

Galois Theory and Its Algebraic Background

SECOND EDITION

Galois theory, the theory of polynomial equations and their solutions, is one of the most fascinating and beautiful subjects in pure mathematics. Using group theory and field theory, it provides a complete answer to the problem of the solubility of polynomial equations by radicals: that is, determining when and how a polynomial equation can be solved by repeatedly extracting roots using elementary algebraic operations.

This textbook contains a fully detailed account of Galois theory and the algebra that it needs, and is suitable for both those following a course of lectures and the independent reader (who is assumed to have no previous knowledge of Galois theory). This second edition has been significantly revised and reordered; the first part develops the basic algebra that is needed, and the second part gives a comprehensive account of Galois theory. There are applications to ruler and compass constructions, and to the solution of classical mathematical problems of ancient times. There are new exercises throughout, and carefully selected examples will help the reader develop a clear understanding of the mathematical theory.

D. J. H. GARLING is Emeritus Reader in Mathematical Analysis at the University of Cambridge and Fellow of St John's College, Cambridge. He has 50 years' experience of teaching undergraduate students and has written several books on mathematics, including *Inequalities: A Journey into Linear Analysis* (Cambridge University Press, 2007) and *A Course in Mathematical Analysis* (three volumes, Cambridge University Press, 2013–2014).

Galois Theory and Its Algebraic Background

SECOND EDITION

D.J.H. Garling
University of Cambridge



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
 UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom
 One Liberty Plaza, 20th Floor, New York, NY 10006, USA
 477 Williamstown Road, Port Melbourne, VIC 3207, Australia
 314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India
 103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.
 It furthers the University's mission by disseminating knowledge in the pursuit of
 education, learning, and research at the highest international levels of excellence.

www.cambridge.org
 Information on this title: www.cambridge.org/9781108838924
 DOI: 10.1017/9781108979184

First edition © Cambridge University Press 1986
 Second edition © D.J.H. Garling 2022

This publication is in copyright. Subject to statutory exception
 and to the provisions of relevant collective licensing agreements,
 no reproduction of any part may take place without the written
 permission of Cambridge University Press.

First published 1986
 Reprinted with corrections 1988, 1991, 1993, 1995
 Second edition 2022

Printed in the United Kingdom by TJ Books Limited, Padstow, Cornwall, 2022

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Names: Garling, D. J. H., author.
 Title: Galois theory and its algebraic background / D.J.H. Garling.
 Other titles: Course in Galois theory
 Description: Second edition. | Cambridge ; New York, NY : Cambridge
 University Press, 2021. | First edition published as Course in Galois
 theory, Cambridge University Press, 1986. | Includes bibliographical references and index.
 Identifiers: LCCN 2021002526 (print) | LCCN 2021002527 (ebook) |
 ISBN 9781108838924 (hardback) | ISBN 9781108969086 (paperback) | ISBN 9781108979184 (epub)
 Subjects: LCSH: Galois theory.
 Classification: LCC QA214 .G367 2021 (print) — LCC QA214 (ebook) | DDC 512/.32–dc23
 LC record available at <https://lcn.loc.gov/2021002526>
 LC ebook record available at <https://lcn.loc.gov/2021002527>

ISBN 978-1-108-83892-4 Hardback
 ISBN 978-1-108-96908-6 Paperback

Cambridge University Press has no responsibility for the persistence or accuracy of
 URLs for external or third-party internet websites referred to in this publication
 and does not guarantee that any content on such websites is, or will remain,
 accurate or appropriate.

Contents

<i>Preface</i>	<i>page ix</i>
PART I THE ALGEBRAIC BACKGROUND	
1 Groups	3
1.1 Groups	3
1.2 Finite Abelian Groups	9
1.3 Finite Permutation Groups	11
1.4 Group Series	17
1.5 Soluble Groups	18
1.6 p -Groups and Sylow Theorems	22
2 Integral Domains	25
2.1 Commutative Rings with 1	25
2.2 Polynomials	26
2.3 Homomorphisms and Ideals	27
2.4 Integral Domains	29
2.5 Fields and Fractions	31
2.6 The Ordered Set of Ideals in an Integral Domain	35
2.7 Factorization	36
2.8 Unique Factorization	38
2.9 Principal Ideal Domains and Euclidean Domains	41
2.10 Polynomials Over Unique Factorization Domains	44
2.11 More About Fields	47
2.12 Kronecker's Algorithm	48
2.13 Eisenstein's Criterion	50
2.14 Localization	51

3	Vector Spaces and Determinants	54
3.1	Vector Spaces	54
3.2	The Infinite-Dimensional Case	60
3.3	Characters and Automorphisms	61
3.4	Determinants	62
PART II THE THEORY OF FIELDS AND GALOIS THEORY		
4	Field Extensions	69
4.1	Introduction	69
4.2	Field Extensions	70
4.3	Algebraic and Transcendental Extensions	73
4.4	Algebraic Extensions	77
4.5	Monomorphisms of Algebraic Extensions	80
5	Ruler and Compass Constructions	81
5.1	Some Classical Problems	81
5.2	Constructible Points	81
6	Splitting Fields	85
6.1	Introduction	85
6.2	Splitting Fields	86
6.3	The Extension of Monomorphisms	89
6.4	Some Examples	94
7	Normal Extensions	98
7.1	Basic Properties	98
7.2	Monomorphisms and Automorphisms	101
8	Separability	103
8.1	Basic Ideas	103
8.2	Monomorphisms and Automorphisms	104
8.3	Galois Extensions	106
8.4	Differentiation	106
8.5	Inseparable Polynomials	108
9	The Fundamental Theorem of Galois Theory	112
9.1	Field Automorphisms, Fixed Fields and Galois Groups	112
9.2	Linear Independence	113
9.3	The Size of a Galois Group is the Degree of the Extension	115
9.4	The Galois Group of a Polynomial	116
9.5	The Fundamental Theorem of Galois Theory	118

10 The Discriminant	122
10.1 The Discriminant	122
11 Cyclotomic Polynomials and Cyclic Extensions	126
11.1 Cyclotomic Polynomials	126
11.2 Irreducibility	128
11.3 The Galois Group of a Cyclotomic Polynomial	129
11.4 A Necessary Condition	131
11.5 Abel's Theorem	132
11.6 Norms and Traces	134
11.7 A Sufficient Condition	135
11.8 Kummer Extensions	137
12 Solution by Radicals	140
12.1 Polynomials with Soluble Galois Groups	140
12.2 Polynomials which are Soluble by Radicals	141
13 Regular Polygons	146
13.1 Fermat Primes and Fermat Numbers	146
13.2 Regular Polygons	147
13.3 Constructing a Regular Pentagon	148
14 Polynomials of Low Degree	149
14.1 Quadratic Polynomials	149
14.2 Cubic Polynomials	150
14.3 Quartic Polynomials	153
15 Finite Fields	156
15.1 Finite Fields	156
15.2 Polynomials in $\mathbb{Z}_p[x]$	157
15.3 Polynomials of Low Degree over a Finite Field	158
16 Quintic Polynomials	161
17 Further Theory	164
17.1 Simple Extensions	165
17.2 The Theorem of the Primitive Element	166
17.3 The Normal Basis Theorem	168
18 The Algebraic Closure of a Field	170
18.1 Introduction	170
18.2 The Existence of an Algebraic Closure	171
18.3 The Uniqueness of an Algebraic Closure	175
18.4 Conclusions	176

19	Transcendental Elements and Algebraic Independence	177
19.1	Transcendental Elements and Algebraic Independence	177
19.2	Transcendence Bases	180
19.3	Transcendence Degree	181
19.4	The Tower Law for Transcendence Degree	182
19.5	Lüroth's Theorem	183
20	Generic and Symmetric Polynomials	186
20.1	Generic and Symmetric Polynomials	186
	<i>Appendix: The Axiom of Choice</i>	189
	<i>Index</i>	192

Preface

Galois theory is one of the most fascinating and enjoyable branches of algebra. The problems with which it is concerned have a long and distinguished history: the problems of duplicating a cube or trisecting an angle go back to the Greeks, and the problem of solving a cubic, quartic or quintic equation to the Renaissance. Many of the problems that are raised are of a concrete kind (and this, surely, is why it is so enjoyable) and yet the needs of the subject have led to substantial development in many branches of abstract algebra: in particular, in the theory of fields, the theory of groups, the theory of vector spaces and the theory of commutative rings.

In this book, Galois theory is treated as it should be, as a subject in its own right. Nevertheless, in the process, I have tried to show its relationship to various topics in abstract algebra: an understanding of the structures of abstract algebra helps give a shape to Galois theory and conversely Galois theory provides plenty of concrete examples which show the point of abstract theory.

The book comprises two unequal parts. In the first part, an account is given of the algebra that is needed for Galois theory. Much of this may well be familiar to the reader, but is included both for completeness and to introduce the terminology and notation that is used. Much of the algebra (groups, rings, fields and vector spaces) has general interest, and of course the development of Galois theory was responsible for the development of many algebraic ideas. We shall concentrate on presenting those algebraic ideas and results that are needed for Galois theory. For example, it is important to know that in the right circumstances, the factorization of polynomials with coefficients in a ring is essentially unique. Group theory plays a large part in Galois theory, but has developed into a huge subject. We shall concentrate on those parts, such as the theory of soluble groups, which are needed in Galois theory.

The second, more substantial, part is concerned with the theory of fields and with Galois theory, and contains the main material of the book; indeed, many readers may wish to start here and refer back to the first part as necessary. Of its nature, the theory develops an inexorable momentum. Nevertheless, there are many digressions (for example, concerning geometric constructions, finite fields and the solution of cubic and quartic equations): one of the pleasures of Galois theory is that there are many examples which illustrate and depend upon the general theory, but which also have an interest of their own. The high point of the book is of course the resolution of the problem of when a polynomial is solvable by radicals. I have, however, tried to emphasize (in the final chapter in particular) that this is not the end of the story: the resolution of the problem raises many new problems, and Galois theory is still a lively subject.

The last three chapters have a more abstract nature, and require the use of Zorn's lemma. In full generality, in the uncountable case, this depends upon the Axiom of Choice; this is discussed in the Appendix. Algebra is principally concerned with finite operations and relations, and is therefore largely concerned with finite or countable sets, and so these chapters have a rather hybrid quality.

Two hundred exercises are scattered through the text. It has been suggested to me that this is rather few: I think that anyone who honestly tries them all will disagree! In my opinion, textbook exercises are often too straightforward, but some of these exercises are quite hard. The successful solution of a challenging problem gives a much better understanding of the powers and limitations of the theory than any number of trivial ones. Remember that mathematics is not a spectator sport!