Cambridge Studies in Advanced Mathematics 53

GROUPS AS GALOIS GROUPS

1 W.M.L. Holcombe *Algebraic automata theory*
2 K. Petersen *Ergodic theory*
3 P.T. Johnstone *Stone spaces*
4 W.H. Schikhof *Ultrametric calculus*
5 J.-P. Kahane *Some random series of functions, 2nd edition*
6 H. Cohn *Introduction to the construction of class fields*
7 J. Lambek & P.J. Scott *Introduction to higher-order categorical logic*
8 H. Matsumura *Commutative ring theory*
9 C.B. Thomas *Characteristic classes and the cohomology of finite groups*
10 M. Aschbacher *Finite group theory*
11 J.L. Alperin *Local representation theory*
12 P. Koosis *The logarithmic integral I*
13 A. Pietsch *Eigenvalues and s-numbers*
14 S.J. Patterson *An introduction to the theory of the Riemann zeta-function*
15 H.J. Baues *Algebraic homotopy*
16 V.S. Varadarajan *Introduction to harmonic analysis on semisimple Lie groups*
17 W. Dicks and M. Dunwoody *Groups acting on graphs*
18 L.J. Corwin and F.P. Greenleaf *Representations of nilpotent Lie groups and their applications*
19 R. Fritsch and R. Piccinini *Cellular structures in topology*
20 H. Klingen *Introductory lectures on Siegel modular forms*
21 P. Koosis *The logarithmic integral II*
22 M.J. Collins *Representations and characters of finite groups*
24 H. Kunita *Stochastic flows and stochastic differential equations*
25 P. Wojtaszczyk *Banach spaces for analysts*
26 J.E. Gilbert and M.A.M. Murray *Clifford algebras and Dirac operators in harmonic analysis*
27 A. Frohlich and M.J. Taylor *Algebraic number theory*
28 K. Goebel and W.A. Kirk *Topics in metric fixed point theory*
29 J.F. Humphreys *Reflection groups and Coxeter groups*
30 D.J. Benson *Representations and cohomology I*
31 D.J. Benson *Representations and cohomology II*
32 C. Allday and V. Puppe *Cohomological methods in transformation groups*
33 C. Soule et al. *Lectures on Arakelov geometry*
34 A. Ambrosetti and G. Prodi *A primer of nonlinear analysis*
35 J. Palis and F. Takens *Hyperbolicity, stability and chaos at homoclinic bifurcations*
37 Y. Meyer *Wavelets and operators 1*
38 C. Weibel *An Introduction to homological algebra*
39 W. Bruns and J. Herzog *Cohen–Macaulay rings*
40 V. Snaith *Explicit Brauer induction*
41 G. Laumon *Cohomology of Drinfeld modular varieties: Part I*
42 E.B. Davies *Spectral theory of differential operators*
43 J. Diestel, H. Jarchow, and A. Tonge *Absolutely summing operators*
44 P. Mattila *Geometry of sets and measures in Euclidean spaces*
45 R. Pinsky *Positive harmonic functions and diffusion*
46 G. Tenenbaum *Introduction to analytic and probabilistic number theory*
47 C. Peskine *Complex projective geometry*
48 Y. Meyer and R. Coifman *Wavelets and operators II*
49 R. Stanley *Enumerative combinatorics*
50 I. Porteous *Clifford algebras and the classical groups*

GROUPS AS GALOIS GROUPS

An Introduction

HELMUT VÖLKLEIN
University of Florida
and
Universität Erlangen

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1996

Library of Congress Cataloging-in-Publication Data
Völklein, Helmut.
Groups as Galois groups: an introduction / Helmut Völklein.
p. cm. – (Cambridge studies in advanced mathematics; 53)
Includes index.
ISBN 0-521-56280-5 (hardcover)
1. Inverse Galois theory. I. Title. II. Series.
QA247.V65 1996
512′.3 – dc20 95-46746
CIP
A catalog record for this book is available from the British Library.

ISBN 0-521-56280-5 hardback

Transferred to digital printing 2004

MEINEN ELTERN
Max und Edeltraut Völklein
UND MEINER FRAU
Sommai
IN LIEBE GEWIDMET

Contents

Preface *page* xiii
Notation xvii

I The Basic Rigidity Criteria

1 Hilbert's Irreducibility Theorem 3
  1.1 Hilbertian Fields 3
    1.1.1 Preliminaries 3
    1.1.2 Specializing the Coefficients of a Polynomial 5
    1.1.3 Basic Properties of Hilbertian Fields 10
  1.2 The Rational Field Is Hilbertian 13
    1.2.1 Analyticity of Roots 14
    1.2.2 The Rational Field Is Hilbertian 16
    1.2.3 Integral Values of Meromorphic Functions 18
  1.3 Algebraic Extensions of Hilbertian Fields 21
    1.3.1 Weissauer's Theorem 21
    1.3.2 Applications 24
2 Finite Galois Extensions of $\mathbb{C}(x)$ 26
  2.1 Extensions of Laurent Series Fields 27
    2.1.1 The Field of Formal Laurent Series over k 27
    2.1.2 Factoring Polynomials over $k[[t]]$ 28
    2.1.3 The Finite Extensions of $\bar{k}((t))$ 30
  2.2 Extensions of $\bar{k}(x)$ 32
    2.2.1 Branch Points and the Associated Conjugacy Classes 32
    2.2.2 Riemann's Existence Theorem and Rigidity 37
3 Descent of Base Field and the Rigidity Criterion 40
  3.1 Descent 40
    3.1.1 Fields of Definition 40
    3.1.2 The Descent from $\bar{\kappa}$ to κ 43
  3.2 The Rigidity Criteria 48

- 3.3 Rigidity and the Simple Groups 51
  - 3.3.1 The Alternating and Symmetric Groups 52
  - 3.3.2 A Formula to Verify Rigidity 53
  - 3.3.3 The Sporadic Groups 54
  - 3.3.4 The Lie Type Groups 55
  - 3.3.5 A Criterion for Groups Modulo Center 56
  - 3.3.6 An Example: The Groups $\mathrm{PSL}_2(q)$ 57

4 Covering Spaces and the Fundamental Group 61

- 4.1 The General Theory 61
  - 4.1.1 Homotopy 61
  - 4.1.2 Coverings 63
  - 4.1.3 The Homotopy Lifting Property 64
  - 4.1.4 Galois Coverings and the Group of Deck Transformations 67
- 4.2 Coverings of the Punctured Sphere 69
  - 4.2.1 The Coverings of the Disc Minus Center 69
  - 4.2.2 Coverings of the Punctured Sphere – Behavior Near a Ramified Point 72
  - 4.2.3 Coverings of Prescribed Ramification Type 76

5 Riemann Surfaces and Their Function Fields 84

- 5.1 Riemann Surfaces 84
- 5.2 The Compact Riemann Surface Arising from a Covering of the Punctured Sphere 87
  - 5.2.1 Construction of an Atlas 87
  - 5.2.2 The Identification between Topological and Algebraic Ramification Type 89
- 5.3 Constructing Generators of $G(L/\mathbb{C}(x))$ 92
- 5.4 Digression: The Equivalence between Coverings and Field Extensions 94

6 The Analytic Version of Riemann's Existence Theorem 96

- 6.1 Abstract Hilbert Spaces 96
  - 6.1.1 Continuous Linear Maps and Orthogonal Complements 96
  - 6.1.2 Banach's Theorem 99
- 6.2 The Hilbert Spaces $L^2(D)$ 100
  - 6.2.1 Square Integrable Functions 101
  - 6.2.2 Functions on a Disc 102
  - 6.2.3 $L^2(D)$ Is a Hilbert Space 103
- 6.3 Cocycles and Coboundaries 105

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

6.3.1 Square Integrable Functions on Coordinate Patches 105
6.3.2 Cocycles 106
6.3.3 The Coboundary Map 107
6.4 Cocycles on a Disc 107
6.4.1 Dolbeault's Lemma 107
6.4.2 Cocycles on a Disc 109
6.5 A Finiteness Theorem 110
6.5.1 The Patching Process 111
6.5.2 Restriction $Z^1(\mathcal{V}) \to Z^1(\mathcal{U})$ 112
6.5.3 Proof of the Finiteness Theorem 114

II Further Directions

7 The Descent from $\mathbb{C}$ to $\bar{k}$ 119
7.1 Extensions of $\mathbb{C}(x)$ Unramified Outside a Given Finite Set 119
7.2 Specializing the Coefficients of an Absolutely Irreducible Polynomial 121
7.3 The Descent from $\mathbb{C}$ to $\bar{k}$ 123
7.4 The Minimal Field of Definition 126
7.5 Embedding Problems over $\bar{k}(x)$ 128
8 Embedding Problems 130
8.1 Generalities 130
8.1.1 Fields over Which All Embedding Problems Are Solvable 130
8.1.2 Minimal Embedding Problems 132
8.2 Wreath Products and Split Abelian Embedding Problems 134
8.2.1 A Rationality Criterion for Function Fields 134
8.2.2 The Group-Theoretic Notion of Wreath Product 135
8.2.3 Wreath Products as Galois Groups 136
8.3 GAR-Realizations and GAL-Realizations 141
8.3.1 Definition and the Main Property of a GAR-Realization 141
8.3.2 GAL-Realizations 144
8.3.3 Digression: Fields of Cohomological Dimension 1 and the Shafarevich Conjecture 149
8.3.4 GAL-Realizations over $\bar{k}$ 153
9 Braiding Action and Weak Rigidity 155
9.1 Certain Galois Groups Associated with a Weakly Rigid Ramification Type 156
9.2 Combinatorial Computation of Δ via Braid Group Action and the Resulting Outer Rigidity Criterion 161
9.3 Construction of Weakly Rigid Tuples 165

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

9.4 An Application of the Outer Rigidity Criterion 169
  9.4.1 Braiding Action through the Matrices $\Phi(Q, \zeta)$ 170
  9.4.2 Galois Realizations for $\mathrm{PGL}_n(q)$ and $\mathrm{PU}_n(q)$ 173
10 Moduli Spaces for Covers of the Riemann Sphere 178
10.1 The Topological Construction of the Moduli Spaces 179
  10.1.1 A Construction of Coverings 179
  10.1.2 Distinguished Conjugacy Classes in the Fundamental Group of a Punctured Sphere 181
  10.1.3 The Moduli Spaces as Abstract Sets 181
  10.1.4 The Topology of the Moduli Spaces 183
  10.1.5 Families of Covers of the Riemann Sphere 186
  10.1.6 The Braid Group 188
  10.1.7 The Braiding Action on Generating Systems 192
  10.1.8 Components of $\mathcal{H}_r^{(A)}(G)$, and the Example of Simple Covers 195
10.2 The Algebraic Structure of the Moduli Spaces 199
  10.2.1 Coverings of Affine Varieties 200
  10.2.2 The Action of Field Automorphisms on the Points of $\mathcal{H}_r^{in}(G)$ 201
  10.2.3 The Algebraic Structure of $\mathcal{H}_r^{(A)}(G)$, and the Proof of Theorem 9.5 205
10.3 Digression: The Inverse Galois Problem and Rational Points on Moduli Spaces 208
  10.3.1 The $\mathbb{Q}$-Structure on $\mathcal{H}_r^{in}(G)$ 208
  10.3.2 Absolutely Irreducible Components of $\mathcal{H}_r^{in}(G)$ Defined over $\mathbb{Q}$ 210
  10.3.3 The Application to PAC-Fields 212
11 Patching over Complete Valued Fields 213
11.1 Power Series over Complete Rings 214
  11.1.1 Absolute Values 214
  11.1.2 Power Series 215
  11.1.3 Algebraic Power Series Are Convergent 216
  11.1.4 Weierstraß Division 217
11.2 Rings of Converging Power Series 218
  11.2.1 The Basic Set-Up 219
  11.2.2 Structure of the Rings A, A_1, and A_2 220
  11.2.3 The Embedding of A into $k[[x-c]]$ 222
11.3 GAGA 222
  11.3.1 Cartan's Lemma 223
  11.3.2 Induced Algebras 225

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

11.3.3 An Elementary Version of 1-Dimensional Rigid GAGA 226
11.4 Galois Groups over $k(x)$ 231
11.4.1 Inductive Construction of Galois Extensions 231
11.4.2 Regular Extensions in Positive Characteristic 235
11.4.3 Galois Realizations of Cyclic Groups 236
11.4.4 Galois Groups and Embedding Problems over $k(x)$ 239

References 243

Index 247

Preface

The goal of the book is to lead the reader to an understanding of recent results on the Inverse Galois Problem: The construction of Galois extensions of the rational field $\mathbb{Q}$ with certain prescribed Galois groups. Assuming only a knowledge of elementary algebra and complex analysis, we develop the necessary background from topology (Chapter 4: covering space theory), Riemann surface theory (Chapters 5 and 6), and number theory (Chapter 1: Hilbert's irreducibility theorem). Classical results like Riemann's existence theorem and Hilbert's irreducibility theorem are proved in full, and applied in our context. The idea of **rigidity** is the basic underlying principle for the described construction methods for Galois extensions of $\mathbb{Q}$.

From the work of Galois it emerged that an algebraic equation $f(x) = 0$, say over the rationals, is solvable by radicals if and only if the associated Galois group G_f is a solvable group. As a consequence, the general equation of degree $n \geq 5$ cannot be solved by radicals because the group S_n is not solvable.

This idea of encoding algebraic–arithmetic information in terms of group theory was the beginning of both Galois theory and group theory. Nowadays we learn basic Galois theory in every first-year algebra course. It has become one of the guiding principles of algebra. One aspect of the theory that remains unsatisfactory is the fact that it is very hard to compute the Galois group of a given polynomial. Therefore, the full correspondence between equations of degree n and subgroups of S_n can only be worked out for very small values of n. Since it is probably impossible to get a full understanding of this correspondence for general n, one is naturally led to the following more reasonable question: Do at least all subgroups of S_n occur in this correspondence, that is, does every subgroup of S_n correspond to some equation of degree n? The most important case is that of irreducible equations, which correspond to the transitive subgroups of S_n.

This question is one formulation of the Inverse Problem of Galois Theory. It is often just called the Inverse Galois Problem. Hilbert was the first to study

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

this problem. His irreducibility theorem shows that it suffices to realize groups as Galois groups over the function field $\mathbb{Q}(x)$. This allows us to use methods from Riemann surface theory and algebraic geometry. Hilbert applied his method to obtain Galois realizations of the symmetric and alternating groups. The next milestone was Shafarevich's realization of all solvable groups over $\mathbb{Q}$ (in the 1950s). His approach is purely number-theoretic, and does not extend to nonsolvable groups.

The classification of finite simple groups, completed around 1980, gave a new direction to the work on the Inverse Galois Problem. It now seemed natural to concentrate first on the simple groups, and get the composite groups later by some kind of inductive procedure. It is not yet clear how this inductive procedure – or embedding problem, in technical terms – would work in general. There are, however, quite a few results in this direction, for example, Serre's obstruction theory for central extensions and Matzat's notion of GAR-realization for extensions with centerless kernel. The latter works best if one wants to realize Galois groups over the full cyclotomic field $\mathbb{Q}_{ab}$, instead of over $\mathbb{Q}$ (because all embedding problems over $\mathbb{Q}_{ab}$ with abelian kernel are solvable). If every nonabelian finite simple group has a GAR-realization over $\mathbb{Q}_{ab}(x)$, then the Inverse Galois Problem has a positive solution over $\mathbb{Q}_{ab}$. Moreover, the lattice of all algebraic extensions of $\mathbb{Q}_{ab}$ would then be known. In technical terms, the absolute Galois group of $\mathbb{Q}_{ab}$ would be a free profinite group of countable rank. The latter is known as Shafarevich's conjecture. We will describe the notion of GAR-realization – a Galois realization with particular extra properties – and the related notions of GAL-realization and GAP-realization in Chapter 8.

The above justifies focusing on the simple groups, more generally, on almost simple groups (i.e., groups between a simple group and its automorphism group). That is what the main body of this book is about. It uses the geometric approach of Hilbert, coupled with the idea of **rigidity** (as Thompson called it). The rigidity criterion (in its various versions) gives purely group-theoretic conditions that force a finite group to occur as a Galois group over $\mathbb{Q}$ (actually over every hilbertian field of characteristic 0). It is generally believed to have been found independently by Belyi, Matzat, and Thompson in the early 1980s. But it should be remarked that it is contained implicitly as a special case in earlier work of Fried ([Fr1] 1977).

The elementary level of our approach is the main difference between this and existing books on the subject by Matzat [Ma1] and Serre [Se1], and the forthcoming book [MM] by Malle and Matzat, which give a much higher level presentation. It has not been my goal to state each result in its greatest generality; rather I have tried to give an introduction to the various ideas involved in the subject. Accordingly, there is no claim for completeness. Omissions include the theory of nonsplit abelian embedding problems and the construction of rigid triples in Lie type groups. For a quite complete description of the known results on the Inverse Galois Problem we refer the reader to [MM]. The same holds true for tracing the origin of results – I have tried to attribute proper credit where it seemed appropriate, but again there is no claim for completeness.

Another related topic that is not touched here is the problem of constructing *explicit* polynomials with a given Galois group. There are quite a few results on this, notably polynomials over $\mathbb{Q}$ found by Malle, Matzat, and others, often with the aid of a computer, see [Ma1], [Malle2]. More recently, Abhyankar [Abh2] has found infinite series of polynomials in positive characteristic with various classical groups as Galois groups.

One particular simplification in the first part of the book is that we avoid the descent from $\mathbb{C}$ to $\bar{\mathbb{Q}}$ (usually done by Weil's descent theory), by a simple trick involving Hilbert's irreducibility theorem. This descent is needed in the second part of the book, however, and we present it in Chapter 7, using the Bertini–Noether Lemma. Further, we avoid the technicalities necessary to introduce profinite groups, and phrase everything in terms of finite Galois extensions. Thus it is hoped that now celebrated results – like Thompson's realization of the monster group – become accessible to a wider mathematical audience.

More recent approaches, based on the earlier work of Fried, try to replace the rigidity conditions by the use of moduli spaces and the braid group action. An introduction to this is given in Chapters 9 and 10. We cannot give a full treatment of this theory because it requires deeper methods of algebraic geometry and several complex variables. More important, this theory is still very much in the process of being shaped, connecting, for example, to recent work of Drinfeld, Ihara, and others on the Grothendieck–Teichmüller group, work of Fried on modular towers, and other topics. In addition, the extension to the generalized braid groups introduced by Brieskorn (and possibly other fundamental groups) is yet to be developed.

To keep in line with the main theme of this book – the idea of rigidity – Chapters 9 and 10 show how the braid group action on generating systems naturally arises from the study of weak rigidity. We derive the resulting Outer Rigidity Criterion using the higher-dimensional version of Riemann's existence theorem (which we cannot prove here).

Finally, Chapter 11 gives an introduction to Harbater's patching method. It is essentially independent of the rest of the book. The idea is to imitate the analytic theory of Chapters 4 to 6 for base fields other than the complex numbers. Complex analysis is replaced by ultrametric analysis, which works over any field that is complete with respect to an ultrametric absolute value.

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

Actually, for our approach very little is required from ultrametric analysis, and we develop it in the first two sections. Riemann's existence theorem does not generalize in its full strength, but certain substitutes are obtained (that also hold over fields of positive characteristic). Results include the solution of the Inverse Galois Problem over the fields $\mathbb{Q}_p(x)$ (where $\mathbb{Q}_p$ is the p-adic field) and a proof of the "geometric case of Shafarevich's conjecture."

The first part of the book (Chapters 1 to 6) gives a full proof of the basic rigidity criteria for the realization of groups as Galois groups. Chapter 1 (Hilbert's irreducibility theorem) is essentially independent of the rest (except for some very basic definitions and lemmas), in the methods as well as in the results. Chapter 1 gives the logical foundation for the other chapters, however; they are concerned with realizing groups G over $\mathbb{Q}(x_1, \ldots, x_n)$, whereas Chapter 1 shows that then G also occurs as a Galois group over $\mathbb{Q}$. The first two sections of Chapter 1 suffice for this conclusion. On a first reading, it may be advisable to skip Chapter 1 and take Hilbert's irreducibility theorem for granted.

Chapter 2 formulates the algebraic version of Riemann's existence theorem and draws some corollaries. Chapter 3 derives the rigidity criterion and gives applications. Chapter 4 is purely topological. It is applied in Chapter 5 to reduce the algebraic version of Riemann's existence theorem to the analytic version. The analytic version is proved in Chapter 6.

The exposition in the second part of the book (especially Chapters 9 and 10) proceeds at a faster pace, whereas I have taken care to keep the first part quite elementary. The first part could be used for a one-semester course for second year graduate students.

This book grew out of notes taken by Ralph Frisch during a course I gave at Erlangen in the summer of 1991. I thank Ralph for his enthusiasm and diligence. Thanks for long years of encouragement, beginning with my first steps in mathematics, are due to Karl Strambach, my teacher and friend. I thank M. Jarden and H. Matzat for long-term invitations to the Institute for Advanced Studies in Jerusalem and to the IWR at the University of Heidelberg, respectively. Further, I thank G. Malle and P. Müller for a critical reading of parts of the manuscript. I acknowledge various remarks and discussions from several colleagues, in particular the above-mentioned and W.-D. Geyer, D. Haran, K. Magaard, J.-P. Serre, J. Thompson, and M. van der Put. Above all, I want to express my deep indebtedness to Mike Fried who introduced me to this exciting area, and in countless conversations and e-mail messages has shared his profound knowledge freely with me.

Helmut Völklein Gainesville

Cambridge University Press
0521562805 - Groups as Galois Groups: An Introduction
Helmut Volklein
Frontmatter
More information

Notation

We let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the set of natural numbers and integers, and the field of rational, real, and complex numbers, respectively.

For G a group, $\mathrm{Aut}(G)$ (resp., $\mathrm{Inn}(G)$) denotes its automorphism group (resp., group of inner automorphisms). $Z(G)$ denotes the center of G, and $C_G(H)$ the centralizer of H in G. The direct resp., semi-direct, product of groups is denoted by $G \times H$ resp., $G \cdot H$. All group actions are from the left, unless otherwise stated. A conjugacy class of a group is called nontrivial if it is different from $\{1\}$ (the class consisting of the neutral element).

The symbol $:=$ means "defined to be equal to." (Thus $x := 2$ means x is defined to be 2.) If K/k is a field extension, we let $\mathrm{Aut}(K/k)$ denote the group of automorphisms of K that are the identity on k. If K/k is Galois, $G(K/k)$ ($=\mathrm{Aut}(K/k)$) denotes the Galois group; for any subfield L of K invariant under $G(K/k)$ we let $\mathrm{res}_{K/L}$ denote the restriction homomorphism $G(K/k) \to G(L/k \cap L)$. If U is a subgroup of $G(K/k)$, then K^U denotes the fixed field of U. If K/k and L/k are field extensions, a k-isomorphism from K to L is an isomorphism that is the identity on k. We let $\bar{k}$ denote an algebraic closure of k.

We use the abbreviation "FG-extension" for "finite Galois extension."