Graduate Texts in Mathematics

Harold M. Edwards

Galois Theory

伽罗瓦理论

Springer

世界图书出版公司
www.wpcbj.com.cn

Harold M. Edwards

Galois Theory

Springer

图书在版编目（CIP）数据

伽罗瓦理论 = Galois Theory：英文/（美）爱德华兹（Edwards，H. M.）著. —影印本. 北京：世界图书出版公司北京公司，2010. 9

ISBN 978 - 7 - 5100 - 2742 - 0

Ⅰ. ①伽… Ⅱ. ①爱… Ⅲ. ①伽罗瓦理论—英文 Ⅳ. ①0153. 4

中国版本图书馆 CIP 数据核字（2010）第 168670 号

书　　名：	Galois Theory
作　　者：	Harold M. Edwards
中 译 名：	伽罗瓦理论
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话：	010 - 64021602，010 - 64015659
电子信箱：	kjb@ wpcbj. com. cn
开　　本：	24 开
印　　张：	7. 5
版　　次：	2010 年 09 月
版权登记：	图字：01 - 2010 - 1413
书　　号：	978 - 7 - 5100 - 2742 - 0/O · 832　　**定　　价：** 29. 00 元

Harold M. Edwards
New York University
Courant Institute of
Mathematical Sciences
251 Mercer Street
New York, NY 10012
USA

AMS Classifications: 12-01, 12-03, 12A55, 01A55

Library or Congress Cataloging in Publication Data
Edwards, Harold M.
Galois theory.
(Graduate texts in mathematics; 101)
Bibliography: p.
Includes index.
1. Galois theory. I. Title. II. Series.
QA247.E383 1984 512'.32 83-20082

9 8 7 6 5 4 3 (Corrected third printing, 1998)

ISBN 0-387-90980-X Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-90980-X Springer-Verlag Berlin Heidelberg New York SPIN 10644911

Graduate Texts in Mathematics 101

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.

continued after index

To Betty

Preface

This exposition of Galois theory was originally going to be Chapter 1 of the continuation of my book *Fermat's Last Theorem*, but it soon outgrew any reasonable bounds for an introductory chapter, and I decided to make it a separate book. However, this decision was prompted by more than just the length. Following the precepts of my sermon "Read the Masters!" [E2], I made the reading of Galois' original memoir a major part of my study of Galois theory, and I saw that the modern treatments of Galois theory lacked much of the simplicity and clarity of the original. Therefore I wanted to write about the theory in a way that would not only explain it, but explain it in terms close enough to Galois' own to make his memoir accessible to the reader, in the same way that I tried to make Riemann's memoir on the zeta function and Kummer's papers on Fermat's Last Theorem accessible in my earlier books, [E1] and [E3]. Clearly I could not do this within the confines of one expository chapter.

And so I decided to write a short book—a sort of volume $1\frac{1}{2}$ of my work on Fermat's Last Theorem—devoted entirely to the basics of Galois theory. There is very little in this book that is not already to be found, however concisely and however lacking in proof, in Galois. The one major exception is the material on factorization of polynomials (§§49–61), which is due to Kronecker and which seems to me to be necessary to give clear meaning to the computations with roots of algebraic equations that Galois and Lagrange performed without inhibition and without comment.

The crux of Galois theory is, appropriately enough, Galois' Proposition I, which is the following characterization of what we call the *Galois group* of an equation. Let $a, b, c, \ldots$ be the n roots (assumed distinct) of an algebraic equation $f(x) = 0$ of degree n. The Galois group is a certain subgroup of the group of permutations of the roots $a, b, c, \ldots$. Galois used it to deter-

mine whether a given polynomial in the roots $F(a, b, c, \ldots)$ has a known value—in modern parlance, to determine whether $F(a, b, c, \ldots)$ is in the ground field. The characteristic property of the Galois group is that $F(a, b, c, \ldots)$ has a known value if and only if

$$F(a, b, c, \ldots) = F(Sa, Sb, Sc, \ldots)$$

for all permutations S of the Galois group. Galois proved the existence and uniqueness of a group with this property by *constructing* it, using what later became known as a Galois resolvent. (This characterization of the Galois group will be more recognizable to readers familiar with modern formulations of Galois theory after they read the first corollary in §41. See also §63.)

The major theorems of Galois, such as the theorems on the solvability of equations by radicals, flow from the study of the relationship between algebraic equations $f(x) = 0$ and the groups associated with them. Of particular importance is the analysis of the way in which the group is reduced when the field of known quantities is extended (Galois' Propositions II–IV).

Some recent texts on Galois theory place mistaken emphasis on the question of finding explicit quintic equations, with rational coefficients, which cannot be solved by radicals. This is a moderately interesting result (one not covered in this book) but it is not a key theorem of Galois theory. Galois showed that an algebraic equation is solvable by radicals if and only if the associated group is solvable. A given quintic with rational coefficients can therefore be tested for solvability. Abel's theorem that the *general* quintic is not solvable states that the equation $x^5 + Bx^4 + Cx^3 + Dx^2 + Ex + F = 0$—an equation with coefficients in the field $\mathbb{Q}(B, C, D, E, F)$ obtained by adjoining five transcendental elements (variables) to $\mathbb{Q}$—is not solvable by radicals. (In Galois theory this follows from the fact that the Galois group of this equation is the full group of 120 permutations of the five roots.) In other words, no field extension of $\mathbb{Q}(B, C, D, E, F)$ obtained by a succession of adjunctions of radicals can ever contain a root of the given equation. This is what it means to say that the quadratic formula

$$x = \frac{-B \pm \sqrt{B^2 - 4C}}{2},$$

and the much more complicated formulas for the cubic and quartic equations (Exercises 1 and 2 of the Sixth Set) have no generalization to the quintic equation.

Having just mentioned the exercises, I hasten to reassure the reader that *the exercises are not essential to the book*. The only proofs that are relegated to the exercises are those that I believe to be too easy, or too much like other proofs already covered, to spend time on in the text. Naturally, the reader who does the exercises will have a far greater understanding of the subject, and will learn many things not contained in the text, but to do all the exercises will surely consume an enormous amount of time. The reader who has just

read the text will have covered all the propositions and methods of proof that I consider to be basic to Galois theory.

What preparation do I assume on the part of the reader? Because terminology changes so much from decade to decade and from field to field, I have tried to assume as little terminology as possible. (When I completed my undergraduate degree 25 years ago, I had had courses in advanced calculus, determinants and matrices, differential equations, measure theory, complex variables, etc., but I had never encountered the definition of a group or an abstract vector space.) However, I have assumed a certain degree of mathematical *experience* on the part of the reader, by which I mean experience in computation and mathematical reasoning. The main theorems of Galois theory state, in the last analysis, that certain computations with polynomials produce certain results. In most cases the computations are too long to do, and the *idea* of the computation is what counts, not any particular cases of it. The reader should have enough mathematical experience (and talent) to be able to conceive a general computation and its properties after having done a few simple examples.

The approach of the book is consistently *algebraic* and *constructive*. The fields considered are those obtained from the rational numbers by adjoining a finite number of algebraic and/or transcendental elements. (Fields with characteristic p are mentioned only in passing. Fields obtained by completion processes—the real and complex numbers, algebraic extensions of p-adic fields—are not considered at all.) *The constructive approach implies that theorems mean what they say.* For example, when a theorem says that an equation is solvable, the proof must give a procedure—however impractical—for constructing a splitting field by the adjunction of radicals. I believe that this approach is very much in tune with Galois' conception of the subject.

Liouville, in the "Avertissment" preceding his publication of Galois' works in 1846, writes of the "vivid pleasure" he enjoyed when he realized that Galois' methods were correct and that his theorems could be rigorously proved. I experienced what I imagine was a similar—if lesser—pleasure when I realized that two parts of Galois' memoir, which I at first thought were mistakes, are perfectly correct. These are the places where Galois later wrote "*On jugera*", in the case of the first, and "Something in this proof needs to be completed—I haven't the time" in the case of the second.

The "*On jugera*" passage is the one where Galois proves the crucial lemma stating that any rational function of the roots can be expressed as a rational function of the Galois resolvent. Poisson had called Galois' proof "insufficient" but pointed out that the lemma followed from a theorem of Lagrange. Galois, rather than elucidate his proof, laconically replied, "That remains to be seen" (freely translated). My opinion is in §37.

The famous statement "I haven't the time" occurs in a marginal note Galois made, probably on the night before the duel, with regard to the proof of his Proposition II, which he said needed to be "completed". Although his

proof appears wrong at first because he adjoins *one* root r of an equation and then uses *other* roots of the equation, and although Liouville [Gl, p. 492] found it necessary to circumvent Galois' proof entirely, I believe now that the proof given in §44 is very close to what Galois had in mind, and that the marginal note was merely prompted by the fact that he had *changed the statement of the Proposition*, and realized that the proof needed to be amended accordingly. (In fact, the Proposition, as stated, is false. The index of the subgroup need not be 1 or p when p is not prime—it must simply be a divisor of p.) A similar situation occurred with Proposition III, where Galois again changed the statement, making it more general, at the last minute, and had only time enough to say, "One will find the proof."

Finally, I hope it is superfluous to add that, while I have said above that most of what is in this book is already in Galois, the converse is far from true. The book contains a rather complete account of Galois' main memoir, "Mémoire sur les conditions de résolubilité des équations par radicaux" (Appendix 1 contains a translation of this memoir) but it does not make any claim to cover his other works. These contain, I am told, remarkable insights into a number of topics, including the theory of Abelian functions and finite simple groups. I return to my perennial refrain: Read the masters.

Acknowledgments

My greatest indebtedness is to Mr. James M. Vaughn, Jr., and the Vaughn Foundation Fund. This book is a direct result of their encouragement and support, for which I am deeply grateful. Work on the book was also supported by a Fellowship of the John Simon Guggenheim Memorial Foundation during 1981/82. I am grateful for both the financial support and the honor of a Guggenheim Fellowship. A large number of friends and colleagues have helped me by reading and commenting on early versions of the manuscript. Some major revisions prompted by their criticisms have not been seen by any of them, so it is even truer than usual that they are entitled to credit for many improvements in the book but free from blame for its faults. I would especially like to thank the following for their help: Jay Goldman, Mel Hausner, M.Y. Hirano, Christian Houzel, Susan Landau, Richard Pollack, Walter Purkert, Michael Rosen, Gabriel Stolzenberg, René Taton, William Y. Vélez, B.L. van der Waerden, and an anonymous reader for Springer-Verlag. Finally, my thanks to New York University and the Courant Institute for their overall support and assistance, including a sabbatical year 1980/81, the excellent library, and the expert word-processing of Connie Engle.

Contents

Galois

§1 Great mathematicians usually have undramatic lives, or, more precisely, the drama of their lives lies in their mathematics and cannot be appreciated by nonmathematicians. The great exception to this rule is Evariste Galois (1811–1832). Galois' life story—what we know of it—is like a romantic novel. Although he was making important mathematical discoveries when he was still in secondary school, he was denied admission to the Ecole Polytechnique, which was the premier institution of higher learning in mathematics at the time, and the mathematical establishment ignored, mislaid, lost, and failed to understand his treatises. Meanwhile, he was persecuted for his political activities and spent many months in jail as a political prisoner. At the age of 20 he was killed in a duel involving, in some mysterious way, honor and a woman. On the eve of the fatal duel he wrote a letter to a friend outlining his mathematical accomplishments and asking that the friend try to bring his work to the attention of the mathematical world. Against great odds, Galois' few supporters did finally, 14 years after his death, succeed in finding an audience for his work, and portions of his writings were published in 1846 by Joseph Liouville in his *Journal de Mathematiques*. After that, recognition of the great importance of his work came very quickly, and Galois began to be regarded, as he is today, as one of the great creative mathematicians of all time.

§2 The purpose of this book is to convey the mathematical drama of Galois' work, so there will be no more mention of his short, unhappy life,* but

* For biographical information see Dupuy [D1], Kiernan [K1], Rothman [R1].

one point needs to be made about its most dramatic feature, namely, the fact that Galois was able, at such an early age and without the benefit of any formal higher education, to make discoveries that would win him lasting fame. Surely many aspiring young mathematicians have been discouraged by Galois' story, saying to themselves something like, "Here I am already x years old, $x - 20$ years older (younger) than Galois was when he *died*, and, although I like math and have always done well at it, I would no more be able to make a great discovery than I would be able to swim the Atlantic." How was Galois able to do it? Was he blessed with some superhuman gift that put him in a class apart? I think not. Of course, talent is essential, and few are as talented as Galois. Still, talent alone is not enough. Galois had to reach the point where he knew enough and had enough techniques at his command to be able to move beyond what had been done before. The secret of how he was able to do this is contained, I believe, in a passage in Dupuy's biography of Galois [D1, p. 206]: "Elementary algebra books never satisfied Galois because he didn't find in them the stamp of the inventors; right from his first year of mathematics he turned to Lagrange."

Lagrange's *Réflexions sur la Résolution Algébrique des Equations* (1771) is the treatise of Lagrange most likely to have inspired the creation of Galois theory. It is an extraordinary work, written in a relaxed, discursive style that was rather common in the eighteenth century, but is virtually unknown in mathematical writing today. It discusses at length the central question of the time in the theory of algebraic equations, namely: What is the essence of the methods by which it is possible to solve equations of degrees 2, 3, and 4? Is it possible to extend these methods to equations of higher degree and, if not, why not? Lagrange gave an insightful answer to the first question, describing the solutions of equations of low degree in terms of a unified technique now known as the technique of the *Lagrange resolvent*.* His answer to the second question, on the other hand, is quite inconclusive. He shows that the technique does not apply in an obvious way to equations of degree 5 or higher, and he discusses some techniques—notably the technique of permuting the roots of an algebraic equation—which are relevant to the applications of Lagrange resolvents to equations of higher degree, but he gives no final answer. In short, it is a paper that gives the reader as much information about the problem as the author can provide and indicates the direction which the author feels further work should take. Viewed in this way, Lagrange's paper seems the perfect source of inspiration for a Galois.

Thus, in order to appreciate Galois' theory, it is natural first to review Lagrange's work. We will go much farther back than that—all the way to ancient Babylon—and then review a few other aspects of the development of algebra before discussing the main features of the work of Lagrange and then moving on to his successors, Gauss and Galois.

* A very similar technique was used a few months earlier by Vandermonde (see §15), but this was unknown to Lagrange.

Quadratic Equations 1700 B.C.

§3 Archeological research in the twentieth century has revealed the surprising fact that the peoples of Mesopotamia in the period around* 1700 B.C. had an advanced mathematical culture, including an excellent sexagesimal system of arithmetic and a knowledge of the Pythagorean theorem (a millennium before Pythagoras!). Of particular relevance to the theory of equations and Galois theory is the knowledge in this ancient culture of a method for the solution of quadratic equations.

According to Neugebauer [N1], the technique commonly used in the Babylonian texts to solve quadratic equations can be viewed as a reduction to a normal form, followed by a method for solving the normal form. The normal form was to *find two numbers given their sum and their product.* In modern algebraic notation, this can be stated: Given two numbers p and s, and given that $xy = p, x + y = s$, find x and y. The steps by which the Babylonians solved this problem are as follows:

1. Take half of s.
2. Square the result.
3. From this subtract p.
4. Take the square root of the result.
5. Add this to half of s; this is one of the two numbers and the other is s minus this one.

For example, if the sum is 10 and the product is 21 then the successive steps give 5, 25, 4, 2, 7 and $10 - 7 = 3$. Thus the two numbers are 7 and 3.

That this normal form is indeed a quadratic equation can be seen by multiplying the equation $s = x + y$ by x to find $sx = x^2 + xy = x^2 + p$. In other words, x is a solution of the quadratic equation $x^2 - sx + p = 0$ and, by symmetry, so is y.

Conversely, the solution of any quadratic equation can *in our notation* be viewed as the solution of a problem in normal form. Specifically, the equation $ax^2 + bx + c = 0$ can be rewritten as $x^2 + (c/a) = -(b/a)x$ and the solution of this equation is equivalent to finding two numbers whose sum is $-b/a$ and whose product is c/a. The Babylonians could *not* reduce *all* quadratic equations to a single normal form, however, because their arithmetic did not include negative numbers. To deal with this fact, they had a second normal form, in which the *difference* and the product of two numbers were given. This is a technical problem of considerable historical interest—it was only a few centuries ago that negative numbers became generally accepted so that polynomial equations did not have to be divided into several cases depending on the signs of the coefficients—but is of no importance to the algebra of the problem and will not be considered further here.

* The texts cannot be closely dated. Neugebauer places them between 1600 and 1800 B.C.