(t_1, t_2, \ldots, t_n)$ be an element of K, where q is a polynomial in $F[x_1, x_2, \ldots, x_n]$. Finding the common denominator of the (nonzero) coefficients of q, we can express $q(t_1, t_2, \ldots, t_n)$ in the form

$$q(t_1, t_2, \ldots, t_n) = \frac{g(t_1, t_2, \ldots, t_n)}{h(s_1, s_2, \ldots, s_n)}$$

where g and h are in $E[x_1, x_2, \ldots, x_n]$. Then

$$q(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)) = \frac{g(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n))}{h(s_1, s_2, \ldots, s_n)}.$$

It follows from (3.6) that

$$\begin{aligned} q(t_1, t_2, \ldots, t_n) = 0 \quad &\Leftrightarrow \quad g(t_1, t_2, \ldots, t_n) = 0 \\ &\Leftrightarrow \quad g(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)) = 0 \\ &\Leftrightarrow \quad q(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)) = 0 \end{aligned} \tag{7.8}$$

for all σ in S_n. Suppose that p and p' are polynomials in $F[x_1, x_2, \ldots, x_n]$ such that

$$p(t_1, t_2, \ldots, t_n) = p'(t_1, t_2, \ldots, t_n).$$

Setting

$$q(t_1, t_2, \ldots, t_n) = p(t_1, t_2, \ldots, t_n) - p'(t_1, t_2, \ldots, t_n)$$

we have from (7.8) that

$$\sigma(p(t_1, t_2, \ldots, t_n)) = \sigma(p'(t_1, t_2, \ldots, t_n)).$$

Therefore, σ is well defined. In fact, once xs are replaced with ts, we see from (7.2) that σ as defined in (7.7) is nothing more than σ as defined in (3.10).

We will use the notation $f(x)$, E, F, K, and σ established in (7.1)–(7.7) throughout the remainder of the chapter. With the next theorem, we begin the gradual introduction of group theory into our study of fields and roots of polynomials.

Theorem 7.5. S_n is a group of (field) automorphisms of K that fix the elements of F pointwise (where multiplication is defined to be composition of automorphisms).

Proof. Straightforward. □

Similar to what was mentioned following Theorem 3.3, it will sometimes be convenient to view S_n as a group of permutations on $\{t_1, t_2, \ldots, t_n\}$ or $\{1, 2, \ldots, n\}$, particularly for purposes of expressing elements of S_n in cycle notation.

Let

$$g(x) = b_n x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

be an arbitrary polynomial in $F[x]$. Take α in K and σ in S_n. Then

$$\begin{aligned}\sigma(g(\alpha)) &= b_n[\sigma(\alpha)]^m + b_{m-1}[\sigma(\alpha)]^{m-1} + \cdots + b_1\sigma(\alpha) + b_0 \\ &= g(\sigma(\alpha)). \end{aligned} \tag{7.9}$$

Thus, if α is a root of $g(x)$, then so is $\sigma(\alpha)$. We will find (7.9) and its generalizations of great importance throughout the rest of the book.

The remaining theorems of this section set out the key properties of general polynomials.

Theorem 7.6. $f(x)$ is irreducible over F.

Proof. Let $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $F[x]$, and suppose that $g(x)$ is not a constant polynomial. Then t_k is a root of $g(x)$ for some $1 \le k \le n$. It follows from (7.9) that $g(\sigma(t_k)) = 0$ for all σ in S_n. Since S_n is transitive (Appendix D), each root of $f(x)$ is a root of $g(x)$, and since $f(x)$ has simple roots, it divides $g(x)$. So, $f(x)$ and $g(x)$ divide each other, hence they have the same degree. Therefore, $h(x)$ is a constant polynomial. □

Theorem 7.7. $[K : F] = n!$.

Proof. The proof is by induction on n. The result is trivial for $n = 1$. Suppose that $n > 1$. By Theorems 2.12(b) and 7.6, $[F(t_1) : F] = n$. Let $E' = E(t_1)$ and

$$f'(x) = \frac{f(x)}{x - t_1} = (x - t_2)(x - t_3)\cdots(x - t_n).$$

It follows from Theorem 7.1 that $t_2, t_3, \ldots, t_n$ are algebraically independent over E'. Therefore, $f'(x)$ is the general polynomial of degree $n - 1$ over E'. Corresponding to (7.2), we have

$$K' = E'(t_2, t_3, \ldots, t_n) = K.$$

Replacing xs with ts in (3.11), we see that $s_{1[1]}, s_{2[1]}, \ldots, s_{n-1[1]}$ are the elementary symmetric polynomials in $t_2, t_3, \ldots, t_n$ over E'. Consistent with (7.3), Theorem 3.8 implies that

$$F' = E'(s_{1[1]}, s_{2[1]}, \ldots, s_{n-1[1]}) = E(t_1, s_1, s_2, \ldots, s_n) = F(t_1).$$

By the induction hypothesis,

$$[K : F(t_1)] = [K' : F'] = (n - 1)!$$

from which it follows that $[K : F] = n!$. □

Theorem 7.8. Let $c_1, c_2, \ldots, c_n$ be distinct nonzero elements of E, and let

$$\varrho = c_1 t_1 + c_2 t_2 + \cdots + c_n t_n.$$

Then:

(a) $\min(\varrho, F) = \prod_{\sigma \in S_n} [x - \sigma(\varrho)]$. (7.10)

(b) $K = F(\varrho)$.

Proof. (a): Let $g(x) = \min(\varrho, F)$, and let $h(x)$ be the right-hand side of (7.10). It follows from (7.9) that $\sigma(\varrho)$ is a root of $g(x)$ for all σ in S_n. Since $t_1, t_2, \ldots, t_n$ are algebraically independent over E, these $n!$ roots are distinct, hence $\deg(g) \geq n!$. However, by the FTSRF, $h(x)$ is a monic polynomial in $F[x]$ of degree $n!$ that has ϱ as a root. Since $g(x)$ divides $h(x)$, we have $g(x) = h(x)$.

(b): By part (a) and Theorem 2.12(b), $[F(\varrho) : F] = |S_n| = n!$. The result now follows from Theorem 7.7. □

7.2 THE BEGINNINGS OF GALOIS THEORY

We continue with the notation and concepts of the preceding section. Following Appendix A, we define an *action* of S_n on K by setting $\sigma \cdot \alpha = \sigma(\alpha)$ for each σ in S_n and each α in K. The *stabilizer* of α under S_n, denoted by $S_n(\alpha)$, is the subgroup of S_n consisting of those automorphisms that fix α, that is,

$$S_n(\alpha) = \{\sigma \in S_n : \sigma(\alpha) = \alpha\}.$$

Theorem 7.9. Let β be a nonzero element of K, let p be a prime, and suppose that F contains a primitive pth root of unity. If σ is in $S_n(\beta^p)$, then either σ is in $S_n(\beta)$ or p divides $\text{ord}(\sigma)$ (or both).

Proof. Since $\sigma(\beta^p) = \beta^p$, we have $[\sigma(\beta)]^p = \beta^p$, hence $[\sigma(\beta)/\beta]^p = 1$. Thus, $\sigma(\beta) = \zeta\beta$, where ζ is a pth root of unity in F. Let $m = \text{ord}(\sigma)$. Then $\sigma^2(\beta) = \zeta^2\beta$, $\sigma^3(\beta) = \zeta^3\beta$, and so on, until $\beta = \sigma^m(\beta) = \zeta^m\beta$. Since $\beta \neq 0$, ζ is also an mth root of unity. If $\zeta = 1$, then $\sigma(\beta) = \beta$; that is, σ is in $S_n(\beta)$. If $\zeta \neq 1$, then ζ is a primitive pth root of unity. Viewing ζ as an element of μ_p, we have $\zeta^m = 1$ and $\text{ord}(\zeta) = p$. It follows from Theorem B.2 that p divides m. □

Theorem 7.10 (Ruffini). Let $n \geq 5$, and let β be a nonzero element of K. Let p be a prime, and suppose that F contains a primitive pth root of unity. If $\sigma = (t_1\ t_2\ t_3)$ and $\tau = (t_3\ t_4\ t_5)$ are in $S_n(\beta^p)$, then they are in $S_n(\beta)$.

Proof. By Theorem 7.9, either σ and τ are in $S_n(\beta)$ or $p = 3$. Suppose that $p = 3$. Since σ and τ are in $S_n(\beta^3)$, so are $\sigma\tau = (t_1\ t_2\ t_3\ t_4\ t_5)$ and $\sigma^2\tau = (t_1\ t_3\ t_4\ t_5\ t_2)$. Again by Theorem 7.9, either $\sigma\tau$ and $\sigma^2\tau$ are in $S_n(\beta)$ or $p = 5$. The second

possibility has been excluded, hence $\sigma = (\sigma^2\tau)(\sigma\tau)^{-1}$ is in $S_n(\beta)$, and therefore, so is τ. □

In Theorems 7.11, 7.13, and 7.14, we assume that F contains certain roots of unity. From the perspective of solving $f(x)$ by radicals over F, this does not represent a limitation because of Theorem 6.15.

We now come to our second version of the Impossibility Theorem. A notable difference from the earlier version (Theorem 6.25), which relied exclusively on polynomials and field theory, is that here we incorporate (a limited amount of) group theory.

Theorem 7.11 (Impossibility Theorem: Ruffini-Abel). Let $n \geq 5$, and suppose that F contains a primitive pth root of unity for every prime p dividing $n!$. Then $f(x)$ is not solvable by irreducible radicals over F.

Proof. Suppose, for a contradiction, that $f(x)$ is solvable by irreducible radicals over F. By Theorems 6.5, 6.19, and 7.7, K is a prime-irreducible radical extension of K. So, there is a tower of fields

$$F = R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots \subset R_n = K$$

where R_i is an irreducible binomial extension of R_{i-1} of prime degree p_i for $i = 1, 2, \ldots, n$. Then $R_i = R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{p_i}$ is in R_{i-1} for each i. We have from Theorem 7.7 that $[K : F] = n!$. Since p_i divides $[K : F]$, F contains a primitive p_ith root of unity for each i. Let σ and τ be as in Theorem 7.10. Clearly, σ and τ fix $R_0 = F$ pointwise. Since $\beta_1^{p_1}$ is in R_0, σ and τ are in $S_n(\beta_1^{p_1})$; by Theorem 7.10, they are in $S_n(\beta_1)$. Thus, σ and τ fix $R_1 = R_0(\beta_1)$ pointwise. Since $\beta_2^{p_2}$ is in R_1, σ and τ are in $S_n(\beta_2^{p_2})$; again by Theorem 7.10, they are in $S_n(\beta_2)$. Thus, σ and τ fix $R_2 = R_1(\beta_2)$ pointwise. Proceeding in this way up the tower of fields, we find that σ and τ are in $S_n(\beta_n)$ and that they fix K pointwise. But t_1 is in K, and it is not fixed by σ. This contradiction shows that $f(x)$ is not solvable by irreducible radicals over F. □

Historically, Theorem 7.11 predates Theorem 6.25, our first version of the Impossibility Theorem. The proof of Theorem 7.11 is ingenious, but it fails to offer much insight into the question of *why* K cannot be realized as an irreducible radical extension of F. Our investigation of this question will take us deeper into the connection between group theory and field theory.

We continue our discussion of the action defined above. Let us take α in K. If α takes precisely m distinct values under the action, we say that α is *m-valued*. For example, each of $s_1, s_2, \ldots, s_n$ is 1-valued, and each of $t_1, t_2, \ldots, t_n$ is n-valued. For each σ in S_n, the corresponding left coset of $S_n(\alpha)$ in S_n is

$$\sigma S_n(\alpha) = \{\sigma\nu : \nu \in S_n(\alpha)\}.$$

There are

$$[S_n : S_n(\alpha)] = \frac{|S_n|}{|S_n(\alpha)|}$$

distinct left cosets of $S_n(\alpha)$ in S_n, and they form a partition of S_n. By Theorem A.2(a), the map

$$\iota\colon \{\sigma S_n(\alpha) : \sigma \in S_n\} \longrightarrow \{\sigma(\alpha) : \sigma \in S_n\}$$
$$\sigma S_n(\alpha) \longmapsto \sigma(\alpha)$$

is a bijection between the left cosets of $S_n(\alpha)$ in S_n and the distinct values taken by α under the action of S_n. Thus, $m = [S_n : S_n(\alpha)]$.

Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ consist of one arbitrarily chosen element from each of the left cosets of $S_n(\alpha)$ in S_n. Then $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_m(\alpha)$ are the m values taken by α. We refer to $\sigma_1, \sigma_2, \ldots, \sigma_m$ as *left coset representatives* of $S_n(\alpha)$ in S_n. In most applications, we take $\sigma_1 = id$. It is easily demonstrated that $\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_m$ are left coset representatives of $S_n(\alpha)$ in S_n for any τ in S_n. Therefore, $\tau\sigma_1(\alpha), \tau\sigma_2(\alpha), \ldots, \tau\sigma_m(\alpha)$ are once again the m values taken by α but possibly in a different order. For a given value α' taken by α, it is clear from the preceding remarks that α' is m-valued, and that its values are precisely those taken by α.

Consistent with (3.14), let

$$\Delta = \Delta_n = \prod_{1 \le i < j \le n} (t_i - t_j).$$

In Appendix D, Δ is used to define a subgroup A_n of S_n called the *alternating group*. We have from (D.3) and (D.4) that

$$A_n = S_n(\Delta) \tag{7.11}$$

and

$$[S_n : A_n] = 2. \tag{7.12}$$

Therefore, Δ is 2-valued, the other value being $-\Delta$. We know from the observations made in connection with (3.15) that Δ^2 is in F. Since Δ is not in F, we have

$$\min(\Delta, F) = x^2 - \Delta^2. \tag{7.13}$$

Thus, $F(\Delta)$ is a prime-irreducible binomial extension of F of degree 2. As is demonstrated in Theorem 7.13, provided that F contains certain roots of unity, $F(\Delta)$ is the only prime-irreducible binomial extension of F contained in K.

Theorem 7.12. Let $n \geq 5$, and let α be an element in $K \backslash F$. Then $S_n(\alpha) = A_n$ if and only if $F(\alpha) = F(\Delta)$.

Proof. ($\Rightarrow$): Since $S_n(\alpha) = A_n$, we have from (7.12) that α is 2-valued. The other value will be denoted by α'. Take σ in $S_n(\alpha)$. Then σ is also in $S_n(\alpha')$. For if not, $\sigma(\alpha') = \alpha$, hence σ^{-1} is not in $S_n(\alpha)$, which is impossible because $S_n(\alpha)$ is a group. Therefore, $S_n(\alpha) \subseteq S_n(\alpha')$. The reverse inclusion follows by symmetry, so $S_n(\alpha) = S_n(\alpha')$. Thus, each element of S_n either fixes both α and α' or maps one to the other. Let

$$b = \alpha + \alpha' \quad \text{and} \quad \beta = \alpha - \alpha'.$$

By the FTSRF, b is in F. However, β is 2-valued, the other value being $-\beta$. Since $S_n(\alpha) = S_n(\alpha')$, we have $S_n(\alpha) \subseteq S_n(\beta)$. By assumption, $A_n = S_n(\alpha)$, so $A_n \subseteq S_n(\beta)$. It follows from

$$[S_n : S_n(\beta)][S_n(\beta) : A_n] = [S_n : A_n] = 2$$

that the only possibilities for $S_n(\beta)$ are S_n and A_n. Suppose that $S_n(\beta) = S_n$. Then, by the FTSRF, $\alpha - \alpha'$ is in F. Since $\alpha + \alpha'$ is in F, so is α, hence $S_n(\alpha) = S_n$. This contradiction shows that

$$S_n(\beta) = A_n = S_n(\Delta)$$

where the second identity follows from (7.11). Take σ in S_n and consider $\sigma(\beta/\Delta) = \sigma(\beta)/\sigma(\Delta)$. If σ is in A_n, then $\sigma(\beta/\Delta) = \beta/\Delta$, and if σ is in $S_n \backslash A_n$, then $\sigma(\beta/\Delta) = (-\beta)/(-\Delta) = \beta/\Delta$. By the FTSRF, β/Δ is in F, hence $\beta = c\Delta$, where c is in F. Then $\alpha - \alpha' = c\Delta$ and $\alpha + \alpha' = b$, hence

$$\alpha, \alpha' = \frac{b \pm c\Delta}{2}.$$

Therefore, $F(\alpha) = F(\Delta)$.

($\Leftarrow$): Since α is in $F(\Delta)$, we have $S_n(\Delta) \subseteq S_n(\alpha)$. By symmetry, $S_n(\alpha) \subseteq S_n(\Delta)$, hence $S_n(\alpha) = S_n(\Delta)$. The result now follows from (7.11). □

Theorem 7.13. Let $n \geq 5$, and suppose that F contains a primitive pth root of unity for every prime p dividing $n!$. Then $F(\Delta)$ is the only prime-irreducible binomial extension of F contained in K.

Proof. Suppose that β_1 is an element in $K \backslash F$ such that $F(\beta_1)$ is an irreducible binomial extension of F of prime degree p_1, where $\beta_1^{p_1}$ is in F. Then $[F(\beta_1) : F] = p_1$, so p_1 divides $[K : F] = n!$. Therefore, F contains a primitive p_1th root of unity. Since $\beta_1^{p_1}$ is in F, we have $S_n(\beta_1^{p_1}) = S_n$. Let $\sigma = (t_i\ t_j\ t_k)$ be an arbitrary 3-cycle, and let $\tau = (t_k\ t_l\ t_m)$, where $t_i, t_j \neq t_l, t_m$. An argument

along the lines of that used in the proof of Theorem 7.11 shows that σ is in $S_n(\beta_1)$. Thus, $S_n(\beta_1)$ contains all 3-cycles in S_n. By Theorem D.6, $A_n \subseteq S_n(\beta_1)$. Since $[S_n : A_n] = 2$, the only possibilities for $S_n(\beta_1)$ are S_n and A_n. Suppose that $S_n(\beta_1) = S_n$. It follows from the FTSRF that β_1 is in F, which contradicts the choice of β_1. Therefore, $S_n(\beta_1) = A_n$, and by Theorem 7.12, $F(\beta_1) = F(\Delta)$. □

Theorem 7.14. Let $n \geq 5$, and suppose that F contains a primitive pth root of unity for every prime p dividing $n!$. Then there is no prime-irreducible binomial extension of $F(\Delta)$ contained in K.

Proof. Suppose that β_2 is an element in $K \backslash F(\Delta)$ such that $F(\Delta, \beta_2)$ is an irreducible binomial extension of $F(\Delta)$ of prime degree p_2, where $\beta_2^{p_2}$ is in $F(\Delta)$. Building on Theorem 7.13, and using the inductive approach of Theorem 7.11, we find that $S_n(\beta_2)$ contains all 3-cycles. An argument similar to that used in the proof of Theorem 7.13 demonstrates that $F(\beta_2) = F(\Delta)$, hence β_2 is in $F(\Delta)$. This contradiction shows that no such β_2 exists. □

As we will see, certain theorems proved using arguments based on polynomials and fields are more easily demonstrated when group theory is incorporated. Indeed, some of the theorems that we initially express in terms of polynomials and fields are effectively theorems in group theory. Theorems 7.13 and 7.14 are cases in point, the group theoretic counterparts being Theorems D.8 and D.7, respectively.

Taken together, Theorems 7.13 and 7.14 demonstrate that, provided certain roots of unity are contained in F, any attempt at constructing a tower of prime-irreducible binomial extensions from F to K begins and ends with $F(\Delta)$. Expressed another way, for any α in $K \backslash F(\Delta)$, $\min(\alpha, F(\Delta))$ is never a binomial polynomial.

For the moment, we set aside the issue of when a minimal polynomial is binomial and take up a somewhat different question. Specifically, we will address the following three problems, proceeding in order: (i) determine an explicit expression for $\min(\gamma, F)$ for arbitrary γ in K, (ii) determine an explicit expression for $\min(\gamma, F(\alpha))$ for arbitrary γ in K, where α is in $F(\gamma)$, and (iii) determine an explicit expression for $\min(\beta, F(\alpha))$ for arbitrary α and β in K.

The following result provides an answer to the first problem in the sequence.

Theorem 7.15. Let γ be an element of K, and let $id = \sigma_1, \sigma_2, \ldots, \sigma_m$ be left coset representatives of $S_n(\gamma)$ in S_n. Then

$$\min(\gamma, F) = \prod_{j=1}^{m} [x - \sigma_j(\gamma)]. \tag{7.14}$$

Proof. Let us denote by $h(x)$ the right-hand side of (7.14). Take τ in S_n and define

$$h^{\tau}(x) = \prod_{j=1}^{m}[x - \tau\sigma_j(\gamma)].$$

As remarked earlier, since $\sigma_1, \sigma_2, \ldots, \sigma_m$, are left coset representatives of $S_n(\gamma)$ in S_n, so are $\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_m$. Therefore, $h^{\tau}(x) = h(x)$ for all τ in S_n. It follows that the coefficients of $h(x)$ are fixed by all τ in S_n. By the FTSRF, $h(x)$ is a monic polynomial in $F[x]$ that has γ as a root. Let $g(x) = \min(\gamma, F)$. Then $g(x)$ divides $h(x)$. We have from (7.9) that

$$g(\sigma_j(\gamma)) = \sigma_j(g(\gamma)) = \sigma_j(0) = 0$$

for all j. Thus, all the roots of $h(x)$ are roots of $g(x)$. Since $h(x)$ has simple roots, it divides $g(x)$. Therefore, $h(x) = g(x)$. □

Example 7.16. Let $n = 3$, and let $F = \mathbb{Q}(s_1, s_2, s_3)$ and $\gamma = t_1t_2$. Then

$$\begin{array}{lll} id(\gamma) = t_1t_2 & (t_1\ t_2)(\gamma) = t_1t_2 & (t_1\ t_3)(\gamma) = t_2t_3 \\ (t_2\ t_3)(\gamma) = t_1t_3 & (t_1\ t_2\ t_3)(\gamma) = t_2t_3 & (t_1\ t_3\ t_2)(\gamma) = t_1t_3. \end{array}$$

Evidently, $S_3(\gamma) = \{id, (t_1\ t_2)\}$. The left cosets of $S_3(\gamma)$ in S_3 are

$$\begin{array}{c} S_3(\gamma) = \{id, (t_1\ t_2)\} \\ (t_1\ t_3)S_3(\gamma) = \{(t_1\ t_3), (t_1\ t_2\ t_3)\} \\ (t_2\ t_3)S_3(\gamma) = \{(t_2\ t_3), (t_1\ t_3\ t_2)\}. \end{array}$$

Choosing $id, (t_1\ t_3), (t_2\ t_3)$ as left coset representatives, we have

$$\begin{aligned} \min(\gamma, F) &= (x - t_1t_2)(x - t_2t_3)(x - t_1t_3) \\ &= x^3 - s_2x^2 + s_1s_3x - s_3^2. \end{aligned}$$ ◊

To address the second problem in our sequence, we rely on the following remarkable result due to Lagrange. With hindsight, this theorem represents the beginnings of what we know today as Galois theory.

Theorem 7.17 (Lagrange). Let α and γ be elements of K. Then

$$F(\alpha) \subseteq F(\gamma) \quad \Leftrightarrow \quad S_n(\gamma) \subseteq S_n(\alpha).$$

Therefore,

$$F(\alpha) = F(\gamma) \quad \Leftrightarrow \quad S_n(\gamma) = S_n(\alpha).$$

Proof. The second assertion follows immediately from the first.

($\Rightarrow$): If α is in $F(\gamma)$, then $S_n(\gamma) \subseteq S_n(\alpha)$.

($\Leftarrow$): Let $[S_n : S_n(\gamma)] = m$, and let $id = \sigma_1, \sigma_2, \ldots, \sigma_m$ be left coset representatives of $S_n(\gamma)$ in S_n. Let $\gamma_j = \sigma_j(\gamma)$ and $\alpha_j = \sigma_j(\alpha)$ for $j = 1, 2, \ldots, m$. Note that the γ_j are distinct, while there are $[S_n(\alpha) : S_n(\gamma)]$ copies of each of the distinct values of the α_j. Let

$$\begin{aligned} c_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_m \\ c_2 &= \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_m\alpha_m \\ c_3 &= \gamma_1^2\alpha_1 + \gamma_2^2\alpha_2 + \cdots + \gamma_m^2\alpha_m \\ &\vdots \\ c_m &= \gamma_1^{m-1}\alpha_1 + \gamma_2^{m-1}\alpha_2 + \cdots + \gamma_m^{m-1}\alpha_m. \end{aligned} \tag{7.15}$$

Any permutation of $t_1, t_2, \ldots, t_n$ merely interchanges the order of the terms in c_j, so c_j is symmetric in $t_1, t_2, \ldots, t_n$ over F for each j. By the FTSRF, each c_j is in F. Viewing (7.15) as a system of m linear equations in the "unknowns" $\alpha_1, \alpha_2, \ldots, \alpha_m$, we "solve" for $\alpha = \alpha_1$ in terms of $\gamma = \gamma_1$ as follows.

Let

$$g(x) = (x - \gamma_1)(x - \gamma_2)\cdots(x - \gamma_m)$$

and

$$h(x) = \frac{g(x)}{x - \gamma} = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0$$

where we note that $b_{m-1} = 1$. Multiplying the first equation in (7.15) by b_0, the second by b_1, and so on, we obtain

$$\begin{aligned} b_0c_1 &= b_0\alpha_1 + b_0\alpha_2 + \cdots + b_0\alpha_m \\ b_1c_2 &= b_1\gamma_1\alpha_1 + b_1\gamma_2\alpha_2 + \cdots + b_1\gamma_m\alpha_m \\ b_2c_3 &= b_2\gamma_1^2\alpha_1 + b_2\gamma_2^2\alpha_2 + \cdots + b_2\gamma_m^2\alpha_m \\ &\vdots \\ b_{m-1}c_m &= b_{m-1}\gamma_1^{m-1}\alpha_1 + b_{m-1}\gamma_2^{m-1}\alpha_2 + \cdots + b_{m-1}\gamma_m^{m-1}\alpha_m. \end{aligned} \tag{7.16}$$

Summing over both sides of (7.16) and observing that $h(\gamma_j) = 0$ for $j = 2, 3, \ldots, m$, we find that

$$\begin{aligned} b_0c_1 + b_1c_2 + \cdots + b_{m-1}c_m &= h(\gamma_1)\alpha_1 + h(\gamma_2)\alpha_2 + \cdots + h(\gamma_m)\alpha_m \\ &= h(\gamma)\alpha. \end{aligned}$$

Since the γ_j are distinct, $h(\gamma) \neq 0$, hence

$$\alpha = \frac{b_0c_1 + b_1c_2 + \cdots + b_{m-1}c_m}{b_0 + b_1\gamma + \cdots + b_{m-2}\gamma^{m-2} + b_{m-1}\gamma^{m-1}}.$$

By Theorem 7.15, $g(x)$ is in $F[x]$. It follows from the Division Algorithm that $h(x)$ is in $F(\gamma)[x]$. Thus, $b_0, b_1, \ldots, b_{m-1}$ are in $F(\gamma)$, and therefore, so is α. □

The next result provides an answer to the second problem in our sequence. A word on the joint acknowledgement is in order. Lagrange was the first to consider polynomials of the form (7.17), while the credit for discovering its irreducibility can reasonably be attributed to Ruffini (Ayoub, 1980).

Theorem 7.18 (Lagrange-Ruffini). Let α and γ be elements of K, with α in $F(\gamma)$, and let $id = \sigma_1, \sigma_2, \ldots, \sigma_m$ be left coset representatives of $S_n(\gamma)$ in $S_n(\alpha)$. Then

$$\min(\gamma, F(\alpha)) = \prod_{j=1}^{m}[x - \sigma_j(\gamma)]. \tag{7.17}$$

Proof. The statement of the theorem makes sense because, by Theorem 7.17, $F(\alpha) \subseteq F(\gamma)$ implies $S_n(\gamma) \subseteq S_n(\alpha)$. The following argument is almost identical to that used in the proof of Theorem 7.15. Let us denote by $h(x)$ the right-hand side of (7.17). Take τ in $S_n(\alpha)$ and define

$$h^{\tau}(x)) = \prod_{j=1}^{m}[x - \tau\sigma_j(\gamma)].$$

Since $\sigma_1, \sigma_2, \ldots, \sigma_m$ are left coset representatives of $S_n(\gamma)$ in $S_n(\alpha)$, so are $\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_m$. Therefore, $h^{\tau}(x) = h(x)$ for all τ in $S_n(\alpha)$. It follows that the coefficients of $h(x)$ are fixed by all τ in $S_n(\alpha)$. That is, if κ is such a coefficient, then $S_n(\alpha) \subseteq S_n(\kappa)$. By Theorem 7.17, $F(\kappa) \subseteq F(\alpha)$, hence $h(x)$ is a monic polynomial in $F(\alpha)[x]$ that has γ as a root. Let $p(x, y)$ be a polynomial in $F[x, y]$ such that $p(x, \alpha) = \min(\gamma, F(\alpha))$. Then $p(x, \alpha)$ divides $h(x)$. Since the σ_j are in $S_n(\alpha)$, we have from (7.9) that

$$p(\sigma_j(\gamma), \alpha) = p(\sigma_j(\gamma), \sigma_j(\alpha)) = \sigma_j(p(\gamma, \alpha)) = \sigma_j(0) = 0$$

for all j. Thus, all the roots of $h(x)$ are roots of $p(x, \alpha)$. Since $h(x)$ has simple roots, it divides $p(x, \alpha)$. Therefore, $h(x) = p(x, \alpha)$. □

It remains to address the third problem in our sequence. Let α and β be arbitrary elements of K. By the Primitive Element Theorem, there is c in F such that $F(\alpha + c\beta) = F(\alpha, \beta)$. Let $\gamma = \alpha + c\beta$. It was demonstrated in Theorem 4.17

that $\min(\beta, F(\alpha))$ and $\min(\gamma, F(\alpha))$ are readily converted into each other. Thus, the solution to the second problem provides an answer to the third.

Theorems 7.19 and 7.20 do not appear in the work of Lagrange and Ruffini. They are included here to show that, along with Theorems 7.17 and 7.18, we are very close to what might be called a *Galois theory of general polynomials*. Theorem 7.19 is a generalization of the FTSRF, and Theorem 7.20 is an example of what we later refer to as a *Galois correspondence*.

Let G be a subgroup of S_n, and let K^G be the set of elements in K that are fixed by G, that is,

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

It is easily verified that K^G is a field between F and K. Trivially, $K^{\langle id \rangle} = K$, and we have from (7.5) that $K^{S_n} = F$.

Theorem 7.19. Let α be an element of K. Then $K^{S_n(\alpha)} = F(\alpha)$.

Proof. Evidently, $F(\alpha) \subseteq K^{S_n(\alpha)}$. Let $K^{S_n(\alpha)} = F(\beta)$ for some β in K. Then β is fixed by $S_n(\alpha)$, so $S_n(\alpha) \subseteq S_n(\beta)$. It follows from Theorem 7.17 that $F(\beta) \subseteq F(\alpha)$. □

With Theorem 7.19, we are able to give near-effortless proofs of Theorems 7.8(b) and 7.12. For Theorem 7.8(b), the algebraic independence of $t_1, t_2, \ldots, t_n$ over E implies that $S_n(\varrho) = \langle id \rangle$, hence $F(\varrho) = K$. In fact, we obtain a slight strengthening of Theorem 7.8(b) by allowing $c_1, c_2, \ldots, c_n$ to be elements in F such that $S_n(\varrho) = \langle id \rangle$. For Theorem 7.12, we have from $S_n(\alpha) = A_n$ and (7.11) that $S_n(\alpha) = S_n(\Delta)$, hence $F(\alpha) = F(\Delta)$. This demonstrates the power inherent in combining field theory with group theory.

Any field between F and K is of the form $F(\alpha)$ for some α in K. Consider the map

$$\begin{aligned} \Lambda\colon \{\text{field between } F \text{ and } K\} &\longrightarrow \{\text{subgroup of } S_n\} \\ F(\alpha) &\longmapsto S_n(\alpha). \end{aligned} \tag{7.18}$$

Suppose that $F(\alpha) = F(\beta)$ for some β in K. By Theorem 7.17, $S_n(\alpha) = S_n(\beta)$, so Λ is well defined. The idea of linking fields between F and K with subgroups of S_n, although implicit in the work of Lagrange, only becomes manifest in the writings of Galois, as we will discuss in Chapter 8.

Theorem 7.20. Λ is a bijection.

Proof. Suppose that α_1 and α_2 in K are such that $S_n(\alpha_1) = S_n(\alpha_2)$. By Theorem 7.19, $F(\alpha_1) = F(\alpha_2)$, so Λ is injective. Let H be a subgroup of S_n and consider

$$\beta = \sum_{\sigma \in H} \sigma(t_1 t_2^2 t_3^3 \cdots t_n^n) = \sum_{\sigma \in H} t_{\sigma(1)} t_{\sigma(2)}^2 t_{\sigma(3)}^3 \cdots t_{\sigma(n)}^n.$$

Clearly, $H \subseteq S_n(\beta)$. Take ν in $S_n(\beta)$. Since the monomial $t_1 t_2^2 t_3^3 \cdots t_n^n$ is a term in β and $\nu(\beta) = \beta$, the monomial $t_{\nu(1)} t_{\nu(2)}^2 t_{\nu(3)}^3 \cdots t_{\nu(n)}^n$ is likewise a term in β. It follows from the algebraic independence of $t_1, t_2, \ldots, t_n$ over E that this is possible only if ν is in H. Therefore, $S_n(\beta) \subseteq H$, hence $S_n(\beta) = H$. Thus, Λ is surjective. □

Recall from Theorem 7.8(b) that $K = F(\varrho)$. An important implication of this equality of fields is that solving $r(x) = \min(\varrho, F)$ by radicals over F is equivalent to solving $f(x)$ by radicals over F. As illustrated below, a potential advantage of this change in focus is that $r(x)$ may be computationally more convenient than $f(x)$. Provided that F contains certain roots of unity, we know from Theorem 7.11 that $f(x)$ is not solvable by irreducible radicals over F when $n \geq 5$. Nevertheless, shifting attention from $f(x)$ to $r(x)$, with a corresponding emphasis on ϱ, provides a useful perspective that will greatly influence our subsequent discussions of solvability and Galois theory. In the present context, this means thinking of K as $F(\varrho)$ rather than as $F(t_1, t_2, \ldots, t_n)$. In the classical literature, ϱ, which we have until now referred to as a primitive element (for K over F), is called a *resolvent*. Unfortunately, this same term has been applied to $r(x)$. To avoid confusion, we will call $r(x)$ a *resolvent polynomial*.

We illustrate some of the above ideas for the case $n = 3$, under the assumption that F contains a primitive cube root of unity ω. We have

$$S_3 = \{id, (t_1\ t_2), (t_1\ t_3), (t_2\ t_3), (t_1\ t_2\ t_3), (t_1\ t_3\ t_2)\}$$
$$A_3 = \{id, (t_1\ t_2\ t_3), (t_1\ t_3\ t_2)\}$$

and

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_2 - t_3).$$

Corresponding to (6.18), let

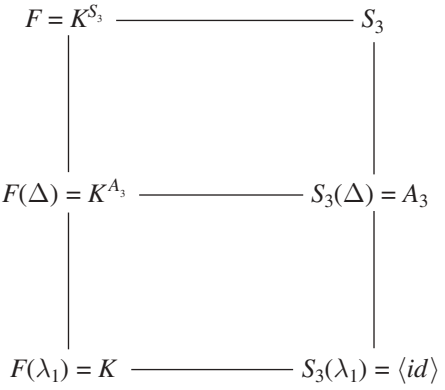
$$\lambda_1 = t_1 + \omega t_2 + \omega^2 t_3.$$

According to the remarks following Theorem 7.19, $K = F(\lambda_1)$, so λ_1 is a resolvent for K over F. We show in (15.5) that λ_1^3 is in $F(\Delta)$. Evidently, $S_3(\lambda_1) = \langle id \rangle$, and it is readily verified that $S_3(\Delta) = A_3$, as would be expected from Theorem 7.12. The diagram below depicts these relationships.

An important observation, and one that is consistent with Theorems 7.17 and 7.20, is that as we "ascend" from F to $F(\lambda_1)$, we simultaneously "descend" from S_3 to $\langle id \rangle$.

Let $r(x) = \min(\lambda_1, F)$. By Theorem 7.8(a),

$$r(x) = \prod_{\sigma \in S_3} [x - \sigma(\lambda_1)].$$



We show in (15.2) that

$$\begin{aligned} r(x) &= (x^3 - \lambda_1^3)(x^3 - \lambda_2^3) \\ &= x^6 - (2s_1^3 - 9s_1s_2 + 27s_3)x^3 + (s_1^2 - 3s_2)^3. \end{aligned} \tag{7.19}$$

Note that $r(x)$ is a quadratic polynomial in x^3. As such, it can be solved by first using the quadratic formula and then taking cube roots. This illustrates the point made above that focusing on the resolvent and the resolvent polynomial sometimes offers computational advantages. Substituting $s_1 = 0$, $s_2 = p$, and $s_3 = -q$ into (7.19) yields

$$r(x) = x^6 + 27qx^3 - 27p^3. \tag{7.20}$$

It is interesting to observe that (7.20) arose previously as (1.10), where it played a central role in the derivation of Cardan's formulas.

CHAPTER 8

CLASSICAL GALOIS THEORY ACCORDING TO GALOIS

In Chapter 7, we presented some of the classical (and toward the end of the chapter, not so classical) results on Galois theory, as it relates to general polynomials. The symmetric group S_n and the FTSRF were especially prominent in those discussions. Their importance can be traced in part to remarks made in connection with (7.8), where it was demonstrated that if q is a polynomial in $F[x_1, x_2, \ldots, x_n]$ such that $q(t_1, t_2, \ldots, t_n) = 0$, then

$$q(\sigma(t_1), \sigma(t_2), \ldots, \sigma(t_n)) = 0$$

for all σ in S_n. This shows that polynomial identities in $t_1, t_2, \ldots, t_n$ over F are symmetric in $t_1, t_2, \ldots, t_n$ over F.

We would like to extend the ideas introduced in Chapter 7 in the context of the general polynomial (which is really not so "general" after all) to arbitrary polynomials over an arbitrary field. In making this transition, we need to be aware that the symmetry property just alluded to may no longer apply. As an illustration, consider $f(x) = (x^2 - 2)(x^2 - 3)$ in $\mathbb{Q}[x]$, which has the roots $\alpha_1, \alpha_2 = \pm\sqrt{2}$ and $\alpha_3, \alpha_4 = \pm\sqrt{3}$. There are numerous polynomials q in $\mathbb{Q}[x_1, x_2, x_3, x_4]$ such that $q(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0$, for example,

$$q(x_1, x_2, x_3, x_4) = x_3^2 - x_1^2 - 1.$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Take $\sigma = (x_1\ x_3)$ in S_4. Then

$$q(\sigma(x_1), \sigma(x_2), \sigma(x_3), \sigma(x_4)) = q(x_3, x_2, x_1, x_4) = x_1^2 - x_3^2 - 1$$

but $q(\alpha_3, \alpha_2, \alpha_1, \alpha_4) \neq 0$. This lack of symmetry suggests that S_4 is "too big" for a study of $f(x)$, and that we need to focus our attention on some subgroup of S_4. But which one?

In this chapter, we present the answer given by Galois. Before proceeding, it should be remarked that the title of the chapter is not literally correct. The material presented in this chapter is based on the *ideas* of Galois, but in several places the exposition uses more modern methods than those to be found in his writings.

At this point, the reader is encouraged to become familiar with Galois's *Mémoire* referred to in the introduction to Chapter 1. An English translation of this remarkable document is provided in Edwards (1984). In fact, this version includes his submission to the Paris Academy of Sciences plus additional material written to a friend the night before the duel that ended his tragically short life. The originality of this work is truly impressive, but it is also notable for another less flattering reason. Setting aside the hastily added material, which admittedly was written *in extremis*, it must be acknowledged that parts of the original *Mémoire* are simply not that clearly presented. In retrospect, we can see that the results announced by Galois were both deep and far reaching, but in more than a few instances the "proofs" that he provides amount to little more than sketches of ideas to be followed. In fact, it would take the efforts of several generations of mathematicians to provide a rigorous treatment of the groundbreaking developments introduced by Galois.

For the rest of the chapter, let F be an arbitrary field, let $f(x)$ be an arbitrary polynomial in $F[x]$ of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, and let K be the splitting field of $f(x)$ over F. We wish to discuss the action of a subgroup of S_n on the roots of $f(x)$. To do so meaningfully, we need to assume that the roots are simple. The next result guarantees that there is no loss of generality incurred by making this assumption.

Theorem 8.1. Let $f(x)$ be a nonconstant polynomial in $F[x]$. Then $f(x)/\gcd(f, D_x(f))$ is a polynomial in $F[x]$, and it has the same roots as $f(x)$ but with the property that its roots are simple.

Proof. As in Theorem 2.8, let $f(x)$ have the factorization

$$f(x) = cg_1(x)^{d_1} g_2(x)^{d_2} \cdots g_m(x)^{d_m}$$

over F, where c is in F and $g_1(x), g_2(x), \ldots, g_m(x)$ are distinct monic polynomials in $F[x]$ that are irreducible over F. By Theorem 2.18, each of $g_1(x), g_2(x), \ldots, g_m(x)$ has simple roots, and by Theorem 2.7, they have no

roots in common. For convenience of notation, let $c = 1$ and $m = 3$, and let us denote $g_j(x)$ by g_j for $j = 1, 2, 3$. Then $f = g_1^{d_1} g_2^{d_2} g_3^{d_3}$ and

$$\begin{aligned} &D_x(f) \\ &\quad = D_x(g_1^{d_1}) g_2^{d_2} g_3^{d_3} + D_x(g_2^{d_2}) g_1^{d_1} g_3^{d_3} + D_x(g_3^{d_3}) g_1^{d_1} g_2^{d_2} \\ &\quad = g_1^{d_1-1} g_2^{d_2-1} g_3^{d_3-1} [d_1 D_x(g_1) g_2 g_3 + d_2 D_x(g_2) g_1 g_3 + d_3 D_x(g_3) g_1 g_2]. \end{aligned} \quad (8.1)$$

Evidently, $\gcd(f, D_x(f))$ is a product of powers of g_1, g_2, and g_3. We first observe that $g_1^{d_1-1} g_2^{d_2-1} g_3^{d_3-1}$ divides $\gcd(f, D_x(f))$. Suppose that g_1 divides the term in square brackets in (8.1), and therefore divides $d_1 D_x(g_1) g_2 g_3$. Since F has characteristic 0, we have $d_1 \neq 0$, so g_1 divides $D_x(g_1)$. But this is impossible because $D_x(g_1)$ has smaller degree than g_1. Similar observations apply to g_2 and g_3, so

$$\gcd(f, D_x(f)) = g_1^{d_1-1} g_2^{d_2-1} g_3^{d_3-1}.$$

Therefore,

$$\frac{f}{\gcd(f, D_x(f))} = g_1 g_2 g_3.$$

□

Note that, given a nonconstant polynomial $f(x)$ in $F[x]$, we can compute $f(x)/\gcd(f, D_x(f))$ explicitly using the Division Algorithm and the Euclidean Algorithm.

Let $c_1, c_2, \ldots, c_n$ be elements in F, and let

$$\psi = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

For each σ in S_n, let

$$\psi_\sigma = c_1\alpha_{\sigma(1)} + c_2\alpha_{\sigma(2)} + \cdots + c_n\alpha_{\sigma(n)}$$

where we note that $\psi = \psi_{id}$. At this point, we view S_n exclusively as a group of permutations on $\{1, 2, \ldots, n\}$. The discussion regarding automorphisms comes later. We say that ψ is a *Galois resolvent* for $f(x)$ over F if $\psi_\sigma \neq \psi_\tau$ for all $\sigma \neq \tau$ in S_n. Observe that the notion of Galois resolvent applies only in the context of splitting fields. By the FTSP,

$$R(x) = \prod_{\sigma \in S_n} (x - \psi_\sigma)$$

is a polynomial in $F[x]$ that has ψ as a root. Evidently, ψ is a Galois resolvent for $f(x)$ over F if and only if $R(x)$ has simple roots.

Theorem 8.2 (Galois). There is a Galois resolvent for $f(x)$ over F.

Proof. Consider

$$p(x_1, x_2, \ldots, x_n) = \prod_{(\sigma,\tau)} [(\alpha_{\sigma(1)} - \alpha_{\tau(1)})x_1 + \cdots + (\alpha_{\sigma(n)} - \alpha_{\tau(n)})x_n]$$

where the product is over all ordered pairs (σ, τ) of distinct permutations in S_n. It follows from the FTSP that p is in $F[x_1, x_2, \ldots, x_n]$. Furthermore, p is not the zero polynomial, for if it were, we would have

$$(\alpha_{\sigma(1)} - \alpha_{\tau(1)})x_1 + \cdots + (\alpha_{\sigma(n)} - \alpha_{\tau(n)})x_n = 0$$

for at least one of the terms of p. But this is possible only if $\alpha_{\sigma(i)} = \alpha_{\tau(i)}$ for $i = 1, 2, \ldots, n$. Since $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct, this would imply that $\sigma = \tau$, which is a contradiction.

We claim that for an arbitrary nonzero polynomial q in $F[x_1, x_2, \ldots, x_n]$, there are elements $c_1, c_2, \ldots, c_n$ in F such that $q(c_1, c_2, \ldots, c_n) \neq 0$. The proof is by induction on n. For $n = 1$, take c_1 to be any element in F other than a root of $q(x_1)$. Suppose that $n > 1$. We can express q as a polynomial in x_n with coefficients in $F[x_1, x_2, \ldots, x_{n-1}]$:

$$q(x_1, x_2, \ldots, x_n) = \sum_{k=0}^{N} q'_k(x_1, x_2, \ldots, x_{n-1})x_n^k.$$

Since q is a nonzero polynomial in $F[x_1, x_2, \ldots, x_n]$, there is $0 \leq k \leq N$ such that q'_k is a nonzero polynomial in $F[x_1, x_2, \ldots, x_{n-1}]$. By the induction hypothesis, there are elements $c_1, c_2, \ldots, c_{n-1}$ in F such that $q'_k(c_1, c_2, \ldots, c_{n-1}) \neq 0$. Then

$$q''(x_n) = q(c_1, c_2, \ldots, c_{n-1}, x_n)$$

is a nonzero polynomial in $F[x_n]$, and we are back to the case of a single indeterminate. This proves the claim.

To complete the proof, we apply the claim to p. Then

$$\psi = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

is the desired Galois resolvent for $f(x)$ over F. □

Theorem 8.3 (Galois). A Galois resolvent for $f(x)$ over F is a primitive element for K over F.

Proof. Let

$$f(x) = x^n - b_1x^{n-1} + b_2x^{n-2} + \cdots + (-1)^{n-1}b_{n-1}x + (-1)^n b_n$$

and let $s_1, s_2, \ldots, s_n$ be the elementary symmetric polynomials in $x_1, x_2, \ldots, x_n$ over F. Then $s_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = b_i$ for $i = 1, 2, \ldots, n$. Let

$$\psi = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

be a Galois resolvent for $f(x)$ over F. Clearly, $F(\psi) \subseteq K$. To prove the reverse inclusion, recall from (3.13) that

$$s_{k[i]} = \sum_{j=0}^{k-1} (-1)^j x_i^j s_{k-j} + (-1)^k x_i^k$$

for $k = 1, 2, \ldots, n-1$ and $i = 1, 2, \ldots, n$. Let $S_n(1)$ be the subgroup of S_n that leaves 1 fixed, and consider

$$\prod_{\nu \in S_n(1)} [y - (c_1x_1 + c_2x_{\nu(2)} + c_3x_{\nu(3)} + \cdots + c_nx_{\nu(n)})]. \tag{8.2}$$

Since $s_{1[1]}, s_{2[1]}, \ldots, s_{n-1[1]}$ are the elementary symmetric polynomials in $x_2, x_3, \ldots, x_n$ over F, by the FTSP and Theorem 3.8, (8.2) is a polynomial in

$$F[s_{1[1]}, s_{2[1]}, \ldots, s_{n-1[1]}, x_1, y] = F[s_1, s_2, \ldots, s_n, x_1, y].$$

Substituting $y = \psi, s_1 = b_1, \ldots, s_n = b_n$ into this polynomial, we obtain a polynomial $g(x_1)$ in $F(\psi)[x_1]$ that has α_1 as a root.

Now, let $S_n(2)$ be the subgroup of S_n that leaves 2 fixed, and consider

$$\prod_{\nu \in S_n(2)} [y - (c_1x_2 + c_2x_{\nu(1)} + c_3x_{\nu(3)} + \cdots + c_nx_{\nu(n)})]. \tag{8.3}$$

Since $s_{1[2]}, s_{2[2]}, \ldots, s_{n-1[2]}$ are the elementary symmetric polynomials in $x_1, x_3, \ldots, x_n$ over F, for the above reasons, (8.3) is a polynomial in

$$F[s_{1[2]}, s_{2[2]}, \ldots, s_{n-1[2]}, x_2, y] = F[s_1, s_2, \ldots, s_n, x_2, y].$$

Substituting $y = \psi, s_1 = b_1, \ldots, s_n = b_n$ into this polynomial, we obtain a polynomial $h(x_2)$ in $F(\psi)[x_2]$. But $h(x_2)$ does not have α_2 as a root, for if it did, we would then have

$$\psi = c_1\alpha_2 + c_2\alpha_{\nu(1)} + c_3\alpha_{\nu(3)} + \cdots + c_n\alpha_{\nu(n)}$$

for some ν in $S_n(2)$, which contradicts the Galois resolvent property of ψ.

For each k, we can think of $s_{k[1]}$ as a polynomial in the indeterminate x_1 with coefficients in $F(s_1, s_2, \ldots, s_n)$. A similar interpretation can be given to $s_{k[2]}$. We now observe that, for each k, $s_{k[1]}$ and $s_{k[2]}$ are formally identical except for the labeling of their respective indeterminates. It follows that

$g(x) = h(x)$. Therefore, α_2 is not a root of $g(x)$, and by analogy, neither is any of $\alpha_3, \alpha_4, \ldots, \alpha_n$.

Let $p(x) = \gcd(f, g)$. Since α_1 is a root of $f(x)$ and $g(x)$, it is a root of $p(x)$. We just demonstrated that α_1 is the only root that $f(x)$ and $g(x)$ have in common, so $p(x) = x - \alpha_1$. Since $f(x)$ and $g(x)$ are polynomials in $F(\psi)[x]$, so is $p(x)$. Therefore, α_1 is in $F(\psi)$, and similarly, $\alpha_2, \alpha_3, \ldots, \alpha_n$ are in $F(\psi)$. It follows that $K \subseteq F(\psi)$. □

Example 8.4. We illustrate the construction in the proof of Theorem 8.3 for $n = 3$. In this case, (8.2) becomes

$$[y - (c_1x_1 + c_2x_2 + c_3x_3)][y - (c_1x_1 + c_2x_3 + c_3x_2)].$$

With some help from *Maple*, we find that

$$\begin{aligned}(c_1x_1 + c_2x_2 + c_3x_3) + (c_1x_1 + c_2x_3 + c_3x_2)&\\ = 2c_1x_1 + (c_2 + c_3)s_{1[1]}&\\ = (2c_1 - c_2 - c_3)x_1 + (c_2 + c_3)s_1&\end{aligned} \tag{8.4}$$

and

$$\begin{aligned}(c_1x_1 + c_2x_2 + c_3x_3)(c_1x_1 + c_2x_3 + c_3x_2)&\\ = c_1^2x_1^2 + c_1(c_2 + c_3)s_{1[1]}x_1 + c_2c_3s_{1[1]}^2&\\ + (-2c_2c_3 + c_2^2 + c_3^2)s_{2[1]}&\\ = (c_1^2 + c_2^2 + c_3^2 - c_1c_2 - c_1c_3 - c_2c_3)x_1^2&\\ + (-c_2^2 - c_3^2 + c_1c_2 + c_1c_3)s_1x_1&\\ + (c_2^2 + c_3^2 - 2c_2c_3)s_2 + c_2c_3s_1^2.&\end{aligned} \tag{8.5}$$

On the other hand, (8.3) becomes

$$[y - (c_1x_2 + c_2x_1 + c_3x_3)][y - (c_1x_2 + c_2x_3 + c_3x_1)]$$

and we have

$$\begin{aligned}(c_1x_1 + c_2x_2 + c_3x_3) + (c_1x_1 + c_2x_3 + c_3x_2)&\\ = 2c_1x_2 + (c_2 + c_3)s_{1[2]}&\\ = (2c_1 - c_2 - c_3)x_2 + (c_2 + c_3)s_1&\end{aligned} \tag{8.6}$$

and

$$\begin{aligned}(c_1x_1 + c_2x_2 + c_3x_3)(c_1x_1 + c_2x_3 + c_3x_2)&\\ = c_1^2x_2^2 + c_1(c_2 + c_3)s_{1[2]}x_2 + c_2c_3s_{1[2]}^2&\end{aligned}$$

$$
\begin{aligned}
&+ (-2c_2c_3 + c_2^2 + c_3^2)s_{2[2]} \\
&= (c_1^2 + c_2^2 + c_3^2 - c_1c_2 - c_1c_3 - c_2c_3)x_2^2 \\
&\quad + (-c_2^2 - c_3^2 + c_1c_2 + c_1c_3)s_1x_2 + \\
&\quad + (c_2^2 + c_3^2 - 2c_2c_3)s_2 + c_2c_3s_1^2. \qquad (8.7)
\end{aligned}
$$

Note that we obtain (8.6) and (8.7) by replacing x_1 and $s_{1[1]}$ in the right-hand sides of (8.4) and (8.5) with x_2 and $s_{1[2]}$. Furthermore, the final expressions in (8.4) and (8.5) are identical to their counterparts in (8.6) and (8.7) if x_1 and x_2 are replaced by x. ◊

Example 8.5. The polynomial $f(x) = (x^2 - 2)(x^2 - 3)$ in $\mathbb{Q}[x]$ has the roots $\pm\sqrt{2}$ and $\pm\sqrt{3}$. The splitting field of $f(x)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let

$$\psi = \sqrt{2} + 2(-\sqrt{2}) + 3\sqrt{3} + 5(-\sqrt{3}) = -(\sqrt{2} + 2\sqrt{3}). \qquad (8.8)$$

Squaring both sides of (8.8), we obtain

$$\psi^2 = 14 + 4\sqrt{2}\sqrt{3}. \qquad (8.9)$$

Substituting $\sqrt{3} = -(\psi + \sqrt{2})/2$ into (8.9) gives

$$\sqrt{2} = \frac{10 - \psi^2}{2\psi} \qquad (8.10)$$

and substituting $\sqrt{2} = -(\psi + 2\sqrt{3})$ into (8.9) yields

$$\sqrt{3} = \frac{-10 - \psi^2}{4\psi}. \qquad (8.11)$$

Therefore, $K = \mathbb{Q}(\psi)$.

We know that $R(x) = \prod_{\sigma \in S_4}(x - \psi_\sigma)$ is a polynomial in $\mathbb{Q}[x]$ of degree 24. With the assistance of *Maple*, we obtain the following factorization of $R(x)$ into polynomials in $\mathbb{Q}[x]$ that are irreducible over $\mathbb{Q}$:

$$
\begin{aligned}
R(x) \;=\; & (x^4 - 28x^2 + 100)(x^4 - 22x^2 + 25)(x^4 - 60x^2 + 36) \\
& \times (x^4 - 70x^2 + 361)(x^4 - 70x^2 + 841)(x^4 - 100x^2 + 2116). \qquad (8.12)
\end{aligned}
$$

Also using *Maple*, we find that $\gcd(R, D_x(R)) = 1$. By Theorem 2.17, $R(x)$ has simple roots, which means that ψ is a Galois resolvent for $f(x)$ over $\mathbb{Q}$. ◊

By Theorem 8.3, a Galois resolvent is a primitive element, but a primitive element may not be a Galois resolvent, as we see in subsequent examples. In

what follows, we require only the primitive element property, so as a reminder, we will write θ in the place of ψ. Thus, $K = F(\theta)$. Our initial goal is to attach a group of permutations to the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x)$, and then show that a related group of automorphisms of K "preserves the algebraic relations" among the roots over F, in a sense to be made explicit below.

Let $r(x) = \min(\theta, F)$. By Theorems 2.18 and 4.9, $r(x)$ has simple roots, all of which are in K. They will be denoted by $\theta = \theta_1, \theta_2, \ldots, \theta_m$, where $m = \deg(r)$. We make repeated use of the observation that $r(x)$ divides any polynomial in $F[x]$ that has θ as a root, in which case θ_j is a root of the polynomial for $j = 1, 2, \ldots, m$.

For $i = 1, 2, \ldots, n$, let $g_i(x)$ be a polynomial in $F[x]$ such that

$$\alpha_i = g_i(\theta).$$

For $j = 1, 2, \ldots, m$, define a map

$$\begin{aligned} \sigma_j : \{\alpha_1, \alpha_2, \ldots, \alpha_n\} &\longrightarrow \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \\ \alpha_i &\longmapsto g_i(\theta_j) \end{aligned}$$

that is,

$$\sigma_j(\alpha_i) = g_i(\theta_j). \tag{8.13}$$

Since $f(g_i(x))$ is a polynomial in $F[x]$ that has θ as a root, θ_j is a root of $f(g_i(x))$, hence $g_i(\theta_j)$ is a root of $f(x)$ for each i and each j. Therefore, $\sigma_j(\alpha_i)$ is in $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, so σ_j is well defined.

Let

$$\mathrm{Gal}(f/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}.$$

Suppose that $\sigma_j(\alpha_i) = \sigma_j(\alpha_k)$ for some i and k. Then $g_i(\theta_j) = g_k(\theta_j)$, so $g_i(x) - g_k(x)$ is a polynomial in $F[x]$ that has θ_j as a root. It follows that θ is also a root, hence

$$\alpha_i = g_i(\theta) = g_k(\theta) = \alpha_k.$$

Thus, each σ_j is a permutation on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. We remark that at this point, it has not been established that the σ_j are distinct. We also remark that once $\theta = \theta_1$ has been chosen, the numbering of $\theta_2, \theta_3, \ldots, \theta_m$ is irrelevant as far as $\mathrm{Gal}(f/F)$ is concerned because any renumbering merely results in a corresponding renumbering of $\sigma_2, \sigma_3, \ldots, \sigma_m$.

The following result has an obvious similarity to (7.8).

Theorem 8.6 (Galois). If q is a polynomial in $F[x_1, x_2, \ldots, x_n]$ such that $q(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$, then

$$q(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)) = 0$$

for each j.

Proof. Since

$$q(\alpha_1, \alpha_2, \ldots, \alpha_n) = q(g_1(\theta), g_2(\theta), \ldots, g_n(\theta))$$

we see that $q(g_1(x), g_2(x), \ldots, g_n(x))$ is a polynomial in $F[x]$ that has θ as a root. Therefore, θ_j is a root, hence

$$q(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)) = q(g_1(\theta_j), g_2(\theta_j), \ldots, g_n(\theta_j)) = 0$$

for each j. □

By Theorem 2.20, each element of K can be expressed in the form $p(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some p in $F[x_1, x_2, \ldots, x_n]$. We now extend σ_j to a map on K by defining

$$\sigma_j : K \longrightarrow K$$
$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) \longmapsto p(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n))$$

that is,

$$\sigma_j(p(\alpha_1, \alpha_2, \ldots, \alpha_n)) = p(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)).$$

Suppose that p' is a polynomial in $F[x_1, x_2, \ldots, x_n]$ such that

$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) = p'(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Setting $q = p - p'$, it follows from Theorem 8.6 that

$$\sigma_j(p(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \sigma_j(p'(\alpha_1, \alpha_2, \ldots, \alpha_n))$$

so σ_j is well defined.

Theorem 8.7. $\sigma_j(\theta) = \theta_j$ for $j = 1, 2, \ldots, m$.

Proof. Let $\theta = p(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some p in $F[x_1, x_2, \ldots, x_n]$. By definition,

$$\sigma_j(\theta) = p(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)). \tag{8.14}$$

Since $\theta = p(g_1(\theta), g_2(\theta), \ldots, g_n(\theta))$, we observe that

$$x - p(g_1(x), g_2(x), \ldots, g_n(x))$$

is a polynomial in $F[x]$ that has θ as a root. Therefore, θ_j is a root, hence

$$\begin{aligned} \theta_j &= p(g_1(\theta_j), g_2(\theta_j), \ldots, g_n(\theta_j)) \\ &= p(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)). \end{aligned} \tag{8.15}$$

It follows from (8.14) and (8.15) that $\sigma_j(\theta) = \theta_j$ for $j = 1, 2, \ldots, m$. □

Theorem 8.8. $\sigma_1, \sigma_2, \ldots, \sigma_m$ are distinct, and $|\mathrm{Gal}(f/F)| = [K : F]$.

Proof. Since the θ_j are distinct, it follows from Theorem 8.7 that the σ_j are distinct. Then

$$|\mathrm{Gal}(f/F)| = m = \deg(r) = [F(\theta) : F] = [K : F].$$

□

Theorem 8.9.

$$\min(\theta, F) = \prod_{\sigma \in \mathrm{Gal}(f/F)} [x - \sigma(\theta)]$$

Proof. This follows from Theorem 8.7 and the definitions of $r(x)$ and $\mathrm{Gal}(f/F)$. □

Theorem 8.10. $\mathrm{Gal}(f/F)$ is the group of (all) automorphisms of K that fix F pointwise (where multiplication is defined to be composition of automorphisms).

Proof. We first show that each σ_j is an automorphism of K that fixes F pointwise. It is trivial that σ_j fixes F pointwise, and easily demonstrated that σ_j is both additive and multiplicative. So, σ_j is a ring homomorphism from K to K. Since K is a field, either $\ker(\sigma_j) = \{0\}$ or $\ker(\sigma_j) = K$, where $\ker(\sigma_j)$ is the kernel of σ_j. The second possibility is excluded by $\sigma_j(1) = 1$, so σ_j is injective. Thus, $[\mathrm{im}(\sigma_j) : F] = [K : F]$. It follows from

$$[K : F] = [K : \mathrm{im}(\sigma_j)][\mathrm{im}(\sigma_j) : F]$$

that $\mathrm{im}(\sigma_j) = K$, so σ_j is surjective. Therefore, σ_j is an automorphism of K that fixes F pointwise for $j = 1, 2, \ldots, m$.

Let τ be an automorphism of K that fixes F pointwise. Then $\tau(\theta)$ is a root of $f(x)$, so $\tau(\theta) = \theta_j$ for some j. Since $K = F(\theta)$, τ is completely determined by its value at θ. It follows from Theorem 8.7 that $\tau = \sigma_j$. Thus, $\mathrm{Gal}(f/F)$ is

the set of (all) automorphisms of K that fix F pointwise. With multiplication defined to be composition of automorphisms, it is now straightforward to show that $\mathrm{Gal}(f/F)$ is a group. □

For the remainder of the chapter, we will make repeated use of Theorem 8.10 but without always referencing it explicitly.

Theorem 8.11. $\mathrm{Gal}(f/F)$ is independent of the choice of primitive element.

Proof. This follows from Theorem 8.10. □

As in Theorem 8.6, let q be a polynomial in $F[x_1, x_2, \ldots, x_n]$ such that $q(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. We refer to an identity such as this as an *algebraic relation* among $\alpha_1, \alpha_2, \ldots, \alpha_n$ over F. There is an infinity of such algebraic relations, but is it possible to identify what could reasonably be considered a core set? Following Theorem 8.6, any algebraic relation can be expressed in the form

$$q(g_1(\theta), g_2(\theta), \ldots, g_n(\theta)) = 0.$$

Since $r(x)$ divides $q(g_1(x), g_2(x), \ldots, g_n(x))$, we have

$$q(g_1(x), g_2(x), \ldots, g_n(x)) = [r(x)]^k s(x)$$

for some $k \geq 1$, where $s(x)$ is a polynomial in $F[x]$ that does not have θ as a root. This shows that algebraic relations among $\alpha_1, \alpha_2, \ldots, \alpha_n$ over F are effectively the identities $r(\theta_j) = 0$ for $j = 1, 2, \ldots, m$. Of course, had we started with a different primitive element for K over F, we would have a different set of identities, but they could be translated into each other by exploiting the properties of primitive elements.

Theorem 8.6 tells us that each σ_j "preserves the algebraic relations" among $\alpha_1, \alpha_2, \ldots, \alpha_n$ over F. Thus, $\mathrm{Gal}(f/F)$ provides an answer to the question raised in the introduction to the chapter about which subgroup of S_n to assign to the polynomial $f(x)$ in $F[x]$. We refer to $\mathrm{Gal}(f/F)$ as the *classical Galois group* of $f(x)$ over F. According to Example 8.15, and in the notation of Chapter 7, if $f(x)$ is the general polynomial of degree n over the subfield E of F, then $\mathrm{Gal}(f/F) = S_n$. This is intuitively reasonable because the roots of a general polynomial would be expected to have only those algebraic relations that are symmetric in the roots.

Let us denote by $K^{\mathrm{Gal}(f/F)}$ the set of elements in K that are fixed pointwise by $\mathrm{Gal}(f/F)$, that is,

$$K^{\mathrm{Gal}(f/F)} = \{\beta \in K : \sigma_j(\beta) = \beta \text{ for } j = 1, 2, \ldots, m\}.$$

It is readily verified that $K^{\mathrm{Gal}(f/F)}$ is a field between F and K.

Theorem 8.12 (Galois). $K^{\mathrm{Gal}(f/F)} = F$.

Proof. Clearly, $F \subseteq K^{\mathrm{Gal}(f/F)}$. To prove the reverse inclusion, observe that each element of $K^{\mathrm{Gal}(f/F)}$ can be expressed in the form $h(\theta)$ for some polynomial $h(x)$ in $F[x]$. By Theorem 8.7,

$$h(\theta_j) = h(\sigma_j(\theta)) = \sigma_j(h(\theta)) = h(\theta)$$

for $j = 1, 2, \ldots, m$. Therefore,

$$h(\theta) = \frac{h(\theta_1) + h(\theta_2) + \cdots + h(\theta_m)}{m}.$$

Since the numerator is symmetric in the roots of $r(x)$, by the FTSP, $h(\theta)$ is in F. Therefore, $K^{\mathrm{Gal}(f/F)} \subseteq F$. □

Let E be a field between F and K. Since K is the splitting field of $f(x)$ over E, it makes sense to write $\mathrm{Gal}(f/E)$. It follows from Theorem 8.10 that $\mathrm{Gal}(f/E)$ is a subgroup of $\mathrm{Gal}(f/F)$. Accordingly, we have a map

$$\begin{aligned} \Upsilon\colon \{\text{field between } F \text{ and } K\} &\longrightarrow \{\text{subgroup of } \mathrm{Gal}(f/F)\} \\ E &\longmapsto \mathrm{Gal}(f/E). \end{aligned} \tag{8.16}$$

Theorem 8.13. Υ is a bijection.

Proof. Suppose that E_1 and E_2 are fields between F and K such that $\mathrm{Gal}(f/E_1) = \mathrm{Gal}(f/E_2)$. By Theorem 8.12, $E_1 = E_2$, so Υ is injective. Let H be a subgroup of $\mathrm{Gal}(f/F)$. We will show that Υ is surjective by finding an element β in K such that $H = \mathrm{Gal}(f/F(\beta))$.

Let $id = \tau_1, \tau_2, \ldots, \tau_l$ be left coset representatives of H in $\mathrm{Gal}(f/F)$, and let

$$g_j(x) = \prod_{\nu \in H} [x - \tau_j \nu(\theta)].$$

for $j = 1, 2, \ldots, l$. Let

$$h(x) = \prod_{(j,k)} [g_j(x) - g_k(x)]$$

where the product is over all ordered pairs (j, k) with $j \neq k$. Since each term in this product corresponds to a distinct ordered pair of distinct left cosets of H in $\mathrm{Gal}(f/F)$, the coefficients of $h(x)$ are fixed by $\mathrm{Gal}(f/F)$. It follows from Theorem 8.12 that $h(x)$ is in $F[x]$. Suppose that $g_j(x) = g_k(x)$ for some $1 \leq j < k \leq l$. Then $\tau_j(\theta)$, which is a root of $g_j(x)$, is also a root of $g_k(x)$. Thus, $\tau_j(\theta) = \tau_k \nu(\theta)$ for some ν in H. Each element of $\mathrm{Gal}(f/F)$ is completely determined by

its value at θ, so $\tau_j = \tau_k \nu$. Therefore, $\tau_j H = \tau_k H$, hence $j = k$. It follows that $h(x)$ is not the zero polynomial.

Let c be an element of F that is not a root of $h(x)$, and let

$$\beta = g_1(c) = \prod_{\nu \in H} [c - \nu(\theta)].$$

Evidently, $H \subseteq \mathrm{Gal}(f/F(\beta))$. To prove the reverse inclusion, take ρ in $\mathrm{Gal}(f/F(\beta))$. Then $\rho H = \tau_j H$ for some j, hence

$$g_j(c) = \prod_{\nu \in H} [c - \rho\nu(\theta)] = \rho\Big(\prod_{\nu \in H} [c - \nu(\theta)] \Big) = \rho(g_1(c)) = g_1(c).$$

Since c is not a root of $h(x)$, we have $j = 1$. Thus, $\rho H = H$, so ρ is in H. Therefore, $\mathrm{Gal}(f/F(\beta)) \subseteq H$. □

Like Λ in (7.18), Υ is an example of what we will later refer to as a Galois correspondence.

We close the chapter with a series of examples.

Example 8.14. We continue with Example 8.5. As was demonstrated in the introduction to this chapter, not all algebraic relations among the roots of $f(x)$ are symmetric over $\mathbb{Q}$. So, $\mathrm{Gal}(f/\mathbb{Q})$ is a proper subgroup of S_4. Squaring both sides of $\psi^2 - 14 = 4\sqrt{2}\sqrt{3}$ gives $\psi^4 - 28\psi^2 + 100 = 0$. Thus, ψ is a root of $r(x) = x^4 - 28x^2 + 100$. We have from (2.14) that $[K : \mathbb{Q}] = 4$. Then Theorem 2.12(b) implies that $r(x) = \min(\psi, \mathbb{Q})$. As can be seen from (8.12), $r(x)$ divides $R(x)$, as would be expected. It can be shown that the roots of $r(x)$ are

$$\psi_1, \psi_2 = -\sqrt{2} \mp 2\sqrt{3} \quad \text{and} \quad \psi_3, \psi_4 = \sqrt{2} \mp 2\sqrt{3}.$$

In order to determine $\mathrm{Gal}(f/\mathbb{Q})$, it is necessary to convert (8.10) and (8.11) into corresponding polynomial expressions. Using the Euclidean Algorithm, we find that

$$1 = \gcd(r, x) = \Big(\frac{1}{100}\Big) r(x) + \Big(\frac{-x^3 + 28x}{100}\Big) x$$

hence

$$\frac{1}{\psi} = \frac{-\psi^3 + 28\psi}{100}.$$

Let

$$h_1(x) = \Big(\frac{10 - x^2}{2}\Big)\Big(\frac{-x^3 + 28x}{100}\Big)$$

and

$$h_2(x) = \Big(\frac{-10 - x^2}{4}\Big)\Big(\frac{-x^3 + 28x}{100}\Big).$$

Using the Division Algorithm, we find that

$$h_1(x) = \Big(\frac{x}{200}\Big)r(x) + \Big(\frac{-x^3 + 18x}{20}\Big)$$

and

$$h_2(x) = \Big(\frac{x}{400}\Big)r(x) + \Big(\frac{x^3 - 38x}{40}\Big).$$

So, we define

$$g_1(x), g_2(x) = \pm\Big(\frac{-x^3 + 18x}{20}\Big)$$

and

$$g_3(x), g_4(x) = \pm\Big(\frac{x^3 - 38x}{40}\Big).$$

Then

$$g_1(\psi), g_2(\psi) = \pm\sqrt{2} \quad \text{and} \quad g_3(\psi), g_4(\psi) = \pm\sqrt{3}.$$

From the following table

j	$g_1(\psi_j)$	$g_2(\psi_j)$	$g_3(\psi_j)$	$g_4(\psi_j)$
1	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$
3	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
4	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$

we determine that $\sigma_1 = id$ and

$$\sigma_2 = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ \sqrt{2} & -\sqrt{2} & -\sqrt{3} & \sqrt{3} \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & \sqrt{3} & -\sqrt{3} \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & -\sqrt{3} & \sqrt{3} \end{pmatrix}.$$

Not surprisingly, the elements of $\mathrm{Gal}(f/\mathbb{Q})$ permute the roots of the irreducible factors of $f(x)$ among themselves. Setting $\sigma = \sigma_2$ and $\tau = \sigma_3$, and using cycle notation, we can write

$$\sigma = (\sqrt{3}, -\sqrt{3}) \quad \text{and} \quad \tau = (\sqrt{2}, -\sqrt{2})$$

where commas have been introduced to improve readability. Therefore,

$$\mathrm{Gal}(f/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\tau\}.$$

$\Diamond$

Example 8.15. In the notation of Chapter 7, let $f(x)$ be the general polynomial of degree n over the subfield E of F. Since $t_1, t_2, \ldots, t_n$ are algebraically independent over E, the primitive element ϱ defined in Theorem 7.8 is a Galois resolvent for $f(x)$ over F. It follows from Theorems 7.8(a) and 8.9 that $\mathrm{Gal}(f/F) = S_n$. $\Diamond$

Example 8.16 (Galois). Let $F = \mathbb{Q}$, and let p be a prime. It follows from either Example 4.8 or Theorem 5.4(a) that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. According to (5.10), the roots of $\Phi_p(x)$ are $\alpha_i = \zeta_p^{e^i}$ for $i = 0, 1, \ldots, p-2$, where e is a primitive congruence root modulo p. In the above notation, let

$$\theta = \zeta_p \quad r(x) = \Phi_p(x) \quad \text{and} \quad \theta_j = \zeta_p^{e^j}$$

for $j = 0, 1, \ldots, p-2$. With $g_i(x) = x^{e^i}$, we have from (8.13) that

$$\sigma_j(\alpha_i) = \zeta_p^{e^{i+j}} = \alpha_{i+j}$$

for $i, j = 0, 1, \ldots, p-2$, where $i + j$ is taken modulo p. Therefore, $\sigma_0 = id$,

$$\sigma_1 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{p-4} & \alpha_{p-3} & \alpha_{p-2} \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{p-3} & \alpha_{p-2} & \alpha_0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{p-4} & \alpha_{p-3} & \alpha_{p-2} \\ \alpha_2 & \alpha_3 & \alpha_4 & \cdots & \alpha_{p-2} & \alpha_0 & \alpha_1 \end{pmatrix}$$

and so on. Thus,

$$\mathrm{Gal}(\Phi_p/\mathbb{Q}) = \langle (\alpha_0\ \alpha_1\ \alpha_2\ \ldots\ \alpha_{p-2}) \rangle$$

which is a cyclic group of order $p-1$. Note that $\theta = \zeta_p$ is not a Galois resolvent for $\Phi_p(x)$ over $\mathbb{Q}$ because $\zeta_p = \alpha_0$ is fixed by all permutations ν in S_n that fix 0.

As an illustration, take $p = 5$. Then

$$\mathrm{Gal}(\Phi_5/\mathbb{Q}) = \{id, (\alpha_0\ \alpha_1\ \alpha_2\ \alpha_3), (\alpha_0\ \alpha_2)(\alpha_1\ \alpha_3), (\alpha_0\ \alpha_3\ \alpha_2\ \alpha_1)\}.$$

The only nontrivial subgroup of $\mathrm{Gal}(\Phi_5/\mathbb{Q})$ is $\langle(\alpha_0\ \alpha_2)(\alpha_1\ \alpha_3)\rangle$. Taking $e = 2$, we have

$$(\alpha_0\ \alpha_2)(\alpha_1\ \alpha_3) = (\zeta_5\ \zeta_5^4)(\zeta_5^2\ \zeta_5^3).$$

By Theorem 8.13, there is precisely one field strictly between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$. It follows from Theorem 13.6(a), and it will be illustrated in Example 13.11, that the field is $\mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}(\zeta_5^2 + \zeta_5^3)$. ◊

Example 8.17. Let F be a field, let $h(x) = x^n - a$ be a polynomial in $F[x]$ that is irreducible over F, and suppose that F contains a primitive nth root of unity ζ. Let β be an arbitrary root of $h(x)$. Then the roots of $h(x)$ are $\alpha_i = \zeta^i\beta$ for $i = 0, 1, \ldots, n-1$. In the above notation, let

$$\theta = \beta \quad r(x) = h(x) \quad \text{and} \quad \theta_j = \zeta^j\beta$$

for $j = 0, 1, \ldots, n-1$. With $g_i(x) = \zeta^i x$, we have from (8.13) that

$$\sigma_j(\alpha_i) = \zeta^{i+j}\beta = \alpha_{i+j}$$

for $i, j = 0, 1, \ldots, n-1$, where $i + j$ is taken modulo n. Therefore, $\sigma_0 = id$,

$$\sigma_1 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-3} & \alpha_{n-2} & \alpha_{n-1} \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{n-2} & \alpha_{n-1} & \alpha_0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-3} & \alpha_{n-2} & \alpha_{n-1} \\ \alpha_2 & \alpha_3 & \alpha_4 & \cdots & \alpha_{n-1} & \alpha_0 & \alpha_1 \end{pmatrix}$$

and so on. Thus,

$$\mathrm{Gal}(h/F) = \langle(\alpha_0\ \alpha_1\ \alpha_2\ \ldots\ \alpha_{n-1})\rangle$$

which is a cyclic group of order n. The connection between irreducible binomial polynomials and cyclic groups will be explored in greater depth in Chapter 10. ◊

CHAPTER 9

MODERN GALOIS THEORY

In this chapter, we present the essentials of Galois theory from a modern perspective. To an even greater extent than in Chapters 7 and 8, the focus is on the interplay between groups and fields. A noticeable change is that we no longer make use of the FTSP or the FTSRF. To a certain extent, especially in Theorem 9.12, this important role is taken over by the Isomorphism Extension Theorem. However, we will not altogether lose sight of the groundwork laid in earlier chapters. In particular, we make frequent use of the Primitive Element Theorem (via Theorem 2.23), a result that is intimately related to the classical notions of resolvent and resolvent polynomial. It must be admitted that this is generally not the approach taken in contemporary expositions of Galois theory. Currently, for example, Theorems 9.2 and 9.5 would be developed using what is referred to as the Theorem on Linear Independence of Characters. Here, we have opted for the possibly less elegant approach based on the Primitive Element Theorem for two reasons: It allows for proofs that are relatively transparent, and it ensures a measure of continuity with earlier chapters.

Let K be a finite extension of F. The *Galois group* of K over F, denoted by $\mathrm{Gal}(K/F)$, is defined to be the set of (field) automorphisms of K that fix F pointwise, that is,

$$\mathrm{Gal}(K/F) = \{\sigma \text{ an automorphism of } K : \sigma(a) = a \text{ for all } a \in F\}.$$

It is readily verified that $\mathrm{Gal}(K/F)$ is indeed a group. Provided that K is the splitting field over F of some polynomial $f(x)$ in $F[x]$, we see from Theorem 8.10

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

that $\mathrm{Gal}(K/F)$ is the same as $\mathrm{Gal}(f/F)$. A notable feature of the present definition of $\mathrm{Gal}(K/F)$ is that we do not require K to be a splitting field.

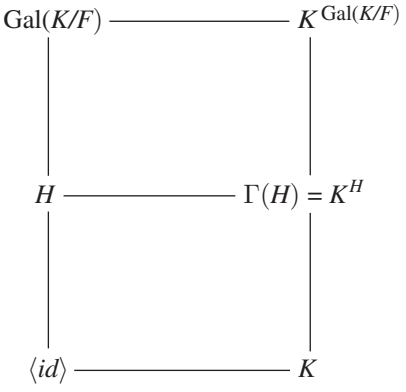
Let H be a subgroup of $\mathrm{Gal}(K/F)$, and let K^H be the set of elements in K that are fixed pointwise by H, that is,

$$K^H = \{\alpha \in K : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

It is straightforward to check that K^H is a field between F and K. The map

$$\begin{aligned} \Gamma\colon \{\text{subgroup of } \mathrm{Gal}(K/F)\} &\longrightarrow \{\text{field between } F \text{ and } K\} \\ H &\longmapsto K^H \end{aligned}$$

is called the *Galois correspondence* between the subgroups of $\mathrm{Gal}(K/F)$ and the fields between F and K. This is depicted in the following figure. For simplicity, in this figure and in those appearing later in the book, "maps to" and "included in" are represented by lines without arrowheads.



Let H_1 and H_2 be subgroups of $\mathrm{Gal}(K/F)$ such that $H_1 \subseteq H_2$. Then $K^{H_2} \subseteq K^{H_1}$, so Γ is order reversing, where "order" is defined in terms of set inclusion. An obvious difference between the map Γ and the maps Λ and Υ defined in (7.18) and (8.16), respectively, is that Γ takes as its domain a set of subgroups, whereas for Λ and Υ the domain is a set of fields. The rationale for the present approach will become apparent as we proceed.

The chapter is divided into two sections. In Section 9.1, we only require K to be a finite extension of F, whereas in Section 9.2, we assume that K is a splitting field over F.

9.1 GALOIS THEORY AND FINITE EXTENSIONS

The following result has an obvious similarity to Theorem 8.6.

Theorem 9.1. Let K be a finite extension of F, and let $\alpha_1, \alpha_2, \ldots \alpha_n$ be arbitrary elements of K. If q is a polynomial in $F[x_1, x_2, \ldots, x_n]$ such that $q(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$, then

$$q(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) = 0$$

for all σ in $\mathrm{Gal}(K/F)$.

Proof. Straightforward. □

Theorem 9.2. If K is a finite extension of F, then $|\mathrm{Gal}(K/F)| \leq [K : F]$.

Proof. Let $K = F(\theta)$ for some θ in K, let $r(x) = \min(\theta, F)$, and take σ in $\mathrm{Gal}(K/F)$. By Theorem 9.1, $\sigma(\theta)$ is a root of $r(x)$. Since σ is completely determined by its value at θ, it follows from Theorem 2.12(b) that

$$|\mathrm{Gal}(K/F)| \leq \deg(r) = [F(\theta) : F] = [K : F].$$

□

Example 9.3. Let $F = \mathbb{Q}, f(x) = x^3 - 2$, and $K = \mathbb{Q}(\sqrt[3]{2})$, where $\sqrt[3]{2}$ is the real cube root of 2. The roots of $f(x)$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where ω is a primitive cube root of unity. Since $f(x)$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Let us take σ in $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ and observe that, by Theorem 9.1, $\sigma(\sqrt[3]{2})$ is a root of $f(x)$. Since ω is not in $\mathbb{Q}(\sqrt[3]{2})$, we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \langle id \rangle$, hence $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$. Thus,

$$|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

The reason for the strict inequality seems to be that $\mathbb{Q}(\sqrt[3]{2})$ does not contain "enough" roots of $f(x)$ to allow all possible automorphisms. ◊

Example 9.4. We continue with Examples 8.5 and 8.14, where $F = \mathbb{Q}$, $f(x) = (x^2 - 2)(x^2 - 3)$, and $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. As was observed in Example 8.14, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. In the notation of this chapter,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\tau\}$$

where σ is the automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that maps $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\mathbb{Q}(\sqrt{2})$ pointwise, and τ is the automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that maps $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\mathbb{Q}(\sqrt{3})$ pointwise. Since $f(x)$ splits over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, all the roots of $f(x)$ are available for automorphisms. This appears to explain why

$$|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}].$$

◊

Theorem 9.5. Let K be a finite extension of F, and let H be a subgroup of $\mathrm{Gal}(K/F)$. Then:
(a) $[K : K^H] = |H|$.
(b) $\mathrm{Gal}(K/K^H) = H$.

Proof. (a): Let $K = K^H(\theta)$ for some θ in K, and let $g(x) = \min(\theta, K^H)$. Using a familiar argument, we see that $f(x) = \prod_{\sigma \in H}[x - \sigma(\theta)]$ is a polynomial in $K^H[x]$ that has θ as a root. By parts (a) and (b) of Theorem 2.12,

$$[K : K^H] = \deg(g) \leq \deg(f) = |H|.$$

Since $H \subseteq \mathrm{Gal}(K/K^H)$, we have from Theorem 9.2 that

$$|H| \leq |\mathrm{Gal}(K/K^H)| \leq [K : K^H].$$

Therefore,

$$[K : K^H] = |H| = |\mathrm{Gal}(K/K^H)|. \tag{9.1}$$

(b): We saw in part (a) that $H \subseteq \mathrm{Gal}(K/K^H)$, and according to (9.1), $|H| = |\mathrm{Gal}(K/K^H)|$. By Theorem 9.2, $\mathrm{Gal}(K/K^H)$ is a finite group, so $H = \mathrm{Gal}(K/K^H)$. □

With only the preceding handful of results at our disposal, we are already in a position to say something of central importance about Γ.

Theorem 9.6. If K is a finite extension of F, then Γ is injective. Furthermore, if H is a subgroup of $\mathrm{Gal}(K/F)$, then $\mathrm{Gal}(K/\Gamma(H)) = H$.

Proof. Suppose that H_1 and H_2 are subgroups of $\mathrm{Gal}(K/F)$ such that $\Gamma(H_1) = \Gamma(H_2)$, that is, $K^{H_1} = K^{H_2}$. By Theorem 9.5(b), $H_1 = H_2$, so Γ is injective. The second assertion is simply a restatement of Theorem 9.5(b). □

Without further assumptions, Γ may not be surjective. To illustrate, recall from Example 9.3 that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \langle id \rangle$. Thus, the image of Γ is $\{\mathbb{Q}(\sqrt[3]{2})\}$, which does not contain the subfield $\mathbb{Q}$ of $\mathbb{Q}(\sqrt[3]{2})$.

Theorem 9.7. If K is a finite extension of F, then K is a splitting field over $K^{\mathrm{Gal}(K/F)}$.

Proof. Let $E = K^{\mathrm{Gal}(K/F)}$. By Theorem 9.5(b), $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/F)$, hence $K^{\mathrm{Gal}(K/E)} = E$. Let $K = F(\theta)$ for some θ in K. Then $f(x) = \prod_{\sigma \in \mathrm{Gal}(K/E)}[x - \sigma(\theta)]$ is a polynomial in $K^{\mathrm{Gal}(K/E)}[x] = E[x]$ that has θ as a root and splits over K. Therefore, K is the splitting field of $f(x)$ over E. □

Theorem 9.8. Let K be a finite extension of F, and let E be a field between F and K. Then

$$\mathrm{Gal}(K/\sigma(E)) = \sigma\mathrm{Gal}(K/E)\sigma^{-1}$$

for all σ in $\mathrm{Gal}(K/F)$.

Proof.

$$\begin{aligned} \tau \in \mathrm{Gal}(K/\sigma(E)) &\Leftrightarrow \tau(\sigma(\alpha)) = \sigma(\alpha) \text{ for all } \alpha \in E \\ &\Leftrightarrow \sigma^{-1}\tau\sigma(\alpha) = \alpha \text{ for all } \alpha \in E \\ &\Leftrightarrow \sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/E) \\ &\Leftrightarrow \tau \in \sigma\mathrm{Gal}(K/E)\sigma^{-1}. \end{aligned}$$

□

Theorem 9.9. Let K be a finite extension of F, and let H be a subgroup of $\mathrm{Gal}(K/F)$. Then

$$K^{\sigma H \sigma^{-1}} = \sigma(K^H)$$

for all σ in $\mathrm{Gal}(K/F)$.

Proof.

$$\begin{aligned} \alpha \in K^{\sigma H \sigma^{-1}} &\Leftrightarrow \sigma\tau\sigma^{-1}(\alpha) = \alpha \text{ for all } \tau \in H \\ &\Leftrightarrow \tau(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha) \text{ for all } \tau \in H \\ &\Leftrightarrow \sigma^{-1}(\alpha) \in K^H \\ &\Leftrightarrow \alpha \in \sigma(K^H). \end{aligned}$$

□

Theorem 9.10. Let K be a finite extension of F, and let E_1 and E_2 be fields between F and K. Then

$$\mathrm{Gal}(K/E_1E_2) = \mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2).$$

Proof. Clearly,

$$\mathrm{Gal}(K/E_1E_2) \subseteq \mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2).$$

Let us take σ in $\mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2)$. Since σ fixes both E_1 and E_2 pointwise, it does the same for E_1E_2, so σ is in $\mathrm{Gal}(K/E_1E_2)$. Therefore,

$$\mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2) \subseteq \mathrm{Gal}(K/E_1E_2).$$

□

Theorem 9.11. Let K be a finite extension of F, and let H_1 and H_2 be subgroups of $\mathrm{Gal}(K/F)$ such that $H_1 \subseteq H_2$. Then

$$[K^{H_1} : K^{H_2}] = [H_2 : H_1].$$

Proof. Since $H_1 \subseteq H_2$, we have $K^{H_2} \subseteq K^{H_1}$, so

$$[K : K^{H_2}] = [K : K^{H_1}][K^{H_1} : K^{H_2}].$$

By Theorem 9.5(a), $[K : K^{H_1}] = |H_1|$ and $[K : K^{H_2}] = |H_2|$, hence

$$[K^{H_1} : K^{H_2}] = \frac{[K : K^{H_2}]}{[K : K^{H_1}]} = \frac{|H_2|}{|H_1|} = [H_2 : H_1].$$

□

Theorems 9.8 and 9.9 display a duality that reflects the Galois correspondence. There are dual results for Theorems 9.10 and 9.11, and they are Theorems 9.14 and 9.15, respectively.

9.2 GALOIS THEORY AND SPLITTING FIELDS

The next result gives conditions that guarantee that equality is reached in Theorem 9.2. Consistent with the remarks made in Examples 9.3 and 9.4, by requiring K to be a splitting field over F, we ensure that there are "enough" roots available to permit the maximum number of automorphisms.

Theorem 9.12. Let K be a finite extension of F. Then the following are equivalent:

(a) K is a splitting field over F.
(b) $|\mathrm{Gal}(K/F)| = [K : F]$.
(c) $K^{\mathrm{Gal}(K/F)} = F$.
(d) Every polynomial in $F[x]$ that is irreducible over F and has a root in K splits over K; equivalently, $\min(\alpha, F)$ splits over K for every α in K.

Proof. All of the assertions are trivial if $K = F$, so assume that K is a proper extension of F.

(a)⇒(b): By assumption, K is the splitting field over F of some polynomial $f(x)$ in $F[x]$. Denoting the roots of $f(x)$ by $\alpha_1, \alpha_2, \ldots, \alpha_n$, we have $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $K = F(\theta)$ for some θ in K, and let $r(x) = \min(\theta, F)$. Let L be the splitting field of $r(x)$ over F, and let $\theta = \theta_1, \theta_2, \ldots, \theta_m$ be the (simple) roots of $r(x)$. Then $L = F(\theta_1, \theta_2, \ldots, \theta_m)$, hence $K \subseteq L$. By the Isomorphism Extension Theorem, there is an isomorphism $\sigma_j : F(\theta) \longrightarrow F(\theta_j)$ extending *id* on F and such that $\sigma_j(\theta) = \theta_j$ for $j = 1, 2, \ldots, m$. Since $\theta = p(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some polynomial p in $F[x_1, x_2, \ldots, x_n]$, we have

$$\theta_j = p(\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)).$$

By Theorem 9.1, each of $\sigma_j(\alpha_1), \sigma_j(\alpha_2), \ldots, \sigma_j(\alpha_n)$ is a root of $f(x)$, so θ_j is in K for all j. Therefore, $L \subseteq K$, hence $L = K$. Since $r(x) = \min(\theta_j, F)$ for all j, we have

$$[F(\theta) : F] = \deg(r) = [F(\theta_j) : F]$$

hence $K = F(\theta_j)$ for all j. So, each σ_j is in $\mathrm{Gal}(K/F)$. Since σ_j is completely determined by its value at θ, and since the θ_j are distinct, we have

$$|\mathrm{Gal}(K/F)| \geq \deg(r) = [K : F].$$

It follows from Theorem 9.2 that $|\mathrm{Gal}(K/F)| = [K : F]$.

(b)⇒(c): Since $F \subseteq K^{\mathrm{Gal}(K/F)}$, we have

$$[K : F] = [K : K^{\mathrm{Gal}(K/F)}][K^{\mathrm{Gal}(K/F)} : F].$$

By Theorem 9.5(a),

$$[K : K^{\mathrm{Gal}(K/F)}] = |\mathrm{Gal}(K/F)| = [K : F]$$

hence $[K^{\mathrm{Gal}(K/F)} : F] = 1$. Therefore, $K^{\mathrm{Gal}(K/F)} = F$.

(c)⇒(d): Take α in K. Then $g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)}[x - \sigma(\alpha)]$ is a polynomial in $K^{\mathrm{Gal}(K/F)}[x] = F[x]$ that has α as a root. Since $\min(\alpha, F)$ divides $g(x)$, and $g(x)$ splits over K, so does $\min(\alpha, F)$.

(d)⇒(a): Let $K = F(\theta)$ for some θ in K, and let $r(x) = \min(\theta, F)$. Since $r(x)$ splits over K, it follows that K is the splitting field of $r(x)$ over F. □

Note that, in the notation of Theorem 9.12, Theorem 4.9 asserts that (a)⇒(d).

Let K be a finite, hence algebraic, extension of F. In contemporary expositions of Galois theory, it is usual to define K to be a *normal extension* of F if it satisfies any of the equivalent conditions of Theorem 9.12, and to be a *separable extension* of F if $\min(\alpha, F)$ has simple roots for all α in K. When K is both a normal and a separable extension of F, it is said to be a *Galois extension* of F. This terminology has the advantage of drawing attention away from the polynomial giving rise to K as a splitting field over F and placing the focus on K as an extension of F. The notion of separability is important in the study of fields having nonzero characteristic. However, as was emphasized at the beginning of Chapter 2, almost all fields considered in this book have characteristic 0; and in this case, by Theorem 2.18, extensions are automatically separable. Furthermore, the definition of what it means to be a Galois extension sometimes varies from author to author. For these reasons, we will stay with the splitting field terminology.

Suppose that K is a splitting field over F and that E is a field between F and K. By Theorem 2.27, K is a splitting field over E; however, E may not be a splitting field over F. To illustrate, it follows from Eisenstein's criterion with $p = 2$ that $x^4 - 2$ is irreducible over $\mathbb{Q}$, hence $\min(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$. Consider

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(i, \sqrt[4]{2})$$

and observe that $\mathbb{Q}(i, \sqrt[4]{2})$ is the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Since $x^4 - 2$ has the root $\sqrt[4]{2}$ in $\mathbb{Q}(\sqrt[4]{2})$ but does not split over $\mathbb{Q}(\sqrt[4]{2})$, by Theorem 9.12, $\mathbb{Q}(\sqrt[4]{2})$ is not a splitting field over $\mathbb{Q}$.

Now, consider the situation where E is a splitting field over F, and K is a splitting field over E. It does not necessarily follow that K is a splitting field over F. Consider

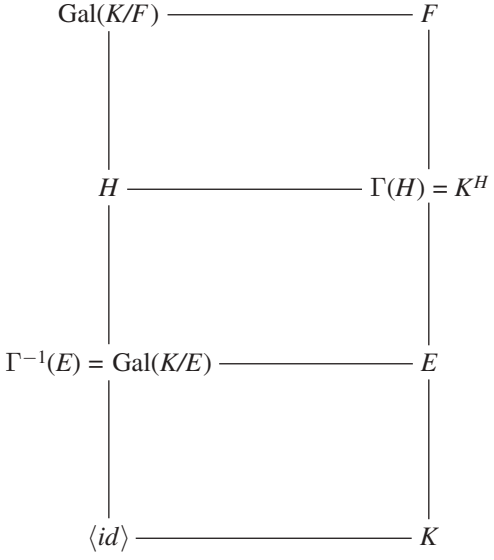
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

and observe that $\mathbb{Q}(\sqrt{2})$ is the splitting field of $\min(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field of $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$. However, as was just demonstrated, $\mathbb{Q}(\sqrt[4]{2})$ is not a splitting field over $\mathbb{Q}$.

Theorem 9.13. If K is a splitting field over F, then Γ is an order-reversing bijection (where "order" is defined in terms of set inclusion). Furthermore, if E is a field between F and K, then $\Gamma^{-1}(E) = \mathrm{Gal}(K/E)$.

Proof. It was demonstrated in Theorem 9.6 that Γ is injective. We have from Theorem 2.27 that K is a splitting field over E. By Theorem 9.12, $K^{\mathrm{Gal}(K/E)} = E$. Thus, $\Gamma(\mathrm{Gal}(K/E)) = E$, so Γ is surjective. Since Γ is bijective, applying Γ^{-1} to $\Gamma(\mathrm{Gal}(K/E)) = E$ yields $\Gamma^{-1}(E) = \mathrm{Gal}(K/E)$. □

The following figure extends the earlier figure of the Galois correspondence, this time depicting Γ as a bijection.



Suppose that K is a finite extension of F but not necessarily a splitting field over F. By Theorem 9.7, K is a splitting field over $K^{\mathrm{Gal}(K/F)}$. It follows from Theorem 9.13 that by restricting the range of Γ to those subfields of K that contain $K^{\mathrm{Gal}(K/F)}$, we create a bijection $\Gamma_|$ between the subgroups of $\mathrm{Gal}(K/F)$

and the fields between $K^{\mathrm{Gal}(K/F)}$ and K. Let E be an arbitrary field between F and K. Then $K^{\mathrm{Gal}(K/F)} \subseteq K^{\mathrm{Gal}(K/E)}$. If K is a splitting field over E, it follows from Theorem 9.12 that $K^{\mathrm{Gal}(K/E)} = E$, hence $K^{\mathrm{Gal}(K/F)} \subseteq E$. Thus, $K^{\mathrm{Gal}(K/F)}$ is the "smallest" field between F and K over which K is a splitting field.

Theorem 9.14. Let K be a finite extension of F, and let H_1 and H_2 be subgroups of $\mathrm{Gal}(K/F)$. Then

$$K^{H_1 \cap H_2} = K^{H_1} K^{H_2}.$$

Proof. By Theorems 9.5(b) and 9.10,

$$\mathrm{Gal}(K/K^{H_1}K^{H_2}) = H_1 \cap H_2. \tag{9.2}$$

According to the above remarks, Γ restricts to a bijection $\Gamma_|$ between the subgroups of $\mathrm{Gal}(K/F)$ and the fields between $K^{\mathrm{Gal}(K/F)}$ and K. Since K^{H_1} and K^{H_2} are fields of this type, so is $K^{H_1}K^{H_2}$. It follows from (9.2) and Theorem 9.13 that

$$\Gamma_|^{-1}(K^{H_1}K^{H_2}) = H_1 \cap H_2$$

hence

$$K^{H_1}K^{H_2} = \Gamma_|(H_1 \cap H_2) = K^{H_1 \cap H_2}.$$

(Observe that although we used Theorem 9.13, K was not required to be a splitting field over F.) □

Theorem 9.15. Let K be a splitting field over F, and let E_1 and E_2 be fields between F and K such that $E_1 \subseteq E_2$. Then

$$[\mathrm{Gal}(K/E_1) : \mathrm{Gal}(K/E_2)] = [E_2 : E_1].$$

Proof. By Theorem 9.13, there are subgroups H_1 and H_2 of $\mathrm{Gal}(K/F)$ such that $E_1 = K^{H_1}$ and $E_2 = K^{H_2}$, hence $H_2 \subseteq H_1$. It follows from Theorems 9.5(b) and 9.11 that

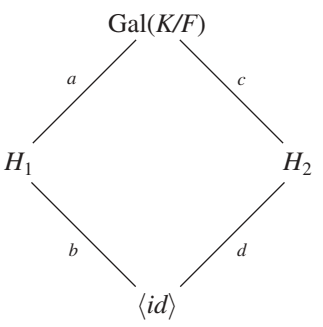
$$[\mathrm{Gal}(K/E_1) : \mathrm{Gal}(K/E_2)] = [H_1 : H_2] = [E_2 : E_1].$$

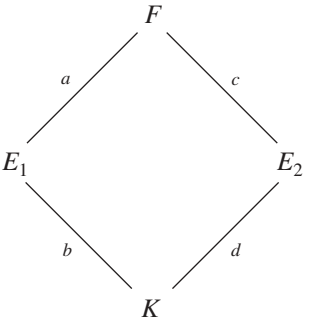
□

Example 9.16. The above two figures of the Galois correspondence are intentionally oversimplified. In practice, subgroups and subfields often present considerably more complex patterns of inclusions. To illustrate, suppose that K is a splitting field over F and that $\mathrm{Gal}(K/F)$ has precisely two proper subgroups, H_1 and H_2, where neither H_1 nor H_2 is a subgroup of the other. The subgroups of $\mathrm{Gal}(K/F)$ and the subfields of K are shown in the following figures, where the interconnecting lines depict inclusions. Thus, H_1 and E_1 correspond via

$$E_1 = K^{H_1} \quad \text{and} \quad H_1 = \mathrm{Gal}(K/E_1)$$

and similarly for E_2 and H_2.





An important feature of these figures is that the indices of subgroups and the degrees of fields have been included. Specifically, the letter on a line joining two groups is the index of the smaller group in the larger, and the letter on a line joining two fields is the degree of the larger field over the smaller. For example, $[\mathrm{Gal}(K/F) : H_1] = a$ and $[H_1 : \langle id \rangle] = b$, and $[E_1 : F] = a$ and $[K : E_1] = b$. The indices and degrees agree because of Theorems 9.11 and 9.15. Example 10.13 gives a concrete illustration of this type of Galois correspondence. ◊

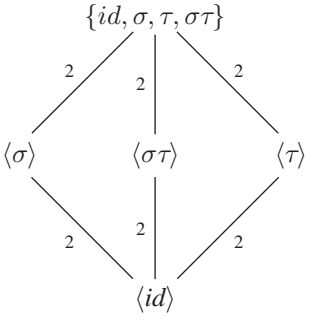
Example 9.17. We continue with Example 9.4. It follows from the definitions of σ and τ that

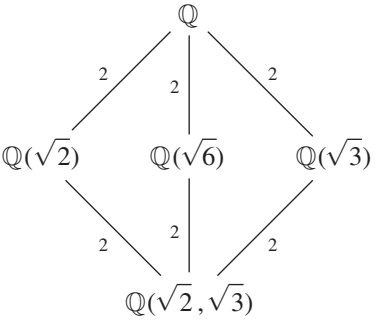
$$\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{2}) \quad \text{hence} \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) = \langle \sigma \rangle$$

and

$$\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \tau \rangle} = \mathbb{Q}(\sqrt{3}) \quad \text{hence} \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})) = \langle \tau \rangle.$$

It is easily shown that $\sigma(\sqrt{6}) = -\sqrt{6} = \tau(\sqrt{6})$. So, we have the following Galois correspondence.





◊

The next result generalizes Theorem 7.18.

Theorem 9.18. Let K be a splitting field over F, let γ be an element of K, and let $id = \sigma_1, \sigma_2, \ldots, \sigma_m$ be left coset representatives of $\mathrm{Gal}(K/F(\gamma))$ in $\mathrm{Gal}(K/F)$. Then

$$\min(\gamma, F) = \prod_{j=1}^{m} [x - \sigma_j(\gamma)]. \tag{9.3}$$

Proof. Let $h(x)$ be the right-hand side of (9.3). Arguing as in Theorem 7.18, and invoking Theorem 9.12, we find that $h(x)$ is a monic polynomial in $F[x]$ that has γ as a root. By Theorem 9.15,

$$\deg(h) = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/F(\gamma))] = [F(\gamma) : F].$$

It follows from Theorem 2.12(b) that $h(x) = \min(\gamma, F)$. □

Let $f(x)$ be a polynomial of degree n in $F[x]$ that has simple roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, and let K be the splitting of $f(x)$ over F. In keeping with the remarks following Theorems 3.3 and 7.5, it will sometimes be convenient to think of $\mathrm{Gal}(K/F)$ as a group of permutations on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ or $\{1, 2, \ldots, n\}$. At times, we will adopt this perspective without additional comment, allowing the context to make the situation clear. Consistent with the definition in Appendix D, we say that $\mathrm{Gal}(K/F)$ is transitive on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ if for every $1 \leq i < j \leq n$ there is σ in $\mathrm{Gal}(K/F)$ such that $\sigma(\alpha_i) = \alpha_j$.

Theorem 9.19. Let $f(x)$ be a polynomial in $F[x]$ with simple roots, and let K be the splitting field of $f(x)$ over F. Then $f(x)$ is irreducible over F if and only if $\mathrm{Gal}(K/F)$, viewed as a group of permutations on the roots of $f(x)$, is transitive.

Proof. ($\Rightarrow$): Let α and β in K be arbitrary roots of $f(x)$. By the Isomorphism Extension Theorem, the identity isomorphism id on F extends (uniquely) to an isomorphism $\tau : F(\alpha) \longrightarrow F(\beta)$ such that $\tau(\alpha) = \beta$. We have from Theorem 2.28 that τ extends in turn to an isomorphism $\sigma : K \longrightarrow K$. Then σ is in $\mathrm{Gal}(K/F)$, and since α and β were arbitrary, $\mathrm{Gal}(K/F)$ is transitive on the roots of $f(x)$.

($\Leftarrow$): Without loss of generality, we may assume that $f(x)$ is monic. Let α in K be a root of $f(x)$, and let $g(x) = \min(\alpha, F)$. Then $g(x)$ divides $f(x)$. By Theorem 9.1, $\sigma(\alpha)$ is a root of $g(x)$ for all σ in $\mathrm{Gal}(K/F)$. Since $\mathrm{Gal}(K/F)$ is transitive, every root of $f(x)$ is root of $g(x)$. The roots of $f(x)$ are simple, so $f(x)$ divides $g(x)$. Since $f(x)$ and $g(x)$ are monic polynomials that divide each other, they are equal. □

In the next theorem, we use Galois theory to provide alternative proofs of earlier results on general polynomials.

Theorem 9.20. In the notation of (7.1)–(7.7), let $f(x)$ be the general polynomial of degree n over the subfield E of F, and let K be the splitting field of $f(x)$ over F. Then:

(a) $f(x)$ is irreducible over F.	[Theorem 7.6]
(b) $[K : F] = n!$.	[Theorem 7.7]
(c) $\mathrm{Gal}(K/F) \cong S_n$.	[Example 8.15]
(d) $K^{S_n} = F$.	[FTSRF]
(e) $\mathrm{disc}(f)$ is in F.	[Theorem 3.15]

The references in square brackets identify earlier proofs of these assertions.

Proof. By Theorem 9.5(a), $[K : K^{S_n}] = |S_n| = n!$, hence

$$[K : F] = [K : K^{S_n}][K^{S_n} : F] \geq n!.$$

It follows from Theorem 2.30 that $[K : F] = n!$ and $[K^{S_n} : F] = 1$, hence $K^{S_n} = F$. This proves (b) and (d). We have from (d) and Theorem 9.5(b) that $\mathrm{Gal}(K/F) \cong S_n$, which proves (c). Since S_n is transitive, (c) and Theorem 9.19 imply that $f(x)$ is irreducible over F. This proves (a). It follows from remarks made in connection with (3.15), definition (3.21), and (d) that $\mathrm{disc}(f)$ is in F, which proves (e). □

Example 9.21. In the notation of Chapter 7, let

$$f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$$

be the general quartic polynomial over $E = \mathbb{Q}(\omega)$, where ω is a primitive cube root of unity. Let t_1, t_2, t_3, t_4 be the roots of $f(x)$, let $F = E(s_1, s_2, s_3, s_4)$ and $K = F(t_1, t_2, t_3, t_4)$, and let

$$\theta_1 = t_1t_2 + t_3t_4.$$

Let

$$D = \{\mathrm{id}, (t_1\ t_2), (t_3\ t_4), (t_1\ t_2)(t_3\ t_4), (t_1\ t_3)(t_2\ t_4), (t_1\ t_4)(t_2\ t_3),\\ (t_1\ t_3\ t_2\ t_4), (t_1\ t_4\ t_2\ t_3)\}$$

and let $\rho = (t_1\ t_2\ t_3)$. With S_4 as displayed in Section 15.3, it can be verified that $\mathrm{Gal}(K/F(\theta_1)) = D$ and that id, ρ, ρ^2 are left coset representatives of D in S_4. Let

$$\theta_2 = \rho(\theta_1) = t_1t_4 + t_2t_3 \quad \text{and} \quad \theta_3 = \rho^2(\theta_1) = t_1t_3 + t_2t_4$$

and let

$$g(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3).$$

By Theorem 9.20(c), $\mathrm{Gal}(K/F) \cong S_4$. It follows from Theorem 9.18 that $g(x) = \min(\theta_1, F)$. Thus, $F(\theta_1, \theta_2, \theta_3)$ is a splitting field over F. In Section 15.3, we show that

$$g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_1^2s_4 - 4s_2s_4 + s_3^2).$$

By Theorems 9.11 and 9.20(d),

$$[K^D : F] = [K^D : K^{S_4}] = [S_4 : D] = 3.$$

Alternatively, it follows from Theorem 9.13 that $K^D = F(\theta_1)$, and from Theorem 2.12(b) that $[F(\theta_1) : F] = 3$, again showing that $[K^D : F] = 3$. ◊

Theorem 9.22. Let K be a splitting field over F, and let E be a field between F and K. Then the following are equivalent:
(a) E is a splitting field over F.
(b) $\sigma(E) = E$ for all σ in $\mathrm{Gal}(K/F)$.
(c) $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$.

In this case, the restriction map

$$\begin{aligned} \iota\colon \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(E/F) \\ \sigma &\longmapsto \sigma_{|E} \end{aligned}$$

gives rise to an isomorphism:

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

Proof. Let $E = F(\psi)$ for some ψ in E.

(a)⇒(b): Take σ in $\mathrm{Gal}(K/F)$, and let $s(x) = \min(\psi, F)$. Since $\sigma(\psi)$ is a root of $s(x)$, and E is a splitting field over F, by Theorem 9.12, $\sigma(\psi)$ is in E. Therefore, $\sigma(E) = F(\sigma(\psi)) \subseteq E$. Replacing σ with σ^{-1}, the same argument shows that $E \subseteq \sigma(E)$. Thus, $E = \sigma(E)$ for all σ in $\mathrm{Gal}(K/F)$.

(b)⇒(c): By Theorem 9.8,

$$\sigma\mathrm{Gal}(K/E)\sigma^{-1} = \mathrm{Gal}(K/\sigma E) = \mathrm{Gal}(K/E).$$

for all σ in $\mathrm{Gal}(K/F)$.

(c) ⇒(a): By Theorem 9.12, $g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)}[x - \sigma(\psi)]$ is a polynomial in $K^{\mathrm{Gal}(K/F)}[x] = F[x]$ that has ψ as a root. For σ in $\mathrm{Gal}(K/F)$, we have from Theorem 9.8 that $\mathrm{Gal}(K/\sigma(E)) = \mathrm{Gal}(K/E)$. By Theorem 9.13, $\sigma(E) = E$. So,

$\sigma(\psi)$ is in E for all σ in $\mathrm{Gal}(K/F)$, hence $g(x)$ splits over E. Thus, E is the splitting field of $g(x)$ over F.

It remains to establish the isomorphism. We have from part (b) that ι is well defined. It is readily verified that ι is a homomorphism and that $\ker(\iota) = \mathrm{Gal}(K/E)$. By Theorem C.3, the proof will be complete if we can demonstrate that ι is surjective. Since $\mathrm{im}(\iota)$ is a subgroup of $\mathrm{Gal}(E/F)$, which is finite, it is sufficient to show that $\mathrm{im}(\iota)$ and $\mathrm{Gal}(E/F)$ have the same order. By Theorems C.3, 9.12, and 9.15, we have

$$|\mathrm{im}(\iota)| = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/E)] = [E : F] = |\mathrm{Gal}(E/F)|.$$

□

Example 9.23. We continue with Example 9.21. Using Theorem D.3, we find that

$$\rho D \rho^{-1} = \{\mathrm{id}, (t_1\ t_4), (t_2\ t_3), (t_1\ t_2)(t_3\ t_4), (t_1\ t_3)(t_2\ t_4), (t_1\ t_4)(t_2\ t_3), \\ (t_1\ t_2\ t_4\ t_3), (t_1\ t_3\ t_4\ t_2)\}$$

and

$$\rho^2 D \rho^{-2} = \{\mathrm{id}, (t_1\ t_3), (t_2\ t_4), (t_1\ t_2)(t_3\ t_4), (t_1\ t_3)(t_2\ t_4), (t_1\ t_4)(t_2\ t_3), \\ (t_1\ t_2\ t_3\ t_4), (t_1\ t_4\ t_3\ t_2)\}$$

hence

$$D \cap \rho D \rho^{-1} \cap \rho^2 D \rho^{-2} = V$$

where

$$V = \{id, (t_1\ t_2)(t_3\ t_4), (t_1\ t_3)(t_2\ t_4), (t_1\ t_4)(t_2\ t_3)\}.$$

Substituting

$$A_4 = V \cup (t_1\ t_2\ t_3)V \cup (t_1\ t_3\ t_2)V \tag{9.4}$$

into

$$S_4 = A_4 \cup (t_1\ t_2)A_4$$

gives

$$S_4 = V \cup (t_1\ t_2)V \cup (t_1\ t_3)V \cup (t_2\ t_3)V \cup (t_1\ t_2\ t_3)V \cup (t_1\ t_3\ t_2)V \tag{9.5}$$

where we note that the union in (9.5) is disjoint. It is readily verified using (9.5) that $V \lhd S_4$ and

$$S_4/V \cong \{id, (t_1\ t_2), (t_1\ t_3), (t_2\ t_3), (t_1\ t_2\ t_3), (t_1\ t_3\ t_2)\} \cong S_3. \tag{9.6}$$

We note in passing that D is not a normal subgroup of S_4 because, for example,

$$(t_2\ t_3)(t_1\ t_2)(t_2\ t_3)^{-1} = (t_1\ t_3)$$

which is not in D.

By Theorem 9.8,

$$\mathrm{Gal}(K/F(\theta_2)) \cong \rho D \rho^{-1} \quad \text{and} \quad \mathrm{Gal}(K/F(\theta_3)) \cong \rho^2 D \rho^{-2}.$$

Since $F(\theta_1, \theta_2, \theta_3) = F(\theta_1)F(\theta_2)F(\theta_3)$, it follows from Theorem 9.10 that

$$\mathrm{Gal}(K/F(\theta_1, \theta_2, \theta_3)) \cong V$$

and then from Theorem 9.13 that

$$K^V = F(\theta_1, \theta_2, \theta_3).$$

Since $V \lhd S_4$, Theorem 9.22 implies that $F(\theta_1, \theta_2, \theta_3)$ is a splitting field over F. This was previously demonstrated in Example 9.21. It follows from (9.6) and Theorem 9.22 that

$$\mathrm{Gal}(F(\theta_1, \theta_2, \theta_3)/F) \cong S_4/V \cong S_3.$$

In order to interpret $\mathrm{Gal}(F(\theta_1, \theta_2, \theta_3)/F)$ as a group of permutations on $\{\theta_1, \theta_2, \theta_3\}$, we need to compute in terms of t_1, t_2, t_3, t_4. The following display shows the relevant calculations where, in the last column, the permutation corresponding to each row is given:

$$\begin{array}{rrrl}
id(\theta_1) = \theta_1 & id(\theta_2) = \theta_2 & id(\theta_3) = \theta_3 & id \\
(t_1\ t_2)(\theta_1) = \theta_3 & (t_1\ t_2)(\theta_2) = \theta_2 & (t_1\ t_2)(\theta_3) = \theta_1 & (\theta_1\ \theta_3) \\
(t_1\ t_3)(\theta_1) = \theta_1 & (t_1\ t_3)(\theta_2) = \theta_3 & (t_1\ t_3)(\theta_3) = \theta_2 & (\theta_2\ \theta_3) \\
(t_2\ t_3)(\theta_1) = \theta_2 & (t_2\ t_3)(\theta_2) = \theta_1 & (t_2\ t_3)(\theta_3) = \theta_3 & (\theta_1\ \theta_2) \\
(t_1\ t_2\ t_3)(\theta_1) = \theta_2 & (t_1\ t_2\ t_3)(\theta_2) = \theta_3 & (t_1\ t_2\ t_3)(\theta_3) = \theta_1 & (\theta_1\ \theta_2\ \theta_3) \\
(t_1\ t_3\ t_2)(\theta_1) = \theta_3 & (t_1\ t_3\ t_2)(\theta_2) = \theta_1 & (t_1\ t_3\ t_2)(\theta_3) = \theta_2 & (\theta_1\ \theta_3\ \theta_2).
\end{array}$$

Thus,

$$\mathrm{Gal}(F(\theta_1, \theta_2, \theta_3)/F) \cong \{id, (\theta_1\ \theta_2), (\theta_1\ \theta_3), (\theta_2\ \theta_3), (\theta_1\ \theta_2\ \theta_3), (\theta_1\ \theta_3\ \theta_2)\} \cong S_3.$$

$\Diamond$

We now consolidate the key results demonstrated above into what will be referred to as the *Fundamental Theorem of Galois Theory* (FTGT). The FTGT will be used repeatedly throughout the remainder of the book.

Theorem 9.24 (Fundamental Theorem of Galois Theory). Let K be a splitting field over F, let H be a subgroup of $\mathrm{Gal}(K/F)$, and let E be a field between F and K. Then:

(a) Γ is an order-reversing bijection.
(b) $\mathrm{Gal}(K/K^H) = H$.
(c) $K^{\mathrm{Gal}(K/E)} = E$.
(d) $|\mathrm{Gal}(K/E)| = [K : E]$.
(e) E is a splitting field over F if and only if $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$. In this case,

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

Proof. See earlier proofs. □

For historical reasons originating with Kronecker, the following result has the unusual title *Theorem on Natural Irrationalities* (TNI). The TNI extends Theorem 4.10 to the setting of Galois theory.

Theorem 9.25 (Theorem on Natural Irrationalities). Let K be a splitting field over F, and let L be a finite extension of F. Then:
(a) KL is a splitting field over L.
(b) The restriction map

$$\begin{aligned} \iota\colon \mathrm{Gal}(KL/L) &\longrightarrow \mathrm{Gal}(K/F) \\ \sigma &\longmapsto \sigma_{|K} \end{aligned}$$

gives rise to an isomorphism:

$$\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L).$$

(c) $[KL : L] = [K : K \cap L]$.
(d) $[KL : F] = \dfrac{[K : F][L : F]}{[K \cap L : F]}$.

Proof. See the figure for Theorem 4.10. The proofs of parts (a), (c), and (d) are the same as those given for the corresponding parts of Theorem 4.10. To prove part (b), let $K = F(\theta)$ for some θ in K, and let $r(x) = \min(\theta, F)$. By Theorem 9.12, K is the splitting field of $r(x)$ over F. Take σ in $\mathrm{Gal}(KL/L)$. Since $\sigma(\theta)$ is a root of $r(x)$, it is in K, hence $\sigma(K) = K$. Therefore, ι is well defined. It is easily verified that ι is a group homomorphism. Take τ in $\ker(\iota)$. Then τ fixes both K and L pointwise, so it fixes KL pointwise, hence $\tau = id$. Therefore, ι is injective. We have from part (a) and the FTGT that

$$\mathrm{Gal}(KL/L) \cong \mathrm{im}(\iota) = \mathrm{Gal}(K/K^{\mathrm{im}(\iota)})$$

and

$$K^{\mathrm{im}(\iota)} = K \cap (KL)^{\mathrm{Gal}(KL/L)} = K \cap L.$$

Therefore,

$$\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L).$$

□

Theorem 9.26. If K_1 and K_2 are splitting fields over F such that $K_1 \cap K_2 = F$, then

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Proof. For $i = 1, 2$, let $K_i = F(\theta_i)$ for some θ_i in K_i, and let $r_i(x) = \min(\theta_i, F)$. Then K_i is the splitting field of $r_i(x)$ over F, so $K_1K_2 = F(\theta_1, \theta_2)$ is the splitting field of $r_1(x)r_2(x)$ over F. Take σ in $\mathrm{Gal}(K_1K_2/F)$. By Theorem 9.22, $\sigma(K_i) = K_i$ for each i, so the map

$$\begin{aligned} \iota\colon \mathrm{Gal}(K_1K_2/F) &\longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ \sigma &\longmapsto (\sigma_{|K_1}, \sigma_{|K_2}) \end{aligned}$$

is well defined. It is easily verified that ι is a group homomorphism. Take τ in $\ker(\iota)$. Then τ fixes both K_1 and K_2 pointwise, so it fixes K_1K_2 pointwise, hence $\tau = id$. Therefore, ι is injective. We have

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{im}(\iota) \subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F). \tag{9.7}$$

It follows from the FTGT that

$$|\mathrm{Gal}(K_1/F)| = [K_1 : F] \qquad |\mathrm{Gal}(K_2/F)| = [K_2 : F] \tag{9.8}$$

and

$$|\mathrm{Gal}(K_1K_2/F)| = [K_1K_2 : F]. \tag{9.9}$$

Since $K_1 \cap K_2 = F$, we have from part (d) of the TNI that

$$[K_1K_2 : F] = [K_1 : F][K_2 : F]. \tag{9.10}$$

Combining (9.8)–(9.10) yields

$$\begin{aligned} |\mathrm{Gal}(K_1K_2/F)| &= |\mathrm{Gal}(K_1/F)|\,|\mathrm{Gal}(K_2/F)| \\ &= |\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)|. \end{aligned} \tag{9.11}$$

Then (9.7) and (9.11) imply that

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

□

We close this chapter with a striking result that is reminiscent of the latter part of Chapter 4. It demonstrates that Galois theory can be a powerful tool for deriving results on polynomials.

Theorem 9.27 (Reciprocity Theorem). Let α and β be algebraic over F, and let

$$f(x) = \min(\alpha, F) \quad \text{and} \quad g(x) = \min(\beta, F).$$

Let

$$f(x) = f_1(x)f_2(x)\cdots f_n(x)$$

be a factorization of $f(x)$ into polynomials in $F(\beta)[x]$ that are irreducible over $F(\beta)$. Similarly, let

$$g(x) = g_1(x)g_2(x)\cdots g_m(x)$$

be a factorization of $g(x)$ into polynomials in $F(\alpha)[x]$ that are irreducible over $F(\alpha)$. Then $n = m$, and renumbering if necessary, we have

$$\frac{\deg(f_i)}{\deg(f)} = \frac{\deg(g_i)}{\deg(g)}$$

for $i = 1, 2, \ldots, n$.

Proof. Let K be the splitting field of $f(x)g(x)$ over F, let E be the splitting field of $f(x)$ over F, and let E_i be the splitting field of $f_i(x)$ over $F(\beta)$ for $i = 1, 2, \ldots, n$. Let

$$\mathcal{A}_i = \{\sigma \in \mathrm{Gal}(K/F) : \sigma(\alpha) \text{ is a root of } f_i(x)\}$$

and let

$$\mathbb{A} = \{\mathcal{A}_i : i = 1, 2, \ldots, n\}.$$

Since $f(x)$ is irreducible over F, by Theorem 9.19, $\mathrm{Gal}(E/F)$ is transitive on the roots of $f(x)$. As K is the splitting field of $f(x)g(x)$ over E, by Theorem 2.28, any automorphism in $\mathrm{Gal}(E/F)$ can be extended to an automorphism in $\mathrm{Gal}(K/F)$. Therefore, $\mathrm{Gal}(K/F)$ is transitive on the roots of $f(x)$. It follows that every root of $f(x)$ is of the form $\sigma(\alpha)$ for some σ in $\mathrm{Gal}(K/F)$, so each $\mathcal{A}_i$ is nonempty. By Theorem 2.18, the roots of $f(x)$ are simple, hence the $\mathcal{A}_i$ are disjoint. This shows that $\mathbb{A}$ is a partition of $\mathrm{Gal}(K/F)$.

Similarly, since $f_i(x)$ is irreducible over $F(\beta)$, $\mathrm{Gal}(E_i/F(\beta))$ is transitive on the roots of $f_i(x)$. As K is the splitting field of $f(x)g(x)$ over E_i, any automorphism in $\mathrm{Gal}(E_i/F(\beta))$ can be extended to an automorphism in $\mathrm{Gal}(K/F(\beta))$. Therefore, $\mathrm{Gal}(K/F(\beta))$ is transitive on the roots of $f_i(x)$ for each i.

Let

$$\mathcal{B}_j = \{\tau \in \mathrm{Gal}(K/F) : \tau(\beta) \text{ is a root of } g_j(x)\}$$

for $j = 1, 2, \ldots, m$, and let

$$\mathbb{B} = \{\mathcal{B}_j : j = 1, 2, \ldots, m\}.$$

Arguing as above, we find that $\mathrm{Gal}(K/F)$ is transitive on the roots of $g(x)$, $\mathrm{Gal}(K/F(\alpha))$ is transitive on the roots of $g_j(x)$ for each j, and $\mathbb{B}$ is a partition of $\mathrm{Gal}(K/F)$.

It is easily verified that the map

$$\begin{aligned} \iota\colon \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(K/F) \\ \sigma &\longmapsto \sigma^{-1} \end{aligned}$$

is a bijection. Therefore, $\iota(\mathbb{A})$ is a partition of $\mathrm{Gal}(K/F)$. We claim that $\iota(\mathbb{A}) = \mathbb{B}$. Since $\mathrm{Gal}(K/F)$ is finite, it is sufficient to show that each $\iota(\mathcal{A}_i)$ is an element of $\mathbb{B}$. Take σ and ρ in $\mathcal{A}_i$. Then σ^{-1} is in $\mathcal{B}_{(i)}$ for some $1 \le (i) \le m$. Since $\sigma(\alpha)$ and $\rho(\alpha)$ are both roots of $f_i(x)$, and since $\mathrm{Gal}(K/F(\beta))$ is transitive on the roots of $f_i(x)$, there is ν in $\mathrm{Gal}(K/F(\beta))$ such that $\nu(\sigma(\alpha)) = \rho(\alpha)$. Then $\rho^{-1}\nu\sigma$ is in $\mathrm{Gal}(K/F(\alpha))$, hence $\rho^{-1}\nu\sigma$ permutes the roots of $g_{(i)}(x)$ among themselves. Since $\sigma^{-1}(\beta)$ is a root of $g_{(i)}(x)$, so is

$$\rho^{-1}\nu\sigma(\sigma^{-1}(\beta)) = \rho^{-1}(\beta).$$

Thus, ρ^{-1} is in $\mathcal{B}_{(i)}$, and it follows that $\iota(\mathcal{A}_i) \subseteq \mathcal{B}_{(i)}$. An analogous argument starting with ι^{-1} shows that $\iota^{-1}(\mathcal{B}_{(i)}) \subseteq \mathcal{A}_{((i))}$ for some $1 \le ((i)) \le n$, so $\mathcal{A}_i \subseteq \iota^{-1}(\mathcal{B}_{(i)}) \subseteq \mathcal{A}_{((i))}$. Since $\mathbb{A}$ is a partition of $\mathrm{Gal}(K/F)$, we have $((i)) = i$, hence $\iota(\mathcal{A}_i) = \mathcal{B}_{(i)}$. This proves the claim. It follows that $n = m$. Renumbering the $\mathcal{B}_j$ and $g_j(x)$ if necessary, we now write $\mathcal{B}_i$ in place of $\mathcal{B}_{(i)}$, and $g_i(x)$ in place of $g_{(i)}(x)$ for $i = 1, 2, \ldots, n$. Accordingly, $\iota(\mathcal{A}_i) = \mathcal{B}_i$, hence $|\mathcal{A}_i| = |\mathcal{B}_i|$ for each i.

With σ in $\mathcal{A}_i$, it is readily demonstrated that the (left) coset $\sigma\mathrm{Gal}(K/F(\alpha))$ of $\mathrm{Gal}(K/F(\alpha))$ in $\mathrm{Gal}(K/F)$ is the set of elements in $\mathrm{Gal}(K/F)$ that map α to $\sigma(\alpha)$. Since the cosets of $\mathrm{Gal}(K/F(\alpha))$ in $\mathrm{Gal}(K/F)$ are disjoint, and since $\mathrm{Gal}(K/F)$ is transitive on the roots of $f(x)$, $\mathcal{A}_i$ is the disjoint union of such cosets, one for each root of $f_i(x)$. The cosets all have the same number of elements, so

$$|\mathcal{A}_i| = \deg(f_i)\,|\mathrm{Gal}(K/F(\alpha))|.$$

By Theorem 2.12(b) and the FTGT,

$$|\mathrm{Gal}(K/F(\alpha))| = [K : F(\alpha)] = \frac{[K : F]}{[F(\alpha) : F]} = \frac{[K : F]}{\deg(f)}.$$

Therefore,

$$|\mathcal{A}_i| = \frac{\deg(f_i)\,[K : F]}{\deg(f)}.$$

Similarly,

$$|\mathcal{B}_i| = \frac{\deg(g_i)\,[K : F]}{\deg(g)}.$$

Then $|\mathcal{A}_i| = |\mathcal{B}_i|$ implies that

$$\frac{\deg(f_i)}{\deg(f)} = \frac{\deg(g_i)}{\deg(g)}$$

for $i = 1, 2, \ldots, n$. □

CHAPTER 10

CYCLIC EXTENSIONS AND CYCLOTOMIC FIELDS

In this chapter, we continue the discussion of binomial polynomials and cyclotomic fields that comprised much of Chapters 5 and 6. This time, however, we develop our ideas using Galois theory.

10.1 CYCLIC EXTENSIONS

We say that a field K is a *cyclic extension* of F if it is a splitting field over F and $\mathrm{Gal}(K/F)$ is cyclic. In this case,

$$\mathrm{Gal}(K/F) = \langle \sigma \rangle = \{\sigma^i : i = 0, 1, \ldots, n-1\}$$

for some σ in $\mathrm{Gal}(K/F)$, where $\sigma^0 = id$ and $n = \mathrm{ord}(\sigma)$. Suppose that F contains an nth root of unity ζ, and let α be an arbitrary element of K. The *Lagrange resolvent* corresponding to ζ and α is defined to be

$$(\zeta, \alpha) = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\alpha) = \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha). \tag{10.1}$$

Evidently, (ζ, α) is in K. With $\mathrm{Gal}(\Phi_p/\mathbb{Q})$ as in Example 8.16, we now see that λ as defined in (6.9) is the Lagrange resolvent (ξ, ζ).

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Theorem 10.1. Let K be a cyclic extension of F of degree n, let $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, and suppose that F contains an nth root of unity ζ. Then, for all α in K:
(a) $\sigma^i((\zeta,\alpha)) = \zeta^{-i}(\zeta,\alpha)$ for $i = 0, 1, 2, \ldots, n-1$.
(b) $(\zeta,\alpha)^n$ is in F.
(c) $(1,\alpha)$ is in F.

Proof. (a): Since $\sigma^n = id$, we have

$$\begin{aligned}\sigma((\zeta,\alpha)) &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha) + \zeta^{n-1}\alpha \\ &= \zeta^{-1}(\zeta,\alpha).\end{aligned}$$

Then

$$\sigma^2((\zeta,\alpha)) = \zeta^{-1}\sigma((\zeta,\alpha)) = \zeta^{-2}(\zeta,\alpha)$$

and so on.

(b): By part (a),

$$\sigma^i((\zeta,\alpha)^n) = [\sigma^i(\zeta,\alpha)]^n = \zeta^{-ni}(\zeta,\alpha)^n = (\zeta,\alpha)^n$$

for each i. It follows from the FTGT that $(\zeta,\alpha)^n$ is in $K^{\mathrm{Gal}(K/F)} = F$.

(c): Since 1 is an nth root of unity, we have from part (a) that $\sigma^i((1,\alpha)) = (1,\alpha)$ for each i. The argument in part (b) shows that $(1,\alpha)$ is in F. □

Theorem 10.2. Continuing with the assumptions of Theorem 10.1, suppose that ζ is a primitive nth root of unity. Then, for all α in K:
(a) $\alpha = \dfrac{1}{n}\displaystyle\sum_{i=0}^{n-1}(\zeta^i,\alpha)$.
(b) If $(\zeta,\alpha) \neq 0$, then $K = F((\zeta,\alpha))$.

Proof. (a): Consider

$$\sum_{i=0}^{n-1}(\zeta^i,\alpha) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(\zeta^i)^j\sigma^j(\alpha) = \sum_{j=0}^{n-1}\sigma^j(\alpha)\sum_{i=0}^{n-1}(\zeta^j)^i.$$

Since ζ is an nth root of unity, ζ^j is a root of

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

for $j = 0, 1, \ldots, n-1$. Furthermore, since ζ is a primitive nth root of unity, $\zeta^j = 1$ if and only if $j = 0$. Therefore,

$$\sum_{i=0}^{n-1}(\zeta^j)^i = \begin{cases} n & \text{if } j = 0 \\ 0 & \text{if } 1 \le j \le n-1 \end{cases}$$

hence $\sum_{i=0}^{n-1}(\zeta^i,\alpha) = n\alpha$.

(b): Let $\lambda = (\zeta, \alpha)$, and suppose that $\sigma^i(\lambda) = \lambda$ for some $0 \le i \le n-1$. By Theorem 10.1(a), $\zeta^{-i}\lambda = \lambda$. Then $\lambda(\zeta^i - 1) = 0$ and $\lambda \neq 0$ imply that $\zeta^i = 1$. Since ζ is a primitive nth root of unity, $i = 0$. Therefore, $\mathrm{Gal}(K/F(\lambda)) = \langle id \rangle$, and by the FTGT, $K = F(\lambda)$.

An alternative, more constructive proof that $K = F(\lambda)$ is available. Let $\lambda_i = (\zeta^i, \alpha)$ and $c_i = \lambda_i / n\lambda^i$ for $i = 0, 1, \ldots, n-1$, where we note that $\lambda = \lambda_1$. Then

$$\sigma\left(\frac{\lambda_i}{\lambda^i}\right) = \frac{\sigma(\lambda_i)}{[\sigma(\lambda)]^i} = \frac{\zeta^{-i}\lambda_i}{[\zeta^{-1}\lambda]^i} = \frac{\lambda_i}{\lambda^i}.$$

By the FTGT, c_i is in F for each i. It follows from part (a) that α can be expressed as

$$\alpha = c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_{n-1}\lambda^{n-1}.$$

Thus, $\{1, \lambda, \lambda^2, \ldots, \lambda^{n-1}\}$ spans K over F. In fact, since $[K : F] = n$, it is a basis for K over F. □

Example 10.3. We continue with Examples 9.21 and 9.23. Recall that $f(x)$ is the general quartic polynomial over $E = \mathbb{Q}(\omega)$ with roots t_1, t_2, t_3, t_4, where ω is a primitive cube root of unity. Also recall that $F = E(s_1, s_2, s_3, s_4)$ and

$$\begin{aligned} \theta_1 &= t_1t_2 + t_3t_4 \\ \theta_2 &= t_1t_4 + t_2t_3 \\ \theta_3 &= t_1t_3 + t_2t_4. \end{aligned}$$

We showed in Example 9.21 that

$$g(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

is in $F[x]$. Consistent with (3.14), let

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_1 - t_4)(t_2 - t_3)(t_2 - t_4)(t_3 - t_4).$$

In Section 15.3, we show that

$$\Delta = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3).$$

Evidently, $F(\Delta, \theta_1) \subseteq F(\theta_1, \theta_2, \theta_3)$. Since $g(x)$ and $x - \theta_1$ are in $F(\theta_1)[x]$, so is

$$h(x) = \frac{g(x)}{x - \theta_1} = (x - \theta_2)(x - \theta_3) = x^2 - (\theta_2 + \theta_3)x + \theta_2\theta_3.$$

Then $\theta_2 + \theta_3$ and $\Delta / h(\theta_1) = \theta_2 - \theta_3$ are in $F(\theta_1, \Delta)$, and therefore, so are θ_2 and θ_3. Thus, $F(\theta_1, \theta_2, \theta_3) \subseteq F(\Delta, \theta_1)$, hence $F(\theta_1, \theta_2, \theta_3) = F(\Delta, \theta_1)$.

It follows from remarks made subsequent to (7.13) that $[F(\Delta) : F] = 2$. We have from Example 9.21 that $F(\theta_1, \theta_2, \theta_3)$ is a splitting field over F, and from Example 9.23 that $\mathrm{Gal}(F(\theta_1, \theta_2, \theta_3)/F) \cong S_3$. By the FTGT,

$$[F(\Delta, \theta_1) : F] = [F(\theta_1, \theta_2, \theta_3) : F] = |\mathrm{Gal}(F(\theta_1, \theta_2, \theta_3)/F)| = |S_3| = 6$$

hence

$$|\mathrm{Gal}(F(\Delta, \theta_1)/F(\Delta))| = [F(\Delta, \theta_1) : F(\Delta)] = \frac{[F(\Delta, \theta_1) : F]}{[F(\Delta) : F]} = 3.$$

By Theorem B.1(c), $\mathrm{Gal}(F(\Delta, \theta_1)/F(\Delta))$ is cyclic. It follows from Theorem D.2 that $\mathrm{Gal}(F(\Delta, \theta_1)/F(\Delta))$ contains, hence is generated by, a 3-cycle. Any automorphism in $\mathrm{Gal}(F(\Delta, \theta_1)/F(\Delta))$ is completely determined by its values at t_1, t_2, t_3, t_4. Renumbering t_1, t_2, t_3, t_4 if necessary, we may assume that the 3-cycle is $\rho = (t_1\ t_2\ t_3)$. Thus, $\mathrm{Gal}(F(\Delta, \theta_1)/F(\Delta)) = \langle \rho \rangle$. Let

$$\begin{aligned} \psi_1 &= (\omega, \theta_1) = \theta_1 + \omega\rho(\theta_1) + \omega^2\rho^2(\theta_1) \\ &= \theta_1 + \omega\theta_2 + \omega^2\theta_3. \end{aligned}$$

Since t_1, t_2, t_3, t_4 are the roots of the general quartic polynomial over E, they are algebraically independent over E, hence $\psi_1 \neq 0$. It follows from Theorem 10.2(b) that

$$F(\theta_1, \theta_2, \theta_3) = F(\Delta, \theta_1) = F(\Delta, \psi_1)$$

and from Theorem 10.1(b) that ψ_1^3 is in $F(\Delta)$. Specifically, we show in Section 15.3 that

$$\psi_1^3 = \frac{27s_1^2s_4 - 9s_1s_2s_3 + 2s_2^3 - 72s_2s_4 + 27s_3^2 + 3i\sqrt{3}\Delta}{2}$$

where we note that $i\sqrt{3} = \omega - \omega^2$ is in F. ◊

Let F be a field, let $h(x)$ be a binomial polynomial of degree n in $F[x]$ that is irreducible over F, and suppose that F contains a primitive nth root of unity. We saw in Example 8.17 that $\mathrm{Gal}(h/F)$, the classical Galois group of $h(x)$ over F, is cyclic of order n. In Theorems 10.4–10.7, we examine in greater detail the important connection between cyclic extensions of a field and irreducible binomial extensions of that field.

Before proceeding, a remark on notation is in order. Let ζ be a primitive nth root of unity, and consider the element (equivalence class) $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$, where $0 \leq a \leq n - 1$. According to the convention established in connection with (5.7), $a + n\mathbb{Z}$ is denoted simply by a. Since $\zeta^{a+kn} = \zeta^a$ for all k in $\mathbb{Z}$, the notation ζ^a is unambiguous. It will be used throughout the rest of the book.

Theorem 10.4. Let $F(\beta)$ be an extension of F of degree m, where $\beta \neq 0$ and β^n is in F for some natural number n. Suppose that F contains a primitive nth root of unity. Then:
(a) $F(\beta)$ is a cyclic extension of F.
(b) m divides n.
(c) β^m is in F, and m is the smallest natural number with this property.
(d) $x^n - \beta^n$ is irreducible over F if and only if $n = m$.

Proof. (a): Let $h(x) = x^n - \beta^n$, and let ζ be a primitive nth root of unity in F. The roots of $h(x)$ are $\zeta^i\beta$ for $i = 0, 1, \ldots, n-1$, so $F(\beta)$ is the splitting field of $h(x)$ over F. We need to show that $\mathrm{Gal}(F(\beta)/F)$ is cyclic. Take σ in $\mathrm{Gal}(F(\beta)/F)$. Since $\sigma(\beta)$ is a root of $h(x)$, $\sigma(\beta) = \zeta^{\iota(\sigma)}\beta$ for some $0 \leq \iota(\sigma) \leq n-1$. This defines a map

$$\begin{aligned} \iota\colon \mathrm{Gal}(F(\beta)/F) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^+ \\ \sigma &\longmapsto \iota(\sigma) \end{aligned}$$

where $(\mathbb{Z}/n\mathbb{Z})^+$ denotes the additive group of the ring $\mathbb{Z}/n\mathbb{Z}$. For τ in $\mathrm{Gal}(F(\beta)/F)$, we have

$$(\sigma\tau)(\beta) = \sigma(\zeta^{\iota(\tau)}\beta) = \zeta^{\iota(\tau)}\sigma(\beta) = \zeta^{\iota(\tau)}\zeta^{\iota(\sigma)}\beta = \zeta^{\iota(\sigma)+\iota(\tau)}\beta.$$

Thus, $\iota(\sigma\tau) = \iota(\sigma) + \iota(\tau)$, so ι is a homomorphism. If $\iota(\sigma) = 0$, then $\sigma = id$, hence ι is injective. Since $\mathrm{Gal}(F(\beta)/F)$ is isomorphic to a subgroup of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^+$, it follows from Theorem B.5 that $\mathrm{Gal}(F(\beta)/F)$ is cyclic.

(b): By the FTGT,

$$|\mathrm{Gal}(F(\beta)/F)| = [F(\beta) : F] = m.$$

Since $\mathrm{Gal}(F(\beta)/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^+$, a group of order n, by Theorem A.1, m divides n.

(c): Let $\mathrm{Gal}(F(\beta)/F) = \langle\sigma\rangle$ for some σ in $\mathrm{Gal}(F(\beta)/F)$. With ι as above, let $\xi = \zeta^{\iota(\sigma)}$. Then $\sigma(\beta) = \xi\beta$, $\sigma^2(\beta) = \xi^2\beta$, and so on. Since $\mathrm{ord}(\sigma) = m$, we have $\beta = \sigma^m(\beta) = \xi^m\beta$. Then $\beta \neq 0$ implies that ξ is an mth root of unity. In fact, ξ is a primitive mth root of unity, otherwise $\mathrm{ord}(\sigma) < m$. It follows from

$$\sigma(\beta^m) = [\sigma(\beta)]^m = (\xi\beta)^m = \beta^m$$

that $\mathrm{Gal}(F(\beta)/F)$ fixes β^m. By the FTGT, β^m is in $K^{\mathrm{Gal}(F(\beta)/F)} = F$. This proves the first assertion. To prove the second assertion, let k be a natural number such that β^k is in F. Then

$$\beta^k = \sigma(\beta^k) = [\sigma(\beta)]^k = \xi^k\beta^k$$

hence $\xi^k = 1$. Viewing ξ as an element of μ_m, it follows from Theorem B.2 that $m = \mathrm{ord}(\xi)$ divides k.

(d): By Theorem 2.12(b), $h(x)$ is irreducible over F if and only if

$$n = \deg(h) = [F(\beta) : F] = m.$$

□

Theorem 10.5. Let K be a cyclic extension of F of degree n, let $K = F(\theta)$ for some θ in K, and suppose that F contains a primitive nth root of unity ζ. Then there is $1 \leq k \leq n-1$ such that $K = F(\beta)$, β^n is in F, and $x^n - \beta^n$ is irreducible over F, where $\beta = (\zeta, \theta^k)$. Therefore, K is an irreducible binomial extension of F.

Proof. The result is trivial for $n = 1$. Suppose that $n > 1$. By the FTGT,

$$|\mathrm{Gal}(K/F)| = [K : F] = n$$

so $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ for some σ in $\mathrm{Gal}(K/F)$, where $\mathrm{ord}(\sigma) = n$. We claim that $(\zeta, \theta^k) \neq 0$ for some $1 \leq k \leq n-1$. Suppose, for a contradiction, that

$$\begin{aligned}(\zeta, \theta^i) &= \theta^i + \zeta\sigma(\theta^i) + \zeta^2\sigma^2(\theta^i) + \cdots + \zeta^{n-1}\sigma^{n-1}(\theta^i) \\ &= \theta^i + \zeta[\sigma(\theta)]^i + \zeta^2[\sigma^2(\theta)]^i + \cdots + \zeta^{n-1}[\sigma^{n-1}(\theta)]^i \\ &= 0\end{aligned}$$

for $i = 1, 2, \ldots, n-1$. Since

$$(\zeta, 1) = 1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \frac{\zeta^n - 1}{\zeta - 1} = 0$$

we have a system of n equations

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \theta & \sigma(\theta) & \sigma^2(\theta) & \cdots & \sigma^{n-1}(\theta) \\ \theta^2 & [\sigma(\theta)]^2 & [\sigma^2(\theta)]^2 & \cdots & [\sigma^{n-1}(\theta)]^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & [\sigma(\theta)]^{n-1} & [\sigma^2(\theta)]^{n-1} & \cdots & [\sigma^{n-1}(\theta)]^{n-1} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

that has the nonzero solution $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$. Therefore, the determinant of the above $n \times n$ matrix equals 0. By Theorem 3.10, this is possible only if $\sigma^i(\theta) = \sigma^j(\theta)$ for some $0 \leq i < j \leq n-1$. Since each element of $\mathrm{Gal}(K/F)$ is completely determined by its value at θ, and since $\mathrm{Gal}(K/F)$ is of order n, no such i and j exist. This contradiction shows that there is $1 \leq k \leq n-1$ such that $(\zeta, \theta^k) \neq 0$. Let $\beta = (\zeta, \theta^k)$. It follows from Theorems 10.1(b), 10.2(b), and 10.4(d) that $K = F(\beta)$, β^n is in F, and $x^n - \beta^n$ is irreducible over F. □

When the cyclic extension of Theorem 10.5 is of prime degree, there is an alternative construction.

Theorem 10.6. Let K be a cyclic extension of F of prime degree p, let θ be an arbitrary element in $K\backslash F$, and suppose that F contains a primitive pth root of unity ζ. Then there is $1 \leq l \leq p-1$ such that $K = F(\gamma)$, γ^p is in F, and $x^p - \gamma^p$ is irreducible over F, where $\gamma = (\zeta^l, \theta)$. Therefore, K is an irreducible binomial extension of F.

Proof. By Theorem 2.15, $K = F(\theta)$. Let

$$E = F((1,\theta),(\zeta,\theta),(\zeta^2,\theta)\ldots,(\zeta^{p-1},\theta)).$$

Evidently, $E \subseteq F(\theta)$, and we have from Theorem 10.2(a) that $F(\theta) \subseteq E$. Therefore, $E = K$. By Theorem 10.1(c), $(1,\theta)$ is in F, so there is $1 \leq l \leq p-1$ such that (ζ^l,θ) is in $K\backslash F$, otherwise $K = F$. Then ζ^l is a primitive pth root of unity. Let $\gamma = (\zeta^l,\theta)$. It follows from Theorems 10.1(b), 10.2(b), and 10.4(d) that $K = F(\gamma)$, γ^p is in F, and $x^p - \gamma^p$ is irreducible over F. □

The next result is central to discussions about solvability of polynomials by radicals. It says that when a field contains certain roots of unity, cyclic extensions of that field and irreducible binomial extensions of that field are the same thing.

Theorem 10.7. Let K be an extension of F of degree n, and suppose that F contains a primitive nth root of unity. Then K is a cyclic extension of F if and only if K is an irreducible binomial extension of F. In this case, there is an element β in K such that $K = F(\beta)$, β^n is in F, and $x^n - \beta^n$ is irreducible over F.

Proof. The result is trivial for $n = 1$. Suppose that $n > 1$.

($\Rightarrow$): This follows immediately from Theorem 10.5.

($\Leftarrow$): Let $K = F(\gamma)$, where γ^m is in F, and $g(x) = x^m - \gamma^m$ is irreducible over F for some m. By Theorem 2.12(b),

$$m = \deg(g) = [F(\gamma) : F] = n.$$

The result now follows from Theorem 10.4(a). □

It would be easy to come away from Theorem 10.7 with the impression that only binomial polynomials give rise to cyclic extensions. However, with the next result, we are able to show that such intuition is misleading.

Theorem 10.8. Let $f(x)$ be a cubic polynomial in $F[x]$ that is irreducible over F, and let K be the splitting field of $f(x)$ over F. If $\mathrm{disc}(f)$ is the square of an element of F, then $\mathrm{Gal}(K/F) \cong A_3$, which is a cyclic group of order 3.

Proof. Let us denote the (simple) roots of $f(x)$ by $\alpha_1, \alpha_2, \alpha_3$, and let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

An argument similar to that used in Theorem 6.21 and Example 10.3 shows that

$$K = F(\alpha_1, \alpha_2, \alpha_3) = F(\delta, \alpha_1).$$

Since $\operatorname{disc}(f) = \delta^2$ and $\operatorname{disc}(f)$ is the square of an element of F, it follows that δ is in F, hence $K = F(\alpha_1)$. By Theorem 2.12(b) and the FTGT,

$$|\operatorname{Gal}(K/F)| = [F(\alpha_1) : F] = 3.$$

Since $A_3 = \langle(\alpha_1\ \alpha_2\ \alpha_3)\rangle$ is the only subgroup of S_3 of order 3 (Section 15.2), we have $\operatorname{Gal}(K/F) \cong A_3$. □

Example 10.9 (7th root of unity). It is possible to solve $\Phi_7(x)$ by radicals over $\mathbb{Q}$ using an approach similar to that presented for $\Phi_5(x)$ in Example 6.6. Here we are interested only in a certain polynomial that arises in the initial steps. We return to $\Phi_7(x)$ in Example 13.13, where it is solved by radicals over $\mathbb{Q}$ using yet another method. Consider

$$\begin{aligned}\frac{\Phi_7(z)}{z^3} &= \frac{(z^6+1)+(z^5+z)+(z^4+z^2)+z^3}{z^3} \\ &= \left(z^3+\frac{1}{z^3}\right)+\left(z^2+\frac{1}{z^2}\right)+\left(z+\frac{1}{z}\right)+1 \qquad (10.2)\end{aligned}$$

and note that

$$\left(z+\frac{1}{z}\right)^2 = \left(z^2+\frac{1}{z^2}\right)+2$$

and

$$\left(z+\frac{1}{z}\right)^3 = \left(z^3+\frac{1}{z^3}\right)+3\left(z+\frac{1}{z}\right).$$

Substituting $x = z + z^{-1}$ into the right-hand side of (10.2) gives

$$f(x) = x^3 + x^2 - 2x - 1. \qquad (10.3)$$

The corresponding reduced polynomial is

$$g(y) = y^3 - \left(\frac{7}{3}\right)y - \frac{7}{27} = \frac{(3y)^3 - 21(3y) - 7}{27}.$$

Let $h(x) = x^3 - 21x - 7$. It follows from Eisenstein's criterion with $p = 7$ that $h(x)$ is irreducible over $\mathbb{Q}$. Let K be the splitting field of $h(x)$ over $\mathbb{Q}$. Using (3.22), we find that $\text{disc}(h) = 3^6 7^2$. By Theorem 10.8, $\text{Gal}(K/\mathbb{Q})$ is cyclic, but $h(x)$ is evidently not binomial. ◊

10.2 CYCLOTOMIC FIELDS

We now use the findings of the previous section to establish some results on the Galois theory of cyclotomic fields. Let ζ be a primitive nth root of unity, and take a in $(\mathbb{Z}/n\mathbb{Z})^\times$. It follows from (5.4) and (5.8) that ζ^a is also a primitive nth root of unity. Thus, ζ and ζ^a are roots of $\Phi_n(x)$. Since $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, by the Isomorphism Extension Theorem, there is a unique isomorphism σ_a in $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ that maps ζ to ζ^a.

Theorem 10.10. For all natural numbers n, the map

$$\begin{aligned} \iota\colon (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \\ a &\longmapsto \sigma_a \end{aligned}$$

is an isomorphism. Therefore, $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ is an Abelian group of order $\varphi(n)$.

Proof. Let ζ be a primitive nth root of unity, and take a and b in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then

$$(\sigma_a\sigma_b)(\zeta) = \sigma_a(\sigma_b(\zeta)) = \sigma_a(\zeta^b) = [\sigma_a(\zeta)]^b = (\zeta^a)^b = \zeta^{ab} = \sigma_{ab}(\zeta).$$

Since σ_a, σ_b, and σ_{ab} are completely determined by their values at ζ, it follows that $\iota(ab) = \iota(a)\iota(b)$, hence ι is a group homomorphism. Suppose that $\iota(a) = id$. Then $\zeta^{a-1} = 1$, and since ζ is a primitive nth root of unity, (5.8) implies that $a = 1$, hence ι is injective. Therefore, $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to a subgroup of $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. According to Theorem 5.4(b) and (5.8), $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ both have order $\varphi(n)$, thus ι is an isomorphism. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is Abelian, so is $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. □

Theorem 10.11. If m and n are relatively prime natural numbers, then

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\mu_{mn})/\mathbb{Q}) &\cong \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \\ &\cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

Proof. This follows from parts (a) and (b) of Theorem 5.5, and Theorems 9.26 and 10.10. □

Theorem 10.12. For p a prime, $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is cyclic of order $p - 1$ with $\varphi(p - 1)$ generators. The isomorphism of Theorem 10.10 establishes a bijection

between the primitive congruence roots modulo p in $\mathbb{F}_p^\times$ and the generators of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ such that $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \langle \sigma_g \rangle$, where g is any primitive congruence root modulo p.

Proof. We have from Theorem 10.10 that $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times$, and from Theorem E.4 that $\mathbb{F}_p^\times$ is cyclic of order $p-1$ with $\varphi(p-1)$ generators. The second assertion follows from the observation that the primitive congruence roots modulo p are precisely the generators of $\mathbb{F}_p^\times$. □

Let p be a prime, let ζ be a primitive pth root of unity, and let g be a primitive congruence root modulo p. By Theorem 10.12, σ_g is a generator of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. Since $\sigma_g(\zeta) = \zeta^g$, we have

$$\sigma_g^2(\zeta) = \sigma_g(\sigma_g(\zeta)) = \sigma_g(\zeta^g) = [\sigma_g(\zeta)]^g = \zeta^{g^2}$$

and in general,

$$\sigma_g^i(\zeta) = \zeta^{g^i} \tag{10.4}$$

for $i = 0, 1, \ldots, p-2$.

Example 10.13 (11th root of unity). By Theorem 10.12, $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$ is cyclic of order 10. The primitive congruence roots modulo 11 are 2, 6, 7, and 8. Taking $g = 2$, we have

i	0	1	2	3	4	5	6	7	8	9
$2^i \pmod{11}$	1	2	4	8	5	10	9	7	3	6

Then $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) = \langle \sigma \rangle$, where $\sigma(\zeta_{11}) = \zeta_{11}^2$. By Theorem B.7(b), $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$ has precisely one subgroup of order 5, namely, $\langle \sigma^2 \rangle$, and one subgroup of order 2, namely, $\langle \sigma^5 \rangle$. It follows from the FTGT that there is precisely one subfield of $\mathbb{Q}(\zeta_{11})$ of degree 2 over $\mathbb{Q}$, and one subfield of $\mathbb{Q}(\zeta_{11})$ of degree 5 over $\mathbb{Q}$. Corresponding to $\langle \sigma^2 \rangle$ and $\langle \sigma^5 \rangle$, consider the sums

$$\begin{aligned} \langle 5, 1 \rangle &= \zeta_{11} + \sigma^2(\zeta_{11}) + \sigma^4(\zeta_{11}) + \sigma^6(\zeta_{11}) + \sigma^8(\zeta_{11}) \\ &= \zeta_{11} + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9 + \zeta_{11}^3 \end{aligned}$$

and

$$\langle 2, 1 \rangle = \zeta_{11} + \sigma^5(\zeta_{11}) = \zeta_{11} + \zeta_{11}^{10}$$

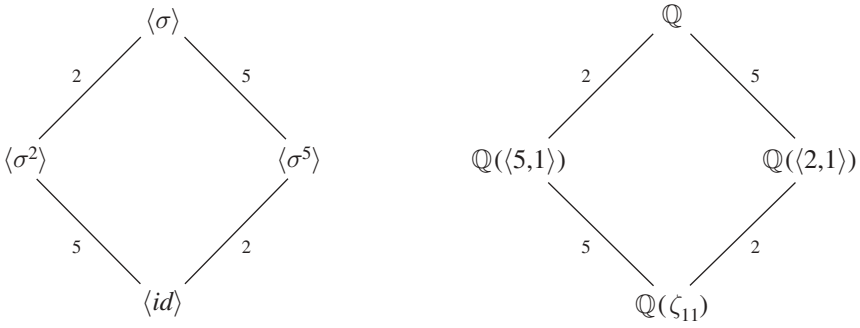
respectively. The angle bracket notation will be explained in Chapter 13. It follows from discussions there that $\mathbb{Q}(\langle 5,1\rangle)$ and $\mathbb{Q}(\langle 2,1\rangle)$ are the subfields of $\mathbb{Q}(\zeta_{11})$ we seek and that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\langle 5,1\rangle) = \langle \sigma^2 \rangle \quad \text{hence} \quad \mathbb{Q}(\zeta_{11})^{\langle \sigma^2 \rangle} = \mathbb{Q}(\langle 5,1\rangle)$$

and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\langle 2,1\rangle) = \langle \sigma^5 \rangle \quad \text{hence} \quad \mathbb{Q}(\zeta_{11})^{\langle \sigma^5 \rangle} = \mathbb{Q}(\langle 2,1\rangle).$$

The Galois correspondence is shown in the following figure.



The reader may wish to refer to Example 9.16, where a general overview of this type of Galois correspondence is provided. ♢

As we show next, forming the compositum with a cyclotomic field produces a field that has properties not unlike those of the original cyclotomic field.

Theorem 10.14. Let F be a field, and let n be a natural number. Then:
(a) $F(\mu_n)$ is the splitting field of $\Phi_n(x)$ over F.
(b) $\mathrm{Gal}(F(\mu_n)/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$.
(c) $[F(\mu_n) : F]$ divides $\varphi(n)$.
(d) If n is prime, then $\mathrm{Gal}(F(\mu_n)/F)$ is cyclic.
(e) If $\Phi_n(x)$ is irreducible over F, then

$$\mathrm{Gal}(F(\mu_n)/F) \cong \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \quad \text{and} \quad [F(\mu_n) : F] = \varphi(n).$$

Proof. (a): Obvious.

(b): Since $\mathbb{Q}(\mu_n)$ is a splitting field over $\mathbb{Q}$, and $F(\mu_n) = F\mathbb{Q}(\mu_n)$, by the TNI,

$$\mathrm{Gal}(F(\mu_n)/F) \cong \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_n) \cap F) \subseteq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}).$$

(c): Since $F(\mu_n)$ is a splitting field over F, by the FTGT,

$$|\mathrm{Gal}(F(\mu_n)/F)| = [F(\mu_n) : F]. \tag{10.5}$$

We have from Theorem 10.10 that

$$|\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})| = \varphi(n). \tag{10.6}$$

The result now follows from part (b) and Theorem A.1.

(d): By Theorem 10.12, $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ is cyclic. The result now follows from part (b) and Theorem B.5.

(e): Let ζ be a primitive nth root of unity. Since $\Phi_n(x)$ is irreducible over F, by Theorems 2.12(b) and 5.3,

$$[F(\mu_n) : F] = [F(\zeta) : F] = \deg(\Phi_n) = \varphi(n). \tag{10.7}$$

Combining (10.5)–(10.7), we find that

$$|\mathrm{Gal}(F(\mu_n)/F)| = |\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})|.$$

The isomorphism now follows from part (b). □

In Example 6.9, the question was posed as to when, for p a prime, $\mathbb{Q}(\mu_p)$ is an irreducible radical extension of $\mathbb{Q}$. We are now in a position to provide an answer.

Theorem 10.15. Let n be a natural number. If $\mathbb{Q}(\mu_n)$ is an irreducible radical extension of $\mathbb{Q}$, then any odd prime that divides $\varphi(n)$ also divides n.

Proof. By Theorem 6.5, $\mathbb{Q}(\mu_n)$ is a prime-irreducible radical extension of $\mathbb{Q}$. So, there is a tower of fields

$$\mathbb{Q} = R_0 \subset R_1 \subset \cdots \subset R_j \subset \cdots \subset R_m = \mathbb{Q}(\mu_n)$$

where R_j is an irreducible binomial extension of R_{j-1} of prime degree p_j for $j = 1, 2, \ldots, m$. Then $R_j = R_{j-1}(\beta_j)$ for some β_j in R_j, where $\beta_j^{p_j}$ is in R_{j-1}, and $h_j(x) = x^{p_j} - \beta_j^{p_j}$ is irreducible over R_{j-1} for each j. By Theorem 5.4(b),

$$\varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}] = p_1 p_2 \cdots p_m.$$

Let q be an odd prime dividing $\varphi(n)$. Then $q = p_k$ for some $1 \leq k \leq m$. Since $\mathbb{Q}(\mu_n)$ is a splitting field over $\mathbb{Q}$, by Theorem 2.27, it is a splitting field over R_{k-1}. It follows from Theorem 9.12 that $h_k(x)$ splits over $\mathbb{Q}(\mu_n)$. Therefore, $\mathbb{Q}(\mu_n)$ contains a primitive qth root of unity ξ, hence $\Phi_q(x)$ splits over $\mathbb{Q}(\mu_n)$. Suppose that q does not divide n. By Theorem 5.5(d), $\Phi_q(x) = \min(\xi, \mathbb{Q}(\mu_n))$,

which is irreducible over $\mathbb{Q}(\mu_n)$. In order for $\Phi_q(x)$ to both split over $\mathbb{Q}(\mu_n)$ and be irreducible over $\mathbb{Q}(\mu_n)$, it must be of degree 1. It follows from Theorem 5.6(a) that $q = 2$, which is impossible because q is odd. Therefore, q divides n. □

As an illustration of Theorem 10.15, since 3 divides $\varphi(14) = 6$ but not 14, $\mathbb{Q}(\mu_{14})$ is not an irreducible radical extension of $\mathbb{Q}$.

A prime p such that $p = 2^m + 1$ for some natural number m is called a Fermat[1] prime. It can be shown that in this case, m must itself be power of 2. The only known Fermat primes are the following:

$$\begin{aligned} 3 &= 2^{2^0} + 1 \\ 5 &= 2^{2^1} + 1 \\ 17 &= 2^{2^2} + 1 \\ 257 &= 2^{2^3} + 1 \\ 65{,}537 &= 2^{2^4} + 1. \end{aligned}$$

The next candidate, $2^{2^5} + 1$, is divisible by 641.

Theorem 10.16. Let p be an odd prime. Then $\mathbb{Q}(\mu_p)$ is an irreducible radical extension of $\mathbb{Q}$ if and only if p is a Fermat prime.

Proof. ($\Rightarrow$): If p is not a Fermat prime, then there is an odd prime q dividing $\varphi(p) = p - 1$. Evidently, q does not divide p, so we have from Theorem 10.15 that $\mathbb{Q}(\mu_p)$ is not an irreducible radical extension of $\mathbb{Q}$.

($\Leftarrow$): If p is a Fermat prime, then $p - 1 = 2^m$ for some natural number m. By Theorem 10.12, $\mathrm{Gal}(\mathbb{Q}(\mu_{p-1})/\mathbb{Q})$ is cyclic of order 2^m. It follows from parts (a) and (b) of Theorem B.7 that there is a unique subgroup G_j of $\mathrm{Gal}(\mathbb{Q}(\mu_{p-1})/\mathbb{Q})$ of order 2^{m-j} for $j = 0, 1, \ldots, m$, and that G_j is a subgroup of G_{j-1} for $j = 1, 2, \ldots, m$. So, we have the solvable series

$$\langle id \rangle = G_m \lhd \cdots \lhd G_j \lhd \cdots \lhd G_0 = \mathrm{Gal}(\mathbb{Q}(\mu_{p-1})/\mathbb{Q})$$

where G_{j-1}/G_j is of order 2, hence cyclic, for $j = 1, 2, \ldots, m$ (Appendix C). By the FTGT, there is a tower of fields

$$\mathbb{Q} = R_0 \subset \cdots \subset R_j \subset \cdots \subset R_m = \mathbb{Q}(\mu_{p-1})$$

where $R_j = \mathbb{Q}(\mu_{p-1})^{G_j}$ and $[R_j : R_{j-1}] = 2$ for $j = 1, 2, \ldots, m$. Let $R_j = R_{j-1}(\theta_j)$ for some θ_j in R_j. Then $\min(\theta_j, R_{j-1})$ is a quadratic polynomial in $R_{j-1}[x]$ that is easily solved by radicals over R_{j-1} using the quadratic formula. Thus, $\mathbb{Q}(\mu_p)$ is an irreducible radical extension of $\mathbb{Q}$. □

[1]Pierre de Fermat (1601–1665) was a French jurist and "amateur" mathematician who, among other accomplishments, made significant contributions to number theory.

To close this chapter, we use Galois theory to give alternative proofs of Theorem 6.7(a) and the second assertion of Theorem 6.10.

Theorem 10.17. Let p be a prime, and let $h(x) = x^p - a$ be a polynomial in $F[x]$, where $a \neq 0$. Suppose that F contains a primitive pth root of unity. If $h(x)$ is reducible over F, then $h(x)$ splits over F.

Proof. Let ζ be a primitive pth root of unity in F, let β be an arbitrary root of $h(x)$, and let $[F(\beta) : F] = m$. By Theorem 10.4(b), m divides p, so $m = 1$ or $m = p$. Since $h(x)$ is reducible over F, Theorem 2.12(b) implies that $m \neq p$. Therefore, $m = 1$, hence β is in F. Since the roots of $h(x)$ are $\zeta^i \beta$ for $i = 0, 1, \ldots, p-1$, the result follows. □

Theorem 10.18. Let p be a prime, and let ζ be a primitive pth root of unity. Then $\mathbb{Q}(\mu_{p-1}, \zeta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1})$ of degree $p - 1$.

Proof. By Theorem 5.5(d), $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\mu_{p-1})$, so we have from Theorem 10.14(e) that

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p-1}, \zeta)/\mathbb{Q}(\mu_{p-1})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

and

$$[\mathbb{Q}(\mu_{p-1}, \zeta) : \mathbb{Q}(\mu_{p-1})] = p - 1.$$

Then Theorem 10.12 implies that $\mathbb{Q}(\mu_{p-1}, \zeta)$ is a cyclic extension of $\mathbb{Q}(\mu_{p-1})$. It follows from Theorem 10.7 that $\mathbb{Q}(\mu_{p-1}, \zeta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1})$. □

To be more explicit about the underlying construction in the proof of Theorem 10.18, let ξ be a primitive $(p-1)$th root of unity, and let $\lambda = (\xi, \zeta)$ be the Lagrange resolvent as defined in (10.1). Then λ is precisely (6.9). We saw in Theorem 6.7(a) that $\lambda \neq 0$. It follows from Theorems 10.1(b), 10.2(b), and 10.4(d) that $\mathbb{Q}(\mu_{p-1}, \zeta) = \mathbb{Q}(\mu_{p-1}, \lambda)$, λ^{p-1} is in $\mathbb{Q}(\mu_{p-1})$, and $x^{p-1} - \lambda^{p-1}$ is irreducible over $\mathbb{Q}(\mu_{p-1})$. Thus, we have reproduced the key findings in the proof of Theorem 6.7(a) using Galois theory.

CHAPTER 11

GALOIS'S CRITERION FOR SOLVABILITY OF POLYNOMIALS BY RADICALS

In this chapter, we are finally in a position to present the crowning achievement of classical Galois theory—Galois's criterion for the solvability of polynomials by radicals. For a discussion of what it means for a group to be *solvable*, the reader is referred to Appendix C. In an effort to make the material presented in this chapter essentially independent of previous results on polynomials, we use Galois theory to prove again two key results from Chapter 6, namely, Theorems 6.15 and 6.19.

Theorem 11.1. Let F be a field, and let n be a natural number. Then there is an extension L of F such that:
(a) L is a splitting field over F.
(b) L contains a primitive nth root of unity.
(c) L is a prime-irreducible radical extension of F with the root of unity property over F.
(d) $\mathrm{Gal}(L/F)$ is solvable.

Proof. The proof is by induction on n. The result is trivial for $n = 1$. Suppose that $n > 1$. Since $\varphi(n) < n$, by the induction hypothesis, there is a field R such that:
(i) R is a splitting field over F.
(ii) R contains a primitive $\varphi(n)$th root of unity.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

(iii) R is a prime-irreducible radical extension of F with the root of unity property over F.
(iv) $\mathrm{Gal}(R/F)$ is solvable.

We will show that $L = R(\mu_n)$ satisfies properties (a)–(d).

(a): By property (i), R is the splitting field over F of some polynomial $g(x)$ in $F[x]$. Then $R(\mu_n)$ is the splitting field over F of the polynomial $g(x)\Phi_n(x)$ in $F[x]$.

(b): Obvious.

(c): It follows from Theorems 10.10 and 10.14(b) that $\mathrm{Gal}(R(\mu_n)/R)$ is Abelian. By Theorems C.12 and C.14, $\mathrm{Gal}(R(\mu_n)/R)$ has a solvable series

$$\langle id \rangle = G_m \lhd \cdots \lhd G_j \lhd G_{j-1} \lhd \cdots \lhd G_0 = \mathrm{Gal}(R(\mu_n)/R)$$

where G_{j-1}/G_j is of prime order p_j, hence cyclic, for $j = 1, 2, \ldots, m$. Clearly, $R(\mu_n)$ is a splitting field over R. By the FTGT, there is a tower of fields

$$R = R_0 \subset \cdots \subset R_{j-1} \subset R_j \subset \cdots \subset R_m = R(\mu_n)$$

where $R_j = R(\mu_n)^{G_j}$, $G_j = \mathrm{Gal}(R(\mu_n)/R_j)$, and $[R_j : R_{j-1}] = p_j$ for each j. By Theorem 2.27, $R(\mu_n)$ is a splitting field over R_{j-1}. Since $G_j \lhd G_{j-1}$, we have from the FTGT that R_j is a splitting field over R_{j-1}, and $\mathrm{Gal}(R_j/R_{j-1}) \cong G_{j-1}/G_j$. Therefore, R_j is a cyclic extension of R_{j-1}. Since p_j divides $[R(\mu_n) : R]$, and since, by Theorem 10.14(c), $[R(\mu_n) : R]$ divides $\varphi(n)$, we have from property (ii) that R contains a primitive p_jth root of unity. It follows from Theorem 10.7 that R_j is an irreducible binomial extension of R_{j-1} for each j. Therefore, $R(\mu_n)$ is a prime-irreducible radical extension of R with the root of unity property over R. According to property (iii), R is a prime-irreducible radical extension of F with the root of unity property over F. Thus, $R(\mu_n)$ is a prime-irreducible radical extension of F with the root of unity property over F.

(d): We have from part (a) that $R(\mu_n)$ is a splitting field over F, and from property (i) that R is a splitting field over F. By the FTGT,

$$\mathrm{Gal}(R(\mu_n)/R) \trianglelefteq \mathrm{Gal}(R(\mu_n)/F)$$

and

$$\mathrm{Gal}(R/F) \cong \mathrm{Gal}(R(\mu_n)/F)/\mathrm{Gal}(R(\mu_n)/R).$$

As was demonstrated in part (c), $\mathrm{Gal}(R(\mu_n)/R)$ is solvable, and according to property (iv), so is $\mathrm{Gal}(R/F)$. It follows from Theorem C.10 that $\mathrm{Gal}(R(\mu_n)/F)$ is solvable. □

We observe that parts (b) and (c) of Theorem 11.1 provide a proof of Theorem 6.15 based on Galois theory.

Theorem 11.2. Let K and L be splitting fields over F, and suppose that $\mathrm{Gal}(L/F)$ is solvable. Then $\mathrm{Gal}(K/F)$ is solvable if and only if $\mathrm{Gal}(KL/L)$ is solvable.

Proof. See the figure for Theorem 4.10.

($\Rightarrow$): Since $\mathrm{Gal}(K/F)$ is solvable, it follows from Theorem C.9 that so is $\mathrm{Gal}(K/K \cap L)$. By the TNI, $\mathrm{Gal}(K/K \cap L) \cong \mathrm{Gal}(KL/L)$, hence $\mathrm{Gal}(KL/L)$ is solvable.

($\Leftarrow$): Since K and L are splitting fields over F, so is KL. It follows from the FTGT that $\mathrm{Gal}(KL/L) \trianglelefteq \mathrm{Gal}(KL/F)$ and

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(KL/F)/\mathrm{Gal}(KL/L).$$

Since $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(KL/L)$ are solvable, by Theorem C.10, so is $\mathrm{Gal}(KL/F)$. Switching the roles of K and L, we find that $\mathrm{Gal}(KL/K) \trianglelefteq \mathrm{Gal}(KL/F)$ and

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(KL/F)/\mathrm{Gal}(KL/K).$$

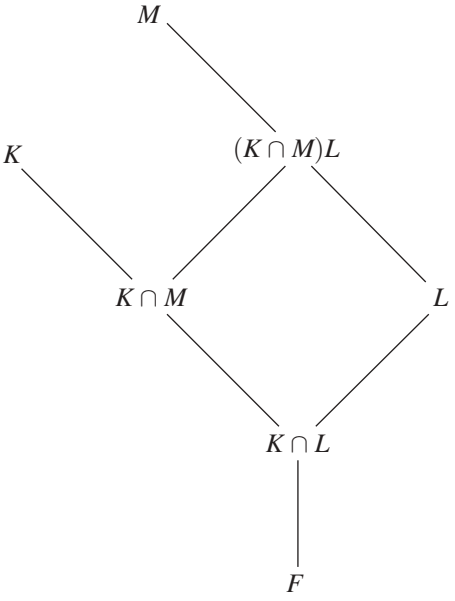
We just demonstrated that $\mathrm{Gal}(KL/F)$ is solvable. By Theorem C.10, so is $\mathrm{Gal}(K/F)$. □

Theorem 11.3. Let K be a splitting field over F, let L be an extension of F, and let M be a splitting field over L. Then $K \cap M$ is a splitting field over $K \cap L$ of degree

$$[K \cap M : K \cap L] = [(K \cap M)L : L] = \frac{[M : L]}{[KM : KL]}$$

and

$$\mathrm{Gal}(K \cap M/K \cap L) \cong \mathrm{Gal}((K \cap M)L/L).$$



Proof. The result is trivial if $K \cap M = K \cap L$, so assume that $K \cap M \neq K \cap L$. Let $K \cap M = (K \cap L)(\theta)$ for some θ in $K \cap M$, and let $f(x) = \min(\theta, K \cap L)$. It follows from Theorem 2.27 that K is a splitting field over $K \cap L$. By Theorem 9.12, $f(x)$ splits over K. We have from Theorem 4.10(b) that $f(x) = \min(\theta, L)$. Since M is a splitting field over L, $f(x)$ also splits over M. Therefore, $f(x)$ splits over $K \cap M$, so $K \cap M$ is the splitting field of $f(x)$ over $K \cap L$. By the TNI,

$$\mathrm{Gal}(K \cap M / K \cap L) \cong \mathrm{Gal}((K \cap M)L/L)$$

and

$$[K \cap M : K \cap L] = [(K \cap M)L : L].$$

We also have from the TNI that

$$[KL : L] = [K : K \cap L] \quad \text{and} \quad [KM : M] = [K : K \cap M]$$

hence

$$[K \cap M : K \cap L] = \frac{[K : K \cap L]}{[K : K \cap M]} = \frac{[KL : L]}{[KM : M]} = \frac{[M : L]}{[KM : KL]}.$$

□

Theorem 11.4. Let K be a splitting field over F, let L be an extension of F, and let M be an irreducible binomial extension of L of prime degree p. Suppose that F contains a primitive pth root of unity. If $K \cap L \neq K \cap M$, then $K \cap M$ is an irreducible binomial extension of $K \cap L$ of degree p.

Proof. See the figure for Theorem 11.4. Note that $L \neq (K \cap M)L$, otherwise $K \cap M \subseteq L$, hence $K \cap L = K \cap M$. By Theorem 2.15, $(K \cap M)L = M$. Since M is an irreducible binomial extension of L of degree p, and F contains a primitive pth root of unity, by Theorem 10.7, M is a cyclic extension of L. In particular, M is a splitting field over L. By Theorem 11.3, $K \cap M$ is a splitting field over $K \cap L$ of degree

$$[K \cap M : K \cap L] = [M : L] = p$$

and

$$\mathrm{Gal}(K \cap M / K \cap L) \cong \mathrm{Gal}(M/L).$$

Therefore, $K \cap M$ is a cyclic extension of $K \cap L$. Again by Theorem 10.7, $K \cap M$ is an irreducible binomial extension of $K \cap L$. □

Since Theorem 11.4 is a restatement of Theorem 6.18, and since Theorem 6.18 is the key to Theorem 6.19, we therefore have a proof of Theorem 6.19 based on Galois theory.

We now arrive at what must be regarded as the high point of Galois's *Mémoire*, his criterion for solvability by radicals.

Theorem 11.5 (Galois). Let $f(x)$ be a polynomial in $F[x]$, and let K be the splitting field of $f(x)$ over F. Then $f(x)$ is solvable by irreducible radicals over F if and only if $\mathrm{Gal}(K/F)$ is solvable.

Proof. ($\Rightarrow$): Let R be an irreducible radical extension of F that contains K. By Theorem 11.1, there is an extension L of F with the following properties:
(a) L is a splitting field over F.
(b) L contains a primitive $[R : F]$th root of unity.
(c) $\mathrm{Gal}(L/F)$ is solvable.

Suppose that K is contained in L. By property (a) and the FTGT, $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$ and

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K).$$

It follows from property (c) and Theorem C.10 that $\mathrm{Gal}(K/F)$ is solvable.

Now, suppose that K is not contained in L. We claim that KL is an irreducible radical extension of L. By Theorem 6.5, R is a prime-irreducible radical extension of F. So, there is a tower of fields

$$F = R_0 \subset R_1 \subset \cdots \subset R_j \subset \cdots \subset R_m = R$$

where R_j is an irreducible binomial extension of R_{j-1} of prime degree q_j for $j = 1, 2, \ldots, m$. Then $R_j = R_{j-1}(\beta_j)$ for some β_j in R_j, where $\beta_j^{q_j}$ is in R_{j-1} for each j. We therefore have the tower

$$L = R_0L \subseteq R_1L \subseteq \cdots \subseteq R_jL \subseteq \cdots \subseteq R_mL = RL \tag{11.1}$$

where $R_jL = R_{j-1}L(\beta_j)$ and $\beta_j^{q_j}$ is in $R_{j-1}L$ for each j. Since $[R : F] = q_1q_2 \cdots q_m$, property (b) implies that L contains a primitive q_jth root of unity for each j. Using Theorem 6.10 to delete redundancies from (11.1), we see that RL is an irreducible radical extension of L. By the TNI, KL is a splitting field over L and $[KL : L] = [K : K \cap L]$. Since $[K : K \cap L]$ divides $[R : F]$, we have from property (b) that L contains a primitive pth root of unity for every prime p dividing $[KL : L]$. Setting $F = L$, $K = KL$, and $R = RL$ in Theorem 6.19, it follows that KL is an irreducible radical extension of L. This proves the claim.

In fact, by Theorem 6.5, KL is a prime-irreducible radical extension of L. So, there is a tower of fields

$$L = M_0 \subset \cdots \subset M_i \subset \cdots \subset M_n = KL$$

where M_i is an irreducible binomial extension of M_{i-1} of prime degree p_i for $i = 1, 2, \ldots, n$. Since $[M_i : M_{i-1}]$ divides $[KL : L]$, M_{i-1} contains a primitive p_ith root of unity. It follows from Theorem 10.7 that M_i is a cyclic extension of M_{i-1}.

By the FTGT, there is a series of groups

$$\langle id \rangle = G_n \subset \cdots \subset G_i \subset \cdots \subset G_0 = \mathrm{Gal}(KL/L)$$

where $G_i = \mathrm{Gal}(KL/M_i)$ for each i. We have from Theorem 2.27 that KL is a splitting field over M_{i-1}. Since M_i is a splitting field over M_{i-1}, the FTGT implies that $G_i \lhd G_{i-1}$ and $G_{i-1}/G_i \cong \mathrm{Gal}(M_i/M_{i-1})$ for each i. Thus, G_{i-1}/G_i is cyclic, hence Abelian, for each i. Therefore, $\mathrm{Gal}(KL/L)$ is solvable. It follows from properties (a) and (c) and Theorem 11.2 that $\mathrm{Gal}(K/F)$ is solvable.

($\Leftarrow$): By Theorem 11.1, there is an extension L of F that has the following properties:

(a) L is a splitting field over F.
(b) L contains a primitive $[K : F]$th root of unity.
(c) L is an irreducible radical extension of F.
(d) $\mathrm{Gal}(L/F)$ is solvable.

We have from properties (a) and (d) and Theorem 11.2 that $\mathrm{Gal}(KL/L)$ is solvable. By Theorem C.14, $\mathrm{Gal}(KL/L)$ has a solvable series

$$\langle id \rangle = G_n \lhd \cdots \lhd G_i \lhd \cdots \lhd G_0 = \mathrm{Gal}(KL/L)$$

where G_{i-1}/G_i is of prime order p_i, hence cyclic, for $i = 1, 2, \ldots, n$. By the TNI, KL is a splitting field over L and $[KL : L] = [K : K \cap L]$. It follows from the FTGT that there is a tower of fields

$$L = M_0 \subset \cdots \subset M_i \subset \cdots \subset M_n = KL$$

where $M_i = (KL)^{G_i}$, $G_i = \mathrm{Gal}(KL/M_i)$, and $[M_i : M_{i-1}] = p_i$ for each i.

We have from Theorem 2.27 that KL is a splitting field over M_{i-1}. Since $G_i \lhd G_{i-1}$, by the FTGT, M_i is a splitting field over M_{i-1}, and $\mathrm{Gal}(M_i/M_{i-1}) \cong G_{i-1}/G_i$ for each i. Therefore, M_i is a cyclic extension of M_{i-1} for each i. Since $[M_i : M_{i-1}]$ divides $[KL : L]$, which in turn divides $[K : F]$, we have from property (b) that L contains a primitive p_ith root of unity. By Theorem 10.7, M_i is an irreducible binomial extension of M_{i-1} for each i. Thus, KL is an irreducible radical extension of L. According to property (c), L is an irreducible radical extension of F. It follows that KL is an irreducible radical extension of F. Therefore, $f(x)$ is solvable by irreducible radicals over F. □

The elegant symmetry of Galois's criterion for solvability by radicals is somewhat obscured in the proof of Theorem 11.5 because of the constant need to ensure that certain roots of unity are available. In the notation of Theorem 11.5, suppose that F already contains the "necessary" roots of unity.

Then Theorems 11.1 and 11.2 are not needed, and by Theorem 6.19, $f(x)$ is solvable by irreducible radicals over F if and only if K is an irreducible radical extension of F. With this simplification, the proof of the revised version of Theorem 11.5 amounts to little more than using the FTGT and Theorem 10.7 to translate statements about a tower of fields into statements about a series of groups, and conversely.

We now arrive at our third and final version of the Impossibility Theorem. Observe that here, unlike in Theorem 7.11 (the second version of the Impossibility Theorem), we do not make assumptions about the presence of roots of unity.

Theorem 11.6 (Impossibility Theorem). In the notation of (7.1)–(7.7), let $f(x)$ be the general polynomial of degree n over a subfield E of F. If $n \geq 5$, then $f(x)$ is not solvable by irreducible radicals over F.

Proof. Let K be the splitting field of $f(x)$ over F. By Theorem 9.20(c), $\mathrm{Gal}(K/F) \cong S_n$, and by Theorem D.9, S_n is not solvable. It follows from Theorem 11.5 that $f(x)$ is not solvable by irreducible radicals over F. □

CHAPTER 12

POLYNOMIALS OF PRIME DEGREE

In order to avoid repetition, we begin by providing a context for the chapter. The focus will be on $f(x)$, a polynomial in $F[x]$ of prime degree p that is irreducible over F, an arbitrary field. By Theorem 2.18, $f(x)$ has simple roots, which we denote by $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$. The splitting field of $f(x)$ over F will be denoted by K. We sometimes, but not always, view $\mathrm{Gal}(K/F)$ as a subgroup of S_p, where S_p is in turn regarded as a group of permutations on $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. Calculations that involve $\mathbb{F}_p$ are performed modulo p. For a in $\mathbb{F}_p^{\times}$, we denote by a^{-1} the multiplicative inverse of a.

Our immediate goal is to characterize $\mathrm{Gal}(K/F)$ as a subgroup of S_p under the assumption that $f(x)$ is solvable by irreducible radicals over F. We know from Theorem 11.5 that $\mathrm{Gal}(K/F)$ is a solvable group, but here our aim is to say something more specific. This will be accomplished in Theorem 12.2 using group-theoretic methods. We motivate the discussion using earlier results on polynomials.

For present purposes only, suppose that F contains a primitive qth root of unity for every prime q dividing $[K : F]$. Since $f(x)$ is solvable by irreducible radicals over F, K is contained in an irreducible radical extension of F. It follows from Theorems 6.5 and 6.19 that K is a prime-irreducible radical extension of F. Let $R_{n-1} \subset R_n = K$ be the last two fields in a tower of irreducible binomial extensions from F to K. By Theorem 6.22(b), $[K : R_{n-1}] = p$. As in the proof of Theorem 11.5, we can construct a solvable series for $\mathrm{Gal}(K/F)$ corresponding to the preceding tower. Let $\langle id \rangle = G_n \subset G_{n-1}$ be the first two groups in the

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

solvable series, that is, $G_{n-1} = \mathrm{Gal}(K/R_{n-1})$. Then $|G_{n-1}| = p$, and since p is a prime, G_{n-1} is cyclic. Let $G_{n-1} = \langle \rho \rangle$, where ρ is some element of G_{n-1} of order p. By Theorem D.11, ρ is a p-cycle. Renumbering the roots of $f(x)$ if necessary, we may assume that

$$\rho = (0\ 1\ 2 \ldots p-1).$$

Let G_{n-2} be the third group in the solvable series. Then $\langle \rho \rangle \lhd G_{n-2}$. We now pursue the question of what characterizes a subgroup of S_p that has $\langle \rho \rangle$ as a normal subgroup. To that end, it is helpful to express certain permutations in S_p as functions on $\mathbb{F}_p$. In particular, we give ρ the functional form

$$\rho(k) = k + 1$$

for k in $\mathbb{F}_p$. Then

$$\rho^b(k) = k + b$$

for b in $\mathbb{F}_p$. Suppose that $\sigma \neq id$ is an element in a subgroup of S_p that has $\langle \rho \rangle$ as a normal subgroup. Then $\sigma \langle \rho \rangle \sigma^{-1} = \langle \rho \rangle$, so $\sigma\rho = \rho^a \sigma$ for some a in $\mathbb{F}_p^\times$. Thus,

$$\sigma(k+1) = \sigma\rho(k) = \rho^a \sigma(k) = \sigma(k) + a \tag{12.1}$$

for all k in $\mathbb{F}_p$. Setting $\sigma(0) = b$, we have $\sigma(1) = a + b$, $\sigma(2) = 2a + b$, and in general, $\sigma(k) = ak + b$. In this way, we are led to the following definition.

For each a in $\mathbb{F}_p^\times$ and each b in $\mathbb{F}_p$, define a map

$$\begin{aligned} \sigma_{(a,b)} \colon \mathbb{F}_p &\longrightarrow \mathbb{F}_p \\ k &\longmapsto ak + b. \end{aligned}$$

Let M_p be the set of all such maps, that is,

$$M_p = \{\sigma_{(a,b)} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p\}.$$

Note that since $\sigma_{(1,b)}(k) = k + b$, we have

$$\sigma_{(1,b)} = \rho^b. \tag{12.2}$$

As the next theorem shows, M_p has a number of interesting properties.

Theorem 12.1.
(a) M_p is a subgroup of S_p of order $p(p-1)$.
(b) M_p is solvable.
(c) $\langle \rho \rangle \trianglelefteq M_p$.

(d) If σ in S_p is such that $\sigma\rho\sigma^{-1}$ is in M_p, then σ is in M_p.
(e) $\langle\rho\rangle\backslash\langle id\rangle$ is the set of (all) p-cycles in M_p.

Proof. (a): It is readily verified that $\sigma_{(a,b)}$ is a permutation on $\mathbb{F}_p$ and that

$$\sigma_{(a,b)}\sigma_{(c,d)} = \sigma_{(ac,ad+b)}. \tag{12.3}$$

Since a and c are in $\mathbb{F}_p^\times$, so is their product, hence M_p is closed under composition. Also, $\sigma_{(1,0)} = id$ and

$$\sigma_{(a,b)}^{-1} = \sigma_{(a^{-1},-a^{-1}b)}.$$

Therefore, M_p is a subgroup of S_p. Suppose that $\sigma_{(a,b)} = \sigma_{(c,d)}$, that is, $ak + b = ck + d$ for all k in $\mathbb{F}_p$. Setting $k = 0$ shows that $b = d$, and then setting $k = 1$ implies that $a = c$. Thus, each (a, b) pair, with a from $\mathbb{F}_p^\times$ and b from $\mathbb{F}_p$, produces a distinct element of M_p. So, M_p is of order $p(p-1)$.

(b): It follows from (12.3) that the map

$$\begin{aligned} \iota\colon M_p &\longrightarrow \mathbb{F}_p^\times \\ \sigma_{(a,b)} &\longmapsto a \end{aligned}$$

is a homomorphism. Evidently, ι is surjective. We have from (12.2) that

$$\ker(\iota) = \{\sigma_{(1,b)} : b \in \mathbb{F}_p\} = \langle\rho\rangle$$

and from Theorem C.3 that $M_p/\langle\rho\rangle \cong \mathbb{F}_p^\times$. By Theorem E.4, $\mathbb{F}_p^\times$ is cyclic, hence Abelian. Therefore, $\langle id\rangle \lhd \langle\rho\rangle \lhd M_p$ is a solvable series for M_p.

(c): This follows from the discussion preceding the definition of M_p.

(d): Since $\sigma\rho\sigma^{-1}$ is in M_p, there are a in $\mathbb{F}_p^\times$ and b in $\mathbb{F}_p$ such that $\sigma\rho\sigma^{-1}(k) = ak + b$ for all k in $\mathbb{F}_p$. By Theorem D.3, $\sigma\rho\sigma^{-1}$ is a p-cycle, so $\sigma\rho\sigma^{-1}$ does not fix any element of $\mathbb{F}_p$. Thus, $(a-1)k + b = 0$ does not have a solution k in $\mathbb{F}_p$. Then $a = 1$, otherwise $k = -(a-1)^{-1}b$ is a solution; and $b \neq 0$, otherwise any k is a solution. Therefore, $\sigma\rho\sigma^{-1} = \rho^b$ for some b in $\mathbb{F}_p^\times$. The argument used in connection with (12.1) shows that σ is in M_p.

(e): Let ϕ be a p-cycle in M_p. By Theorem D.3, there is τ in S_p such that $\phi = \tau\rho\tau^{-1}$. It follows from part (d) that τ is in M_p and then from part (c) that ϕ is in $\langle\rho\rangle$. Thus, $\langle\rho\rangle$ contains all p-cycles in M_p. Since $\langle\rho\rangle$ is of order p, by Theorems B.1(a) and D.11, every element of $\langle\rho\rangle\backslash\langle id\rangle$ is a p-cycle. □

In the older literature, M_p is called the *metacyclic group*, which accounts for the choice of notation.

We assumed at the beginning of the chapter that $f(x)$ is irreducible over F and set out to characterize $\mathrm{Gal}(K/F)$ under the assumption that $f(x)$ is solvable by irreducible radicals over F. In light of Theorems 9.19 and 11.5, we are therefore

asking what it means for a subgroup of S_p to be both transitive and solvable. Before answering this question, we need one more group-theoretic notion and a few of its consequences, all of which are readily verified. For each τ in S_p, the map

$$\begin{aligned} \iota_\tau : S_p &\longrightarrow S_p \\ \sigma &\longmapsto \tau\sigma\tau^{-1} \end{aligned}$$

is an automorphism of S_p referred to as the *inner automorphism* associated with τ. If H_1 and H_2 are subgroups of S_p, then $H_1 \trianglelefteq H_2$ if and only if $\iota_\tau(H_1) \trianglelefteq \iota_\tau(H_2)$. For each σ in S_p, $\iota_\tau(\langle\sigma\rangle) = \langle\iota_\tau(\sigma)\rangle$. For each σ in S_p and each k in $\mathbb{F}_p$, σ fixes k if and only if $\iota_\tau(\sigma)$ fixes $\tau(k)$.

Theorem 12.2. Let G be a transitive subgroup of S_p. Then the following are equivalent:
(a) G is solvable.
(b) $\iota_\tau(G)$ is a subgroup of M_p for some τ in S_p.
(c) id is the only element of G that fixes at least two elements of $\mathbb{F}_p$.

Proof. Since G is transitive and $p \geq 2$, we have $G \neq \langle id\rangle$.

(a)⇒(b): By Theorem C.14, G has a solvable series

$$\langle id\rangle = G_n \lhd \cdots \lhd G_i \lhd \cdots \lhd G_0 = G$$

where $[G_{i-1} : G_i] = p_i$ is prime for $i = 1, 2, \ldots, n$. Suppose that $n > 1$. Since G_0 is transitive and $G_1 \lhd G_0$, by Theorem D.10, G_1 is transitive. Similarly, since G_1 is transitive and $G_2 \lhd G_1$, again by Theorem D.10, G_2 is transitive. Proceeding in this way, we find that G_{n-1} is transitive. By Theorem D.12, G_{n-1} contains a p-cycle, which we denote by ϕ. Since $\langle\phi\rangle$ is of order p, and G_{n-1} is of order p_n, we have $p_n = p$ and $G_{n-1} = \langle\phi\rangle$. (Note the similarity of this argument to that used in the proof of Theorem 6.22.) By Theorem D.3, there is τ in S_p such that $\iota_\tau(\phi) = \rho$. Let $H_i = \iota_\tau(G_i)$ for $i = 0, 1, \ldots, n$. It follows from the above results on inner automorphisms that H has the solvable series

$$\langle id\rangle = H_n \lhd \cdots \lhd H_i \lhd \cdots \lhd H_0 = H$$

where $[H_{i-1} : H_i] = p_i$ and $H_{n-1} = \langle\rho\rangle$. Since $H_{n-1} \lhd H_{n-2}$, $\sigma\rho\sigma^{-1}$ is in $H_{n-1} \subseteq M_p$ for all σ in H_{n-2}. By Theorem 12.1(d), $H_{n-2} \subseteq M_p$. Similarly, since $H_{n-2} \lhd H_{n-3}$, $\sigma\rho\sigma^{-1}$ is in $H_{n-2} \subseteq M_p$ for all σ in H_{n-3}. Again by Theorem 12.1(d), $H_{n-3} \subseteq M_p$. Proceeding in this way, we find that $\iota_\tau(G) = H \subseteq M_p$. If $n = 1$, the obvious modifications can be made to the above argument.

(b)⇒(c): If $\sigma_{(a,b)}$ in M_p fixes the distinct elements k and l in $\mathbb{F}_p$, then $ak + b = k$ and $al + b = l$, from which it follows that $(a-1)(k-l) = 0$. Therefore, $a = 1$, hence $b = 0$, which means that $\sigma_{(a,b)} = id$. Thus, id is the only element

of M_p that fixes at least two elements of $\mathbb{F}_p$. Since $\iota_\tau(G)$ is a subgroup of M_p, the above results on inner automorphisms show that G has the same property.

(c)$\Rightarrow$(a): Since G is transitive, by Theorem D.12, G contains a p-cycle μ. By Theorem D.3, there is τ in S_p such that $\iota_\tau(\mu) = \rho$. In light of the above results on inner automorphisms, no loss of generality is incurred by assuming that ρ is in G. Take σ in G, and let $\phi = \sigma\rho\sigma^{-1}$. Then $\phi^b\sigma = \sigma\rho^b$ for all b in $\mathbb{F}_p$, hence

$$\rho^{-\sigma(b)}\phi^b\sigma(k) = \rho^{-\sigma(b)}\sigma\rho^b(k) = \sigma(b+k) - \sigma(b) \tag{12.4}$$

for all k in $\mathbb{F}_p$. Note that since σ is a bijection, $\sigma(k+1) - \sigma(k) \neq 0$ for all k in $\mathbb{F}_p$. Therefore, as k ranges over $\mathbb{F}_p$, the p differences $\sigma(k+1) - \sigma(k)$ give rise to at most $p-1$ distinct values. So, there are distinct elements l and m in $\mathbb{F}_p$ such that

$$\sigma(l+1) - \sigma(l) = \sigma(m+1) - \sigma(m).$$

It follows from (12.4) that

$$\rho^{-\sigma(l)}\phi^l\sigma(0) = \rho^{-\sigma(m)}\phi^m\sigma(0)$$

and

$$\rho^{-\sigma(l)}\phi^l\sigma(1) = \rho^{-\sigma(m)}\phi^m\sigma(1).$$

Since ρ and ϕ are in G,

$$(\rho^{-\sigma(l)}\phi^l)^{-1}(\rho^{-\sigma(m)}\phi^m) = \phi^{-l}\rho^{\sigma(l)-\sigma(m)}\phi^m$$

is an element of G that fixes $\sigma(0)$ and $\sigma(1)$. By assumption,

$$\phi^{-l}\rho^{\sigma(l)-\sigma(m)}\phi^m = id$$

hence

$$\phi^{l-m} = \rho^{\sigma(l)-\sigma(m)}.$$

Therefore, $\phi = \phi^{(l-m)(l-m)^{-1}}$ is in $\langle\rho\rangle \subseteq M_p$. But $\phi = \sigma\rho\sigma^{-1}$, so we have from Theorem 12.1(d) that σ is in M_p. Since σ was arbitrary, $G \subseteq M_p$. By Theorems C.9 and 12.1(b), G is solvable. □

Theorem 12.2 tells us that, up to isomorphism, the only subgroups of S_p that are transitive and solvable are M_p and certain of its subgroups. In particular, up to isomorphism, M_p is the "largest" such subgroup of S_p.

The next theorem is a striking result due to Galois. It appeared in his *Mémoire*.

Theorem 12.3 (Galois). $f(x)$ is solvable by irreducible radicals over F if and only if $K = F(\alpha_i, \alpha_j)$, where α_i and α_j are any two distinct roots of $f(x)$.

Proof. Since $f(x)$ is irreducible over F, by Theorem 9.19, $\mathrm{Gal}(K/F)$ is a transitive subgroup of S_p. So, Theorem 12.2 applies. Then

$f(x)$ is solvable by irreducible radicals over F.
- $\Leftrightarrow$ $\mathrm{Gal}(K/F)$ is solvable. [Theorem 11.5]
- $\Leftrightarrow$ id is the only element of $\mathrm{Gal}(K/F)$ that fixes at least two roots of $f(x)$. [Theorem 12.2]
- $\Leftrightarrow$ $\mathrm{Gal}(K/F(\alpha_i, \alpha_j)) = \langle id \rangle$ for all $i \neq j$.
- $\Leftrightarrow$ $K = F(\alpha_i, \alpha_j)$ for all $i \neq j$. [FTGT]

□

We now provide an alternative—and especially elegant—proof of Theorem 6.23 based on Galois theory. Recall the discussion leading up to (3.26), where $f(x)$ is a polynomial in $\mathbb{R}[x]$ that has r real roots and c pairs of nonreal complex roots.

Theorem 12.4 (Kronecker). Let F be a subfield of $\mathbb{R}$, and let $p \geq 5$. If $f(x)$ is solvable by irreducible radicals over F, then $r = 1$ or $r = p$.

Proof. As was pointed out in Theorem 6.23, since p is odd, $f(x)$ has at least one real root, so $r \geq 1$. Suppose that $r > 1$, and let α_i and α_j be distinct real roots. By Theorem 12.3, $K = F(\alpha_i, \alpha_j) \subseteq \mathbb{R}$, so $r = p$. □

The following result provides insight into a special case of Theorem 12.4.

Theorem 12.5. Let F be a subfield of $\mathbb{R}$, and let $p \geq 5$. If $f(x)$ has precisely $p - 2$ real roots, then $f(x)$ is not solvable by irreducible radicals over F.

Proof. Since $f(x)$ is in $\mathbb{R}[x]$, by the Fundamental Theorem of Algebra, K is a subfield of $\mathbb{C}$. It was remarked in connection with (3.26) that complex conjugation is an automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$ pointwise. Let τ be the restriction of complex conjugation to K. Since K is a splitting field over F, by Theorem 9.22, τ is in $\mathrm{Gal}(K/F)$. Let α be one of the two nonreal complex roots of $f(x)$. Its complex conjugate $\tau(\alpha)$ is the other, and τ fixes the remaining $p - 2$ real roots of $f(x)$. Therefore, viewing $\mathrm{Gal}(K/F)$ as a subgroup of S_p, τ is a transposition. By Theorems 9.19 and D.12, $\mathrm{Gal}(K/F)$ contains a p-cycle. It follows from Theorem D.13 that $\mathrm{Gal}(K/F) \cong S_p$. By Theorem D.9, $\mathrm{Gal}(K/F)$ is not solvable. The result now follows from Theorem 11.5. □

Theorem 12.6. Let F be a subfield of $\mathbb{R}$, and let $p \geq 5$. If $(p - 1)/2$ is even and $\mathrm{disc}(f) < 0$, then $f(x)$ is not solvable by irreducible radicals over F.

Proof. In the context of this chapter, (3.26) becomes $p = r + 2c$. If $r = 1$, then $c = (p-1)/2$ is even, and if $r = p$, then $c = 0$ (also even). Since $\text{disc}(f) < 0$, we have from Theorem 3.18 that c is odd, so $r = 1$ and $r = p$ are impossible. It follows from Theorem 12.4 that $f(x)$ is not solvable by irreducible radicals over F. □

Theorem 12.7. Let F be a subfield of $\mathbb{R}$, let $p \geq 5$, and let $f(x) = x^p + ax + b$, where $a, b \neq 0$. If $(p-1)/2$ is even and

$$-\frac{a^p}{b^{p-1}} > \frac{p^p}{(p-1)^{p-1}} \tag{12.5}$$

then $f(x)$ is not solvable by irreducible radicals over F.

Proof. With $(p-1)/2$ even, we have from Theorem 3.17 that

$$\text{disc}(f) = (p-1)^{p-1}a^p + p^p b^{p-1}.$$

Noting that (12.5) is equivalent to $\text{disc}(f) < 0$, the result now follows from Theorem 12.6. □

Part of the reason that Galois's *Mémoire* was rejected by the Paris Academy of Sciences was that his theorems did not provide an "external" criterion for a polynomial to be solvable by radicals, that is, one based on the coefficients of the polynomial rather than its roots. Theorem 12.7 is a response to that criticism, at least for a certain family of polynomials in $\mathbb{R}[x]$. As an illustration, let $f(x) = x^5 - 10x + 5$. By Eisenstein's criterion with $p = 5$, $f(x)$ is irreducible over $\mathbb{Q}$. Since (12.5) is satisfied, $f(x)$ is not solvable by irreducible radicals over $\mathbb{Q}$. This same finding appeared in Example 6.24.

We close this chapter with a result that shows that M_p arises in the familiar context of binomial polynomials over $\mathbb{Q}$.

Theorem 12.8. Let $h(x) = x^p - a$ be a polynomial in $\mathbb{Q}[x]$ that is irreducible over $\mathbb{Q}$, let β be a root of $h(x)$, and let ζ be a primitive pth root of unity. Then $\mathbb{Q}(\zeta, \beta)$ is the splitting field of $h(x)$ over $\mathbb{Q}$, and $\text{Gal}(\mathbb{Q}(\zeta, \beta)/\mathbb{Q}) \cong M_p$.

Proof. The roots of $h(x)$ are $\zeta^i \beta$ for $i = 0, 1, \ldots, p-1$, hence $\mathbb{Q}(\zeta, \beta)$ is the splitting field of $h(x)$ over $\mathbb{Q}$. Note that

$$\begin{aligned} [\mathbb{Q}(\zeta, \beta) : \mathbb{Q}] &= [\mathbb{Q}(\zeta, \beta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] \\ &= [\mathbb{Q}(\zeta, \beta) : \mathbb{Q}(\zeta)](p-1) \end{aligned} \tag{12.6}$$

and

$$[\mathbb{Q}(\zeta, \beta) : \mathbb{Q}] = [\mathbb{Q}(\zeta, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\zeta, \beta) : \mathbb{Q}(\beta)]p.$$

Since $p-1$ and p are relatively prime, and they both divide $[\mathbb{Q}(\zeta,\beta):\mathbb{Q}]$, we have

$$[\mathbb{Q}(\zeta,\beta):\mathbb{Q}] \geq p(p-1).$$

By Theorem 2.12(c).

$$[\mathbb{Q}(\zeta,\beta):\mathbb{Q}(\zeta)] \leq [\mathbb{Q}(\beta):\mathbb{Q}] = p.$$

It follows from (12.6) that

$$[\mathbb{Q}(\zeta,\beta):\mathbb{Q}] \leq p(p-1).$$

Therefore,

$$[\mathbb{Q}(\zeta,\beta):\mathbb{Q}] = p(p-1).$$

By the FTGT,

$$|\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q})| = p(p-1).$$

Take τ in $\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q})$. Then $\tau(\zeta)$ is a root of $\Phi_p(x)$, and $\tau(\beta)$ is a root of $h(x)$. Therefore, $\tau(\zeta)=\zeta^a$ for some a in $\mathbb{F}_p^\times$, and $\tau(\beta)=\zeta^b\beta$ for some b in $\mathbb{F}_p$. These two values completely determine τ, which we now denote by $\tau_{(a,b)}$. Thus,

$$\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q}) = \{\tau_{(a,b)} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p\}.$$

Since $\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q})$ is of order $p(p-1)$, the $\tau_{(a,b)}$ are distinct.

Let $\tau_{(a,b)}$ and $\tau_{(c,d)}$ be arbitrary elements of $\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q})$. Then

$$\tau_{(a,b)}\,\tau_{(c,d)}(\zeta) = \tau_{(a,b)}(\tau_{(c,d)}(\zeta)) = \tau_{(a,b)}(\zeta^c) = [\tau_{(a,b)}(\zeta)]^c = \zeta^{ac}$$

and

$$\begin{aligned}\tau_{(a,b)}\tau_{(c,d)}(\beta) &= \tau_{(a,b)}(\tau_{(c,d)}(\beta)) = \tau_{(a,b)}(\zeta^d\beta) = \tau_{(a,b)}(\zeta^d)\tau_{(a,b)}(\beta)\\ &= (\zeta^{ad})(\zeta^b\beta) = \zeta^{ad+b}\beta.\end{aligned}$$

Therefore,

$$\tau_{(a,b)}\tau_{(c,d)} = \tau_{(ac,ad+b)}. \tag{12.7}$$

It follows from (12.3) and (12.7) that the map

$$\begin{aligned}\iota\colon \mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q}) &\longrightarrow M_p\\ \tau_{(a,b)} &\longmapsto \sigma_{(a,b)}\end{aligned}$$

is a group homomorphism. It is readily verified that ι is injective, and since $\mathrm{Gal}(\mathbb{Q}(\zeta,\beta)/\mathbb{Q})$ and M_p both have order $p(p-1)$, they are isomorphic. □

CHAPTER 13

PERIODS OF ROOTS OF UNITY

Let p be a prime, let $p-1=q_1q_2\cdots q_n$ be a factorization of $p-1$ into not necessarily distinct primes, and let ζ be a primitive pth root of unity. In Theorem 6.7(a), and again in Theorem 10.18, we showed that $\mathbb{Q}(\mu_{p-1},\zeta)$ is an irreducible binomial extension of $\mathbb{Q}(\mu_{p-1})$. In fact, according to Theorem 6.5, $\mathbb{Q}(\mu_{p-1},\zeta)$ is a prime-irreducible radical extension of $\mathbb{Q}(\mu_{p-1})$. So, there is a tower of fields

$$\mathbb{Q}(\mu_{p-1})=R_0\subset R_1\subset\cdots\subset R_i\subset\cdots\subset R_n=\mathbb{Q}(\mu_{p-1},\zeta)$$

where R_i is an irreducible binomial extension of R_{i-1} of prime degree q_i for $i=1,2,\ldots,n$. Then $R_i=R_{i-1}(\beta_i)$ for some β_i in R_i, where $\beta_i^{q_i}$ is in R_{i-1}, and $x^{q_i}-\beta_i^{q_i}$ is irreducible over R_{i-1} for each i.

In the proof of Theorem 6.7(a) and in the discussion subsequent to Theorem 10.18, we defined an element λ in $\mathbb{Q}(\mu_{p-1},\zeta)$ and demonstrated that it has the following properties: $\mathbb{Q}(\mu_{p-1},\zeta)=\mathbb{Q}(\mu_{p-1},\lambda)$, λ^{p-1} is in $\mathbb{Q}(\mu_{p-1})$, and $x^{p-1}-\lambda^{p-1}$ is irreducible over $\mathbb{Q}(\mu_{p-1})$. Remarks made in the context of Theorem 6.7(a) show that $\sqrt[m_i]{\lambda^{p-1}}$ meets the requirements to be β_i, where $m_i=q_1q_2\cdots q_i$ for $i=1,2,\ldots,n$. Although this approach is satisfactory from the theoretical point of view, the computational burden involved in finding an explicit expression for λ^{p-1} as an element of $\mathbb{Q}(\mu_{p-1})$ can be significant. Even in the relatively simple case $p=5$ discussed in Example 6.8, it was convenient to rely on *Maple*.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

An alternative approach is available. Let θ_i be an arbitrary element in $R_i \backslash R_{i-1}$, and let ξ_i be a primitive q_ith root of unity in $\mathbb{Q}(\mu_{p-1})$. We have from Theorems 10.5 and 10.6 that there are $1 \leq k_i, l_i \leq q_i - 1$ such that $(\xi_i, \theta_i^{k_i})$ and $(\xi_i^{l_i}, \theta_i)$ have the requisite properties to be β_i for $i = 1, 2, \ldots, n$. The question then arises as to whether the θ_i can be selected in a way that offers computational advantages. In this chapter, we show that this is possible using the theory of periods of roots of unity as developed by Gauss.

A rather humble illustration will motivate the discussion. Recall Example 6.6, where $\Phi_5(x)$ was solved by irreducible radicals over $\mathbb{Q}$. In that setting, we considered

$$\gamma_1 = \zeta_5 + \zeta_5^{-1} = \zeta_5 + \zeta_5^4$$

and

$$\gamma_2 = \zeta_5^2 + \zeta_5^{-2} = \zeta_5^2 + \zeta_5^3.$$

Noting that

$$\Phi_5(\zeta_5) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$$

we have $\gamma_1 + \gamma_2 = -1$, and it is easily demonstrated that $\gamma_1 \gamma_2 = -1$. Since γ_1 is not in $\mathbb{Q}$, it follows that

$$\min(\gamma_1, \mathbb{Q}) = (x - \gamma_1)(x - \gamma_2) = x^2 + x - 1.$$

Note that $\min(\gamma_1, \mathbb{Q})$ is the same as (6.7). The argument used in Example 6.6 shows that

$$\min(\zeta_5, \mathbb{Q}(\gamma_1)) = x^2 - \gamma_1 x + 1.$$

Thus, we can construct the extension $\mathbb{Q}(\gamma_1)$ of $\mathbb{Q}$ by solving $\min(\gamma_1, \mathbb{Q})$ over $\mathbb{Q}$, and then construct the extension $\mathbb{Q}(\zeta_5)$ of $\mathbb{Q}(\gamma_1)$ by solving $\min(\zeta_5, \mathbb{Q}(\gamma_1))$ over $\mathbb{Q}(\gamma_1)$.

The reason this works out so conveniently is that $5 - 1$ is a power of 2, making the calculations amenable to the quadratic formula. Also of crucial importance is the particular way in which the 5th roots of unity enter into γ_1 and γ_2. With only four roots of unity to contend with, we might have proceeded on a trial-and-error basis in an effort to find sums with the properties exhibited by γ_1 and γ_2. Aside from there being no a priori reason to expect such nicely behaved sums to exist, the undertaking would be daunting for the next prime that might be considered for such an approach, namely, 17. This points to the need for a systematic way of creating sums of roots of unity with desirable properties.

Let ζ be a primitive pth root of unity, and let F be a field over which $\Phi_p(x)$ is irreducible. According to Theorems 5.4(a) and 5.5(d), $F = \mathbb{Q}$ and $F = \mathbb{Q}(\mu_{p-1})$

are suitable choices. Then $K = F(\zeta)$ is the splitting field of $\Phi_p(x)$ over F, and by Theorems 10.12 and 10.14(e), $\mathrm{Gal}(K/F)$ is cyclic of order $p-1$. Let g be a primitive congruence root modulo p. We have from (10.4) and Theorem 10.12 that $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, where

$$\sigma^k(\zeta) = \zeta^{g^k} \tag{13.1}$$

for $k = 0, 1, \ldots, p-2$.

Before proceeding, we make a few general observations so as to avoid unnecessary repetition in the remainder of the chapter. Since $\mathrm{Gal}(K/F)$ is Abelian, all subgroups to be considered are normal, all extensions are splitting fields, and the FTGT is available in all settings.

The next three theorems spell out the crucial implications of $\mathrm{Gal}(K/F)$ being a cyclic group. The first result informs us that the existence of subgroups of $\mathrm{Gal}(K/F)$, hence the existence of fields between F and K, is governed entirely by the divisors of $|\mathrm{Gal}(K/F)| = p-1$.

Theorem 13.1. Let $r \leq p-1$ be a natural number. Then the following are equivalent:
(a) r divides $p-1$.
(b) $\mathrm{Gal}(K/F)$ has a subgroup of order r.
(c) There is field between F and K over which K has degree r.

Proof. (a)⇒(b): This follows from Theorem B.7(a).

(b)⇒(c): Let H be a subgroup of $\mathrm{Gal}(K/F)$ of order r. By Theorem 9.11, $[K : K^H] = r$.

(c)⇒(a): Let E be a field between F and K such that $[K : E] = r$. Then

$$p - 1 = [K : F] = r[E : F].$$

□

Theorem 13.2. Let r be a natural number dividing $p-1$, and let

$$H_r = \langle\sigma^{(p-1)/r}\rangle \quad \text{and} \quad K_r = K^{H_r}.$$

Then:
(a) H_r is the unique subgroup of $\mathrm{Gal}(K/F)$ of order r.
(b) K_r is the unique field between F and K over which K has degree r.

Proof. (a): This follows from Theorem B.7(b).

(b): As in the proof of Theorem 13.1, K_r has the desired property. If E is a field between F and K such that $[K : E] = r$, then $|\mathrm{Gal}(K/E)| = r$. It follows from part (a) that $\mathrm{Gal}(K/E) = H_r$, hence $E = K^{H_r} = K_r$. □

Theorem 13.3. Let r and s be natural numbers dividing $p-1$. Then the following are equivalent:
(a) s divides r.

(b) $H_s \subseteq H_r$.
(c) $K_r \subseteq K_s$.

Proof. (a)⇒(b): Since s divides r,

$$H_s = \langle \sigma^{(p-1)/s} \rangle \subseteq \langle \sigma^{(p-1)/r} \rangle = H_r.$$

(b)⇒(c): Since $H_s \subseteq H_r$,

$$K_r = K^{H_r} \subseteq K^{H_s} = K_s.$$

(c)⇒(a): Since $K_r \subseteq K_s$, we have from Theorem 13.2(b) that

$$[K_s : K_r] = \frac{[K : K_r]}{[K : K_s]} = \frac{r}{s}.$$

□

With these preliminaries settled, we now turn to the matter of how to define and compute with sums of roots of unity.

Let b be a natural number dividing $p - 1$, and let

$$p - 1 = ab.$$

Then

$$H_b = \langle \sigma^a \rangle = \{\sigma^{ja} : j = 0, 1, \ldots, b - 1\} \tag{13.2}$$

and

$$K_b = K^{H_b}. \tag{13.3}$$

Thus,

$$H_b = \mathrm{Gal}(K/K_b)$$

$$[K : K_b] = b \quad \text{and} \quad [K_b : F] = a. \tag{13.4}$$

For completeness, we observe that

$$H_1 = \langle id \rangle \qquad H_{p-1} = \mathrm{Gal}(K/F)$$

and

$$K_1 = K \qquad K_{p-1} = F.$$

For each m in $\mathbb{F}_p$, let

$$\langle b, m\rangle = \sum_{j=0}^{b-1} \zeta^{g^{ja}m}. \tag{13.5}$$

The expression $\langle b, m\rangle$ is referred to as a *period* of b terms. For the particular case $b = p - 1$ and $m = 1$, we find from (5.10) and $\Phi_p(\zeta) = 0$ that

$$\langle p-1, 1\rangle = \sum_{k=0}^{p-2} \zeta^{g^k} = -1. \tag{13.6}$$

Recall the definition of σ in (13.1). Since

$$\zeta^{g^{ja}m} = [\sigma^{ja}(\zeta)]^m = \sigma^{ja}(\zeta^m)$$

we can express (13.5) as

$$\langle b, m\rangle = \sum_{j=0}^{b-1} \sigma^{ja}(\zeta^m). \tag{13.7}$$

Then $\langle b, 0\rangle = b$ and

$$\langle b, 1\rangle = \sum_{j=0}^{b-1} \sigma^{ja}(\zeta). \tag{13.8}$$

Note that each term in (13.8) corresponds to an element of H_b. It follows that $\langle b, 1\rangle$ is fixed by H_b. So, $\langle b, 1\rangle$ is in K^{H_b}, and we have $F(\langle b, 1\rangle) \subseteq K_b$. We will see shortly that equality holds.

We have from (13.7) that

$$\langle b, g^i\rangle = \sum_{j=0}^{b-1} \sigma^{ja}(\zeta^{g^i}) = \sum_{j=0}^{b-1} \sigma^{ja+i}(\zeta) = \sigma^i(\langle b, 1\rangle) \tag{13.9}$$

for $i = 0, 1, \ldots, a-1$. We refer to the $\langle b, g^i\rangle$ as the *a periods of b terms*. It follows from (13.9) that

$$\sigma(\langle b, g^i\rangle) = \sigma^{i+1}(\langle b, 1\rangle) = \langle b, g^{i+1}\rangle$$

for $i = 0, 1, \ldots, a-1$, and more generally that

$$\sigma^k(\langle b, g^i\rangle) = \langle b, g^{i+k}\rangle \tag{13.10}$$

for $i, k = 0, 1, \ldots, a-1$.

Consider the elements $id, \sigma, \sigma^2, \ldots, \sigma^{a-1}$ in $\mathrm{Gal}(K/F)$. If $\sigma^r H_b = \sigma^s H_b$ for some $0 \le r < s \le a-1$, then σ^{s-r} is in H_b, hence $s - r = ja$ for some $0 \le j \le b-1$. But $s - r < a$, thus $j = 0$, so $r = s$. Since each $\sigma^i H_b$ has b elements, and $\mathrm{Gal}(K/F)$ is of order $p-1$, it follows that

$$id, \sigma, \sigma^2, \ldots, \sigma^{a-1}$$

are (left = right) coset representatives of H_b in $\mathrm{Gal}(K/F)$.

Theorem 13.4.
(a) The $\langle b, g^i \rangle$ do not have any terms in common.
(b) The $\langle b, g^i \rangle$ are linearly independent over F.
(c) The $\langle b, g^i \rangle$ have distinct values.

Proof. (a): As can be seen from (13.9), each term in $\langle b, g^i \rangle$ corresponds to an element in the coset $\sigma^i H_b$ of H_b in $\mathrm{Gal}(K/F)$. Since the distinct cosets form a partition of $\mathrm{Gal}(K/F)$, and since $\zeta, \sigma(\zeta), \sigma^2(\zeta), \ldots, \sigma^{p-2}(\zeta)$ are distinct, the $\langle b, g^i \rangle$ do not have any terms in common.

(b): By assumption, $\Phi_p(x)$ is irreducible over F. We have from Theorem 2.11(a) that $\{1, \zeta^2, \ldots \zeta^{p-2}\}$, hence $\{\zeta, \zeta, \ldots, \zeta^{p-1}\}$, is a basis for K over F. It now follows from part (a) that the $\langle b, g^i \rangle$ are linearly independent over F.

(c): This follows from part (b). □

We have from (13.6) and Theorem 13.4(a) the following generalization of (13.6):

$$\sum_{i=0}^{a-1} \langle b, g^i \rangle = \langle p-1, 1 \rangle = -1. \tag{13.11}$$

Suppose that we had based the construction of the a periods of b terms on another primitive congruence root modulo p. According to Theorem 13.2(a), H_b is the only subgroup of $\mathrm{Gal}(K/F)$ of order b. Therefore, we would have arrived at the same set of cosets, hence the same periods. Now, suppose that we had proceeded using another primitive pth root of unity ξ. Since $\xi = \sigma^r(\zeta)$ for some $0 \le r \le p-2$ and since $\sigma^r, \sigma^{r+1}, \sigma^{r+2}, \ldots, \sigma^{r+a-1}$ are coset representatives of H_b in $\mathrm{Gal}(K/F)$, again the same periods would have resulted. Thus, the values of the a periods of b terms do not depend on the choice of primitive congruence root modulo p or the primitive pth root of unity.

As an illustration, let $p = 13$ and $b = 3$. The primitive congruence roots modulo 13 are 2, 6, 7, and 11. The values of 2^k and $7^k \pmod{13}$ for $k = 0, 1, \ldots, 11$ are shown in the following arrays. These numerical results confirm the observations made in the preceding paragraph.

$$
\begin{array}{llll}
2^0 \equiv 1 & 2^3 \equiv 8 & 2^6 \equiv 12 & 2^9 \equiv 5 \\
2^1 \equiv 2 & 2^4 \equiv 3 & 2^7 \equiv 11 & 2^{10} \equiv 10 \\
2^2 \equiv 4 & 2^5 \equiv 6 & 2^8 \equiv 9 & 2^{11} \equiv 7
\end{array}
$$

$$
\begin{array}{llll}
7^0 \equiv 1 & 7^3 \equiv 5 & 7^6 \equiv 12 & 7^9 \equiv 8 \\
7^1 \equiv 7 & 7^4 \equiv 9 & 7^7 \equiv 6 & 7^{10} \equiv 4 \\
7^2 \equiv 10 & 7^5 \equiv 11 & 7^8 \equiv 3 & 7^{11} \equiv 2
\end{array}
$$

Example 13.5 (13th root of unity). Let $p = 13$, $F = \mathbb{Q}$, and $K = \mathbb{Q}(\zeta_{13})$. Taking $g = 2$, we have

k	0	1	2	3	4	5	6	7	8	9	10	11
$2^k \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7

Then $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}) = \langle \sigma \rangle$, where $\sigma(\zeta_{13}) = \zeta_{13}^2$. The periods of roots of unity are as follows:

$$
\begin{aligned}
\langle 1, 2^0 \rangle &= \langle 1, 1 \rangle = \zeta_{13} \\
\langle 1, 2^1 \rangle &= \langle 1, 2 \rangle = \zeta_{13}^2 \\
\langle 1, 2^2 \rangle &= \langle 1, 4 \rangle = \zeta_{13}^4 \\
&\vdots \\
\langle 1, 2^9 \rangle &= \langle 1, 5 \rangle = \zeta_{13}^5 \\
\langle 1, 2^{10} \rangle &= \langle 1, 10 \rangle = \zeta_{13}^{10} \\
\langle 1, 2^{11} \rangle &= \langle 1, 7 \rangle = \zeta_{13}^7
\end{aligned}
$$

$$
\begin{aligned}
\langle 2, 2^0 \rangle &= \langle 2, 1 \rangle = \zeta_{13} + \zeta_{13}^{12} \\
\langle 2, 2^1 \rangle &= \langle 2, 2 \rangle = \zeta_{13}^2 + \zeta_{13}^{11} \\
\langle 2, 2^2 \rangle &= \langle 2, 4 \rangle = \zeta_{13}^4 + \zeta_{13}^9 \\
\langle 2, 2^3 \rangle &= \langle 2, 8 \rangle = \zeta_{13}^8 + \zeta_{13}^5 \\
\langle 2, 2^4 \rangle &= \langle 2, 3 \rangle = \zeta_{13}^3 + \zeta_{13}^{10} \\
\langle 2, 2^5 \rangle &= \langle 2, 6 \rangle = \zeta_{13}^6 + \zeta_{13}^7
\end{aligned}
$$

$$
\begin{aligned}
\langle 3, 2^0 \rangle &= \langle 3, 1 \rangle = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9 \\
\langle 3, 2^1 \rangle &= \langle 3, 2 \rangle = \zeta_{13}^2 + \zeta_{13}^6 + \zeta_{13}^5 \\
\langle 3, 2^2 \rangle &= \langle 3, 4 \rangle = \zeta_{13}^4 + \zeta_{13}^{12} + \zeta_{13}^{10} \\
\langle 3, 2^3 \rangle &= \langle 3, 8 \rangle = \zeta_{13}^8 + \zeta_{13}^{11} + \zeta_{13}^7
\end{aligned}
$$

$$\langle 4, 2^0\rangle = \langle 4, 1\rangle = \zeta_{13} + \zeta_{13}^8 + \zeta_{13}^{12} + \zeta_{13}^5$$
$$\langle 4, 2^1\rangle = \langle 4, 2\rangle = \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{11} + \zeta_{13}^{10}$$
$$\langle 4, 2^2\rangle = \langle 4, 4\rangle = \zeta_{13}^4 + \zeta_{13}^6 + \zeta_{13}^9 + \zeta_{13}^7$$

$$\langle 6, 2^0\rangle = \langle 6, 1\rangle = \zeta_{13} + \zeta_{13}^4 + \zeta_{13}^3 + \zeta_{13}^{12} + \zeta_{13}^9 + \zeta_{13}^{10}$$
$$\langle 6, 2^1\rangle = \langle 6, 2\rangle = \zeta_{13}^2 + \zeta_{13}^8 + \zeta_{13}^6 + \zeta_{13}^{11} + \zeta_{13}^5 + \zeta_{13}^7.$$

Note that for each b, once we have $\langle b, 1\rangle$, we can obtain the remaining periods of b terms by using (13.10). Consistent with (13.6) and (13.11), we have

$$\langle 12, 1\rangle = \zeta_{13} + \zeta_{13}^2 + \zeta_{13}^4 + \cdots + \zeta_{13}^5 + \zeta_{13}^{10} + \zeta_{13}^7 = -1$$

and

$$\langle 2, 1\rangle + \langle 2, 2\rangle + \langle 2, 4\rangle + \langle 2, 8\rangle + \langle 2, 3\rangle + \langle 2, 6\rangle = -1$$
$$\langle 3, 1\rangle + \langle 3, 2\rangle + \langle 3, 4\rangle + \langle 3, 8\rangle = -1$$
$$\langle 4, 1\rangle + \langle 4, 2\rangle + \langle 4, 4\rangle = -1$$
$$\langle 6, 1\rangle + \langle 6, 2\rangle = -1.$$

$\Diamond$

The next result sets out the key properties of the $\langle b, g^i\rangle$ as they relate to K_b as an extension of F.

Theorem 13.6.
(a) $\min(\langle b, 1\rangle, F) = \prod_{i=0}^{a-1} (x - \langle b, g^i\rangle)$.
(b) $K_b = F(\langle b, g^i\rangle)$ for $i = 0, 1, \ldots, a-1$.
(c) The $\langle b, g^i\rangle$ are a basis for K_b over F.

Proof. (a): We claim that $H_b = \mathrm{Gal}(K/F(\langle b, 1\rangle))$. It was observed above that $\langle b, 1\rangle$ is fixed by H_b, so $H_b \subseteq \mathrm{Gal}(K/F(\langle b, 1\rangle))$. Take ν in $\mathrm{Gal}(K/F(\langle b, 1\rangle))$. Since the distinct cosets of H_b in $\mathrm{Gal}(K/F)$ form a partition of $\mathrm{Gal}(K/F)$, $\nu = \sigma^r\tau$ for some $0 \le r \le a-1$ and some τ in H_b. So, $\tau(\langle b, 1\rangle) = \langle b, 1\rangle$, and we have from (13.9) that

$$\langle b, 1\rangle = \nu(\langle b, 1\rangle) = \sigma^r\tau(\langle b, 1\rangle) = \sigma^r(\langle b, 1\rangle) = \langle b, g^r\rangle.$$

Then Theorem 13.4(c) implies that $r = 0$, hence ν is in H_b. Therefore, $\mathrm{Gal}(K/F(\langle b, 1\rangle)) \subseteq H_b$. This proves the claim. Since K is a splitting field over F, and $id, \sigma, \ldots, \sigma^{a-1}$ are coset representatives of $\mathrm{Gal}(K/F(\langle b, 1\rangle))$ in $\mathrm{Gal}(K/F)$, the result follows from (13.9) and Theorem 9.18.

(b): We have from (13.4) that $[K_b : F] = a$. By part (a) and Theorem 2.12(b), $[F(\langle b, g^i \rangle) : F] = a$ for each i. Then Theorem 13.2(b) implies that $K_b = F(\langle b, g^i \rangle)$ for each i.

(c): By Theorem 13.4(b), the $\langle b, g^i \rangle$ are linearly independent over F. Since there are a of them, and $[K_b : F] = a$, the $\langle b, g^i \rangle$ are a basis for K_b over F.

It is instructive to provide an alternative proof that the $\langle b, g^i \rangle$ span K_b over F. Since $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ is a basis for K over F, each γ in K can be expressed uniquely in the form

$$\gamma = \sum_{i=0}^{a-1} \sum_{j=0}^{b-1} c_{ij} \sigma^{ja+i}(\zeta) \tag{13.12}$$

where the c_{ij} are in F. Note that each of the a inner sums in (13.12) corresponds to a coset of H_b in $\mathrm{Gal}(K/F)$. Now, suppose that γ is in $K_b = K^{H_b}$, that is, $\sigma^{ja}(\gamma) = \gamma$ for $j = 0, 1, \ldots, b-1$. It follows from $\sigma^{ja}\sigma^i H_b = \sigma^i H_b$ that the elements of H_b permute the elements of each coset among themselves, and do so in a cyclic manner. The uniqueness of the expression for γ in terms of the basis implies that

$$c_{i0} = c_{i1} = \cdots = c_{ij} = \cdots = c_{i,b-1}$$

for $i = 0, 1, \ldots, a-1$. It follows from (13.9) that

$$\gamma = \sum_{i=0}^{a-1} c_{i0} \left[\sum_{j=0}^{b-1} \sigma^{ja+i}(\zeta) \right] = \sum_{i=0}^{a-1} c_{i0} \langle b, g^i \rangle.$$

Thus, the $\langle b, g^i \rangle$ span K_b over F. □

Theorem 13.6(b) is a remarkable result. It demonstrates that not only do we have $K_b = F(\langle b, 1 \rangle)$, as claimed earlier, but also that each of the other $a-1$ periods of b terms is a primitive element for K_b over F.

With a and b as above, let d be a natural number dividing b, and let $b = cd$. Then

$$p - 1 = ab = acd.$$

We have from (13.2) and (13.3) that

$$H_d = \langle \sigma^{ac} \rangle = \{\sigma^{jac} : j = 0, 1, \ldots, d-1\}$$

and $K_d = K^{H_d}$. An important observation is that, by Theorem 13.3, H_d is a subgroup of H_b, and K_d is an extension of K_b. It follows from (13.4) that

$$[H_b : H_d] = c = [K_d : K_b].$$

Since $K_b = F(\langle b, 1\rangle)$ and $K_d = F(\langle d, 1\rangle)$, we have the Galois correspondence below as a framework for constructing a tower of fields from F to K. Note that $K_d = K_b(\langle d, 1\rangle)$. We seek an explicit expression for $\min(\langle d, 1\rangle, K_b)$ as a polynomial in $K_b[x]$.

$$\begin{array}{ccc}
H_{p-1} = \langle \sigma \rangle & \text{———} & K_{p-1} = F \\
\Big| a & & \Big| a \\
H_b = \langle \sigma^a \rangle & \text{———} & K_b = F(\langle b,1\rangle) \\
\Big| c & & \Big| c \\
H_d = \langle \sigma^{ac} \rangle & \text{———} & K_d = F(\langle d,1\rangle)
\end{array}$$

Since $p - 1 = acd$, there are ac periods of d terms. However, we are primarily interested in the c of them that sum to $\langle b, 1\rangle$, as described below. We have from (13.5) and (13.7) that

$$\langle d, m\rangle = \sum_{j=0}^{d-1} \zeta^{g^{jac} m} = \sum_{j=0}^{d-1} \sigma^{jac}(\zeta^m)$$

hence

$$\langle d, 1\rangle = \sum_{j=0}^{d-1} \sigma^{jac}(\zeta)$$

and

$$\langle d, g^{ia}\rangle = \sum_{j=0}^{d-1} \sigma^{jac+ia}(\zeta) = \sigma^{ia}(\langle d, 1\rangle) \tag{13.13}$$

for $i = 0, 1, \ldots, c - 1$.

It can be verified that $id, \sigma^a, \sigma^{2a}, \ldots, \sigma^{(c-1)a}$ are coset representatives of H_d in H_b. Note from (13.13) that each term in $\langle d, g^{ia}\rangle$ corresponds to an element in the coset $\sigma^{ia}H_d$ of H_d in H_b. Since the distinct cosets form a partition of H_b, it follows from (13.8) that

$$\sum_{i=0}^{c-1}\langle d, g^{ia}\rangle = \langle b, 1\rangle. \tag{13.14}$$

Theorem 13.7.

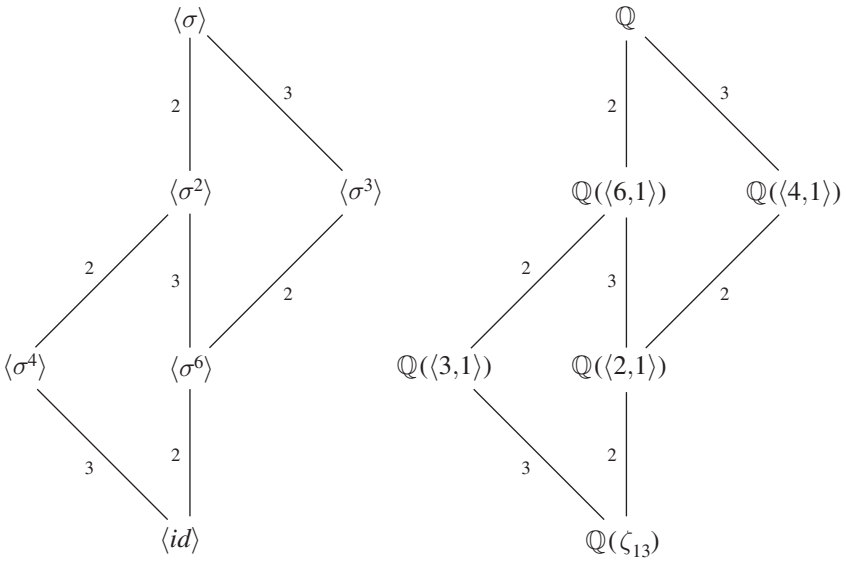
$$\min(\langle d, 1\rangle, K_b) = \prod_{i=0}^{c-1}(x - \langle d, g^{ia}\rangle).$$

Proof. We remarked above that $K_d = K_b(\langle d, 1\rangle)$, so $H_d = \mathrm{Gal}(K/K_b(\langle d, 1\rangle))$. Since K is a splitting field over K_b, and $id, \sigma^a, \sigma^{2a}, \ldots, \sigma^{(c-1)a}$ are coset representatives of H_d in $H_b = \mathrm{Gal}(K/K_b)$, the result follows from (13.13) and Theorem 9.18. □

With Theorems 13.6 and 13.7, an approach to constructing a tower of fields from $F = K_{p-1}$ to $K = K_1$ is much clarified. Ultimately, the construction rests on a choice of divisors of $p - 1$, as we now describe. The process begins with $\langle p - 1, 1\rangle$, under the assumption that its terms are ordered as in (13.6). For the initial step, we choose a divisor b of $p - 1$ and obtain the extension $K_b = F(\langle b, 1\rangle)$ of K_{p-1} and the minimal polynomial $\min(\langle b, 1\rangle, K_{p-1})$. Setting $a = (p - 1)/b$, we can think of $\langle b, 1\rangle$ as being derived from $\langle p - 1, 1\rangle$ by forming the sum of successive ath terms of $\langle p - 1, 1\rangle$ starting with ζ. Since $\langle p - 1, 1\rangle$ is the sum of the a periods of b terms, beginning the selection process with some other term of $\langle p - 1, 1\rangle$ possibly results in a different period of b terms, but according to Theorem 13.6, we still arrive at K_b and $\min(\langle b, 1\rangle, F)$. By Theorem 13.6, the conjugates of $\langle b, 1\rangle$ over K_{p-1} are precisely the a periods of b terms, and they sum to $\langle p - 1, 1\rangle$.

For the next step, we choose a divisor d of b and obtain the extension $K_d = K_b(\langle d, 1\rangle)$ of K_b and the minimal polynomial $\min(\langle d, 1\rangle, K_b)$. Setting $c = b/d$, we can think of $\langle d, 1\rangle$ as being derived from $\langle b, 1\rangle$ by forming the sum of successive cth terms of $\langle b, 1\rangle$ starting with ζ. By Theorem 13.7, the conjugates of $\langle d, 1\rangle$ over K_b are the c periods of b terms that sum to $\langle b, 1\rangle$. If a further step is needed, we choose a divisor f of d, and so on. Thus, the choice of divisors leads to a series of periods of roots of unity, each "contained in" the preceding period, and eventually terminating in the period of 1 term ζ.

Example 13.8 (13th root of unity). We continue with Example 13.5. The Galois correspondence is shown in the following figure.



Consider the tower of fields from $K_{12} = \mathbb{Q}$ to $K_1 = \mathbb{Q}(\zeta_{13})$ that takes the path through $K_6 = \mathbb{Q}(\langle 6, 1\rangle)$ and $K_3 = \mathbb{Q}(\langle 3, 1\rangle$. We have from Example 13.5 that

$$\langle 6, 1\rangle + \langle 6, 2\rangle = -1$$
$$\langle 3, 1\rangle + \langle 3, 2\rangle + \langle 3, 4\rangle + \langle 3, 8\rangle = -1$$

and

$$\langle 6, 1\rangle = \langle 3, 1\rangle + \langle 3, 4\rangle.$$

It follows from Theorem 13.6 that

$$K_6 = \mathbb{Q}(\langle 6, 1\rangle) = \mathbb{Q}(\langle 6, 2\rangle)$$
$$K_3 = \mathbb{Q}(\langle 3, 1\rangle) = \mathbb{Q}(\langle 3, 2\rangle) = \mathbb{Q}(\langle 3, 4\rangle) = \mathbb{Q}(\langle 3, 8\rangle)$$

and

$$\min(\langle 6, 1\rangle, \mathbb{Q}) = (x - \langle 6, 1\rangle)(x - \langle 6, 2\rangle)$$
$$\min(\langle 3, 1\rangle, \mathbb{Q}) = (x - \langle 3, 1\rangle)(x - \langle 3, 2\rangle)(x - \langle 3, 4\rangle)(x - \langle 3, 8\rangle).$$

We have from Theorem 13.7 that

$$\min(\langle 3, 1\rangle, K_6) = (x - \langle 3, 1\rangle)(x - \langle 3, 4\rangle).$$

In order to solve a polynomial such as $\min(\langle 3,1\rangle, K_6)$ by radicals over K_6, we need to express its coefficients explicitly as elements of K_6. We have already noted that $\langle 3,1\rangle + \langle 3,4\rangle = \langle 6,1\rangle$. Using the results of Example 13.5, it is easy to show that $\langle 3,1\rangle\langle 3,4\rangle = \langle 6,2\rangle + 2$. In general, computing sums of periods is relatively straightforward, but finding products of periods can be laborious. In Theorem 13.9, we provide a method that converts products into sums. ◊

For purposes of computing with periods of roots of unity, it is convenient to introduce cyclic groups generated by powers of g:

$$C_b = \langle g^a \rangle = \{g^{ja} : j = 0, 1, 2, \ldots, b-1\}.$$

In this notation, (13.5) becomes

$$\langle b, m\rangle = \sum_{k \in C_b} \zeta^{km}.$$

An important observation is that if n is in mC_b (equivalently, if $nC_b = mC_b$), then

$$\langle b, n\rangle = \sum_{k \in C_b} \zeta^{kn} = \sum_{k \in nC_b} \zeta^{k} = \sum_{k \in mC_b} \zeta^{k} = \sum_{k \in C_b} \zeta^{km} = \langle b, m\rangle. \tag{13.15}$$

This identity simply says that when computing a period, we are free to start the sum with any element in the relevant coset and then sequentially add further terms.

The next two results provide helpful tools for performing calculations with periods of roots of unity.

Theorem 13.9. For all r and s in $\mathbb{F}_p^\times$,

$$\langle b, r\rangle\langle b, s\rangle = \sum_{k \in C_b} \langle b, kr + s\rangle$$

where $kr + s$ is taken modulo p.

Proof. By definition,

$$\langle b, r\rangle = \sum_{k \in C_b} \zeta^{kr} \quad \text{and} \quad \langle b, s\rangle = \sum_{l \in C_b} \zeta^{ls}.$$

Since l is in C_b, we have $lrC_b = rC_b$. It follows from (13.15) that $\langle b, lr\rangle = \langle b, r\rangle$, so

$$\begin{aligned}\langle b, r\rangle\langle b, s\rangle &= \sum_{l\in C_b}\langle b, lr\rangle\zeta^{ls} = \sum_{l\in C_b}\Bigg(\sum_{k\in C_b}\zeta^{klr}\zeta^{ls}\Bigg)\\ &= \sum_{k\in C_b}\Bigg(\sum_{l\in C_b}\zeta^{l(kr+s)}\Bigg) = \sum_{k\in C_b}\langle b, kr+s\rangle.\end{aligned}$$

□

We will see numerous applications of Theorem 13.9 in the examples to follow.

Theorem 13.10.

$$\langle 2, g^k\rangle = \zeta^{g^k} + \zeta^{g^{k+(p-1)/2}} = 2\,\mathrm{Re}(\zeta^{g^k})$$

for $k = 0, 1, \ldots, (p-3)/2$.

Proof. The first identity follows from the definition of periods of 2 terms. By Theorem E.6,

$$g^{k+(p-1)/2} \equiv g^k g^{(p-1)/2} \equiv -g^k \pmod{p}$$

hence

$$\zeta^{g^{k+(p-1)/2}} = \zeta^{-g^k}$$

The second identity now follows from (6.5). □

To illustrate Theorem 13.10, let $p = 13$ and $g = 2$. We have from Example 13.5 that

$$\begin{aligned}\langle 2, 2^0\rangle &= \langle 2, 1\rangle = 2\ \mathrm{Re}(\zeta_{13})\\ \langle 2, 2^1\rangle &= \langle 2, 2\rangle = 2\ \mathrm{Re}(\zeta_{13}^2)\\ \langle 2, 2^2\rangle &= \langle 2, 4\rangle = 2\ \mathrm{Re}(\zeta_{13}^4)\end{aligned}$$

and so on.

The remainder of the chapter is devoted to illustrating the above theory with three extensive examples. We know from Theorem 10.16 that $\mathbb{Q}(\zeta_p)$ is an irreducible radical extension of $\mathbb{Q}$ if and only if p is a Fermat prime. Recall that the first three (of the five known) Fermat primes are 3, 5, and 17. Evidently, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ is an irreducible radical extension of $\mathbb{Q}$, and we saw

in Example 6.6 that the same is true of $\mathbb{Q}(\zeta_5)$. In Example 13.11, we explore $\mathbb{Q}(\zeta_5)$ as an extension of $\mathbb{Q}$, and also $\mathbb{Q}(\mu_4, \zeta_5)$ as an extension of $\mathbb{Q}(\mu_4)$. In Example 13.12, we investigate $\mathbb{Q}(\mu_{17})$ as an extension of $\mathbb{Q}$, culminating in Gauss's remarkable identity that expresses $\cos(2\pi/17) = \mathrm{Re}(\zeta_{17})$ in terms of radicals over $\mathbb{Q}$. In Example 13.13, we examine $\mathbb{Q}(\mu_6, \zeta_7)$ as an extension of $\mathbb{Q}(\mu_6)$.

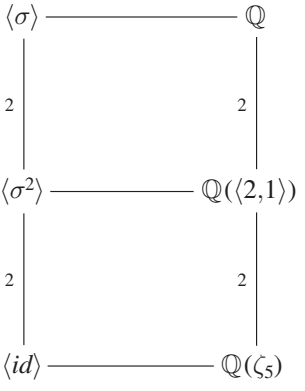
To avoid repetition, we state here that (13.6), (13.11), and (13.14), as well as Theorems 13.6, 13.7, 13.9, and 13.10 will be used repeatedly in what follows, but without further mention. Since the calculations involve something of a standard format, the style of presentation is rather abbreviated, with certain details omitted. We adopt the convention that the square root of a positive real number denotes the positive value.

Example 13.11 (5th root of unity). Let $p = 5$, $F = \mathbb{Q}$, and $K = \mathbb{Q}(\zeta_5)$. Recall from Example 6.8 that with $g = 2$, we have

k	0	1	2	3
$2^k \pmod 5$	1	2	4	3

Then $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(\zeta_5) = \zeta_5^2$.

Since $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ is of order 4, it follows from Theorems 13.2(b) and 13.3(c) that there is only one tower of fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$ consisting of prime binomial extensions. In each case, the prime is 2. The Galois correspondence is shown in the following figure.



The subgroups of C_4 are

$$\begin{aligned} C_4 &= \langle 2 \rangle = \{1, 2, 4, 3\} \\ C_2 &= \langle 2^2 \rangle = \{1, 4\} \\ C_1 &= \langle 2^4 \rangle = \{1\}. \end{aligned}$$

Step 1. Calculate $\langle 2, 1 \rangle$.
The cosets of C_2 in C_4 are

$$C_2 = \{1, 4\} \quad \text{and} \quad 2C_2 = \{2, 3\}$$

and the periods of 2 terms are

$$\langle 2, 1 \rangle = \zeta_5 + \zeta_5^4 \quad \text{and} \quad \langle 2, 2 \rangle = \zeta_5^2 + \zeta_5^3.$$

Then

$$\langle 2, 1 \rangle + \langle 2, 2 \rangle = -1$$

and

$$\begin{aligned} \langle 2, 1 \rangle \langle 2, 2 \rangle &= \sum_{k \in C_2} \langle 2, k + 2 \rangle = \langle 2, 3 \rangle + \langle 2, 6 \rangle \\ &= \langle 2, 2 \rangle + \langle 2, 1 \rangle = -1. \end{aligned}$$

In the preceding calculation, the identity $\langle 2, 3 \rangle = \langle 2, 2 \rangle$ follows from 2 and 3 being in the same coset, and the identity $\langle 2, 6 \rangle = \langle 2, 1 \rangle$ results from the congruence $6 \equiv 1 \pmod 5$. We have

$$\begin{aligned} \min(\langle 2, 1 \rangle, \mathbb{Q}) &= (x - \langle 2, 1 \rangle)(x - \langle 2, 2 \rangle) \\ &= x^2 + x - 1. \end{aligned} \tag{13.16}$$

Note that (13.16) is the same as (6.7) in Example 6.6.

Since $\langle 2, 1 \rangle = 2 \operatorname{Re}(\zeta_5)$ and $\langle 2, 2 \rangle = 2 \operatorname{Re}(\zeta_5^2)$, we can use their numerical values to determine the signs of certain square roots. In this way, we find that

$$\langle 2, 1 \rangle, \langle 2, 2 \rangle = \frac{-1 \pm \sqrt{5}}{2}.$$

This method of determining signs of square roots will be used throughout.

It was claimed in Example 8.16 that there is precisely one field strictly between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$, namely, $\mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}(\zeta_5^2 + \zeta_5^3)$. We now see that this claim was well founded.

Step 2. Calculate ζ_5.
The periods of 1 term needed to calculate ζ_5 are

$$\langle 1,1\rangle = \zeta_5 \quad \text{and} \quad \langle 1,4\rangle = \zeta_5^4.$$

Then

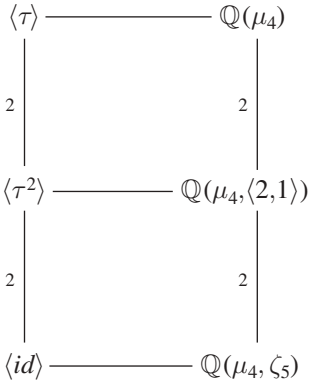
$$\begin{aligned}\min(\zeta_5, \mathbb{Q}(\langle 2,1\rangle)) &= (x - \langle 1,1\rangle)(x - \langle 1,4\rangle)\\ &= x^2 - \langle 2,1\rangle x + 1\\ &= x^2 + \left(\frac{1-\sqrt{5}}{2}\right)x + 1.\end{aligned}$$

The same calculations that were performed in Example 6.6 now lead to the explicit expressions for ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4 given in (6.8).

We next explore $\mathbb{Q}(\mu_4, \zeta_5)$ as an extension of $\mathbb{Q}(\mu_4)$. By Theorems 5.5(d) and 10.14(e),

$$\mathrm{Gal}(\mathbb{Q}(\mu_4, \zeta_5)/\mathbb{Q}(\mu_4)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}).$$

Let $\mathrm{Gal}(\mathbb{Q}(\mu_4, \zeta_5)/\mathbb{Q}(\mu_4)) = \langle\tau\rangle$, where $\tau(\zeta_5) = \zeta_5^2$. The Galois correspondence is shown in the following figure.



We return to the issue discussed in the introduction to this chapter, and seek to replace $\langle 2,1\rangle$ and $\langle 1,1\rangle$ with Lagrange resolvents so as to exhibit $\mathbb{Q}(\mu_4, \zeta_5)$ as an irreducible radical extension of $\mathbb{Q}(\mu_4)$. Ordinarily, Theorems 10.5 and 10.6 offer distinct computational approaches. However, the extensions being considered here are of degree 2, so the results are the same.

With $p = 2$, the primitive root of unity is -1. Since

$$\begin{aligned}&\mathrm{Gal}(\mathbb{Q}(\mu_4, \langle 2,1\rangle)/\mathbb{Q}(\mu_4))\\ &\quad\cong \mathrm{Gal}(\mathbb{Q}(\mu_4, \zeta_5)/\mathbb{Q}(\mu_4))/\mathrm{Gal}(\mathbb{Q}(\mu_4, \zeta_5)/\mathbb{Q}(\mu_4, \langle 2,1\rangle))\\ &\quad= \langle\tau\rangle/\langle\tau^2\rangle = \langle\tau\langle\tau^2\rangle\rangle\end{aligned}$$

and

$$\mathrm{Gal}(\mathbb{Q}(\mu_4, \zeta_5)/\mathbb{Q}(\mu_4, \langle 2, 1\rangle) = \langle \tau^2 \rangle$$

the corresponding Lagrange resolvents are

$$\begin{aligned}\beta_1 = (-1, \langle 2, 1\rangle) &= \langle 2, 1\rangle + (-1)\tau(\langle 2, 1\rangle) = \langle 2, 1\rangle - \langle 2, 2\rangle \\ &= (\zeta_5 + \zeta_5^4) - (\zeta_5^2 + \zeta_5^3)\end{aligned}$$

and

$$\begin{aligned}\beta_2 = (-1, \langle 1, 1\rangle) &= \langle 1, 1\rangle + (-1)\tau^2(\langle 1, 1\rangle) = \langle 1, 1\rangle - \langle 1, 4\rangle \\ &= \zeta_5 - \zeta_5^4.\end{aligned}$$

We have from (6.8) that

$$\beta_1 = \sqrt{5} \quad \text{and} \quad \beta_2 = \frac{i\sqrt{10 + 2\sqrt{5}}}{2}.$$

Note that β_1^2 is in $\mathbb{Q}(\mu_4) = \mathbb{Q}(i)$ and β_2^2 is in $\mathbb{Q}(\mu_4, \beta_1)$, as expected. Then

$$\mathbb{Q}(\mu_4) \subset \mathbb{Q}(\mu_4, \sqrt{5}) \subset \mathbb{Q}\left(\mu_4, \sqrt{10 + 2\sqrt{5}}\right) = \mathbb{Q}(\mu_4, \zeta_5) \tag{13.17}$$

is a tower of irreducible binomial extensions from $\mathbb{Q}(\mu_4)$ to $\mathbb{Q}(\mu_4, \zeta_5)$. We see that (13.17) is identical to (6.14). ◊

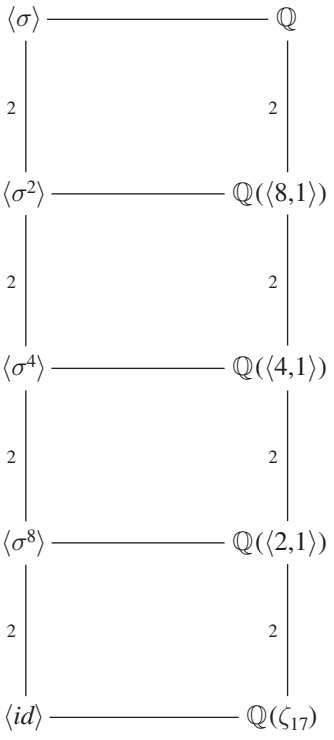
Example 13.12 (17th root of unity). Let $p = 17$, $F = \mathbb{Q}$, and $K = \mathbb{Q}(\zeta_{17})$. The primitive congruence roots modulo 17 are 3, 5, 6, 7, 10, 11, 12, and 14. Taking $g = 3$, we have

k	0	1	2	3	4	5	6	7
$3^k \pmod{17}$	1	3	9	10	13	5	15	11

8	9	10	11	12	13	14	15
16	14	8	7	4	12	2	6

Then $\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) = \langle \sigma \rangle$, where $\sigma(\zeta_{17}) = \zeta_{17}^3$.

Similar to Example 13.11, since $\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q})$ is of order 16, by Theorems 13.2(b) and 13.3(c), there is only one tower of fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{17})$ consisting of prime binomial extensions. Once again, in each instance, the prime is 2. The Galois correspondence is shown in the following figure.



The subgroups of C_{16} are

$$\begin{aligned} C_{16} &= \langle 3\rangle = \{1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6\} \\ C_8 &= \langle 3^2\rangle = \{1,9,13,15,16,8,4,2\} \\ C_4 &= \langle 3^4\rangle = \{1,13,16,4\} \\ C_2 &= \langle 3^8\rangle = \{1,16\} \\ C_1 &= \langle 3^{16}\rangle = \{1\}. \end{aligned}$$

Step 1. Calculate $\langle 8,1\rangle$ and $\langle 8,3\rangle$.
The cosets of C_8 in C_{16} are

$$C_8 = \{1,9,13,15,16,8,4,2\} \quad \text{and} \quad 3C_8 = \{3,10,5,11,14,7,12,6\}$$

and the periods of 8 terms are

$$\langle 8,1\rangle = \zeta_{17} + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16} + \zeta_{17}^8 + \zeta_{17}^4 + \zeta_{17}^2$$

and

$$\langle 8,3\rangle = \zeta_{17}^3 + \zeta_{17}^{10} + \zeta_{17}^5 + \zeta_{17}^{11} + \zeta_{17}^{14} + \zeta_{17}^7 + \zeta_{17}^{12} + \zeta_{17}^6.$$

Then

$$\begin{aligned}
\langle 8,1\rangle + \langle 8,3\rangle &= -1 \\
\langle 8,1\rangle\langle 8,3\rangle &= \sum_{k\in C_8} \langle 8, k+3\rangle \\
&= \langle 8,4\rangle + \langle 8,12\rangle + \langle 8,16\rangle + \langle 8,1\rangle \\
&\quad + \langle 8,2\rangle + \langle 8,11\rangle + \langle 8,7\rangle + \langle 8,5\rangle \\
&= \langle 8,1\rangle + \langle 8,3\rangle + \langle 8,1\rangle + \langle 8,1\rangle \\
&\quad + \langle 8,1\rangle + \langle 8,3\rangle + \langle 8,3\rangle + \langle 8,3\rangle \\
&= 4[\langle 8,1\rangle + \langle 8,3\rangle] = -4
\end{aligned}$$

and

$$\begin{aligned}
\min(\langle 8,1\rangle, \mathbb{Q}) &= (x - \langle 8,1\rangle)(x - \langle 8,3\rangle) \\
&= x^2 + x - 4.
\end{aligned}$$

Therefore,

$$\langle 8,1\rangle, \langle 8,3\rangle = \frac{-1 \pm \sqrt{17}}{2}.$$

Step 2. Calculate $\langle 4,1\rangle$ and $\langle 4,3\rangle$.
The cosets of C_4 in C_{16} are

$$C_4 = \{1,13,16,4\} \qquad 3C_4 = \{3,5,14,12\}$$

$$9C_4 = \{9,15,8,2\} \qquad 10C_4 = \{10,11,7,6\}$$

and the periods of 4 terms are

$$\langle 4,1\rangle = \zeta_{17} + \zeta_{17}^{13} + \zeta_{17}^{16} + \zeta_{17}^4 \qquad \langle 4,3\rangle = \zeta_{17}^3 + \zeta_{17}^5 + \zeta_{17}^{14} + \zeta_{17}^{12}$$

$$\langle 4,9\rangle = \zeta_{17}^9 + \zeta_{17}^{15} + \zeta_{17}^8 + \zeta_{17}^2 \qquad \langle 4,10\rangle = \zeta_{17}^{10} + \zeta_{17}^{11} + \zeta_{17}^7 + \zeta_{17}^6.$$

Then

$$\begin{aligned}
\langle 4,1\rangle + \langle 4,9\rangle &= \langle 8,1\rangle \\
\langle 4,1\rangle\langle 4,9\rangle &= \sum_{k\in C_4} \langle 4, k+9\rangle \\
&= \langle 4,10\rangle + \langle 4,5\rangle + \langle 4,8\rangle + \langle 4,13\rangle \\
&= \langle 4,3^3\rangle + \langle 4,3\rangle + \langle 4,3^2\rangle + \langle 4,1\rangle = -1
\end{aligned}$$

and

$$\begin{aligned}\min(\langle 4,1\rangle, \mathbb{Q}(\langle 8,1\rangle)) &= (x - \langle 4,1\rangle)(x - \langle 4,9\rangle)\\ &= x^2 - \langle 8,1\rangle x - 1.\end{aligned}$$

Therefore,

$$\langle 4,1\rangle = \frac{\langle 8,1\rangle + \sqrt{\langle 8,1\rangle^2 + 4}}{2} = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4}. \tag{13.18}$$

Similarly,

$$\langle 4,3\rangle + \langle 4,10\rangle = \langle 8,3\rangle \qquad \langle 4,3\rangle\langle 4,10\rangle = -1$$

$$\begin{aligned}\min(\langle 4,3\rangle, \mathbb{Q}(\langle 8,1\rangle)) &= (x - \langle 4,3\rangle)(x - \langle 4,10\rangle)\\ &= x^2 - \langle 8,3\rangle x - 1\end{aligned}$$

and

$$\langle 4,3\rangle = \frac{\langle 8,3\rangle + \sqrt{\langle 8,3\rangle^2 + 4}}{2} = \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4}.$$

Step 3. Calculate $\langle 2,1\rangle$.
The cosets of C_2 in C_{16} are

$$\begin{array}{llll} C_2 = \{1,16\} & 3C_2 = \{3,14\} & 9C_2 = \{9,8\} & 10C_2 = \{10,7\}\\ 13C_2 = \{13,4\} & 5C_2 = \{5,12\} & 15C_2 = \{15,2\} & 11C_2 = \{11,6\}\end{array}$$

and the periods of 2 terms needed to calculate $\langle 2,1\rangle$ are

$$\begin{aligned}\langle 2,1\rangle &= \zeta_{17} + \zeta_{17}^{16} & \langle 2,3\rangle &= \zeta_{17}^{3} + \zeta_{17}^{14}\\ \langle 2,13\rangle &= \zeta_{17}^{13} + \zeta_{17}^{4} & \langle 2,5\rangle &= \zeta_{17}^{5} + \zeta_{17}^{12}.\end{aligned}$$

Then

$$\begin{aligned}\langle 2,1\rangle + \langle 2,13\rangle &= \langle 4,1\rangle\\ \langle 2,1\rangle\langle 2,13\rangle = \sum_{k\in C_2}\langle 2,k+13\rangle &= \langle 2,14\rangle + \langle 2,12\rangle\\ &= \langle 2,3\rangle + \langle 2,5\rangle = \langle 4,3\rangle\end{aligned}$$

and

$$\begin{aligned}\min(\langle 2,1\rangle, \mathbb{Q}(\langle 4,1\rangle)) &= (x - \langle 2,1\rangle)(x - \langle 2,13\rangle)\\ &= x^2 - \langle 4,1\rangle x + \langle 4,3\rangle.\end{aligned}$$

Therefore,

$$\langle 2,1\rangle = \frac{\langle 4,1\rangle + \sqrt{\langle 4,1\rangle^2 - 4\langle 4,3\rangle}}{2} \tag{13.19}$$

where

$$\langle 4,1\rangle^2 - 4\langle 4,3\rangle = \frac{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}{4}. \tag{13.20}$$

Step 4. Calculate ζ_{17} and $\cos(2\pi/17)$.
The periods of 1 term needed to calculate ζ_{17} are

$$\langle 1,1\rangle = \zeta_{17} \quad \text{and} \quad \langle 1,16\rangle = \zeta_{17}^{16}.$$

Then

$$\langle 1,1\rangle + \langle 1,16\rangle = \langle 2,1\rangle \qquad \langle 1,1\rangle\langle 1,16\rangle = 1$$

and

$$\begin{aligned}\min(\zeta_{17}, \mathbb{Q}(\langle 2,1\rangle)) &= (x - \langle 1,1\rangle)(x - \langle 1,16\rangle) \\ &= x^2 - \langle 2,1\rangle x + 1.\end{aligned}$$

Therefore,

$$\zeta_{17} = \frac{\langle 2,1\rangle + i\sqrt{4 - \langle 2,1\rangle^2}}{2}$$

hence

$$\cos\left(\frac{2\pi}{17}\right) = \frac{\langle 2,1\rangle}{2}.$$

Making the various substitutions using (13.18)–(13.20), we obtain Gauss's celebrated identity:

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right).$$

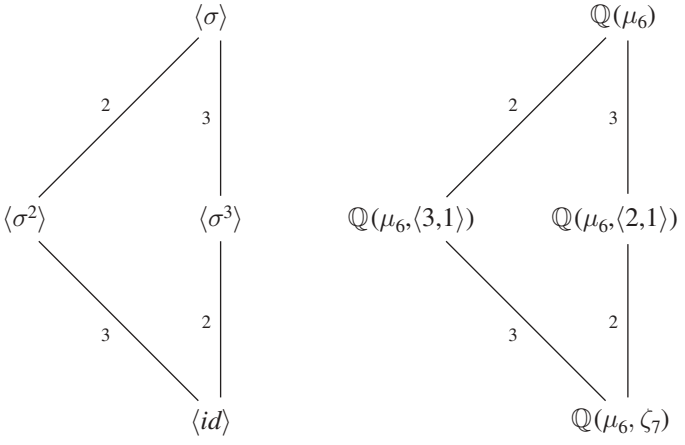
$\Diamond$

Example 13.13 (7th root of unity). Let $p = 7$, $F = \mathbb{Q}(\mu_6)$, and $K = \mathbb{Q}(\mu_6, \zeta_7)$. Recall from Example 6.9 that with $g = 3$, we have

j	0	1	2	3	4	5
$3^j \pmod 7$	1	3	2	6	4	5

Then $\mathrm{Gal}(\mathbb{Q}(\mu_6, \zeta_7)/\mathbb{Q}(\mu_6)) = \langle \sigma \rangle$, where $\sigma(\zeta_7) = \zeta_7^3$.

Since $\mathrm{Gal}(\mathbb{Q}(\mu_6, \zeta_7)/\mathbb{Q}(\mu_6))$ is of order 6, by Theorems 13.2(b) and 13.3(c), there are precisely two towers of fields between $\mathbb{Q}(\mu_6)$ and $\mathbb{Q}(\mu_6, \zeta_7)$ consisting of prime binomial extensions. In one tower, the first extension is of degree 2, and the second is of degree 3, while in the other tower, the degrees are 3 and 2, respectively. This confirms an assertion made in Example 6.9 on the existence of such towers. The Galois correspondence is shown in the following figure.



In Example 6.9, we defined

$$\lambda = \zeta_7 - \omega\zeta_7^3 + \omega^2\zeta_7^2 - \zeta_7^6 + \omega\zeta_7^4 - \omega^2\zeta_7^5$$

and observed that $\mathbb{Q}(\mu_6, \zeta_7) = \mathbb{Q}(\mu_6, \lambda)$, and that

$$\lambda^6 = \frac{-7(71 - 39i\sqrt{3})}{2}$$

is in $\mathbb{Q}(\mu_6)$. Since

$$[\mathbb{Q}(\mu_6, \lambda^2) : \mathbb{Q}(\mu_6)] = 3 \quad \text{and} \quad [\mathbb{Q}(\mu_6, \lambda^3) : \mathbb{Q}(\mu_6)] = 2$$

it follows that

$$\mathbb{Q}(\mu_6, \lambda^2) = \mathbb{Q}(\mu_6, \langle 2, 1 \rangle) \quad \text{and} \quad \mathbb{Q}(\mu_6, \lambda^3) = \mathbb{Q}(\mu_6, \langle 3, 1 \rangle).$$

In relation to the above diagram, (6.15) and (6.16) correspond to the paths from $\mathbb{Q}(\mu_6)$ to $\mathbb{Q}(\mu_6, \zeta_7)$ through $\mathbb{Q}(\mu_6, \langle 2, 1\rangle)$ and $\mathbb{Q}(\mu_6, \langle 3, 1\rangle)$, respectively. For the present example, we choose the latter route. This means that the calculations to follow involve solving a quadratic polynomial and then a cubic polynomial. The calculations corresponding to the alternate route are given in Example 9.2.2 of Cox (2012). That approach requires solving a cubic polynomial and then a quadratic polynomial. In fact, the cubic polynomial is precisely (10.3).

Using the methods of Example 14.4, it can be shown that

$$\lambda^3 = \frac{\sqrt{7}(3\sqrt{3} + 13i)}{2}.$$

Since $(i\sqrt{3})(i\sqrt{7}) = -\sqrt{3}\sqrt{7}$, we anticipate that $i\sqrt{7}$ will make an appearance in the calculations leading to $\mathbb{Q}(\mu_6, \langle 3, 1\rangle)$.

Step 1. Calculate $\langle 3, 1\rangle$.
The 2 periods of 3 terms are

$$\langle 3, 1\rangle = \zeta_7 + \zeta_7^2 + \zeta_7^4 \quad \text{and} \quad \langle 3, 3\rangle = \zeta_7^3 + \zeta_7^6 + \zeta_7^5.$$

Then

$$\langle 3, 1\rangle + \langle 3, 3\rangle = -1 \qquad \langle 3, 1\rangle\langle 3, 3\rangle = 2$$

and

$$\begin{aligned}\min(\langle 3, 1\rangle, \mathbb{Q}(\mu_6)) &= (x - \langle 3, 1\rangle)(x - \langle 3, 3\rangle) \\ &= x^2 + x + 2.\end{aligned}$$

Therefore,

$$\langle 3, 1\rangle, \langle 3, 3\rangle = \frac{-1 \pm i\sqrt{7}}{2}.$$

Step 2. Calculate ζ_7.
The periods of 1 term needed to calculate ζ_7 are

$$\langle 1, 1\rangle = \zeta_7 \qquad \langle 1, 2\rangle = \zeta_7^2 \quad \text{and} \quad \langle 1, 4\rangle = \zeta_7^4.$$

Then

$$\begin{aligned}\langle 1, 1\rangle + \langle 1, 2\rangle + \langle 1, 4\rangle &= \langle 3, 1\rangle \\ \langle 1, 1\rangle\langle 1, 2\rangle + \langle 1, 1\rangle\langle 1, 4\rangle + \langle 1, 2\rangle\langle 1, 4\rangle &= \langle 3, 3\rangle \\ \langle 1, 1\rangle\langle 1, 2\rangle\langle 1, 4\rangle &= 1\end{aligned}$$

hence

$$\begin{aligned}\min(\zeta_7, \mathbb{Q}(\mu_6, \langle 3,1\rangle)) &= (x - \langle 1,1\rangle)(x - \langle 1,2\rangle)(x - \langle 1,4\rangle)\\ &= x^3 - \langle 3,1\rangle x^2 + \langle 3,3\rangle x - 1\\ &= x^3 + \left(\frac{1 - i\sqrt{7}}{2}\right)x^2 + \left(\frac{-1 - i\sqrt{7}}{2}\right)x - 1.\end{aligned}$$

The corresponding reduced polynomial is

$$g(y) = y^3 + \left(\frac{-i\sqrt{7}}{3}\right)y + \left(\frac{-14 + i\sqrt{7}}{27}\right).$$

Using Cardan's formulas, and in the notation of Section 1.2, we find that

$$\zeta_7 = \frac{-1 + i\sqrt{7}}{6} + \frac{\lambda_1 + \lambda_2}{3}$$

where

$$\lambda_1 = \sqrt[3]{\frac{14 + 3\sqrt{3}\sqrt{7} - i\sqrt{7}}{2}}$$

and

$$\lambda_2 = \omega\sqrt[3]{\frac{14 - 3\sqrt{3}\sqrt{7} - i\sqrt{7}}{2}}$$

and where, as usual, $\omega = (-1 + i\sqrt{3})/2$. As required by (1.12), the values of λ_1 and λ_2 are chosen so that $\lambda_1\lambda_2 = i\sqrt{7}$. ◊

CHAPTER 14

DENESTING RADICALS

Let $F(\alpha, \beta)$ be an irreducible radical extension of F such that

$$F \subset F(\alpha) \subset F(\alpha, \beta)$$

where $F(\alpha)$ is an irreducible binomial extension of F of degree $m > 1$, with α^m in F, and where $F(\alpha, \beta)$ is an irreducible binomial extension of $F(\alpha)$ of degree $n > 1$, with β^n in $F(\alpha)$. Let $\alpha^m = c$, and let $\beta^n = g(\alpha)$ for some $g(x)$ in $F[x]$. Then $\alpha = \sqrt[m]{c}$ and

$$\beta = \sqrt[n]{g(\sqrt[m]{c})}. \tag{14.1}$$

In (14.1) the radicals are *nested* in an obvious sense of the word. Under certain circumstances the number of levels of nesting can be reduced, in which case we say that the expression has been *denested*.

Identities (14.2)–(14.7) illustrate some of the diverse ways in which denesting can occur. Here and in what follows, we adopt the convention that the square root, cube root, etc., of a positive real number denotes the positive value.

$$\sqrt{5 + 2\sqrt{6}} = \sqrt{2} + \sqrt{3} = \frac{3 + \sqrt{6}}{\sqrt{3}} \tag{14.2}$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

$$\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}} = \sqrt{5}+\sqrt{11-2\sqrt{29}}$$
$$= \frac{5+\sqrt{55-10\sqrt{29}}}{\sqrt{5}} \tag{14.3}$$

$$\sqrt[3]{-1+\sqrt[3]{2}} = \frac{1-\sqrt[3]{2}+(\sqrt[3]{2})^2}{\sqrt[3]{9}} \tag{14.4}$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}}{3} \tag{14.5}$$

$$\sqrt[6]{7\sqrt[3]{20}-19} = \frac{\sqrt[3]{5}-\sqrt[3]{2}}{\sqrt[3]{3}} \tag{14.6}$$

$$\sqrt[4]{\frac{3+2\sqrt[4]{5}}{3-2\sqrt[4]{5}}} = \frac{\sqrt[4]{5}+1}{\sqrt[4]{5}-1} \tag{14.7}$$

Continuing with the above notation, we say that β has a *Zippel denesting* over F if there is an irreducible binomial extension $F(\gamma)$ of F of degree n, with γ^n in F, such that β is in $F(\alpha,\gamma)$. Setting $\gamma^n = e$, we have

$$\beta = h(\sqrt[m]{c}, \sqrt[n]{e})$$

for some $h(x,y)$ in $F[x,y]$. Thus, β has been denested.

Using the following table, it is readily verified that the left-hand sides of (14.2)–(14.4) have Zippel denestings. We make the further observation that in each case, $\gamma\beta$ is in $F(\alpha)$. As we now show, provided that F contains a primitive nth root of unity, this feature completely characterizes Zippel denestings.

Identity	F	α	β	γ
(14.2)	$\mathbb{Q}$	$\sqrt{6}$	$\sqrt{5+2\sqrt{6}}$	$\sqrt{3}$
(14.3)	$\mathbb{Q}(\sqrt{29})$	$\sqrt{55-10\sqrt{29}}$	$\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}}$	$\sqrt{5}$
(14.4)	$\mathbb{Q}$	$\sqrt[3]{2}$	$\sqrt[3]{-1+\sqrt[3]{2}}$	$\sqrt[3]{9}$

Theorem 14.1 (Zippel-Landau). Let L be an extension of F, let $L(\beta)$ be an irreducible binomial extension of L of degree n, with β^n in L, and let K be an extension of F of degree n. Suppose that F contains a primitive nth root of unity. Then the following are equivalent:

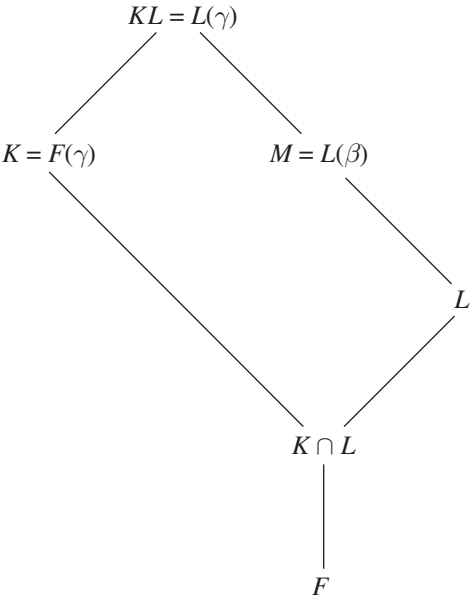
(a) There is an element γ in K such that $K = F(\gamma)$, γ^n is in F, and β is in $L(\gamma)$.

(b) There is an element ϕ in K such that $K = F(\phi)$, ϕ^n is in F, and $\phi\beta$ is in L.

In this case, $F(\gamma) \cap L = F$ and $L(\gamma) = L(\beta)$.

Proof. The result is trivial for $n = 1$. Suppose that $n > 1$.

(a)⇒(b): Let $M = L(\beta)$. By assumption, β is in $L(\gamma)$, hence $M \subseteq KL = L(\gamma)$.



Since F contains a primitive nth root of unity, K is the splitting field of $x^n - \gamma^n$ over F. By the TNI,

$$[KL : M][M : L] = [KL : L] = [K : K \cap L] = \frac{[K : F]}{[K \cap L : F]}.$$

Then $[M : L] = n = [K : F]$ implies that $K \cap L = F$ and $KL = M$, that is, $F(\gamma) \cap L = F$ and $L(\gamma) = L(\beta)$.

Since M is an irreducible binomial extension of L of degree n, and L contains a primitive nth root of unity, by Theorem 10.7, $\mathrm{Gal}(M/L)$ is cyclic of order

n. Then $\mathrm{Gal}(M/L) = \langle\sigma\rangle$ for some σ in $\mathrm{Gal}(M/L)$, with $\mathrm{ord}(\sigma) = n$. Since $K \cap L = F$ and $KL = M$, it follows from the TNI that

$$\langle\sigma\rangle = \mathrm{Gal}(M/L) = \mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L) = \mathrm{Gal}(K/F) = \langle\sigma_{|K}\rangle.$$

Therefore, $\mathrm{ord}(\sigma) = \mathrm{ord}(\sigma_{|K})$.

Since $x^n - \beta^n$ is a polynomial in $L[x]$, $\sigma(\beta)$ is a root of $x^n - \beta^n$, hence $\sigma(\beta) = \zeta\beta$, where ζ is an nth root of unity in F. Then $\sigma^2(\beta) = \zeta^2\beta$, $\sigma^3(\beta) = \zeta^3\beta$, and so on. It follows that ζ is a primitive nth root of unity, otherwise $\mathrm{ord}(\sigma) < n$. Similarly, since $x^n - \gamma^n$ is a polynomial in $F[x]$, $\sigma_{|K}(\gamma) = \xi\gamma$, where ξ is also a primitive nth root of unity. Then $\xi = \zeta^k$ for some $1 \le k \le n-1$. As required by (5.4), k and n are relatively prime. By Theorem E.1, there are integers r and s such that $-rk + sn = 1$. Then

$$\sigma(\gamma^r\beta) = [\sigma_{|K}(\gamma)]^r\sigma(\beta) = (\xi\gamma)^r(\zeta\beta) = (\zeta^{rk}\gamma^r)(\zeta\beta) = \gamma^r\beta.$$

It follows from the FTGT that $\gamma^r\beta$ is in $M^{\mathrm{Gal}(M/L)} = L$.

Let $\phi = \gamma^r$. Evidently, $F(\phi) \subseteq F(\gamma)$ and ϕ^n is in F. Since

$$\gamma = (\gamma^r)^{-k}\gamma^{sn} = c\phi^{-k}$$

where $c = (\gamma^n)^s$ is in F, it follows that $F(\gamma) \subseteq F(\phi)$, hence $F(\phi) = F(\gamma)$.

(b)⇒(a): $[F(\phi) : F] = n > 1$ implies that $\phi \neq 0$. Let $\gamma = \phi$. Since $\gamma\beta$ is in L, β is in $L(\gamma)$. □

Returning to the notation in the introductory remarks to the chapter and setting $L = F(\alpha)$, we see that Theorem 14.1 gives necessary and sufficient conditions for β to have a Zippel denesting over F. We now apply this criterion to the quadratic case.

Theorem 14.2. Let a, b, and c be elements of F such that $\sqrt{c}$ is not in F and $\sqrt{a + b\sqrt{c}}$ is not in $F(\sqrt{c})$. Let $d = \sqrt{a^2 - b^2c}$. If d is in F and $\sqrt{(a+d)/2}$ and $\sqrt{(a-d)/2}$ are not in F, then $\sqrt{a + b\sqrt{c}}$ has a Zippel denesting over F. Specifically,

$$\sqrt{a + b\sqrt{c}} = \left(\pm\sqrt{\frac{a+d}{2}}\right) + \left(\pm\sqrt{\frac{a-d}{2}}\right) \tag{14.8}$$

for an appropriate choice of signs.

Proof. We have from Theorem 14.1 that $\sqrt{a + b\sqrt{c}}$ has a Zippel denesting over F if and only if $\sqrt{r}\sqrt{a + b\sqrt{c}}$ is in $F(\sqrt{c})$ for some element r in F such that $\sqrt{r}$ is not in F. This is equivalent to

$$\sqrt{a + b\sqrt{c}} = \frac{s + t\sqrt{c}}{\sqrt{r}}$$

for some s and t in F. Without loss of generality, we take $t = 1$:

$$\sqrt{a + b\sqrt{c}} = \frac{s + \sqrt{c}}{\sqrt{r}}. \tag{14.9}$$

To find expressions for r and s in terms of a, b, and c, we square both sides of (14.9) and treat the resulting equation

$$(ar - s^2 - c) + (br - 2s)\sqrt{c} = 0$$

like a polynomial identity in the "variable" $\sqrt{c}$. Setting the "coefficients" equal to zero, we obtain

$$ar - s^2 - c = 0 \tag{14.10}$$

and

$$br - 2s = 0. \tag{14.11}$$

Using (14.11) to eliminate s from (14.10), we find that

$$b^2r^2 - 4ar + 4c = 0$$

which has solutions

$$r = \frac{2(a \pm d)}{b^2} \tag{14.12}$$

where

$$d = \sqrt{a^2 - b^2c}. \tag{14.13}$$

We have from (14.12) that

$$\sqrt{r} = \frac{\pm\sqrt{2(a \pm d)}}{b} \tag{14.14}$$

and from (14.11) and (14.12) that

$$s = \frac{a \pm d}{b}. \tag{14.15}$$

It follows from (14.13) that

$$\sqrt{c} = \frac{\pm\sqrt{a^2 - d^2}}{b}. \tag{14.16}$$

Since d is in F, so are r and s, and since $\sqrt{2(a+d)}$ and $\sqrt{2(a-d)}$ are not in F, neither is $\sqrt{r}$. Substituting (14.14)–(14.16) into (14.9) gives (14.8). □

Example 14.3. Identity (14.2) is easily derived using Theorem 14.2. To derive identity (14.3), let $F = \mathbb{Q}(\sqrt{29})$, and let $a = 16 - 2\sqrt{29}$, $b = 2$, and $c = 55 - 10\sqrt{29}$. Then $\sqrt{c} = \sqrt{55 - 10\sqrt{29}}$ is not in F, $d = 2\sqrt{29} - 6$ is in F, and

$$\sqrt{\frac{a+d}{2}} = \sqrt{5} \quad \text{and} \quad \sqrt{\frac{a-d}{2}} = \sqrt{11 - 2\sqrt{29}}$$

are not in F. So, Theorem 14.2 applies, and we obtain identity (14.3). ◊

Example 14.4 (5th root of unity). In Example 6.8, we considered $\lambda^4 = -15 + 20i$ in $\mathbb{Q}(i)$. To find a denested expression for $\lambda^2 = \sqrt{-15 + 20i}$, let $F = \mathbb{Q}$, and let $a = -15$, $b = 20$, and $c = -1$. Then $\sqrt{c} = i$ is not in F, $d = 25$ is in F, and

$$\sqrt{\frac{a+d}{2}} = \sqrt{5} \quad \text{and} \quad \sqrt{\frac{a-d}{2}} = 2i\sqrt{5}$$

are not in F. We have from Theorem 14.2 that

$$\lambda^2 = -\sqrt{5}(1 + 2i)$$

after an appropriate choice of signs.

To find a denested expression for $\lambda = \sqrt{-\sqrt{5}(1+2i)}$, let $F = \mathbb{Q}(\sqrt{5})$, and let $a = -\sqrt{5}$, $b = -2\sqrt{5}$, and $c = -1$. Then $\sqrt{c} = i$ is not in F, $d = 5$ is in F, and

$$\sqrt{\frac{a+d}{2}} = \frac{\sqrt{10 - 2\sqrt{5}}}{2} \quad \text{and} \quad \sqrt{\frac{a-d}{2}} = i\frac{\sqrt{10 + 2\sqrt{5}}}{2}$$

are not in F. We find from Theorem 14.2 that

$$\lambda = \frac{-\sqrt{10 - 2\sqrt{5}}}{2} + i\frac{\sqrt{10 + 2\sqrt{5}}}{2}$$

after choosing signs appropriately. ◊

CHAPTER 15

CLASSICAL FORMULAS REVISITED

In this chapter, we return to the theme of Chapter 1 and use Galois theory to derive "formulas" for solving quadratic, cubic, and quartic general polynomials by radicals over an arbitrary field. A large part of the work involved is finding explicit expressions for certain Lagrange resolvents. For this purpose, frequent use is made of Theorems 10.1 and 10.2. Recall the notation and definitions presented in (7.1)–(7.7): F is a field, $f(x)$ in $F[x]$ is the general polynomial of degree n over the subfield E of F, the roots of $f(x)$ are $t_1, t_2, \ldots, t_n$, and $K = F(t_1, t_2, \ldots, t_n)$ is the splitting field of $f(x)$ over F. In what follows, we assume for convenience that S_n acts on $\{1, 2, \ldots, n\}$. For brevity, the details of certain calculations have been omitted.

15.1 GENERAL QUADRATIC POLYNOMIAL

Let E be an arbitrary field, and let $F = E(s_1, s_2)$ and $K = F(t_1, t_2)$. The general quadratic polynomial over E is

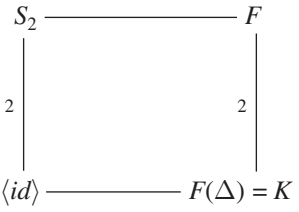
$$f(x) = x^2 - s_1 x + s_2 = (x - t_1)(x - t_2).$$

The only solvable series for S_2 is

$$\langle id \rangle \lhd S_2 = \langle (1\ 2) \rangle.$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

We consider the following Galois correspondence.



By definition, $\Delta = t_1 - t_2$. It is instructive to go through the formality of demonstrating what we already know to be true from earlier chapters, namely, that $K = F(\Delta)$ and Δ^2 is in F.

Consider

$$\mathrm{Gal}(K/F) = S_2 = \langle (1\ 2) \rangle$$

and let $\rho = (1\ 2)$. Since -1 is the primitive quadratic root of unity, we have

$$(-1, \Delta) = \Delta + (-1)\rho(\Delta) = 2\Delta.$$

By Theorems 10.1(b) and 10.2(b), $K = F(\Delta)$ and Δ^2 is in F. The latter result also follows from $\Delta^2 = s_1^2 - 4s_2$. The roots of $x^2 - \Delta^2$, which are Δ and $-\Delta$, are algebraically indistinguishable. As we see shortly, both appear in the formulas for t_1 and t_2. Switching Δ for $-\Delta$ merely interchanges the expressions for t_1 and t_2.

We have the following Lagrange resolvents:

$$\begin{aligned}
(1, t_1) &= t_1 + \rho(t_1) = t_1 + t_2 = s_1 \\
(-1, t_1) &= t_1 + (-1)\rho(t_1) = t_1 - t_2 = \Delta \\
(1, t_2) &= t_2 + \rho(t_2) = t_2 + t_1 = s_1 \\
(-1, t_2) &= t_2 + (-1)\rho(t_2) = t_2 - t_1 = -\Delta.
\end{aligned}$$

By Theorem 10.2(a),

$$t_1 = \frac{(1, t_1) + (-1, t_1)}{2} = \frac{s_1 + \Delta}{2} = \frac{s_1 + \sqrt{s_1^2 - 4s_2}}{2}$$

$$t_2 = \frac{(1, t_2) + (-1, t_2)}{2} = \frac{s_1 - \Delta}{2} = \frac{s_1 - \sqrt{s_1^2 - 4s_2}}{2}$$

or more succinctly,

$$t_1, t_2 = \frac{s_1 \pm \sqrt{s_1^2 - 4s_2}}{2}.$$

Setting $a = s_1$ and $b = s_2$ gives the quadratic formula (1.3).

15.2 GENERAL CUBIC POLYNOMIAL

Let E be an arbitrary field containing ω, the primitive cube root of unity as defined in (1.13), and let $F = E(s_1, s_2, s_3)$ and $K = F(t_1, t_2, t_3)$. The general cubic polynomial over E is

$$\begin{aligned} f(x) &= x^3 - s_1x^2 + s_2x - s_3 \\ &= (x - t_1)(x - t_2)(x - t_3). \end{aligned}$$

The only solvable series for S_3 is

$$\langle id \rangle \lhd A_3 \lhd S_3$$

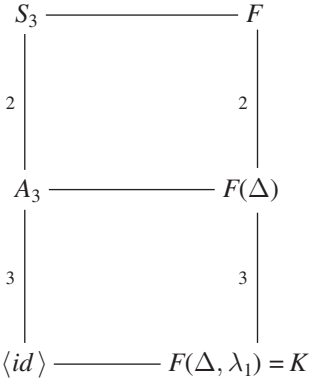
where

$$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

and

$$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle.$$

We consider the following Galois correspondence, which appeared in somewhat modified form at the end of Chapter 7.



Step 1. Define Δ and show that $K^{A_3} = F(\Delta)$ and Δ^2 is in F.
By definition,

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_2 - t_3).$$

Since

$$\mathrm{Gal}(K^{A_3}/F) = \mathrm{Gal}(K^{A_3}/K^{S_3}) \cong S_3/A_3 \cong \langle (1\ 2) \rangle$$

an argument similar to the one used in Section 15.1 shows that $K^{A_3} = F(\Delta)$ and Δ^2 is in F. The latter result also follows from (3.19).

Step 2. Define λ_1 and show that $K = F(\Delta, \lambda_1)$ and λ_1^3 is in $F(\Delta)$.
To define λ_1, we need an element of K that is not fixed by A_3. Clearly, t_1 will serve this purpose. Consider

$$\mathrm{Gal}(K/K^{A_3}) = \mathrm{Gal}(K^{\langle id\rangle}/K^{A_3}) \cong A_3/\langle id\rangle \cong \langle (1\ 2\ 3)\rangle$$

and let $\rho = (1\ 2\ 3)$. Let

$$\begin{aligned}\lambda_1 &= t_1 + \omega t_2 + \omega^2 t_3 = (\omega, t_1)\\ \lambda_2 &= t_1 + \omega^2 t_2 + \omega t_3 = (\omega^2, t_1).\end{aligned}$$

It can be shown that

$$\lambda_1\lambda_2 = s_1^2 - 3s_2. \tag{15.1}$$

By Theorems 10.1(b) and 10.2(b), $K = F(\Delta, \lambda_1)$ and λ_1^3 is in $F(\Delta)$.

Since $\mathrm{Gal}(K/F(\lambda_1)) = \langle id\rangle$, the coset representatives of $\mathrm{Gal}(K/F(\lambda_1))$ in S_3 comprise all of S_3. It follows from

$$\begin{array}{lll} id\,\lambda_1 = \lambda_1 & (1\ 2)\lambda_1 = \omega\lambda_2 & (1\ 3)\lambda_1 = \omega^2\lambda_2 \\ (2\ 3)\lambda_1 = \lambda_2 & (1\ 2\ 3)\lambda_1 = \omega^2\lambda_1 & (1\ 3\ 2)\lambda_1 = \omega\lambda_1 \end{array}$$

and

$$\begin{aligned}(x-\lambda_1)(x-\omega\lambda_1)(x-\omega^2\lambda_1) &= x^3 - \lambda_1^3\\ (x-\lambda_2)(x-\omega\lambda_2)(x-\omega^2\lambda_2) &= x^3 - \lambda_2^3\end{aligned}$$

as well as Theorem 9.18, (15.1), and (15.4) to follow that

$$\begin{aligned}\min(\lambda_1, F) &= (x^3 - \lambda_1^3)(x^3 - \lambda_2^3)\\ &= x^6 - (\lambda_1^3 + \lambda_2^3)x^3 + (\lambda_1\lambda_2)^3\\ &= x^6 - (2s_1^3 - 9s_1s_2 + 27s_3)x^3 + (s_1^2 - 3s_2)^3. \end{aligned}\tag{15.2}$$

We seek explicit expressions for λ_1^3 and λ_2^3 as elements of $F(\Delta)$. It follows from

$$\begin{aligned}\lambda_1^3 - \lambda_2^3 &= (\lambda_1 - \lambda_2)(\lambda_1 - \omega\lambda_2)(\lambda_1 - \omega^2\lambda_2)\\ \lambda_1 - \lambda_2 &= (\omega - \omega^2)(t_2 - t_3)\\ \lambda_1 - \omega\lambda_2 &= (1-\omega)(t_1 - t_2)\\ \lambda_1 - \omega^2\lambda_2 &= (1-\omega^2)(t_1 - t_3)\end{aligned}$$

and

$$(\omega - \omega^2)(1 - \omega)(1 - \omega^2) = 3i\sqrt{3}$$

that

$$\lambda_1^3 - \lambda_2^3 = 3i\sqrt{3}\Delta \tag{15.3}$$

where we note that $i\sqrt{3}$ is in F. We have from

$$\lambda_1^3 + \lambda_2^3 = (\lambda_1 + \lambda_2)(\lambda_1 + \omega\lambda_2)(\lambda_1 + \omega^2\lambda_2)$$

and

$$\begin{aligned}\lambda_1 + \lambda_2 &= 3t_1 - s_1\\ \lambda_1 + \omega\lambda_2 &= \omega^2(3t_3 - s_1)\\ \lambda_1 + \omega^2\lambda_2 &= \omega(3t_2 - s_1)\end{aligned}$$

that

$$\lambda_1^3 + \lambda_2^3 = 2s_1^3 - 9s_1s_2 + 27s_3. \tag{15.4}$$

Combining (15.3) and (15.4) yields

$$\lambda_1^3, \lambda_2^3 = \frac{2s_1^3 - 9s_1s_2 + 27s_3 \pm 3i\sqrt{3}\Delta}{2} \tag{15.5}$$

hence

$$\lambda_1, \lambda_2 = \sqrt[3]{\frac{2s_1^3 - 9s_1s_2 + 27s_3 \pm 3i\sqrt{3}\Delta}{2}}$$

where λ_1 and λ_2 are chosen so that (15.1) is satisfied. Thus, (15.5) gives the desired expressions for expressions for λ_1^3 and λ_2^2.

Step 3. Derive expressions for t_1, t_2, and t_3.
With $\rho = (1\ 2\ 3)$ as in Step 2, we have the following Lagrange resolvents:

$$\begin{array}{lll}(1, t_1) = s_1 & (\omega, t_1) = \lambda_1 & (\omega^2, t_1) = \lambda_2\\ (1, t_2) = s_1 & (\omega, t_2) = \omega^2\lambda_1 & (\omega^2, t_2) = \omega\lambda_2\\ (1, t_3) = s_1 & (\omega, t_3) = \omega\lambda_1 & (\omega^2, t_3) = \omega^2\lambda_2.\end{array}$$

By Theorem 10.2(a),

$$t_1 = \frac{s_1 + \lambda_1 + \lambda_2}{3}$$
$$t_2 = \frac{s_1 + \omega^2\lambda_1 + \omega\lambda_2}{3}$$
$$t_3 = \frac{s_1 + \omega\lambda_1 + \omega^2\lambda_2}{3}.$$

15.2.1 Reduced Cubic Polynomial

Substituting $s_1 = 0$, $s_2 = p$, and $s_3 = -q$ into certain of the above expressions, and denoting t_1, t_2, t_3 by $\beta_1, \beta_2, \beta_3$, respectively, we obtain (2.31) and the formulas presented in Sections 1.2 for the reduced cubic polynomial:

$$\Delta^2 = -4p^3 - 27q^2$$

$$\lambda_1\lambda_2 = -3p$$

$$\lambda_1, \lambda_2 = 3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

$$\beta_1 = \frac{\lambda_1 + \lambda_2}{3}$$

$$\beta_2 = \frac{\omega^2\lambda_1 + \omega\lambda_2}{3}$$

$$\beta_3 = \frac{\omega\lambda_1 + \omega^2\lambda_2}{3}.$$

15.3 GENERAL QUARTIC POLYNOMIAL

Let E be an arbitrary field containing ω, and let $F = E(s_1, s_2, s_3, s_4)$ and $K = F(t_1, t_2, t_3, t_4)$. The general quartic polynomial over E is

$$\begin{aligned} f(x) &= x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 \\ &= (x - t_1)(x - t_2)(x - t_3)(x - t_4). \end{aligned}$$

A solvable series for S_4 is

$$\langle id \rangle \lhd C \lhd V \lhd A_4 \lhd S_4$$

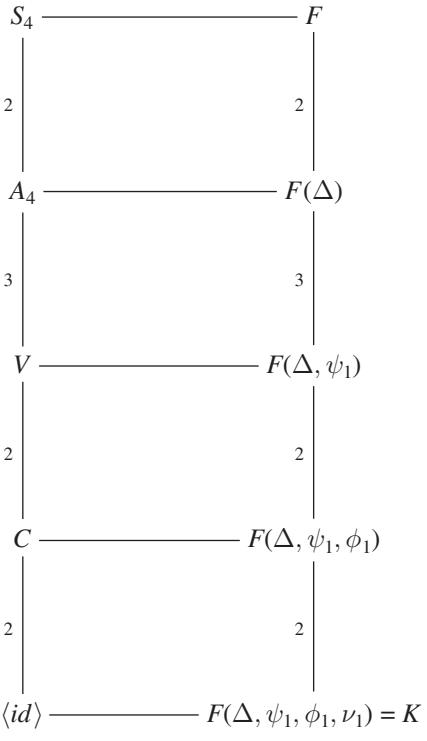
where

$$\begin{aligned}
S_4 = \{&id, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4),\\
&(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\
&(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2),\\
&(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\\
A_4 = \{&id, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\\
&(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\\
V = \{&id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}
\end{aligned}$$

and

$$C = \{id, (1\ 2)(3\ 4)\}.$$

We consider the following Galois correspondence.



Step 1. Define Δ and show that $K^{A_4} = F(\Delta)$ and Δ^2 is in F.

By definition,

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_1 - t_4)(t_2 - t_3)(t_2 - t_4)(t_3 - t_4).$$

Since

$$\mathrm{Gal}(K^{A_4}/F) = \mathrm{Gal}(K^{A_4}/K^{S_4}) \cong S_4/A_4 \cong \langle (1\ 2) \rangle$$

an argument analogous to that employed in Sections 15.1 and 15.2 shows that $K^{A_4} = F(\Delta)$ and Δ^2 is in F. The latter result also follows from (3.20).

Step 2. Define ψ_1 and show that $K^V = F(\Delta, \psi_1)$ and ψ_1^3 is in $F(\Delta)$.
To define ψ_1, we need an element of K that is fixed by V but not by any larger subgroup of A_4. Our choice is $\theta_1 = t_1t_2 + t_3t_4$, but there are other possibilities, such as $(t_1 - t_2)(t_3 - t_4)$ and $(t_1 + t_2)(t_3 + t_4)$. Recalling (9.4), consider

$$\mathrm{Gal}(K^V/K^{A_4}) \cong A_4/V \cong \langle (1\ 2\ 3) \rangle$$

and let $\rho = (1\ 2\ 3)$. In Example 9.21, we defined the conjugates of θ_1 over F,

$$\begin{aligned}
\theta_1 &= t_1t_2 + t_3t_4 \\
\theta_2 &= t_1t_4 + t_2t_3 = \rho(\theta_1) \\
\theta_3 &= t_1t_3 + t_2t_4 = \rho^2(\theta_1)
\end{aligned}$$

and showed that

$$\min(\theta_1, F) = (x - \theta_1)(x - \theta_2)(x - \theta_3).$$

Let v_1, v_2, v_3 be the "elementary symmetric polynomials" in θ_1, θ_2, θ_3, respectively. It can be shown that

$$\begin{aligned}
v_1 &= \theta_1 + \theta_2 + \theta_3 = s_2 \\
v_2 &= \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = s_1s_3 - 4s_4 \\
v_3 &= \theta_1\theta_2\theta_3 = s_1^2s_4 - 4s_2s_4 + s_3^2.
\end{aligned}$$

Then

$$\min(\theta_1, F) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_1^2s_4 - 4s_2s_4 + s_3^2).$$

Let

$$\begin{aligned}
\psi_1 &= \theta_1 + \omega\theta_2 + \omega^2\theta_3 = (\omega, \theta_1) \\
\psi_2 &= \theta_1 + \omega^2\theta_2 + \omega\theta_3 = (\omega^2, \theta_1).
\end{aligned}$$

By Theorems 10.1(b) and 10.2(b), $F(\Delta, \psi_1) = K^V$ and ψ_1^3 is in $F(\Delta)$.

We seek explicit expressions for ψ_1^3 and ψ_2^3 as elements of $F(\Delta)$. Since $\min(\theta_1, F)$ is a cubic polynomial in $F[x]$, the approach leading to (15.5) can be adapted to the present situation by placing ψ_1, ψ_2 in the roles of λ_1, λ_2, respectively, and $\theta_1, \theta_2, \theta_3$ in the roles of t_1, t_2, t_3, respectively. Then v_1, v_2, v_3 correspond to s_1, s_2, s_3, respectively. The counterpart to Δ is

$$\Delta' = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3).$$

Since

$$\begin{aligned}\theta_1 - \theta_2 &= (t_1 - t_4)(t_2 - t_3)\\ \theta_1 - \theta_3 &= (t_1 - t_3)(t_2 - t_4)\\ \theta_2 - \theta_3 &= (t_1 - t_2)(t_3 - t_4)\end{aligned}$$

we have $\Delta' = \Delta$. Therefore,

$$\begin{aligned}\psi_1^3 - \psi_2^3 &= 3i\sqrt{3}\Delta\\ \psi_1^3 + \psi_2^3 &= 2v_1^3 - 9v_1v_2 + 27v_3\\ &= 27s_1^2s_4 - 9s_1s_2s_3 + 2s_2^3 - 72s_2s_4 + 27s_3^2\\ \psi_1^3, \psi_2^3 &= \frac{2v_1^3 - 9v_1v_2 + 27v_3 \pm 3i\sqrt{3}\Delta}{2}\\ &= \frac{27s_1^2s_4 - 9s_1s_2s_3 + 2s_2^3 - 72s_2s_4 + 27s_3^2 \pm 3i\sqrt{3}\Delta}{2}\end{aligned} \tag{15.6}$$

and

$$\psi_1, \psi_2 = \sqrt[3]{\frac{27s_1^2s_4 - 9s_1s_2s_3 + 2s_2^3 - 72s_2s_4 + 27s_3^2 \pm 3i\sqrt{3}\Delta}{2}}$$

where ψ_1 and ψ_2 are chosen so that

$$\psi_1\psi_2 = v_1^2 - 3v_2 = -3s_1s_3 + s_2^2 + 12s_4 \tag{15.7}$$

is satisfied. Thus, (15.6) gives the desired expressions for expressions for ψ_1^3 and ψ_2^2.

Step 3. Define ϕ_1 and show that $K^C = F(\Delta, \psi_1, \phi_1)$ and ϕ_1^2 is in $F(\Delta, \psi_1)$. To define ϕ_1, we need an element of K that is fixed by C but not by any larger subgroup of V. Our choice is $\varepsilon = t_1 + t_2$, but again there are alternatives, such as $t_3 + t_4$. Consider

$$\mathrm{Gal}(K^C/K^V) \cong V/C \cong \langle (1\ 3)(2\ 4) \rangle$$

and let $\rho = (1\ 3)(2\ 4)$. Let

$$\begin{aligned}\phi_1 &= t_1 + t_2 - t_3 - t_4 = (-1, \varepsilon)\\ \phi_2 &= t_1 - t_2 - t_3 + t_4\\ \phi_3 &= t_1 - t_2 + t_3 - t_4.\end{aligned} \tag{15.8}$$

By Theorem 10.1(b) and 10.2(b), $F(\Delta, \psi_1, \phi_1) = K^C$ and ϕ_1^2 is in $F(\Delta, \psi_1)$.

We seek an explicit expression for ϕ_1^2 as an element of $F(\Delta, \psi_1)$. It can be shown that

$$\begin{aligned}\phi_1^2 &= s_1^2 - 4s_2 + 4\theta_1\\ \phi_2^2 &= s_1^2 - 4s_2 + 4\theta_2\\ \phi_3^2 &= s_1^2 - 4s_2 + 4\theta_3.\end{aligned} \tag{15.9}$$

By Theorem 10.2(a),

$$\theta_1 = \frac{s_2 + \psi_1 + \psi_2}{3}.$$

It follows from the first identity in (15.9) that

$$\phi_1^2 = s_1^2 - 4s_2 + 4\Big(\frac{s_2 + \psi_1 + \psi_2}{3}\Big). \tag{15.10}$$

Then (15.7) implies that $F(\Delta, \psi_1) = F(\Delta, \psi_1, \psi_2)$. Thus, (15.10) is the desired expression for ϕ_1^2.

Step 4. Define ν_1 and show that $K = F(\Delta, \psi_1, \phi_1, \nu_1)$ and ν_1^2 is in $F(\Delta, \psi_1, \phi_1)$. To define ν_1, we need an element of K that is not fixed by C. An obvious choice is t_1. Consider

$$\mathrm{Gal}(K/K^C) = \mathrm{Gal}(K^{\langle id\rangle}/K^C) \cong C/\langle id\rangle \cong \langle (1\ 2)(3\ 4)\rangle$$

and let $\rho = (1\ 2)(3\ 4)$. Let

$$\begin{aligned}\nu_1 &= t_1 - t_2 = (-1, t_1)\\ \nu_2 &= t_3 - t_4 = (-1, t_3).\end{aligned}$$

Then

$$\nu_1\nu_2 = \theta_3 - \theta_2. \tag{15.11}$$

By Theorems 10.1(b) and 10.2(b), $F(\Delta, \psi_1, \phi_1, \nu_1) = K$ and ν_1^2 is in $F(\Delta, \psi_1, \phi_1)$.

We seek an explicit expression for ν_1^2 as an element of $F(\Delta, \psi_1, \phi_1)$. It can be shown that

$$\nu_1^2 + \nu_2^2 = s_1^2 - 2s_2 - 2\theta_1 = \frac{-\phi_1^2 + 3s_1^2}{2} - 4s_2 \tag{15.12}$$

where the second equality follows from the first identity in (15.9). It can also be shown that

$$\nu_1^2 - \nu_2^2 = \phi_2\phi_3$$

and

$$\phi_1\phi_2\phi_3 = s_1^3 - 4s_1s_2 + 8s_3 \tag{15.13}$$

hence

$$\nu_1^2 - \nu_2^2 = \frac{s_1^3 - 4s_1s_2 + 8s_3}{\phi_1}. \tag{15.14}$$

Combining (15.12) and (15.14) yields

$$\nu_1^2, \nu_2^2 = \frac{-\phi_1^2 + 3s_1^2}{4} - 2s_2 \pm \frac{s_1^3 - 4s_1s_2 + 8s_3}{2\phi_1}. \tag{15.15}$$

Therefore,

$$\nu_1, \nu_2 = \sqrt{\frac{-\phi_1^2 + 3s_1^2}{4} - 2s_2 \pm \frac{s_1^3 - 4s_1s_2 + 8s_3}{2\phi_1}}$$

where ν_1 and ν_2 are chosen so that (15.11) is satisfied. Thus, (15.15) gives the desired expression for ν_1^2.

Step 5. Derive expressions for t_1, t_2, t_3, and t_4.
With $\rho = (1\ 2)(3\ 4)$ as in Step 4, we have the following Lagrange resolvents:

$$\begin{aligned}
(1, t_1) &= \frac{s_1 + \phi_1}{2} \qquad (-1, t_1) = \nu_1 \\
(1, t_2) &= \frac{s_1 + \phi_1}{2} \qquad (-1, t_2) = -\nu_1 \\
(1, t_3) &= \frac{s_1 - \phi_1}{2} \qquad (-1, t_3) = \nu_2 \\
(1, t_4) &= \frac{s_1 - \phi_1}{2} \qquad (-1, t_4) = -\nu_2.
\end{aligned}$$

By Theorem 10.2(a),

$$t_1, t_2 = \frac{1}{2}\Big(\frac{s_1 + \phi_1}{2} \pm \nu_1\Big) = \frac{s_1 + \phi_1}{4} \pm \frac{\nu_1}{2}$$
$$t_3, t_4 = \frac{1}{2}\Big(\frac{s_1 - \phi_1}{2} \pm \nu_2\Big) = \frac{s_1 - \phi_1}{4} \pm \frac{\nu_2}{2}$$

or equivalently,

$$t_1, t_2 = \frac{s_1 + \phi_1}{4} \pm \frac{1}{2}\sqrt{\frac{-\phi_1^2 + 3s_1^2}{4} - 2s_2 + \frac{s_1^3 - 4s_1 s_2 + 8s_3}{2\phi_1}}$$
$$t_3, t_4 = \frac{s_1 - \phi_1}{4} \pm \frac{1}{2}\sqrt{\frac{-\phi_1^2 + 3s_1^2}{4} - 2s_2 - \frac{s_1^3 - 4s_1 s_2 + 8s_3}{2\phi_1}}.$$

15.3.1 Reduced Quartic Polynomial

Substituting $s_1 = 0$, $s_2 = p$, $s_3 = -q$, and $s_4 = r$ into certain of the above expressions, and denoting t_1, t_2, t_3, t_4 by $\beta_1, \beta_2, \beta_3, \beta_4$, respectively, we obtain formulas presented in Section 1.3 for the reduced quartic polynomial:

$$\min(\theta_1, F) = x^3 - px^2 - 4rx + 4pr - q^2$$

$$\phi_1^2 = 4(\theta_1 - p)$$

$$\beta_1, \beta_2 = \frac{\phi_1}{4} \pm \frac{1}{2}\sqrt{-\frac{\phi_1^2}{4} - 2p - \frac{4q}{\phi_1}}$$

$$\beta_3, \beta_4 = -\frac{\phi_1}{4} \pm \frac{1}{2}\sqrt{-\frac{\phi_1^2}{4} - 2p + \frac{4q}{\phi_1}}$$

15.3.2 Alternative Quartic Formulas

With ϕ_1, ϕ_2, and ϕ_3 as in (15.8), it is straightforward to show that

$$\begin{aligned} t_1 &= \frac{s_1 + \phi_1 + \phi_2 + \phi_3}{4} \\ t_2 &= \frac{s_1 + \phi_1 - \phi_2 - \phi_3}{4} \\ t_3 &= \frac{s_1 - \phi_1 - \phi_2 + \phi_3}{4} \\ t_4 &= \frac{s_1 - \phi_1 + \phi_2 - \phi_3}{4}. \end{aligned} \tag{15.16}$$

To use these formulas, we need a way of calculating ϕ_1, ϕ_2, and ϕ_3 without having explicit values of t_1, t_2, t_3, and t_4 in advance. It can be verified that

$$\mathrm{Gal}(K/F(\phi_1)) \cong \{id, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

and that

$$id, (1\ 3), (1\ 4), (2\ 3), (2\ 4), (1\ 3)(2\ 4)$$

are coset representatives of $\mathrm{Gal}(K/F(\phi_1))$ in $\mathrm{Gal}(K/F)$. We have from

$$\begin{array}{lll} id\,\phi_1 = \phi_1 & (1\ 3)\phi_1 = -\phi_2 & (1\ 4)\phi_1 = -\phi_3 \\ (2\ 3)\phi_1 = \phi_3 & (2\ 4)\phi_1 = \phi_2 & (1\ 3)(2\ 4)\phi_1 = -\phi_1 \end{array}$$

and Theorem 9.18 that

$$\begin{aligned} \min(\phi_1, F) &= (x-\phi_1)(x+\phi_1)(x-\phi_2)(x+\phi_2)(x-\phi_3)(x+\phi_3) \\ &= (x^2-\phi_1^2)(x^2-\phi_2^2)(x^2-\phi_3^2) \\ &= x^6 - w_1x^4 + w_2x^2 - w_3 \end{aligned}$$

where w_1, w_2, w_3 are the "elementary symmetric polynomials" in $\phi_1^2, \phi_2^2, \phi_3^2$, respectively. It can be shown that

$$\begin{aligned} w_1 &= \phi_1^2 + \phi_2^2 + \phi_3^2 = 3s_1^2 - 8s_2 \\ w_2 &= \phi_1^2\phi_2^2 + \phi_1^2\phi_3^2 + \phi_2^2\phi_3^2 \\ &\quad = 3s_1^4 - 16s_1^2s_2 + 16s_1s_3 + 16s_2^2 - 64s_4 \\ w_3 &= \phi_1^2\phi_2^2\phi_3^2 = (s_1^3 - 4s_1s_2 + 8s_3^2)^2 \end{aligned}$$

hence

$$\begin{aligned} \min(\phi_1, F) = x^6 &- (3s_1^2 - 8s_2)x^4 \\ &+ (3s_1^4 - 16s_1^2s_2 + 16s_1s_3 + 16s_2^2 - 64s_4)x^2 \\ &- (s_1^3 - 4s_1s_2 + 8s_3^2)^2. \end{aligned}$$

Note that $\min(\phi_1, F)$ is a cubic polynomial in x^2. As such, it can be solved by radicals over F using the formulas given above for the general cubic polynomial. To use (15.16) in practice, we choose three of the six roots of $\min(\phi_1, F)$ in such a way that (15.13) is satisfied. Depending on the choices, we get (15.16) as presented or (15.16) with t_1, t_2, t_3, t_4 renumbered.

We now place (15.16) in the context of the Galois correspondence that began this section. As shown in Step 1,

$$K^{A_4} = F(\Delta). \tag{15.17}$$

We have from Example 9.23 that $K^V = F(\theta_1, \theta_2, \theta_3)$. It follows from (15.9) and (15.13) that

$$K^V = F(\phi_1^2, \phi_2^2). \tag{15.18}$$

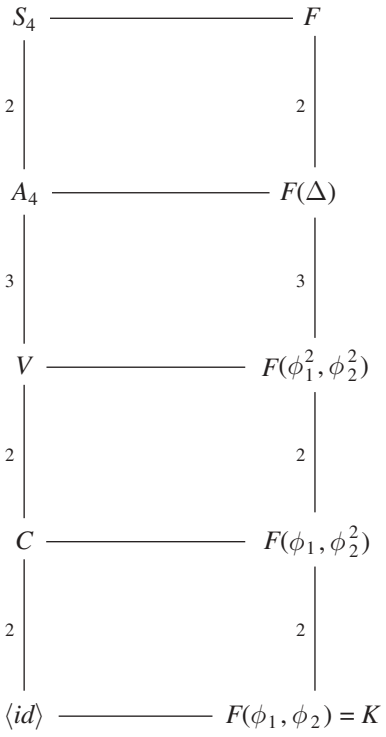
According to Step 3, $K^C = K^V(\phi_1)$, which can be combined with (15.18) to give

$$K^C = F(\phi_1, \phi_2^2). \tag{15.19}$$

Finally, (15.13) and (15.16) show that

$$K = F(\phi_1, \phi_2). \tag{15.20}$$

With (15.17)–(15.20), we can revise the earlier Galois correspondence as follows:



APPENDIX A

COSETS AND GROUP ACTIONS

The identity element of an arbitrary group will be denoted by id. Let G be a group, and let H be a subgroup of G. For each element g of G, the corresponding *left coset* of H in G is

$$gH = \{gh : h \in H\}$$

and the *right coset* is

$$Hg = \{hg : h \in H\}.$$

The cardinality of an arbitrary set $\mathcal{S}$ will be denoted by $|\mathcal{S}|$. We refer to $|G|$ as the *order* of G. If $|G|$ is finite, we say that G is a *finite group*, otherwise an *infinite group*. Suppose that G is a finite group. It is easily demonstrated that

$$|gH| = |H| = |Hg|$$

for all g in G.

Theorem A.1 (Lagrange's Theorem). Let G be a finite group, and let H be a subgroup of G. Then there are $|G|/|H|$ distinct left (right) cosets of H in G, and they form a partition of G.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Proof. If $gH \cap g'H$ is nonempty for some g and g' in G, then $gh = g'h'$ for some h and h' in H. Therefore, $gh'' = g'h'h^{-1}h''$ for all h'' in H, hence $gH \subseteq g'H$. Likewise for the reverse inclusion, so $gH = g'H$. Since left cosets with a nonempty intersection are equal, the distinct left cosets of H in G form a partition of G. Furthermore, since all left cosets of H in G have $|H|$ elements, the number of distinct left cosets is $|G|/|H|$. The proof for right cosets is similar. □

Let G be a finite group, and let H be a subgroup. We refer to the number of left (or right) cosets of H in G as the *index* of H in G and denote it by

$$[G : H] = \frac{|G|}{|H|}.$$

If H' is a subgroup of G containing H, then

$$[G : H] = [G : H'][H' : H].$$

Let $[G : H] = m$, and let $g_1, g_2, \ldots, g_m$ consist of one arbitrarily chosen element from each of the distinct left cosets of H in G. We refer to $g_1, g_2, \ldots, g_m$ as *left coset representatives* of H in G. Since the distinct left cosets of H in G form a partition of G, the union

$$G = g_1H \cup g_2H \cup \cdots \cup g_mH$$

is disjoint. Take g in G. It is readily verified that $gg_1, gg_2, \ldots, gg_m$ are left coset representatives of H in G.

A (left) *action* of a group G on a (nonempty, possibly infinite) set $\mathcal{A}$ is a map

$$\begin{aligned} G \times \mathcal{A} &\longrightarrow \mathcal{A} \\ (g, a) &\longmapsto g \cdot a \end{aligned}$$

satisfying the following conditions:

(i) $id \cdot a = a$ for all a in $\mathcal{A}$.
(ii) $g \cdot (g' \cdot a) = (gg') \cdot a$ for all g and g' in G and all a in $\mathcal{A}$.

In this case, we say that G acts on $\mathcal{A}$.

For a in $\mathcal{A}$, the *orbit* of a under the action (of G on $\mathcal{A}$) is

$$Ga = \{g \cdot a : g \in G\}.$$

Thus, Ga consists of the distinct values taken by $g \cdot a$ as g ranges over G. The action is called *transitive* if, given any two elements a and a' in $\mathcal{A}$, there

is g in G such that $g \cdot a = a'$. This is equivalent to saying that $\mathcal{A}$ has only one orbit under the action. Suppose that the orbits Ga and Ga' have a nonempty intersection. Then there are g and g' in G such that $g \cdot a = g' \cdot a'$, which implies that $Ga = Ga'$. Thus, the distinct orbits under the action form a partition of $\mathcal{A}$.

For a in $\mathcal{A}$, the *stabilizer* of a under the action is

$$G(a) = \{g \in G : g \cdot a = a\}.$$

It is easily verified that $G(a)$ is a subgroup of G and that

$$G(g \cdot a) = gG(a)g^{-1}$$

for all g in G.

Theorem A.2. Let G be a finite group acting on $\mathcal{A}$, and let a be an arbitrary element of $\mathcal{A}$. Then:
(a) The map

$$\begin{aligned} \iota\colon \{gG(a) : g \in G\} &\longrightarrow Ga \\ gG(a) &\longmapsto g \cdot a \end{aligned} \tag{A.1}$$

is well defined and bijective.
(b) $|G| = |Ga|\,|G(a)|$.
(c) If $\mathcal{A}$ is finite and the action is transitive, then $|G| = |\mathcal{A}|\,|G(a)|$.

Proof. (a): It is readily verified that ι is well defined and surjective. If $g \cdot a = g' \cdot a$ for some g, g' in G, then $gG(a) = g'G(a)$, so ι is injective.

(b): By Theorem A.1, the domain of ι has $|G|/|G(a)|$ elements. Since ι is bijective, we have $|G|/|G(a)| = |Ga|$.

(c): Since the action is transitive, $Ga = \mathcal{A}$. The result now follows from part (b). □

Take a in $\mathcal{A}$, let $[G : G(a)] = m$, and let $g_1, g_2, \ldots, g_m$ be left coset representatives of $G(a)$ in G. Since the distinct left cosets of $G(a)$ in G form a partition of G, it follows from (A.1) that

$$Ga = \{g_j \cdot a : j = 1, 2, \ldots, m\}$$

and that the $g_j \cdot a$ are distinct. Evidently, this way of expressing Ga is independent of the choice of left coset representatives.

Theorem A.3 (Cauchy's Theorem). Let G be a group of order n, and let p be a prime dividing n. Then G contains an element of order p.

Proof. Consider the set of p-tuples

$$\mathcal{A} = \{(g_1, g_2, \ldots, g_p) : g_i \in G \text{ for } i = 1, 2, \ldots, p; g_1 g_2 \cdots g_p = id\}.$$

The first $p-1$ components in a p-tuple can be chosen arbitrarily, and this determines the pth component. Therefore, $\mathcal{A}$ has n^{p-1} elements. Since $g_1 g_2 \cdots g_p = id$, we have $g_2 g_3 \cdots g_p = g_1^{-1}$ and then $g_2 g_3 \cdots g_p g_1 = id$. Thus, if $(g_1, g_2, g_3, \ldots, g_p)$ is in $\mathcal{A}$, then so is $(g_2, g_3, \ldots, g_p, g_1)$. In the notation of Appendices B and D, let $\rho = (1\ 2\ \ldots\ p)$, and let $\langle\rho\rangle$ be the cyclic subgroup of S_p generated by ρ. Define an action of $\langle\rho\rangle$ on $\mathcal{A}$ by setting

$$\begin{aligned}\rho \cdot (g_1, g_2, g_3, \ldots, g_p) &= (g_{\rho(1)}, g_{\rho(2)}, g_{\rho(3)}, \ldots, g_{\rho(p)}) \\ &= (g_2, g_3, \ldots, g_p, g_1).\end{aligned}$$

By Theorem A.2(b),

$$p = |\langle\rho\rangle| = |\langle\rho\rangle a|\,|\langle\rho\rangle(a)|$$

for all a in $\mathcal{A}$. Thus, each orbit under the action has either 1 element or p elements. Let r be the number of distinct orbits with 1 element, and s the number of distinct orbits with p elements. Since the distinct orbits form a partition of $\mathcal{A}$, we have $n^{p-1} = r + sp$. By assumption, p divides n, so p divides r. Since the orbit of $(id, id, \ldots, id)$ has 1 element, $r \neq 0$, so there are at least p orbits with 1 element. To be in such an orbit, the corresponding p-tuple must be of the form $(g, g, \ldots, g)$ for some g in G, in which case $g^p = id$. Take $g \neq id$. □

APPENDIX B

CYCLIC GROUPS

Let G be a finite group, and let g be an element of G. The *cyclic* subgroup of G *generated* by g is

$$\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$$

where, by definition, $g^0 = id$. Clearly, $\langle g \rangle$ is the smallest subgroup of G that contains g. Since G is finite, the sequence $id, g, g^2, g^3, \ldots$ has a repeated element. The smallest natural number exponent to give a repeated element will be denoted by $\text{ord}(g)$ and referred to as the *order* of g. By definition, $g^{\text{ord}(g)} = g^k$ for some $0 \leq k < \text{ord}(g)$, hence $g^{\text{ord}(g)-k} = id$. The minimal property of $\text{ord}(g)$ implies that $k = 0$, so $g^{\text{ord}(g)} = id$. Therefore, id is the first repeated element in the sequence, and the sequence repeats itself cyclically every $\text{ord}(g)$ steps. Thus, $\text{ord}(g)$ could have been defined as the smallest natural number m such that $g^m = id$. Since $gg^{\text{ord}(g)-1} = id$, we have $g^{\text{ord}(g)-1} = g^{-1}$. It follows that

$$\langle g \rangle = \{g^i : i = 0, 1, \ldots, \text{ord}(g) - 1\}$$

hence $|\langle g \rangle| = \text{ord}(g)$. Thus, the "order of g" equals the "order of $\langle g \rangle$."

If $G = \langle g \rangle$ for some g in G, we say that G is *cyclic*. Suppose that G is cyclic, and let h be an element of G. Then h generates G, that is, $\langle h \rangle = G$, if and only if $\text{ord}(h) = |G|$.

Theorem B.1. Let G be a group of order n. Then:
(a) $\text{ord}(g)$ divides n for all g in G.

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

(b) $g^n = id$ for all g in G.
(c) If n is prime, then G is cyclic.

Proof. (a): Since $\text{ord}(g) = |\langle g \rangle|$, we have

$$n = |G| = [G : \langle g \rangle] \, \text{ord}(g). \tag{B.1}$$

(b): Let $m = \text{ord}(g)$. By part (a), m divides n, so $g^n = (g^m)^{n/m} = id$.
(c) Since n is prime, $G \neq \langle id \rangle$. Take g in $G \backslash \langle id \rangle$. Then $\text{ord}(g) \neq 1$, so we have from (B.1) that $\text{ord}(g) = n$, hence $G = \langle g \rangle$. □

Theorem B.2. Let G be a finite group, and let g be an element of G. If m is an integer such that $g^m = id$, then $\text{ord}(g)$ divides m.

Proof. Let $k = \text{ord}(g)$, and let $|m| = qk + r$, where q and r are positive integers, with $0 \leq r < k$. Then

$$id = g^{|m|} = (g^k)^q g^r = g^r.$$

The minimal property of k implies that $r = 0$. □

The *greatest common divisor* (gcd) is defined in Appendix E.

Theorem B.3. Let G be a finite group, let g be an element of G, and let m be an integer. Then

$$\text{ord}(g^m) = \frac{\text{ord}(g)}{\gcd(m, \text{ord}(g))}.$$

Proof. Let $a = \text{ord}(g^m)$, $b = \text{ord}(g)$, and $c = \gcd(b, m)$. Setting $r = b/c$ and $s = m/c$, we have $\gcd(r, s) = 1$. Since $(g^m)^r = (g^b)^s = id$, by Theorem B.2, a divides r. Similarly, since $(g^m)^a = id$, by Theorem B.2, b divides ma. That is, rc divides sca, hence r divides sa. Since r and s are relatively prime, r divides a. Thus, a and r divide each other, so they are equal. □

Theorem B.4. Let G be a finite Abelian group, and let g and h be elements of G. If $\text{ord}(g)$ and $\text{ord}(h)$ are relatively prime, then

$$\text{ord}(gh) = \text{ord}(g) \, \text{ord}(h).$$

Proof. Let $a = \text{ord}(g)$, $b = \text{ord}(h)$, and $c = \text{ord}(gh)$. Since G is Abelian, we have

$$(gh)^{ab} = id \quad g^{bc} = (gh)^{bc} = id \quad \text{and} \quad h^{ac} = (gh)^{ac} = id.$$

By Theorem B.2, c divides ab, a divides bc, and b divides ac. Since a and b are relatively prime, they each divide c, hence ab divides c. Thus, c and ab divide each other, so they are equal. □

Theorem B.5. Any subgroup of a finite cyclic group is cyclic.

Proof. Let G be a finite cyclic group with generator g, and let H be a subgroup of G. The result is trivial for $H = \langle id \rangle$, so assume otherwise. Each element of $H \backslash \langle id \rangle$ is of the form g^k for some natural number k. Let m be the smallest such natural number, and let $k = qm + r$, with $0 \leq r < m$. Then $g^k = (g^m)^q g^r$, and since g^k and g^m are in H, so is g^r. It follows from the minimal property of m that $r = 0$, hence $H = \langle g^m \rangle$. □

The *phi-function* φ is discussed in Appendix E.

Theorem B.6. Let G be a cyclic group of order n with generator g, and let m be an integer. Then:
(a) g^m is a generator of G if and only if $\gcd(m, n) = 1$.
(b) G has $\varphi(n)$ generators.

Proof. (a): An element of G is a generator if and only if it is of order n. By Theorem B.3, $\text{ord}(g^m) = n/\gcd(m, n)$. Therefore, g^m is a generator of G if and only if $\gcd(m, n) = 1$.

(b): This follows from part (a) and the definition of $\varphi(n)$. □

Let G be a group of order n. For each natural number $d \leq n$, let $\mathcal{O}_d$ be the set of elements in G of order d, that is,

$$\mathcal{O}_d = \{g \in G : \text{ord}(g) = d\}.$$

Provided that $\mathcal{O}_d$ is nonempty, each of its elements generates a (cyclic) subgroup of G of order d. By Theorem A.1, d divides n. Since the nonempty $\mathcal{O}_d$ are disjoint, they form a partition of G. We therefore have the disjoint union

$$G = \bigcup_{\substack{d|n \\ \mathcal{O}_d \neq \phi}} \mathcal{O}_d \tag{B.2}$$

hence

$$n = \sum_{d|n} |\mathcal{O}_d|. \tag{B.3}$$

Theorem B.7. Let G be a cyclic group of order n with generator g, and let d be a natural number. Then:

(a) G has a subgroup of order d if and only if d divides n.
(b) If d divides n, then G has precisely one subgroup of order d, and it is $\langle g^{n/d}\rangle$.
(c) If d divides n, then $\mathcal{O}_d \subseteq \langle g^{n/d}\rangle$ and $|\mathcal{O}_d| = \varphi(d)$.

Proof. (a): Suppose that H_d is a subgroup of G of order d. By Theorem A.1, $d = |H_d|$ divides $n = |G|$. Conversely, suppose that d divides n. By Theorem B.3,

$$\operatorname{ord}(g^{n/d}) = \frac{n}{\gcd(n/d, n)} = d$$

so $\langle g^{n/d}\rangle$ is of order d.

(b): We just demonstrated that $\langle g^{n/d}\rangle$ is of order d. According to Theorem B.5, any subgroup of G of order d equals $\langle g^m\rangle$ for some $0 \le m \le n-1$. Then $\operatorname{ord}(g^m) = d$, hence $g^{md} = id$. By Theorem B.2, n divides md, and since d divides n, it follows that n/d divides m. Therefore, $\langle g^m\rangle \subseteq \langle g^{n/d}\rangle$. Since $\langle g^m\rangle$ and $\langle g^{n/d}\rangle$ both have order d, they are equal.

(c): The generators of $\langle g^{n/d}\rangle$ are in $\mathcal{O}_d$, and each element of $\mathcal{O}_d$ generates a cyclic subgroup of G of order d. Since $\langle g^{n/d}\rangle$ is the only such subgroup, $\mathcal{O}_d$ is the set of generators of $\langle g^{n/d}\rangle$. Therefore, $\mathcal{O}_d \subseteq \langle g^{n/d}\rangle$, and by Theorem B.6(b), $|\mathcal{O}_d| = \varphi(d)$. □

Theorem B.8. For all natural numbers n,

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

Proof. Let G be an arbitrary cyclic group of order n. By Theorem B.7(c), $|\mathcal{O}_d| = \varphi(d)$ for each d dividing n. The result now follows from (B.3). □

Theorem B.9. If G is a cyclic group of order n, then

$$G = \bigcup_{d|n} \mathcal{O}_d$$

where the union is disjoint.

Proof. By Theorem B.7(c), $|\mathcal{O}_d| = \varphi(d) \neq 0$ for each d dividing n. The result now follows from (B.2). □

Theorem B.10. Let G be a group of order n. Then the following are equivalent:
(a) G is cyclic.
(b) For each natural number d dividing n, G contains precisely one cyclic subgroup of order d.

(c) For each natural number d dividing n, G contains at most one cyclic subgroup of order d.

Proof. (a)⇒(b): This follows from Theorem B.7(b).

(b)⇒(c): Trivial.

(c)⇒(a): Suppose that G contains a cyclic subgroup H_d of order d. The generators of H_d are in $\mathcal{O}_d$, and each element of $\mathcal{O}_d$ generates a cyclic subgroup of G of order d. Since H_d is the only such subgroup, $\mathcal{O}_d$ is the set of generators of H_d. By Theorem B.6(b), $|\mathcal{O}_d| = \varphi(d)$. It follows from (B.3) and Theorem B.8 that

$$n = \sum_{d|n} |\mathcal{O}_d| \leq \sum_{d|n} \varphi(d) = n.$$

Therefore, $|\mathcal{O}_d| = \varphi(d)$ for each d dividing n. In particular, this is true for $d = n$. So, G has $\varphi(n)$ generators, and is therefore cyclic. □

APPENDIX C

SOLVABLE GROUPS

Let G be a group. A subgroup N of G is said to be a *normal subgroup* if $gNg^{-1} = N$ (equivalently, $gN = Ng$) for all g in G. In this case, we write $N \trianglelefteq G$. If N is a proper subgroup, we write $N \triangleleft G$.

A *normal series* for G is a series of subgroups

$$\langle id \rangle = G_0 \triangleleft \cdots \triangleleft G_{i-1} \triangleleft G_i \triangleleft \cdots \triangleleft G_n = G$$

where G_{i-1} is a (proper) normal subgroup of G_i for $i = 1, 2, \ldots, n$. The quotient groups G_i/G_{i-1} are termed the *factors* of the normal series. Note that the definition requires G_{i-1} to be a normal subgroup of G_i but not necessarily a normal subgroup of G. A group is said to be *solvable* if it has a normal series with factors that are Abelian. In this case, the normal series is called a *solvable series*.

For subgroups H_1 and H_2 of G, let

$$H_1H_2 = \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}.$$

Theorem C.1. Let G be a group, let $N \trianglelefteq G$, and let H be a subgroup of G. Then $HN = NH$ is a subgroup of G.

Proof. Since $N \trianglelefteq G$, $hN = Nh$ for all h in H, hence $HN = NH$. Take h, h' in H and n, n' in N. Then $nh' = h''n''$ for some h'' in H and some n'' in N, so

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

$(hn)(h'n') = (h'h'')(n''n')$ is in HN. Therefore, HN is closed under multiplication. Evidently, id is in HN. Inverses are in HN because $(hn)^{-1} = n^{-1}h^{-1}$ is in NH for all h in H and all n in N. □

Theorem C.2. Let G be a group, and let $N \trianglelefteq G$. If H_1 and H_2 are subgroups of G such that $H_1 \trianglelefteq H_2$, then $H_1N \trianglelefteq H_2N$. If H_2/H_1 is Abelian, then so is H_2N/H_1N.

Proof. By Theorem C.1, H_1N is a subgroup of the group H_2N. Take h_2n in H_2N. Then

$$\begin{aligned} h_2nH_1N &= h_2nNH_1 && \text{[Theorem C.1]} \\ &= h_2NH_1 \\ &= h_2H_1N && \text{[Theorem C.1]} \\ &= H_1h_2N && [H_1 \trianglelefteq H_2] \\ &= H_1h_2Nn \\ &= H_1Nh_2n && [N \trianglelefteq G] \end{aligned}$$

so $H_1N \trianglelefteq H_2N$.

Now, suppose that H_2/H_1 is Abelian, and take h_2n and $h_2'n'$ in H_2N. As shown above, $h_2nH_1N = h_2H_1N$, and likewise $h_2'n'H_1N = h_2'H_1N$. Then

$$\begin{aligned} (h_2nH_1N)(h_2'n'H_1N) &= (h_2H_1N)(h_2'H_1N) \\ &= (h_2h_2'H_1)N \\ &= (h_2H_1)(h_2'H_1)N \\ &= (h_2'H_1)(h_2H_1)N && [H_2/H_1 \text{ Abelian}] \\ &= (h_2'h_2H_1)N \\ &= (h_2'H_1N)(h_2H_1N) \\ &= (h_2'n'H_1N)(h_2nH_1N) \end{aligned}$$

so H_2N/H_1N is Abelian. □

Let G and G' be groups, and let $\iota\colon G \longrightarrow G'$ be a homomorphism. The *kernel* of ι is

$$\ker(\iota) = \{g \in G : \iota(g) = id\}$$

and *image* of ι is

$$\text{im}(\iota) = \{\iota(g) : g \in G\}.$$

It is easily demonstrated that $\ker(\iota) \trianglelefteq G$ and that $\text{im}(\iota)$ is a subgroup of G'.

Theorem C.3 (First Isomorphism Theorem). Let G and G' be groups, and let $\iota\colon G \longrightarrow G'$ be a homomorphism. Then

$$G/\ker(\iota) \cong \mathrm{im}(\iota).$$

If ι is surjective, then $G/\ker(\iota) \cong G'$.

Proof. The map

$$\begin{aligned} G/\ker(\iota) &\longrightarrow \mathrm{im}(\iota) \\ g\ker(\iota) &\longmapsto \iota(g) \end{aligned}$$

is well defined and an isomorphism. □

Theorem C.4 (Second Isomorphism Theorem). Let G be a group, let H be a subgroup of G, and let $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H, N \trianglelefteq HN$, and

$$H/(H \cap N) \cong HN/N. \tag{C.1}$$

Proof. By Theorem C.1, HN is a subgroup of G, so the assertion makes sense. Since $N \trianglelefteq G$, we have $N \trianglelefteq HN$. The map

$$\begin{aligned} H &\longrightarrow HN/N \\ h &\longmapsto hN \end{aligned}$$

is a surjective homomorphism with kernel $H \cap N$. Then (C.1) follows from the First Isomorphism Theorem. □

Theorem C.5 (Third Isomorphism Theorem). Let G be a group, and let $N_1 \trianglelefteq G$ and $N_2 \trianglelefteq G$, where $N_1 \subseteq N_2$. Then $N_2/N_1 \trianglelefteq G/N_1$ and

$$(G/N_1)/(N_2/N_1) \cong G/N_2. \tag{C.2}$$

Proof. The map

$$\begin{aligned} G/N_1 &\longrightarrow G/N_2 \\ gN_1 &\longmapsto gN_2 \end{aligned}$$

is well defined and a surjective homomorphism with kernel N_2/N_1. Then (C.2) follows from the First Isomorphism Theorem. □

Theorem C.6. Let G and G' be groups, let $\iota\colon G \longrightarrow G'$ be a homomorphism, and let $N = \ker(\iota)$. Then:

(a) If H is a subgroup of G, then $\iota(H)$ is a subgroup of $\iota(G)$ and $\iota^{-1}(\iota(H)) = HN$.

(b) If $H \trianglelefteq G$, then $\iota(H) \trianglelefteq \iota(G)$.

(c) If H' is a subgroup of G', then $\iota^{-1}(H')$ is a subgroup of $\iota^{-1}(G')$ and $\iota(\iota^{-1}(H')) = H' \cap \mathrm{im}(\iota)$.

Proof. Straightforward. □

Theorem C.7. Let G and G' be groups, and let $\iota\colon G \longrightarrow G'$ be a surjective homomorphism. If $H' \trianglelefteq G'$, then $\iota^{-1}(H') \trianglelefteq G$ and

$$G/\iota^{-1}(H') \cong G'/H'. \tag{C.3}$$

Proof. The map

$$\begin{aligned} G &\longrightarrow G'/H' \\ g &\longmapsto \iota(g)H' \end{aligned}$$

is a surjective homomorphism with kernel $\iota^{-1}(H') \trianglelefteq G$. Then (C.3) follows from the First Isomorphism Theorem. □

Theorem C.8 (Correspondence Theorem). Let G and G' be groups, and let $\iota\colon G \longrightarrow G'$ be a surjective homomorphism. Then the map

$$\begin{aligned} \iota^*\colon \{\text{subgroup of } G \text{ containing } \ker(\iota)\} &\longrightarrow \{\text{subgroup of } G'\} \\ H &\longmapsto \iota(H) \end{aligned}$$

is an order-preserving bijection (where the ordering is defined by inclusion). Furthermore, ι^* preserves normality in the following sense: If H_1 and H_2 are subgroups of G that contain $\ker(\iota)$, then $H_1 \trianglelefteq H_2$ if and only if $\iota(H_1) \trianglelefteq \iota(H_2)$.

Proof. The definition of ι^* make sense because of Theorem C.6(a). Let $N = \ker(\iota)$, and let G_1 and G_2 be subgroups of G that contain N. Suppose that $\iota(G_1) = \iota(G_2)$. By Theorem C.6(a),

$$G_1 = \iota^{-1}(\iota(G_1)) = \iota^{-1}(\iota(G_2)) = G_2$$

so ι^* is injective. Let H' be a subgroup of G', and let $H = \iota^{-1}(H')$. By Theorem C.6(c), $\iota(H) = H'$, so ι^* is surjective. Thus, ι^* is a bijection, and clearly, it is order preserving.

To show that ι^* preserves normality, let H_1 and H_2 be subgroups of G containing N, where $H_1 \trianglelefteq H_2$. Let ε be the restriction of ι to H_2. Then $\varepsilon\colon H_2 \longrightarrow \varepsilon(H_2)$ is a surjective homomorphism with $\ker(\varepsilon) = N$. Evidently, $\varepsilon(H_1) = \iota(H_1)$ and $\varepsilon(H_2) = \iota(H_2)$. By Theorem C.6(b), $\varepsilon(H_1) \trianglelefteq \varepsilon(H_2)$. Conversely, suppose that $\varepsilon(H_1) \trianglelefteq \varepsilon(H_2)$. By Theorems C.6(a) and C.7,

$$H_1 = \varepsilon^{-1}(\varepsilon(H_1)) \trianglelefteq \varepsilon^{-1}(\varepsilon(H_2)) = H_2.$$

□

We will use the Correspondence Theorem in the following manner. Let G be a group, and let $N \trianglelefteq G$. Then

$$\begin{aligned} \iota\colon G &\longrightarrow G/N \\ g &\longmapsto gN \end{aligned}$$

is a surjective homomorphism, and ι^* is an order- and normality-preserving bijection between the subgroups of G containing N and the subgroups of G/N.

Theorem C.9. A subgroup of a solvable group is solvable.

Proof. Let G be a solvable group with solvable series

$$\langle id \rangle = G_0 \triangleleft \cdots \triangleleft G_i \triangleleft \cdots \triangleleft G_n = G.$$

Let H be a subgroup of G, and let $H_i = H \cap G_i$ for $i = 0, 1, \ldots, n$. Since H_i is a subgroup of G_i, and $G_{i-1} \trianglelefteq G_i$, it follows from the Second Isomorphism Theorem that $H_{i-1} = H_i \cap G_{i-1} \trianglelefteq H_i$ and

$$H_i/H_{i-1} \cong H_i G_{i-1}/G_{i-1} \subseteq G_i/G_{i-1}.$$

Since G_i/G_{i-1} is Abelian, so is H_i/H_{i-1}. Deleting redundancies from

$$\langle id \rangle = H_0 \trianglelefteq \cdots \trianglelefteq H_i \trianglelefteq \cdots \trianglelefteq H_n = H$$

we obtain a solvable series for H. □

Theorem C.10. Let G be a group, and let $N \trianglelefteq G$. Then G is solvable if and only if N and G/N are solvable.

Proof. ($\Rightarrow$): That N is solvable follows from Theorem C.9. Let

$$\langle id \rangle = G_0 \triangleleft \cdots \triangleleft G_i \triangleleft \cdots \triangleleft G_n = G$$

be a solvable series for G. By Theorem C.2, we have

$$N = G_0 N \trianglelefteq \cdots \trianglelefteq G_i N \trianglelefteq \cdots \trianglelefteq G_n N = G.$$

It follows from the Correspondence Theorem that

$$N/N = G_0 N/N \trianglelefteq \cdots \trianglelefteq G_i N/N \trianglelefteq \cdots \trianglelefteq G_n N/N = G/N. \tag{C.4}$$

Since $N \trianglelefteq G_i N, G_{i-1} N \trianglelefteq G_i N$, and $N \subseteq G_{i-1} N$, the Third Isomorphism Theorem implies that

$$[(G_i N)/N]/[(G_{i-1} N)/N] \cong (G_i N)/(G_{i-1} N).$$

Since G_i/G_{i-1} is Abelian, by Theorem C.2, so is $G_iN/G_{i-1}N$, and therefore, so is $[(G_iN)/N]/[(G_{i-1}N)/N]$. Deleting redundancies from (C.4), we obtain a solvable series for G/N.

($\Leftarrow$): It follows from the Correspondence Theorem that a solvable series for G/N takes the form

$$N/N = H_0/N \lhd \cdots \lhd H_i/N \lhd \cdots \lhd H_n/N = G/N$$

where

$$N = H_0 \lhd H_1 \lhd \cdots \lhd H_i \lhd \cdots \lhd H_n = G. \tag{C.5}$$

Since $N \trianglelefteq H_i, H_{i-1} \trianglelefteq H_i$, and $N \subseteq H_{i-1}$, it follows from the Third Isomorphism Theorem that

$$(H_i/N)/(H_{i-1}/N) \cong H_i/H_{i-1}.$$

Since $(H_i/N)/(H_{i-1}N)$ is Abelian, so is H_i/H_{i-1}. Appending (C.5) to a solvable series for N gives a solvable series for G. □

A group is said to be *simple* if the only normal subgroups it contains are itself and $\langle id \rangle$. A normal series with simple factors is called a *composition series*.

Theorem C.11. Every finite group has a composition series.

Proof. Let G be a finite group. The set of normal subgroups of G is nonempty because it contains $\langle id \rangle$, and the set is finite because G is finite. Let G' be a maximal normal subgroup of G; that is, G' is not contained in any other normal subgroup of G, except G. By the Correspondence Theorem, G/G' is simple. We apply the same procedure to G' to get a maximal normal subgroup G'' of G' such that G'/G'' is simple, and so on. Since G is finite, this process eventually terminates with $\langle id \rangle$, resulting in a composition series for G. □

Theorem C.12. Every finite Abelian group is solvable.

Proof. Let G be a finite Abelian group. By Theorem C.11, G has a composition series. Since G is Abelian, the composition series is a normal series with Abelian factors. □

Theorem C.13. If $G \neq \langle id \rangle$ is a finite, simple Abelian group, then G is of prime order.

Proof. Take g in $G \backslash \langle id \rangle$. Since G is Abelian, $\langle g \rangle$ is a normal subgroup, and since G is simple, we have $G = \langle g \rangle$. It follows from Theorem B.7(b) that $\langle g \rangle$ is of prime order, otherwise it would contain a nontrivial (normal) subgroup. □

Theorem C.14. A finite group is solvable if and only if it has a solvable series with factors of prime order.

Proof. ($\Rightarrow$): Let G have the solvable series

$$\langle id \rangle = G_0 \lhd \cdots \lhd G_{i-1} \lhd G_i \lhd \cdots \lhd G_n = G. \tag{C.6}$$

Since G is finite, so is G_i/G_{i-1}. It follows from the Correspondence Theorem and Theorem C.11 that G_i/G_{i-1} has a composition series of the form

$$G_{i-1}/G_{i-1} \lhd \cdots \lhd H/G_{i-1} \lhd H'/G_{i-1} \lhd \cdots \lhd G_i/G_{i-1} \tag{C.7}$$

where

$$G_{i-1} \lhd \cdots \lhd H \lhd H' \lhd \cdots \lhd G_i. \tag{C.8}$$

By definition, $(H'/G_{i-1})/(H/G_{i-1})$ is simple. Since G_i/G_{i-1} is finite and Abelian, so is H'/G_{i-1}, and therefore, so is $(H'/G_{i-1})/(H/G_{i-1})$. By Theorem C.13, $(H'/G_{i-1})/(H/G_{i-1})$ is of prime order. Since $G_{i-1} \trianglelefteq H', H \trianglelefteq H'$, and $G_{i-1} \subseteq H$, it follows from the Third Isomorphism Theorem that

$$(H'/G_{i-1})/(H/G_{i-1}) \cong H'/H.$$

Thus, H'/H is of prime order, hence cyclic, and therefore Abelian. Forming the union of series such as (C.8), one for each pair of consecutive groups in (C.6), we obtain a solvable series for G with factors of prime order.

($\Leftarrow$): Factors of prime order are cyclic, hence Abelian. □

APPENDIX D

PERMUTATION GROUPS

We assume that $n \geq 2$. Let S_n be the set of bijective functions on $\mathcal{B} = \{1, 2, \ldots, n\}$. Defining group multiplication to be composition of functions, we make S_n into a group called the *symmetric group* on $\mathcal{B}$. Each σ in S_n can be displayed as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

We create an action of $\langle\sigma\rangle$ on $\mathcal{B}$ by setting $\sigma \cdot a = \sigma(a)$ for all a in $\mathcal{B}$. Let $|\langle\sigma\rangle a| = k$. It can be shown that

$$\langle\sigma\rangle a = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a)\}.$$

Corresponding to $\langle\sigma\rangle a$ is the permutation in S_n that maps a to $\sigma(a)$, $\sigma(a)$ to $\sigma^2(a)$, and so on, while leaving all other elements of $\mathcal{B}$ fixed. We denote this permutation by

$$(\, a \;\; \sigma(a) \;\; \sigma^2(a) \;\; \ldots \;\; \sigma^{k-1}(a) \,)$$

and refer to it as a *cycle*, or more precisely as a cycle of *length* k or a k*-cycle*. Note that any k-cycle has order k. The starting point for a cycle is irrelevant, so

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

the above cycle could equally be expressed, for example, as

$$(\sigma(a)\ \sigma^2(a)\ \ldots\ \sigma^{k-1}(a)\ a) \quad \text{or} \quad (\sigma^2(a)\ \ldots\ \sigma^{k-1}(a)\ a\ \sigma(a)).$$

Cycles with no elements in common are said to be *disjoint*.

Theorem D.1. Every permutation in S_n can be written as the product of disjoint cycles, and in exactly one way (up to order of terms).

Proof. This follows from the above remarks. □

For example, consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$$

in S_6. Then σ has the cycle decomposition $\sigma = (1\ 2\ 4)(3\ 6)(5)$. *We adopt the convention that cycles of length* 1 *are suppressed*. Thus, $\sigma = (1\ 2\ 4)(3\ 6)$, or equivalently $\sigma = (3\ 6)(1\ 2\ 4)$ since disjoint cycles commute.

The inverse of a cycle is easily determined. Let

$$\sigma = (a_1\ a_2\ a_3\ \ldots\ a_{k-1}\ a_k)$$

then

$$\sigma^{-1} = (a_k\ a_{k-1}\ \ldots\ a_3\ a_2\ a_1).$$

A cycle of length 2 is called a *transposition*. Any cycle can be written as the product of transpositions in numerous ways. For example,

$$(a_1\ a_2\ a_3\ a_4\ \ldots\ a_{k-1}\ a_k) = (a_1\ a_2)\,(a_2\ a_3)\,(a_3\ a_4)\cdots(a_{k-1}\ a_k) \tag{D.1}$$

and

$$(a_1\ a_2\ a_3\ a_4\ \ldots\ a_{k-1}\ a_k) = (a_1\ a_k)\,(a_1\ a_{k-1})\cdots(a_1\ a_3)\,(a_1\ a_2). \tag{D.2}$$

Since any permutation is the product of cycles, it follows that S_n is generated by its transpositions.

Theorem D.2. The order of a product of disjoint cycles equals the least common multiple of their orders.

Proof. Let σ_j be a k_j-cycle for $j = 1, 2, \ldots, m$, and suppose that the σ_j are disjoint. Let r be the least common multiple of $k_1, k_2, \ldots, k_m$, and let $\sigma = \sigma_1\sigma_2\cdots\sigma_m$. Since the σ_j are disjoint, they commute, and since each k_j divides r, we have $\sigma^r = \sigma_1^r\sigma_2^r\cdots\sigma_m^r = id$. Let s be a natural number such that

$\sigma^s = id$. Then $\sigma_1^s \sigma_2^s \cdots \sigma_m^s = id$, which is possible only if $\sigma_j^s = id$ for each j. By Theorem B.2, $k_j = \text{ord}(\sigma_j)$ divides s for each j, and therefore, so does r. Thus, $r = \text{ord}(\sigma)$. □

Theorem D.3. Take σ and ν in S_n, and let ν have the cycle decomposition

$$\nu = (a_1\ a_2\ \ldots\ a_k)\,(b_1\ b_2\ \ldots\ b_l)\ \cdots.$$

Then $\sigma\nu\sigma^{-1}$ has the cycle decomposition

$$\sigma\nu\sigma^{-1} = (\,\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)\,)\,(\,\sigma(b_1)\ \sigma(b_2)\ \ldots\ \sigma(b_l)\,)\ \cdots\ .$$

Proof. Let $\tau = (a\ b)$ be a transposition in S_n. Then

$$\sigma\tau\sigma^{-1}(\sigma(a)) = \sigma(b) \quad \text{and} \quad \sigma\tau\sigma^{-1}(\sigma(b)) = \sigma(a).$$

For $c \neq \sigma(a), \sigma(b)$, we have $\sigma^{-1}(c) \neq a, b$. It follows that $\tau(\sigma^{-1}(c)) = \sigma^{-1}(c)$, hence $\sigma\tau\sigma^{-1}(c) = c$. Therefore,

$$\sigma\tau\sigma^{-1} = (\,\sigma(a)\ \sigma(b)\,).$$

We have from (D.1) that

$$\begin{aligned}
&\sigma(a_1\ a_2\ a_3\ \ldots\ a_k)\sigma^{-1} \\
&\quad = [\sigma(a_1\ a_2)\sigma^{-1}]\,[\sigma(a_2\ a_3)\sigma^{-1}]\ \cdots\ [\sigma(a_{k-1}\ a_k)\sigma^{-1}] \\
&\quad = (\,\sigma(a_1)\ \sigma(a_2)\,)\,(\,\sigma(a_2)\ \sigma(a_3)\,)\ \cdots\ (\,\sigma(a_{k-1})\ \sigma(a_k)\,) \\
&\quad = (\,\sigma(a_1)\ \sigma(a_2)\ \sigma(a_3)\ \ldots\ \sigma(a_{k-1})\ \sigma(a_k)\,)
\end{aligned}$$

and similarly,

$$\sigma(b_1\ b_2\ \ldots\ b_l)\sigma^{-1} = (\,\sigma(b_1)\ \sigma(b_2)\ \sigma(b_3)\ \ldots\ \sigma(b_{l-1})\ \sigma(b_l)\,).$$

The result now follows from

$$\begin{aligned}
&\sigma[(a_1\ a_2\ \ldots\ a_k)\,(b_1\ b_2\ \ldots\ b_l)\ \cdots]\sigma^{-1} \\
&\quad = [\sigma(a_1\ a_2\ \ldots\ a_k)\sigma^{-1}]\,[\sigma(b_1\ b_2\ \ldots\ b_l)\sigma^{-1}]\ \cdots.
\end{aligned}$$ □

For the moment, we adopt the notation and perspective of Chapter 7 and view S_n as a group of field automorphisms on $F(t_1, t_2, \ldots, t_n)$. Thus, we have

$$\Delta = \prod_{1 \le i < j \le n} (t_i - t_j)$$

and

$$\sigma(\Delta) = \prod_{1 \le i < j \le n} (t_{\sigma(i)} - t_{\sigma(j)})$$

for each σ in $\mathcal{S}_n$. We define the *sign* of σ to be

$$\operatorname{sgn}(\sigma) = \frac{\sigma(\Delta)}{\Delta}.$$

Evidently, $\operatorname{sgn}(\sigma)$ equals 1 or -1. Note that $\{1, -1\}$ is a cyclic group under multiplication.

Theorem D.4. The map $\operatorname{sgn}\colon S_n \longrightarrow \{1, -1\}$ is a group homomorphism.

Proof. Take σ and τ in S_n. Since $\tau(\Delta) = \pm\Delta$, we have

$$\frac{\sigma\tau(\Delta)}{\tau(\Delta)} = \frac{\sigma(\Delta)}{\Delta} = \operatorname{sgn}(\sigma)$$

hence

$$\operatorname{sgn}(\sigma\tau) = \frac{\sigma\tau(\Delta)}{\Delta} = \frac{\sigma\tau(\Delta)}{\tau(\Delta)} \cdot \frac{\tau(\Delta)}{\Delta} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau). \qquad \square$$

A permutation σ in S_n is said to be *even* if $\operatorname{sgn}(\sigma) = 1$ and *odd* if $\operatorname{sgn}(\sigma) = -1$. The kernel of sgn, denoted by A_n, is called the *alternating group*:

$$A_n = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\}.$$

That is, A_n is the subgroup of S_n consisting of even permutations. In the context of Chapter 7, A_n is the stabilizer of Δ:

$$A_n = S_n(\Delta) = \{\sigma \in S_n : \sigma(\Delta) = \Delta\}. \tag{D.3}$$

Since A_n is the kernel of a homomorphism, $A_n \lhd S_n$. For any transposition τ in S_n, the coset τA_n is the set of odd permutations in S_n. Therefore, A_n has order $n!/2$, hence

$$[S_n : A_n] = 2. \tag{D.4}$$

We see from (D.1) and (D.2) that every permutation in S_n can be written as (decomposed into) a product of transpositions but not in a unique manner. However, as we now show, there is something invariant about such decompositions. Note that since sgn is a group homomorphism,

$$\operatorname{sgn}(\sigma\nu\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\nu)[\operatorname{sgn}(\sigma)]^{-1} = \operatorname{sgn}(\nu) \tag{D.5}$$

for all σ and ν in $\mathcal{S}_n$.

Theorem D.5. In any decomposition of a permutation into transpositions, the number of transpositions is always either even or odd, in accordance with the sign of the permutation.

Proof. Expressing Δ as

$$\Delta = (t_1 - t_2)\Big[\prod_{3\le j\le n}(t_1 - t_j)\Big]\Big[\prod_{3\le j\le n}(t_2 - t_j)\Big]\Big[\prod_{3\le i<j\le n}(t_i - t_j)\Big]$$

we see that $\operatorname{sgn}((1\ 2)) = -1$. It follows from (D.5) that

$$\operatorname{sgn}((1\ 3)) = \operatorname{sgn}((2\ 3)(1\ 2)(2\ 3)) = \operatorname{sgn}((1\ 2)) = -1$$
$$\operatorname{sgn}((1\ 4)) = \operatorname{sgn}((3\ 4)(1\ 3)(3\ 4)) = \operatorname{sgn}((1\ 3)) = -1$$

and so on. So, $\operatorname{sgn}((1\ a)) = -1$ for all $a \neq 1$ in $\mathcal{B}$. For arbitrary $a \neq b$ in $\mathcal{B}$, we have $(1\ a)(1\ b)(1\ a) = (a\ b)$. Therefore, $\operatorname{sgn}(\tau) = -1$ for all transpositions τ in S_n. Take ν in S_n, and let $\nu = \tau_1\tau_2\cdots\tau_m$ be a decomposition of ν into m transpositions. Then

$$\operatorname{sgn}(\nu) = \operatorname{sgn}(\tau_1)\operatorname{sgn}(\tau_2)\cdots\operatorname{sgn}(\tau_m) = (-1)^m. \qquad \square$$

Theorem D.6. For $n \ge 3$, A_n is generated by the 3-cycles in S_n.

Proof. Since A_n is the subgroup of S_n consisting of even permutations, it is generated by permutations of the form $(a_1\ a_2)(a_3\ a_4)$. If $(a_1\ a_2)$ and $(a_3\ a_4)$ are equal, then $(a_1\ a_2)(a_3\ a_4) = id$. If $(a_1\ a_2)$ and $(a_3\ a_4)$ have one element in common, say $a_2 = a_4$, then $(a_1\ a_2)(a_3\ a_4) = (a_1\ a_2\ a_3)$. If $(a_1\ a_2)$ and $(a_3\ a_4)$ have no element in common, then $(a_1\ a_2)(a_3\ a_4) = (a_1\ a_2\ a_3)(a_2\ a_3\ a_4)$. $\square$

Theorem D.7. For $n \ge 5$, A_n is simple.

Proof. Let $N \trianglelefteq A_n$, with $N \neq \langle id\rangle$. We need to show that $N = A_n$. Suppose that N contains a 3-cycle, which we may assume to be $\rho = (1\ 2\ 3)$. Let

$$\nu = \begin{pmatrix} 1 & 2 & 3 \\ a_1 & a_2 & a_3 \end{pmatrix}$$

where a_1, a_2, a_3 are arbitrary elements in $\mathcal{B}$. If ν is even (that is, if ν is in A_n), then $\nu\rho\nu^{-1} = (a_1\ a_2\ a_3)$ is in N. If ν is odd, let a_4 and a_5 be elements in $\mathcal{B}$ other than a_1, a_2, a_3. Then $(a_4\ a_5)\nu$ is even and

$$[(a_4\ a_5)\nu]\rho[(a_4\ a_5)\nu]^{-1} = (a_1\ a_2\ a_3)$$

is in N. This shows that N contains all 3-cycles. By Theorem D.6, $A_n \subseteq N$, hence $N = A_n$.

It remains to show that N contains a 3-cycle. Take α in $N\backslash\langle id\rangle$, let $\text{ord}(\alpha) = m$, and let p be a prime dividing m. Let $\sigma = \alpha^{m/p}$, and let $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ be the decomposition of σ into disjoint cycles. Since σ is of order p, by Theorem D.2, each of $\sigma_1, \sigma_2, \ldots, \sigma_k$ is a p-cycle. There are three cases to consider.

Case I. $p \geq 5$.
Renumbering if necessary, we may assume that

$$\sigma_1 = (1\ 2\ 3\ 4\ 5\ \ldots\ p).$$

Take $\beta = (1\ 2)(3\ 4)$ in A_n. Then

$$\beta\sigma_1\beta^{-1} = (2\ 1\ 4\ 3\ 5\ \ldots\ p)$$

hence

$$(1\ 3\ 5\ 4\ 2)\beta\sigma_1\beta^{-1} = (1\ 3\ 5\ 4\ 2)(2\ 1\ 4\ 3\ 5\ \ldots\ p) = \sigma_1.$$

Since $\beta, \sigma_2, \sigma_3, \ldots, \sigma_k$ are disjoint, and disjoint cycles commute, we have

$$(1\ 3\ 5\ 4\ 2)\beta\sigma\beta^{-1} = \sigma$$

hence

$$(1\ 3\ 5\ 4\ 2) = \sigma(\beta\sigma\beta^{-1})^{-1}.$$

Since σ and $\beta\sigma\beta^{-1}$ are in N, so is $(1\ 3\ 5\ 4\ 2)$. Take $\gamma = (1\ 3)(2\ 4)$ in A_n. Then

$$\gamma(1\ 3\ 5\ 4\ 2)\gamma^{-1} = (3\ 1\ 5\ 2\ 4)$$

is in N, and therefore, so is

$$(1\ 3\ 5\ 4\ 2)(3\ 1\ 5\ 2\ 4) = (1\ 4\ 5).$$

Case II. $p = 3$.
If $k = 1$, then σ is a 3-cycle and there is nothing to prove. Suppose that $k \geq 2$, in which case $n \geq 6$. Renumbering if necessary, we may assume that $\sigma_1 = (1\ 2\ 3)$ and $\sigma_2 = (4\ 5\ 6)$. Take $\beta = (1\ 2)(3\ 4)$ in A_n. Then

$$\beta\sigma_1\sigma_2\beta^{-1} = (1\ 4\ 2)(3\ 5\ 6)$$

hence

$$(1\ 3\ 4\ 2\ 5)\beta\sigma_1\sigma_2\beta^{-1} = (1\ 3\ 4\ 2\ 5)(1\ 4\ 2)(3\ 5\ 6) = \sigma_1\sigma_2.$$

Since $\beta, \sigma_3, \sigma_4, \ldots, \sigma_k$ are disjoint, we have

$$(1\ 3\ 4\ 2\ 5)\beta\sigma\beta^{-1} = \sigma$$

hence

$$(1\ 3\ 4\ 2\ 5) = \sigma(\beta\sigma\beta^{-1})^{-1}.$$

Since σ and $\beta\sigma\beta^{-1}$ are in N, so is (1 3 4 2 5), and we are back to Case I.

Case III. $p = 2$.
Since σ is in $N \subseteq A_n$, k must be even, so $k \geq 2$. Renumbering if necessary, we may assume that $\sigma_1 = (1\ 2)$ and $\sigma_2 = (3\ 4)$. Take $\beta = (1\ 2\ 3)$ in A_n. Then

$$\beta\sigma_1\sigma_2\beta^{-1} = (1\ 4)(2\ 3)$$

hence

$$(1\ 3)(2\ 4)\beta\sigma_1\sigma_2\beta^{-1} = (1\ 3)(2\ 4)(1\ 4)(2\ 3) = \sigma_1\sigma_2.$$

Since $\beta, \sigma_3, \sigma_4, \ldots, \sigma_k$ are disjoint, we have

$$(1\ 3)(2\ 4)\beta\sigma\beta^{-1} = \sigma$$

hence

$$(1\ 3)(2\ 4) = \sigma(\beta\sigma\beta^{-1})^{-1}.$$

Since σ and $\beta\sigma\beta^{-1}$ are in N, so is $(1\ 3)(2\ 4)$. Take $\gamma = (1\ 3)(2\ 5)$ in A_n. Then

$$\gamma(1\ 3)(2\ 4)\gamma^{-1} = (1\ 3)(4\ 5)$$

is in N, and therefore, so is

$$[(1\ 3)(2\ 4)][(1\ 3)(4\ 5)] = (2\ 4\ 5).$$

Thus, N contains a 3-cycle. □

Theorem D.8. For $n \geq 5$, the only normal subgroups of S_n are itself, A_n, and $\langle id \rangle$.

Proof. The proof is almost identical to that of Theorem D.7, except that here we assume that $N \trianglelefteq S_n$, as opposed to the situation in Theorem D.7, where $N \trianglelefteq A_n$. If we replace A_n with S_n in each of Cases I–III, the arguments proceed as before, and we find that $A_n \subseteq N$. However, in Case III, σ was restricted to $N \subseteq A_n$, so $k = 1$ was excluded. Accordingly, we now consider that possibility, which means

that σ is a transposition in N. Let ν be an arbitrary element in S_n. Then $\nu\sigma\nu^{-1}$ is in N, and by Theorem D.3, this gives rise to all transpositions as ν ranges over S_n. Since S_n is generated by its transpositions, we have $N = S_n$. Therefore, $A_n \subseteq N \subseteq S_n$. It follows from

$$[S_n : N][N : A_n] = [S_n : A_n] = 2$$

that N is either A_n or S_n. □

We remark that Theorems D.7 and D.8 are the group-theoretic counterparts to Theorems 7.14 and 7.13, respectively.

Theorem D.9. S_n is solvable only if $n \leq 4$.

Proof. We saw in Chapter 15 that S_n is solvable for $n \leq 4$. Take $n \geq 5$. By Theorems D.7 and D.8, the only normal series for S_n are

$$\langle id \rangle \lhd S_n \quad \text{and} \quad \langle id \rangle \lhd A_n \lhd S_n.$$

Since

$$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4) \quad \text{and} \quad (1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3)$$

we see that A_n and S_n are not Abelian. Therefore, S_n is not solvable. □

A subgroup H of S_n is said to be *transitive* if, for any a and b in $\mathcal{B}$, there is σ in H such that $\sigma(a) = b$.

Theorem D.10. Let p be a prime, and let G be a transitive subgroup of S_p. If $H \trianglelefteq G$ and $H \neq \langle id \rangle$, then H is transitive.

Proof. Define an action of H on $\mathcal{B}$ by setting $\tau \cdot a = \tau(a)$ for each τ in H and each a in $\mathcal{B}$. Take σ in G. Since $H \trianglelefteq G$, we have $Ha = (\sigma^{-1}H\sigma)a$, hence $\sigma(Ha) = H\sigma(a)$, where $H\sigma(a)$ is the orbit of $\sigma(a)$ under the action. Therefore,

$$|Ha| = |\sigma(Ha)| = |H\sigma(a)|$$

for all σ in G. Since G is transitive, it follows that all orbits under the action have the same number of elements, which we denote by r. The action partitions $\mathcal{B}$ into, say, s distinct orbits. So, $p = rs$, and since p is prime, either $r = 1$ or $s = 1$. If $r = 1$, then $Ha = \{a\}$ for all a in $\mathcal{B}$, hence $H = \langle id \rangle$, which contradicts the choice of H. Thus, $s = 1$, hence $Ha = \mathcal{B}$ for all a in $\mathcal{B}$. Therefore, H is transitive on $\mathcal{B}$. □

Theorem D.11. Let p be a prime. The only elements of S_p of order p are the p-cycles.

Proof. Let σ in S_p be of order p, and let ν be a cycle in the decomposition of σ into disjoint cycles. By Theorem D.2, ν is of order p, so it is a p-cycle. Therefore, $\sigma = \nu$. □

Theorem D.12. Let p be a prime, and let G be a subgroup of S_p. If G is transitive, then G contains a p-cycle.

Proof. Define an action of G on $\mathcal{B}$ by setting $\sigma \cdot a = \sigma(a)$ for each σ in G and each a in $\mathcal{B}$. By Theorem A.2(c), $|G| = p|G(a)|$ for all a in $\mathcal{B}$. It follows from Theorem A.3 that G contains an element ν of order p. By Theorem D.11, ν is a p-cycle. □

Theorem D.13. Let p be a prime, and let G be a subgroup of S_p. If G contains a transposition and a p-cycle, then $G = S_p$.

Proof. Relabeling the elements of $\mathcal{B}$ if necessary, and taking a power of the p-cycle if necessary, we may assume that the transposition is $(1\ 2)$ and the p-cycle is $\rho = (1\ 2\ \ldots\ p)$. So, G contains

$$\rho(1\ 2)\rho^{-1} = (2\ 3)$$
$$\rho(2\ 3)\rho^{-1} = (3\ 4)$$

and so on, which implies that G contains

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$$
$$(1\ 3)(3\ 4)(1\ 3) = (1\ 4)$$

and so on. For arbitrary $a \neq b$ in $\mathcal{B}$, we have $(1\ a)(1\ b)(1\ a) = (a\ b)$, so G contains all transpositions. Therefore, $G = S_p$. □

APPENDIX E

FINITE FIELDS AND NUMBER THEORY

Let $a_1, a_2, \ldots, a_n$ be integers, not all of which are zero. The *greatest common divisor* of $a_1, a_2, \ldots, a_n$, denoted by $\gcd(a_1, a_2, \ldots, a_n)$, is the largest natural number that divides each of $a_1, a_2, \ldots, a_n$. For an arbitrary natural number c,

$$\gcd(ca_1, ca_2, \ldots, ca_n) = c \gcd(a_1, a_2, \ldots, a_n).$$

We say that $a_1, a_2, \ldots, a_n$ are *relatively prime* (to each other) if $\gcd(a_1, a_2, \ldots, a_n) = 1$.

Theorem E.1. For all integers m and n, there are integers a and b such that

$$\gcd(m, n) = am + bn.$$

Proof. The proof is essentially that given for the Division Algorithm, except that the absolute value of integers is used as a measure of magnitude instead of the degree of polynomials. □

The *phi-function* φ is defined as follows. For each natural number n, $\varphi(n)$ is the number of natural numbers less than or equal to n that are relatively prime to n, that is,

$$\varphi(n) = |\{k : 1 \leq k \leq n; \gcd(k, n) = 1\}|.$$

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Theorem E.2. Let m and n be relatively prime natural numbers. Then $\varphi(mn) = \varphi(m)\varphi(n)$. Let $n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ be the factorization of n into distinct primes. Then

$$\varphi(n) = p_1^{d_1-1}(p_1 - 1)p_2^{d_2-1}(p_2 - 1) \cdots p_m^{d_m-1}(p_m - 1).$$

Proof. We have from (5.4) that $|\pi_n| = \varphi(n)$ for all natural numbers n. By Theorem 5.2(b), $|\pi_{mn}| = |\pi_m|\,|\pi_n|$, hence $\varphi(mn) = \varphi(m)\varphi(n)$. Let p be a prime, and let d be a natural number. The natural numbers less than or equal to p^d that are not relatively prime to p^d are precisely those that are divisible by p, of which there are p^{d-1}. Therefore,

$$\varphi(p^d) = p^d - p^{d-1} = p^{d-1}(p - 1).$$

It follows from the multiplicative property of φ just demonstrated that

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{d_1})\varphi(p_2^{d_2}) \cdots \varphi(p_m^{d_m}) \\ &= p_1^{d_1-1}(p_1 - 1)p_2^{d_2-1}(p_2 - 1) \cdots p_m^{d_m-1}(p_m - 1).\end{aligned}$$ □

As discussed in Chapter 5, the group of units of an arbitrary field $\mathcal{F}$ is $\mathcal{F}^\times = \mathcal{F}\backslash\{0\}$.

Theorem E.3. Let $\mathcal{F}$ be a field (possibly of nonzero characteristic), and let $\mathcal{G}$ be a subgroup of $\mathcal{F}^\times$ of order n. Then $\mathcal{G}$ is cyclic with $\varphi(n)$ generators.

Proof. Let d be a natural number dividing n. Let $\mathcal{H}_d$ be a subgroup of $\mathcal{G}$ of order d, and consider the polynomial $h(x) = x^d - 1$ in $\mathcal{F}[x]$. By Theorem B.1(b), each of the d elements of $\mathcal{H}_d$ is a root of $h(x)$. Since $h(x)$ has at most d roots, $\mathcal{H}_d$ comprises all of them. Thus, $\mathcal{H}_d$ is the only subgroup of $\mathcal{G}$ of order d (cyclic or otherwise). By Theorems B.6(b) and B.10, $\mathcal{G}$ is cyclic with $\varphi(n)$ generators. □

Theorem E.4. Let p be a prime. Then $\mathbb{F}_p^\times$ is cyclic of order $p - 1$ with $\varphi(p - 1)$ generators.

Proof. This follows from Theorem E.3. □

Theorem E.5 (Fermat's Little Theorem). Let p be a prime, and let a be a nonzero integer. Then $a^{p-1} \equiv 1 \pmod{p}$, hence $a^p \equiv a \pmod{p}$.

Proof. Viewing a as an element of $\mathbb{F}_p^\times$, it follows from Theorems B.1(b) and E.4 that $a^{p-1} = 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$. The second congruence follows from the first. □

Theorem E.6. Let p be an odd prime, and let g be a primitive congruence root modulo p. Then $g^{(p-1)/2} \equiv -1 \pmod{p}$.

Proof. By Theorem E.5,

$$(g^{(p-1)/2}+1)(g^{(p-1)/2}-1) = g^{p-1}-1 \equiv 0 \,(\mathrm{mod}\, p).$$

Since $\mathbb{F}_p$ is a field, either

$$g^{(p-1)/2} \equiv 1 \,(\mathrm{mod}\, p) \quad \text{or} \quad g^{(p-1)/2} \equiv -1 \,(\mathrm{mod}\, p).$$

The former possibility is excluded, otherwise the order of g in $\mathbb{F}_p^{\times}$ would be less than $p-1$. □

For each natural number m, the *binomial formula* is

$$(x_0+x_1)^m = \sum_{i=0}^{m} \binom{m}{i} x_0^i x_1^{m-i}. \tag{E.1}$$

We refer to

$$\binom{m}{i} = \frac{m!}{i!\,(m-i)!}$$

as a *binomial coefficient*. By definition, $0! = 1$, hence

$$\binom{m}{0} = 1 = \binom{m}{m}.$$

The binomial formula generalizes to the *multinomial formula*,

$$(x_0+x_1+\cdots+x_n)^m = \sum_{(i_0,i_1,\ldots,i_n)} \binom{m}{i_0, i_1, \ldots, i_n} x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}$$

where the sum is over all $(n+1)$-tuples of nonnegative integers $(i_0, i_1, \ldots, i_n)$ such that $i_0 + i_1 + \cdots + i_n = m$. We refer to

$$\binom{m}{i_0, i_1, \ldots, i_n} = \frac{m!}{i_0!\, i_1! \cdots i_n!}$$

as a *multinomial coefficient*. All multinomial coefficients, hence all binomial coefficients, are natural numbers.

Theorem E.7. Let p be a prime, and let $f(x)$ be a polynomial in $\mathbb{Z}[x]$. Then $[f(x)]^p = f(x^p) + pg(x)$, where $g(x)$ is in $\mathbb{Z}[x]$.

Proof. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$. It can be shown that the multinomial coefficient

$$\binom{p}{i_0, i_1, \ldots, i_n}$$

is divisible by p except when $i_0 = p$, or $i_1 = p, \ldots$, or $i_n = p$, in which case the multinomial coefficient equals 1. Therefore,

$$(x_0 + x_1 + \cdots + x_n)^p = x_0^p + x_1^p + \cdots + x_n^p + ph(x_0, x_1, \ldots, x_n)$$

where h is in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$. Setting $x_i = a_i x^i$ for $i = 0, 1, \ldots, n$, we find that

$$[f(x)]^p = a_n^p x^{pn} + a_{n-1}^p x^{p(n-1)} + \cdots + a_1^p x^p + a_0^p + ps(x)$$

where $s(x)$ is in $\mathbb{Z}[x]$. By Theorem E.5, for each i, we have $a_i^p = a_i + b_i p$ for some b_i in $\mathbb{Z}$. Let

$$r(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

Then

$$[f(x)]^p = f(x^p) + pr(x^p) + ps(x).$$

We take $g(x) = r(x^p) + s(x)$. □

APPENDIX F

FURTHER READING

The table below provides references for specific theorems and examples appearing in this book that are less likely to be found in standard expositions of Galois theory. The citations given are suggestions for further reading and at the same time acknowledgements of the work of others. The excellent books by Cox (2012) and Tignol (2001) are general sources for several chapters of this book, particularly Chapters 8, 12, and 13.

Topic	References
Theorem 3.9	Minác (2003)
Theorem 3.11	Minác (2003)
	Section 4.2 of Tignol (2001)
Theorem 3.17	Masser (1966)
	Goodstein (1969)
Theorem 3.18	Exercise 3.5(4) of Escofier (2001)
	Exercise 4 of Chapter 8 of Tignol (2001)
	Theorem 8.10 of Tignol (2001)
Theorem 3.19	Theorem 1.3.1 of Cox (2012)
Theorem 4.10(b)	Lemma 34j of Hadlock (1978)
Theorem 4.11	Lemma of Section 44 of Edwards (1984)
Theorems 4.13 and 4.14	Theorem IV of Dörrie (1965)

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

Topic	References
	Proposition of Section 44 of Edwards (984)
	Theorem 8 of Article 58 of Weisner (1938)
Theorem 4.16(a)	Theorem IV of Dörrie (1965)
Theorem 4.17	Theorem 10 of Article 58 of Weisner (1938)
Theorem 5.4	Article 134 of Clark (1971)
	Theorem 9.1.9 of Cox (2012)
	Proposition of Section 70 of Edwards (1984)
	Theorem 4.2.6 of Weintraub (2006)
Example 6.8	Section 21.2 of Stewart (2004)
Theorem 6.15	Theorem 9.2.14 of Cox (2012)
	Theorem 21.2 of Stewart (2004)
	Corollary 12.29 of Tignol (2001)
Theorems 6.18 and 6.19	Articles 237–240 of Burnside and Panton (1960)
	Appendices A and B of Pesic (2003)
	Rosen (1995)
	Section 13.3 of Tignol (2001)
Theorem 6.21	Section 8.6 of Cox (2012)
	Section 14.7 of Dummit and Foote (2004)
	Theorem 102 of Rotman (1990)
	Section 8.8 of van der Waerden (1991)
Theorem 6.22	Section 68 of Edwards (1984)
Theorem 6.23	Chapter 25 of Dörrie (1965)
Theorem 7.2	Theorems 10.6 and 10.7 of Howie (2006)
Theorems 7.10 and 7.11	Ayoub (1980, 1982)
	Section 13.4 of Tignol (2001)
Theorem 7.12	Section 29 of Dehn (1960)
	Article 231 of Burnside and Panton (1960)
Theorem 7.13	Article 232 of Burnside and Panton (1960)
Theorem 7.14	Article 233 of Burnside and Panton (1960)
Theorem 7.17	Articles 229 and 230 of Burnside and Panton (1960)
	Theorems 12.1.6 and 12.1.9 of Cox (2012)
	Sections 35 and 36 of Dehn (1960)
	Sections 29 and 30 of Edwards (1984)
	Theorem 10.4 of Tignol (2001)
Theorem 7.20	Proposition 10.5 of Tignol (2001)
Theorem 8.2	Section 32 of Edwards (1984)
Theorem 8.3	Theorem of Article 58 of Dickson (1902)
	Section 37 of Edwards (1984)
	Proposition 14.7 of Tignol (2001)
Theorem 8.10	Theorem of Article 69 of Dickson (1902)
	Corollary of Section 41 of Edwards (1984)
	Corollaries 14.12 and 14.14 of Tignol (2001)

Topic	References
Theorem 8.12	Section 68 of Dehn (1960)
	Proposition I of Section 41 of Edwards (1984)
Theorem 8.13	Theorem of Article 70 of Dickson (1902)
Theorem 9.27	Exercise 10 of Sixth Exercise Set of Edwards (1984)
Theorems 10.1 and 10.2	Section 10.6 of Escofier (2001)
Theorem 10.4	F1 of Chapter 14 of Lorenz (2006)
Theorem 10.5	Section 2 of Chapter II.2 of Postnikov (2004)
Theorem 11.2	Lemma 8.3.1 of Cox (2012)
Theorem 12.2	Section 14.1 of Cox (2012)
	Section 85 of Dehn (1960)
	Article 100 of Dickson (1902)
	Theorems 14.38 and 14.40 of Tignol (2001)
Theorem 12.7	Corollary 14.43 of Tignol (2001)
Theorem 12.8	Subsection A of Section 6.4 of Cox (2012)
Chapter 13	Section VII of Gauss (1801)
Theorem 13.3	Proposition 9.2.1 of Cox (2012)
Theorem 13.4	Proposition 9.2.4 of Cox (2012)
Theorem 13.6	Proposition 9.2.6 and Corollary 9.2.7 of Cox (2012)
	Propositions 12.22–12.24 of Tignol (2001)
Theorem 13.7	Proposition 9.2.8 of Cox (2012)
	Proposition 12.25 of Tignol (2001)
Example 13.8	Section 14.5 of Dummit and Foote (2004)
Theorem 13.9	Proposition 9.2.9 of Cox (2012)
Theorem 13.10	Example 9.2.5 of Cox (2012)
	Section 12.4 of Tignol (2001)
Example 13.11	Article 137 of Clark (1971)
Example 13.12	Article 138 of Clark (1971)
	Section 2.7 of Hadlock (1978)
	Chapter 7 of Rademacher (1964)
Example 13.13	Example 9.2.2 of Cox (2012)
Theorem 14.1	Landau (1992, 1994)
	Zippel (1985)
Theorem 14.2	Borodin et al. (1985)
	Zippel (1985)
Chapter 15	Articles 146–148 of Clark (1971)
	Chapter VIII of Dehn (1960)
	Chapters I and IV of Dickson (1902)
	Section 8.8 of van der Waerden (1991)
Theorem A.3	Article 55 of Clark (1971)

REFERENCES

BOOKS AND MONOGRAPHS ON GALOIS THEORY AND RELATED TOPICS

E. Artin, *Galois Theory*, 2nd ed. (University of Notre Dame Press, Notre Dame, 1944).

J. R. Bastida, *Field Extensions and Galois Theory*. (Addison-Wesley, Menlo Park, CA, 1984).

J. Bewersdorff, *Galois Theory for Beginners: A Historical Perspective*. (American Mathematical Society, Providence, RI, 2006).

W. S. Burnside and A. W. Panton, *The Theory of Equations: With an Introduction to the Theory of Binary Quadratic Forms*, Volume II. (Dover, New York, 1960), (Unabridged and unaltered republication of seventh edition published by Longmans, Green and Company in 1928.).

A. Chambert-Loir, *A Field Guide to Algebra*. (Springer, New York, 2005).

A. Clark, *Elements of Abstract Algebra*. (Wadsworth, Belmont, CA, 1971).

R. Cooke, *Classical Algebra: Its Nature, Origins, and Uses*. (John Wiley & Sons, Inc., Hoboken, NJ, 2008).

D. A. Cox, *Galois Theory*, 2nd ed. (John Wiley & Sons, Inc., Hoboken, NJ, 2012).

E. Dehn, *Algebraic Equations: An Introduction to the Theories of Lagrange and Galois*. (Dover, Mineola, NY, 1960), (Unabridged and corrected republication of book originally published by Columbia University Press in 1930.).

L. E. Dickson, Introduction to the Theory of Algebraic Equations. In: *Congruence of Sets and Other Monographs*. (Chelsea, New York, 1902, 1967).

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.

H. Dörrie, *Section 25: Abel's Impossibility Theorem*. In: *100 Great Problems of Elementary Mathematics: Their History and Solution*. (Dover, New York, 1965).

D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. (John Wiley & Sons, Inc., Hoboken, NJ, 2004).

H. M. Edwards, *Galois Theory*. (Springer-Verlag, New York, 1984).

J.-P. Escofier, *Galois Theory*. (Springer, New York, 2001).

M. H. Fenrick, *Introduction to the Galois Correspondence*. (Birkhäuser, Boston, MA, 1992).

L. Gaal, *Classical Galois Theory with Examples*, 4th ed. (Chelsea, New York, 1988).

D. J. H. Garling, *A Course in Galois Theory*. (Cambridge University Press, Cambridge, 1986).

C. F. Gauss, *Disquisitiones Arithmeticae: English Edition*. (Springer-Verlag, New York, 1966).

C. R. Hadlock, *Field Theory and Its Classical Problems*. (Mathematical Association of America, Washington, DC, 1978).

J. M. Howie, *Fields and Galois Theory*. (Springer, London, 2006).

N. Jacobson, *Basic Algebra 1*, 2nd ed. (W. H. Freeman & Company, New York, 1985).

R. B. King, *Beyond the Quartic Equation*. (Birkhäuser, Boston, MA, 1996).

S. Lang, *Algebra*, 3rd ed. (Addison-Wesley, Reading, MA, 1993).

F. Lorenz, *Algebra: Fields and Galois Theory*, Volume I. (Springer, New York, 2006).

Maplesoft, *Maple User Manual*. (Waterloo Maple Inc., Toronto, 2011).

G. B. Mathews and W. E. H. Berwick, *Algebraic Equations*. (Hafner, New York, 1929).

P. Morandi, *Field Theory and Galois Theory*. (Springer, New York, 1996).

P. Pesic, *Abel's Proof: An Essay on the Sources of Meaning of Mathematical Unsolvability*. (MIT Press, Cambridge, 2003).

M. M. Postnikov, *Foundations of Galois Theory*. (Dover, Mineola, 2004), (Unabridged and unaltered republication of the first English edition originally published by The MacMillan Company in 1962.).

H. Rademacher, *Lectures on Elementary Number Theory*. (Robert E. Kreiger, Malabar, FL, 1964).

L. T. Rigatelli, *Evariste Galois, 1811–1832*. (Birkhäuser Verlag, Basel, 1996).

S. Roman, *Field Theory*. (Springer-Verlag, New York, 1995).

J. Rotman, *Galois Theory*, 2nd ed. (Springer, New York, 1990).

I. Stewart, *Galois Theory*, 3rd ed. (Chapman & Hall/CRC, Boca Raton, FL, 2004).

J. Swallow, *Exploratory Galois Theory*. (Cambridge University Press, Cambridge, 2004).

J.-P. Tignol, *Galois' Theory of Algebraic Equations*. (World Scientific, Singapore, 2001).

B. L. van der Waerden, *Algebra*, 7th ed., Volume I. (Springer-Verlag, New York, 1991).

S. H. Weintraub, *Galois Theory*. (Springer, New York, 2006).

L. Weisner, *Introduction to the Theory of Equations*. (Macmillan, New York, 1938).

PAPERS ON GALOIS THEORY AND RELATED TOPICS

R. G. Ayoub, Paolo Ruffini's contributions to the quintic. Archive for History of Exact Sciences **23**, 253–277 (1980).

R. G. Ayoub, On the nonsolvability of the general polynomial. American Mathematical Monthly **89**, 397–401 (1982).

O. Bolza, On the theory of substitution groups and its applications to algebraic equations. American Journal of Mathematics **13**, 59–144 (1890–91).

A. Borodin, R. Fagin, J. E. Hopcroft, and M. Tompa, Decreasing the nesting depth of expressions involving square roots. Journal of Symbolic Computation **1**, 169–188 (1985).

L. Gårding and C. Skau, Niels Henrik Abel and solvable equations. Archive for History of Exact Sciences **48**, 81–103 (1994).

R. L. Goodstein, The discriminant of a certain polynomial. The Mathematical Gazette **53**, 60–61 (1969).

B. M. Kiernan, The development of Galois theory from Lagrange to Artin. Archive for History of Exact Sciences **8**, 40–154 (1971–72).

S. Landau, A note on "Zippel denesting". Journal of Symbolic Computation **13**, 41–45 (1992).

S. Landau, How to tangle with a nested radical. The Mathematical Intelligencer **16**, 49–55 (1994).

D. W. Masser, The discriminants of special functions. The Mathematical Gazette **50**, 158–160 (1966).

J. H. McKay, Another proof of Cauchy's group theorem. American Mathematical Monthly **66**, 119 (1959).

J. Minác, Newton's identities once again! American Mathematical Monthly **110**, 232–234 (2003).

J. Pierpont, Galois' theory of algebraic equations. Part I. Rational resolvents. Annals of Mathematics, 2nd series **1**, 113–143 (1899–1900).

J. Pierpont, Galois' theory of algebraic equations. Part II. Irrational resolvents. Annals of Mathematics, 2nd series **2**, 22–56 (1900–1901).

I. Radloff, Évariste Galois: principles and applications. Historia Mathematica **29**, 114–137 (2002).

M. I. Rosen, Niels Hendrik Abel and equations of the fifth degree. American Mathematical Monthly **102**, 495–505 (1995).

T. Rothman, Genius and biographers: the fictionalization of Evariste Galois. American Mathematical Monthly **89**, 84–106 (1982).

R. Zippel, Simplification of expressions involving radicals. Journal of Symbolic Computation **1**, 189–210 (1985).

This page intentionally left blank

INDEX

A Classical Introduction to Galois Theory, First Edition. Stephen C. Newman.