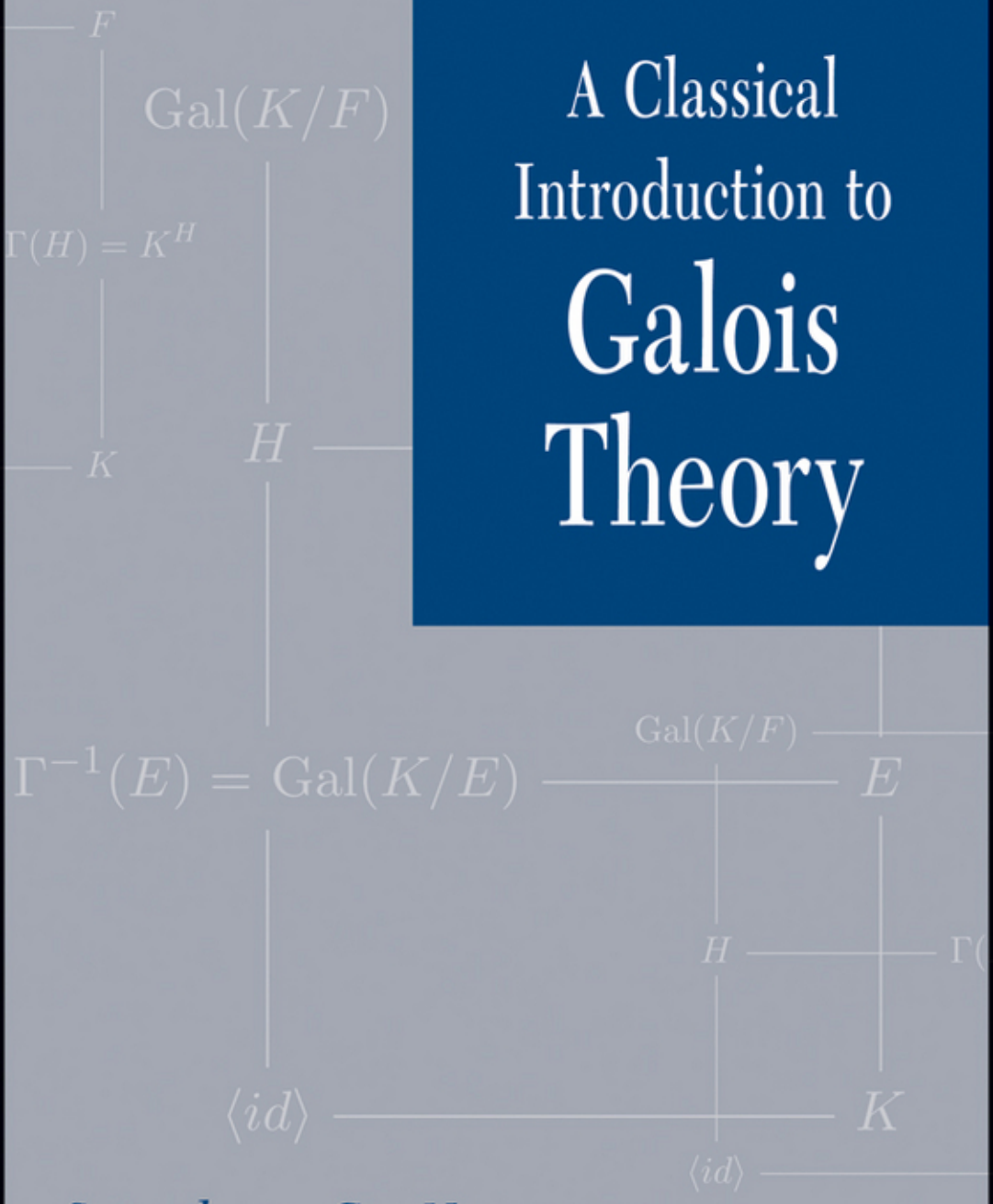
A Classical Introduction to Galois Theory



Stephen C. Newman

WILEY

A CLASSICAL INTRODUCTION TO GALOIS THEORY

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

CONTENTS

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

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

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

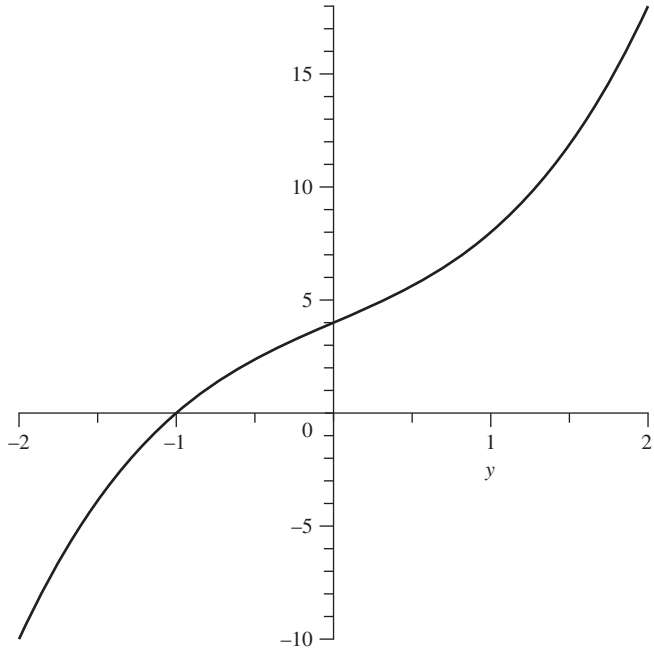
$$\begin{aligned}
\beta_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \\
\beta_2 &= \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}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

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

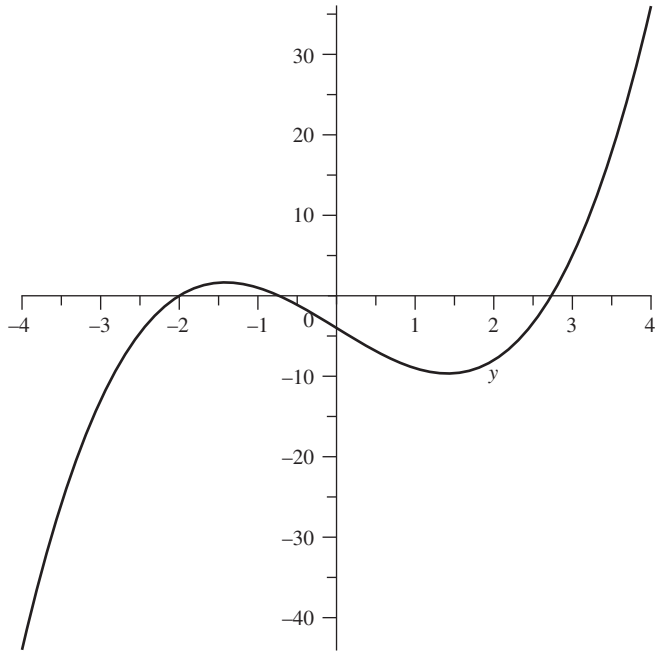
$$g(y) = (y+1)(y^2 - y + 4)$$

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

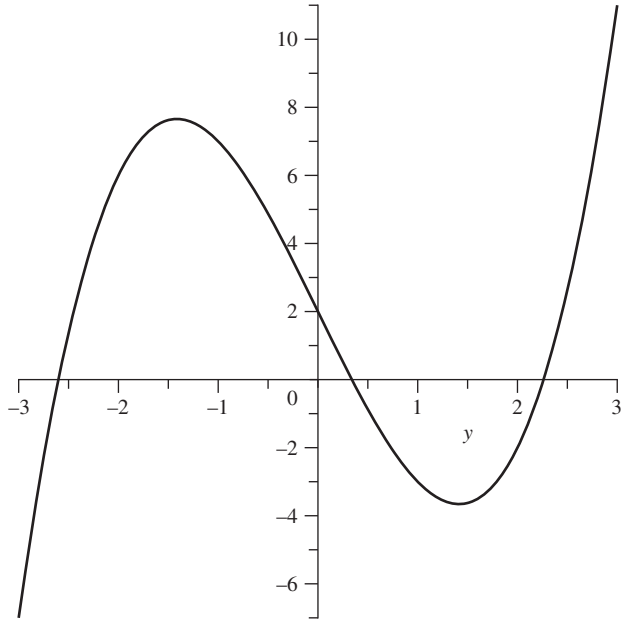
$$g(y) = (y+2)(y^2 - 2y - 2)$$

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

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