This book describes a constructive approach to the inverse Galois problem: Given a finite group $G$ and a field $K$, determine whether there exists a Galois extension of $K$ whose Galois group is isomorphic to $G$. Further, if there is such a Galois extension, find an explicit polynomial over $K$ whose Galois group is the prescribed group $G$.

The main theme of the book is an exposition of a family of “generic” polynomials for certain finite groups, which give all Galois extensions having the required group as their Galois group. The existence of such generic polynomials is discussed, and where they do exist, a detailed treatment of their construction is given. The book also introduces the notion of “generic dimension” to address the problem of the smallest number of parameters required by a generic polynomial.
Mathematical Sciences Research Institute Publications

45

Generic Polynomials
Constructive Aspects of the Inverse Galois Problem
Generic Polynomials
Constructive Aspects of the
Inverse Galois Problem

Christian U. Jensen
University of Copenhagen

Arne Ledet
Texas Tech University

Noriko Yui
Queen's University, Kingston, Ontario
Contents

Acknowledgments ix

Introduction 1
  0.1. The Inverse Problem of Galois Theory 1
  0.2. Milestones in Inverse Galois Theory 3
  0.3. The Noether Problem and Its History 5
  0.4. Strategies 8
  0.5. Description of Each Chapter 9
  0.6. Notations and Conventions 13
  0.7. Other Methods 15

Chapter 1. Preliminaries 17
  1.1. Linear Representations and Generic Polynomials 17
  1.2. Resolvent Polynomials 23
  Exercises 26

Chapter 2. Groups of Small Degree 29
  2.1. Groups of Degree 3 30
  2.2. Groups of Degree 4 31
  2.3. Groups of Degree 5 38
  2.4. Groups of Degree 6 50
  2.5. Groups of Degree 7 51
  2.6. Groups of Degree 8, 9 and 10 56
  2.7. Groups of Degree 11 57
  Exercises 60

Chapter 3. Hilbertian Fields 63
  3.1. Definition and Basic Results 63
  3.2. The Hilbert Irreducibility Theorem 67
  3.3. Noether’s Problem and Dedekind’s Theorem 71
  Exercises 80

Chapter 4. Galois Theory of Commutative Rings 83
  4.1. Ring Theoretic Preliminaries 83
  4.2. Galois Extensions of Commutative Rings 84
  4.3. Galois Algebras 90
  Exercises 93
Chapter 5. Generic Extensions and Generic Polynomials 95
5.1. Definition and Basic Results 95
5.2. Retract-Rational Field Extensions 98
5.3. Cyclic Groups of Odd Order 102
5.4. Regular Cyclic 2-Extensions and Ikeda’s Theorem 106
5.5. Dihedral Groups 109
5.6. \( p \)-Groups in characteristic \( p \) 117
Exercises 123

Chapter 6. Solvable Groups I: \( p \)-Groups 127
6.1. Quaternion Groups 128
6.2. The Central Product \( QC \) 142
6.3. The Quasi-Dihedral Group 146
6.4. The Cyclic Group of Order 8 152
6.5. The Dihedral Group \( D_8 \) 155
6.6. Heisenberg Groups 161
Exercises 165

Chapter 7. Solvable Groups II: Frobenius Groups 169
7.1. Preliminaries 169
7.2. Wreath Products and Semi-Direct Products 173
7.3. Frobenius Groups 175
Exercises 180

Chapter 8. The Number of Parameters 187
8.1. Basic Results 187
8.2. Essential Dimension 190
8.3. Lattices: Better Bounds 196
8.4. \( p \)-Groups in Characteristic \( p \), Revisited 201
8.5. Generic Dimension 201
Exercises 204

Appendix A. Technical Results 207
A.1. The ‘Seen One, Seen Them All’ Lemma 207
A.2. Tensor Products 210
A.3. Linear Disjointness 213
A.4. The Hilbert Nulstellensatz 214

Appendix B. Invariant Theory 217
B.1. Basic Concepts 217
B.2. Invariants 220
B.3. Bracket Polynomials 222
B.4. The First Fundamental Theorem of Invariant Theory 227
Exercises 244

Bibliography 247

Index 255
Acknowledgments

During the course of this work, the authors were supported by various research grants.

Arne Ledet was a postdoctoral fellow at Queen’s University in Canada. Ledet was awarded a research grant from the Advisory Research Committee of Queen’s University in the first year (1996–97). In the second year (1997–98), Ledet was supported by a research grant of Noriko Yui from the Natural Sciences and Engineering Research Council of Canada (NSERC). In the fall semester of 1999, Ledet took part in the special half year program ‘Galois Groups and Fundamental Groups’ at the Mathematical Sciences Research Institute (MSRI) in Berkeley, California, supported by a grant from the Danish Research Council.

Christian U. Jensen was partially supported by the Algebra Group Grant from the Danish Research Council.

Noriko Yui was partially supported by a research grant from the NSERC.

During the completion of this work, the three authors benefitted from the Research in Pairs (RIP) program at Mathematisches Forschungsinstitut für Mathematik at Oberwolfach, supported by the Volkswagen-Stiftung.

A more-or-less complete version was produced while Ledet and Yui were at the MSRI, participating in the Algorithmic Number Theory Program, Fall 2000. Further work on the part of Ledet was supported by a Research Fellowship at Tokyo Metropolitan University for the period December 26, 2000, to May 2001, as well as by a research grant of Professor Miyake. Further work on the part of Yui was supported by Visiting Professorships at CRM Barcelona, Max-Planck Institut für Mathematik Bonn, and at FIM ETHZ Zürich.

Finally, the authors wish to express their gratitude to a number of colleagues, who either read various drafts of the text, offering suggestions and comments, or discussed the subject matter with us. In particular, thanks go to (in alphabetical order) J. Buhler, H. Cohen, J.-L. Colliot-Thélène, D. Harbater, K. Hashimoto, I. Kaplansky, G. Kemper, H. W. Lenstra, Jr., B. H. Matzat, J. Mináč, K. Miyake, Z. Reichstein and D. Saltman.