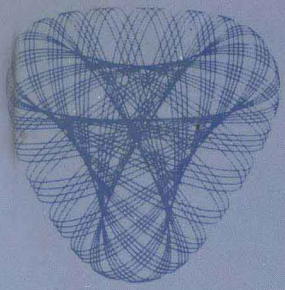

Galois Theory

Second edition

Ian Stewart

CHAPMAN AND HALL MATHEMATICS

Galois Theory

Second edition

Ian Stewart

Reader, Mathematics Institute,
University of Warwick, Coventry

London New York
Chapman and Hall

First published in 1973 by Chapman and Hall Ltd
11 New Fetter Lane, London EC4P 4EE

Published in the USA by Chapman and Hall
29 West 35th Street, New York NY 10001

Reprinted 1979, 1984
Second edition 1989

Typeset in 10/12 Times by KEYTEC, Bridport, Dorset

Printed in Great Britain by T. J. Press (Padstow) Ltd, Padstow

ISBN 0 412 34540 4 (hardback)
0 412 34550 1 (paperback)

British Library Cataloguing in Publication Data

Stewart, Ian 1945–
Galois Theory – 2nd ed.
1. Galois theory
I. Title
512'.32
ISBN 0-412-34540-4

Library of Congress Cataloging in Publication Data

Stewart, Ian.
Galois theory/Ian Stewart. – 2nd ed.
p. cm.
Bibliography: p.
Includes indexes.
ISBN 0-412-34540-4. – ISBN 0-412-34550-1 (pbk.)
1. Galois theory. I. Title.
QA214.S74 1989
512'.3–dc20

Galois Theory

Portrait of Évariste Galois aged fifteen (Fig. 1).

Illustration acknowledgements

The following illustrations are reproduced, with permission, from the sources listed.

Figures 1, 6, 7–9, 10, 20 from *Écrits et Mémoires Mathématiques d'Évariste Galois*, Robert Bourgne and J.-P. Azra, Gauthier-Villars, Paris 1962.

Figure 23 from *Carl Friedrich Gauss: Werke*, Vol. X, Georg Olms Verlag, Hildesheim and New York 1973.

Figure 4 from *History of Mathematics*, David Eugene Smith, Dover Publications Inc., New York 1951.

Figure 22 from *A Source Book in Mathematics*, David Eugene Smith, McGraw-Hill, New York and London 1929.

Figures 3, 5 from *The History of Mathematics: an Introduction*, David M. Burton, Allyn and Bacon Inc., Boston 1985.

Preface to the first edition

Galois theory is a showpiece of mathematical unification, bringing together several different branches of the subject and creating a powerful machine for the study of problems of considerable historical and mathematical importance. This book is an attempt to present the theory in such a light, and in a manner suitable for second- and third-year undergraduates.

The central theme is the application of the Galois group to the quintic equation. As well as the traditional approach by way of the 'general' polynomial equation I have included a direct approach which demonstrates the insolubility by radicals of a specific quintic polynomial with integer coefficients, which I feel is a more convincing result. The abstract Galois theory is set in the context of arbitrary field extensions, rather than just subfields of the complex numbers; the resulting gain in generality more than compensates for the extra work required. Other topics covered are the problems of duplicating the cube, trisecting the angle, and squaring the circle; the construction of regular polygons; the solution of cubic and quartic equations; the structure of finite fields; and the 'fundamental theorem of algbra'. The last is proved by almost purely algebraic methods, and provides an interesting application of Sylow theory.

In order to make the treatment as self-contained as possible, and to bring together all the relevant material in a single volume, I have included several digressions. The most important of these is a proof of the transcendence of π, which all mathematicians should see at least once in their lives. There is a discussion of Fermat numbers, to emphasize that the problem of regular polygons, although reduced to a simple-looking question in number theory, is by no means completely solved. A construction for the regular 17-gon is given, on the grounds that such an unintuitive result requires more than just an existence proof.

Much of the motivation for the subject is historical, and I have taken the opportunity to weave historical comments into the body of the book where appropriate. There are two sections of purely historical matter: a short sketch of the history of polynomials, and a biography of Évariste Galois. The latter is culled from several sources (listed in the references) of which by far the most useful and accurate is that of Dupuy (1896).

I have tried to give plenty of examples in the text to illustrate the general theory, and have devoted one chapter to a detailed study of the Galois group of a particular field extension. There are nearly two hundred exercises, with twenty harder ones for the more advanced student.

Many people have helped, advised, or otherwise influenced me in writing this book, and I am suitably grateful to them. In particular my thanks are due to Rolph Schwarzenberger and David Tall, who read successive drafts of the manuscript; to Len Bulmer and the staff of the University of Warwick Library for locating documents relevant to the historical aspects of the subject; to Ronnie Brown for editorial guidance and much good advice; and to the referee who pointed out a multitude of sins of omission and commission on my part, whose name I fear will forever remain a mystery to me, owing to the system of secrecy without which referees would be in continual danger of violent retribution from indignant authors.

University of Warwick
Coventry
April 1972

IAN STEWART

Preface to the second edition

It is sixteen years since the first edition of *Galois Theory* appeared. Classical Galois theory is not the kind of subject that undergoes tremendous revolutions, and a large part of the first edition remains intact in this, its successor. Nevertheless, a certain thinning at the temples and creaking of the joints have become apparent, and some rejuvenation is in order.

The main changes in this edition are the addition of an introductory overview and a chapter on the calculation of Galois groups. I have also included extra motivating examples and modified the exercises. Known misprints have been corrected, but since this edition has been completely reset there will no doubt be some new ones to tax the reader's ingenuity (and patience). The historical section has been modified in the light of new findings, and the publisher has kindly permitted me to do what I wanted to do in the first edition, namely, include photographs from Galois's manuscripts, and other historical illustrations. Some of the mathematical proofs have been changed to improve their clarity, and in a few cases their correctness. Some material that I now consider superfluous has been deleted. I have tried to preserve the informal style of the original, which for many people was the book's greatest virtue.

The new version has benefited from advice from several quarters. Lists of typographical and mathematical errors have been sent to me by Stephen Barber, Owen Brison, Bob Coates, Philip Higgins, David Holden, Frans Oort, Miles Reid, and C. F. Wright. The Open University used the first edition as the basis for course M333, and several members of its Mathematics Department have passed on to me the lessons that were learned as a result. I record for posterity my favourite example of OU wit, occasioned by a mistake in the index: '226:

Stéphanie D. xix. Should refer to page xxi (the course of true love never does run smooth, nor does it get indexed correctly).'

I am grateful to them, and to their students, who acted as unwitting guinea-pigs: take heart, for your squeaks have not gone unheeded.

University of Warwick
Coventry
December 1988

IAN STEWART

Notes to the reader

Theorems, lemmas, propositions, corollaries, and the like are numbered consecutively within chapters by numbers of the form **m.n** where **m** is the chapter number and **n** indicates the position within the chapter.

Exercises are given at the end of each chapter (with two exceptions) and are numbered in a similar fashion. Harder exercises are signalled by an asterisk (*). Solutions are given to some of the exercises, mostly those whose solution can be made brief.

Definitions are usually, but not always, signalled by the word **Definition**.

Equations which need to be referred to are numbered (m.n) as above, at the right-hand side of the page, the numbering starting afresh with each chapter.

References are given at the back, and are signalled in the text in the form 'William (1066)'.

STRUCTURE

Each brick (see Fig. 2 overleaf) represents a chapter. Mathematical dependence of chapters corresponding to structural dependence of bricks.

For a short course aimed directly at the insolubility of the quintic equation the sequence of Chapters 1–4, 7–11, 13, 14, is recommended. Alternatively the third subsection of Chapter 13 may be omitted, together with the second half of Chapter 14 and Chapter 15 substituted.

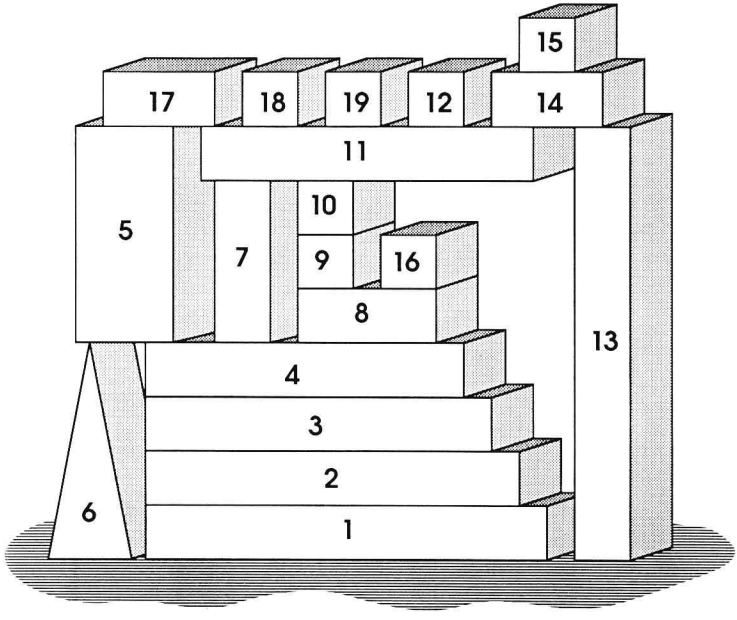

Fig. 2 Structure of the book: each chapter depends on those that support it.

Historical introduction

Polynomial equations have a lengthy history. A Babylonian tablet of *c.* 1600 BC poses problems which reduce to the solution of quadratic equations (Midonick, 1965, p. 48); and it is clear from the tablets that the Babylonians possessed methods of solving them (Bourbaki, 1969, p. 92) although they had no algebraic notation with which to express their solution. The ancient Greeks solved quadratics by geometrical constructions, but there is no sign of an algebraic formulation until at least AD 100 (Bourbaki, 1969, p. 92). They also had methods applicable to cubic equations, involving points of intersection of conics. Algebraic solutions of the cubic were unknown, and in 1494 Pacioli ended his *Summa di Arithmetica* (Fig. 3) with the remark that the solution of the equations $x^3 + mx = n$ and $x^3 + n = mx$ was as impossible at the existing state of knowledge as squaring the circle.

The Renaissance mathematicians at Bologna discovered that the solution of the cubic could be reduced to that of three basic types: $x^3 + px = q$, $x^3 = px + q$, $x^3 + q = px$. They were forced to distinguish these cases because they did not recognize the existence of negative numbers. Scipio del Ferro is believed on good authority (Bortolotti, 1925) to have solved all three types; he certainly passed on his method for one type to a student, Fior. News of the solution leaked out, and others were encouraged to try their hand; and solutions were rediscovered by Niccolo Fontana (nicknamed Tartaglia, Fig. 4) in 1535. Fontana demonstrated his methods in a public competition with Fior, but refused to reveal the details. Finally he was persuaded to tell them to the physician Girolamo Cardano, having first sworn him to secrecy. But when Cardano's *Ars Magna* appeared in 1545 it contained a complete discussion of Fontana's solution – with full acknowledgement to the discoverer. Although Cardano (1931) claimed motives of the highest order, Fontana was justifiably annoyed, and in the ensuing wrangle the history of the discovery became public knowledge.

Fig. 3 A page from Pacioli's *Summa di Arithmetica*.

The *Ars Magna* (Fig. 5) also contained a method, due to Ludovico Ferrari, of solving the quartic equation by reducing it to a cubic.

All the formulae discovered had one striking property, which can be illustrated by Fontana's solution of $x^3 + px = q$:

$$x = \sqrt[3]{\left[\frac{q}{2} + \sqrt{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)}\right]} + \sqrt[3]{\left[\frac{q}{2} - \sqrt{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)}\right]}$$

The expression is built up from the coefficients by repeated addition, subtraction, multiplication, division, and extraction of roots. Such expressions became known as *radical* expressions. Since all equations of degree $\leqslant 4$ were now solved, it was natural to ask how the quintic equation could be solved by radicals.

Fig. 4 Niccolo Fontana (Tartaglia), who discovered how to solve cubic equations.

Many mathematicians attacked the problem. Tschirnhaus claimed a solution, recognized as fallacious by Leibniz. Euler failed to solve the problem but found new methods for the quartic. Lagrange took an important step in 1770 when he unified the separate tricks used for the equations of degree $\leqslant 4$. He showed that they depended on finding functions of the roots of the equation which were unchanged by certain permutations of those roots; and he showed that this approach failed when tried on the quintic. A general feeling that the quintic could not be solved by radicals was now in the air; and in 1813 Ruffini attempted to give a proof of the impossibility. His paper appeared in an obscure journal, with several gaps in the proof (Bourbaki, 1969, p. 103) and attracted little attention. The question was finally settled by Abel in 1824, who proved conclusively that the general quintic equation was insoluble by radicals.

The problem now arose of finding a way of deciding whether or not a given equation could be solved by radicals. Abel was working on it when he died in 1829. In 1832 a young Frenchman, Évariste Galois, was


HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

Fig. 5 Title page of Cardano's *Ars Magna*.

killed in a duel. He had for some time sought recognition for his mathematical theories, submitting three memoirs to the Academy of Sciences in Paris. They were all rejected; and his work appeared to be lost to the mathematical world. Then, on 4 July 1843, Joseph Liouville addressed the academy. He opened with these words:

> 'I hope to interest the Academy in announcing that among the papers of Évariste Galois I have found a solution, as precise as it is profound, of this beautiful problem: whether or not it is soluble by radicals. . . .'

The life of Galois

Évariste Galois (Fig. 6) was born at Bourg-la-Reine near Paris on 25 October 1811. His father Nicolas-Gabriel Galois was a Republican (Kollros, 1949) and head of the village liberal party; after the return to the throne of Louis XVIII in 1814 he became mayor. Évariste's mother Adelaide-Marie (née Demante) was the daughter of a jurisconsult. She was a fluent reader of Latin, thanks to a solid education in religion and the classics.

For the first twelve years of his life Galois was educated by his mother, who passed on to him a thorough grounding in the classics. His childhood appears to have been a happy one. At the age of ten he was offered a place at the college of Reims, but his mother preferred to keep him at home. In October 1823 he entered the *lycée* Louis-le-Grand. During his first term there the students rebelled and refused to chant in chapel, and a hundred of them were expelled.

Galois performed well during his first two years at school, obtaining first prize in Latin; but then boredom set in. He was made to repeat the next year's classes, but this simply aggravated the tedium. It was during this period that Galois began to take a serious interest in mathematics. He came across a copy of Legendre's *Éléments de Géométrie*, a classic text which broke with the Euclidean tradition of school geometry. It is said (see Bell, 1965), that he read it 'like a novel' and mastered it in one reading. The school algebra texts could not compete with Legendre's masterpiece, and Galois turned instead to the original memoirs of Lagrange and Abel. At the age of fifteen he was reading material written for professional mathematicians. But his classwork remained uninspired; it would seem that he had lost all interest in it. His teachers misunderstood him and accused him of affecting ambition and originality.

Galois was an untidy worker, as can be seen from some of his manuscripts (Bourgne and Azra, 1962); and he tended to work in his head, committing only the results of his deliberations to paper. His