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

Mathematical Sciences Research Institute Publications

1 Freed/Uhlenbeck: *Instantons and Four-Manifolds*, second edition
2 Chern (ed.): *Seminar on Nonlinear Partial Differential Equations*
3 Lepowsky/Mandelstam/Singer (eds.): *Vertex Operators in Mathematics and Physics*
4 Kac (ed.): *Infinite Dimensional Groups with Applications*
5 Blackadar: *K-Theory for Operator Algebras*, second edition
6 Moore (ed.): *Group Representations, Ergodic Theory, Operator Algebras, and Mathematical Physics*
7 Chorin/Majda (eds.): *Wave Motion: Theory, Modelling, and Computation*
8 Gersten (ed.): *Essays in Group Theory*
9 Moore/Schochet: *Global Analysis on Foliated Spaces*
10–11 Drasin/Earle/Gehring/Kra/Marden (eds.): *Holomorphic Functions and Moduli*
12–13 Ni/Peletier/Serrin (eds.): *Nonlinear Diffusion Equations and Their Equilibrium States*
14 Goodman/de la Harpe/Jones: *Coxeter Graphs and Towers of Algebras*
15 Hochster/Huneke/Sally (eds.): *Commutative Algebra*
16 Ihara/Ribet/Serre (eds.): *Galois Groups over* $\mathbb{Q}$
17 Concus/Finn/Hoffman (eds.): *Geometric Analysis and Computer Graphics*
18 Bryant/Chern/Gardner/Goldschmidt/Griffiths: *Exterior Differential Systems*
19 Alperin (ed.): *Arboreal Group Theory*
20 Dazord/Weinstein (eds.): *Symplectic Geometry, Groupoids, and Integrable Systems*
21 Moschovakis (ed.): *Logic from Computer Science*
22 Ratiu (ed.): *The Geometry of Hamiltonian Systems*
23 Baumslag/Miller (eds.): *Algorithms and Classification in Combinatorial Group Theory*
24 Montgomery/Small (eds.): *Noncommutative Rings*
25 Akbulut/King: *Topology of Real Algebraic Sets*
26 Judah/Just/Woodin (eds.): *Set Theory of the Continuum*
27 Carlsson/Cohen/Hsiang/Jones (eds.): *Algebraic Topology and Its Applications*
28 Clemens/Kollár (eds.): *Current Topics in Complex Algebraic Geometry*
29 Nowakowski (ed.): *Games of No Chance*
30 Grove/Petersen (eds.): *Comparison Geometry*
31 Levy (ed.): *Flavors of Geometry*
32 Cecil/Chern (eds.): *Tight and Taut Submanifolds*
33 Axler/McCarthy/Sarason (eds.): *Holomorphic Spaces*
34 Ball/Milman (eds.): *Convex Geometric Analysis*
35 Levy (ed.): *The Eightfold Way*
36 Gavosto/Krantz/McCallum (eds.): *Contemporary Issues in Mathematics Education*
37 Schneider/Siu (eds.): *Several Complex Variables*
38 Billera/Björner/Green/Simion/Stanley (eds.): *New Perspectives in Geometric Combinatorics*
39 Haskell/Pillay/Steinhorn (eds.): *Model Theory, Algebra, and Geometry*
40 Bleher/Its (eds.): *Random Matrix Models and Their Applications*
41 Schneps (ed.): *Galois Groups and Fundamental Groups*
42 Nowakowski (ed.): *More Games of No Chance*
43 Montgomery/Schneider (eds.): *New Directions in Hopf Algebras*

Volumes 1–4 and 6–27 are published by Springer-Verlag

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

CAMBRIDGE
UNIVERSITY PRESS

Christian U. Jensen
Department of Mathematics
University of Copenhagen
Universitetsparken 5
DK-2100 København Ø
Denmark

Arne Ledet
Department of Mathematics and Statistics
Texas Tech University
Lubbock, TX 79409-1042
United States

Noriko Yui
Department of Math. and Stat.
Queen's University
Kingston, Ontario
Canada K7L 3N6

The Mathematical Sciences Research Institute wishes to acknowledge support by the National Science Foundation. This book includes material based upon work supported by NSF Grant 9810361.

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

Printed in the United States of America

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

Library of Congress Cataloging in Publication data available

ISBN 0 521 81998 9 hardback

Contents

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.

Introduction

0.1. The Inverse Problem of Galois Theory

Let G be a finite group, and let K be a field. The Inverse Problem of Galois Theory, as formulated for the pair (G, K), consists of two parts:

(A) General existence problem. *Determine whether G occurs as a Galois group over K. In other words, determine whether there exists a Galois extension M/K such that the Galois group* $\mathrm{Gal}(M/K)$ *is isomorphic to G.*

We call such a Galois extension M a *G-extension* over K.

(B) Actual construction. *If G is realisable as a Galois group over K, construct explicit polynomials over K having G as a Galois group. More generally, construct a family of polynomials over a K having G as Galois group.*

The classical Inverse Problem of Galois Theory is the existence problem for the field $K = \mathbb{Q}$ of rational numbers.

It would of course be particularly interesting if the family of polynomials we construct actually gives *all* G-extensions of K. One obvious way of formulating this is in the form of a *parametric* or *generic* polynomial:

Definition 0.1.1. Let $P(\mathbf{t}, X)$ be a monic polynomial in $K(\mathbf{t})[X]$, where $\mathbf{t} = (t_1, \ldots, t_n)$ and X are indeterminates, and let $\mathbb{M}$ be the splitting field of $P(\mathbf{t}, X)$ over $K(\mathbf{t})$. Suppose that $P(\mathbf{t}, X)$ satisfies the following conditions:

(i) $\mathbb{M}/K(\mathbf{t})$ is Galois with Galois group $\mathrm{Gal}(\mathbb{M}/K(\mathbf{t})) \simeq G$, and
(ii) every Galois extension M/K with $\mathrm{Gal}(M/K) \simeq G$ is the splitting field of a polynomial $P(\mathbf{a}, X)$ for some $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$.

Then we say that $P(\mathbf{t}, X)$ *parametrises* G-extensions of K, and call $P(\mathbf{t}, X)$ a *parametric polynomial*.

The parametric polynomial $P(\mathbf{t}, X)$ is said to be *generic*, if it satisfies the following additional condition:

(iii) $P(\mathbf{t}, X)$ is parametric for G-extensions over any field containing K.

Remark. The motivation for this definition is roughly speaking as follows:

Condition (i) ensures that we *are* in fact looking specifically at the structure of G-extensions, cf. section 3.3 in Chapter 3, and are not getting the G-extensions in (ii) merely by 'degenerate' specialisations. For instance: A cyclic extension of degree 4 is of course the splitting field of a quartic polynomial. However, the splitting field of an arbitrary quartic polynomial is unlikely to be cyclic.

Condition (ii) is a demand that the 'family' of G-extensions given by our polynomial $P(\mathbf{t}, X)$ covers *all* G-extensions. This was, after all, the whole point.

Condition (iii) expresses the experiental fact that our analysis and construction may well make use only of such properties of K as are inherited by larger fields, saving us the trouble of having to analyse the situation over such fields separately. Also, adopting an algebraic geometric viewpoint for a moment, that the study of varieties over a field (which encompasses Galois theory through extensions of function fields) does not merely consider the rational points over the ground field itself, but also those over extension fields.

The next natural question after (B) one may ask is thus:

(C) Construction of generic polynomials. *Given K and G as above, determine whether a generic polynomial exists for G-extensions over K, and if so, find it.*

Remark. We point out that the definition of generic polynomials given here is weaker than the one given by DeMeyer in [DM], where it is required that all subgroups of G can be obtained by specialisations as well. However, over infinite fields, the two concepts coincide (see Chapter 5).

The t_i's are the *parameters* of the generic polynomial. This raises a further question:

(D) The Number of Parameters. *What is the smallest possible number of parameters for a generic polynomial for G-extensions over K? (Again, assuming existence.)*

Remarks. The existence problem (A) has been solved in the affirmative in some cases. On the other hand, for certain fields, not every finite group occurs as a Galois group.

(1) If $K = \mathbb{C}(t)$, where t is an indeterminate, any finite group G occurs as a Galois group over K. This follows basically from the Riemann Existence Theorem. More generally, the absolute Galois group of the function field $K(t)$ is free pro-finite with infinitely many generators, whenever K is algebraically closed, cf. [Hrb2] and [Pop].

(2) If $K = \mathbb{F}_q$ is a finite field, the Galois group of every polynomial over K is a cyclic group.

(3) If K is a $\mathfrak{p}$-adic field, any polynomial over K is solvable, cf. e.g. [Lo2, §25 Satz 5].

(4) If K is a $\mathfrak{p}$-adic field, and $K(t)$ a function field over K with indeterminate t, any finite group G occurs as a Galois group over $K(t)$, by the Harbater Existence Theorem [Hrb1].

Remarks. Concerning the problem (C) about generic polynomials, sometimes results are known in greater generality than just for a single pair (G, K).

(1) The polynomial $X^p - X - t$ is generic for cyclic extensions of degree p over $\mathbb{F}_p$ for all primes p, by Artin-Schreier theory. The polynomial $X^n - t$ is generic for cyclic extensions of degree n over fields containing the primitive n^{th} roots of unity, for all $n \in \mathbb{N}$, by Kummer theory.

(2) The polynomial $X^n + t_1 X^{n-1} + \cdots + t_n$ is generic for S_n-extensions for any field and any $n \in \mathbb{N}$, where S_n is the symmetric group on n letters. This

indicates that we might (and should) try to find generic polynomials for *families* of pairs (G, K), rather than focus on an individual pair (G, K).

(3) It is also of course trivial that the existence of generic polynomials over K for groups G and H (not necessarily distinct) implies the existence of a generic polynomial for the direct product $G \times H$.

The Inverse Galois Problem is particularly significant when K is the field $\mathbb{Q}$ of rational numbers (or, more generally, an algebraic number field), or a function field in several indeterminatess over $\mathbb{Q}$ (or over an algebraic number field).

In this connection, an especially interesting version of the Inverse Problem (over $\mathbb{Q}$) concerns *regular* extensions: Let $\mathbf{t} = (t_1, t_2, \dots, t_n)$ be indeterminates. A finite Galois extension $\mathbb{M}/\mathbb{Q}(\mathbf{t})$ is then called regular, if $\mathbb{Q}$ is relatively algebraically closed in $\mathbb{M}$, i.e., if every element in $\mathbb{M} \setminus \mathbb{Q}$ is transcendental over $\mathbb{Q}$. The big question is then

The Regular Inverse Galois Problem. *Is every finite group realisable as the Galois group of a regular extension of* $\mathbb{Q}(t)$?

Whenever we have a Galois extension $\mathbb{M}/\mathbb{Q}(\mathbf{t})$ (regular or not), it is an easy consequence of the Hilbert Irreducibility Theorem (covered in Chapter 3 below) that there is a 'specialisation' $M/\mathbb{Q}$ with the same Galois group. Moreover, if $\mathbb{M}/\mathbb{Q}(\mathbf{t})$ is regular, we get such specialised extensions M/K over *any* Hilbertian field in characteristic 0, in particular over all algebraic number fields. Hence the special interest in the Regular Inverse Galois Problem.

Concerning the existence problem (A), there are already several monographs addressing the problem, e.g., Malle and Matzat [M&M2] and Völklein [Vö]. In this book, our main aim is then to consider problem (C), the construction of generic polynomials with prescribed finite groups as Galois groups.

The nature of the Inverse Problem of Galois Theory, in particular its constructive aspects, resembles that of the Diophantine problems, and it has been an intractably difficult problem; it is still unsolved.

0.2. Milestones in Inverse Galois Theory

The Inverse Galois Problem was perhaps known to Galois. In the early nineteenth century, the following result was known as folklore:

The Kronecker-Weber Theorem. *Any finite abelian group G occurs as a Galois group over $\mathbb{Q}$: Indeed G is realized as the Galois group of a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is an n^{th} root of unity for some natural number n.*

For proof, we refer to e.g. [Lo3, Ch. 13] (or indeed most books on class field theory). For the first part (existence), it follows easily from the fact that there are infinitely many primes $\equiv 1 \pmod{n}$ for any natural number n. For a simple proof of this last statement, see [Hs3].

As for the actual construction, there were examples of polynomials realizing abelian groups G as Galois groups over $\mathbb{Q}$, which were constructed using Gaussian periods.

The first systematic study of the Inverse Galois Problem started with Hilbert in 1892. Hilbert used his Irreducibility Theorem (see Chapter 3) to establish the following results:

THEOREM 0.2.1. *For any $n \geq 1$, the symmetric group S_n and the alternating group A_n occur as Galois groups over $\mathbb{Q}$.*

Further, Hilbert constructed parametric polynomials for S_n, however, he was not able to come up with parametric polynomials for A_n. (Indeed, this problem remains open even today.)

In 1916, E. Noether [Noe] raised the following question:

(0.2.2) THE NOETHER PROBLEM. Let $M = \mathbb{Q}(t_1, \ldots, t_n)$ be the field of rational functions in n indeterminates. The symmetric group S_n of degree n acts on M by permuting the indeterminates. Let G be a transitive subgroup of S_n, and let $K = M^G$ be the subfield of G-invariant rational functions of M. *Is K a rational extension of $\mathbb{Q}$? I.e., is K isomorphic to a field of rational functions over $\mathbb{Q}$?*

If the Noether Problem has an affirmative answer, G can be realised as a Galois group over $\mathbb{Q}$, and in fact over any Hilbertian field of characteristic 0, such as an algebraic number field (cf. section 3.3 of Chapter 3). Additionally, we get information about the structure of G-extensions over *all* fields of characteristic 0 (cf. section 5.1 of Chapter 5).

The next important step was taken in 1937 by A. Scholz and H. Reichardt [Sco, Rei] who proved the following existence result:

THEOREM 0.2.3. *For an odd prime p, every finite p-group occurs as a Galois group over $\mathbb{Q}$.*

The final step concerning solvable groups was taken by Shafarevich [Sha] (with correction appended in 1989; for a full correct proof, the reader is referred to Chapter IX of the book by Neukirch, Schmidt and Wingberg [NS&W, 2000]), extending the result of Iwasawa [Iw] that any solvable group can be realized as a Galois group over the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$.

THEOREM 0.2.4. (SHAFAREVICH) *Every solvable group occurs as a Galois group over $\mathbb{Q}$.*

Shafarevich's argument, however, is not constructive, and so does not produce a polynomial having a prescribed finite solvable group as a Galois group.

Some remarks regarding simple groups. Of the finite simple groups, the projective groups $\mathrm{PSL}(2, p)$ for some odd primes p were among the first to be realized. The existence was established by Shih in 1974, and later polynomials were constructed over $\mathbb{Q}(t)$ by Malle and Matzat:

THEOREM 0.2.5. (a) (SHIH [Shi]) *Let p be an odd prime such that either 2, 3 or 7 is a quadratic non-residue modulo p. Then $\mathrm{PSL}(2, p)$ occurs as a Galois group over $\mathbb{Q}$.*

(b) (Malle & Matzat [M&M1]) *Let p be an odd prime with $p \not\equiv \pm 1 \pmod{24}$. Then explicit families of polynomials over $\mathbb{Q}(t)$ with Galois group $\mathrm{PSL}(2,p)$ can be constructed.*

(c) (Belyi [Bel1]) *Let k be a finite field of odd characteristic, and let G be $\mathrm{SL}(n,k)$, $\mathrm{PSL}(n,k)$, $\mathrm{Sp}(2n,k)$, $\mathrm{SO}(2n+1,k)$, $U(n,k)$, etc. Then there exist finite extensions $L \supseteq K$ of $\mathbb{Q}$ such that $K/\mathbb{Q}$ is abelian and L/K is Galois with Galois group G.*

Belyi (in [Bel2]) also realized simple Chevalley groups of certain types as Galois groups over the maximal cyclotomic field.

For the 26 sporadic simple groups, all but possibly one, namely, the Mathieu group $\mathbf{M}_{23}$, have been shown to occur as Galois groups over $\mathbb{Q}$. For instance:

Theorem 0.2.6. (Matzat & al.) *Four of the Mathieu groups, namely $\mathbf{M}_{11}$, $\mathbf{M}_{12}$, $\mathbf{M}_{22}$ and $\mathbf{M}_{24}$, occur as Galois groups over $\mathbb{Q}$.*

Matzat and his collaborators further constructed families of polynomials over $\mathbb{Q}(t)$ with Mathieu groups as Galois groups.

The most spectacular result is, perhaps, the realization of the Monster group, the largest sporadic simple group, as a Galois group over $\mathbb{Q}$ by Thompson [Th]. In 1984, Thompson succeeded in proving the following existence theorem:

Theorem 0.2.7. (Thompson) *The monster group occurs as a Galois group over $\mathbb{Q}$.*

Most of the aforementioned results dealt with the existence question (A) for $K = \mathbb{Q}$.

Later several families of simple linear groups were realized as Galois groups over $\mathbb{Q}$ (see Malle and Matzat [M&M2]).

It should be noted that all these realization results of simple groups were achieved via the rigidity method (see section 0.7 below) and the Hilbert Irreducibility Theorem (see Chapter 3).

0.3. The Noether Problem and Its History

In this monograph, we will be mostly concerned with constructive aspects of the Inverse Galois Problem. We will be focusing on the question (C), construction of generic polynomials having prescribed finite groups as Galois groups.

The Noether Problem (NP) concerning rational extensions over $\mathbb{Q}$ has a long preceding history.

An extension L/K is called *rational* if there exists a transcendence basis $\{\beta_i\}_{i\in I}$ such that $L = K(\{\beta_i\}_{i\in I})$, in which case L is K-isomorphic to the field $K(\{t_i\}_{i\in I})$ of rational functions in the t_i's.

In 1875, Lüroth [Lü] (for a more contemporary reference, see Jacobson [Ja2, 8.14]) proved the following result:

Theorem 0.3.1. (Lüroth) *Let L/K be a rational field extension of transcendence degree 1. Then any subfield of L containing K is either K or a rational extension $K(t)$ where t is an indeterminate.*

In this connection, there arose the so-called Lüroth problem:

(0.3.2) The Lüroth Problem. Let L be an arbitrary rational extension of a field K. Is any subfield of L containing K rational over K?

Some positive answers to the Lüroth Problem were obtained. In 1894, Castelnuovo showed the following result:

Theorem 0.3.3. (Castelnuovo [Ca]) *Let K be algebraically closed of characteristic 0. If L is a rational extension over K of transcendence degree 2, then any subfield of L containing K is rational over K.*

However, it was shown by Zariski [Z] in 1958 that this is no longer true if K has positive characteristic.

To state more results on the Lüroth problem and related topics, we now introduce the notion of *unirational* and *stably rational* extensions of fields.

A field extension L/K is said to be *unirational* if L is a subfield of a rational extension of K, and *stably rational* if $L(u_1, u_2, \ldots, u_r)$ is rational over K for some r, that is, if L becomes rational over K after adjoining a finite number of indeterminates.

In geometric terms an irreducible algebraic variety defined over K is rational, resp. unirational, resp. stably rational if its fields of rational functions is a rational, resp. unirational, resp. stably rational extension of K.

Clearly, we have the following implications:

$$\text{rational} \Rightarrow \text{stably rational} \Rightarrow \text{unirational}.$$

However, the arrows are not reversible. The first candidates for examples showing that 'unirational' does not imply 'rational' were discussed by Enriques [En] in 1897, and G. Fano [Fn] in 1904. The first correct and well-documented examples are due to B. Segre, who considered smooth cubic surfaces $X \subset \mathbb{P}^3_K$ and wrote a series of papers on that subject in the decade 1940–1950. He proved that such a surface is unirational if it has a K-rational point. His simplest example of a unirational but non-rational surface is a smooth cubic surface X/K over $K = \mathbb{R}$ such that the topological space $X(\mathbb{R})$ has two connected components. See [Sg1], as well as [Sg2].

The first example of a stably rational but not rational extension was given by Beauville, Colliot-Thélène, Sansuc and Swinnerton-Dyer [Be&al]. Their example is a non-rational surface which is stably rational over $\mathbb{Q}$. We will give an example of a field which is unirational but not stably rational on p. 57 in Chapter 2.

We should here mention some other known examples of unirational but not rational extensions. Segre (cited above) gave examples of unirational but not rational surfaces, developing along the way the theory of linear systems with base points. Clemens and Griffiths (in [C&G]) constructed the intermediate Jacobian of the cubic threefold. This Jacobian is a unirational but not a rational variety over $\mathbb{C}$. Another example was constructed by Iskovskih and Manin [I&M] as a counterexample to the Lüroth Problem, using generalization of the theory of linear systems with base points. Their example was a quartic threefold

in $\mathbb{P}^4$ over $\mathbb{C}$. For non-algebraically closed fields, there are several articles addressing non-rationality question of varieties (mostly surfaces). Also, elementary examples were given by Artin and Mumford in [Ar&M]. We are not going into a detailed discussion of those examples, but refer the interested reader to the papers cited above, as well as Ojanguren [Oj], and the references therein.

The Lüroth Problem led to a related problem. Let G be a finite group acting faithfully on $L/\mathbb{Q}$ (i.e., G is a group of automorphisms of L fixing the base field $\mathbb{Q}$), and pick a special subfield of L, namely the fixed field L^G. Then the Lüroth Problem in this context is the Noether Problem (NP) formulated in (0.2.2) for $K = \mathbb{Q}$. Prior to Noether, Burnside considered the problem concerning the fixed point fields of automorphisms of rational function fields (which later was popularised by the name of 'the Noether Problem'), and he obtained several results:

THEOREM 0.3.4. (BURNSIDE 1908, [Bs]) *The fixed field of C_3 acting regularly on $K(t_1, t_2, t_3)$ is rational over K provided that K contains the third roots of unity. Similarly, the fixed field of A_4 acting regularly on $K(t_1, t_2, t_3, t_4)$ is rational (under some conditions on the ground field K).*

By the classical theorem that any symmetric rational function is a rational function in the elementary symmetric polynomials, it follows that the Noether Problem has a positive answer for the symmetric group S_n. E. Noether and some of her contemporaries gave positive answers for several other groups of small degree. Here are some results for solvable groups:

THEOREM 0.3.5. (a) (FURTWÄNGLER 1925, [Fu]) *The Noether Problem has a positive solution for every solvable transitive subgroup G of S_p, where $p = 3, 5, 7, 11$, for $K = \mathbb{Q}$ and G acting as a regular permutation group of the indeterminates $t_1, \ldots, t_n$, $n = |G|$.*

(b) (GRÖBNER 1934, [Grö]) *The Noether Problem has a positive answer for the quaternion group Q_8.*

For the alternating groups A_n, the Noether Problem is still open: For A_5 the answer is affirmative, and this was proved by Maeda [Mae] in 1989. However, for A_n, $n \geq 6$, the answer remains unknown.

It turns out that the Noether Problem does not always have a positive answer. This raises yet another question: *For which groups G does it fail to have an affirmative solution?*

In 1925, Furtwängler noticed that his argument (proving point (a) in the Theorem above) did not work for the cyclic group C_{47}. Swan and V. E. Voskresenskii (working independently) gave counter-examples to the Noether Problem for the cyclic groups C_{47}, C_{113}, C_{223}, etc., in their papers [Swn1, 1969] and [Vo1, 1970]. Later, more conceptual and accessible, and also stronger, results were obtained by H. Lenstra [Len]: For instance, he shows that the smallest group for which the Noether Problem fails is the cyclic group C_8, and further he gave a complete classification of abelian groups for which the Noether Problem fails. (See also Saltman [Sa1, 1982].)

0.4. Strategies

As we mentioned above, a positive solution to the Noether Problem for a finite group G over $\mathbb{Q}$ yields a positive solution to the question (A), concerning the existence of a G-extension, and moreover it gives rise to a positive answer to the question (C), about generic polynomials. We will push Noether's strategy to its fuller extent.

Noether's strategy: Invariant theory. Noether's strategy may work well for the symmetric groups S_n, but as we have seen above, it becomes complicated for other groups, even of small order.

Closer analysis concerning the existence (and construction) of polynomials with Galois group G turns out to be more productive if we consider generalisations of the original Noether Problem. Of course, the Noether Problem can be formulated over any field, rather than just $\mathbb{Q}$. Also we may take different actions of G on the function fields.

Let K be any field and let $M = K(t_1, t_2, \ldots, t_n)$ be the field of rational functions over K in n indeterminates $\mathbf{t} = (t_1, t_2, \ldots, t_n)$. Let G be a finite group. Depending on the action of G on the field M, we have several variants of the Noether Problem. We now formulate the Noether Problem (NP), Linear Noether Problem (LNP), and General Noether Problem (GNP) depending on the action of G.

(0.4.1) The Noether Problem (NP). Assume that G acts on M as a transitive permutation group on the set $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ of indeterminates, and let $L = M^G$. Is L rational over K?

(0.4.2) The Linear Noether Problem (LNP). Let G be a (finite) subgroup of $GL_n(K)$, and define a G-action on M by $\sigma t_i = a_{1i}t_1 + \cdots + a_{ni}t_n$ when $(a_{1i}, \ldots, a_{ni}) \in K^n$ is the image of the i^{th} canonical basis vector under σ. Let $L = M^G$. Is L rational over K?

(0.4.3) The General Noether Problem (GNP). Let G be a (finite) subgroup of the K-automorphism group $\mathrm{Aut}_K(M)$, and let $L = M^G$. Is L rational over K?

The inclusions are NP $\subset$ LNP $\subset$ GNP.

From now on we assume that our ground field K is infinite. We note that, by a Theorem of Kuyk [Ku, Thm. 1], an affirmative answer to the Noether Problem (NP) for a group G over an infinite field K implies the existence of a generic polynomial for G-extensions over K (cf. also section 5.1 in Chapter 5).

Now we will encode various implications in the following diagram. We consider a pair (G, K) where we assume that G is a finite group and K is an infinite field.

$$\begin{array}{ccccc} \text{NP} & \Rightarrow \text{Generic Poly} & \Rightarrow \text{Regular Ext} & \underset{(*)}{\Rightarrow} & \text{Galois Ext} \\ \Uparrow & & \Uparrow & & \\ \text{LNP} & & \text{GNP} & & \end{array}$$

Here $(*)$ means that K is assumed to be Hilbertian, cf. Chapter 3. Note that the reverse implications do not hold. Parametric polynomials are not included in the diagram. It is obvious that

$$\text{Generic Polynomial} \Rightarrow \text{Parametric Polynomial}.$$

However, there are examples of pairs (G, K) for which parametric polynomials can be constructed over K, while generic polynomial cannot. For instance, the pair $(C_8, \mathbb{Q})$ gives an example of C_8-parametric polynomials over $\mathbb{Q}$, but no generic C_8-polynomials.

0.5. Description of Each Chapter

The main theme of this monograph is the construction of generic polynomials having a prescribed finite group G as Galois group.

Chapter 1, 'Preliminaries', contains, as the name implies, some basic results needed in the remainder of the text, mostly on linear representations of finite groups.

In Chapter 2, we confine ourselves to groups of small degree. Specifically we look into the following problem: Let K be a field and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ be irreducible and separable. Then $\mathrm{Gal}(f/K)$ is a transitive subgroup of the symmetric group S_n. We restrict ourselves to groups of degree 3, 4, 5, 6, 7 and 11, although it is already known that all groups of degree ≤ 15 occur as Galois groups over $\mathbb{Q}$. (See [M&M2] and [Kl&M].) Our main concern is to give criteria for recognising a polynomial with a specified group as Galois group by making use of the resolvent polynomials. We also exhibit generic polynomials for the groups of degree 3, 4 and 5. For instance, we have the following result:

THEOREM 0.5.1. (BRUMER) *A generic polynomial for the dihedral group D_5 of degree 5 over an arbitrary field K is given as follows:*

$$f(s,t,X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t$$

over $K(s,t)$ where s and t are indeterminates.

We also demonstrate the non-existence of a generic C_8-polynomial over $\mathbb{Q}$, and as a consequence get the following two examples of fixed subfields of the function field $\mathbb{Q}(s,t,u)$ in three indeterminates s,t,u, both with a C_4-action, where one is rational and the other not:

THEOREM 0.5.2. (a) *Let σ be the automorphism on $\mathbb{Q}(s,t,u)$ given by*

$$\sigma\colon s \mapsto t, \quad t \mapsto u, \quad u \mapsto -\frac{1}{stu}.$$

Then σ has order 4 and $\mathbb{Q}(s,t,u)^{C_4}/\mathbb{Q}$ is not rational.

(b) *Let τ be the automorphism on $\mathbb{Q}(s,t,u)$ given by*

$$\tau\colon s \mapsto t, \quad t \mapsto u, \quad u \mapsto \frac{1}{stu}.$$

Then τ has order 4 and $\mathbb{Q}(s,t,u)^{C_4}/\mathbb{Q}$ is rational.

The example (a) in the above theorem is perhaps the simplest (easiest to prove) example of a unirational but non-rational field extension, having transcendence degree 3 over $\mathbb{Q}$. For a proof of this theorem, see Chapter 2. Colliot-Thélène has communicated to us an example of a unirational but non-rational extension of transcendence degree 2 over $\mathbb{Q}$, namely the quotient field of the ring

$$\mathbb{Q}[x, y, z]/(x^3 - x - y^2 - z^2),$$

cf. also Ojanguren in [Oj] and Beauville et al. in [Be&al].

In Chapter 3, we give a complete proof of the Hilbert Irreducibility Theorem. This theorem plays an important role to establish the existence of polynomials with a prescribed finite group as a Galois group. In fact, most of the positive results in the Inverse Galois Problem depend on the Hilbert Irreducibility Theorem, more precisely, on producing *regular* extensions over $\mathbb{Q}$.

In this chapter, we also consider (briefly) the Regular Inverse Galois Problem mentioned earlier. For the symmetric group S_n and the alternating group A_n, regular extensions are constructed over $\mathbb{Q}$.

Unfortunately, the Hilbert Irreducibility Theorem, as we prove it, is not constructive, i.e., it does not indicate how to pick a suitable specialisation to produce polynomials over $\mathbb{Q}$ (or an algebraic number field) for a given group G. This is not a serious difficulty, however, since the set of suitable specialisations is dense, and choosing at random has a pretty good chance of success.

In Chapter 4, we present a generalisation of the usual Galois theory of fields to a Galois theory of commutative rings. For extensions of fields (so-called Galois algebras), this generalisation was first carried out independently by D. K. Faddeev and H. Hasse.[1] For a nice exposition of this topic, the reader is referred to the original work by Chase, Harrison and Rosenberg [CH&R], as well as DeMeyer and Ingraham [D&I], and Greither [Gr]. Our account of the theory is mostly based on [D&I], although we have avoided any reference to separable algebras (which is the central topic of that work). An advantage of introducing this general notion of a Galois extension is to avoid case by case analysis based on whether the ground fields contain roots of unity or not. In short, this theory may be regarded as a base change theory and also as refinement of 'reduction modulo primes' allowing us to treat specialisations in more streamlined fashion.

Chapter 5 is the backbone of this monograph. In this chapter we give a thorough discussion about generic extensions and generic polynomials. Incidentally, when the ground field K is infinite, the notions of generic extensions and generic polynomials do coincide as proved by Ledet in [Le10]. As we remarked above, not all finite groups, even abelian groups, have generic polynomials. The first question of our interest is the characterisation of finite abelian groups for which generic polynomials exist.

THEOREM 0.5.3. (LENSTRA) *Let G be a finite abelian group and $K = \mathbb{Q}$. Then generic polynomials exist for $(G, \mathbb{Q})$ if and only if G has no elements of order 8.*

[1] In the 1940's, when communication between Germany and Russia was less than perfect.

Group	Field	Generic polynomial
C_2, C_4	Arbitrary	Yes
C_n, n odd	Arbitrary	Yes
C_{2^e}, $e > 2$	$\mathbb{Q}$	No
p-group	Char. p	Yes
Q_8	Char. $\neq 2$	Yes
D_n, n odd	Arbitrary	Yes
D_8, QD_8, M_{16}	Arbitrary	Yes
$F_{p\ell}$	$\mathbb{Q}$	Yes, if $8 \nmid \ell$
S_n	Arbitrary	Yes
A_4	Arbitrary	Yes
A_5	Arbitrary	Yes

TABLE 1. Generic Polynomials

This Theorem is a composite of results from Chapters 2 and 5.

Summary of the existence of generic polynomials is tabulated in Table 1.

Certain other cases are known as well, of course, such as the cyclic group C_n of order n, over fields containing the primitive n^{th} roots of unity. Also, abelian groups can be considered by writing them as direct products of cyclic groups. For $n > 5$, it is unknown whether A_n has a generic polynomial (over any field). Most known negative results stem from the non-existence of generic C_{2^e}-polynomials, $e > 2$, over $\mathbb{Q}$, which also excludes abelian groups containing elements of order 8, as well as Frobenius groups $F_{p\ell}$ with $8 \mid \ell$. In [Sa3], Saltman exhibits some p-groups of high order (p^9) that do not possess generic polynomials over *any* field of characteristic 0.

REMARKS. (1) The crucial fact in proving that there is no generic C_8-polynomial over $\mathbb{Q}$ is that the unramified C_8-extension of the field $\mathbb{Q}_2$ of 2-adic numbers is not induced (by scalar extension) from a C_8-extension of $\mathbb{Q}$. It would seem plausible that something similar might work in other cases, but nothing is known.

(2) The smallest group for which the question of existence of a generic polynomial over $\mathbb{Q}$ is unanswered is the quaternion group of order 16, cf. Chapter 6. The next is the special linear group $\mathrm{SL}(2,3)$ of order 24.

We also give a treatment of p-groups in characteristic $p > 0$. More specifically, we prove that generic polynomials always exist in that case, a result basically due to Gaschütz [Ga].

In Chapter 6 we will consider certain p-groups in characteristic $\neq p$, mostly for $p = 2$. These include dihedral groups D_{2^n}, the quasi-dihedral groups QD_{2^n} and the quaternion groups Q_{2^n}, as well as the the Heisenberg group of order p^3.

We construct generic polynomials over field K of characteristic different from 2 for Q_8, QD_8 as well as for the central product QC of Q_8 and C_4.

Chapter 7 is concerned with some other solvable groups, i.e., dihedral groups and Frobenius groups of prime degree. (For our purposes, a Frobenius group is a semi-direct product $F_{p\ell} = C_p \rtimes C_\ell$, where $\ell \mid p-1$, and C_ℓ acts faithfully. See also [Pa].) We prove:

THEOREM 0.5.4. (a) *Let p be an odd prime, and let $\ell \mid p-1$. Then a generic polynomial for the frobenius group $F_{p\ell}$ over $\mathbb{Q}$ exists if and only if $8 \nmid \ell$.*

(b) *For the Frobenius groups $F_{p(p-1)/2}$ where p is a prime with $p \equiv 3 \pmod 4$, there is an explicit family of polynomials over $\mathbb{Q}$ with Galois group $F_{p(p-1)/2}$.*

Finally in Chapter 8, we will address question (D), i.e., the question of how many parameters are needed in a generic polynomial. Let (G, K) be a pair of a finite group G and a field K. When there is a generic polynomial over K realising G as a Galois group, a lower bound for the number of parameters is given by the *essential dimension*, $\operatorname{ed}_K G$, which is defined by Buhler and Reichstein [B&R1] as follows: Suppose that G acts regularly on the rational extension $K(t_1, t_2, \ldots, t_n)$ where $n = |G|$. Consider all G-extensions M/L such that $K \subseteq L \subseteq K(t_1, t_2, \ldots, t_n)^G$ and $K(t_1, t_2, \ldots, t_n)$ is the compositum of M and $K(t_1, t_2, \ldots, t_n)^G$. The essential dimension $\operatorname{ed}_K G$ of G over K is then the minimum of the transcendence degrees $\operatorname{tr.deg}_K L$, where L runs through all fields considered above.

THEOREM 0.5.5. (a) *If there is a generic polynomial over K for a group G, then the number of parameters is at least $\operatorname{ed}_K G$.*

(b) *Let (G, K) be a pair of a finite group G and a field K. A necessary condition for the existence of a generic G-polynomial with one parameter is that G embeds into $\mathrm{PGL}_2(K)$.*

However, if G is a finite group for which there exists a generic G-polynomial over K, it is an open problem whether there is a generic G-polynomial with exactly $\operatorname{ed}_K G$ parameters. In general it is rather difficult to find the exact number of parameters in a generic polynomial for a group G. We have only rudimentary results. Even for cyclic groups, we do not have entirely satisfactory answers.

THEOREM 0.5.6. (SMITH) *For C_{p^n}, where p^n is an odd prime power, there is a generic polynomial over $\mathbb{Q}$ with $p^{n-1}(p-1)/2$ parameters.*

This is not an optimal result, however: For $p^n = 7$, it can be shown (in a non-explicit way) that there is a generic polynomial with two parameters. Similarly, there is a generic C_{11}-polynomial over $\mathbb{Q}$ with only four parameters. On the other hand, Smith's result is completely constructive, and allows us to produce the polynomial if desired.

In Chapter 8, we also prove the following result:

THEOREM 0.5.7. (BUHLER & REICHSTEIN) *Let p^n be a prime power. Then the essential dimension for the cyclic group C_{p^n} over $\mathbb{Q}$ is at most $\varphi(p-1)p^{n-1}$, where φ is the Euler φ-function.*

It appears plausible that this may in fact give the exact value of the essential dimension. Also, for $p^n = 2$, 3, 4, 5, 7, 9, 11 and 13, it can be shown that generic polynomials exist with the number of parameters exactly equal to the upper bound on the essential dimension. (For $p^n = 8$, there is no generic polynomial over $\mathbb{Q}$.) Thus, one may pose the following 'double conjecture':

CONJECTURE. The essential dimension over $\mathbb{Q}$ for the cyclic group C_{p^n}, p^n a prime power, is exactly $\varphi(p-1)p^{n-1}$, and when p^n is odd there is a generic C_{p^n}-polynomial over $\mathbb{Q}$ with $\varphi(p-1)p^{n-1}$ parameters.

More generally, $\varphi(p-1)p^{n-1}$ gives an upper bound for the essential dimension of the semi-direct product $\mathbb{Z}/p^n \rtimes (\mathbb{Z}/p^n)^*$. In particular, for $n = 1$ it provides an upper bound on the essential dimension of any solvable group of degree p.

For non-prime powers, we can get bounds using an 'addition formula': For groups G and H, Corollary 8.2.9 from Chapter 8 gives $\mathrm{ed}_K(G \times H) \leq \mathrm{ed}_K G + \mathrm{ed}_K H$. This can be shown to give the exact value of $\mathrm{ed}_{\mathbb{Q}} C_n$ for a few composite n, notably $n = 6$, 10 and 12, and one may conjecture that it works generally.

This Chapter also contains a summary of results on the essential dimension for p-groups in characteristic $p > 0$, and some remarks regarding the *generic dimension* of a finite group over a field, which we define to be the minimal number of parameters in a generic polynomial.

We conjecture that that the generic dimension coincides with the essential dimension when both are finite.

Finally we should point out that a generic polynomial over $\mathbb{Q}$ for a finite group G can have no two consecutive coefficients equal to 0, cf. Exercise 5.4 in Chapter 5. For instance, no trinomials of degree $n \geq 4$ can be a generic polynomial for a finite group.

In this connection a problem arises: *When a finite group G is realisable as a Galois group over $\mathbb{Q}$, can G be realised as a Galois group of a totally real number field?*

Regarding this problem, it has been shown by Serre that if *every* finite group is realisable as a Galois group over $\mathbb{Q}$, then it is in fact possible to realise them inside $\mathbb{R}$. (This result will be published in a paper by J. Klüners and G. Malle.)

Appendix A contains various technical results and definitions that are relevant to the main text, but did not fit into it. This includes: The 'Seen one, seen them all' Lemma, Tensor products, Linear disjointness and the Hilbert Nullstellensatz.

Appendix B contains a brief account of invariant theory, needed for the treatment of quintic equations in Chapter 2.

0.6. Notations and Conventions

GROUPS. The groups and related concepts are
S_n: the symmetric group of degree n, of order $n!$.
A_n: the alternating group of degree n, of order $n!/2$.
C_n: the cyclic group of order n.
D_n: the dihedral group of order $2n$.

$F_{p\ell}$: The Frobenius group of order $p\ell$, with $\ell \mid p-1$.
$QD_{2^{n-1}}$: the quasi-dihedral group of order 2^n.
Q_{2^n}: the quaternion group of order 2^n.
M_{2^n}: the modular group of order 2^n.
H_{p^3}: The Heisenberg group of order p^3.
$\mathbf{M}_{11}, \mathbf{M}_{12}, \mathbf{M}_{22}, \mathbf{M}_{23}, \mathbf{M}_{24}$: the Mathieu groups
$\mathrm{PSL}_2(\mathbb{F}_q)$: the projective special linear group of 2×2 matrices over the finite field $\mathbb{F}_q$ of q elements.
$\mathrm{PSL}(2,p) = \mathrm{PSL}_2(\mathbb{F}_p)$, where p is a prime.
$\mathrm{GL}_n(K)$: the general linear group of $n \times n$ matrices with entries in K.
$\mathrm{GL}(n,q) = \mathrm{GL}_n(\mathbb{F}_q)$.
$\mathrm{PGL}_n(K)$: the projective general linear group of $n \times n$ matrices with entries in K.
$\mathrm{PGL}(n,q) = \mathrm{PGL}_n(\mathbb{F}_q)$.
G^n: The direct product of n copies of the group G.
$G_1 \wr G_2$: the wreath product of two groups G_1 and G_2.
$|G|$: the order of a finite group G.
$Z(G)$: the center of a group G.
μ_n: the group of nth roots of unity (within a field).

Fields and rings. From commutative algebra, we use
$\mathbb{Q}$: the field of rational numbers.
$\mathbb{R}$: the field of real numbers
$\mathbb{C}$: the field of complex numbers
$\mathbb{Q}_p$: the field of p-adic rational numbers.
K_v: the completion/localisation of the field K with respect to a discrete valuation v.
$K(\mu_n)$: the n^{th} cyclotomic field over K.
$K(\mathbf{t}) = K(t_1, t_2, \ldots, t_n)$: the field of rational functions in the indeterminates $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ over a field K.
$K[\mathbf{s}] = K[s_1, s_2, \ldots, s_r]$: the polynomial ring in the indeterminates $\mathbf{s} = (s_1, s_2, \ldots, s_r)$ over a field K.
$R_{\mathfrak{p}}$: The localisation of the commutative ring R in the prime ideal $\mathfrak{p}$, i.e., the ring of fractions r/s with $r \in R$ and $s \in R \setminus \mathfrak{p}$.
R_a: The localisation of the commutative ring in the powers of the element $a \in R$, i.e., the ring of fractions r/a^n with $r \in R$ and $n \in \mathbb{N}$.
R^n: The direct sum of n copies of the ring R.
$W_n(L)$: the ring on n-dimensional Witt vectors over a field L.
$\wp$: the map $W_n(L) \to W_n(L)$ given by

$$\wp\colon (a_0, \ldots, a_{n-1}) \mapsto (a_0^p, \ldots, a_{n-1}^p) - (a_0, \ldots, a_{n-1}).$$

Invariants. Various constants associated with fields and groups:
$\ell(K)$: the level of a field K, which is the smallest natural number n for which -1 is a sum of n squares in K, with $\ell(K) = \infty$ if -1 is not a sum of squares.
$\mathrm{tr.deg}_K L$: the transcendence degree of a field L over a field K.
$\mathrm{ed}_K G$: the essential dimension of a finite group G over a field K.
$\mathrm{gd}_K G$: the generic dimension of a finite group G over a field K.

0.7. Other Methods

We should mention that this monograph is not meant to discuss 'all' existing methods on the Inverse Galois Problem. There are already a number of other monographs and textbooks available: Conner and Perlis [C&P], Malle and Matzat [M&M2], Völklein [Vö], Schneps and Lochak [S&L], Serre [Se2], among others.

The rigidity method: Galois coverings of $\mathbb{P}^1$. Let $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{C})$ denote the projective line over $\mathbb{C}$. It is a rational curve of genus $g = 0$, i.e., the Riemann sphere. Let C be a projective non-singular algebraic curve defined over $\mathbb{C}$, of genus $g \geq 1$. Let $\mathrm{Aut}(C)$ denote the group of automorphisms of C. It is known that if $g \geq 2$, then $\mathrm{Aut}(C)$ is a finite group. In fact, if $g \geq 2$, then $\mathrm{Aut}(C)$ is a finite group of order $\leq 84(g-1)$, cf. Hurwitz in [Hw]. (If $g = 1$, $\mathrm{Aut}(C)$ may be infinite.) Let G be a finite group contained in $\mathrm{Aut}(C)$. By a *G-covering*, we mean a quadruple $\Lambda = (C, \mathbb{P}^1, \pi, \phi)$, where

(i) $\mathbb{P}^1$ is the projective line over $\mathbb{C}$,
(ii) C is a projective non-singular algebraic curve of genus $g > 1$,
(iii) $\pi\colon C \to \mathbb{P}^1$ is a surjective rational mapping, and
(iv) $\phi\colon G \hookrightarrow \mathrm{Aut}(C)$ is a monomorphism,

such that the function field of C is a Galois extension of the function field of $\mathbb{P}^1$ and $\phi(G) \subseteq \mathrm{Aut}(C)$ coincides with the group of covering transformations of $\pi\colon C \to \mathbb{P}^1$.

Now suppose that we are given a finite group G. The problem is to construct a Galois covering $\Lambda = (\tilde{C}, \mathbb{P}^1, \pi, \phi)$ having G as the group of automorphisms of $\tilde{C}$. A natural choice for such a curve is $\tilde{C} = C/G$. Then the function field of $\tilde{C}$ is $\mathbb{C}(C)^G \subset \mathbb{C}(C)$ such that $\mathbb{C}(C)$ is Galois over $\mathbb{C}(\tilde{C})$ with Galois group G.

For a fuller exposition of this approach, the readers are referred to the monograph by Malle and Matzat [M&M2], and for the geometric version of the rigidity method to the recent monograph of Völklein [Vö]. Another account is Serre's book [Se2], which discusses, among other things, the rigidity method and the regular inverse Galois problem.

Trace forms. Whenever we have a finite Galois extension M/K with Galois group $G = \mathrm{Gal}(M/K)$, we can consider G as a transitive subgroup of the symmetric group S_n for some natural number n. Let $\widetilde{S}_n$ be the *stem cover* of S_n, i.e., the double cover

$$1 \to \{\pm 1\} \to \widetilde{S}_n \to S_n \to 1$$

in which transpositions lift to elements of order 2, and products of two disjoint transpositions lift to elements of order 4. We then get a double cover $\widetilde{G}$ of G, and we can ask: Can M/K be extended to a $\widetilde{G}$-extension F/K? The answer to that question involves the study of *trace forms*, i.e., quadratic forms of the type $x \mapsto \mathrm{Tr}_{L/K}(x^2)$ defined on a field extension L/K, and have been used by Mestre [Mes] and others to realise stem covers of alternating groups as regular extensions over $\mathbb{Q}$. Realisation of the stem covers of S_n and A_n will not be discussed in this monograph. A survey on trace forms can be found in the

monographs of Conner and Perlis [C&P]. Serre [Se2] studied the trace form $\mathrm{Tr}_{L/K}(x^2)$ in detail.

Methods of Ihara, Schneps, etc. There is an excellent MSRI Conference Proceedings *Galois Groups over* $\mathbb{Q}$, [IR&S], edited by Ihara, Ribet and Serre. There the absolute Galois groups acting on algebraic fundamental groups were extensively discussed.

There are also a two-volume work by Schneps and Lochak, [S&L], where Grothendieck's theory of *dessins d'enfants* (Combinatorial Galois Theory) is treated. The main objects are the moduli spaces $\mathcal{M}_{g,n}$ of genus g curves with n marked points. Combinatorial Galois theory is developed addressing the question to what extent the absolute Galois group of $\mathbb{Q}$ is determined as a profinite group by its action on the fundamental group of the moduli space $\mathcal{M}_{g,n}$.

These works are mostly concerned with realisations of pro-finite groups as Galois groups, and accordingly will lead us too far from the Inverse Galois Problem treated here.

CHAPTER 1

Preliminaries

In this chapter, we collect some results necessary for the subsequent discussions of Galois theory and the Inverse Galois Problem. These include linear representations and their relation to (the existence of) generic polynomials, as well as a brief introduction to resolvent polynomials. The material is of a somewhat technical nature, but as we will be making extensive use of it right from the outset, it will not interrupt the progression of the material to put it at this place, rather than in an appendix.

1.1. Linear Representations and Generic Polynomials

We start with some considerations relating to the Noether Problem which will make finding generic polynomials somewhat easier:

Let G be a finite group, and consider a *representation* of G, i.e., a homomorphism $G \to \mathrm{GL}_K(V)$, where $\mathrm{GL}_K(V)$ is the general linear group for a finite-dimensional K-vector space V. This simply means that V can be considered as a left $K[G]$-module, where $K[G]$ is the group ring.[1]

If M/K is a Galois extension with group G, the Galois action of G on M gives a representation (with M as V), and by the Normal Basis Theorem the $K[G]$-module M is free of rank 1, i.e., isomorphic to $K[G]$ itself.

More generally: Let G be a finite group. We may represent G as a permutation group on a set X with n elements for some n. In this case, we say that G has a *permutation representation of degree* n, that is, G is regarded as a subgroup of S_n. Corresponding to this is a linear representation, in which G acts on the n-dimensional K-vector space K^n by permuting the canonical basis vectors. By abuse of notation, we will refer to this linear representation also as a permutation representation.

We can always represent G as a permutation group of degree $|G|$ by considering it as permuting the elements of G itself by left multiplication. This is the *regular* representation of G, and it is *transitive*, i.e., for all $\alpha, \beta \in X = G$ there is a $\sigma \in G$ with $\sigma\alpha = \beta$.

A representation is *faithful*, if the homomorphism $G \to \mathrm{GL}_K(V)$ is injective, i.e., if no non-trivial element in G acts as the identity on V. Thus the above example is faithful.

[1] In this text, only left modules will be considered. So, from now on, 'module' will mean 'left module'.

As our interest is in Galois theory, we will first look at the question of when the $K[G]$-module V can be considered as a submodule of $K[G]$. To this end, we introduce the *dual* space of V, $V^* = \mathrm{Hom}_K(V, K)$. It is a $K[G]$-module by $\sigma(\varphi)\colon \mathbf{v} \mapsto \varphi(\sigma^{-1}\mathbf{v})$ for $\sigma \in G$ and $\varphi \in V^*$ (giving us the so-called *contragredient representation*, cf. [Hu, V.§16 Def. 16.11]), and it is easily seen that V and V^{**} are isomorphic as $K[G]$-modules. Also, $-^*$ is an *exact contravariant* functor: If $\psi\colon U \to V$ is a $K[G]$-linear map, there is an induced map $\psi^* = \psi\circ\colon V^* \to U^*$, and ψ is injective (resp. surjective) if and only if ψ^* is surjective (resp. injective).

As a (simple) example, we point out that $K[G]^* \simeq K[G]$.

It is now clear that V can be embedded in $K[G]$ if and only if V^* is *cyclic*, i.e., a homomorphic image of $K[G]$. And working out the details, we get the following: If V^* is generated (over $K[G]$) by φ, an embedding of V into $K[G]$ is given by

$$\mathbf{v} \mapsto \sum_{\sigma\in G} \varphi(\sigma^{-1}\mathbf{v})\sigma, \quad \mathbf{v} \in V.$$

Reintroducing the G-extension from the Example above, we have:

Proposition 1.1.1. *Let M/K be a G-extension, and let there be given a representation $G \to \mathrm{GL}_K(V)$. If the dual representation $G \to \mathrm{GL}_K(V^*)$ is cyclic, then the K-vector space V can be embedded in M in a way that respects the group action.*

We note that one case in which the dual representation is cyclic is when there is a subgroup H of G and a vector $\mathbf{u} \in V$, such that $(\sigma\mathbf{u})_{\sigma\in H}$ is a basis for V.

We also note that, by Maschke's Theorem ([Ja2, 5.2 p. 253], or Exercise 7.2 in Chapter 7 below), $K[G]$ is the direct sum of all the irreducible representations of G over K, whenever $\mathrm{char}\, K \nmid |G|$. Thus, in this case, V can be embedded in $K[G]$ if and only if the irreducible constituents of V all have multiplicity 1.

The Linear Noether Problem. If V is a finite-dimensional vector space over the field K, we let $K(V)$ denote a rational function field in which the homogeneous linear polynomials have been identified with V. Thus, a K-basis for V is a transcendence basis for $K(V)/K$. The action of the general linear group $\mathrm{GL}_K(V)$ then extends to $K(V)$. Similarly, we will use $K[V]$ to denote a polynomial ring with the homogeneous linear polynomials identified with V. (Formally: $K[V]$ is the commutative tensor algebra for V over K, and $K(V)$ is the quotient field of $K[V]$.)

Now, let G be a finite subgroup of $\mathrm{GL}_K(V)$. We then have G acting on $K(V)$. This generalises the permutation representations considered in connection with the Noether Problem, since S_n can be identified with the subgroup of $\mathrm{GL}_n(K)$ consisting of matrices with exactly one 1 in each row and each column, and 0's elsewhere. (In other words: S_n acts on K^n by permuting the coordinates.)

This makes it natural to generalise Noether's approach, cf. also the Introduction:

(1.1.2) The Linear Noether Problem (LNP). If the finite group G is considered as a subgroup of a general linear group $\mathrm{GL}_K(V)$ over the field K,

we can let it act on $K(V)$. The question is then as with the original Noether Problem: *Is the fixed field $K(V)^G$ a purely transcendental extension of K?*

EXAMPLE. (ABHYANKAR, [Ab]) Let q be a prime power, and let K be a field containing $\mathbb{F}_q$. Also, let $\mathrm{GL}(n,q) = \mathrm{GL}_n(\mathbb{F}_q)$, and let $\mathbf{s} = (s_1, \ldots, s_n)$ be indeterminates. Denote the splitting field of the polynomial

$$f(X) = X^{q^n} + s_1 X^{q^{n-1}} + \cdots + s_n X$$

over $K(\mathbf{s})$ by $\mathbb{M}$. It is relatively easy to see that the roots of $f(X)$ make up an n-dimensional $\mathbb{F}_q$-vector space. We will refer to such a polynomial as *vectorial*. Also, if $\mathbf{t} = (t_1, \ldots, t_n)$ is a basis for this space, the t_i's are algebraically independent and $\mathbb{M} = K(\mathbf{t})$.

Thus, if we let $\mathrm{GL}(n,q)$ act linearly on $K(\mathbf{t})$, the fixed field has the form $K(\mathbf{s})$ for indeterminates $\mathbf{s} = (s_1, \ldots, s_n)$ in $K[\mathbf{t}]$, and so we have a $\mathrm{GL}(n,q)$-extension $K(\mathbf{t})/K(\mathbf{s})$.[2]

If M/K is a $\mathrm{GL}(n,q)$-extension, we can embed $\mathbb{F}_q^n$ (and in fact K^n) into M in a way that preserves the linear action. The image of $\mathbb{F}_q^n$ in M necessarily generates M over K, and M is the splitting field of the corresponding specialisation of $f(X)$.

Hence, $f(X) \in \mathbb{F}_q(\mathbf{s})[X]$ is generic for $\mathrm{GL}(n,q)$-extensions over $\mathbb{F}_q$.

In fact, a positive answer to a Linear Noether Problem will — under one slight restriction — always give rise to generic polynomials, as the following result from [K&Mt, Thm. 7] shows:

PROPOSITION 1.1.3. *Let G be a finite group, and let K be an* infinite *field. Also, let G be embedded into $\mathrm{GL}_K(V)$ for some V, and assume that the corresponding Linear Noether Problem has an affirmative answer. Then there is a generic G-polynomial over K with $n = \dim_K V$ parameters.*

REMARK. In [Kn, 1955] Kuniyoshi proved that the Noether Problem always has an affirmative answer for p-groups in characteristic p, and in [Ga, 1959] Gaschütz proved the same for *any* Linear Noether Problem. Thus, we can conclude that generic polynomials always exist for p-groups over an *infinite* field in characteristic p.

We will give a proof of Gaschütz' result in section 5.6 of Chapter 5 below, together with a more 'cost-effective' construction of generic polynomials.

We obtain Proposition 1.1.3 as an obvious corollary to the following

PROPOSITION 1.1.4. *Let G be a finite group, and let K be an* infinite *field. Also, let G be embedded into $\mathrm{GL}_K(V)$ for some V, and let $K(\mathbf{u}) = K(u_1, \ldots, u_r)$ be a rational function field. Furthermore, let $F(\mathbf{u}, X) \in K(\mathbf{u})[X]$ be a monic polynomial, and assume that $K(V)$ is the splitting field over $K(V)^G$ of a specialisation of $F(\mathbf{u}, X)$. Then* any *G-extension M/L with $L \supseteq K$ is obtained as the splitting field of a specialisation of $F(\mathbf{u}, X)$ (over L).*

[2] As well as an argument that a polynomial where the roots form an n-dimensional $\mathbb{F}_q$-vector space has the same form as $f(X)$.

PROOF. First, note that, for any $\varphi \in V^*$, the kernel of the map $g_\varphi\colon V \to K[G]$, given by

$$g_\varphi\colon \mathbf{v} \mapsto \sum_{\sigma\in G} \varphi(\sigma^{-1}\mathbf{v})\sigma, \quad \mathbf{v} \in V,$$

and considered above, is $\bigcap_{\sigma\in G} \ker \sigma(\varphi)$. In particular, $\ker g_\varphi \subseteq \ker \varphi$, and so we can pick $\varphi_1, \dots, \varphi_d \in V^*$ (for some d) such that $\bigcap_i \ker g_{\varphi_i} = 0$. This gives us an injective $K[G]$-linear map

$$\mathbf{v} \mapsto (g_{\varphi_1}(\mathbf{v}), \dots, g_{\varphi_d}(\mathbf{v}))$$

from V into $K[G]^d$, i.e., $V \hookrightarrow K[G]^d$. Thus, if $\mathbf{s}_1, \dots, \mathbf{s}_d$ are d sets of $|G|$ indeterminates, each permuted regularly by G, we have an embedding $K[V] \hookrightarrow K[\mathbf{s}_1, \dots, \mathbf{s}_d]$.

Now, let $f(\mathbf{s}_1, \dots, \mathbf{s}_d)$ be any non-zero polynomial in $K[\mathbf{s}_1, \dots, \mathbf{s}_d]$. Then, if $q_2 \in \mathbb{N}$ is picked greater than the highest exponent of any indeterminate in $\mathbf{s}_1$, the polynomial $f(\mathbf{s}_1, \mathbf{s}_1^{q_2}, \mathbf{s}_3, \dots, \mathbf{s}_d)$ is non-zero as well. (Here, $\mathbf{s}_1^{q_2}$ means the ordered set of q_2^{th} powers of the indeterminates in $\mathbf{s}_1$.) It follows that, for a suitable choice of $q_2, \dots, q_d$, the polynomial $f(\mathbf{s}_1, \mathbf{s}_1^{q_2}, \dots, \mathbf{s}_1^{q_d})$ is non-zero. Also, the map $g(\mathbf{s}_1, \dots, \mathbf{s}_d) \mapsto g(\mathbf{s}_1, \mathbf{s}_1^{q_2}, \dots, \mathbf{s}_d^{q_d})$ is a K-algebra homomorphism $K[\mathbf{s}_1, \dots, \mathbf{s}_d] \twoheadrightarrow K[\mathbf{s}_1]$ respecting the G-action.

Assume now that $K(V)$ is the splitting field over $K(V)^G$ of a specialisation $F(\mathbf{t}, X)$, $\mathbf{v} = (t_1, \dots, t_r) \in (K(V)^G)^r$. For a suitable $w \in K[V] \setminus 0$, we have that $t_1, \dots, t_r$ belong to the localised ring $K[V]_w$ (i.e., the ring of elements of the form a/w^e for $a \in K[V]$ and $e \in \mathbb{N}$), and also that $F(\mathbf{v}, X) \in K[V]_w[X]$. Moreover, we can — for each $\sigma \in G \setminus 1$ – pick a root $\xi \in K[V]_w$ of $F(\mathbf{t}, X)$ with $\sigma\xi \neq \xi$ and require $1/(\sigma\xi - \xi) \in K[V]_w$. Let w' be the image of w in $K[\mathbf{s}_1, \dots, \mathbf{s}_d]$, and pick the q_i's as above to ensure that w' maps to a non-zero element $w'' \in K[\mathbf{s}_1]$. We then have homomorphisms

$$K[V]_w \hookrightarrow K[\mathbf{s}_1, \dots, \mathbf{s}_d]_{w'} \twoheadrightarrow K[\mathbf{s}_1]_{w''},$$

all respecting the G-action.

If M/L is a G-extension, we can, by the algebraic independence of the elements in G over M (Theorem 4.3.7 in Chapter 4 below, or [Ja1, 4.14]), find $\theta \in M$ such that $\boldsymbol{\theta} = (\sigma\theta)_{\sigma\in G}$ is a normal basis for M/L and $w''(\boldsymbol{\theta}) \neq 0$. Thus, we have

$$K[V]_w \hookrightarrow K[\mathbf{s}_1, \dots, \mathbf{s}_d]_{w'} \twoheadrightarrow K[\mathbf{s}_1]_{w''} \to M,$$

with the last map defined as follows: If $\mathbf{s}_1 = (s_\sigma)_{\sigma\in G}$ with $\sigma s_\tau = s_{\sigma\tau}$, we map s_σ to $\sigma\theta$. This gives us a K-algebra homomorphism $K[V]_w \to M$ respecting the G-action. Letting $\mathbf{a} = (a_1, \dots, a_r)$ be the images of $\mathbf{t}$ in M, we see that $a_1, \dots, a_r \in L$ and that $F(\mathbf{a}, X)$ splits completely in $M[X]$. Also, G acts faithfully on the roots of $F(\mathbf{a}, X)$: For $\sigma \in G \setminus 1$ we have that $\sigma\xi - \xi$ is invertible in $K[V]_w$ for some root ξ of $F(\mathbf{t}, X)$, and so the image $\sigma\bar{\xi} - \bar{\xi}$ cannot be 0 in M, meaning that σ acts non-trivially on ξ. Hence, M must be the splitting field of $F(\mathbf{a}, X)$ over L. □

From this Proposition, we immediately get various other Corollaries:

PROPOSITION 1.1.5. *Let K be an infinite field and G a finite group. A monic G-polynomial $P(\mathbf{s}, X)$ over $K(\mathbf{s})$ is generic if and only if some 'Noether extension' $K(V)/K(V)^G$ is obtained by specialisation, i.e., if and only if $K(V)$ is the splitting field over $K(V)^G$ of $P(\mathbf{a}, X)$ for some specialisation $\mathbf{a}$ of $\mathbf{s}$ in $K(V)^G$.*

In particular: If there is a generic G-polynomial over K, there is an *irreducible* generic G-polynomial, since we can replace $P(\mathbf{s}, X)$ by an irreducible polynomial in $K(\mathbf{s})[X]$ with the same splitting field.

COROLLARY 1.1.6. *Let K be an infinite field and G a finite group, and let $(P_i(\mathbf{s}_i, X))_{i\in I}$ be a family of G-polynomials over rational function fields $K(\mathbf{s}_i)$, such that every G-extension of fields containing K is obtained by specialising some $P_j(\mathbf{s}_j, X)$. Then one of the $P_i(\mathbf{s}_i, X)$'s is generic.*

Hence, the obvious 'loosening' of the definition of generic polynomials — allowing a family of cases rather than a single case — does not lead to anything new.

Another consequence is the following result from [K&Mt, Thm. 3]:

PROPOSITION 1.1.7. *Let K be an infinite field and G a finite group. Consider a faithful linear action of G on the K-vector space V, and assume that M/K is a subextension of $K(V)/K$ on which G acts faithfully. If the fixed field M^G is rational over K with generating transcendence basis $s_1, \ldots, s_r$, there is a generic G-polynomial over K with parameters $s_1, \ldots, s_r$.*

It is also clear from the Proposition that a construction of G-extensions over K is generic, if it only makes use of properties of K that are inherited by extension fields in which K is relatively algebraically closed, such as the degree of cyclotomic extensions.

REMARK. In [DM], DeMeyer uses a seemingly stronger concept of generic polynomial than the one we are using: He demands that it produce not only all G-extensions, but also all H-extensions for subgroups H of G. Call such a polynomial 'descent-generic'.

Since our Proposition above did not include anything about the Galois group of $F(\mathbf{s}, X)$ over $K(\mathbf{s})$, and since a specialisation giving $K(V)$ over $K(V)^G$ also gives $K(V)$ over $K(V)^H$ for any $H \subseteq G$, we now have

PROPOSITION 1.1.8. (KEMPER, [Ke2]) *Over an infinite field, a generic polynomial is 'descent-generic'.*

Returning now to the Linear Noether Problem, we note a few simple results from invariant theory, that will prove helpful later on. First of all, we record

THE INVARIANT BASIS LEMMA. *Let M/K be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(M/K)$, and let W be a finite-dimensional M-vector space on which G acts* semi-linearly*, i.e., such that $\sigma(a\mathbf{w}) = \sigma a\, \sigma\mathbf{w}$ for $a \in M$ and $\mathbf{w} \in W$. Then W has an* invariant basis*, i.e., an M-basis of vectors in the K-subspace W^G of G-invariant elements.*

Clearly, any K-basis for W^G is then an M-basis for W.

PROOF. We follow the argument given in [K&M]: If $(\theta_1, \ldots, \theta_s)$ is a basis for M over K, then $\sum_\sigma \sigma\theta_i\, \sigma\mathbf{w} \in W^G$ for i and all $\mathbf{w}$. Proposition 4.3.6 in

Chapter 4 below (or [Ja1, 4.14]) now gives us that the elements of W^G generate W over M. □

The next result follows from the Invariant Basis Lemma.

THE NO-NAME LEMMA. *Let G be a finite group acting faithfully on a finite-dimensional K-vector space V, and let U be a faithful $K[G]$-submodule of V. Then the extension $K(V)^G/K(U)^G$ is rational.*

PROOF. Inside $K(V)$, we have the $K(U)$-vector space $K(U) \cdot V$ generated by V. It is easily seen that $\dim_{K(U)} W = \dim_K V - \dim_K U + 1$, and since the G-action is semi-linear, there is — by the Invariant Basis Lemma — an invariant basis $1, w_1, \ldots, w_s$. Since s is the transcendence degree of $K(V)/K(U)$, we get that $w_1, \ldots, w_s$ are algebraically independent over $K(U)$ and that $K(V) = K(U)(w_1, \ldots, w_s)$, from which we get $K(V)^G = K(U)^G(w_1, \ldots, w_s)$. □

In particular: If G is a transitive subgroup of order n in S_m, we can consider G as acting on both $V = K^n$ and $U = K^m$ by permuting coordinates. Also, we can embed U into V as a $K[G]$-module. (PROOF: In G, we have a subgroup H of index m corresponding to the embedding $G \subseteq S_m$, and G permutes the canonical basis vectors in U in the same way it permutes the cosets σH in G. To each basis vector in U, we now associate the sum over the corresponding coset of canonical basis vectors in V.) It follows that $K(V)^G/K$ is rational if $K(U)^G/K$ is.

EXAMPLE. Let S_n act transitively on $n! = n \cdot (n-1) \cdots 2 \cdot 1$ indeterminates $\mathbf{t} = (t_1, \ldots, t_{n!})$. Then $K(\mathbf{t})^{S_n}/K$ is rational.

Finally, let us make the following observation, taken from [Ke1, Prop. 1.1(a)]: Let $G \hookrightarrow \mathrm{GL}_K(V)$ for a finite-dimensional K-vector space V, and consider the subfield $K(V)_0$ of homogeneous elements of degree 0. (A *homogeneous element* in $K(V)$ is an element of the form f/g, where $f, g \in K[V]$ are homogeneous. The *degree* is then defined as $\deg f - \deg g$.) Then G acts on $K(V)_0$ through the projective linear group $\mathrm{PGL}_K(V)$. In fact, $K(V)_0 = K(v_2/v_1, \ldots, v_n/v_1)$, when $v_1, \ldots, v_n$ is a K-basis for V, and the action of $\mathrm{GL}_K(V)$ on $K(V)$ becomes an action of $\mathrm{PGL}_K(V)$ on $K(V)_0$. Moreover, we have $K(V)^G = K(V)_0^G(x)$, when $x \in K(V)^G \setminus (0)$ is homogeneous of minimal positive degree: There *are* non-zero homogeneous elements in $K(V)^G$ of positive degree, since G acts on the homogeneous components of the elements in $K[V]$, meaning that $K[V]^G$, and hence $K(V)^G$, is in fact generated by homogeneous elements. (Since any element in $K(V)$ can be written as f/g for some $f \in K[V]$ and some $g \in K[V]^G$.) Now, let x be non-zero homogeneous of minimal positive degree $d > 0$, and let $f \in K(V)^G$ be homogeneous of degree e. We may write $e = qd + r$ for $0 \leq r < d$, getting f/x^q homogeneous of degree r. By assumption, we must then have $r = 0$ and $f/x^q \in K(V)_0^G$, and therefore $f \in K(V)_0^G(x)$.

When we start with a two-dimensional representation, this 'homogenisation' brings us down to transcendence degree 1, where everything is rational by Lüroth (Theorem 0.3.1 in the Introduction). For convenience, we prove Lüroth's Theorem in the special form we need:

LÜROTH'S THEOREM (SPECIAL CASE). *Let K be a field and $G \subseteq \mathrm{PGL}_2(K)$ a finite group of order n acting on $K(X)$. Let*

$$Y^n + r_{n-1}Y^{n-1} + \cdots + r_0 = \prod_{\sigma \in G}(Y - \sigma X) \in K(X)^G[Y].$$

Then there is an $i \in \{0, \ldots, n-1\}$ with $r_i \notin K$, and for any such i, we have $K(X)^G = K(r_i)$.

PROOF. Obviously, $r_i \notin K$ for some $i \in \{0, \ldots, n-1\}$. Since r_i is a polynomial of degree $\leq n$ in $(\sigma X)_{\sigma \in G}$, we can write it as $r_i = f_i/g_i$, where $f_i, g_i \in K[X]$ have degrees $\leq n$. It follows that $[K(X) : K(r_i)] \leq n$, and since $K(r_i) \subseteq K(X)^G$ and $[K(X) : K(X)^G] = n$, we must have $K(X)^G = K(r_i)$. □

REMARK. Thus, if $G \hookrightarrow \mathrm{GL}_2(K)$ the fixed field $K(x, y)^G$ is rational over K, and we have an explicit procedure for finding a generating transcendence basis.

In this connection, we can also note two additional simple facts, cf. [Ke1, Prop. 1.3]: The kernel of G's action on $K(V)_0$ is the subgroup $G \cap K^*$ of scalar matrices in G, and the degree d above equals the order of $G \cap K^*$. (The first part follows trivially by considering the action on v_i/v_1 and using the unique factorisation in $K[V]$. As for the second: By Galois theory, $K(V)_0(x) = K(V)^{G \cap K^*}$, and by [Ja2, Thm. 8.38] we have $[K(V) : K(V)_0(x)] = d$ since $x/v_1^d \in K(V)_0$.)

1.2. Resolvent Polynomials

Let $f(X)$ be an irreducible polynomial over K of degree $n \geq 1$ and let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in its splitting field M over K. The symmetric group S_n acts (as always) on $K[x_1, \ldots, x_n]$ by permuting the indeterminates x_i. For an element $P \in K[x_1, \ldots, x_n]$, let $P^{S_n} = \{P_1, P_2, \ldots, P_\ell\}$ be the orbit of P under the action of S_n.

DEFINITION 1.2.1. The *resolvent* polynomial is defined by

$$R(P, f)(X) = \prod_{i=1}^{\ell}(X - P_i(\alpha_1, \ldots, \alpha_n)).$$

Since the coefficients of $R(P, f)(X)$ are symmetric polynomials in the α_i's, the resolvent is defined over K.

EXAMPLE. If $P = c_1x_1 + c_2x_2 + \cdots + c_kx_k$, where $c_1, c_2, \ldots, c_k \in K$ and $k \leq n$, we call $R(P, f)(X)$ a *linear resolvent* polynomial. If there is no possibility of misunderstanding (i.e., if $f(X)$ is implicitly meant), we will often denote this resolvent by $P_N(X)$, where $N = \binom{n}{k}$ is its degree. Thus, for instance,

$$P_{n(n-1)/2}(X) = R(x_1 + x_2, f)(X) = \prod_{1 \leq i < j \leq n}(X - (\alpha_i + \alpha_j)).$$

LEMMA 1.2.2. *Let p be a prime, and let $f(X)$ be an irreducible polynomial of degree p over a field K of characteristic 0. Also, let $P = b_1x_1 + b_2x_2 + \cdots + b_px_p$ with $b_i \in \mathbb{Q}$. Then $R(P, f)(X)$ always has distinct roots.*

Furthermore, if $R(P, f)(X)$ has an irreducible factor of degree p over K, then its splitting field over K is the same as that of $f(X)$.

PROOF. The first part is a consequence of the following

SUBLEMMA. *Let $\sigma \in \mathrm{Gal}(f/K)$ have order p, and let $\alpha_1 = \alpha$, $\alpha_2 = \sigma\alpha$, ..., $\alpha_p = \sigma^{p-1}\alpha$ be the roots of $f(X)$. If, for $c_1, \dots, c_p \in K$, we have $c_1\alpha_1 + \cdots + c_p\alpha_p \in K$, then the polynomial*

$$g(X) = c_1 + c_2X + \cdots + c_pX^{p-1}$$

has a root that is a primitive p^{th} root of unity.[3]

PROOF OF SUBLEMMA. Let $L = K(\alpha)$ and $M = K(\alpha_1, \dots, \alpha_p)$. Consider the map

$$\varphi = c_1 1 + c_2\sigma + \cdots + c_p\sigma^{p-1} \colon L \to M.$$

If $c_1 + \cdots + c_p = 0$, we replace each c_i by $c_i + 1$.

Now, by assumption, $\varphi(\alpha) \in K$. Moreover, since $\varphi(K) = K$, we can find $a \in K$ with $\varphi(\alpha) = \varphi(a)$, and hence $\beta = \alpha - a \in \ker\varphi \setminus 0$.

Next, we replace K, L and M by the p^{th} cyclotomic fields $K' = K(\mu_p)$, $L' = L(\mu_p)$ and $M' = M(\mu_p)$. Letting $P = \langle\sigma\rangle$ be a p-Sylow subgroup in $\mathrm{Gal}(M'/K')$, we then consider the fixed field $F = M'^P$ instead of K, and the single field M' instead of L and M. We still have a linear map $\varphi_F \colon M' \to M'$, and since $\varphi_F(\beta) = 0$, we have $\ker\varphi_F \neq 0$.

Clearly, M'/F is a C_p-extension, and so $M' = F(\sqrt[p]{b})$ for some $b \in F$. Also, $\sigma(\sqrt[p]{b}) = \zeta \cdot \sqrt[p]{b}$ for a primitive p^{th} root of unity ζ. In the basis

$$(1, \sqrt[p]{b}, \dots, (\sqrt[p]{b})^{p-1}),$$

φ_F is given by the diagonal matrix

$$\begin{pmatrix} g(1) & & & & \\ & g(\zeta) & & & \\ & & g(\zeta^2) & & \\ & & & \ddots & \\ & & & & g(\zeta^{p-1}) \end{pmatrix},$$

and since it is not injective, we must have $g(\xi) = 0$ for some primitive p^{th} root of unity ξ.

Switching back, if necessary, to the original c_i's, we will of course still have $g(\xi) = 0$. Q.E.D.

To prove the first part of Lemma 1.2.2, we proceed as follows: If $R(P, f)(X)$ has a multiple root, it means that $c_1\alpha_1 + \cdots + c_p\alpha_p = 0$ for some choice of the $c_i \in \mathbb{Q}$ with $c_1 + \cdots + c_p = 0$ and not all c_i's equal to 0. In particular, the c_i's are not all equal. Thus, by the Sublemma, the polynomial $c_1 + c_2X + \cdots + c_pX^{p-1} \in \mathbb{Q}[X]$ must have a non-trivial common divisor with $X^{p-1} + \cdots + X + 1$. This, however, is only possible if all the c_i's *are* equal.

As for the second part: If $q(X)$ is an irreducible factor of $R(P, f)(X)$ of degree p, the splitting field M of $f(X)$ over K obviously contains the splitting

[3]The Sublemma is true for any field K of characteristic $\neq p$. By implication, Lemma 1.2.2 is true for any field of characteristic $\ell > 0$, provided that $\ell \neq p$ and the p^{th} cyclotomic extension of $\mathbb{F}_\ell$ has degree $p - 1$.

field M' of $q(x)$ over K. By [Hu, II.§1 Sätze 1.3 & 1.5] the group $\mathrm{Gal}(M/M')$ is trivial, since its order is not divisible by p. (Sketch of proof: The orbits in $\{\alpha_1, \ldots, \alpha_p\}$ under $N = \mathrm{Gal}(M/M')$ are permuted transitively by $G = \mathrm{Gal}(M/\mathbb{Q})$. Hence, p equals the number of orbits times the number of elements in an orbit. If $N \neq 1$, there is more than one element in an orbit, and so N acts transitively on $\{\alpha_1, \ldots, \alpha_p\}$, contradicting $p \nmid |N|$.) Thus, $M' = M$. □

REMARKS. (1) The lemma is no longer true if p is replaced by a composite number, as $X^4 - 2$ shows. Similarly, it may fail if the coefficients a_i are not in $\mathbb{Q}$: If ζ is a primitive third root of unity, the linear resolvent

$$R(x_1 - \zeta x_2, X^3 - a)(X) = X^6 - 3(2\zeta + 1)aX^3$$

has 0 as a triple root.

(2) The linear resolvents $R(x_1 + \cdots + x_k, f)(X)$ and $R(x_1 + \cdots + x_{p-k}, f)(X)$, $1 \leq k \leq p-1$, are just transformations of each other, and so we will generally look only at the case $k \leq (p-1)/2$.

PROPOSITION 1.2.3. (SOICHER & MCKAY) *Let $f(X) \in K[X]$ be an irreducible and separable polynomial over K of degree $n \geq 2$. Let $P = c_1x_1 + c_2x_2$ with c_1, c_2 distinct non-zero elements in K such that $R(P, f)(X)$ has distinct roots. Then $\mathrm{Gal}(f/K)$ has order n if and only if $R(P, f)(X)$ factors into a product of irreducible polynomials of degree n over K.*

This result is taken from [S&M], and the proof is elementary.

Following Williamson ([Wil], quoting Soicher's thesis), we now describe a practical way of computing resolvent polynomials: For polynomials $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ and $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$, the *Sylvester resultant* is defined as the $(m+n) \times (m+n)$ determinant

$$\mathrm{Res}(f,g) = \begin{vmatrix}
1 & a_{m-1} & a_{m-2} & \ldots & a_0 & & & \\
 & 1 & a_{m-1} & a_{m-2} & \ldots & a_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & 1 & a_{m-1} & a_{m-2} & \ldots & a_0 \\
1 & b_{n-1} & \ldots & b_1 & b_0 & & & \\
 & 1 & b_{n-1} & \ldots & b_1 & b_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & 1 & b_{n-1} & \ldots & b_1 & b_0
\end{vmatrix},$$

cf. [Syl]. It is then well-known and fairly elementary, as shown for instance in [Ja1, Thm. 5.7], that $\mathrm{Res}(f,g) = 0$ if and only if $f(X)$ and $g(X)$ have a common root, from which it is easy to deduce that

$$\mathrm{Res}(f,g) = \prod_{i,j}(\alpha_i - \beta_j),$$

where $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are the roots of $f(X)$ and $g(X)$, respectively. (Sketch of proof: Considering the α's and β's as indeterminates, we obviously

have that the right side divides the left, and that the quotient introduces no additional roots. Since they have the same constant term considered as polynomials in the α's, the quotient has constant term 1, and so must be equal to 1.)

Now, if c_1, c_2 are distinct non-zero elements, as in Proposition 1.2.3 above, we get

$$R(c_1x_1 + c_2x_2, f)(X) = \frac{\operatorname{Res}((-c_2)^n f((X-Y)/c_2), c_1^n f(Y/c_1))}{(c_1+c_2)^n f(X/(c_1+c_2))},$$

where the resultant is taken with respect to a new indeterminate Y, and the denominator is understood to be X^n when $c_1 = -c_2$. On the other hand, for $c_1 = c_2 = 1$ we get instead

$$\operatorname{Res}((-1)^n f(X-Y), f(Y)) = 2^n f(X/2) R(x_1 + x_2, f)(X)^2.$$

These methods generalise to linear resolvents with respect to other first-degree polynomials. In this way resolvent polynomials can be computed efficiently.

Remarks. (1) If the purpose of computing $R(c_1x_1 + c_2x_2, f)(X)$ is to study the action of $\mathrm{Gal}(f/K)$ on ordered pairs of roots, the simplest choice of c_1 and c_2 is $c_1 = 1$ and $c_2 = t$ an indeterminate, i.e., to work over $K(t)$. This generalises to ordered tuples in the obvious way.

(2) From the well-known formula

$$d(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i)$$

for the discriminant of a polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with roots $\alpha_1, \ldots, \alpha_n$, it is easily seen that

$$d(f) = (-1)^{n(n-1)/2} n^n \operatorname{Res}(f, f'/n).$$

In particular, for a trinomial $f(X) = X^n + aX + b$, we get

$$d(f) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}a^n + n^n b^{n-1}\big).$$

Exercises

Exercise 1.1. Let

$$f(X) = X^n + t_{n-1}X^{n-1} + \cdots + t_1X + t_0$$

be the 'general' n^{th}-degree polynomial (that is, $t_0, \ldots, t_{n-1}$ are indeterminates). Prove that $d(f)$ is an irreducible polynomial in the t's.

Exercise 1.2. Prove that the resultant of two monic polynomials $f(X)$ and $g(X)$ in $K[X]$ is zero, if and only if $f(X)$ and $g(X)$ have a common root.

Exercise 1.3. Let $f(X)$, $g(X)$ and $h(X)$ be monic polynomials over the same field. Prove that

$$\operatorname{Res}(fg, h) = \operatorname{Res}(f, h) \operatorname{Res}(g, h).$$

Exercise 1.4. Let $f(X)$ and $g(X)$ be monic polynomials over the same field. Prove that

$$d(fg) = \operatorname{Res}(f, g)^2 d(f) d(g).$$

EXERCISE 1.5. (1) Let $n > m > 0$ with $\gcd(m, n) = 1$. Find a formula for the discriminant of $X^n + aX^m + b$. [Hint: Formula on p. 80.]

(2) Let $f(X)$ be a monic polynomial, and let $g(X) = f(X^n)$ for some n. Express $d(g)$ in terms of $f(0)$ and $d(f)$.

EXERCISE 1.6. Let the (m, n)-resultant of two polynomials

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0$$

and

$$g(X) = a_n X^n + b_{n-1} X^{n-1} + \cdots + b_0$$

be given as the $(m + n) \times (m + n)$ determinant

$$\mathrm{Res}_{(m,n)}(f, g) = \begin{vmatrix} a_m & a_{m-1} & a_{m-2} & \dots & a_0 & & & & \\ & a_m & a_{m-1} & a_{m-2} & \dots & a_0 & & & \\ & & \ddots & & & & \ddots & & \\ & & & a_m & a_{m-1} & a_{m-2} & \dots & a_0 & \\ b_n & b_{n-1} & \dots & b_1 & b_0 & & & & \\ & b_n & b_{n-1} & \dots & b_1 & b_0 & & & \\ & & \ddots & & & & \ddots & & \\ & & & b_n & b_{n-1} & \dots & b_1 & b_0 & \end{vmatrix}.$$

What does $\mathrm{Res}_{(m,n)}(f, g)$ look like if $a_m, b_n \neq 0$? If one of a_m and b_n is zero? If both are?

(3) Consider a polynomial

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 \in K[X],$$

as well as the associated 'binary form'

$$F_m(X, Y) = a_m X^m + a_{m-1} X^{m-1} Y + \cdots + a_1 X Y^{m-1} + a_0 Y^m$$

in two indeterminates X and Y. (Note that $F_m(X, Y)$ depends on both $f(X)$ and m, since m need not be the actual degree of $f(X)$.) Prove that the non-trivial zeroes in K^2 for $F_m(X, Y)$ (i.e., zeroes other than $(0, 0)$) lie on lines through the origin (so-called 'projective points'). Prove that the ordinary zeroes α of $f(X)$ correspond to projective zeroes through $(\alpha, 1)$. Prove that $F_m(X, Y)$ may have *one* additional projective zero, namely the line through $(1, 0)$ ('infinity'). Finally, prove that $\mathrm{Res}_{(m,n)}(f, g) = 0$ if and only if the corresponding forms $F_m(X, Y)$ and $G_n(X, Y)$ have a common projective zero. (We refer to Appendix B for more on binary forms and projetive zeroes.)