Generic Polynomials

Constructive Aspects of the Inverse Galois Problem

Christian U. Jensen
Arne Ledet
Noriko Yui

MATHEMATICAL SCIENCES
RESEARCH INSTITUTE
PUBLICATIONS

45

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

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

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.

Contents

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 $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ 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.

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