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.)

CHAPTER 2

Groups of Small Degree

In this chapter, we will look at 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 an irreducible and separable polynomial over K. Then the Galois group $\mathrm{Gal}(f/K)$ is a transitive subgroup of S_n, determined up to conjugation. Obviously, there are only finitely many possibilities. How do we recognise the Galois group among them?

Here, the first step (at least in characteristic $\neq 2$) is to look at the discriminant $d(f)$ of $f(X)$, since we know that $\mathrm{Gal}(f/K)$ is contained in A_n if and only if $d(f)$ is a square in K. Beyond that, it becomes convenient to introduce various so-called *resolvent polynomials* associated to $f(X)$.

We will concentrate on polynomials of small degree, i.e., $n \leq 11$, and will give comprehensive results only for $n = 3$, 4, 5, 7 and 11 over $\mathbb{Q}$.

REMARK. For the groups of degree 7 and 11, the above is *all* we will be doing in this chapter. That is, we will be giving criteria for recognising polynomials with a specified Galois group. The results for groups of degree 7 and 11 are largely taken from [BJ&Y]. Generic polynomials are only known for a few of these groups, i.e., the symmetric groups (for all n), cyclic groups (for odd n, as well as for $n \leq 6$) and dihedral groups (for odd n, as well as for $n \leq 8$). Here, the symmetric group is trivial, while the cyclic and dihedral groups will be covered later, in Chapter 5 below.

For groups of degree 3 and 4, we will consider generic polynomials as well as the Noether Problem, which in these cases is fairly easy to solve.

For groups of degree 5, we will not look at the Noether Problem, although it is known to have an affirmative answer for all groups concerned, by results of Furtwängler [Fu] for the solvable groups, and Maeda [Mae] for the alternating group A_5.

We note that all groups of degree ≤ 15 are known to occur as Galois groups over $\mathbb{Q}$ (and in fact for regular extensions of $\mathbb{Q}(t)$), cf. [M&M2] and [Kl&M]. Also, in the context of algebraic number fields, we refer to [Cn1, §6.3], which covers polynomials of degree ≤ 7, including degree 6.

Historically, we point out that generic polynomials over $\mathbb{Q}$ for groups of degree 3 and 4 (except the symmetric groups themselves) are given by Seidelmann in [Sei].[1] However, from our point of view, Seidelmann's polynomials are unnecessarily complicated, as they are intended to express more generally what a polynomial with the given Galois group looks like.

[1] Without proof, citing the authors Dissertation (Erlangen 1916).

2.1. Groups of Degree 3

Let $f(X) = X^3 + a_2X^2 + a_1X + a_0 \in K[X]$, where K has characteristic $\neq 2$. Then the discriminant of $f(X)$ is given by

$$d(f) = a_1^2a_2^2 - 4a_1^3 - 4a_0a_2^2 - 27a_0^2 + 18a_0a_1a_2.$$

THEOREM 2.1.1. *Suppose that f is irreducible over K. Then*

$$\mathrm{Gal}(f/\mathbb{Q}) \simeq \begin{cases} S_3, & \text{if } d(f) \notin (K^*)^2 \\ C_3, & \text{if } d(f) \in (K^*)^2. \end{cases}$$

EXAMPLE. A generic polynomial for S_3 is

$$f(X) = X^3 + tX + t \in K(t)[X].$$

A generic polynomial for $C_3 = A_3$ is

$$f(X) = X^3 - tX^2 + (t-3)X + 1 \in K(t)[X],$$

cf. [Se2, 1.1]. Both of these polynomials work in characteristic 2 as well.

PROOF. It is not hard to see directly that every Galois extension with Galois group of degree 3 (over an arbitrary field) is the splitting field of a polynomial of the form $X^3 + aX + a$. (Sketch of proof: Let M/K be a C_3- or S_3-extension, and let L/K be a subextension of degree 3. M will be the splitting field of the minimal polynomial of any element $\theta \in L \setminus K$. We now pick θ to have a minimal polynomial of the form $X^3 + aX + b$, $a, b \neq 0$, and scale θ to get $a = b$.) Thus, $X^3 + tX + t$ is generic for S_3.

Next, look at $K(s)$, s an indeterminate, and let $t = (-s^3 + 3s - 1)/(s - s^2)$. Then s is a root of $X^3 - tX^2 + (t-3)X + 1$, and the conjugates are $1/(1-s)$ and $1 - 1/s$. Hence, $K(s)/K(t)$ is Galois with group C_3. In particular, $X^3 - tX^2 + (t-3)X + 1$ is irreducible with square discriminant.

Now, let L/K be a C_3-extension. The matrix $\mathbf{B} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ has order 3 in the general linear group $\mathrm{GL}_2(K)$, and so, by Proposition 1.1.1 in Chapter 1, there exists x and y in L, linearly independent over K, such that $\sigma x = -y$ and $\sigma y = x - y$. Let $z = x/y$. Then $z \notin K$, i.e., $L = K(z)$. Also, $\sigma z = 1/(1-z)$. Since $z \neq 0, 1$, we can specialise t above to $(-z^3 + 3z - 1)/(z - z^2)$. □

EXAMPLE. Let K be a field of characteristic $\neq 3$, and let $C_3 = \langle\sigma\rangle$ act on $U = K^2$ by $\sigma(a, b) = (-b, a - b)$. This translates to $\sigma\colon s \mapsto t$, $t \mapsto -s - t$ on $K(U) = K(s, t)$, and it is easily seen that $K(s, t)^{C_3} = K(u, v)$ for

$$u = \frac{s^2 + t^2 + st}{st(s + t)} \quad \text{and} \quad v = \frac{s^3 - 3st^2 - t^3}{st(s + t)}.$$

So, $K(s, t)^{C_3}/K$ is rational, and since U can be embedded into $V = K^3$ (with permutation action), the Noether Problem has an affirmative answer for C_3 as well: Let σ permute x, y and z cyclically, and $s = x - y$, $t = y - z$. Then we get

that

$$K(x,y,z)^{C_3} = K\big(\frac{(x-y)^2+(y-z)^2+(x-y)(y-z)}{(x-y)(y-z)(x-z)},\\ \frac{(x-y)^3-3(x-y)(y-z)^2-(y-z)^3}{(x-y)(y-z)(x-z)},\\ x+y+z\big).$$

(The third generator can be replaced by $x/(x-y)+y/(y-z)+z/(z-x)$ if $\operatorname{char} K = 3$.)

EXAMPLE. For future reference, we record the following consequence of the above example: Notice that the generators we have found for $K(x,y,z)^{C_3}$ are homogeneous of degrees -1, 0 and 1. If we call them X, Y and Z for convenience, we thus have $K(x,y,z)^{C_3} = K(X,Y,Z) = K(XZ,Y)(Z)$, from which it follows that $K(x,y,z)_0^{C_3} = K(XZ,Y)$: '$\supseteq$' is obvious, and since $K(x,y,z)^{C_3}$ is rational over both fields of transcendence degree 1, we get equality. (Cf. also [Ke1, Prop. 1.1(b) + proof].)

Now, $K(x,y,z)_0 = K(s,t)$, where $s = x/y$ and $t = y/z$, and on this field σ acts by $s \mapsto t$, $t \mapsto 1/st$.

Thus, we can conclude the following: Let σ be the automorphism on the rational function field $K(s,t)$ given by $\sigma\colon s \mapsto t$, $t \mapsto 1/st$. Then σ has order 3, and the fixed field $K(s,t)^{C_3}$ is rational over K. More precisely,

$$K(s,t)^{C_3} = K\Big(\frac{s^3t^3-3st^2+t^3+1}{t(s-1)(t-1)(st-1)},\\ \frac{s^3t^3-3s^2t^3+6st^2-3st+t^3-3t^2+1}{t(s-1)(t-1)(st-1)}\Big).$$

This is an example in support of the General Noether Problem.

The Noether Problem for S_3 is of course trivial.

2.2. Groups of Degree 4

Let $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in K[X]$ be irreducible, where (once again) K is a field of characteristic $\neq 2$. In this case, the discriminant $d(f)$ of $f(X)$ cannot alone determine the structure of the Galois group of $f(X)$ over K.

The transitive subgroups of S_4 are V_4 (the Klein Vierergruppe), C_4, D_4 (the dihedral group of degree 4, i.e., the symmetry group of a square, cf. also Definition 5.5.1 in Chapter 7 below), A_4 and S_4.

DEFINITION 2.2.1. Let $\alpha_1, \dots, \alpha_4$ be the roots of f in M. The *cubic resolvent* of $f(X)$ is the polynomial

$$g(Y) = [Y - (\alpha_1\alpha_2 + \alpha_3\alpha_4)]\,[Y - (\alpha_1\alpha_3 + \alpha_2\alpha_4)]\,[Y - (\alpha_1\alpha_4 + \alpha_2\alpha_3)].$$

Clearly, $g(Y) \in K[Y]$, and it is easy to compute that

$$g(Y) = Y^3 - a_2Y^2 + (a_1a_3 - 4a_0)Y - (a_0a_3^2 - 4a_0a_2 + a_1^2).$$

Also, as $d(g) = d(f)$, it is clear that $g(Y)$ has no multiple roots.

THEOREM 2.2.2. *With $g(Y)$ as in Definition 2.2.1, let L denote the splitting field of $g(Y)$ over K, and set $m = [L:K]$. Then m equals 1, 2, 3 or 6, and we have*

$$\mathrm{Gal}(f/K) \simeq \begin{cases} S_4, & \text{if } m = 6 \\ A_4, & \text{if } m = 3 \\ V_4, & \text{if } m = 1 \\ D_4 \text{ or } C_4, & \text{if } m = 2. \end{cases}$$

PROOF. It is clear that $m \mid 3!$, and that $L \subseteq M$.

If $3 \mid m$, we get the result from $d(g) = d(f)$ and $m \mid [M:K]$.

If there is a 4-cycle in $\mathrm{Gal}(f/K)$, two of the roots of $g(Y)$ are interchanged by it, and so $m > 1$.

Finally, if $\mathrm{Gal}(f/K) = V_4$, the roots of $g(Y)$ are all in K, and so $m = 1$. □

When $m = 2$, we need a criterion to distinguish D_4 from C_4, and rely on the following 'folklore' result:

THEOREM 2.2.3. *Suppose $m = 2$. Then $g(Y)$ is reducible over K and factors as $g(Y) = (Y - r)(Y^2 + sY + t) \in K[Y]$ where $Y^2 + sY + t$ is irreducible over K. Put $L = K(\sqrt{s^2 - 4t})$. Then $\mathrm{Gal}(f/K) \simeq C_4$ if and only if $X^2 - rX + a_0$ and $X^2 + a_1X + (a_2 - r)$ both have roots in L.*

PROOF. We may take $r = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in K$. Then

$$X^2 - rX + a_0 = (X - \alpha_1\alpha_2)(X - \alpha_3\alpha_4)$$

and

$$X^2 + a_3X + a_2 - r = (X - (\alpha_1 + \alpha_2))(X - (\alpha_3 + \alpha_4)).$$

If $\mathrm{Gal}(f/K) \simeq C_4$, then L is the unique quadratic subfield of M. So the roots of the above quadratic equations must belong to L.

Conversely, suppose that the two quadratic equations have roots in L. To show that $\mathrm{Gal}(f/K) \simeq C_4$, it suffices to prove that $[M:K] \leq 4$. First note that $M = L(\alpha_1, \alpha_2)$. Moreover, since $\alpha_1 + \alpha_2 \in L$ and $\alpha_1\alpha_2 \in L$, we have $[L(\alpha_1, \alpha_2):L] \leq 2$. Since $m = [L:K] = 2$, it follows that $[M:K] \leq 4$. □

COROLLARY 2.2.4. *Let $f(X) = X^4 + aX^2 + b \in K[X]$, and assume that $f(X)$ is irreducible over K. Then the following assertions hold:*

(a) *If $b \in (K^*)^2$, then $\mathrm{Gal}(f/K) \simeq V_4$.*
(b) *If $b \notin (K^*)^2$, but $b(a^2 - 4b) \in (K^*)^2$, then $\mathrm{Gal}(f/K) \simeq C_4$.*
(c) *If $b \notin (K^*)^2$ and $b(a^2 - 4b) \notin (K^*)^2$, then $\mathrm{Gal}(f/K) \simeq D_4$.*

PROOF. The cubic resolvent of f takes the following simple form

$$g(Y) = Y^3 - aY^2 - 4bY + 4ab = (Y - a)(Y^2 - 4b).$$

Let $m = [L:K]$ and apply Theorem 2.2.2. If $b \in (K^*)^2$, then $m = 1$ and $\mathrm{Gal}(f/K) \simeq V_4$. If $b \notin (K^*)^2$, then $m = 2$. Consider the polynomials $X^2 - aX + b$ and X^2 from Theorem 2.2.3. Then $\mathrm{Gal}(f/K) \simeq C_4$ if and only if $(-a \pm \sqrt{a^2 - 4b})/2 \in K(\sqrt{4b}) = K(\sqrt{b})$ if and only if $\sqrt{a^2 - 4b} \in K(\sqrt{b})$ if and only if $b(a^2 - 4b) \in (K^*)^2$, since $a^2 - 4b$ is not a square in K. □

Note that any V_4-, C_4- or D_4-extension in characteristic $\neq 2$ *is* obtained as the splitting field of a polynomial of the form $X^4 + aX^2 + b$.

EXAMPLE. Let p and q be two distinct primes such that $p > 3$ and $p^2 - 4q > 0$. Let $f(X) = X^4 - pX^2 + q \in \mathbb{Q}[X]$. Then f is irreducible over $\mathbb{Q}$. Moreover, f has four real roots and its Galois group $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to D_4.

And now to consider the groups one by one:

The Klein Vierergruppe. There is of course very little to say about V_4: If K is a field of characteristic $\neq 2$, there is an obvious two-dimensional representation, from which we get the linear Noether extension $K(x, y)/K(x^2, y^2)$. We leave it to the reader to solve the Noether Problem for the regular representation, and simply note that the above gives a generic polynomial $(X^2 - s)(X^2 - t)$ in parameters s and t.[2]

The cyclic group. We start by giving a *construction* of extensions with Galois group C_4:

THEOREM 2.2.5. *Let $K(\sqrt{a})/K$ be a quadratic extension. Then $K(\sqrt{a})/K$ can be embedded in a C_4-extension if and only if a is a sum of two squares in K, if and only if a is a norm in $K(\sqrt{a})/K$. Furthermore, if $a = x^2 + y^2$ for $x, y \in K$, all the C_4-extensions containing $K(\sqrt{a})/K$ are of the form*

$$K(\sqrt{r(a + x\sqrt{a})})/K, \quad r \in K^*,$$

and if $a = \alpha^2 - a\beta^2$ for $\alpha, \beta \in K$, the C_4-extensions containing $K(\sqrt{a})/K$ are

$$K(\sqrt{r(\alpha + \beta\sqrt{a})})/K, \quad r \in K^*.$$

PROOF. It is clear that a is a sum of two squares in K if and only if a is a norm in $K(\sqrt{a})/K$, if and only if -1 is a norm in $K(\sqrt{a})/K$.

Now, let M/K be a C_4-extension containing $\sqrt{a}$, and let σ generate $C_4 = \mathrm{Gal}(M/K)$. Then $M = K(\sqrt{a}, \sqrt{\omega})$ for some $\omega \in K(\sqrt{a})$, and by Kummer Theory we have $\sigma\sqrt{\omega}/\sqrt{\omega} = z \in K(\sqrt{a})^*$. Then $z\,\sigma z = \sigma^2\sqrt{\omega}/\sqrt{\omega} = -1$, i.e., z has norm -1 in $K(\sqrt{a})/K$.

Conversely, if $z \in K(\sqrt{a})$ has norm -1 over K, by Hilbert 90 we can find $\omega \in K(\sqrt{a})^*$ such that $\sigma\omega/\omega = z^2$, where σ generates $\mathrm{Gal}(K(\sqrt{a})/K)$. This ω cannot be a square in $K(\sqrt{a})$, and so $M/K = K(\sqrt{a}, \sqrt{\omega})/K$ is an extension of degree 4. The conjugates of $\sqrt{\omega}$ over K are $\pm\sqrt{\omega}$ and $\pm z\sqrt{\omega}$, and so M/K is a Galois extension. We extend σ by $\sigma\sqrt{\omega} = z\sqrt{\omega}$ to get an element of order 4, i.e., M/K is a C_4-extension.

In the two cases above, we can let

$$z = \frac{a - x\sqrt{a}}{y\sqrt{a}}, \text{ resp. } z = \frac{\alpha - \beta\sqrt{a}}{\sqrt{a}},$$

and Lemma A.1.1 from Appendix A gives the rest. □

[2] This polynomial is not, of course, irreducible. See Exercise 2.4(1) for an irreducible generic V_4-polynomial.

EXAMPLE. The field $\mathbb{Q}(\sqrt{5})$ can be embedded into a C_4-extension of $\mathbb{Q}$, e.g., $\mathbb{Q}(\sqrt{5+\sqrt{5}})/\mathbb{Q}$; however, $\mathbb{Q}(\sqrt{3})$ cannot be.

COROLLARY 2.2.6. *The polynomial*

$$f(s,t,X) = X^4 - 2s(1+t^2)X^2 + s^2t^2(1+t^2) \in K(s,t)[X]$$

is generic for C_4-extensions over K. Specifically, C_4-extensions are obtained by specialisations such that $s \neq 0$ and $1+t^2$ is not a square.

PROOF. If $a = p^2+q^2 \in K^* \setminus (K^*)^2$, we can replace a by a/p^2 to get $a = 1+t^2$ for a suitable t. $f(r,t,X)$ is the minimal polynomial for $\sqrt{r(a+\sqrt{a})}$ over K in this case. □

EXAMPLE. Let K be a field of characteristic $\neq 2$, and let $C_4 = \langle\sigma\rangle$ act on $U = K^2$ by $\sigma(a,b) = (-b,a)$. This translates to $\sigma\colon s \mapsto t$, $t \mapsto -s$ on $K(U) = K(s,t)$, and it is easily seen that $K(s,t)^{C_4} = K(u,v)$ for

$$u = \frac{s^2-t^2}{st} \quad \text{and} \quad v = s^2+t^2.$$

Thus, $K(s,t)^{C_4}/K$ is rational. Since U can be embedded into $V = K^4$ (equipped with the permutation action of C_4), we conclude that the Noether Problem has a positive answer for C_4.

In fact, we have: Let x, y, z and w be indeterminates over K, and let σ act by

$$\sigma\colon x \mapsto y, \quad y \mapsto z, \quad z \mapsto w, \quad w \mapsto x.$$

With $s = x-z$ and $t = y-w$ we have the representation above, and

$$K(x,y,z,w) = K\big(s,t,x+y+z+w, s^2(x+z)+t^2(y+w)\big).$$

Consequently,

$$\begin{aligned} K(x,y,z,w)^{C_4} &= K((s^2-t^2)/st, s^2+t^2, x+y+z+w, \\ &\qquad\qquad s^2(x+z)+t^2(y+w)) \\ &= K\big(\frac{(x-z)^2-(y-w)^2}{(x-z)(y-w)}, \\ &\qquad x+y+z+w, (x-z)^2+(y-w)^2, \\ &\qquad\quad (x-z)^2(x+z)+(y-w)^2(y+w)\big). \end{aligned}$$

REMARK. As in the Example on p. 31, the fact that the generators (call them X, Y, Z and W) for $K(x,y,z,w)^{C_4}$ found above are homogeneous (of degrees 0, 1, 2 and 3, respectively) implies that

$$K(x,y,z,w)_0^{C_4} = K(X, Z/Y^2, W/Y^3).$$

Thus, on the rational function field $K(s,t,u)$ (where $s = x/y$, $t = y/z$ and $u = z/w$) we have an automorphism σ of order 4 given by

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

and the fixed field $K(s,t,u)^{C_4}$ is rational over K.

The dihedral group. In considering the dihedral group D_4, we use the following representation:

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau \rangle.$$

THEOREM 2.2.7. *Let M/K be a V_4-extension, i.e., for some $a, b \in K^*$ we have $M = K(\sqrt{a}, \sqrt{b})$. Then M/K can be embedded in a D_4-extension F/K such that $F/K(\sqrt{b})$ is cyclic, if and only if ab is a norm in $K(\sqrt{a})/K$. Furthermore, if $ab = \alpha^2 - a\beta^2$ for $\alpha, \beta \in K$, all the D_4-extensions in question are of the form*

$$K(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b})/K, \quad r \in K^*.$$

PROOF. The fixed field of τ inside F is of course a quadratic extension of $K(\sqrt{a})$, and so has the form $K(\sqrt{a}, \sqrt{\omega})$ for some $\omega \in K(\sqrt{a})^*$. Then $F = K(\sqrt{a}, \sqrt{\omega}, \sqrt{b})$, and by Kummer Theory $\sigma\sqrt{\omega} = x\sqrt{\omega}$ for some $x \in K(\sqrt{a}, \sqrt{b})$. Clearly, $x\,\sigma x = -1$, and since $\tau\sigma = \sigma^3\tau$ we get $\tau x = -x$. Letting $z = x\sqrt{a}\sqrt{b}$, we then have $z \in K(\sqrt{a})$ and $z\,\sigma z = ab$. Hence, ab is a norm in $K(\sqrt{a})/K$.

Conversely, if $z \in K(\sqrt{a})$ has norm ab over K, we can find $\omega \in K(\sqrt{a})^*$ with $\sigma\omega/\omega = z^2/ab$ by Hilbert 90, and it is easily seen that $K(\sqrt{\omega}, \sqrt{a}, \sqrt{b})/K$ is then a D_4-extension as desired. If $z = \alpha - \beta\sqrt{a}$, we can let $\omega = \alpha + \beta\sqrt{a}$. Lemma A.1.1 (from Appendix A) gives the rest. □

EXAMPLE. If a and -1 are quadratically independent in K^*,[3] the extension $K(\sqrt[4]{a}, i)/K$, $i = \sqrt{-1}$, is a D_4-extension.

COROLLARY 2.2.8. *The polynomial*

$$g(s, t, X) = X^4 - 2stX^2 + s^2t(t-1) \in K(s, t)[X]$$

is generic for D_4-extensions over K. Specifically, D_4-extensions are obtained by specialisations such that $s \neq 0$ and t and $t - 1$ are quadratically independent.

PROOF. Let a and b be quadratically independent and $ab = \alpha^2 - a\beta^2$. If $\alpha \neq 0$, we replace a and b by $a(\alpha/\beta)^2$ and b/β^2 to get $a = b + 1$. If $\alpha = 0$, we write $a = x^2 - y^2$ for $x, y \in K^*$ and replace a and b by $1 - (y/x)^2$ and $-(y/x)^2$, again getting $a = b + 1$. We can then let $\alpha = a$ and $\beta = 1$. $g(r, a, X)$ is the minimal polynomial for $\sqrt{r(\alpha + \beta\sqrt{a})}$ over K in this case. □

EXAMPLE. Let K be a field of characteristic $\neq 2$. Then D_4 has a two-dimensional representation that translates to $K(s, t)$ as

$$\sigma\colon s \mapsto t, \quad t \mapsto -s,$$
$$\tau\colon s \mapsto t, \quad t \mapsto s.$$

The minimal polynomial of s over $K(s, t)^{D_4}$ is then $X^4 - (s^2 + t^2)X^2 + s^2t^2$, and from Corollary 2.2.4 we get that $K(s, t)^{D_4} = K(s^2 + t^2, s^2t^2)$.

[3] See the end of section A.1 in Appendix A for the meaning of 'quadratically independent'.

For D_4 as a subgroup of S_4, we let it act on $K(x,y,z,w)$ by

$$\sigma\colon x\mapsto y,\quad y\mapsto z,\quad z\mapsto w,\quad w\mapsto x,$$
$$\tau\colon x\mapsto y,\quad y\mapsto x,\quad z\mapsto w,\quad w\mapsto z.$$

As with C_4, we can then let $s=x-z$ and $t=y-w$, getting

$$K(x,y,z,w)=K\big(s,t,x+y+z+w,s^2(x+z)+t^2(y+w)\big),$$

and thus

$$\begin{aligned}K(x,y,z,w)^{D_4}&=K(s^2+t^2,s^2t^2,x+y+z+w,\\&\qquad\qquad s^2(x+z)+t^2(y+w))\\&=K\big(x+y+z+w,(x-z)^2+(y-w)^2,\\&\qquad(x-z)^2(x+z)+(y-w)^2(y+w),\\&\qquad\qquad(x-z)^2(y-w)^2\big).\end{aligned}$$

Remark. Theorems 2.2.5 and 2.2.7, as well as their corollaries, emphasise the similarity between C_4- and D_4-extensions indicated in Theorem 2.2.2. This similarity will be exploited in section 6.4 of Chapter 6 below.

The alternating group. Of the groups of degree 4, the alternating group is the most complicated:

Let K be a field in characteristic not 2 or 3. We solve the Noether Problem and find (for infinite K) a generic polynomial by proceeding in several steps:

(1) There is a linear action of A_4 on K^3, obtained by considering S_4 as the rotation group of the cube.[4] If we write

$$A_4=\langle\sigma,\rho_1,\rho_2\mid\sigma^3=\rho_1^2=1,\ \sigma\rho_1\sigma^{-1}=\rho_2,\ \sigma\rho_2\sigma^{-1}=\rho_1\rho_2=\rho_2\rho_1\rangle,$$

this gives us an A_4-action on $K(x,y,z)$ given by

$$\sigma\colon x\mapsto y,\qquad y\mapsto z,\qquad z\mapsto x,$$
$$\rho_1\colon x\mapsto -x,\quad y\mapsto -y,\quad z\mapsto z.$$

Also, the $K[A_4]$-module K^3 then sits inside K^4 (with permutation action), and so we have $K(x,y,z)/K(x,y,z)^{A_4}$ sitting inside $K(\mathbf{t})/K(\mathbf{t})^{A_4}$ for $\mathbf{t}=(t_1,t_2,t_3,t_4)$, with $K(\mathbf{t})^{A_4}/K(x,y,z)^{A_4}$ rational of transcendence degree 1. (Generated by $t_1+t_2+t_3+t_4$, in fact.)

(2) Stepping down to the homogeneous degree-0 part $K(x,y,z)_0=K(s,t)$, $s=x/y$, $t=y/z$, we have

$$\sigma\colon s\mapsto t,\quad t\mapsto 1/st,\quad\text{and}\quad\rho_1\colon s\mapsto s,\quad t\mapsto -t.$$

(Also, $K(x,y,z)^{A_4}/K(s,t)^{A_4}$ is rational of transcendence degree 1, generated by $xyz/(x^2+y^2+z^2)$.) Clearly, $K(s,t)^{V_4}=K(s^2,t^2)$, and so we are left with the extension $K(s^2,t^2)/K(s^2,t^2)^{C_3}$ for $C_3=\langle\sigma\rangle$.

(3) Letting $u=s^2$ and $v=t^2$, we now ask: If $C_3=\langle\sigma\rangle$ acts on $K(u,v)$ by

$$\sigma\colon u\mapsto v,\quad v\mapsto 1/uv,$$

[4]This may only make sense geometrically over fields like $\mathbb{Q}$ and $\mathbb{R}$, but the action is there in any case.

is $K(u,v)^{C_3}/K$ rational? From the Example on p. 31 we know that the answer is 'yes', and that in fact

$$K(u,v)^{C_3} = K\Bigg(\frac{u^3v^3-3uv^2+v^3+1}{v(u-1)(v-1)(uv-1)}, \\ \frac{u^3v^3-3u^2v^3+6uv^2-3uv+v^3-3v^2+1}{v(u-1)(v-1)(uv-1)}\Bigg).$$

(4) All in all: $K(s,t)/K(s,t)^{A_4}$ is an extension of rational function fields, sitting inside the Noether Extension. Thus, the Noether Problem has a positive answer for A_4, and if K is infinite, there *is* a generic A_4-polynomial in two parameters over K.

(5) By Proposition 1.1.5 from Chapter 1, we can now find a generic polynomial for A_4 over K by expressing the minimal polynomial for, say, $s+t+1/st$ over $K(s,t)^{A_4}$ in terms of the generators found above. Denoting these generators by α and β, resp., we thus get the following result:

THEOREM 2.2.9. *Let K be a field of characteristic not 2 or 3. Then the polynomial*

$$F(\alpha,\beta,X) = X^4 - \frac{6A}{B}X^2 - 8X + \frac{9A^2-12(\alpha^3-\beta^3+27)B}{B^2}$$

in $K(\alpha,\beta)[X]$, where

$$A = \alpha^3-\beta^3-9\beta^2-27\beta-54,$$
$$B = \alpha^3-3\alpha\beta^2+2\beta^3-9\alpha\beta+9\beta^2-27\alpha+27\beta+27,$$

is generic for A_4 over K.

EXAMPLE. Let $K=\mathbb{Q}$ and $\alpha=\beta=0$. Then we get the polynomial

$$X^4+12X^2-8X+24,$$

and it is easily seen that this is an A_4-polynomial over $\mathbb{Q}$.

REMARK. Regarding step (5) in the Example above: Suppose that u and v in $K(x,y)$ are algebraically independent over K, where K is a field, and that $f \in K(x,y)$ is known (somehow) to lie in $K(u,v)$. How can we find a rational function $g \in K(X,Y)$ with $f = g(u,v)$?

Write $u = u_1/u_2$, $v = v_1/v_2$ and $f = f_1/f_2$ as quotients of polynomials in $K[x,y]$, and consider g as a quotient of two polynomials g_1 and g_2 with coefficients to be determined. For practical purposes, we set an upper limit d to the degree, separately in X and Y, of terms in g_1 and g_2. Now, we want to have

$$f = \frac{f_1}{f_2} = \frac{g_1(u,v)}{g_2(u,v)} = \frac{u_2^d v_2^d g_1(u,v)}{u_2^d v_2^d g_2(u,v)},$$

i.e.,

$$G(x,y) = f_1\, u_2^d v_2^d g_2(u,v) - f_2\, u_2^d v_2^d g_1(u,v) = 0.$$

Here, $G(x,y)$ is a polynomial with coefficients that are linear combinations of the coefficients of g_1 and g_2. Thus, the form of g_1 and g_2 can be determined by linear algebra. (And if there is only the zero solution, we must increase d and try again. Since our assumption is that g exists, it will eventually be found.)

This procedure can be efficiently implemented on a computer. The coefficients of $F(\alpha, \beta, X)$ in the Example were found using MAPLE.

There are of course other ways to solve the Noether Problem. Hashimoto has described to us a method for producing explicit rational generators for

$$\mathbb{Q}(x_1, \ldots, x_n)^{A_n}/\mathbb{Q}$$

for $n = 3, 4$, complete with formulas for the generators in terms of the elementary symmetric symbols and the discriminant, and vice verse. At present, it is unclear whether this method generalises to higher n.

Also, a solution to the Noether Problem for A_3 and A_4 over any field is given in [Hj].

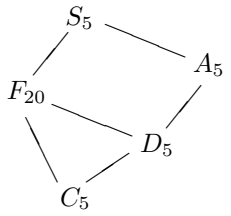
The symmetric group. The Noether Problem for S_4 is trivial, and it is easy to see that $X^4 + sX^2 + tX + t$ is generic.

REMARK. We have now seen that the groups C_4, D_4, V_4, A_4 and S_4 can be parametrised as Galois groups over $\mathbb{Q}$ using only two parameters. As we shall see later, in Chapter 8, this is optimal: None of these groups have generic polynomials with only one parameter. (Of course, C_4 requires only one parameter over $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. The other groups, however, demand two parameters over *any* field in characteristic 0.)

2.3. Groups of Degree 5

Let $f(X) \in K[X]$ be a an irreducible quintic polynomial with discriminant $d(f)$ over a field K of characteristic $\neq 2$. Let M denote a splitting field of f over K.

The transitive subgroups of S_5 are (up to conjugation) C_5, D_5 (the dihedral group of degree 5, i.e., the symmetries of a regular pentagon), F_{20} (the Frobenius group of order 20, i.e., the affine maps on $\mathbb{F}_5$, cf. also Chapter 7 below), A_5 and S_5. The inclusions are



meaning that C_5, D_5 and A_5 correspond to square discriminant, and F_{20} and S_5 to non-square discriminant. The groups C_5, D_5 and F_{20} are solvable groups, while A_5 is simple.

The groups of degree 5 have the following permutation representations: Let

$$\rho = (234), \quad \sigma = (12345) \quad \text{and} \quad \omega = (2354).$$

Then

$$A_5 = \langle \sigma, \rho, \omega^2 \rangle, \quad F_{20} = \langle \sigma, \omega \rangle, \quad D_5 = \langle \sigma, \omega^2 \rangle \quad \text{and} \quad C_5 = \langle \sigma \rangle.$$

REMARK. The quintic polynomials have a long history, going back at least to Leibniz and Tschirnhaus. The latter introduced what is now called Tschirnhaus transformations, cf. Chapter 6 (on p. 141) below, for the purpose of reducing general quintic polynomials to simpler polynomials, hoping thereby to find radical expressions for the roots similar to those known for cubic and quartic polynomials (although Leibniz already had expressed scepticism about the success of this method).

In 1706, De Moivre found a family of quintic polynomials, namely $f(x) = x^5 + 10px^3 + 20p^2x + q$, that could be solved by radicals. (Indeed,

$$\sqrt[5]{-q/2 + \sqrt{q^2/4 + 32p^2}} + \sqrt[5]{-q/2 - \sqrt{q^2/4 + 32p^2}}$$

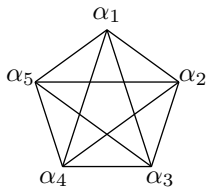
is a root, and for all rational values of p and q the Galois group of $f(x)$ over $\mathbb{Q}$ is F_{20} unless $f(x)$ is reducible.)

The next important step was made by Malfatti, who in 1771 published a paper (*De aequationibus quadrato-cubicis disquisitio analytica*) where he reduced the solvability of a quintic polynomial to the solvability of a sextic 'resolvant' imitating the construction of a cubic resolvent of a quartic polynomial. In essence his polynomial was a disguised version of what is now sometimes known as the Weber resolvent, cf. below. Malfatti was discouraged by the fact that his resolvent polynomial had a higher degree than the quintic he started from. But he showed that if the resolvent sextic had a rational root, then the original quintic polynomial could be solved by radicals. From a modern point of view he actually decided when the Galois group of the quintic is solvable, i.e., the roots can be expressed by radicals.

Malfatti's results were forgotten for nearly seventy years and apparently not known to Abel and Galois. Related resolvents were obtained in the nineteenth century by Jacobi, Cayley, Harley and Cockle.[5]

Even when it is known that a quintic is solvable by radicals it is a highly nontrivial task to find the radical expressions of roots explicitly. The first systematic treatment of this problem can be found in McClintock's 1884 paper [McC]. To some extent this paper has had the same fate as Malfatti's paper: It has been almost forgotten until this day.

The Weber resolvent. Let $f(X) = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in K[X]$, and let $\alpha_1, \ldots, \alpha_5$ be its roots in M, indexed to correspond with the permutation representation of $\mathrm{Gal}(f/K)$ implied above. Identify them with the vertices of a pentagon



[5]Meaning that what we will call the Weber resolvent may with equal justification be called the Cayley resolvent, or maybe the Cayley-Weber resolvent.

and let

$$u_1 := v_1 - v_2$$

where

$$v_1 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1$$

and

$$v_2 = \alpha_1\alpha_3 + \alpha_3\alpha_5 + \alpha_5\alpha_2 + \alpha_2\alpha_4 + \alpha_4\alpha_1.$$

Geometrically, v_1 (resp. v_2) corresponds to the sum of the sides of the pentagon $\alpha_1\alpha_2\cdots\alpha_5$ (resp. the sum of the sides of the associated pentagram). Then v_1 and v_2 are fixed under D_5. Also,

$$\omega u_1 = \omega v_1 - \omega v_2 = v_2 - v_1 = -u_1$$

so that u_1^2 is fixed under F_{20}. Now, we note that the cosets A_5/D_5 (and S_5/F_{20}) are represented by the elements

$$\{(1), (123), (132), (125), (152), (134)\},$$

and let

$$u_2 = (123)u_1,\ u_3 = (132)u_1,\ u_4 = (125)u_1,\ u_5 = (152)u_1,\ u_6 = (134)u_1.$$

Then $u_1, \ldots, u_6$ are permuted by A_5, and σ acts transitively on the elements $u_2, \ldots, u_6$. Also, ω maps $u_1, \ldots, u_6$ to $-u_1, \ldots, -u_6$, meaning that S_5 acts on $u_1^2, \ldots, u_6^2$.

We let $g(Y) = \prod_{i=1}^{6}(Y - u_i)$.

PROPOSITION 2.3.1. *With $g(Y)$ as above, we may write*

$$g(Y) = Y^6 + b_4Y^4 + b_2Y^2 + b_0 - 32\Delta Y \in K(\Delta)[Y]$$

where b_{2i}, $i = 0, 1, 2$, is a symmetric polynomial of degree $4(6-i)$ in the α_i's, and $\Delta = \prod_{1\le i<j\le 5}(\alpha_i - \alpha_j) = \sqrt{d(f)}$.

PROOF. Observe that Δ is invariant under A_5. We may write

$$g(Y) = Y^6 + b_5Y^5 + b_4Y^4 + b_3Y^3 + b_2Y^2 + b_1Y + b_0 \in K(\Delta)(Y).$$

Note that

$$\omega g(Y) = g(-Y) = Y^6 - b_5Y^5 + b_4Y^4 - b_3Y^3 + b_2Y^2 - b_1Y + b_0.$$

Now for $\tau \in A_5$, $\tau g(Y) = g(Y)$, and hence $\omega\tau g(Y) = g(-Y)$. Therefore, b_{2i}, $i = 0, 1, 2$ are symmetric polynomials in the α_i's, and b_{2i+1}, $i = 0, 1, 2$ are skew-symmetric polynomials in the α_i's. Consequently, $b_{2i+1} = B_{2i+1}\,\Delta$ where the B_{2i+1}'s are symmetric polynomials in the α_i's for $i = 0, 1, 2$. As u_i is homogeneous of degree 2 in the α_i's, it follows that b_j have degree $2(6-j)$ in the α_i's. But Δ is homogeneous of degree 10. Accordingly, $B_5 = B_3 = 0$ and B_1 is some constant, in fact, -32. So we have $g(Y) = Y^6 + b_4Y^4 + b_2Y^2 + b_0 - 32\Delta Y$. □

REMARK. Actually calculating b_0, b_2 and b_4 is a job for a computer, and the result is

$$\begin{aligned}
b_0 = &-64a_2^4 - 176a_3^2a_1^2 + 28a_3^4a_1 - 16a_4^2a_3^2a_2^2 - 1600a_4^2a_0^2 - 64a_4a_2a_1^2 \\
&- 80a_3^2a_2a_0 + 384a_4^3a_1a_0 + 640a_4a_2^2a_0 - 192a_4^2a_3a_2a_0 \\
&- 1600a_2a_1a_0 - 128a_4^2a_2^2a_1 + 48a_4a_3^3a_0 - 640a_4a_3a_1a_0 \\
&+ 64a_4^3a_3a_2a_1 + 64a_4a_3a_2^3 + 224a_4^2a_3a_1^2 + 224a_3a_2^2a_1 \\
&+ 8a_4a_3^4a_2 - 112a_4a_3^2a_2a_1 - 16a_4^2a_3^3a_1 - 16a_3^3a_2^2 - 64a_4^4a_1^2 \\
&+ 4000a_3a_0^2 - a_3^6 + 320a_1^3, \\
b_2 = &\ 3a_3^4 - 16a_4a_3^2a_2 + 16a_4^2a_2^2 + 16a_4^2a_3a_1 - 64a_4^3a_0 + 16a_3a_2^2 \\
&- 8a_3^2a_1 - 112a_4a_2a_1 + 240a_4a_3a_0 + 240a_1^2 - 400a_2a_0, \\
b_4 = &-3a_3^2 + 8a_4a_2 - 20a_1.
\end{aligned}$$

DEFINITION 2.3.2. Let $f(X) \in K[X]$ be monic, irreducible and quintic, and let $g(Y) = Y^6 + b_4Y^4 + b_2Y^2 + b_0 - 32\Delta Y$ be as above. The *Weber sextic resolvent* is then the polynomial

$$G(Z) = (Z^3 + b_4Z^2 + b_2Z + b_0)^2 - 2^{10}\, d(f)\, Z \in K[Z].$$

Clearly, the roots of $G(Z)$ are $u_1^2, \ldots, u_6^2$.

We can now characterise quintic polynomials with solvable Galois group:

THEOREM 2.3.3. *$\mathrm{Gal}(f/K)$ is solvable if and only if the Weber sextic resolvent $G(Z)$ of f has a root in K.*

PROOF. If $\mathrm{Gal}(f/K)$ is solvable, we have $\mathrm{Gal}(f/K) \subseteq F_{20}$, and hence (say) $u_1^2 \in K$.

Conversely, assume that $G(Z)$ has a root in K. If $\mathrm{Gal}(f/K)$ is *not* solvable, all the u_i^2's are conjugate, and hence equal. Therefore, we can write

$$G(Z) = (Z - t)^6 = (Z^3 - 3tZ^2 + 3t^2Z - t^3)^2,$$

where $u^2 = t$. Comparing this with the above expression for $G(Z)$, we get

$$(Z^3 + b_4Z^2 + b_2Z + b_0)^2 - (Z^3 - 3tZ^2 + 3t^2Z - t^3)^2 = 2^{10}d(f)Z.$$

Comparing coefficients on both sides, we get

$$b_4 = -3t, \quad b_2 = 3t^2, \quad b_0 = -t^3 \quad \text{and} \quad d(f) = 0,$$

contradicting the separability of $f(X)$. □

Using the discriminant and the Weber sextic resolvent, we can now distinguish between the possible Galois groups of an irreducible quintic, with the exception of C_5 and D_5.

In characteristic 0, a criterion was given by Williamson [Wil] (cf. also [J&Y82], where it is done without invoking resolvents) to tell the cyclic group C_p and the dihedral group

$$D_p = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \tau\sigma = \sigma^{p-1}\tau \rangle$$

apart, when p is an odd prime $\equiv 1 \pmod 4$.

In this case, both C_p and D_p are subgroups of A_p, and so cannot be distinguished by the discriminant. However, by Proposition 1.2.3 in Chapter 1, the resolvent $R(x_1 - x_2, f)(X)$ factors into irreducible polynomials of degree p if and only if $\mathrm{Gal}(f/K) \simeq C_p$. Moreover, if $\mathrm{Gal}(f/K) \simeq D_p$, the irreducible factors of $R(x_1 - x_2, f)(X)$ have degree $2p$, and the quadratic subextension of the splitting field is then $K(\sqrt{-d})/K$, where d is the constant term of any such irreducible factor.[6]

We will now briefly consider the special case of trinomials of *Bring-Jerrard* form $f(X) = X^5 + aX + b$ over the rational numbers. Such polynomials always have at least one pair of complex (i.e., non-real) roots, meaning that C_5 cannot occur as Galois group in this case. (Also, if there are only two complex roots, the Galois group is S_5.)

First, we note that the Weber sextic resolvent in this case is

$$G(Z) = (Z^3 - 20aZ^2 + 240a^2Z + 320a^3)^2 - 2^{10}(4^4a^5 + 5^5b^4)Z,$$

giving us

$$H(Z) = 2^{-12}G(4Z) = (Z - a)^4(Z^2 - 6aZ + 25a^2) - 5^5b^4Z.$$

If $f(X)$ is irreducible over $\mathbb{Q}$, we can of course distinguish between the four possible Galois groups by looking at $H(Z)$ and the discriminant $d(f) = 4^4a^5 + 5^5b^4$.

A parametrised description of quintic trinomials with solvable Galois group is then given as follows:

THEOREM 2.3.4. (WEBER) *Let $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ be irreducible. If $a = 0$, then $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{20}$. Otherwise, $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_5$ (resp. F_{20}) if and only if*

(i) *$d(f) \in (\mathbb{Q}^*)^2$ (resp. $\notin (\mathbb{Q}^*)^2$) and*
(ii) *a and b has the form*

$$a = \frac{5^5\lambda\mu^4}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)}, \quad b = a\mu,$$

for some $\lambda, \mu \in \mathbb{Q}$ with $\lambda \neq 1$ and $\mu \neq 0$.

PROOF. The statement for $a = 0$ is clear. Thus, assume $a \neq 0$. Let r be a rational root of $H(Z)$ and write $r = a\lambda$, $b = a\mu$. Then

$$H(r) = a^6(\lambda - 1)^4(\lambda^2 - 6\lambda + 25) - 5^5a^5\lambda\mu^4 = 0,$$

from which we derive condition (ii). □

REMARK. It is an easy consequence of Ikeda's Theorem (section 5.4 of Chapter 5 below) that there are D_5- and F_{20}-extensions of $\mathbb{Q}$ contained in $\mathbb{R}$. (Since

[6] As far as the quadratic subextension goes, this is the best we can do: Since the p-cycles generate A_p, there is no rational function in p indeterminates expressing $\sqrt{-d}$ independently of the ordering of the roots.

there are C_2- and C_4-extensions contained in $\mathbb{R}$.) Thus, the trinomials above do not give us all D_5- or F_{20}-extensions of $\mathbb{Q}$.

EXAMPLE. Let

$$f(X) = X^5 + \frac{5^5 t}{(t-1)^4(t^2-6t+25)}(X+1) \in \mathbb{Q}(t)[X].$$

Then $\mathrm{Gal}(f/\mathbb{Q}(t)) \simeq F_{20}$.

As in the case of groups of degree 4, we will now proceed to treat the groups one at a time. However, as stated in the beginning of the chapter, we will not consider the Noether Problem, but simply construct generic polynomials.

The cyclic group. In the case of the cyclic group, we restrict ourselves to the case of characteristic 0, i.e., to producing a generic C_5-polynomial over $\mathbb{Q}$. The more general case of characteristic $\neq 5$ is treated in Chapter 5.

Consider first a C_5-extension $M/\mathbb{Q}$, and let σ denote a generator for $C_5 = \mathrm{Gal}(M/\mathbb{Q})$. Let ζ be a primitive fifth root of unity. Clearly, then, $M(\mu_5)/\mathbb{Q}(\mu_5)$ is a C_5-extension, and $M(\mu_5)/\mathbb{Q}$ is a $C_5 \times C_4$-extension generated by $\sigma \in \mathrm{Gal}(M(\mu_5)/\mathbb{Q}(\mu_5))$ and $\kappa \in \mathrm{Gal}(M(\mu_5)/M)$, the latter given by $\kappa\zeta = \zeta^2$. By Kummer theory, we have $M(\mu_5) = \mathbb{Q}(\mu_5, \sqrt[5]{\alpha})$ for an $\alpha \in \mathbb{Q}(\mu_5)^*$, and we may assume $\sigma(\sqrt[5]{\alpha}) = \zeta \cdot \sqrt[5]{\alpha}$.

Now, since $\sigma\kappa = \kappa\sigma$, we get $\kappa(\sqrt[5]{\alpha}) = x(\sqrt[5]{\alpha})^2$ for some $x \in \mathbb{Q}(\mu_5)^*$, and since $\kappa^4 = 1$, we get

$$\sqrt[5]{\alpha} = \kappa^4(\sqrt[5]{\alpha}) = x^8\kappa x^4\kappa^2 x^2\kappa^3 x(\sqrt[5]{\alpha})^{16},$$

i.e.,

$$\alpha^{-3} = x^8\kappa x^4\kappa^2 x^2\kappa^3 x(\sqrt[5]{\alpha})^{16}.$$

Thus, we see that we have $M(\mu_5) = \mathbb{Q}(\mu_5, \sqrt[5]{\beta})$ for a β of the form

$$\beta = \frac{\kappa^2 x^2 \kappa^3 x}{x^2 \kappa x}, \quad x \in \mathbb{Q}(\mu_5)^*.$$

On the other hand: If we take a β of this form (and assume it not to be a fifth power), we can extend κ from $\mathbb{Q}(\mu_5)$ to $M(\mu_5) = \mathbb{Q}(\mu_5, \sqrt[5]{\beta})$ by $\kappa(\sqrt[5]{\beta}) = x/\kappa^2 x(\sqrt[5]{\beta})^2$ and define σ by $\sigma(\sqrt[5]{\beta}) = \zeta \cdot \sqrt[5]{\beta}$ to get a $C_5 \times C_4$-extension $M(\mu_5)/\mathbb{Q}$.

A primitive element for the C_5-subextension $M/\mathbb{Q} = M^{C_4}/\mathbb{Q}$ is then $\theta = \sum_{i=0}^{3} \kappa^i(\sqrt[5]{\beta})$, since this element is obviously in M, but not in $\mathbb{Q}(\mu_5)$.

Finally, since β is a function of $\kappa^2 x/x$, it is unchanged if we modify x by a factor from $\mathbb{Q}(\zeta + 1/\zeta)$, and it changes it sign if we multiply x by $\zeta - 1/\zeta$. In either case, $M(\mu_5)$ is unchanged, since -1 is a fifth power. Thus, we may assume x to be of the form

$$x = y_1 + y_2(\zeta + 1/\zeta) + (\zeta - 1/\zeta) = s + 2\zeta + t\zeta^2 + t\zeta^3,$$

where $s = y_1 - y_2 + 1$ and $t = -y_2 + 1$. Calculation now gives us that the minimal polynomial for θ over $\mathbb{Q}$ is

$$f(s,t,X) = X^5 - 10X^3 + 20\big(\frac{5(s^2+t^2-2s-2t+4)}{T} - 1\big)X^2 + 5\big(\frac{40(s^2+t^2-2s-2t+2)}{T} - 3\big)X + 4S/T^2,$$

with

$$\begin{aligned} S &= 200s(2s^2 + s^2t - 6s + 3st^2 + 3t^3 - 6t^2 + 4) + 200(s+t)^3 \\ &\quad - 100(s+t)^4 + 20T + 25T(s^2+t^2-2s-2t) - T^2 \quad \text{and} \\ T &= s^4 - 2s^3 - 2s^3t + 4s^2 + 8s^2t - s^2t^2 - 8s - 4st \\ &\quad - 4st^2 + 2st^3 + 16t^2 - 6t^3 + t^4 + 16. \end{aligned}$$

(Here, T is simply the norm of x.)

If we consider s and t as indeterminates, we see that this is a C_5-polynomial over $\mathbb{Q}(s,t)$, *and* that it is a generic C_5-polynomial, by the remarks in section 1.1 of Chapter 1, since the only property of $\mathbb{Q}$ we made use of was the degree of the fifth cyclotomic field.

The dihedral group. As an abstract representation of D_5 we use

$$D_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = 1,\ \tau\sigma = \sigma^4\tau \rangle.$$

Let K be an arbitrary field, and define automorphisms σ and τ on the rational function field $K(u,v)$ by

$$\begin{aligned} \sigma\colon &\qquad u \mapsto v \mapsto \frac{1-v}{u}, \\ \tau\colon &\qquad u \mapsto v \mapsto u. \end{aligned}$$

It is then easy to see that $\sigma^5 = \tau^2 = 1$ and $\tau\sigma = \sigma^4\tau$, and hence that we have an action of D_5 on $K(u,v)$. In particular, we have an example of the General Noether Problem (GNP): Is the fixed field $K(u,v)^{D_5}$ rational over K?

To answer this, we note that the minimal polynomial for u over $K(u,v)^{D_5}$ is

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

where

$$s = u + v + \frac{1-v}{u} + \frac{u+v-1}{uv} + \frac{1-u}{v}$$

and

$$t = \frac{(1-u)(1-v)(1-u-v)}{uv}.$$

Thus, $K(s,t) \subseteq K(u,v)^{D_5}$ and $K(u,v)/K(s,t)$ is Galois with Galois group D_5 or F_{20}.

If $\operatorname{char} K \neq 2$, there is no problem: The discriminant of the polynomial is the square

$$t^2(4t^5 - 4t^4 - 24st^3 - 40t^3 - s^2t^2 + 34st^2 + 91t^2 + 30s^2t + 14st - 4t - s^2 + 4s^3)^2,$$

and so the Galois group for $K(u,v)/K(s,t)$ must be D_5.

If $\operatorname{char} K = 2$, we need only prove that

$$\operatorname{Gal}(\mathbb{F}_2(u,v)/\mathbb{F}_2(s,t)) \simeq D_5,$$

since we cannot get a larger Galois group over a larger ground field. To this end, we note that the canonical epimorphism $\mathbb{Z}[s,t] \twoheadrightarrow \mathbb{F}_2[s,t]$ extends to an epimorphism $\mathbb{Z}[s,t]_{(2)} \twoheadrightarrow \mathbb{F}_2(s,t)$, where $\mathbb{Z}[s,t]_{(2)}$ is the localisation in the prime ideal generated by 2. Using Proposition 3.3.2 from Chapter 3 below, we get that

$$\operatorname{Gal}(\mathbb{F}_2(u,v)/\mathbb{F}_2(s,t)) \hookrightarrow \operatorname{Gal}(\mathbb{Q}(u,v)/\mathbb{Q}(s,t)) \simeq D_5.$$

Thus, in either case, $K(u,v)^{D_5} = K(s,t)$.

The advantage of this particular D_5-action is that it is — in a sense — generic:

THEOREM 2.3.5. (BRUMER) *Let K be an arbitrary field. The polynomial*

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

in $K(s,t)[X]$ is then generic for D_5-extensions over K.

PROOF. We already know that the polynomial gives a D_5-extension of $K(s,t)$. All that is left to show is that any D_5-extension M/K can be obtained by specialising $f(s,t,X)$:

Let $L = M^{\langle\tau\rangle}$. For $x \in L \setminus K$, we look at

$$a = \frac{(\sigma^3 x - \sigma x)(x - \sigma^4 x)}{(\sigma^3 x - x)(\sigma x - \sigma^4 x)} \in M$$

and $b = \sigma a$. It is easy to see that the conjugates of a are b, $(1-b)/a$, $(a+b-1)/ab$ and $(1-a)/b$. Thus, a has degree 1 or 5 over K. If $a \in K$, we must have $a = b = (1-a)/a$, i.e., $a^2 + a - 1 = 0$. Otherwise, a and b generates M/K and behaves in the same way as u and v in the above Example, giving us our specialisation.

So, we need to show that x can be chosen in such a way that $a^2 + a - 1 \neq 0$: Consider a as a rational function in the conjugates of x, i.e., $a = F(x)$. Substituting x^2 for x, we have

$$A = F(x^2) = a\bar{a}, \quad \text{where} \quad \bar{a} = \frac{(\sigma^3 x + \sigma x)(x + \sigma^4 x)}{(\sigma^3 x + x)(\sigma x + \sigma^4 x)}.$$

We claim that $\bar{a} \neq 1$: If it were, the numerator and denominator would be equal, meaning that $(x - \sigma x)(\sigma^3 x - \sigma^4 x) = 0$, an obvious contradiction.

Now, looking at $F(x + cx^2)$ for $c \in K$, we see that it is a rational function

$$F(x + cx^2) = \frac{P + Qc + Rc^2}{P' + Q'c + R'c^2}$$

in c over M. Furthermore, $P/P' = a$ and $R/R' = A$. Since $a \neq A$, we conclude that $F(x + cx^2)$ is not constant, and since K is infinite (by virtue of having a D_5-extension) it assumes infinitely many values. Clearly then, we can choose x to avoid any finitely many values for a. □

REMARK. Using the result on p. 42, one can show that the quadratic subextension (in characteristic $\neq 2$) of the splitting field of the polynomial $f(s,t,X)$ is obtained by adjoining to $K(s,t)$ a square root of

$$-(4t^5-4t^4-24st^3-40t^3-s^2t^2+34st^2+91t^2 \\ +30s^2t+14st-4t-s^2+4s^3).$$

The Frobenius group. For F_{20}, it is possible to proceed in a manner similar to that for D_5:

THEOREM 2.3.6. (LECACHEUX, [Lc, Thm. 3.1]) *The polynomial*

$$g(s,t,X)=X^5+(td-2s-17/4)X^4+(3td+d+13s/2+1)X^3 \\ -(td+11s/2-8)X^2+(s-6)X+1\in K(s,t)[X],$$

where $d=s^2+4$, is generic for F_{20} over any field K of characteristic $\neq 2$.

PROOF. First we note that the Weber sextic resolvent of $g(s,t,X)$ has a root $d(6st+2s+4t+13)^2/4$ in $K(s,t)$, meaning that the Galois group is at most F_{20}. It only remains to prove that $g(s,t,X)$ is in fact parametric:

Let M/K be an F_{20}-extension, and let $x_1,\dots,x_5\in M\setminus K$ be conjugate elements permuted by F_{20} in accordance with our permutation representation.

Let

$$x=\frac{(x_2-x_5)(x_4-x_3)}{(x_2-x_4)(x_5-x_3)} \quad\text{and}\quad y=\sigma x.$$

Then

$$\sigma y=\frac{1-y}{x},\quad \omega x=\frac{x}{x-1} \quad\text{and}\quad \omega y=\frac{y-1}{x+y-1}.$$

Moreover, $\omega^2 x=x$, and so $u=(x-1)/x^2$ is ω-invariant.

The conjugates of u are

$$u=\frac{x-1}{x^2},\frac{y-1}{y^2},\frac{x(1-x-y)}{(y-1)^2},-\frac{xy(1-x)(1-y)}{(1-x-y)^2},\frac{y(1-x-y)}{(x-1)^2},$$

and ω permutes the last four transitively. Thus, if these conjugates are actually distinct, they generate M/K. If they are not distinct, we have $u^5=-1$, and as in the proof of Brumer's Theorem above, we can select the x_i's to avoid that.

Now we see, by direct calculation, that the minimal polynomial for u over K is exactly $g(a,b,X)$ for suitably chosen a and b. □

The alternating group. As with the cyclic group, we will only consider A_5-extensions in characteristic 0. The construction given below was communicated to us by Joe Buhler.

In the next section, we show that

$$f(s,t,X)=X^5+sX^3+tX+t\in\mathbb{Q}(s,t)[X]$$

is generic for S_5 over $\mathbb{Q}$. It follows from this that some specialisation of s and t in $\mathbb{Q}(x_1,\dots,x_5)^{A_5}$ will give us $\mathbb{Q}(x_1,\dots,x_5)/\mathbb{Q}(x_1,\dots,x_5)^{A_5}$ as splitting field. For our argument, it is necessary to know that s and t are then algebraically

independent over $\mathbb{Q}$. This follows from Corollary 8.1.3 in Chapter 8 below:[7] If they were algebraically dependent, the splitting field of $X^5 + sX^3 + tX + t$ inside $\mathbb{Q}(x_1, \ldots, x_5)$ would have transcendence degree 1 over $\mathbb{Q}$, and would so be rational by the Corollary. Consequently, we would have A_5 acting on a function field $\mathbb{Q}(u)$, and hence $A_5 \subseteq \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(u)) = \mathrm{PGL}_2(\mathbb{Q})$ (cf. [Ja2, 8.14]). But the projective general linear group $\mathrm{PGL}_2(\mathbb{Q})$ contains no elements of order 5.

Thus, to find a generic 2-parameter polynomial for A_5 over $\mathbb{Q}$, it suffices to demonstrate that $\mathbb{Q}(s, t, \Delta)/\mathbb{Q}$ is rational, where Δ is the different of f, i.e., the square root of the discriminant

$$d = (108s^5 + 16s^4t - 900s^3t - 128s^2t^2 + 2000st^2 + 3125t^2 + 256t^3)t^2.$$

To do this, we start by writing

$$\begin{aligned} 5^5 d &= 5^5 \Delta^2 \\ &= (5^5 t^2 + 1000st^2 - 450s^3t + 54s^5)^2 - 4(9s^2 - 20t)^3(s^2 - 5t)^2, \end{aligned}$$

or, with $u = t^2/s^5$ and $v = t/s^2$,

$$5^5\Delta^2 = [(5^5 u + 1000v^2 - 450v + 54)^2 - 4(9 - 20v)^3(1 - 5v)^2]s^{10}.$$

For convenience, we let

$$P = 1000v^2 - 450v + 54 \quad \text{and} \quad Q = (9 - 20v)(1 - 5v)$$

to get

$$5^5\Delta^2 = [(5^5 u + P)^2 - 4(9 - 20v)Q^2]s^{10},$$

and hence

$$5\Big(\frac{25\,\Delta}{s^5 Q}\Big)^2 = \Big(\frac{5^5 u + P}{Q}\Big)^2 - 4(9 - 20v).$$

Letting

$$A = \frac{25\,\Delta}{s^5 Q} \quad \text{and} \quad B = \frac{5^5 u + P}{Q},$$

we claim that $\mathbb{Q}(s, t, \Delta) = \mathbb{Q}(A, B)$: '$\supseteq$' is obvious. '$\subseteq$': Clearly, $v \in \mathbb{Q}(A, B)$, and hence so is u. But $v^2/u = s$ and $s^2 v = t$.

To actually get the generic polynomial, we only have to write out s and t as elements of $\mathbb{Q}(A, B)$, and following the above argument we get

THEOREM 2.3.7. *Let A and B be indeterminates, and let $C = 5A^2 - B^2 + 3$. With*

$$\begin{aligned} s &= \frac{125\,C^2}{4(BC^2 - 52BC + 576B - 10C^2 + 360C - 3456)}, \\ t &= \frac{3125\,C^5}{256(BC^2 - 52BC + 576B - 10C^2 + 360C - 3456)^2}, \end{aligned}$$

the polynomial $X^5 + sX^3 + tX + t \in \mathbb{Q}(A, B)[X]$ is then generic for A_5 over $\mathbb{Q}$.

[7] And we point out that the proof of the Roquette-Ohm result (Proposition 8.1.1) and its Corollary are self-contained relative to the rest of the text, and can easily be read at this point.

The symmetric group. As stated in the previous section, the polynomial $X^5 + sX^3 + tX + t$ is generic for S_5 over $\mathbb{Q}$. This result is essentially due to Hermite [He, 1861], who showed that every quintic equation $X^5+a_4X^4+a_3X^3+a_2X^2+a_1X+a_0 = 0$ can be transformed into one of the form

$$Z^5 + LZ^3 + M\Delta^2 Z + I\Delta^3 = 0,$$

where Δ is the different of the original equation and L, M and I are elements in the ground field. Scaling the indeterminate by Δ then ensures that all coefficients are in the ground field, and a further scaling makes the coefficients in degrees 0 and 1 equal (provided that $M \neq 0$, which is 'generically' the case, cf. below). The argument makes use of classical invariant theory, and we refer to Appendix B for the details.

PROPOSITION 2.3.8. *Let s and t be indeterminates. Then the polynomial $X^5 + sX^3 + tX + t \in \mathbb{Q}(s,t)[X]$ is generic for S_5 over $\mathbb{Q}$.*

PROOF. Let $\mathbf{e} = (e_1, \ldots, e_5)$ be the elementary symmetric symbols in the indeterminates $\mathbf{x} = (x_1, \ldots, x_5)$, i.e.,

$$e_1 = x_1 + \cdots + x_5, \ \ldots, \ e_5 = x_1 \cdots x_5,$$

and consider the Noether extension $\mathbb{Q}(x_1, \ldots, x_5)/\mathbb{Q}(e_1, \ldots, e_5)$. Following Hermite, we write down the element

$$\begin{aligned} X_1 = &[(x_1 - x_2)(x_1 - x_5)(x_4 - x_3) + (x_1 - x_3)(x_1 - x_4)(x_2 - x_5)]\times \\ &[(x_1 - x_2)(x_1 - x_3)(x_5 - x_4) + (x_1 - x_4)(x_1 - x_5)(x_2 - x_3)]\times \\ &[(x_1 - x_2)(x_1 - x_4)(x_5 - x_3) + (x_1 - x_3)(x_1 - x_5)(x_4 - x_2)]. \end{aligned}$$

This element, as can be seen by direct computation (cf. Exercise 2.14), is invariant under all permutations of $x_2, \ldots, x_5$, but not under a cyclic permutation of $x_1, \ldots, x_5$. (For the latter: Note that setting $x_1 = x_2 = x_3$ makes $X_1 = 0$, but setting $x_2 = x_3 = x_4$ does not.) Next, the quotient

$$Z_1 = \frac{X_1}{(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)}$$

is in reduced form, and hence not symmetric. It is, however, invariant under permutations of $x_2, \ldots, x_5$, and so has five conjugates over $\mathbb{Q}(\mathbf{e})$. Call these $Z_1, \ldots, Z_5$, and let

$$\begin{aligned} F(X) &= (X - Z_1)(X - Z_2)(X - Z_3)(X - Z_4)(X - Z_5) \\ &= X^5 + AX^4 + BX^3 + CX^2 + DX + E. \end{aligned}$$

It is obvious that this polynomial has $\mathbb{Q}(\mathbf{x})$ as splitting field over $\mathbb{Q}(\mathbf{e})$. We prove below, using results from Appendix B, that $A = C = 0$. From this it follows that $D \neq 0$:

If $D = 0$, the polynomial $X^5 + sX^3 + t$ would be S_5-generic over $\mathbb{Q}$. However, a polynomial of this form cannot have more than three distinct real roots, and hence cannot be specialised to produce an S_5-extension of $\mathbb{Q}$ contained in $\mathbb{R}$. That there are such extensions can be demonstrated by exhibiting one: The

splitting field of $X^5 - 12X^3 + 32X + 1$ is an S_5-extension, and this polynomial has five real roots.

Converting $F(X)$ to the form $X^5 + sX^3 + tX + t$ is now simply a matter of scaling X.

Proving $A = C = 0$ is somewhat more involved, and we will do it by proving Hermite's result that $Z = Z_1\Delta$ satisfies an equation of the form

$$Z^5 + LZ^3 + M\Delta^2 Z + I\Delta^3 = 0.$$

Notice first that Z is in fact a polynomial in $\mathbf{x}$, of degree 15, and that it changes its sign under odd permutations of $x_2, \ldots, x_5$ and is invariant under even permutations. Consider now the conjugates $Z, Z', \ldots, Z^{(4)}$ of Z under the 5-cycle (12345), and let

$$G(X) = (X - Z) \cdots (X - Z^{(4)}).$$

From the described behaviour of Z_1, it is clear that the even-degree symmetric polynomials in $Z, Z', \ldots, Z^{(4)}$ are symmetric in $\mathbf{x}$, and the odd-degree symmetric polynomials anti-symmetric in $\mathbf{x}$. (Since the former contain an even power of Δ, and the latter an odd power.) Thus,

$$G(X) = X^5 + a\Delta X^4 + bX^3 + c\Delta X^2 + dX + e\Delta,$$

where a, b, c, d, e are symmetric in the x_i's.

Now, the elements a/Δ and c/Δ (as well as b, d and e/Δ) are, by construction, 'almost' invariants of the quintic form

$$e_0x^5 - e_1x^4y + e_2x^3y^2 - e_3x^2y^3 + e_4xy^4 - e_5y^5,$$

in that they are obtained from invariants by specialising in $e_0 = 1$ (or $y_1 = y_2 = y_3 = y_4 = y_5 = 1$). It is clear how the introduction of e_0 and y_i's in the above calculations will turn X_1 into a bracket polynomial and Z_1 into a rational function in the brackets, cf. section B.3 of Appendix B. We will therefore simply consider a/Δ and c/Δ as invariants.

The degree of a/Δ in the x_i's and y_j's is 10, and it therefore has weight 5, and thus degree 2 in $\mathbf{e}$. By the Example on p. 226 in Appendix B, there are no non-zero degree-2 invariants for the binary quintic, i.e., $a = 0$.

Similarly, the weight of c/Δ is 35 and the degree in $\mathbf{e}$ hence 14. Again by the Example on p. 226, there are no degree-14 invariants for the quintic either, so $c = 0$. □

NOTE. The element Z_1 is the above proof can be rewritten as

$$Z_1 = \frac{c_3x_1^3 + c_2x_1^2 + c_1x_1 + c_0}{5x_1^4 - 4e_1x_1^3 + 3e_2x_1^2 - 2e_3x_1 + e_4},$$

where

$$c_3 = -8e_1^2e_4 + 4e_1e_2e_3 - e_2^3 + 20e_2e_4 - 10e_3^2,$$
$$c_2 = 40e_1^2e_5 - 4e_1e_2e_4 - 2e_1e_3^2 + e_2^2e_3 - 100e_2e_5 + 20e_3e_4,$$
$$c_1 = -20e_1e_2e_5 4e_1e_3e_4 + 2e_2^2e_4 - e_2e_3^2 + 100e_3e_5 - 40e_4^2,$$
$$c_0 = -20e_1e_3e_5 + 8e_1e_4^2 + 10e_2^2e_5 - 4e_2e_3e_4 + e_3^3.$$

Attempting to verify $A = C = 0$ on a computer is complicated by the size of the expressions involved: $A = 0$ is fairly easy, whereas $C = 0$ has resisted all 'brute force' attempts by the authors. And of course, even if the computer succeeded in establishing $C = 0$, this would still be unsatisfactory since it does not justify why we picked that Z_1 in the first place.

Remarks. (1) We have constructed two-parameter generic polynomials for all the transitive subgroups of S_5. For the cyclic and dihedral groups, one-parameter generic polynomials exist over $\mathbb{Q}(\sqrt{5})$, cf. Chapter 5. For the others, two parameters are needed over all fields of characteristic 0, as we shall see in Chapter 8 below. (Although the argument in this case was essentially given in the beginning of the section on A_5.)

(2) An alternative proof of Hermite's result was given by Coray in [Co], using methods from algebraic geometry rather than invariant theory. The idea of Coray's proof is as follows:

Let $L/K = K(\theta)/K$ be a separable extension of degree 5, and consider an expression of the form

$$x = x_0 + x_1\theta + \cdots + x_4\theta^4 \in L.$$

Let $\mathrm{Tr}_{L/K}\colon L \to K$ be the trace map. The expressions $\mathrm{Tr}_{L/K}(x)$ and $\mathrm{Tr}_{L/K}(x^3)$ are homogeneous polynomials in $x_0, \ldots, x_4$ (of degree 1 and 3, respectively), and so we can consider the projective variety V in $\mathbb{P}^4(K)$ given by

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{L/K}(x^3) = 0.$$

Coray then proves the following: If $\mathrm{char}\, K \neq 3$, then V has a K-rational point. The corresponding $x \in L$ has a minimal polynomial of the desired form.

2.4. Groups of Degree 6

We will not go into details about groups of degree 6, for the simple reason that there are quite a lot of them. For instance, S_3, S_4 and S_5 can all be considered as transitive subgroups of S_6, by virtue of having order 6, being the rotation group for a cube, and having six 5-Sylow subgroups, respectively. In fact, S_4 can be embedded transitively into S_6 in two fundamentally different ways, by $(123) \mapsto (123)(456)$, $(34) \mapsto (15)(36)$, and by $(123) \mapsto (123)(456)$, $(34) \mapsto (13)(24)(56)$. The second of these embeddings corresponds to S_4 as the rotation group of a cube, while the first is obtained by identifying S_4 with the full symmetry group of a tetrahedron and maps into A_6. The image of A_4 is the same under both maps, and is transitive in S_6 as well. The embedding of S_5 into S_6 can also be described geometrically, by considering S_5 as the full

symmetry group of a dodecahedron, meaning that A_5 (the rotation group) is also transitive in S_6.

EXAMPLE. The polynomial $f(X) = X^6 - X^4 - 1 \in \mathbb{Q}[X]$ is irreducible, and the splitting field is an S_4-extension. The associated embedding of S_4 into S_6 is the first listed above. The discriminant is $d(f) = 2^6 31^2$.

The polynomial $g(X) = X^6 + 4X^4 - 27X^2 + 31 \in \mathbb{Q}[X]$ is also irreducible, and in fact has the same splitting field as $f(X)$. However, the embedding $S_4 \hookrightarrow S_6$ associated to $g(X)$ is the second listed above, and $d(g) = -2^6 11^4 31^3$.

EXAMPLES. If $f(X) \in \mathbb{Q}[X]$ is a quintic polynomial with Galois group S_5 or A_5, the Weber sextic resolvent $G(Z)$ will be an irreducible sextic polynomial with the same splitting field, corresponding to the transitive embedding of S_5 or A_5 into S_6.

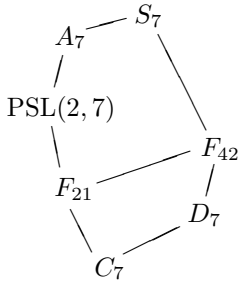
(1) The polynomial $X^6 + 6X^5 - 124$ is irreducible over $\mathbb{Q}$ with Galois group A_5.

(2) The polynomial $X^6 + 2X^5 + 3X^4 + 4X^3 + 5X^2 + 6X + 7$ is irreducible over $\mathbb{Q}$ with Galois group S_5.

NOTE. By invariant-theoretical methods similar to those used in the previous section for S_5, one can prove a result by Joubert [Jou, 1867] that $X^6 + sX^4 + tX^2 + uX + u$ is generic for S_6 over $\mathbb{Q}$.

2.5. Groups of Degree 7

The transitive subgroups of S_7 are C_7, D_7 (the dihedral group of degree 7, consisting of the symmetries of a regular heptagon), F_{21}, F_{42} (both Frobenius groups, consisting of affine transformations on $\mathbb{F}_7$), $\mathrm{PSL}(2,7)$ (the projective special linear group of 2×2 matrices over $\mathbb{F}_7$), A_7 and S_7. The groups C_7, D_7, F_{21} and F_{42} are solvable, while $\mathrm{PSL}(2,7)$ and A_7 are simple groups. The inclusions are



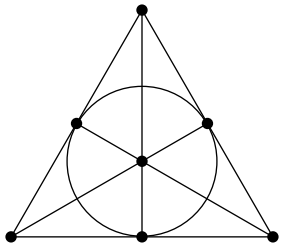
The solvable groups have the following respective permutation representations: Let $\sigma = (1234567)$ and $\omega = (243756)$. Then

$$F_{42} = \langle \sigma, \omega \rangle, \quad F_{21} = \langle \sigma, \omega^2 \rangle, \quad D_7 = \langle \sigma, \omega^3 \rangle, \quad \text{and} \quad C_7 = \langle \sigma \rangle,$$

where the relations between σ and ω are $\sigma^7 = \omega^6 = 1$ and $\sigma\omega = \omega\sigma^3$.

Here we consider mainly the realization of $\mathrm{PSL}(2,7)$ as a Galois group, cf. also [EF&M]. Therefore, construction of septimic polynomials with Galois group $\mathrm{PSL}(2,7)$ is our next task.

For any odd prime $p \geq 5$, $\mathrm{PSL}(2,p)$ is a simple group of order $(p-1)p(p+1)/2$. In particular, $\mathrm{PSL}(2,7)$ is simple of order 168. It becomes a permutation group of degree 7 via the isomorphism $\mathrm{PSL}(2,7) \simeq \mathrm{GL}(3,2)$ (cf. [Hu, II.§6 Satz 6.14]), since $\mathrm{GL}(3,2)$ obviously acts transitively on the non-zero elements in $\mathbb{F}_2^3$ (also known as the *Fano plane* or the *seven-point projective plane* $\mathbb{P}^2(\mathbb{F}_2)$).



As a permutation group it is 2-, but not 3-transitive. Here, a subgroup G of S_n is *k-transitive* if, for any two given k-tuples $(a_1,\ldots,a_k)$ and $(b_1,\ldots,b_k)$ of distinct numbers from $\{1,\ldots,n\}$, there exists a $\sigma \in G$ with $\sigma a_i = b_i$ for all i.

We make use of multiple transitivity to characterise septimic polynomials with Galois group $\mathrm{PSL}(2,7)$ over a field K of characteristic 0.

LEMMA 2.5.1. *Let $f(X) \in K[X]$ be an irreducible septimic polynomial, and let M denote its splitting field over K. Let $\alpha_1,\alpha_2,\ldots,\alpha_7$ be its roots in M. Also, let*

$$\mathcal{O}_2 = \{\alpha_i + \alpha_j \mid 1 \leq i < j \leq 7\}$$

and

$$\mathcal{O}_3 = \{\alpha_i + \alpha_j + \alpha_k \mid 1 \leq i < j < k \leq 7\}.$$

The the sets $\mathcal{O}_2$ and $\mathcal{O}_3$ have cardinalities 21 and 35, respectively. Furthermore, $\mathrm{PSL}(2,7)$ acts transitively on $\mathcal{O}_2$, but intransitively on $\mathcal{O}_3$.

PROOF. Lemma 1.2.2 in Chapter 1 gives us the cardinalities. The group $\mathrm{PSL}(2,7)$ acts transitively on $\mathcal{O}_2$, since it is 2-transitive. It cannot act transitively on $\mathcal{O}_3$, as $35 \nmid 168$. □

We now define the resolvent polynomials

$$P_{21}(X) = \prod_{1\leq i<j\leq 7} (X - (\alpha_i + \alpha_j))$$

and

$$P_{35}(X) = \prod_{1\leq i<j<k\leq 7} (X - (\alpha_i + \alpha_j + \alpha_k)).$$

They have distinct roots by Lemma 2.5.1, and we can characterise septimic polynomials with Galois group $\mathrm{PSL}(2,7)$ by means of them:

THEOREM 2.5.2. *Let $f(X) \in K[X]$ be an irreducible polynomial of degree 7. Then $\mathrm{Gal}(f/K) \simeq \mathrm{PSL}(2,7)$ if and only if the following conditions are satisfied:*

(i) *$d(f) \in (K^*)^2$,*

(ii) $P_{21}(X)$ *is irreducible over* K*, and*
(iii) $P_{35}(X)$ *factors into a product of two irreducible polynomials of degree* 7 *and degree* 28 *over* K*.*

PROOF. Condition (i) guarantees that $\mathrm{Gal}(f/K) \subseteq A_7$, and condition (ii) tells us that $\mathrm{Gal}(f/K)$ acts transitively on $\mathcal{O}_2$. Thus, it is F_{21}, $\mathrm{PSL}(2,7)$ or A_7. Since A_7 acts transitively on $\mathcal{O}_3$, it is excluded by condition (iii). F_{21} is excluded as well, since it cannot act transitively on a set of 28 elements. On the other hand: If $\mathrm{Gal}(f/K) \simeq \mathrm{PSL}(2,7)$, we see that it (through identification with $\mathrm{GL}(3,2)$) acts transitively on the subset of $\mathcal{O}_3$ corresponding to bases for $\mathbb{F}_2^3$ (triangles in $\mathbb{P}^2(\mathbb{F}_2)$). There are 28 bases. Thus, we have (iii). □

EXAMPLE. Consider trinomials of the form $f(X) = X^7 + aX + b \in K[X]$. The discriminant is given by

$$d(f) = -6^6a^7 - 7^7b^6.$$

The polynomials $P_{21}(X)$ and $P_{35}(X)$ are respectively given as follows:

$$\begin{aligned} P_{21}(X) = X^{21} &- 25aX^{15} - 57bX^{14} - 53a^2X^9 - 30abX^8 - 27a^3X^3 \\ &+ 27a^2b^2X^2 - 9ab^2X + b^3 \in K[X] \end{aligned}$$

and

$$\begin{aligned} P_{35}(X) = X^{35} &+ 40aX^{29} + 302bX^{28} - 1614a^2X^{23} + 2706abX^{22} \\ &+ 3828b^2X^{21} - 5072a^3X^{17} + 2778a^2bX^{16} - 18084ab^2X^{15} \\ &+ 36250b^3X^{14} - 5147a^4X^{11} - 1354a^3bX^{10} - 21192a^2b^2X^9 \\ &- 26326ab^3X^8 - 7309b^4X^7 - 1728a^5X^5 - 1728a^4bX^4 \\ &+ 720a^3b^2X^3 + 928a^2b^3X^2 - 64ab^4X - 128b^5. \end{aligned}$$

First, let $f(X) = X^7 - 7X + 3$ (TRINKS' polynomial). Then $f(X)$ is irreducible over $\mathbb{Q}$. As $d(f) = 3^8 7^8$, we have $\mathrm{Gal}(f/\mathbb{Q}) \subseteq A_7$. Furthermore, $P_{21}(X)$ is irreducible over $\mathbb{Q}$, while

$$\begin{aligned} P_{35}(X) = &(X^7 + 14X^6 - 42X^2 - 21X + 9) \\ &\times (\text{an irreducible polynomial of degree 28 over } \mathbb{Q}). \end{aligned}$$

Therefore, $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathrm{PSL}(2,7)$. Next, let $f(X) = X^7 - 154X + 99$. Then $f(X)$ is irreducible over $\mathbb{Q}$. We have $d(f) = 3^6 7^8 11^6 113^2$. Here $P_{21}(X)$ remains irreducible over $\mathbb{Q}$, while $P_{35}(X)$ factors as

$$\begin{aligned} P_{35}(X) = &(X^7 - 231X^3 - 462X^2 + 77X + 66) \\ &\times (\text{an irreducible polynomial of degree 28 over } \mathbb{Q}). \end{aligned}$$

Therefore $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathrm{PSL}(2,7)$.

The factorization property of the polynomial $P_{35}(X)$ gives characterization for a septimic polynomial over K having any transitive subgroup of S_7 as Galois group:

THEOREM 2.5.3. *Let* $f(X) \in K[X]$ *be irreducible of degree* 7*. Then we have the following:*

(a) $\mathrm{Gal}(f/K) \simeq A_7$ *or* S_7 *if and only if* $P_{35}(X)$ *is irreducible over* K.
(b) $\mathrm{Gal}(f/K) \simeq \mathrm{PSL}(2,7)$ *if and only if* $P_{35}(X)$ *factors into a product of two irreducible polynomials of degree* 7 *and degree* 28 *over* K.
(c) $\mathrm{Gal}(f/K) \simeq F_{42}$ *if and only if* $P_{35}(X)$ *factors into a product of two irreducible polynomials of degree* 14 *and* 21 *over* K.
(d) $\mathrm{Gal}(f/K) \simeq F_{21}$ *if and only if* $P_{35}(X)$ *factors into a product of three distinct irreducible polynomials of degree* 21, 7 *and* 7 *over* K.
(e) $\mathrm{Gal}(f/K) \simeq D_7$ *if and only if* $P_{35}(X)$ *factors into a product of four distinct irreducible polynomials of degree* 14, 7, 7 *and* 7 *over* K.
(f) $\mathrm{Gal}(f/K) \simeq C_7$ *if and only if* $P_{35}(X)$ *factors into a product of five distinct irreducible polynomials of degree* 7 *over* K.

PROOF. We have only to prove 'only if' in each case:
(a) is clear, since A_7 and S_7 are 3-transitive.
(b) is Theorem 2.5.2.
(c) and (d): Considering F_{21} and F_{42} as groups of affine transformation on $\mathbb{F}_7$, we see that the orbit of $\{0,1,2\}$ has 21 elements with respect to both groups. On the other hand, the orbits of $\{0,1,3\}$ and $\{0,1,5\}$ are distinct of order 7 over F_{21}, whereas they are equal of order 14 over F_{42}.
(e) is obvious, if we consider D_7 as the symmetry group of the regular heptagon.
(f) is trivial. □

EXAMPLES. Let $f(X) = X^7 - X - 1$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq S_7$.
(2) Let $f(X) = X^7 - 56X - 48$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq A_7$.
(3) Let $f(X) = X^7 - 7$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{42}$. More generally, if $f(X) = X^7 - a \in \mathbb{Q}[X]$ with $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^7$, then $f(X)$ is irreducible over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{42}$.
(4) Let $f(X) = X^7 + 14X^6 - 56X^4 + 56X^2 - 16$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{21}$.
(5) Let $f(X) = X^7 - 7X^6 - 7X^5 - 7X^4 - 1$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_7$.
(6) Let $f(X) = X^7 + X^6 - 12X^5 - 7X^4 + 28X^3 + 14X^2 - 9X + 1$. Then $f(X)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f/\mathbb{Q}) \simeq C_7$.

THEOREM 2.5.4. (MALLE AND MATZAT) *Let*

$$f(t,X) = X^7 - 56X^6 + 609X^5 + 1190X^4 + 6356X^3 + 4536X^2 - 6804X - 5832 - tX^3(X+1) \in \mathbb{Q}(t)[X].$$

Then $f(t,X)$ *is irreducible over* $\mathbb{Q}(t)$ *with* $\mathrm{Gal}(f/\mathbb{Q}(t)) \simeq \mathrm{PSL}(2,7)$.

Furthermore, for any $a \in \mathbb{Z}$ *with* $a \equiv 1 \pmod{35}$, $f(a,X)$ *is irreducible over* $\mathbb{Q}$ *with* $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathrm{PSL}(2,7)$.

This is a combination of Satz 3 and Zusatz 3 in [M&M1].

PROOF. The result of the Zusatz ('*Furthermore, ...*') is an immediate consequence of the main result, since $f(a, X)$ is irreducible modulo 7 and factors as a product of a linear, a quadratic and and a quartic polynomial modulo 5: The discriminant is a square, and the Galois group $\mathrm{Gal}(f(a, X)/\mathbb{Q})$ cannot be larger than $\mathrm{PSL}(2, 7)$; by Dedekind's Theorem (Theorem 3.3.3 in Chapter 3 below) it must be $\mathrm{PSL}(2, 7)$. The main result can be obtained by noting that $f(t, X) = -f(-9, t, -X)$, where $f(a, A, X)$ is the LaMacchia polynomial as given in the following theorem. □

THEOREM 2.5.5. (LAMACCHIA, [LaM]) *Let a and A be indeterminates, and let*

$$\begin{aligned} f(a, A, X) = {} & X^7 + 2(1 - 3a)X^6 + (-3 + 4a + 8a^2)X^5 \\ & + (-2 + 6a - 14a^2)X^4 + (2 - 4a + 6a^2 - 8a^3)X^3 + 8(2 + a)a^2X^2 \\ & + 4(-3 + 2a)a^2X - 8a^3 + AX^3(1 - X) \in \mathbb{Q}(a, A)[X]. \end{aligned}$$

Then $f(a, A, X)$ is irreducible, and the Galois group over $\mathbb{Q}(a, A)$ is isomorphic to $\mathrm{PSL}(2, 7)$.

PROOF. From the specialisations given in the partial proof above, it is clear that the Galois group is at least $\mathrm{PSL}(2, 7)$, i.e., either $\mathrm{PSL}(2, 7)$, A_7 or S_7. Now, in $\mathbb{Q}[a, A, X, Y]$, we have

$$Y^3(1 - Y)f(a, A, X) + X^3(1 - X)f(a, -A, Y) = p(X, Y)q(X, Y)$$

where $p(X, Y)$ has degree 4 in X, with highest degree term $Y^3 - Y^2$, and $q(X, Y)$ has degree 3 in X, with highest degree term Y. Let β be a root of $f(a, -A, Y)$ over $\mathbb{Q}(a, A)$. Then $\beta \neq 0, 1$, and so

$$\beta^3(1 - \beta)f(a, A, X) = p(X, \beta)q(X, \beta)$$

is a factorisation of $f(a, A, X)$ over $\mathbb{Q}(a, A, \beta)$ into factors of degrees 3 and 4. Thus, since $f(a, -A, Y)$ is irreducible over $\mathbb{Q}(a, A)$, the order of

$$\mathrm{Gal}(f(a, A, X)/\mathbb{Q}(a, A))$$

divides $7 \cdot 3! \cdot 4!$. In particular, it is not divisible by 5, eliminating A_7 and S_7. □

REMARKS. (1) In [Sw3], Swallow exhibits three explicit substitutions $(a, A) = (a_0, g(t)) \in \mathbb{Q} \times \mathbb{Q}(t)$ such that the specialised LaMacchia polynomial $f(a_0, g(t), X)$ is a $\mathrm{PSL}(2, 7)$-polynomial over $\mathbb{Q}(t)$, and such that the splitting field can be embedded in an $\mathrm{SL}(2, 7)$-extension of $\mathbb{Q}(t)$.

(2) It is clear that the splitting field over $\mathbb{Q}(a, A)$ of $f(a, A, X)$ (resp. over $\mathbb{Q}(t)$ of Malle and Matzat's polynomial $f(t, X)$) is a *regular* $\mathrm{PSL}(2, 7)$-extension, since $f(a, A, X)$ (resp. $f(t, X)$) is irreducible in $\mathbb{C}[a, A, X]$ (resp. $\mathbb{C}[t, X]$). (In the case of $f(t, X)$, this is also inherent in the construction given in [M&M1].)

(3) The polynomials $f(a, A, X)$ and $f(t, X)$ merely demonstrates the *existence* of $\mathrm{PSL}(2, 7)$-extensions over $\mathbb{Q}$ (and over Hilbertian fields in characteristic 0). Nothing in the construction guarantees that they are generic, or even parametric. In fact, as we shall see in Chapter 8 below, $f(t, X)$ cannot possibly be generic.

NOTE. In this section, we have given no generic polynomials whatsoever. Later, in Chapters 5 and 7, we will prove the existence of generic polynomials for C_7 and D_7. A construction similar to the one used for D_7 exists to produce generic polynomials for F_{21} and F_{42} as well. For S_7, construction is a trivial matter. This leaves A_7 and $\mathrm{PSL}(2,7)$, for which the existence or non-existence of generic polynomials remain open questions.

2.6. Groups of Degree 8, 9 and 10

Groups of degree 8, 9 and 10 will not be treated exhaustively in this monograph. The cyclic, dihedral, quasi-dihedral and quaternion groups of degree 8 are considered in Chapter 6 below, as is the Heisenberg group of order 27. Cyclic and dihedral groups of degree 9 and 10 are covered by the results of Chapter 7. Beyond that, we will simply make some remarks about a case where the Noether Problem fails:

The cyclic group of order eight. It is time to give an example where a generic polynomial does *not* exist: Assume that $f(\mathbf{t}, X) \in \mathbb{Q}(\mathbf{t})[X]$ is generic for C_8-extensions over $\mathbb{Q}$ (where $\mathbf{t}$ is some set of indeterminates), and let $L_2/\mathbb{Q}_2$ be the unramified C_8-extension of the field $\mathbb{Q}_2$ of 2-adic numbers. Then L_2 is the splitting field over $\mathbb{Q}_2$ of some specialisation $f(\mathbf{a}, X)$ of $f(\mathbf{t}, X)$. (And here we may of course assume that both $f(\mathbf{t}, X)$ and $f(\mathbf{a}, X)$ are irreducible.) Now, by Krasner's Lemma (see e.g. [Lo1, §25] or [Ja2, 9.8 Excs. 6–7]) we can modify the coefficients of $f(\mathbf{a}, X)$ slightly without changing the splitting field. In particular, we can replace $\mathbf{a}$ with a tuple consisting of rational numbers. Consider this done.

The splitting field of $f(\mathbf{a}, X)$ over $\mathbb{Q}$ is at most a C_8-extension, and thus exactly a C_8-extension, since the composite with $\mathbb{Q}_2$ is L_2. Hence, L_2 is the composite of $\mathbb{Q}_2$ and a C_8-extension of $\mathbb{Q}$. But Wang proved in [Wa, 1948] that this is not the case, and so we have a contradiction.

SKETCH OF ARGUMENT. (Cf. [Swn2, §5]) Let $L/\mathbb{Q}$ be a C_8-extension with $L_2 = L\mathbb{Q}_2$, and let $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ be the quadratic subextension, where D is a square-free integer. Since 2 is inert in $L/\mathbb{Q}$, we have $D \equiv 5 \pmod 8$, and can pick a prime divisor $p \not\equiv 1 \pmod 8$ of D. The completion $L_p/\mathbb{Q}_p$ of $L/\mathbb{Q}$ with respect to a prime $p \mid D$ is again a C_8-extension, and we see that

$$e_{L_p/\mathbb{Q}_p} = 8 \quad \text{and } f_{L_p/\mathbb{Q}_p} = 1.$$

Thus, p is tamely ramified, and it follows that the ramification index divides the order of the multiplicative group of the residue field, cf. [F&T, Ch. III Thm. 28], i.e., $p \equiv 1 \pmod 8$, contradicting our choice of p. The argument works for higher powers of 2 as well. □

The conclusion is that there is no generic polynomial for C_8-extensions over $\mathbb{Q}$, a fact first observed by Lenstra [Len, 1974]. By Proposition 5.1.8 above, this implies that there is no generic C_8-extension over $\mathbb{Q}$ either, cf. [Sa1, Thm. 5.11]. It also implies that C_8 provides a counter-example to Noether's Strategy, cf. [Ku, 1964] and the above results.

EXAMPLE. A consequence of this is the following: Let the automorphism σ on $\mathbb{Q}(s,t,u)$ be given by

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

Then σ has order 4, and the fixed field $\mathbb{Q}(s,t,u)^{C_4}$ is *not* rational over $\mathbb{Q}$. Thus, we have an explicit example of Lüroth's Theorem failing for higher transcendence degrees.

This follows from the negative answer to the Noether Problem for C_8: With $s = x/y$, $t = y/z$ and $u = z/w$, the field $\mathbb{Q}(s,t,u)$ is the homogeneous degree-0 part of $\mathbb{Q}(x,y,z,w)$, and σ is the restriction of

$$\sigma'\colon x \mapsto y, \quad y \mapsto z, \quad z \mapsto w, \quad w \mapsto -x,$$

which has order 8. By the No-name Lemma, $\mathbb{Q}(x,y,z,w)^{C_8}/\mathbb{Q}$ cannot be rational (as the representation obviously sits inside the regular one), and so neither can $\mathbb{Q}(s,t,u)^{C_4}/\mathbb{Q}$.

We leave it as a simple exercise to see that it cannot be stably rational either.

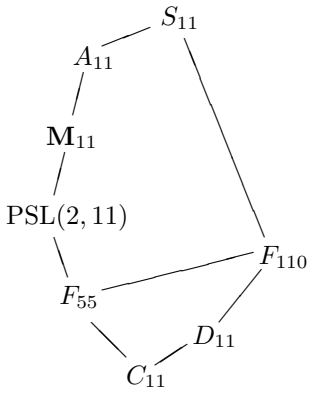
Compare this to the result in the Remark on p. 34, where the automorphism only differs from the one above by a sign (u mapping to $1/stu$ instead of $-1/stu$), but where the fixed field *is* rational.

Parametric polynomials for C_8 over a wide range of fields, including $\mathbb{Q}$, are constructed in [Sch]. We will give a general (but non-generic) description of C_8-extensions in Chapter 6 below.

We note that further examples of groups not having generic polynomials are given in [Sa3]. Specifically, Saltman constructs a group of order p^9 that does not possess a generic polynomial over any algebraically closed field of characteristic other than p.

2.7. Groups of Degree 11

The transitive subgroups of S_{11} are C_{11}, D_{11} (the dihedral group), F_{55}, F_{110} (both Frobenius groups), $\mathrm{PSL}(2,11)$ (the projective special linear group), $\mathbf{M}_{11}$ (the Mathieu group), A_{11} and S_{11}. The inclusions are



The groups C_{11}, D_{11}, F_{55} and F_{110} are solvable, while $\mathrm{PSL}(2,11)$, $\mathbf{M}_{11}$ and A_{11} are simple.

These groups are represented as permutation groups in the following way: Let $\sigma = (1\,2\,3\ldots10\,11)$ and $\omega = (1\,2\,4\,8\,5\,10\,9\,7\,3\,6)$. Then

$$F_{110} = \langle\sigma,\omega\rangle, \quad F_{55} = \langle\sigma,\omega^2\rangle, \quad D_{11} = \langle\sigma,\omega^5\rangle \quad \text{and} \quad C_{11} = \langle\sigma\rangle.$$

Furthermore,

$$\mathrm{PSL}(2,11) = \langle\sigma,\tau\rangle \quad \text{and} \quad \mathbf{M}_{11} = \langle\sigma,\tau'\rangle,$$

where $\tau = (3\,11)(4\,5)(6\,10)(7\,8)$ and $\tau' = (3\,7\,11\,8)(4\,10\,5\,6)$. The relations here are

$$\sigma^{11} = \tau^2 = (\sigma\tau)^3 = (\sigma^4\tau\sigma^6\tau)^2 = 1$$

and

$$\sigma^{11} = \tau'^4 = (\sigma\tau'^2)^3 = \sigma^4\tau'^2\sigma^{-5}\tau'^2 = 1,$$
$$(\sigma^{-4}\tau'^{-1})^3 = \sigma^{-1}\tau'\sigma^{-2}\tau', \quad \sigma^{-5}\tau'^2\sigma^2\tau' = (\sigma^3\tau'^{-1}\sigma\tau')^{-1},$$

cf. [C&M] and [G&M].

The Mathieu group $\mathbf{M}_{11}$ has order 7920, and is characterized by being sharply 4-transitive, by

THEOREM 2.7.1. [Pa, Thms. 21.5+21.8] (JORDAN) *Let G be a non-trivial sharply k-transitive group of degree n. If $k \geq 4$, then either $k = 4$, $n = 11$, or $k = 5$, $n = 12$.*

Moreover, the Mathieu group $\mathbf{M}_{11}$ is sharply 4-transitive of degree 11, and the Mathieu group $\mathbf{M}_{12}$ is sharply 5-transitive of degree 12.

$\mathrm{PSL}(2,11)$ has order 660 and is 2- but not 3-transitive.

To distinguish the various possible Galois groups for $f(X)$ over a field K of characteristic 0, we look at the resolvent

$$P_{165}(X) = R(x_1 + x_2 + x_3, f)(X) \in K[X]$$

and its factorisation. By Lemma 1.2.2 in Chapter 1, $P_{165}(X)$ has no multiple roots.

THEOREM 2.7.2. *Let $f(X) \in K[X]$ be a monic irreducible polynomial of degree 11, and let $P_{165}(X)$ be as above. Then the following assertions hold:*

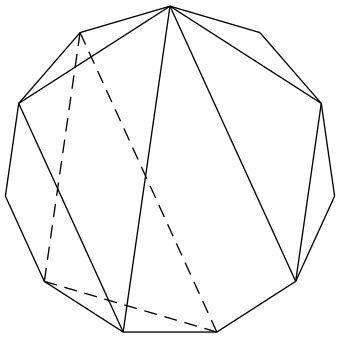
(a) $\mathrm{Gal}(f/K) \simeq \mathbf{M}_{11}$, A_{11} *or* S_{11}, *if and only if $P_{165}(X)$ is irreducible over K.*
(b) $\mathrm{Gal}(f/K) \simeq \mathrm{PSL}(2,11)$, *if and only if $d(f)$ is a square in K and $P_{165}(X)$ factors as a product of two irreducible polynomials of degrees 55 and 110 over K.*
(c) $\mathrm{Gal}(f/K) \simeq F_{110}$, *if and only if $d(f)$ is not a square in K and $P_{165}(X)$ factors as a product of two irreducible polynomials of degree 55 and 110 over K.*
(d) $\mathrm{Gal}(f/K) \simeq F_{55}$, *if and only if $P_{165}(X)$ factors as a product of three irreducible polynomials of degree 55 over K.*

(e) $\mathrm{Gal}(f/K) \simeq D_{11}$, *if and only if* $P_{165}(X)$ *factors as a product of five irreducible polynomials of degree* 22 *and five irreducible polynomials of degree* 11 *over* K.
(f) $\mathrm{Gal}(f/K) \simeq C_{11}$, *if and only if* $P_{165}(X)$ *factors as a product of fifteen irreducible polynomials of degree* 11 *over* K.

PROOF. As in the proof of Theorem 2.5.3, it is enough to prove 'only if' in each case.

(a) is clear, since $\mathbf{M}_{11}$, A_{11} and S_{11} are 4-transitive.

To prove the rest, we will look at triangles inscribed in a regular 11-gon. They correspond to the roots of $P_{165}(X)$, and are naturally divided into families of 11 each, closed under rotation: 10 families of asymmetrical triangles and 5 families of symmetrical triangles. The asymmetrical families come in pairs of mirror images.



Since C_{11} consists *only* of rotations, we immediately get (f). (e) follows as well, since D_{11} includes reflections as well as rotations.

The 55 symmetrical triangles are permuted transitively by F_{55}, whereas the asymmetrical triangles are divided into two sets of 55 triangles each. (F_{55} cannot take an asymmetrical triangle to its mirror image.) This proves (d). Looking at F_{110} instead, we see that mirroring is then available, and so F_{110} permutes the 110 asymmetrical triangles transitively, giving us (c).

Finally, by careful checking, we see that $\mathrm{PSL}(2, 11)$ will map symmetrical triangles to asymmetrical triangles, but that the two sets of asymmetrical triangles defined by F_{55} are still kept separate. Thus we have (b). □

For distinguishing $\mathbf{M}_{11}$, A_{11} and S_{11}, we have the following

PROPOSITION 2.7.3. *Let* $f(X) \in K[X]$ *be irreducible of degree* 11, *and assume that* $P_{165}(X)$ *is irreducible as well. Then* $\mathrm{Gal}(f/K) \simeq \mathbf{M}_{11}$ *if and only if the resolvent*

$$P_{462}(X) = R(x_1 + \cdots + x_5, f)(X) \in K[X]$$

is reducible. If $P_{462}(X)$ *is irreducible, we have* $\mathrm{Gal}(f/K) \simeq A_{11}$ *or* S_{11}, *depending on whether* $d(f)$ *is a square in* K *or not.*

REMARKS. (1) The resolvent $P_{330}(X) = R(x_1 + \cdots + x_4, f)$ is left irreducible by $\mathbf{M}_{11}$, and so provides no information.

(2) In [McK], McKay proves the following: $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathbf{M}_{11}$ if and only if $d(f) \in (\mathbb{Q}^*)^2$ and $P_{462}(X)$ factors as a product of two irreducible polynomials of degrees 66 and 396.

(3) In [M&Z], Matzat and Zeh-Marschke prove the existence of $\mathbf{M}_{11}$-extensions of $\mathbb{Q}(t)$, and thus of $\mathbb{Q}$, cf. also Thm. 6.12 in Ch. I of [M&M2].

NOTE. For the solvable groups of degree 11, we will consider generic polynomials later, in Chapters 5 and 7, and again the symmetric group is uninteresting. For the remaining groups, $\mathrm{PSL}(2, 11)$, $\mathbf{M}_{11}$ and A_{11}, it is not known whether generic polynomials exist.

Exercises

EXERCISE 2.1. Find a $q \in \mathbb{Q}$, such that $X^3 + qX + q$ and $X^3 - 2$ have the same splitting field.

EXERCISE 2.2. Find cubic polynomials over $\mathbb{Q}$ with Galois group S_3, such that the quadratic subfields of the splitting fields are $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{7})$.

EXERCISE 2.3. Find a generating transcendence basis for the extension

$$K(s, t, u)^{C_4}/K$$

in the Remark on p. 34.

EXERCISE 2.4. Let K be a field of characteristic $\neq 2$.

(1) Prove that $g(u, v, X) = X^4 + uX^2 + v^2 \in K(u, v)[X]$ is generic for V_4 over K.

(2) Prove that $g(u, v, X) = X^4 + uX^2 + u^2/(v^2 + 4) \in K(u, v)[X]$ is generic for C_4 over K.

(3) Prove that $g(u, v, X) = X^4 + uX^2 + v \in K(u, v)[X]$ is generic for D_4 over K.

EXERCISE 2.5. Prove that $X^4 + 12X^2 - 8X + 24$ is an A_4-polynomial over $\mathbb{Q}$, as claimed in the Example on p. 37.

EXERCISE 2.6. Let $F(\alpha, \beta, X) \in K(\alpha, \beta)[X]$ be the generic A_4-polynomial from Theorem 2.2.9, and let $G(\alpha, \beta, X) \in K(\alpha, \beta, X)$ be the minimal polynomial over $K(\alpha, \beta)$ for s^2, so that $G(\alpha, \beta, X)$ 'expresses' the cubic subextension of the A_4-extension given by $F(\alpha, \beta, X)$.

(1) Write the coefficients of $G(\alpha, \beta, X)$ as rational functions in α and β.

(2) Prove that $G(\alpha, \beta, X)$ is generic for C_3 over K. [Hint: Demonstrate first that if L/K is a C_3-extension, there is an A_4-extension of $K(t)$, such that the cubic subextension is $L(t)/K(t)$.]

EXERCISE 2.7. There are three non-abelian groups of order 12, namely A_4, the dihedral group

$$D_6 = \langle \sigma, \tau \mid \sigma^6 = \tau^2 = 1,\ \tau\sigma = \sigma^5\tau \rangle$$

and the semi-direct product

$$C_3 \rtimes C_4 = \langle u, v \mid u^3 = v^4 = 1,\ vu = u^2 v \rangle.$$

Find generic polynomials for D_6 and $C_3 \rtimes C_4$. [Hint: $D_6 = S_3 \times C_2$. A $C_3 \rtimes C_4$-extension is the composite of an S_3- and a C_4-extension.]

EXERCISE 2.8. (1) Use Weber's Theorem 2.3.4 to prove the following result, due to Roland, Yui and Zagier [RY&Z]: An irreducible quintic Bring-Jerrard polynomial $X^5 + aX + b \in \mathbb{Q}[X]$ has Galois group D_5 if and only if there are $\alpha, \beta \in \mathbb{Q}$ with

$$a = \frac{5\alpha^4}{4}(\beta^2+1)^2(\beta^2+\beta-1)(\beta^2-\beta-1),$$
$$b = \frac{\alpha^5}{2}(\beta^2+1)^3(\beta^2+\beta-1)(2\beta-1)(\beta+2).$$

[Hint: Replace λ and μ by u and v, where $\lambda = 5(u+1)/(u-1)$ and $v = 5\mu/(\lambda-1)$.]

(2) Using the remark on p. 42, find the quadratic subextension of a D_5-extensions of the kind considered in (1).

(3) Prove that $X^5+\frac{1}{4}X+\frac{6}{5}$ has Galois group D_5 over $\mathbb{Q}$, and that the quadratic subfield is $\mathbb{Q}(i)$.

EXERCISE 2.9. Prove that $X^5 + 15X^3 + 81$ has Galois group D_5 over $\mathbb{Q}$, and find the quadratic subextension.

EXERCISE 2.10. Use Brumer's result to find a D_5-polynomial over $\mathbb{Q}$ with five real roots.

EXERCISE 2.11. Find the Weber sextic resolvent for X^5+X+3 and its Galois group over $\mathbb{Q}$.

EXERCISE 2.12. Prove that the Weber sextic resolvent of an irreducible quintic is either irreducible or the product of a linear factor and an irreducible quintic factor. In either case, prove that the Weber sextic resolvent and the original quintic have the same splitting field.

EXERCISE 2.13. Let K be a field of characteristic $\neq 2$. We will produce a generic A_4-polynomial without invoking the Noether Extension and the related results:

(1) Let M/K be an A_4-extension, and let L/K be the C_3-subextension. Prove that $M = L(\sqrt{xy}, \sqrt{yz})$ for some $x \in L$ with conjugates y and z, and that conversely $L(\sqrt{xy}, \sqrt{yz})/K$ is A_4 whenever xy is not a square in L.

(2) Find a generic A_4-polynomial from a generic C_3-polynomial by letting x be a 'sufficiently general' element in a C_3-extension. Construct the polynomial to have three parameters.

EXERCISE 2.14. Write the element X_1 from the proof of Proposition 2.3.8 as

$$X_1 = (A+B)(C+D)(E+F),$$

with $A, \ldots, F$ taken in the order given in the proof. Determine how the permutations (23) and (2345) acts on $A, \ldots, F$. Then prove that S_4 leaves X_1 invariant by establishing the equalities

$$A+B = -C+D, \quad C+D = E-F, \quad E+F = A-B.$$

EXERCISE 2.15. Prove that the Noether Problem for the cyclic group C_6 over $\mathbb{Q}$ has an affirmative answer.

EXERCISE 2.16. Prove that $X^6 + 6X^5 + 100$ has Galois group A_6 over $\mathbb{Q}$. [Hint: Reduction modulo primes.]

EXERCISE 2.17. Let $f(t, X) \in \mathbb{Q}[t, X]$ be the $\mathrm{PSL}(2, 7)$-polynomial from Theorem 2.5.4. Prove that $f(a, X)$ has Galois group $\mathrm{PSL}(2, 7)$ over $\mathbb{Q}$ for $a \equiv -1, \pm 6 \bmod 35$.

EXERCISE 2.18. Let $f(X) = X^8 + a_7X^7 + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ have Galois group C_8 over $\mathbb{Q}$. Prove that $\bar{f}(X)$ is reducible in $\mathbb{F}_2[X]$.

EXERCISE 2.19. Consider the C_4-action on $\mathbb{Q}(s, t, u)$ given in the Example on p. 57. Prove that the fixed field of $C_2 \subseteq C_4$ is rational over $\mathbb{Q}$. Conclude that there is a C_2-action on the rational function field $\mathbb{Q}(x, y, z)$, such that $\mathbb{Q}(x, y, z)^{C_2}/\mathbb{Q}$ is not rational.

CHAPTER 3

Hilbertian Fields

This chapter contains the basic theory of Hilbertian fields, most notably the Hilbert Irreducibility Theorem and its proof. Also, it should hopefully give the first indications of the interest and importance of the Noether Problem.

For our purposes, the most suitable formulation of the theorem is as follows:

THE HILBERT IRREDUCIBILITY THEOREM. *Let K be an algebraic number field and let $f(\mathbf{t}, X) \in K(\mathbf{t})[X]$ be an irreducible polynomial, where $\mathbf{t} = (t_1, \ldots, t_n)$ are indeterminates. Then there exist infinitely many $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ such that the specialisation $f(\mathbf{a}, X) \in K[X]$ is well-defined and irreducible over K. The specialisation can be chosen to have*

$$\mathrm{Gal}(f(\mathbf{t}, X)/K(\mathbf{t})) \simeq \mathrm{Gal}(f(\mathbf{a}, X)/K).$$

This result is proved below, as Corollary 3.2.4 and Theorem 3.3.5.

EXAMPLE. Let $G = S_n$ act on $M = \mathbb{Q}(t_1, \ldots, t_n)$. The field of S_n-invariants is $K = M^{S_n} = \mathbb{Q}(e_1, \ldots, e_n)$ where

$$e_i = \sum_{1 \le j_1 < \cdots < j_i \le n} t_{j_1} t_{j_2} \ldots t_{j_i}$$

denotes the i^{th} elementary symmetric polynomial for $i = 1, 2, \ldots, n$. K is a purely transcendental extension of degree n, and M is a Galois extension of K with Galois group S_n.

Furthermore, M is the splitting field of the irreducible polynomial

$$f(e_1, \ldots, e_n, X) = X^n - e_1 X^{n-1} + e_2 X^{n-2} + \cdots + (-1)^n e_n \in K[X].$$

We may assign to each e_i a value $a_i \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. The Hilbert Irreducibility Theorem then asserts that there exist infinitely many n-tuples $(a_1, a_2, \ldots, a_n) \in \mathbb{Q}^n$ such that the polynomial

$$f(X) = X^n - a_1 X^{n-1} + a_2 X^{n-2} + \cdots + (-1)^n a_n \in \mathbb{Q}[X]$$

is irreducible over $\mathbb{Q}$ and the Galois group of the splitting field is isomorphic to S_n. Unfortunately, there is no effective method for determining which n-tuples fail to give S_n as its Galois group over $\mathbb{Q}$.

3.1. Definition and Basic Results

DEFINITION 3.1.1. Let K be a field, and let $f(\mathbf{t}, \mathbf{x})$ be an irreducible polynomial in $K(\mathbf{t})[\mathbf{x}] = K(t_1, \ldots, t_r)[x_1, \ldots, x_s]$. We then define the *Hilbert f-set* $H_{f/K}$ as the set of tuples $\mathbf{a} = (a_1, \ldots, a_r) \in K^r$ such that $f(\mathbf{a}, \mathbf{x}) \in K[\mathbf{x}]$ is

well-defined and irreducible. Furthermore, we define a *Hilbert set* of K^r to be the intersection of finitely many Hilbert f-sets and finitely many subsets of K^r of the form $\{\mathbf{a} \mid g(\mathbf{a}) \neq 0\}$ for a non-zero $g(\mathbf{t}) \in K[\mathbf{t}]$.

The field K is called *Hilbertian*, if the Hilbert sets of K^r are non-empty for all r. In this case, they must necessarily be infinite.

In other words: K is Hilbertian if, for any finitely many irreducible polynomials $f_1(\mathbf{t}, \mathbf{x}), \ldots, f_m(\mathbf{t}, \mathbf{x}) \in K(\mathbf{t})[\mathbf{x}]$ and any finitely many non-zero polynomials $g_1(\mathbf{t}), \ldots, g_n(\mathbf{t}) \in K[\mathbf{t}]$, there exists an $\mathbf{a} = (a_1, \ldots, a_r) \in K^r$ such that $f_1(\mathbf{a}, \mathbf{x}), \ldots, f_m(\mathbf{a}, \mathbf{x}) \in K[\mathbf{x}]$ are well-defined and irreducible, and that $g_1(\mathbf{a})$, $\ldots, g_n(\mathbf{a})$ are non-zero.

Remark. Obviously, finite fields are not Hilbertian. Neither are the real or complex numbers. If K is Henselian with respect to a non-trivial valuation, K is not Hilbertian. This includes $\mathfrak{p}$-adic number fields and Laurent series fields. It also demonstrates that 'Hilbertian' is not a Galois theoretical property as such: As we shall see below, the field $\mathbb{Q}$ is Hilbertian. However, the *Puiseux field* $\mathbb{P}(\mathbb{Q}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\!(t^{1/n})\!)$ is Henselian, and thus not Hilbertian, even though $\mathbb{Q}$ and $\mathbb{P}(\mathbb{Q})$ have the same absolute Galois group, cf. [vdW, Satz p. 53].[1]

Reduction of the criterion. First of all, it is clear that we need only consider the case $r = 1$ to determine if a field is Hilbertian: Let $f_1(\mathbf{t}, \mathbf{x}), \ldots, f_m(\mathbf{t}, \mathbf{x})$ be elements of $K(\mathbf{t})[\mathbf{x}]$ and $g_1(\mathbf{t}), \ldots, g_n(\mathbf{t})$ elements of $K[\mathbf{t}]$ as above. We may of course assume $f_1(\mathbf{t}, \mathbf{x}), \ldots, f_m(\mathbf{t}, \mathbf{x}) \in K[\mathbf{t}, \mathbf{x}]$. For $i = 1, \ldots, n$, we pick a non-zero term $g_i'(t_1)t_2^{e_2} \cdots t_r^{e_r}$ in $g_i(\mathbf{t})$ considered as an element of $K(t_1)[t_2, \ldots, t_r]$. If K has the Hilbertian property for $r = 1$, we can pick $a \in K$ such that $f_1(a, \mathbf{t}', \mathbf{x})$, $\ldots$, $f_m(a, \mathbf{t}', \mathbf{x})$ (with $\mathbf{t}' = (t_2, \ldots, t_r)$) are irreducible and $g_1'(a), \ldots, g_n'(a) \neq 0$. It follows that $g_1(a, \mathbf{t}'), \ldots, g_n(a, \mathbf{t}')$ are non-zero, and we can proceed with t_2.

Thus, we can assume $r = 1$.

Now, let $K[\mathbf{x}]_d$ denote the set of polynomials in $K[\mathbf{x}]$ of degree $< d$ in each indeterminate. We then have the *Kronecker specialisation* $S_d \colon K[\mathbf{x}]_d \to K[Y]$, given by

$$S_d(f) = f(Y, Y^d, \ldots, Y^{d^{s-1}}), \quad f \in K[\mathbf{x}]_d.$$

For $f = x_1^{e_1} \cdots x_s^{e_s}$, we have $S_d(x_1^{e_1} \cdots x_s^{e_s}) = Y^{e_1 + de_2 + \cdots + d^{s-1}e_s}$, and so we see that S_d is injective and maps $K[\mathbf{x}]_d$ onto $K[Y]_{d^s}$. Moreover, if $f, g \in K[\mathbf{x}]_d$ with $fg \in K[\mathbf{x}]_d$, we have

$$S_d(fg) = S_d(f)S_d(g).$$

Let $f \in K[\mathbf{x}]_d$, and assume $S_d(f)$ reducible: $S_d(f) = g'h'$ for polynomials $g', h' \in K[y]$. g' and h' must then have degree $< d^s$, and so $g' = S_d(g)$, $h' = S_d(h)$ for polynomials $g, h \in K[\mathbf{x}]_d$. If $gh \in K[\mathbf{x}]_d$, this means that $f = gh$. Hence, we get

Kronecker's Criterion. *f is irreducible, if and only if for every non-trivial factorisation $S_d(f) = S_d(g)S_d(h)$ the polynomial gh does not belong to $K[\mathbf{x}]_d$.*

[1] Although it is not stated that way, the argument in [vdW] gives: Let K be a field in characteristic 0. Then a finite extension of $\mathbb{P}(K)$ has the form $\mathbb{P}(L)/\mathbb{P}(K)$ for a (unique) finite extension L/K.

Let $f(t, \mathbf{x}) \in K(t)[\mathbf{x}]$ be irreducible, and assume that f has degree $< d$ in each x_i. Write

$$S_d(f) = \prod_{i=1}^{n} f_i(t, y),$$

where the f_i's are irreducible in $K(t)[y]$. Consider the Hilbert set of K consisting of those $a \in K$ for which $f_1(a, Y), \ldots, f_n(a, Y) \in K[Y]$ are well-defined and irreducible. Then $S_d(f)(a, Y) = \prod_i f_i(a, Y)$ is the irreducible factorisation of $S_d(f)(a, Y)$.

Every factorisation of $S_d(f)$ comes from $\prod_i f_i(t, Y)$. Since f is irreducible, every factorisation will introduce a monomial of degree $\geq d$ by Kronecker's criterion. Avoiding the finitely many points where one of these monomials is zero, we see that $f(a, \mathbf{x})$ is irreducible.

Hence, the Hilbert f-set $U_{f/K}$ contains a Hilbert set obtained from polynomials with $s = 1$.

Conclusion. We need only consider the case $r = s = 1$.

These reductions are standard, and can be found in e.g. [La, Ch. 8] or [Ha, Ch. 4].

Proposition 3.1.2. *Let K be a field of characteristic 0. Then the following conditions are equivalent:*

(i) *K is Hilbertian.*
(ii) *If $f(t, X) \in K[t, X]$ is irreducible of degree > 0 in X, there are infinitely many elements $a \in K$ such that $f(a, X)$ is irreducible in $K[X]$.*
(iii) *If $f(t, X) \in K[t, X]$ has no roots in $K(t)$ (as a polynomial in X) there is an $a \in K$ such that $f(a, X)$ has no roots in K.*

Proof. (i) $\Rightarrow$ (ii) is obvious.

(ii) $\Rightarrow$ (iii): Let $f(t, X) \in K[t, X]$ have no roots in $K(t)$. (iii) is clear if $\deg_X f = 0$, so assume $n = \deg_X f > 0$, and let $\mathbb{M}$ be the splitting field of $f(t, X)$ over $K(t)$. Given $a \in K$, we let $\mathcal{O}$ denote the integral closure of $K[t]_{(t-a)}$ in $\mathbb{M}$, and for all but finitely many a the roots of $f(t, X)$ are contained in $\mathcal{O}$. In that case, any maximal ideal $\mathfrak{m}$ in $\mathcal{O}$ containing $t - a$ will give us a field $M = \mathcal{O}/\mathfrak{m}$ that contains the splitting field of $f(a, X)$. We restrict our attention to such a's.

Now, let Θ be a primitive element for $\mathbb{M}/K(t)$, and let $g(t, X) \in K(t)[X]$ be the minimal polynomial for Θ over $K(t)$. Again, by avoiding finitely many a's, we may assume $g(t, X) \in K[t]_{(t-a)}[X]$. The roots of $f(t, X)$ are polynomials of degree $< n$ in Θ over $K(t)$, and (after another restriction of a) in fact over $K[t]_{(t-a)}$. Since $f(t, X)$ has no roots in $K(t)$, all of the roots are polynomials of degree > 0, and consequently they all have a non-zero coefficient in a non-constant term. If we eliminate those a for which this coefficient disappears, we are still left with all but finitely many $a \in K$, and we pick one for which $g(a, X) \in K[X]$ is irreducible. Then the roots of $f(a, X)$ are not in K.

(iii) $\Rightarrow$ (i): Let $f_1(t, X), \ldots, f_n(t, X) \in K(t)[X]$ be irreducible and monic. We must prove the existence of infinitely many $a \in K$ such that $f_1(a, X), \ldots, f_n(a, X) \in K[X]$ are well-defined and irreducible. Let $\mathbb{M}$ be the splitting field of the product $f_1(t, X) \cdots f_n(t, X)$ over K. We will consider only a's for which

all the polynomials $f_1(t,X),\dots,f_n(t,X)$ are in $K[t]_{(t-a)}[X]$, and will let $\mathcal{O}$ be the integral closure of $K[t]_{(t-a)}$ in $\mathbb{M}$. As above, we get a field $M=\mathcal{O}/\mathfrak{m}$ containing the roots of $f_1(a,X),\dots,f_n(a,X)$ by letting $\mathfrak{m}$ be a maximal ideal in $\mathcal{O}$ containing $t-a$.

Look first at $f_1(t,X)$, and let $\Theta_1,\dots,\Theta_s\in\mathcal{O}$ be the roots. For any non-empty subset $S\subsetneq\{1,\dots,s\}$ the polynomial $g(X)=\prod_{i\in S}(X-\Theta_i)$ is *not* in $K(t)[X]$, since $f_1(t,X)$ is irreducible. Thus, it has a coefficient $\xi\in\mathbb{M}\setminus K(t)$. Let $h_{1,S}(t,X)\in K[t]_{(t-a)}[X]$ be the minimal polynomial for ξ over $K(t)$. Since any factorisation of $f_1(a,X)$ in $K[X]$ must include a factor $\bar{g}(X)$ for some S, we can ensure the irreducibility of $f_1(a,X)$ by choosing $a\in K$ such that none of the polynomials $h_{1,S}(a,X)$ have roots in K. Similarly for the other $f_i(t,X)$'s. And since none of the polynomials $h_{i,S}(t,X)$ we get have roots in $K(t)$, we can multiply them to get a single polynomial $h(t,X)$ without any roots in $K(t)$. Adding factors $X^2-(t-b)$ for any finitely many specialisations we wish to avoid, we can now use (iii) to get an $a\in K$ with $f_1(a,X),\dots,f_n(a,X)$ irreducible in $K[X]$. And since we *can* avoid any finitely many a's, there must be infinitely many possibilities. □

Field extensions. We will now prove that a finite separable extension of a Hilbertian field is again Hilbertian. (In fact, an arbitrary finite extension of a Hilbertian field is Hilbertian, but we do not need that.)

LEMMA 3.1.3. *Let L/K be a finite separable field extension, and let $\sigma_1,\dots,\sigma_n$, $n=[L:K]$, be the different embeddings of L into its Galois closure. For any monic non-constant polynomial $f(t,X)\in L(t)[X]$ we can then find $h(t)\in L(t)$ such that the polynomials $\sigma_1 f(t,X+h(t)),\dots,\sigma_n f(t,X+h(t))$ are distinct.*

PROOF. It is obviously enough that $\sigma_1 f(t,h(t)),\dots,\sigma_n f(t,h(t))$ (the constant terms) are distinct.

We write $f(t,X)=X^m+a_{m-1}(t)X^{m-1}+\cdots+a_0(t)$, and let $m=qm'$, where $q=1$ if $\operatorname{char}K=0$, and q is the highest power of $\operatorname{char}K$ dividing m if $\operatorname{char}K>0$. Let $h(t)=t^N+\theta t^{N-1}$ for a primitive element θ for L/K and some suitably huge N. Then

$$f(t,h(t))=t^{mN}+m'\theta^q t^{mN-q}+\text{lower order terms.}$$

Since $m'\theta^q$ is a primitive element for L/K, $h(t)$ has the desired property. □

PROPOSITION 3.1.4. *If L/K is finite separable, then every Hilbert set of L contains a Hilbert set of K.*

PROOF. Let $f(t,X)\in L(t)[X]$ be monic and irreducible. Also, let M/K be the Galois closure of L/K. In $M(t)[X]$ we write $f(t,X)=f_1(t,X)\cdots f_n(t,X)$, where $f_1(t,X),\dots,f_n(t,X)$ are monic, irreducible and conjugate over L. By Lemma 3.1.3 we can translate $f_1(t,X)$ to get $g(t,X)\in M(t)[X]$ such that all the conjugates $\sigma g(t,X)$, $\sigma\in G=\operatorname{Gal}(M/K)$, are distinct. Let

$$G(t,X)=\prod_{\sigma\in G}\sigma g(t,X).$$

Then $G(t, X) \in K[t](X)$ is irreducible and monic. Consider the Hilbert set H consisting of those $a \in K$ for which $G(a, X) \in K[X]$ is well-defined and irreducible and $f_1(a, X), \ldots, f_n(a, X) \in M[X]$ are well-defined and distinct. For $a \in H$, $g(a, X)$ is irreducible, and hence so are $f_1(a, X), \ldots, f_n(a, X)$. As $f_1(a, X)$, $\ldots$, $f_n(a, X)$ are distinct and conjugate over L, $f(a, X) = f_1(a, X) \cdots f_n(a, X) \in L[X]$ is well-defined and irreducible. Hence, the Hilbert set H is contained in the Hilbert f-set given by $f(t, X)$. □

COROLLARY 3.1.5. *A finite separable extension of a Hilbertian field is again Hilbertian.*

COROLLARY 3.1.6. *Let L/K be finite separable. Then every Hilbert set of L^r contains a Hilbert set of K^r.*

PROOF. In the reduction from r to $r-1$ given above, we can pick $a \in K$. □

EXAMPLE. Let K be a Hilbertian field of characteristic $\neq 2$, and let L/K be a cyclic extension of degree 3. Let σ generate the Galois group $\mathrm{Gal}(L/K)$. Also, let $\theta \in L$ be a primitive element for L/K. Consider the polynomial

$$f(t, X) = X^2 - (t + \theta)(t + \sigma\theta) \in L[t, X].$$

It is obviously irreducible, since $(t + \theta)(t + \sigma\theta)$ is not a square in $L[t]$. Hence, there exists $a \in K$ such that $f(a, X) \in L[X]$ is irreducible. Let $\alpha = a + \theta$, $\beta = \sigma\alpha = a + \sigma\theta$ and $\gamma = \sigma\beta$. Then $\alpha\beta$ and $\beta\gamma$ are quadratically independent over L, and $M/K = L(\sqrt{\alpha\beta}, \sqrt{\beta\gamma})/K$ is an A_4-extension.

Thus, a cyclic extension of degree 3 over a Hilbertian field can always be extended to an A_4-extension.[2]

This example demonstrates that Corollary 3.1.6 is often a much more useful result that Corollary 3.1.5. (Quite apart from the fact that it is a stronger statement.)

REMARKS. (1) As noted at the beginning of this section, any finite extension of a Hilbertian field is Hilbertian. See e.g. [F&J, Cor. 11.10] for a proof in the case of a purely inseparable extension. However, the Hilbertian fields we consider all have characteristic 0, and so we have no need of the inseparable case.

(2) More is known about Hilbertian fields and separable algebraic extensions than just Corollary 3.1.5. It can be shown, for instance, that L is Hilbertian if K is Hilbertian and L/K is a (pro-finite) Galois extension with finitely generated Galois group, cf. [F&J, Prop. 15.5]. See [Hr] for further examples.

3.2. The Hilbert Irreducibility Theorem

In this section we will prove the so-called Hilbert Irreducibility Theorem, first proved by Hilbert in 1892 in [Hi]: $\mathbb{Q}$ is Hilbertian. This theorem is the reason for the term 'Hilbertian.' Our treatment largely follows [Ha, Ch. 4].

LEMMA 3.2.1. *Let K be a field, and let $f(t, X) \in K(t)[X]$ have degree n. Assume that $f(t, X)$ has n distinct roots over $K(t)$. Then $f(a, X) \in K[X]$ is well-defined and has n distinct roots over K for all but finitely many $a \in K$.*

[2]The argument given is easily modified for the case $\mathrm{char}\, K = 2$.

PROOF. We may of course assume $f(t,X) \in K(t)[X]$ to be monic. That $f(t,X)$ has n distinct roots over $K(t)$ means that the discriminant $d(f(t,X))$ is non-zero. But then $f(a,X) \in K[X]$ will have n distinct roots whenever $f(a,X)$ is well-defined with non-zero discriminant, which is for all but finitely many $a \in K$. □

DEFINITION 3.2.2. Let $f(t,X) \in K(t)[X]$ be a polynomial of degree n. A point $a \in K$ is then called a *regular* point for $f(t,X)$, if $f(a,X) \in K[X]$ is well-defined and has n distinct roots.

LEMMA 3.2.3. *Let $f(t,X) \in \mathbb{C}(t)[X]$ be monic of degree n, and let $a \in \mathbb{C}$ be a regular point. Then there exist* analytic root functions *on a neighbourhood N of a, i.e., n analytic functions $\theta_1, \ldots, \theta_n \colon N \to \mathbb{C}$ such that*

$$f(z,X) = \prod_{i=1}^{n} (X - \theta_i(z)), \quad z \in N.$$

PROOF. Obviously, we only have to find, given a root α of $f(a,X)$, an analytic function θ on a neighbourhood N of a, such that $\theta(a) = \alpha$ and $f(z,\theta(z)) = 0$ for $z \in N$.

We need the Residue Theorem, which (in the form we will use) states that

$$\frac{1}{2\pi i} \oint_\gamma G(z)\, dz = \sum_\zeta \mathrm{Res}(G,\zeta),$$

when $G \colon \Omega \to \mathbb{C}$ is a meromorphic function defined on an open subset Ω of $\mathbb{C}$, γ is a circle periphery inside Ω (traversed counter-clockwise) and ζ runs through the (finitely many) poles of G in the open circle disc bounded by γ. The *residue*, $\mathrm{Res}(G,\zeta)$, of G in a point ζ of Ω is the degree -1 coefficient in the Laurent series expansion of G around ζ.

Now, if $F \colon \Omega \to \mathbb{C}$ is analytic, the function $G = F'/F$ is meromorphic, and a zero ζ of F of multiplicity n becomes a pole of G of multiplicity 1 and residue n. Thus, from the Residue Theorem, we get that

$$\frac{1}{2\pi i} \oint_\gamma \frac{F'(z)}{F(z)}\, dz$$

equals the number of zeroes of F inside the circle γ, counted with multiplicity.

More generally, if $\varphi \colon \Omega \to \mathbb{C}$ is analytic, the residue of $F'\varphi/F$ at a zero ζ of F is equal to $\varphi(\zeta)$ times the multiplicity n_ζ of ζ, and so

$$\frac{1}{2\pi i} \oint_\gamma \frac{F'(z)}{F(z)} \varphi(z)\, dz = \sum_\zeta n_\zeta\, \varphi(\zeta),$$

cf. also [S&Z, III.§9].

Returning now to the problem of finding root functions, we note first that there is a neighbourhood U of α such that $f(a,z) \neq 0$ for $z \in U \setminus \{\alpha\}$. Let $\delta > 0$ be such that the disc $D(\alpha,\delta)$ with center α and radius δ is contained in U, and

let γ be the boundary. Then

$$\frac{1}{2\pi i}\oint_\gamma \frac{\frac{\partial}{\partial z}f(a,z)}{f(a,z)}\,dz = 1.$$

Since $f(t,z)$ is continuous in both t and z, there is a neighbourhood N of a such that $f(t,z)\neq 0$ for $t\in N$ and z on γ. Thus,

$$H(t) = \frac{1}{2\pi i}\oint_\gamma \frac{\frac{\partial}{\partial z}f(t,z)}{f(t,z)}\,dz$$

is defined on N. Clearly, it is continuous, and by the above considerations it assumes only integer values, meaning that $H(t)=1$ for all $t\in N$.

Consequently, there is, for $t\in N$, only a single root $\theta(t)\in D(\alpha,\delta)$ of $f(t,X)$, and this gives us a root function $\theta\colon N\to\mathbb{C}$. Again by the considerations above, we have

$$\theta(t) = \frac{1}{2\pi i}\oint_\gamma \frac{\frac{\partial}{\partial z}f(t,z)}{f(t,z)}\,z\,dz,$$

showing that $\theta\colon N\to\mathbb{C}$ is in fact analytic, cf. [S&Z, II.§3]. □

Remark. A more direct proof of Lemma 3.2.3 (find a power series and prove it converges) can be found in [Ha, Ch. 4]. Note, however, that we actually prove a stronger result, since we do not use the fact that the coefficients in $f(t,X)$ are rational functions, but only that they are meromorphic.

H. A. Schwarz' Mean Value Theorem. *Let $a_0<\cdots<a_m$ be real numbers, and let $f\colon[a_0,a_m]\to\mathbb{R}$ be an m times differentiable function. Then there exists an $a\in(a_0,a_m)$, such that*

$$\frac{f^{(m)}(a)}{m!} = \frac{W}{V},$$

where

$$V = \begin{vmatrix} 1 & a_0 & \dots & a_0^m \\ \vdots & & \ddots & \vdots \\ 1 & a_m & \dots & a_m^m \end{vmatrix}$$

is the Vandermonde determinant, and

$$W = \begin{vmatrix} 1 & a_0 & \dots & a_0^{m-1} & f(a_0) \\ \vdots & & \ddots & & \vdots \\ 1 & a_m & \dots & a_m^{m-1} & f(a_m) \end{vmatrix}.$$

Proof. (1) If g is an m times differentiable function of $[a_0,a_m]$ with $g(a_i)=f(a_i)$ for all i, we have $g^{(m)}(a)=f^{(m)}(a)$ for some $a\in(a_0,a_m)$: Since $f-g$ is 0 in the $m+1$ points $a_0,\dots,a_m$, $(f-g)'$ has at least m zeroes in (a_0,a_m) by the usual Mean Value Theorem. It follows that $(f-g)''$ has at least $m-1$ zeroes, etc., and finally that $(f-g)^{(m)}$ has at least one zero.

(2) Now, let $g(X) = b_m X^m + \cdots + b_0 \in \mathbb{R}[X]$ be the unique polynomial of degree $\leq m$ with $g(a_i) = f(a_i)$. By (1), $f^{(m)}(a) = g^{(m)}(a) = m!\, b_m$ for some $a \in (a_0, a_m)$. On the other hand, we find the coefficients of $g(X)$ by solving

$$\begin{pmatrix} 1 & a_0 & \dots & a_0^m \\ \vdots & & \ddots & \vdots \\ 1 & a_m & \dots & a_m^m \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} f(a_0) \\ \vdots \\ f(a_m) \end{pmatrix},$$

and Cramer's Rule gives us $b_m = W/V$. □

And now we are ready to prove

THE HILBERT IRREDUCIBILITY THEOREM. *$\mathbb{Q}$ is Hilbertian.*

PROOF. Let $f(t, X) \in \mathbb{Z}[t, X]$ have degree n in X, and assume that it has no roots in $\mathbb{Q}(t)$. We must prove that there is an $a \in \mathbb{Q}$ such that $f(a, X) \in \mathbb{Q}[X]$ has no rational root. By Proposition 3.1.2, this will establish the result.

The first thing we do is to translate $f(t, X)$ such that 0 becomes a regular point. Next, we replace $f(t, X)$ by $t^d f(1/t, X)$, where d is the degree of f in t. By Lemma 3.2.3, we then have root functions $\theta_1, \dots, \theta_n$ defined on a neighbourhood of ∞, i.e., for all t with $|t|$ greater than some $T \in \mathbb{R}_+$. These root functions are reciprocal power series, i.e., power series in t^{-1}, and

$$f(t, X) = g(t) \prod_{i=1}^{n} (X - \theta_i(t)) \in \mathbb{C}(\!(t^{-1})\!)[X],$$

where $g(t) \in \mathbb{Q}[t]$ is the coefficient of X^n in $f(t, X)$. Since $g(t) \neq 0$ for $|t| > T$, it can be ignored.

Now, if $a \in \mathbb{Q}$ (with $a > T$) is such that none of $\theta_1(a), \dots, \theta_N(a)$ are rational, then obviously $f(a, X)$ has no rational roots. Thus, we wish to prove that there is such an a.

Pick one of the $\theta_i(t)$'s and call it simply $\theta(t)$. By construction, $\theta(t)$ is a reciprocal power series over $\mathbb{C}$, convergent for $|t| > T$. Also, it is trivially algebraic over $\mathbb{Q}(t)$, since

$$f(t, \theta(t)) = b_k(t)\theta(t)^n + \cdots + b_0(t) = 0$$

for suitable $b_0(t), \dots, b_n(t) \in \mathbb{Z}[t]$, $b_n(t) \neq 0$. Replacing $y(t)$ by $z(t) = b_n(t)y(t)$ we get

$$z(t)^n + c_{n-1}(t)z(t)^{n-1} + \cdots + c_0(t) = 0$$

for $c_0(t), \dots, c_{n-1}(t) \in \mathbb{Z}[t]$. Since $\mathbb{Z}$ is integrally closed, it is clear that if $z(a)$ is rational for some $a \in \mathbb{Z}$, it is in fact integral.

As $\theta(t) \in \mathbb{C}(\!(t^{-1})\!)$ and $b_n(t) \in \mathbb{Z}[t]$, we get

$$z(t) = d_\ell t^\ell + d_{\ell-1} t^{\ell-1} + \cdots + d_1 t + d_0 + d_{-1} t^{-1} + \cdots + d_{-i} t^{-i} + \cdots \in \mathbb{C}(\!(t^{-1})\!).$$

Since $\theta(t)$ is not a rational function over $\mathbb{Q}$, $z(t)$ is not a polynomial over $\mathbb{Q}$. Thus, if $z(t)$ *is* a polynomial in t, it must have an irrational coefficient, and it follows that $z(a) \in \mathbb{Z}$ only holds for finitely many $a \in \mathbb{Z}$.

If any of the d_i's are non-real, we also only have $z(a) \in \mathbb{Z}$ for finitely many $a \in \mathbb{Z}$: Let d_i be the first non-real coefficient, i.e., $d_\ell, \dots, d_{i+1} \in \mathbb{R}$, $d_i \notin \mathbb{R}$. Then $\operatorname{Im} z(t)/t^i = \operatorname{Im}(d_i + d_{i-1}t^{-1} + \dots) \to \operatorname{Im} d_i$ for $t \to \infty$, and so, for large enough t, $z(t)$ is not even real.

Finally, assume that all the d_i's are real, and that $z(t)$ is not a polynomial. Then

$$z^{(m)}(t) = \frac{D}{t^q} + \text{terms involving higher powers of } t^{-1}$$

for some $m, q \in \mathbb{N}$ and $D \in \mathbb{R}^*$. Then $t^q z^{(m)}(t) \to D$ for $t \to \infty$, and so $0 < |z^{(m)}(t)| < 2|D|/t^q$ for all $t > T'$ for some $T' \geq T$.

If there are only finitely many natural numbers a with $z(a) \in \mathbb{Z}$, all is well. Otherwise, let $a_0 < \dots < a_m$ be $m+1$ natural numbers with $a_0 > T'$ and $z(a_i) \in \mathbb{Z}$. With z substituted for f in the Schwarz Mean Value Theorem, we get $W \in \mathbb{Z} \setminus \{0\}$, and so $|W| \geq 1$. It follows that

$$\frac{2|D|}{m!a_0^q} \geq \frac{2|D|}{m!a^q} \geq \frac{|z^{(m)}(a)|}{m!} \geq \frac{1}{|V|}$$

for some $a \in (a_0, a_m)$, and hence

$$\frac{m!}{2|D|}a_0^q \leq |V| = \prod_{i<j}(a_j - a_i) \leq (a_m - a_0)^{m(m+1)/2}.$$

Thus, $\alpha a_0^\beta < a_m - a_0$ for suitable positive constants α and β. If we choose $T'' \geq T'$ such that $\alpha T''^\beta \geq mn$, this means that among any $mn+1$ succesive integers $\geq T''$ there are at most m with $z(a) \in \mathbb{Z}$, and hence $\theta(a) \in \mathbb{Q}$.

We can now prove our original claim: For those $\theta_i(t)$ that are rational in finitely many natural numbers only, we pick $T' > T$ greater than any of these. For the rest, we choose m big enough to work for them all, and pick T'' greater than or equal to all the T''s and T'''s obtained as above. Then, whenever we have $mn+1$ successive integers $\geq T''$, there are at most m in which any given $\theta_i(t)$ is rational, and so at least one where none of them are. □

COROLLARY 3.2.4. *Algebraic number fields are Hilbertian.*

3.3. Noether's Problem and Dedekind's Theorem

Let S be a commutative ring with unit, and let the finite group G act on S by automorphisms. Also, let $R = S^G$ be the subring of fixed points.

REMARK. Consider a finite Galois extension M/K with Galois group $G = \operatorname{Gal}(M/K)$. If K is the quotient field of an integrally closed domain R, we can let S be the integral closure of R in M. Alternatively, we can let S be the ring generated over R by the roots of a monic polynomial $f(X) \in R[X]$ with splitting field M over K.

It is easily seen that $\mathfrak{m} \cap R$ is maximal in R whenever $\mathfrak{m}$ is maximal in S, and that $\mathfrak{a}S$ is a proper ideal in S if $\mathfrak{a}$ is a proper ideal in R.

For a given maximal ideal $\mathfrak{m}$ in S we define the *decomposition group* as

$$D = D_\mathfrak{m} = \{\sigma \in G \mid \sigma\mathfrak{m} = \mathfrak{m}\},$$

and the *inertia group* as

$$I = I_{\mathfrak{m}} = \{\sigma \in G \mid \forall s \in S\colon \sigma s \equiv s \pmod{\mathfrak{m}}\}.$$

Thus, D consists of all the elements in G that give rise to an automorphism on $\lambda = S/\mathfrak{m}$, and I is the kernel of the induced action of D on λ. In particular, D/I acts faithfully on λ, and it is clear that $\kappa = R/\mathfrak{m}\cap R$ is a point-wise invariant subfield. It is also clear that λ/κ is algebraic.

LEMMA 3.3.1. *Assume that λ/κ is separable. Then λ/κ is a finite Galois extension with $\mathrm{Gal}(\lambda/\kappa) \simeq D/I$ (by the induced action).*

PROOF. (Cf. [Lo1, §16.3].) An element $s \in S$ is a root of

$$p(X) = \prod_{\sigma\in G}(X - \sigma s) \in R[X].$$

It follows that every element $\bar{s} \in \lambda$ is algebraic over κ of degree $\leq |G|$, and that the minimal polynomial splits completely over λ. Thus, λ/κ is finite Galois (of degree $\leq |G|$).

Next, let $R' = S^D$. We claim that $R'/\mathfrak{m}\cap R' = \kappa$: Let $\sigma_1 = 1, \ldots, \sigma_r$ represent the cosets σD in G. Then the maximal ideals $\sigma_1\mathfrak{m}$, …, $\sigma_r\mathfrak{m}$ are distinct, and we can (for $i > 1$) pick $x \in \sigma_i^{-1}\mathfrak{m} \setminus \mathfrak{m}$. Now, $\prod_{\sigma\in D}\sigma a \in \sigma_i^{-1}\mathfrak{m} \setminus \mathfrak{m}$, and thus $\sigma_i^{-1}\mathfrak{m} \cap R' \neq \mathfrak{m} \cap R'$. By the Chinese Remainder Theorem we can, for $a \in R'$, pick $a' \in R'$ with $a - a' \in \mathfrak{m}$ and $a' \in \sigma_2^{-1}\mathfrak{m} \cap \cdots \cap \sigma_r^{-1}\mathfrak{m}$. Then $\sigma_1 a' \cdots \sigma_r a' \in R$ is congruent to a modulo $\mathfrak{m} \cap R'$.

Thus, we may assume $D = G$: Let $s \in S$ such that $\lambda = \kappa(\bar{s})$, and let $p(X) = \prod_{\sigma\in G}(X - \sigma s) \in R[X]$. For $\rho \in \mathrm{Gal}(\lambda/\kappa)$ we have $p(\rho\bar{s}) = 0$, and so $\rho\bar{s} = \overline{\sigma s}$ for some $\sigma \in G$, meaning that ρ is induced by σ. □

An important special case of this result arises as follows: Let R be a domain with quotient field K, and let M/K be finite Galois with Galois group $G = \mathrm{Gal}(M/K)$. Let $f(X) \in R[X]$ be a monic polynomial with splitting field M over K, and let $S \subseteq M$ be a domain containing R and the roots of $f(X)$, such that $R = S \cap K$ and $\sigma S = S$ for all $\sigma \in G$.

If $d(f) \notin \mathfrak{m}$, the polynomial $\bar{f}(X) \in \kappa[X]$ is has no multiple roots. Let $s_1, \ldots, s_n \in S$ be the roots of $f(X)$ in S, so that $\bar{s}_1, \ldots, \bar{s}_n \in \lambda$ are the roots of $\bar{f}(X)$. For $\sigma \in D \setminus 1$ we have $\sigma s_i \neq s_i$ for some i, and hence $\bar{\sigma}\bar{s}_i \neq \bar{s}_i$. This gives us

PROPOSITION 3.3.2. *If $d(f) \notin \mathfrak{m} \cap R$, the map $D \twoheadrightarrow \mathrm{Gal}(\lambda/\kappa)$ is an isomorphism, and D and $\mathrm{Gal}(\lambda/\kappa)$ are identical as permutation groups on the roots of $f(X)$ (resp. $\bar{f}(X)$).*

REMARK. It is possible to give a direct proof of Proposition 3.3.2 using Galois theory of commutative rings, as described in Chapter 4 below:

Assume $d(f) \notin \mathfrak{m}$. We can then replace R and S by $R[1/d(f)]$ and $S[1/d(f)]$ to get that S/R is Galois with group G. (Replacing R and S like this does not change κ and λ.) This gives us a Galois algebra $S \otimes_R \kappa/\kappa$ with group G. Clearly, $\lambda = S/\mathfrak{m}$ is a simple component of $S \otimes_R \kappa$, and the elements in G that maps λ

to itself are exactly those of D. Thus, λ/κ is Galois with Galois group D, and we have the Proposition.

A classical application of this is

THEOREM 3.3.3. (DEDEKIND) *Let $f(X) \in \mathbb{Z}[X]$ be monic with discriminant $d \in \mathbb{Z}$. If p is a prime not dividing d, and $\bar{f}(X) = f_1(X) \cdots f_r(X)$ is the decomposition of $\bar{f}(X) \in \mathbb{F}_p[X]$ in irreducible factors, then $\mathrm{Gal}(f/\mathbb{Q})$ contains a permutation of cycle type $(\delta_1, \ldots, \delta_r)$, where δ_i is the degree of $f_i(X)$.*

PROOF. Let σ generate $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$. Then σ permutes the roots of $f_i(X)$ cyclically, i.e., σ contains a cycle of length δ_i. □

Now, if K is a Hilbertian field, and $f(\mathbf{t}, X) \in K(\mathbf{t})[X]$ is monic, irreducible and separable, we can find $\mathbf{a} \in K^r$, such that $f(\mathbf{a}, X) \in K[X]$ is well-defined and irreducible. Let $\mathfrak{m} = (t_1 - a_1, \ldots, t_r - a_r) \subseteq K[\mathbf{t}]$. Localising in $\mathfrak{m}$, we get an integrally closed domain $R = K[\mathbf{t}]_{\mathfrak{m}}$ with maximal ideal $\mathfrak{m}_{\mathfrak{m}}$ and residue field $K = K[\mathbf{t}]/\mathfrak{m}$, the residue map being specialisation in $\mathbf{a}$. Moreover, $f(\mathbf{t}, X) \in R[X]$.

Hence, if $d(f(\mathbf{t}, X)) \notin \mathfrak{m}_{\mathfrak{m}}$, i.e., $d(f(\mathbf{a}, X)) \neq 0$, we get

$$\mathrm{Gal}(f(\mathbf{a}, X)/K) \subseteq \mathrm{Gal}(f(\mathbf{t}, X)/K(\mathbf{t})).$$

If $\mathbb{M}/K(\mathbf{t})$ is finite Galois, we can pick a primitive element $\Theta \in \mathbb{M}$ and look at the minimal polynomial $g(\mathbf{t}, X) \in K(\mathbf{t})[X]$. Specialising $g(\mathbf{t}, X)$ as above to get $\mathrm{Gal}(g(\mathbf{a}, X)/K) \subseteq \mathrm{Gal}(g(\mathbf{t}, X)/K(\mathbf{t}))$, we see that we then have $\mathrm{Gal}(g(\mathbf{a}, X)/K) \simeq \mathrm{Gal}(g(\mathbf{t}, X)/K(\mathbf{t}))$, since $\mathrm{Gal}(g(\mathbf{a}, X)/K)$ has order at least equal to the degree of $g(\mathbf{a}, X)$, whereas $\mathrm{Gal}(g(\mathbf{t}, X)/K(\mathbf{t}))$ has order exactly equal to the degree of $g(\mathbf{t}, X)$.

Hence we have

RESULT 3.3.4. *Let K be a Hilbertian field. If a finite group G occurs as a Galois group over $K(\mathbf{t})$, it occurs over K as well.*

This justifies Noether's Strategy as described in the Introduction.

But we can do better:

THEOREM 3.3.5. *Let K be a Hilbertian field, and let $f(\mathbf{t}, X) \in K(\mathbf{t})[X]$ be monic, irreducible and separable. Then there is a Hilbert set of K^r on which the specialisations $f(\mathbf{a}, X) \in K[X]$ of $f(\mathbf{t}, X)$ are well-defined, irreducible and $\mathrm{Gal}(f(\mathbf{a}, X)/K) \simeq \mathrm{Gal}(f(\mathbf{t}, X)/K)$.*

PROOF. Let $\mathbb{M}$ be the splitting field of $f(\mathbf{t}, X)$ over $K(\mathbf{t})$, and let $\Theta \in \mathbb{M}$ be a primitive element with minimal polynomial $g(\mathbf{t}, X) \in K(\mathbf{t})[X]$. The roots of $g(\mathbf{t}, X)$ are then

$$\Theta = \gamma_1(\mathbf{t}, \Theta), \gamma_2(\mathbf{t}, \Theta), \ldots, \gamma_N(\mathbf{t}, \Theta),$$

where $N = [\mathbb{M} : K(\mathbf{t})]$ and $\gamma_i(\mathbf{t}, X) \in K(\mathbf{t})[X]$ has degree $< N$. That $\gamma_i(\mathbf{t}, \Theta)$ is a root of $g(\mathbf{t}, X)$ means that $g(\mathbf{t}, X) \mid g(\mathbf{t}, \gamma_i(\mathbf{t}, X))$, and so we can specialise to ensure that the roots of $g(\mathbf{a}, X)$ are $\theta = \gamma_1(\mathbf{a}, \theta)$, $\gamma_2(\mathbf{a}, \theta)$, …, $\gamma_N(\mathbf{a}, \theta)$, where θ is one of the roots.

Similarly, the roots of $f(\mathbf{t}, X)$ are

$$\varphi_1(\mathbf{t}, \Theta), \ldots, \varphi_n(\mathbf{t}, \Theta),$$

where n is the degree of $f(\mathbf{t}, X)$ and $\varphi_j(\mathbf{t}, X) \in K(\mathbf{t})[X]$ has degree $< N$, and we can specialise to obtain that the roots of $f(\mathbf{a}, X)$ are $\varphi_1(\mathbf{a}, \theta)$, $\ldots$, $\varphi_n(\mathbf{a}, \theta)$.

We know that we can specialise to get

$$\mathrm{Gal}(g(\mathbf{a}, X)/K) \simeq \mathrm{Gal}(g(\mathbf{t}, X)/K(\mathbf{t})).$$

All we need is to ensure that the splitting field of $f(\mathbf{a}, X)$ over K equals the splitting field M of $g(\mathbf{a}, X)$:

Let $\sigma \in \mathrm{Gal}(\mathbb{M}/K(\mathbf{t}))$. σ is given by $\sigma\Theta = \gamma_i(\mathbf{t}, \Theta)$ for some i, and when we specialise properly, $\bar{\sigma}\theta = \gamma_i(\mathbf{a}, \theta)$. Now, for a given j, $\sigma\varphi(\mathbf{t}, \Theta) = \varphi_k(\mathbf{t}, \Theta)$ for a k depending on σ and j, i.e., $\varphi_j(\mathbf{t}, \gamma_i(\mathbf{t}, X)) - \varphi_k(\mathbf{t}, X)$ is divisible by $g(\mathbf{t}, X)$, and by specialising properly, we get $\bar{\sigma}\varphi_j(\mathbf{a}, \theta) = \varphi_k(\mathbf{a}, \theta)$. Doing this for all σ and j, we can obtain that $\bar{\sigma} \in \mathrm{Gal}(M/K)$ permutes the roots of $f(\mathbf{a}, X)$ in exactly the same way as $\sigma \in \mathrm{Gal}(\mathbb{M}/K(\mathbf{t}))$ permutes the roots of $f(\mathbf{t}, X)$. In particular, no $\sigma \neq 1$ leaves the roots of $f(\mathbf{a}, X)$ invariant, and so the splitting field of $f(\mathbf{a}, X)$ is all of M. □

Remark. There is an obvious problem with the Hilbert Irreducibility Theorem: It is not particularly explicit. That is to say, it is not clear how to *find* the points where specialisation yields an irreducible polynomial. And this problem is of course emphasised in Theorem 3.3.5 above, where we need to preserve not only irreducibility but also the Galois group.

One way around this problem, insofar as there is one, is to keep track of how we construct our parametric/generic polynomials, so that we can produce exact conditions afterwards.

Another is to note, by Exercise 3.3(3), that Hilbert sets in $\mathbb{Q}^n$ are dense. Picking a specialisation at random therefore has a fair chance of working.

In any case, the problem is not a serious one.

Regular extensions. A finite Galois extension $\mathbb{M}/K(\mathbf{t})$ is called *regular* (over K), if K is relatively algebraically closed in $\mathbb{M}$, i.e., if no element in $\mathbb{M} \setminus K$ is algebraic over K.

More generally, an extension field $\mathbb{M}$ of K is *regular* over K, if $\mathbb{M}$ and L are linearly disjoint over K for all finite extensions L/K, i.e., if $\mathbb{M} \otimes_K L$ is a field, cf. section A.3 in Appendix A.

The advantage of regular extensions is the following elementary observation:

Proposition 3.3.6. *If $\mathbb{M}/K(\mathbf{t})$ is a regular Galois extension with Galois group $G = \mathrm{Gal}(\mathbb{M}/K(\mathbf{t}))$ and L/K is an arbitrary field extension, the composite $\mathbb{F} = \mathbb{M}L(\mathbf{t})$ is a regular G-extension of $L(\mathbf{t})$, when $\mathbf{t} = (t_1, \ldots, t_n)$ are considered as indeterminates over L.*

Proof. First of all: It is clear that if there is a field extension L/K, for which $\mathbb{F}/L(\mathbf{t})$ is *not* a regular G-extension, there is one where L/K is finitely generated. Thus, it is enough to consider three cases: (1) L/K is finite separable, (2) L/K is purely inseparable of degree $p = \mathrm{char}\, K$, and (3) L/K is rational of degree 1.

Cases (1) and (2) are almost trivial, and in case (3) the only problem is to show that $K(s)$ is relatively algebraically closed in $\mathbb{L}(s)$, if K is relatively algebraically closed in an extension field $\mathbb{L}$:

Assume $u \in \mathbb{L}(s)$ to be algebraic over $K(s)$. We can of course normalise to get that u is integral over $K[s]$, and hence $u \in \mathbb{L}[s]$. (Since $\mathbb{L}[s]$ is integrally closed.) Thus, for suitable $f_0, \dots, f_{r-1} \in K[s]$ we have

$$u^r + f_{r-1}u^{r-1} + \cdots + f_0 = 0.$$

For each $a \in K$, this gives us an equation

$$u(a)^r + f_{r-1}(a)u(a)^{r-1} + \cdots + f_0(a) = 0,$$

and so $u(a) \in K$. If $|K| > \deg u$, this completes the proof: $u \in K[s]$. Otherwise, we take L/K finite with $|L| > \deg u$ and look at $\mathbb{L}L/L$, getting $u \in L[s] \cap \mathbb{L}[s] = K[s]$. □

Thus we have the following consequence of Theorem 3.3.5:

COROLLARY 3.3.7. *If there exists a regular G-extension over K, every Hilbertian field containing K has a G-extension.*

One way of obtaining regular extensions is by generic polynomials:

PROPOSITION 3.3.8. *Let $f(\mathbf{t}, X) \in K(\mathbf{t})[X]$ be a generic polynomial for G-extensions over K. Then the splitting field $\mathbb{M}$ of $f(\mathbf{t}, X)$ over $K(\mathbf{t})$ is a regular G-extension over K.*

PROOF. We have to show that K is relatively algebraically closed in $\mathbb{M}$. Now, if this were not the case, we would have some algebraic subextension $L/K \subseteq \mathbb{M}/K$, and the Galois group $\mathrm{Gal}(f(\mathbf{t}, X)/L(\mathbf{t}))$ were then a proper subgroup of G. Thus, we must show that $f(\mathbf{t}, X)$ has Galois group G over $L(\mathbf{t})$ for all algebraic extensions L/K, and in fact we will do it for *any* extension L/K:

Let L be an extension field of K. If $\mathrm{Gal}(f(\mathbf{t}, X)/L(\mathbf{t}))$ is a proper subgroup of G, the same is true for $\mathrm{Gal}(f(\mathbf{t}, X)/L'(\mathbf{t}))$ for any extension field L' of L. Pick L' to have a G-extension F'/L'. (This is always possible.)

Since $f(\mathbf{t}, X)$ is generic for G-extensions over K, F' is the splitting field over L' of a specialisation $f(\mathbf{a}, X)$ for some $\mathbf{a} \in L'^n$. By Lemma 3.3.1, we have

$$G = \mathrm{Gal}(F'/L') \subseteq \mathrm{Gal}(f(\mathbf{t}, X)/L'(\mathbf{t})) \subseteq \mathrm{Gal}(f(\mathbf{t}, X)/L(\mathbf{t})) \subseteq G.$$

We conclude that $\mathrm{Gal}(f(\mathbf{t}, X)/L(\mathbf{t})) = G$, as desired. □

Thus, loosely speaking, if we know what a G-extension over a Hilbertian field K is supposed to look like, there will be one.

We note the following: If $\mathbb{L}/K(\mathbf{s})$ and $\mathbb{M}/K(\mathbf{t})$ are regular Galois extensions, the extensions $\mathbb{L}(\mathbf{t})/K(\mathbf{s}, \mathbf{t})$ and $\mathbb{M}(\mathbf{s})/K(\mathbf{s}, \mathbf{t})$ are linearly disjoint (i.e., $\mathbb{L}(\mathbf{t}) \cap \mathbb{M}(\mathbf{s}) = K(\mathbf{s}, \mathbf{t})$) and the composite $\mathbb{L}(\mathbf{t})\mathbb{M}(\mathbf{s})/K(\mathbf{s}, \mathbf{t})$ is regular.

REMARK. It follows that a regular G-extension over a Hilbertian field K implies the existence of infinitely many G-extensions of K.

Most of the interest in regular extensions is focused on extensions of $\mathbb{Q}(t)$, i.e., involving only a single indeterminate, due to the fact that this is the kind of regular extensions obtained by algebraic geometry, from function fields of curves. In connection with such extensions, the following conjecture — already mentioned in the Introduction – is of interest:

THE REGULAR INVERSE GALOIS PROBLEM. *Is every finite group is realisable as the Galois group of a regular extension $\mathbb{M}/\mathbb{Q}(t)$?*

Clearly, an affirmative answer to the Regular Inverse Galois Problem would immediately give an affirmative answer to the usual Inverse Galois Problem (for $\mathbb{Q}$) as well.

Since every regular Galois extension $\mathbb{M}/\mathbb{Q}(t)$ specialises to Galois extensions $M/\mathbb{Q}$ with the same Galois group, in effect 'parametrising' an infinite family of Galois extensions of $\mathbb{Q}$, another natural conjecture is that these families cover everything:

THE BECKMANN-BLACK CONJECTURE. (*Cf.* [Be], [Bl1].) *Let G be a finite group. Every G-extension of $\mathbb{Q}$ is obtained by specialising a regular G-extension of $\mathbb{Q}(t)$.*

If a given finite group G satisfies the Beckmann-Black Conjecture, it is said to have the *arithmetic lifting property*. This can of course be formulated for an arbitrary field rather than just $\mathbb{Q}$.

LEMMA 3.3.9. *Let $p(\mathbf{t}, X) \in K(\mathbf{t})[X]$ be a G-polynomial with splitting field $\mathbb{M}$ over $K(\mathbf{t})$. If $\mathbb{M}/K(\mathbf{t})$ contains a subextension $L(\mathbf{t})/K(\mathbf{t})$ coming from an algebraic extension L/K, then L/K is contained in every G-extension M/K obtained by specialising $p(\mathbf{t}, X)$.*

PROOF. Let $R = K[\mathbf{t}, 1/t]$, where $t \in K[\mathbf{t}]$ is a common denominator for the coefficients of $p(\mathbf{t}, X)$, and let S be the integral closure of R in $\mathbb{M}$. If M/K is a G-extension obtained by specialising $p(\mathbf{t}, X)$ in $\mathbf{a} \in K^n$, the specialisation of S in a maximal ideal containing $\ker(\mathbf{t} \mapsto \mathbf{a})$ must contain M, and since M/K is a G-extension, it must equal M. Since S contains L, so does M. □

In particular: If $p(\mathbf{t}, X)$ specialises to give two linearly disjoint G-extensions of K, then $\mathbb{M}/K(\mathbf{t})$ *is* regular.

PROPOSITION 3.3.10. *Let K be a Hilbertian field, and let $p(\mathbf{t}, X) \in K(\mathbf{t})[X]$ give a regular G-extension of $K(\mathbf{t})$. Then there exists a specialisation $q(s, X)$ of $p(\mathbf{t}, X)$ over $K(s)$, such that $q(s, X)$ gives a regular G-extension of $K(s)$, and such that any finitely many prescribed G-extensions of K obtained by specialising $p(\mathbf{t}, X)$ can also be obtained by specialising $q(s, X)$.*

PROOF. Let $p(\mathbf{a}_1, X)$, ..., $p(\mathbf{a}_r, X)$ be the finitely many specialisations. We can assume, by previous remarks, that two of these specialisations give linearly disjoint G-extensions. Now, pick $\mathbf{s} \in K(s)^n$, such that $\mathbf{s}$ specialises to $\mathbf{a}_1, \ldots, \mathbf{a}_r$ for suitable values of s, and let $q(s, X) = p(\mathbf{s}, X)$. Then $q(s, X)$ specialises to $p(\mathbf{a}_1, X)$,..., $p(\mathbf{a}_r, X)$, and so it must be separable. Also, its Galois group must be G, and since it has two linearly disjoint G-specialisations, the splitting field is regular over K. □

Thus, if there is a generic G-polynomial over the Hilbertian field K, then G has the arithmetic lifting property over K.

Symmetric and alternating groups. Let $n \in \mathbb{N}$, and consider the polynomial $f(t,X) = X^n + tX + t \in \mathbb{Q}(t)[X]$. It is irreducible by the Eisenstein Criterion (applied in $\mathbb{Q}[t]$), and so the Galois group $\mathrm{Gal}(f(t,X)/\mathbb{Q}(t))$ is a transitive subgroup of S_n. We note that

$$d(f) = (-1)^{n(n-1)/2} t^{n-1}[(1-n)^{n-1}t + n^n].$$

We reduce modulo the maximal ideal $(t+\frac{1}{2})$ in $\mathbb{Q}[t]$, and look at $f(-\frac{1}{2},X) = X^n - \frac{1}{2}X - \frac{1}{2} \in \mathbb{Q}[X]$. It can be written

$$f(-\tfrac{1}{2},X) = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + \tfrac{1}{2}).$$

The second factor is irreducible, since its roots are the reciprocals of the roots of $X^{n-1} + 2X^{n-2} + \cdots + 2X + 2$, which is irreducible by Eisenstein. Hence, by Proposition 3.3.2, $\mathrm{Gal}(f(t,X)/\mathbb{Q}(t))$ contains a subgroup that fixes one root and permutes the others transitively, i.e., $\mathrm{Gal}(f(t,X)/\mathbb{Q}(t))$ is 2-transitive.[3]

Next, let $s = t + n^n/(1-n)^{n-1}$ and write

$$g(s,X) = f(t,X) = X^n + \big(s - \frac{n^n}{(1-n)^{n-1}}\big)X + \big(s - \frac{n^n}{(1-n)^{n-1}}\big).$$

Clearly,

$$d(g) = (-1)^{n(n-1)/2}(1-n)^{n-1}s\big(s - \frac{n^n}{(1-n)^{n-1}}\big)^{n-1}.$$

Looking at $g(s,X)$ over $\mathbb{C}(\!(s)\!)$, we then have

$$\mathrm{Gal}(g(s,X)/\mathbb{C}(\!(s)\!)) \subseteq \mathrm{Gal}(g(s,X)/\mathbb{Q}(s)) = \mathrm{Gal}(f(t,X)/\mathbb{Q}(t)) \subseteq S_n.$$

Also, since $d(g)$ is not a square in $\mathbb{C}(\!(s)\!)$, $\mathrm{Gal}(g(s,X)/\mathbb{C}(\!(s)\!))$ cannot be trivial. Now, modulo s, we get

$$g(0,X) = X^n - \frac{n^n}{(1-n)^{n-1}}X - \frac{n^n}{(1-n)^{n-1}},$$

and after scaling we are looking at

$$h(X) = X^n - nX + (n-1) \in \mathbb{C}[X].$$

$h(X)$ has 1 as a double root, and $n-2$ simple roots. Thus, by Hensel's Lemma (see e.g. [Ja2, 9.11]), $g(s,X)$ has $n-2$ simple roots in $\mathbb{C}(\!(s)\!)$. This means that $\mathrm{Gal}(g(s,X)/\mathbb{C}(\!(s)\!))$ must act by permuting the remaining two roots, and we conclude that $\mathrm{Gal}(f(t,X)/\mathbb{Q}(t))$ contains a transposition.

It is trivial that the only 2-transitive subgroup of S_n containing a transposition is S_n, and so we have

PROPOSITION 3.3.11. *For all $n \in \mathbb{N}$, the splitting field of X^n+tX+t over $\mathbb{Q}(t)$ is a regular S_n-extension.*

[3]This can also be seen by adjoining a root Θ of $f(t,X)$, note that $\mathbb{Q}(t)(\Theta) = \mathbb{Q}(\Theta)$, and prove that the polynomial $f(t,X)/(X-\Theta)$ is irreducible in $\mathbb{Q}(\Theta)[X]$.

That the splitting field is regular follows from the fact that $d(f)$ is not quadratically equivalent to a rational number.[4] (Alternatively, by noting that if 2-transitivity is proved as indicated in the footnote, everything works over $\mathbb{C}$ as well as over $\mathbb{Q}$.)

COROLLARY 3.3.12. *Let $n \in \mathbb{N}$. Then the polynomial*

$$p(t,X) = \begin{cases} X^n + \dfrac{(-1)^{(n-1)/2}t^2 - n^n}{(n-1)^{n-1}}(X+1), & n \text{ odd} \\ X^n + \dfrac{n^n}{(-1)^{n/2}t^2 + (n-1)^{n-1}}(X+1), & n \text{ even} \end{cases}$$

gives a regular A_n-extension of $\mathbb{Q}(t)$.

PROOF. First, assume n odd. Then the quadratic subextension of the splitting field of $f(t,X) = X^n + tX + t$ over $\mathbb{Q}(t)$ is $\mathbb{Q}(t)(u)$, where

$$u = \sqrt{(-1)^{n(n-1)/2}[(1-n)^{n-1}t + n^n]}.$$

It is obvious that $\mathbb{Q}(t)(u) = \mathbb{Q}(u)$, and thus that the splitting field of $f(t,X)$ over $\mathbb{Q}(u)$ is a regular A_n-extension. So, we let $p(u,X) = f(t,X)$ and express t in terms of u.

Next, assume n even. We start by letting $s = 1/t$. Then the quadratic subextension of the splitting field of $f(1/s,X) = X^n + 1/s\,X + 1/s$ over $\mathbb{Q}(s) = \mathbb{Q}(t)$ is $\mathbb{Q}(s)(v)$, where

$$v = \sqrt{(-1)^{n(n-1)/2}[(1-n)^{n-1} + n^n s]},$$

and it is clear that $\mathbb{Q}(s)(v) = \mathbb{Q}(v)$, meaning that the splitting field of $f(1/s,X)$ over $\mathbb{Q}(v)$ is a regular A_n-extension. So, we let $p(v,X) = f(1/s,X)$. □

In particular, the symmetric and alternating groups occur as Galois groups over all algebraic number fields.

Note that $p(t,X)$ is an expression in t^2 and X, and that therefore obviously the splitting field of $p(t,X)$ over $\mathbb{Q}(t^2)$ is a regular S_n-extension.

More generally, consider a field K in characteristic 0 and an element $a \in K^*$. Then $p(\sqrt{a}\,t, X)$ gives a regular A_n-extension of $K(\sqrt{a})(t) = K(\sqrt{a})(\sqrt{a}\,t)$, and if $a \notin (K^*)^2$ this is an S_n-extension of $K(t)$ having $K(t,\sqrt{a})/K(t)$ as its quadratic subextension. If K is Hilbertian, we can then specialise, i.e., we have

COROLLARY 3.3.13. *Let K be a Hilbertian field in characteristic 0. Then any quadratic extension of K can be embedded in an S_n-extension.*

In connection with regular S_n-extensions, we also have

THEOREM 3.3.14. (HILBERT) *Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial of degree n satisfying the following conditions:*

(i) *The derivative $f'(X)$ is irreducible in $\mathbb{Q}[X]$; and*
(ii) *$f(X)$ assumes distinct values in the zeroes of $f'(X)$.*

Then the splitting field of $f(X) - t \in \mathbb{Q}(t)[X]$ over $\mathbb{Q}(t)$ is a regular S_n-extension.

[4] See section A.1 in Appendix A for the definition of 'quadratically equivalent'.

REMARK. In [Hi], Hilbert proved a somewhat stronger result: Instead of condition (i), it is enough that the roots of $f'(X)$ are simple.

PROOF. We can obviously assume $f(0) = 0$. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X$.

First of all, note that $f(X)-t$ is irreducible over $\mathbb{Q}(t)$, since $-X^n[f(1/X)-t]/t$ is, by the Eisenstein Criterion applied to the prime $1/t$ in $\mathbb{Q}[1/t]$. Thus, the Galois group $\mathrm{Gal}(f(X) - t/\mathbb{Q}(t))$ is a transitive subgroup of S_n.

Next, we let s be a root of $f(X) - t$ over $\mathbb{Q}(t)$. Then $t = f(s)$, and so $\mathbb{Q}(t)(s) = \mathbb{Q}(s)$. Also, $(f(X) - f(s))/(X - s)$ is irreducible in $\mathbb{Q}[s, X]$, since it can be written as a polynomial of degree $n - 1$ in X over $\mathbb{Q}[X - s]$, specialising to $f'(X)$ modulo the prime ideal $(X-s)$. Thus, $\mathrm{Gal}(f(X)-t/\mathbb{Q}(t))$ is 2-transitive in S_n.

Finally, we wish to prove that the Galois group contains a transposition. By translating X and t, we may assume that $f'(0) = 0$, i.e., we have $a_1 = 0$ and $a_2 \neq 0$.

We now look at $f(X) - t$ over $\mathbb{C}(\!(t)\!)$. Modulo t, we have simply $f(X)$, and by assumption $f(X)$ has the double root 0 and $n - 2$ simple roots. Thus, by Hensel's Lemma, we get that $\mathrm{Gal}(f(X) - t/\mathbb{C}(\!(t)\!))$ is at most cyclic of order 2, generated by a transposition. On the other hand, using the resultant formula for the discriminant of $f(X) - t$, we see that

$$d(f(X) - t) = \pm 2a_2 t\,[d(f/X) + t \cdot (\text{polynomial in } t)],$$

which is not a square in $\mathbb{C}(\!(t)\!)$. Thus, the Galois group over $\mathbb{C}(\!(t)\!)$ is non-trivial.

Regularity follows, since the last part of the argument demonstrates that the discriminant of $f(X) - t$ is not a square over an extension field containing $\mathbb{C}$, so that it cannot be quadratically equivalent to a rational number. □

REMARK. There is an interesting analogy between realisations of the symmetric group S_n as Galois group over function fields like $\mathbb{Q}(t)$ or $\mathbb{C}(t)$ and over $\mathbb{Q}$.

In the number fields case there are two main tools:

(A) Minkowski's theorem that any proper algebraic extension of $\mathbb{Q}$ has at least one ramified prime.

(B) Hilbert's theory of inertia groups, ramification groups, etc.

By these results one obtains the following (cf. [Ko]):

PROPOSITION 3.3.15. *The Galois group of an irreducible polynomial $f(X) \in \mathbb{Q}[X]$ of degree n is S_n if the discriminant $d(f)$ of $f(X)$ is equal to the discriminant of a quadratic number field. In this case the splitting field of $f(X)$ is an unramified A_n-extension of $\mathbb{Q}(\sqrt{d(f)})$.*

If there is a prime number p such that p but not p^2 divides $d(f)$, then the Galois group of $f(X)$ over $\mathbb{Q}$ contains a transposition. Therefore, in this case the Galois group must be the symmetric group S_n if n is assumed to be a prime number.

In the function field case the analogous tools are:

(A') For the function field $\mathbb{C}(t)$ there is no proper algebraic extension of $\mathbb{C}(t)$ which is unramified at all places (with $\mathbb{C}$ as residue field) except at ∞. (In geometric terms: There is no unramified covering of the affine line $\mathbb{A}^1$ over $\mathbb{C}$.)

(B') The Hilbert theory of inertia groups and ramification groups, suitably modified for function fields.

From this one derives the following:

PROPOSITION 3.3.16. *Let $f(t, X)$ be an irreducible polynomial in $\mathbb{Q}[t, X]$ or $\mathbb{C}[t, X]$, with discriminant $d(f)$ (with respect to x). $d(f)$ is polynomial in t. If $d(f)$ has at least one simple root, then the Galois group of $f(t, X)$ with respect to X contains a transposition. Hence the Galois group will be the symmetric group S_n if the degree of $f(t, x)$ (with respect to X) is n, where n is a prime number.*

If the above discriminant $d(f)$ no multiple roots at all, then the Galois group of $f(t, X)$ with respect to X is S_n, where n is the degree of $f(t, X)$ with respect to X, which this time can be an arbitrary positive integer.

The latter polynomials include all the polynomials given above, as well as the 'Morse polynomials' introduced by Hilbert (i.e., the polynomials mentioned in the Remark following Theorem 3.3.14 above, cf. also [Se2, p. 39]). But the set-back here is that (A') cannot be proved by purely algbraic means, so the method applied here is less elementary than the one used above.

The above shows the abundance of polynomials with the symmetric group as Galois group. For instance, using the fact that the discriminant of a trinomial $f(X) = X^n + pX^m + q$, where $n > m > 0$ and $\gcd(n, m) = 1$, is

$$d(f) = (-1)^{n(n-1)/2} q^{m-1} \{n^n q^{n-m} - (-1)^n (n-m)^{n-m} m^m p^n\},$$

one obtains a large class of polynomials with S_n as Galois group. To take a simple explicit example, the polynomial $x^n + tx^m + 1$ has S_n as Galois group (both over $\mathbb{Q}(t)$ and $\mathbb{C}(t)$) if and only of $\gcd(n, m) = 1$.

Exercises

EXERCISE 3.1. Let K be a Hilbertian field, and let $f(X), g(X) \in K[X]$. Assume: For all $a \in K$ there is a $b \in K$ such that $f(a) = g(b)$. Prove that $f(X) = g(h(X))$ for an $h(X) \in K[X]$. In particular: Prove that $f(X)$ is a square in $K[X]$ if it assumes only square values in K.

EXERCISE 3.2. Let K be a Hilbertian field. Prove that the rational function field $K(t)$ is again Hilbertian.

EXERCISE 3.3. (1) Let $D \subseteq \mathbb{C}$ be an open disc centered on the real axis, and let $f_1, \ldots, f_n \colon D \to \mathbb{C}$ be meromorphic functions on D. Assume that they are algebraic over $\mathbb{Q}(t)$, but that none of them are in $\mathbb{Q}(t)$ itself. Prove that the set

$$\{q \in \mathbb{Q} \cap D \mid f_1(q), \ldots, f_n(q) \text{ irrational}\}$$

is dense in $\mathbb{Q} \cap D$. [Hint: Use the proof of the Hilbert Irreducibility Theorem.]

(2) Prove that a Hilbert set in $\mathbb{Q}$ is dense. (Thus, of course, establishing the Irreducibility Theorem again.)

(3) Prove that a Hilbert set in $\mathbb{Q}^n$ is dense.

EXERCISE 3.4. Let $\mathbf{s} = (s_1, \dots, s_n)$ and $\mathbf{t} = (t_1, \dots, t_n)$ be sets of indeterminates, and define the *Kronecker resolvent* W as

$$W(X) = \prod_{\sigma \in S_n} \big(X - \sum_{i=1}^{n} s_i t_{\sigma i}\big) \in \mathbb{Z}[\mathbf{s}, \mathbf{t}, X].$$

(1) Prove that the coefficients of $W(X)$ as a polynomial in $\mathbf{t}$ and X are symmetric in the s_i's, and hence that we can write

$$W(X) = W(\mathbf{e})(X) = X^{n!} + h_{n!-1}(\mathbf{e}, \mathbf{t})X^{n!-1} + \cdots + h_0(\mathbf{e}, \mathbf{t})$$

for polynomials $h_i(\mathbf{e}, \mathbf{t}) \in \mathbb{Z}[\mathbf{e}, \mathbf{t}]$, where $\mathbf{e} = (e_1, \dots, e_n)$ are the elementary symmetric symbols in the s_i's.

(2) Let K be a field, and let $f(X) \in K[X]$ have degree n and no multiple roots. Define the Kronecker resolvent of $f(X)$ as the polynomial

$$W(f)(X) = W(\mathbf{a})(X) \in K[\mathbf{t}, X],$$

where $\mathbf{a} = (a_1, \dots, a_n)$ are the elementary symmetric symbols in the roots of $f(X)$, i.e., $\pm$ the coefficients. Prove that the irreducible factors of $W(f)(X)$ all have degree $|\operatorname{Gal}(f/K)|$.

(3) Let K be a field. Prove that $W(\mathbf{s})(X) \in K(\mathbf{e})[\mathbf{t}, X]$ is irreducible.

(4) Let $f(X) \in \mathbb{Q}[X]$ be monic of degree n with n distinct real roots. Prove that a polynomial $g(X)$ obtained from $f(X)$ by changing the coefficients by less than some $\delta > 0$ will still have n distinct real roots. Then prove the existence of S_n-extensions of $\mathbb{Q}$ contained in $\mathbb{R}$.

EXERCISE 3.5. Let G be a finite group.

(1) Show that G can be realised as the Galois group of an extension M/K of subfields of $\mathbb{R}$.

(2) Assume the existence of a generic G-polynomial over $\mathbb{Q}$. Prove that there is a G-extension of $\mathbb{Q}$ contained in $\mathbb{R}$.

EXERCISE 3.6. Let $\mathbb{M}/\mathbb{Q}(t)$ be a regular quadratic extension. Prove that, for some $n \in \mathbb{N}$, $\mathbb{M}/\mathbb{Q}(t)$ cannot be embedded in a C_{2^n}-extension. [Hint: For some irreducible $\pi \in \mathbb{Q}[t]$, the π-adic valuation is ramified in $\mathbb{M}/\mathbb{Q}(t)$. It follows that it is completely ramified in any C_{2^n}-extension of $\mathbb{Q}(t)$ containing $\mathbb{M}$. Arguing as in [G&J, 2.4], we get the primitive $2^{n\,\text{th}}$ roots of unity in $\mathbb{Q}[t]/(\pi)$.]

EXERCISE 3.7. (1) Let n be odd. Prove that the splitting field of

$$X^n + \big((-1)^{(n-1)/2} n t^2 - 1\big)(nX + (n-1))$$

over $\mathbb{Q}(t)$ is a regular A_n-extension.

(2) Let $f(X) = X^5 + (5h^2 - 1)(5X + 4)$. Prove that $\operatorname{Gal}(f/\mathbb{Q}) \simeq A_5$ if $h \equiv \pm 1 \pmod{21}$.

EXERCISE 3.8. Let n be even. Prove that the splitting field of

$$X^n + nX^{n-1} + \big((-1)^{n/2} t^2 + (n-1)^{n-1}\big)$$

over $\mathbb{Q}(t)$ is a regular A_n-extension.

CHAPTER 4

Galois Theory of Commutative Rings

The usual — and well-known — Galois theory of fields generalises to a Galois theory of commutative rings. This generalisation, first described by Chase, Harrison and Rosenberg in [CH&R], is a convenient tool in the study of generic polynomials, for reasons that will become clear in Chapter 5 below.

This chapter gives a self-contained introduction to the Galois theory of commutative rings. The fundamental idea is very simple: Let a finite group G act on a commutative ring S as automorphisms, and consider S/S^G to be a Galois extension if all the inertia groups are trivial, cf. section 3.3 of Chapter 3.

4.1. Ring Theoretic Preliminaries

Let R be a commutative ring. In the tradition of commutative algebra, we assume all rings to have a unit element, all subrings to share this unit element, and all ring homomorphisms to preserve it. In particular, all modules are supposed to be unitary.

A standard reference for commutative algebra is Atiyah-MacDonald [A&M].

LEMMA 4.1.1. *Let M be a finitely generated R-module, and let $\mathfrak{m}$ be a maximal ideal in R. If $\mathfrak{m}M = M$, then $aM = 0$ for some $a \in R \setminus \mathfrak{m}$*

PROOF. Localising, we have $\mathfrak{m}_\mathfrak{m} M_\mathfrak{m} = M_\mathfrak{m}$. That $aM = 0$ for an $a \in R \setminus \mathfrak{m}$ simply means $M_\mathfrak{m} = 0$. Assume $M_\mathfrak{m} \neq 0$, and let $m_1, \ldots, m_n \in M_\mathfrak{m}$ be a minimal generating set. Then $m_1 = a_1 m_1 + \cdots + a_n m_n$ for suitable $a_1, \ldots, a_n \in \mathfrak{m}$, and so $(1-a_1)m_1 = a_2 m_2 + \cdots + a_n m_n$. Since $1-a_1$ is invertible in $R_\mathfrak{m}$, $M_\mathfrak{m}$ is generated by $m_2, \ldots, m_n$, contradicting the minimality. We conclude that $M_\mathfrak{m} = 0$. □

PROPOSITION 4.1.2. *Let M be a finitely generated R-module, and let $\mathfrak{a}$ be an ideal in R. Then $\mathfrak{a}M = M$ if and only if $R = \operatorname{ann}_R M + \mathfrak{a}$.*

PROOF. 'If' is clear.

'Only if': Assume $\operatorname{ann}_R M + \mathfrak{a}$ to be a proper ideal. Then $\operatorname{ann}_R M + \mathfrak{a} \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in R, and hence $\mathfrak{m}M = M$. But this means that $aM = 0$ for some $a \in R \setminus \mathfrak{m}$, contraditing $\operatorname{ann}_R M \subseteq \mathfrak{m}$. □

NAKAYAMA'S LEMMA. *Let M be a finitely generated R-module, and let N be a submodule such that $M = \mathfrak{m}M + N$ for all maximal ideals $\mathfrak{m}$ in R. Then $M = N$.*

PROOF. Replacing M by M/N, we must prove: If $\mathfrak{m}M = M$ for all $\mathfrak{m}$, then $M = 0$. But by the above Proposition, we have $\operatorname{ann}_R M + \mathfrak{m} = R$ for all $\mathfrak{m}$, i.e., $\operatorname{ann}_R M \not\subseteq \mathfrak{m}$, and hence $\operatorname{ann}_R M = R$ and $M = 0$. □

LEMMA 4.1.3. *Let P be an R-module. Then P is (finitely generated) projective, if and only if there exists (finite) families $(p_i)_i$ and $(f_i)_i$ of elements $p_i \in P$ and R-homomorphisms $f_i \colon P \to R$, such that $p = \sum_i f_i(p)p_i$ for all $p \in P$.*

PROOF. 'If': Let F be the free R-module with basis $(e_i)_i$, and define $\pi \colon F \to P$ by $\pi(e_i) = p_i$ and $i \colon P \to F$ by $i(p) = \sum_i f_i(p)e_i$. Then $\pi \circ i = 1_P$, and so $F \simeq P \oplus \ker \pi$.

'Only if': $F = P \oplus Q$ is free for some R-module Q. Let $(e_i)_i$ be a basis, and write $e_i = p_i + q_i$ with $p_i \in P$, $q_i \in Q$. Let $\pi_i \colon F \to R$ be the i^{th} coordinate function, and let $f_i = \pi_i|_P$. For $p \in P$, we then have

$$\begin{aligned} p &= \sum_i \pi_i(p)e_i = \sum_i f_i(p)(p_i + q_i) \\ &= \sum_i f_i(p)p_i + \sum_i f_i(p)q_i = \sum_i f_i(p)p_i, \end{aligned}$$

since $\sum_i f_i(p)q_i \in P \cap Q = 0$. □

For an R-module M, we define $I_R M$ as the ideal generated by the images of the elements of $\operatorname{Hom}_R(M, R)$.

COROLLARY 4.1.4. *If P is a finitely generated projective R-module, then $R = \operatorname{ann}_R P + I_R P$.*

PROOF. By the Lemma, $I_R P \cdot P = P$. Proposition 4.1.2 gives the result. □

PROPOSITION 4.1.5. *Let P be a finitely generated projective R-module. Then $\operatorname{Hom}_R(P, R) \otimes_R M \simeq \operatorname{Hom}_R(P, M)$ by $f \otimes m \mapsto [p \mapsto f(p)m]$ for all R-modules M.*

PROOF. Let $P = P' \oplus P''$. Then the isomorphism holds for P, if and only if it holds for both P' and P''. Since it is trivial for $P = R$, we get it for finitely generated free modules, and then for finitely generated projective modules. □

Finally, a definition:

DEFINITION 4.1.6. Let M be an R-module. Then we say that M has *rank* n, $n \in \mathbb{N}$, written $\operatorname{rank}_R M = n$, if $M/\mathfrak{m}M$ has dimension n over $R/\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ in R.

4.2. Galois Extensions of Commutative Rings

We can now define the concept of a Galois extension of a commutative ring R. Our approach follows [D&I, Ch. III §1] and [Sa1]. (Additional references are the more recent [Gr] and the original paper [CH&R, 1965].)

DEFINITION 4.2.1. Let S/R be an extension of commutative rings, i.e., R is a subring of S, and let G be a finite group acting as R-algebra automorphisms on S. Then we define S^G as the subring

$$S^G = \{s \in S \mid \forall \sigma \in G\colon \sigma s = s\},$$

and say that S/R is a *Galois extension with group* G, if

(i) $S^G = R$, and
(ii) for any maximal ideal $\mathfrak{m}$ in S and any $\sigma \in G \setminus \{1\}$, there is an $s \in S$ such that $\sigma s - s \notin \mathfrak{m}$.

REMARKS. (1) From (ii) it immediately follows that G acts *faithfully* on S, i.e., that no $\sigma \in G\setminus\{1\}$ acts as the identity. Moreover, if S/R is a field extension, this is *all* condition (ii) means, and so this definition extends the usual concept of Galois field extensions.

(2) If K is a field, the K-algebra automorphisms on K^n are exactly the permutations of the coefficients, i.e., $\operatorname{Aut}_K K^n = S_n$. It is easily seen that K^n/K is a Galois extension with group G if and only if G is transitive in S_n of order n. In particular, an extension S/R of commutative rings can be a Galois extension with respect to several different groups.

(3) Let S/R be a Galois extension with group G, and assume that R and S are domains with quotient fields K and L, respectively. Then the G-action extends to L, and L/K is again a Galois extension with group G. It follows that $G = \operatorname{Aut}_K L = \operatorname{Aut}_R S$, and so G *is* given by S/R in this case. More generally, G is given by S/R (as $\operatorname{Aut}_R S$) if S is *connected*, i.e., with no idempotents other than 0 and 1. See [D&I, Ch. III Cor. 1.7] for proof.

(4) Let $K/\mathbb{Q}$ be a finite Galois extension. It is then clear that the automorphisms on the Dedekind ring $\mathcal{O}_K$ are exactly the restrictions of the elements in $G = \operatorname{Gal}(K/\mathbb{Q})$. However, $\mathcal{O}_K/\mathbb{Z}$ is not a Galois extension (unless $K = \mathbb{Q}$), since condition (ii) is not satisfied for ramified primes. In fact, condition (ii) can be thought of as saying 'the G-action is faithful and S/R is unramified'.

PROPOSITION 4.2.2. *As above, let S/R be an extension of commutative rings, and let G be a finite group acting on S by R-algebra automorphisms. Then S/R is a Galois extension with group G, if and only if*

(i) $S^G = R$, *and*
(ii) *there exist $x_i, y_i \in S$, such that $\sum_i x_i \sigma y_i = \delta_{\sigma,1}$ for all $\sigma \in G$.*[1]

PROOF. First, assume that S/R is a Galois extension with group G, and let $\sigma \in G \setminus \{1\}$. The ideal generated by $(1-\sigma)S$ is all of S, and so we have $x_1(\sigma), \dots, x_n(\sigma), y_1(\sigma), \dots, y_n(\sigma) \in S$ with $\sum_{i=1}^n x_i(\sigma)(y_i(\sigma) - \sigma y_i(\sigma)) = 1$. Let $x_{n+1}(\sigma) = -\sum_{i=1}^n x_i(\sigma)\sigma y_i(\sigma)$ and $y_{n+1}(\sigma) = 1$. Then $\sum_i x_i(\sigma)\rho y_i(\sigma) = \delta_{1,\rho}$ for $\rho = 1, \sigma$.

[1] δ is the Kronecker delta, i.e., $\delta_{\sigma,1}$ is 1 when $\sigma = 1$ and 0 otherwise.

Picking such sets $x_i(\sigma), y_i(\sigma)$ for all $\sigma \in G \setminus \{1\}$, we get the desired x_i's and y_i's by expanding the product

$$\prod_{\sigma \neq 1} \Big(\sum_{i=1}^{n_\sigma} x_i(\sigma) \rho y_i(\sigma)\Big) = \delta_{\rho,1},$$

since clearly this results in a sum of the desired kind. The x_i's will then be all products of $x_j(\sigma)$'s for σ running through $G \setminus \{1\}$, and similarly for the y_i's.

Conversely, assume (i) and (ii) satisfied, and let $\mathfrak{m}$ be a maximal ideal in S. If, for some $\sigma \in G \setminus \{1\}$, we had $(1-\sigma)S \subseteq \mathfrak{m}$, we would get $1 = \sum_i x_i(y_i - \sigma y_i) \in \mathfrak{m}$. □

Until further notice, we will let S/R be a Galois extension with group G.

THE DEDEKIND INDEPENDENCE THEOREM. *The elements in G are linearly independent over S.*

PROOF. Assume $\sum_\sigma s_\sigma \, \sigma x = 0$ for all $x \in S$. Then

$$s_\sigma = \sum_\tau s_\tau \tau \Big(\sum_i x_i \, \tau^{-1} \sigma y_i\Big) = \sum_i \Big(\sum_\tau s_\tau \tau x_i\Big) \sigma y_i = 0,$$

as wanted. □

Thus, if we let $S\{G\}$ denote the *twisted group ring* of G over S, i.e., the elements in $S\{G\}$ has the form $\sum_\sigma s_\sigma \sigma$ for $s_\sigma \in S$ and the multiplication is defined by $(s\sigma)(t\tau) = s\sigma t \, \sigma\tau$, we have a ring monomorphism $j\colon S\{G\} \to \operatorname{End}_R S$ given by $j(\sum_\sigma s_\sigma \sigma)\colon x \mapsto \sum_\sigma s_\sigma \, \sigma x$.

PROPOSITION 4.2.3. *$j\colon S\{G\} \to \operatorname{End}_R S$ is an isomorphism.*

PROOF. Let $f \in \operatorname{End}_R S$, and let $s_\sigma = \sum_i f(x_i) \, \sigma y_i$. Then

$$\begin{aligned} f(x) &= f\Big(\sum_{i,\sigma} x_i \, \sigma y_i \, \sigma x\Big) = \sum_i f(x_i) \sum_\sigma \sigma(y_i x) \\ &= \sum_{\sigma,i} f(x_i) \, \sigma y_i \, \sigma x = \sum_\sigma s_\sigma \, \sigma x \end{aligned}$$

and so $f = j(\sum_\sigma s_\sigma \sigma)$. □

We define the *trace* $\operatorname{Tr}_{S/R}\colon S \to R$ by $\operatorname{Tr}_{S/R}(x) = \sum_\sigma \sigma x$.

PROPOSITION 4.2.4. *Every R-linear map $f\colon S \to R$ has the form $f(x) = \operatorname{Tr}_{S/R}(cx)$ for a unique $c \in S$.*

PROOF. Clearly, $f(x) = \sum_\sigma s_\sigma \sigma x$ for some choice of s_σ's in S, since f is R-linear from S into $R \subseteq S$. As $f(x) \in R$ for all x, we have $\rho f(x) = f(x)$ for all $\rho \in G$, and hence $s_\sigma = \rho s_{\rho^{-1}\sigma}$ or $s_\sigma = \sigma s_1$, i.e., we can let $c = s_1$. □

In other words: $\operatorname{Hom}_R(S, R)$ is free of rank 1 over S with $\operatorname{Tr}_{S/R}$ as its generator.[2]

LEMMA 4.2.5. *S is finitely generated projective as an R-module.*

[2]Alternatively: $\operatorname{Tr}_{S/R}\colon S \to R$ is a *duality*.

PROOF. We let $f_i(s) = \sum_\sigma \sigma(sy_i)$. Then $s = \sum_i f_i(s)x_i$ for all s, and so S is finitely generated projective by Lemma 4.1.3. □

PROPOSITION 4.2.6. *Again, let S/R be an extension of commutative rings, and let the finite group G act on S by R-algebra automorphisms. Then S/R is a Galois extension with group G, if and only if*

(i) *$S^G = R$, and*
(ii) *the map $\ell\colon s \otimes t \mapsto (s\,\sigma t)_\sigma$ is an isomorphism $S \otimes_R S \simeq S^{(G)}$, where $S^{(G)}$ is the direct product over G of copies of S.*

PROOF. First, assume that S/R is a Galois extension with group G. Then we have isomorphisms

$$S \otimes_R S \simeq S \otimes_R \mathrm{Hom}_R(S, R) \simeq \mathrm{Hom}_R(S, S) \simeq S^{(G)}$$

given by $s \otimes t \mapsto s \otimes \mathrm{Tr}_{S/R}(t\cdot)$, $s \otimes f \mapsto [x \mapsto sf(x)]$ and $f \mapsto (s_\sigma)_\sigma$, where $f(x) = \sum_\sigma s_\sigma \sigma x$. The composite map is ℓ.

On the other hand, if $\sum_i x_i \otimes y_i = \ell^{-1}(\delta_{\sigma,1})_\sigma$, we get condition (ii) of Proposition 4.2.2. □

PROPOSITION 4.2.7. *$\mathrm{Tr}_{S/R}\colon S \to R$ is surjective.*

PROOF. By Corollary 4.1.4, we have $I_R S = R$, and so there exists $g_j \in \mathrm{Hom}_R(S, R)$ and $s_j \in S$, such that $1 = \sum_j g_j(s_j)$. Now

$$1 = \sum_j g_j(s_j) = \sum_j \mathrm{Tr}_{S/R}(c_j s_j) = \mathrm{Tr}_{S/R}(\sum_j c_j s_j).$$

This completes the proof, since $\mathrm{Tr}_{S/R}$ is R-linear. □

COROLLARY 4.2.8. *R is an R-direct summand in S.*

THEOREM 4.2.9. *If R is an R'-algebra, and T is another commutative R'-algebra, then $S \otimes_{R'} T/R \otimes_{R'} T$ is a Galois extension with group G, when $\sigma \in G$ is identified with $\sigma \otimes 1 \in \mathrm{Aut}_{R\otimes_{R'}T}(S \otimes_{R'} T)$. Furthermore, if U/T is a Galois extension with group H, then $S \otimes_{R'} U/R \otimes_{R'} T$ is a Galois extension with group $G \times H$, acting by $(\sigma, \tau)(s \otimes u) = \sigma s \otimes \tau u$.*

PROOF. $R \otimes_{R'} T \subseteq S \otimes_{R'} T$, since R is an R'-direct summand of S. Since $x_i \otimes 1, y_i \otimes 1 \in S \otimes_{R'} T$ with $\sum_i (x_i \otimes 1)\sigma(y_i \otimes 1) = \delta_{\sigma,1}$, we have condition (ii) of Proposition 4.2.2. It remains to prove $R \otimes_{R'} T = (S \otimes_{R'} T)^G$: Since $S \otimes_{R'} T/(S \otimes_{R'} T)^G$ is Galois with group G, the trace is onto. But the trace of $s \otimes t$ is $\mathrm{Tr}_{S/R}(s) \otimes t \in R \otimes_{R'} T$. Thus, we have the desired equality.

As for the second part of the theorem: It is trivial that $G \times H$ acts on $S \otimes_{R'} U$, and that condition (ii) of Proposition 4.2.2 is satisfied. Since $S \otimes_{R'} U/R \otimes_{R'} U$ is a Galois extension with group G, we have $(S \otimes_{R'} U)^{G\times 1} = R \otimes_{R'} U$. Similarly, we have $(R \otimes_{R'} U)^{1\times H} = R \otimes_{R'} T$, from which we get $(S \otimes_{R'} U)^{G\times H} = R \otimes_{R'} T$. □

In particular, if T/R is a commutative algebra, $S \otimes_R T/T$ is a Galois extension with group G, and if T/R is a Galois extension with group H, $S \otimes_R T/R$ is a Galois extension with group $G \times H$.

COROLLARY 4.2.10. *S has rank $|G|$ as an R-module.*

PROOF. First: If R is a field, we have

$$(\dim_R S)^2 = \dim_R S \otimes_R S = \dim_R S^{(G)} = |G| \dim_R S,$$

and since $\dim_R S < \infty$, the result follows.

In the general case, we let $\mathfrak{m}$ be a maximal ideal in R. Then $S/\mathfrak{m}S$ is a Galois extension over $R/\mathfrak{m}$ with group G by Theorem 4.2.9, and hence $\dim_{R/\mathfrak{m}} S/\mathfrak{m}S = |G|$. □

REMARK. If the R-algebra S is finitely generated free as an R-module, we have a *trace* $\mathrm{Tr}_{S/R}\colon S \to R$ defined in the usual way: $\mathrm{Tr}_{S/R}(s)$ is the trace of the linear map $x \mapsto sx$ on S. Using Proposition 4.2.6, it is not hard to see that this trace coincides with the one already defined, when S/R is a Galois extension with group G.

Thus, we have the following: Let S/R be a Galois extension with group G. For every prime ideal $\mathfrak{p}$ in R, the localisation $S_\mathfrak{p}/R_\mathfrak{p}$ is then a Galois extension with group G as well. Also, $S_\mathfrak{p}$ is free over $R_\mathfrak{p}$ of rank $n = |G|$ (by a standard argument), and the trace (defined either way) is a duality. In other words, S/R is an *étale algebra*. This is reasonable, as étale algebras can be thought of as generalising separable field extensions, and we certainly expect Galois extensions to be separable.

THEOREM 4.2.11. *Let S/R be a Galois extension with group G. Then S/S^H is Galois with group H for $H \subseteq G$. Also, if $S^{H_1} = S^{H_2}$ for subgroups H_1 and H_2, then $H_1 = H_2$. Finally, S^N/R is a Galois extension with group G/N if $N \triangleleft G$.*

PROOF. The first part is obvious from Definition 4.2.1.

Next, let H_1 and H_2 be subgroups with $S^{H_1} = S^{H_2}$, and let H be the subgroup generated by H_1 and H_2. Then $S^H = S^{H_1}$, and consequently $|H| = \mathrm{rank}_{S^H} S = \mathrm{rank}_{S^{H_1}} S = |H_1|$, i.e., $H_1 = H$. Similarly, $H_2 = H$.

Now, if $N \triangleleft G$, G/N acts on S^N. Of the conditions in Proposition 4.2.2, (i) is obvious, and we only need to prove (ii):

$\ell\colon S \otimes_R S \to S^{(G)}$ is an isomorphism, and so there exists $x \in S \otimes_R S$ with $\ell(x)_\sigma = 1$ for $\sigma \in N$ and $= 0$ for $\sigma \notin N$. Now, $S \otimes_R S/S^N \otimes_R S^N$ is a Galois extension with group $N \times N$, and the action of $N \times N$ on $S \otimes_R S$ corresponds to $(\sigma, \tau)(s_\rho)_\rho = (\sigma s_{\sigma^{-1}\rho\tau})_\rho$ on $S^{(G)}$. Thus, x is invariant, i.e., $x \in S^N \otimes_R S^N$, and we can pick $x_j, y_j \in S^N$ such that $x = \sum_j x_j \otimes y_j$. □

REMARK. Let L/K be a Galois field extension with Galois group G. Then $L[X]/K[X]$ is a Galois extension with group G as well. Let $A = \{f(X) \in L[X] \mid f(0) \in K\}$. A is obviously a subalgebra of $L[X]$, but is not of the form $L[X]^H$ for any subgroup H of G (provided $L \neq K$, of course). Thus, the correspondance $H \mapsto S^H$ from subgroups to subalgebras is not in general onto.

COROLLARY 4.2.12. *Let S/R be a Galois extension with group G, and let H be a subgroup of G. Then S^H is finitely generated projective as an R-module, and* $\mathrm{rank}_R S^H = [G : H]$.

PROOF. Since S^H is an S^H-direct summand of S, it is in particular an R-direct summand. Thus, S^H is finitely generated projective.

As for the rank: Since $(S/\mathfrak{m}S)^H = S^H/\mathfrak{m}S^H$ for any maximal ideal $\mathfrak{m}$ in R, we may assume R to be a field. Thus, S^H is free over R with some rank d.

Looking at $S \otimes_R S/S$, with G acting on the second copy of S, we have that $(S \otimes_R S)^H = S \otimes_R S^H$, and so $(S \otimes_R S)^H$ is free over S of rank d. However, $S \otimes_R S \simeq S^{(G)}$ as an S-module, and the G-action carries over as $\sigma(s_\rho)_\rho = (s_{\rho\sigma})_\rho$, and so it is easy to see that $(S \otimes_R S)^H$ has rank $[G:H]$ over S. □

Now, let S/R be a Galois extension with group H, and let G be a finite group containing H. We know that G permutes the cosets σH by left multiplication, and it is possible to extend H's action on S to an action of G on the direct sum of $d = [G:H]$ copies of S in accordance with this permutation action:

First, let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_d \in G$ represent the cosets σH in G. For convenience, we write the direct sum of copies of S as $S\varepsilon_1 \oplus \cdots \oplus S\varepsilon_d$. Thus, $\varepsilon_1, \ldots, \varepsilon_d$ are orthogonal idempotents in the new R-algebra, and we want to define a G-action by demanding that

$$\sigma(s\varepsilon_1) = (hs)\varepsilon_i$$

when $\sigma = \sigma_i h$, $h \in H$. (This is where it is convenient to have $\sigma_1 = 1$, so that 'dividing' σ_1's action between s and ε_1 does not pose a problem.) Since $s\,\varepsilon_i = \sigma_i(s\,\varepsilon_1)$, we must then have that

$$\sigma(s\,\varepsilon_i) = \sigma\sigma_i(s\,\varepsilon_1) = h_{\sigma,i} s\,\varepsilon_{\sigma(i)},$$

where where $\sigma\sigma_i = \sigma_{\sigma(i)} h_{\sigma,i}$ for $h_{\sigma,i} \in H$. Writing this out in full, we see that

$$\sigma(\sum_{i=1}^{d} s_i\,\varepsilon_i) = \sum_{i=1}^{d} h_{\sigma,\sigma^{-1}(i)} s_{\sigma^{-1}(i)}\,\varepsilon_i$$

for $\sigma \in G$ and $s_i \in S$. It is easily seen that this *does* define a G-action on the R-algebra

$$\mathrm{Ind}_H^G(S) = \bigoplus_{i=1}^{d} Se_i.$$

We call $\mathrm{Ind}_H^G(S)/R$ the *induced algebra*.

Remarks. (1) In deriving the above G-action, it was practical to assume $\sigma_1 = 1$. However, once we have the formula for $\sigma(\sum_o s_i\,\varepsilon_i)$, we see that it works for *any* set of coset representatives.

(2) If $\tau_i = \sigma_i h_i'$, $h_i' \in H$, is another set of coset representative, and $\bigoplus_i S\delta_i$ is defined as above, $s\varepsilon_i \mapsto h_i'^{-1} s\,\delta_i$ is an isomorphism preserving the G-action. Hence, $\mathrm{Ind}_H^G(S)$ is well-defined.

Proposition 4.2.13. *The induced algebra* $\mathrm{Ind}_H^G(S)/R$ *is a Galois extension with group* G.

Proof. It is trivial to check the definition: (i) An element $s = \sum_i se_i \in \mathrm{Ind}_H^G(S)^G$ is in particular invariant under H, from which it follows that $s_1 \in S^H = R$. Applying $\sigma_2, \ldots, \sigma_d$ then proves that $s = \sum_i s_1\varepsilon_i = s_1 \in R$.

(ii) A maximal ideal in $\mathrm{Ind}_H^G(S)$ has the form $\mathfrak{m}\varepsilon_j \oplus \bigoplus_{i\neq j} S\varepsilon_i$ for a maximal ideal $\mathfrak{m}$ in S. If $\sigma \in G \setminus \{1\}$ maps ε_j to itself, we can pick s in $S\varepsilon_j$ in accordance

with the definition, since S/R is a Galois extension. Otherwise, we can let $s = \varepsilon_j$. □

4.3. Galois Algebras

Let K be a field.

DEFINITION 4.3.1. A Galois extension of a field is called a *Galois algebra*.

REMARK. Galois algebras were introduced by Hasse in [Hs1, Hs2, 1947–48] to deal with Galois theoretical embedding problems. For a more comprehensive treatment of Galois algebras in that context, we refer to [IL&F].

Now, let S/K be a Galois algebra with group G, and $\mathfrak{m}$ be a maximal ideal in S. Let $H = \{\sigma \in G \mid \sigma\mathfrak{m} = \mathfrak{m}\}$, and let $\sigma_1 = 1, \dots, \sigma_d \in G$ represent the cosets σH in G. Then $\sigma_1\mathfrak{m} = \mathfrak{m}, \dots, \sigma_d\mathfrak{m}$ are exactly the different images of $\mathfrak{m}$ under G. Let $\mathfrak{a} = \bigcap_i \sigma_i\mathfrak{m}$. Then $\sigma\mathfrak{a} = \mathfrak{a}$ for $\sigma \in G$, and so G acts on $S/\mathfrak{a}$. Since condition (ii) of Proposition 4.2.2 is trivial, we conclude that $S/\mathfrak{a}$ is a Galois extension of $(S/\mathfrak{a})^G$ (with group G). Since the trace on $S/\mathfrak{a}$ is induced from the trace on S, we must have $(S/\mathfrak{a})^G = K$, i.e., $S/\mathfrak{a}$ is a Galois extension of K with group G. Thus, $S/\mathfrak{a}$ and S have the same dimension over K, and we conclude that $\mathfrak{a} = 0$.

From the Chinese Remainder Theorem we then get that

$$S \simeq \bigoplus_{i=1}^{d} S/\sigma_i\mathfrak{m}.$$

In particular, S is a direct sum of isomorphic field extensions. Let $\varepsilon_1 = \varepsilon, \dots, \varepsilon_d$ be the corresponding idempotents. They are permuted transitively by G, since $\sigma_i\varepsilon = \varepsilon_i$. Also, H acts on $L = S\varepsilon$ as a field extension of K. L/L^H is trivially a Galois extension with group H, and since $[L : L^H] = [L : K]$, we have $L^H = K$, and so L/K is a Galois extension with group H.

Clearly, $S = \bigoplus_i \sigma_i(L\varepsilon)$, i.e., the elements have the form

$$a = \sum_{i=1}^{d} \sigma_i(a_i\varepsilon), \quad a_i \in L,$$

and the G-action is given by

$$\sigma a = \sum_{i=1}^{n} \sigma_i(h_{\sigma,\sigma^{-1}(i)} a_{\sigma^{-1}(i)}\varepsilon),$$

where $\sigma\sigma_i = \sigma_{\sigma(i)} h_{\sigma,i}$ and $h_{\sigma,i} \in H$.

Thus, $S = \mathrm{Ind}_H^G(L)$. This completely describes Galois algebras, since conversely $\mathrm{Ind}_H^G(L)/K$ is a Galois algebra with group G whenever L/K is a Galois extension with group H.

REMARKS. (1) From this description of Galois algebras, we immediately get the following: An algebra S/K is a Galois algebra with respect to *some* finite group, if and only if S is the direct sum of a finite number d of copies of a Galois field extension L/K. In that case, the possible groups are all groups G of order $\dim_K S = d[L : K]$ containing a subgroup isomorphic to $H = \mathrm{Gal}(L/K)$.

In particular, it is not only possible for an algebra S/K to be a Galois algebra with respect to several different groups, but even to be a Galois algebra with respect to the same group in several fundamentally different ways, since G may contain copies of H not conjugate under automorphisms. The simplest example would be $G = C_4 \times C_2$ and $H = C_2$.

(2) If $S/K = \mathrm{Ind}_H^G(L)/K$ is a Galois algebra and $N \lhd G$, then S^N/K is a Galois algebra as well, and in fact $S^N \simeq \mathrm{Ind}_{H/N\cap H}^{G/N}(L^{N\cap H})$: Let $n_1, \dots, n_s \in N$, $s = [NH : H]$, represent to cosets nH in NH. Then $\delta = \sum_{i=1}^{s} n_i\varepsilon$ is a primitive idempotent in S^N. We conclude that there are $[G : NH]$ simple components, each of degree $[NH : N] = [H : N \cap H]$ over K. We can embed $L^{N\cap H}$ into $S^N\delta$ by $x \mapsto \sum_i n_i(x\varepsilon)$, giving us $S^N f \simeq L^{N\cap H}$.

As a consequence of this, we see that S^N is a field if and only if $G = NH$. Thus, letting $N = \Phi(G)$ be the Frattini group of G (cf. [Hu, III.§3]) we get: S is a field if and only if $S^{\Phi(G)}$ is a field.

We note that if ε is a primitive idempotent for the Galois algebra S/K, and θ generates a normal basis for the simple component $S\varepsilon$, the conjugates of $\theta\varepsilon$ constitute a basis for S/K, i.e.,

PROPOSITION 4.3.2. *Let S/K be a Galois algebra with group G. Then the $K[G]$-module S is free of rank* 1.

The converse of Proposition 4.3.2 is obviously not true: A commutative K-algebra with a G-action is not necessarily a Galois algebra, just because it is free of rank 1 as a $K[G]$-module.[3] However, we *do* have

PROPOSITION 4.3.3. *Let S/K be a separable commutative algebra (i.e., S is the direct sum of finitely many finite separable field extensions of K). Let the finite group G act on S/K, and assume $|G| = \dim_K S$ and $S^G = K$. Then S/K is a Galois algebra with group G.*

PROOF. Let $\varepsilon_1, \dots, \varepsilon_d$ be the primitive idempotents in S. Clearly, they are permuted by G, and the number of orbits is less than or equal to $\dim_K S^G$. Hence, G acts transitive on $\varepsilon_1, \dots, \varepsilon_d$, and S is the direct sum of isomorphic field extensions. With $H = \{\sigma \in G \mid \sigma\varepsilon_1 = \varepsilon_1\}$ and $L = S\varepsilon_1$, we then have H acting on L and $|H| = [L : K]$. From $S^G = K$, we get $L^H = K$, and so L/K is Galois with Galois group H. It follows that $S = \mathrm{Ind}_H^G(L)$, and so S/K is a Galois algebra with group G. □

HILBERT 90. *Let S/K be a Galois algebra with group G. Then $H^1(G, S^*) = 1$.*

PROOF. Let $f \in Z^1(G, S^*)$, i.e., $f : G \to S^*$ with $f_{\sigma\tau} = f_\sigma\, \sigma f_\tau$ for $\sigma, \tau \in G$.

Pick a primitive idempotent $\varepsilon \in S$, let $L = S\varepsilon$ be the corresponding field extension of K, and let $H = \{\sigma \in G \mid \sigma\varepsilon = \varepsilon\} = \mathrm{Gal}(L/K)$. Also, let $\sigma_1 = 1, \sigma_2, \dots, \sigma_d \in G$ represent the cosets σH in G, and write $f_\sigma = \sum_i f_\sigma^{(i)}\, \sigma_i\varepsilon$ with

[3] The simplest example being the ring $K[\varepsilon] = K[t]/(t^2)$ of *dual numbers* (in characteristic $\neq 2$): If C_2 acts on $K[\varepsilon]$ by changing the sign of ε, we get a free $K[C_2]$-module that is not a Galois algebra.

$f_\sigma^{(i)} \in L^*$. By the Dedekind Independence Theorem, we can find $a \in L$ with $\sum_{\sigma\in H} f_\sigma^{(1)}\,\sigma a \neq 0$. Let $x = a\varepsilon$. Then

$$\begin{aligned} y &= \sum_{\sigma\in G} f_\sigma\,\sigma x = \sum_{i=1}^{d}\sum_{\sigma\in H} f_{\sigma_i\sigma}\,(\sigma a\,\sigma_i\varepsilon) \\ &= \sum_{i=1}^{d}\big(\sum_{\sigma\in H} f_{\sigma_i\sigma^{(i)}}\,\sigma a\big)\sigma_i\varepsilon \\ &= \sum_{i=1}^{d}\big(f_{\sigma_i}^{(i)}\sum_{\sigma\in H} f_\sigma^{(1)}\,\sigma a\big)\sigma_i\varepsilon \in S^*, \end{aligned}$$

and $\sigma y = f_\sigma^{-1} y$ for $\sigma \in G$, i.e., f is principal. □

COROLLARY 4.3.4. *Let S/K be a Galois algebra with group C_n, let σ generate C_n, and let $\zeta \in K^*$ be a primitive n^{th} root of unity. Then $S = K[\alpha]$ for an $\alpha \in S^*$ with $\sigma\alpha = \zeta\alpha$ (and hence $\alpha^n \in K^*$).*

We conclude the section with a few technical results adapted from [Ja1, 4.14], where they are used to prove the Normal Basis Theorem. They can be used for that purpose here also, to establish Proposition 4.3.2 above.

We let S/K be a Galois algebra with group G and look at a subgroup H of G of index $d = [G:H]$. Also, we let $\sigma_1, \dots, \sigma_d \in G$ represent the cosets σH in G.

LEMMA 4.3.5. *$\sigma_1, \dots, \sigma_d$ are linearly independent over S when considered as homomorphisms $S^H \to S$. (I.e., if $a_1, \dots, a_d \in S$ are such that $a_1\,\sigma_1 x + \cdots + a_d\,\sigma_d x = 0$ for all $x \in S^H$, then $a_1 = \cdots = a_d = 0$.)*

This lemma is easily proved by taking scalar extension to a field L with $S \otimes_K L \simeq L^{|G|}$, such as a simple component. (If S/K is a Galois field extension, the standard proof of the Dedekind Independence Theorem — assume that a non-trivial linear combination gives the zero map, and reduce the number of terms — can be applied as well.)

PROPOSITION 4.3.6. *Let $s_1, \dots, s_d \in S^H$. Then $s_1, \dots, s_d$ is a basis for S^H/K, if and only if*

$$\begin{vmatrix} \sigma_1 s_1 & \dots & \sigma_d s_1 \\ \vdots & \ddots & \vdots \\ \sigma_1 s_d & \dots & \sigma_d s_d \end{vmatrix} \in S^*.$$

PROOF. 'If' is obvious, since the rows are then independent over K. (And we have $\dim_K S^H = d$ by Corollary 4.2.12.)

'Only if': Assume that the determinant is not in S^*. Then there exists $t_1, \dots, t_d \in S$ not all zero, such that $t_1\,\sigma_1 s_i + \cdots + t_d\,\sigma_d s_i = 0$ for all i. By Lemma 4.3.5, $s_1, \dots, s_d$ cannot generate S^H over K, and is thus not a basis. □

THEOREM 4.3.7. *Assume K to be infinite. Then $\sigma_1, \dots, \sigma_d$ are algebraically independent over S. (I.e., if $f(x_1, \dots, x_d) \in S[x_1, \dots, x_d]$ with $f(\sigma_1 x, \dots, \sigma_d x) = 0$ for all $x \in S^H$, then $f(x_1, \dots, x_n) = 0$.)*

PROOF. Let $f(x_1,\dots,x_n)\in S[x_1,\dots,x_n]$, and assume the map

$$x\mapsto f(\sigma_1 x,\dots,\sigma_d x)$$

from S^H to S to be everywhere zero. If we introduce new indeterminates $y_1,\dots,y_d$ and let $x_i = y_1\,\sigma_i s_1+\cdots+y_d\,\sigma_i s_d$, we get a polynomial $g(y_1,\dots,y_d)=f(x_1,\dots,x_d)\in S[y_1,\dots,y_d]$ that vanishes on K. This implies that $g(y_1,\dots,y_d)=0$, and since the transformation from $y_1,\dots,y_d$ to $x_1,\dots,x_d$ is invertible (look at the matrix), we conclude that $f(x_1,\dots,x_n)=0$. □

Exercises

EXERCISE 4.1. Let R be a commutative ring and P a finitely generated R-module. Prove that $R=\operatorname{ann}_R P\oplus I_R P$. [Hint: $\operatorname{ann}_R P$ annihilates $I_R P$.]

EXERCISE 4.2. Let M/K be a Galois extension of fields with Galois group $G=\operatorname{Gal}(M/K)$. Describe $\operatorname{Aut}_K M^n$.

EXERCISE 4.3. Let S/R be an extension of commutative rings, and let G be a finite group acting on S by R-algebra automorphisms. Prove that S/R is a Galois extension with group G, if and only if S is a finitely generated projective R-module and the map $j\colon S\{G\}\to\operatorname{End}_R S$ from Proposition 4.2.3 is an isomorphism, cf. [D&I, Ch. III Prop. 1.2]. [Hint: Localise to prove $R=Z(\operatorname{End}_R S)=Z(S\{G\})=S^G$ (where Z denotes the center). Proposition 4.2.4 will hold, and condition (ii) in Proposition 4.2.6 can then be proven as before.]

EXERCISE 4.4. Let T/R be an extension of commutative rings, and let the finite group E act on T as R-algebra automorphisms. Let N be a normal subgroup of E, and let $S=T^N$ and $G=E/N$. Prove that T/R is Galois with group E if and only if T/S is Galois with group N *and* S/R is Galois with group G.

EXERCISE 4.5. Let S/R be a Galois extension with group G, and let M be an $S\{G\}$-module.

(1) Let

$$M^G=\{m\in M\mid\forall\sigma\in G\colon \sigma m=m\}$$

and prove: $S\otimes_R M^G$ is an $S\{G\}$-module by the action on S, and the map $\psi\colon S\otimes_R M^G\to M$, given by $\psi(s\otimes m)=sm$, is an $S\{G\}$-homomorphism.

(2) Prove that ψ is an isomorphism. [Hint: Consider elements in $\operatorname{Hom}_R(S,R)$ as homomorphisms $S\to M^G$ to get a map $\operatorname{Hom}_R(S,R)\otimes_{S\{G\}} M\to M^G$. Now prove that this map is onto, and that the composite map

$$S\otimes_R(\operatorname{Hom}_R(S,R)\otimes_{S\{G\}} M)\to S\otimes_R M^G\to M$$

is an isomorphism.] This generalises the Invariant Basis Lemma.

(3) Prove that M^G is an R-direct summand of M, and conclude that M^G is R-projective if M is S-projective.

(4) Prove that

$$\operatorname{Hom}_R(S,R)\otimes_{S\{G\}} S\simeq R$$

by

$$\operatorname{Tr}_{S/R}(c\cdot)\otimes s\mapsto\operatorname{Tr}_{S/R}(cs),$$

and use this to prove $\operatorname{Hom}_R(S,R)\otimes_{S\{G\}} M\simeq M^G$. Then prove that S is $S\{G\}$-projective.

EXERCISE 4.6. Let R be a commutative ring.

(1) Prove that the following conditions are equivalent for a finitely generated faithful projective R-module P:

(i) P has rank 1.
(ii) $\mathrm{Hom}_R(P, R)$ has rank 1.
(iii) $\mathrm{End}_R P \simeq R$.
(iv) $\mathrm{Hom}_R(P, R) \otimes_R P \simeq R$.

(2) Let $\mathcal{P}(R)$ be the set of isomorphism classes of finitely generated faithful projective R-modules of rank 1, and define a multiplication on $\mathcal{P}(R)$ by $[P][Q] = [P \otimes_R Q]$. Prove that this multiplication is well-defined and makes $\mathcal{P}(R)$ into an abelian group. This is the *projective class group*.

EXERCISE 4.7. Let S/R be a Galois extension with group G. As usual, we define the *first cohomology group*

$$H^1(G, S^*) = Z^1(G, S^*)/B^1(G, S^*),$$

where $Z^1(G, S^*)$ is the group of *crossed homomorphisms*, i.e., maps $f\colon G \to S^*$ satisfying $f_{\sigma\tau} = f_\sigma \, \sigma f_\tau$, and $B^1(G, S^*)$ is the subgroup of *principal crossed homomorphisms*, i.e., those of the form $\sigma \mapsto \sigma s/s$ for an $s \in S^*$.

(1) Define, for $f \in Z^1(G, S^*)$, a map θ_f on $S\{G\}$ by $\theta_f(s\sigma) = s f_\sigma \sigma$. Prove that this is an R-automorphism on $S\{G\}$ and that $\theta_{fg} = \theta_f \theta_g$. Also, prove that θ_f is a conjugation if f is principal.

(2) Define, again for $f \in Z^1(G, S^*)$, an $S\{G\}$-action on S by $x \cdot s = \theta_f(x)s$, and prove that this gives us an $S\{G\}$-module S_f. Then prove that S_f^G is finitely generated R-projective of rank 1, giving us an element $[S_f^G] \in \mathcal{P}(R)$.

(3) Prove that $S_{fg}^G \simeq S_f^G \otimes_R S_g^G$, and that $S_f^G \simeq R$ if f is principal.

(4) (HILBERT 90) Prove that $[f] \mapsto [S_f^G]$ is an injective homomorphism $H^1(G, S^*) \hookrightarrow \mathcal{P}(R)$.

CHAPTER 5

Generic Extensions and Generic Polynomials

We now present the theory of generic extensions, including the connection with the Noether Problem as stated in the Introduction. Generic extensions, originally introduced by Saltman in [Sa1, 1982], can be used to describe Galois extensions in cases where calculating a generic polynomial would be difficult and uninformative. However, as we will see below, the existence of generic polynomials and generic extensions for a group G are equivalent over an *infinite* field of arbitrary characteristic, and a generic extension can always (in principle, at least) be used to produce a generic polynomial. We will then construct generic extensions/polynomials for some families of groups, namely cyclic groups of odd order and dihedral groups of odd degree, both in characteristic 0, and p-groups in characteristic p.

5.1. Definition and Basic Results

Let S/R and S'/R' be Galois extensions of commutative rings with the same finite group G as Galois group, and assume that R' is an R-algebra. An R-algebra homomorphism $\varphi\colon S \to S'$ is then called a *Galois homomorphism*, if $\varphi(\sigma s) = \sigma\varphi(s)$ for $s \in S$ and $\sigma \in G$.

Now, let S/R and T/R be Galois extensions with group G, and let $\varphi\colon S \to T$ be a Galois homomorphism.

If R is a field, we look at the primitive idempotents $\varepsilon_1, \ldots, \varepsilon_d \in S$. They are permuted transitively by G and add up to 1, from which it follows that none of the images $\delta_i = \varphi(\varepsilon_i) \in T$ are 0. Hence, $\delta_1, \ldots, \delta_d$ are non-zero orthogonal idempotents in T, and φ maps $S\varepsilon_i$ to $T\delta_i$. Since $S\varepsilon_i$ is a field, φ must be injective, and is thus an isomorphism.

Next, let R be arbitrary. For any maximal ideal $\mathfrak{m}$ in R, $S/\mathfrak{m}S$ and $T/\mathfrak{m}T$ are Galois extensions of $R/\mathfrak{m}$ with group G, and so the induced Galois homomorphism $\varphi_{\mathfrak{m}}\colon S/\mathfrak{m}S \to T/\mathfrak{m}T$ is an isomorphism, i.e., $T = \mathfrak{m}T + \varphi(S)$. By Nakayama's Lemma, $T = \varphi(S)$, i.e., φ is surjective. Now, $T = S/\ker\varphi$ is R-projective, and so $S \simeq T \oplus \ker\varphi$ over R. For any maximal ideal $\mathfrak{m}$ in R, $\ker\varphi/\mathfrak{m}\ker\varphi = 0$, since S and T have the same rank, and so $\ker\varphi = 0$, i.e., φ is injective.

PROPOSITION 5.1.1. *A Galois homomorphism $\varphi\colon S/R \to T/R$ is an isomorphism.*

From this we get

COROLLARY 5.1.2. *Let S/R be a Galois extension with group G, and let R' and S' be subrings of R and S resp., such that S'/R' is a Galois extension with group G by restricted action. Then $S' \otimes_{R'} R \simeq S$ by $s' \otimes r \mapsto s'r$.*

PROOF. $s' \otimes r \mapsto s'r$ is a Galois homomorphism from $S' \otimes_{R'} R/R$ to S/R. □

COROLLARY 5.1.3. *If S/R is a Galois extension with group $G \times H$, the map $s \otimes t \mapsto st$ is an isomorphism $S^{G\times 1} \otimes_R S^{1\times H} \simeq S$.*

If $\varphi\colon R \to R'$ is a ring homomorphism, R' becomes an R-algebra by $rx = \varphi(r)x$, and so we get a Galois extension $S \otimes_R R'/R'$ with group G. We denote the tensor product $S \otimes_R R'$ by $S \otimes_\varphi R'$ in this case.

REMARK. Note that $S \otimes_\varphi R'$ is, loosely speaking, just S with R replaced by R'. That is, any polynomial relation over R between elements in S, including conjugates under the G-action, carry over by replacing the coefficients by their images under φ.

More precisely: Since S is finitely generated over R, we can write $S \simeq R[\mathbf{x}]/\mathfrak{a}$ for indeterminates $\mathbf{x} = (x_1, \dots, x_n)$ and an ideal $\mathfrak{a}$ in $R[\mathbf{x}]$. We then get $S \otimes_\varphi R' \simeq R'[\mathbf{x}]/\varphi(\mathfrak{a})R'$, meaning that $S \otimes_\varphi R'$ has the same generators and relations as S, only over R' instead of R. The G-action carries over as well, as it is defined on the generators.

For instance: Let $R = \mathbb{Z}[\frac{1}{2}, t, 1/t]$ and $S = \mathbb{Z}[\frac{1}{2}, \sqrt{t}, 1/t]$. Then S/R is a Galois extension with group C_2, acting by changing the sign of $\sqrt{t}$. A homomorphism φ from R to a commutative ring R' exists whenever 2 is a unit in R', and in that case $s = \varphi(t)$ can be any unit in R'. The tensor product $S \otimes_R R'$ is then the ring $R'[\sqrt{s}] \simeq R'[X]/(X^2 - s)$, with C_2 acting by changing the sign of $\sqrt{s}$.

DEFINITION 5.1.4. Let K be a field and G a finite group. A Galois extension S/R with group G is called a *generic G-extension* over K, if

(i) R is of the form $K[\mathbf{t}, 1/t]$ for some number d of indeterminates $\mathbf{t} = (t_1, \dots, t_d)$, and an element $t \in K[\mathbf{t}] \setminus (0)$; and
(ii) whenever L is an extension field of K and T/L is a Galois algebra with group G, there is a K-algebra homomorphism $\varphi\colon R \to L$, such that $S \otimes_\varphi L/L$ and T/L are isomorphic as Galois extensions (i.e., by a Galois homomorphism). The map φ is called a *specialisation*.

For convenience, we will call a ring $R = K[\mathbf{t}, 1/t]$ as in (i) a *localised polynomial ring* over K.

EXAMPLES. (1) If $\operatorname{char} K \neq 2$, $K[\sqrt{t}, 1/\sqrt{t}]/K[t, 1/t]$ is a generic quadratic extension.

(2) If $\operatorname{char} K \neq 2$ and K has more than 5 elements, we can get a generic C_4-extension by letting $R = K[t_1, t_2, 1/t_1t_2(1 + t_2^2)] \subseteq K(t_1, t_2)$ and $S = R[\sqrt{\theta}] \subseteq K(t_1, t_2, \sqrt{\theta})$, where $\theta = t_1(1 + t_2^2 + \sqrt{1 + t_2^2})$. (If $K = \mathbb{F}_3$ or $\mathbb{F}_5$, this will not give us the 'split' extension K^4/K.)

(3) If $\operatorname{char} K = p \neq 0$, $K[\theta_t]/K[t]$ is a generic C_p-extension, when θ_t is a root of $X^p - X - t$.

PROPOSITION 5.1.5. *Let S/R be a generic G-extension over K, and let L be an extension field of K. Then $S \otimes_K L/R \otimes_K L$ is a generic G-extension over L.*

PROOF. If $R = K[\mathbf{t}, 1/t]$, then $R \otimes_K L = L[\mathbf{t}, 1/t]$. Now, let M be an extension field of L, and let T/M be a Galois algebra with group G. Then there is a specialisation $\varphi\colon R \to M$, such that $S \otimes_\varphi M/M \simeq T/M$ as Galois extensions. It is then clear that the specialisation $\psi\colon R \otimes_K L \to M$, given by $\psi(r \otimes x) = \varphi(r)x$, gives an isomorphism $(S \otimes_K L) \otimes_\psi M/L \simeq T/M$. □

PROPOSITION 5.1.6. *Let G and H be finite groups, and let S/R and U/T be generic G- and H-extensions, resp., over K. Then $S \otimes_K U/R \otimes_K T$ is a generic $G \times H$-extension over K.*

PROOF. If $R = K[\mathbf{t}, 1/t]$ and $T = K[\mathbf{v}, 1/v]$, we get $R \otimes_K T = K[\mathbf{t}, \mathbf{v}, 1/tv]$. Also, by Corollary 5.1.3, a $G \times H$-extension is the tensor product of a G- and an H-extension, and so we can specialise separately. □

PROPOSITION 5.1.7. *Let S/R be a generic E-extension, where $E = N \rtimes G$. Then S^N/R is a generic G-extension.*

PROOF. Let T/L, $L \supseteq K$, be a G-extension. Then $\mathrm{Ind}_G^E(T)/L$ is an E-extension, and hence we have a specialisation $\varphi\colon R \to L$ with $S \otimes_\varphi R \simeq \mathrm{Ind}_G^E(T)$. By restriction, we get $S^N \otimes_\varphi R \simeq \mathrm{Ind}_G^E(T)^N \simeq T$. □

In view of the equivalence of generic polynomials and generic extensions that we will prove in Theorem 5.2.5 below, this implies the following unexpected result, cf. Exercise 5.6: A generic $N \rtimes G$-polynomial gives rise to a generic G-polynomial.

Generic Galois extensions give rise to generic polynomials as follows:

PROPOSITION 5.1.8. *Let S/R be a generic G-extension over K. Then there is a generic polynomial for G-extensions over K.*

PROOF. First of all: For $s \in S$, we define

$$\mathrm{Min}(s, R) = \prod_{s' \in Gs} (X - s'),$$

i.e., $\mathrm{Min}(s, R)$ is the product of the distinct conjugates of $X - s$ under G. It is clear that $\mathrm{Min}(s, R) \in R[X]$, and we claim that $\mathrm{Min}(s, R)$ is separable in $\mathbb{K}[X]$, where $\mathbb{K} = K(\mathbf{t})$ is the quotient field of R: Let $\mathfrak{m}$ be a maximal ideal in $S \otimes_R \mathbb{K}$, and let $\mathbb{L} = S \otimes_R \mathbb{K}/\mathfrak{m}$. Then $\mathbb{L}$ is a simple component of $S \otimes_R \mathbb{K}$, and hence a Galois field extension of $\mathbb{K}$. Also, $\mathrm{Min}(s, R)$ splits in linear factors over $\mathbb{L}$, since it does over S. Hence, $\mathrm{Min}(s, R)$ is separable.[1]

Now, let $s_1, \ldots, s_m$ generate S over R, and let

$$f(X) = \prod_{i=1}^{m} \mathrm{Min}(s_i, R).$$

Then $f(X)$ is a monic separable polynomial in $\mathbb{K}[X]$. The splitting field of $f(X)$ over $\mathbb{K}$ is the simple component $\mathbb{L}$ from above, and so $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = H \subseteq G$ by the results of section 4.3 above.

[1] Here, 'separable' means that the irreducible factors have no multiple roots.

Next, let M/L be a G-extension of fields with $L \supseteq K$. Then there is a specialisation $\varphi\colon R \to L$, such that $S \otimes_\varphi L \simeq M$. It follows that M is the splitting field of $\varphi(f)(X) \in L[X]$, and by Lemma 3.3.1 in Chapter 3, $\mathbb{L}/\mathbb{K}$ is a G-extension. □

COROLLARY 5.1.9. *Let S/R be a generic G-extension over K, and let $\mathbb{K}$ be the quotient field of R. Then S is a domain, and the quotient field $\mathbb{L} = S \otimes_R \mathbb{K}$ is a regular G-extension of $\mathbb{K}$.*

Generic Galois extensions and Noether's Problem. Let K be an *infinite* field, and let G be a transitive subgroup of the symmetric group S_n for some n. Then G acts on $\mathbb{M} = K(\mathbf{t}) = K(t_1, \ldots, t_n)$ by permuting the indeterminates, and we have a G-extension $\mathbb{M}/\mathbb{K}$, where $\mathbb{K} = \mathbb{M}^G$.

Assume that Noether's Problem has an affirmative answer in this case, i.e., that $\mathbb{K}$ is purely transcendental over K, and write $\mathbb{K} = K(\mathbf{s})$ for algebraically independent elements $\mathbf{s} = (s_1, \ldots, s_n)$.

Since $\mathbb{M}/\mathbb{K}$ is a Galois extension with group G, there exist elements $x_i, y_i \in \mathbb{M}$ with $\sum_i x_i\, \sigma y_i = \delta_{\sigma,1}$ for all $\sigma \in G$. For a suitable $s \in K[\mathbf{s}]$, these x_i's and y_i's are all integral over $R = K[\mathbf{s}, 1/s]$, and so the integral closure S of R in $\mathbb{M}$ is a Galois extension of R with group G.

THEOREM 5.1.10. (SALTMAN) *S/R is generic for G over K.*

PROOF. We let $H = \{\sigma \in G \mid \sigma t_1 = t_1\}$, and let $\sigma_1, \ldots, \sigma_n \in G$ with $\sigma_i t_1 = t_i$. The σ_i's then represent the cosets σH in G. Also, we pick $t \in \mathbb{K} \cap K[\mathbf{t}] \setminus (0)$ such that $S \subseteq K[\mathbf{t}, 1/t]$.

Now, look at a G-extension T/L, where L is a field extension of K. Since $t \in K[\mathbf{t}]$ is not 0, there is an $a \in T^H$ such that $t(\sigma_1 a, \ldots, \sigma_n a) \in L^*$ by Theorem 4.3.7, and we can define $\varphi\colon K[\mathbf{t}, 1/t] \to T$ by $\varphi(t_i) = \sigma_i a$. This φ respects the G-action, and so induces a Galois homomorphism $\varphi \otimes 1\colon S \otimes_R L \to T$. □

EXAMPLE. Look at S_n itself. The fixed field $\mathbb{K}$ is then $K(\mathbf{e}) = K(e_1, \ldots, e_n)$, where e_i is the i^{th} elementary symmetric polynomial in $\mathbf{t}$. Let d be the discriminant of $e_1, \ldots, e_n$. Then S/R is a generic S_n-extension, when $R = K[\mathbf{e}, 1/d]$ and $S = K[\mathbf{t}, 1/d]$.

5.2. Retract-Rational Field Extensions

As we saw in Theorem 5.1.10 above, a generic G-extension exists over an infinite field K if the Noether Problem has a positive answer, i.e., if $K(\mathbf{t})^G$ is a rational (purely transcendental) extension of K. This result can be refined, cf. [Sa2], to precisely specify the structure $K(\mathbf{t})^G$ must have in order for K to possess a generic G-extension.

For the rest of this section, K denotes an *infinite* field. This is necessary for our argument, which uses Theorem 4.3.7. It is much less clear to what extent it is necessary for the conclusions, but since we are not overly concerned with Galois extensions of finite fields, we will not worry about that.[2]

[2]After work on this monograph had been completed, F. DeMeyer communicated to one of the authors some preliminary work with T. McKenzie, that adresses these points.

DEFINITION 5.2.1. A field extension L/K is *retract-rational* if there are K-algebra domains (K-*domains* for short) R and T together with a K-algebra homomorphism $\varphi\colon R \to T$, such that the following conditions are satisfied:

(i) R is a localised polynomial ring over K,
(ii) L is the quotient field of T, and
(iii) $\varphi\colon R \to T$ is split (i.e., there exists a K-algebra homomorphism $\psi\colon T \to R$ with $\varphi \circ \psi = 1_T$).

Trivially, finitely generated rational extensions are retract-rational. So are stably rational extensions.

LEMMA 5.2.2. *A field extension L/K is retract-rational if and only if L is the quotient field of a finitely generated K-algebra T with the following property: Let $(A, \mathfrak{m})$ be a local K-domain, and let $f\colon T \to A/\mathfrak{m}$ be a K-algebra homomorphism. Then f factors through A (as a K-algebra homomorphism).*

PROOF. 'If': We can find a K-algebra epimorphism $\varphi\colon K[\mathbf{t}] = K[t_1, \dots, t_n] \twoheadrightarrow T$ for some n. Let $\mathfrak{p} = \varphi^{-1}(0)$. It is a prime ideal, and we can localise to get $\varphi_{\mathfrak{p}}\colon K[\mathbf{t}]_{\mathfrak{p}} \twoheadrightarrow L$. By assumption, we can lift the inclusion $T \subseteq L$ to a homomorphism $\psi\colon T \to K[\mathbf{t}]_{\mathfrak{p}}$. Letting $t \in K[\mathbf{t}]$ be a common denominator for $\psi(\varphi(t_i)) \in K(\mathbf{t})$, we have $\psi(T) \subseteq K[\mathbf{t}, 1/t]$, and it follows that L/K is retract-rational.

'Only if': Let T, R and φ be as in the Definition. Obviously, $f\colon T \to A/\mathfrak{m}$ is induced by a homomorphism $f'\colon R \to A/\mathfrak{m}$, and this lifts to $F\colon R \to A$, since A is local. Now $F \circ \psi\colon T \to A$ is the desired lifting. □

THEOREM 5.2.3. (SALTMAN & DEMEYER) *Let K be a field and G a finite group, and let there be given a faithful transitive action of G on a set $\mathbf{t} = (t_1, \dots, t_m)$ of m indeterminates, for some m. Then the following conditions are equivalent:*

(i) *There is a generic G-extension over K.*
(ii) *For any local K-domain $(A, \mathfrak{m})$, the G-extensions of the residue field $A/\mathfrak{m}$ come from G-extensions of A by tensoring.* (*This is the* lifting property.)
(iii) *$K(\mathbf{t})^G/K$ is retract-rational.*

REMARK. Saltman [Sa2] proved the above result in the case where G acted regularly on $n = |G|$ indeterminates. In [DM], DeMeyer then established the stronger version stated here.

PROOF OF THEOREM 5.2.3. (i) ⇒ (ii): Let S/R be a generic G-extension over K, and write $R = K[\mathbf{t}, 1/t] = K[t_1, \dots, t_n, 1/t]$. Also, let $(A, \mathfrak{m})$ be a local K-domain with residue field L, and let T/L be a G-extension. Since $L \supseteq K$, there is a specialisation $\varphi\colon R \to L$ with $T/L \simeq S \otimes_\varphi L/L$. As A is local, we can lift this φ to a $\Phi\colon R \to A$ and get the desired lifting by $S \otimes_\Phi A/A$.

(ii) ⇒ (iii): Let $H = \{\sigma \in G \mid \sigma t_1 = t_1\}$, and let $\sigma_1, \dots, \sigma_m \in G$ represent the cosets σH in G. We may of course assume $\sigma_i t_1 = t_i$. For some $t \in K[\mathbf{t}] \setminus (0)$, we get a G-extension $K[\mathbf{t}, 1/t]$ of $T = K[\mathbf{t}, 1/t]^G$. It is clear that $K(\mathbf{t})^G$ is the quotient field of T, and that T is a finitely generated K-algebra.

Let $(A, \mathfrak{m})$ be a local K-domain, and let $f\colon T \to L = A/\mathfrak{m}$ be a K-algebra homomorphism. Then $K[\mathbf{t}, 1/t] \otimes_f L/L$ is a G-extension, and by the lifting property it comes from a G-extension U/A. Now, any pre-image in U^H of $t_1 \otimes 1 \in K[\mathbf{t}, 1/t]$ will define a G-equivariant homomorphism $K[\mathbf{t}, 1/t] \to U$, and the restriction to T is a lifting of f to a map $F\colon T \to A$. Lemma 5.2.2 finishes the argument.

(iii) $\Rightarrow$ (i): Let $\varphi\colon R \to T \subseteq K(\mathbf{t})^G$ express the retract-rationality according to the definition. It is easily seen that T is intregrally closed. Let U be the integral closure of T in $K(\mathbf{t})$. By localising in some element in T (which we can do without changing the assumption) we obtain that U/T is a G-extension, and that the t_σ's are in U. Moreover, we can find $t \in K[\mathbf{t}]^G \setminus (0)$ such that $U \subseteq K[\mathbf{t}, 1/t]$, since U is finitely generated over T (by e.g. [Z&S, p. 267]).

Now, let L be an extension field of K, and let V/L be a G-extension. Precisely as in the proof of Theorem 5.1.10, we see that there exists $v \in V$ with $t(\sigma_1 v, \dots, \sigma_m v) \in L^*$, and we get a Galois homomorphism $f\colon t_i \mapsto \sigma_i v$ from U/T to V/L. (Here, $\sigma_1, \dots, \sigma_m$ are as in (ii) $\Rightarrow$ (iii) above.)

Thus, U/T is 'almost generic', and we convert it into a true generic extension S/R by letting $S = U \otimes_\psi R$: Clearly, we have a Galois homomorphism $S/R \to U/T$ extending φ, given by $u \otimes r \mapsto \varphi(r)u$, and so any specialisation of U/T is a specialisation of S/R as well. □

This, together with the No-name Lemma (from section 1.1 in Chapter 1), generalises Theorem 5.1.10, in that we now only require the fixed field $K(\mathbf{t})^G$ to be retract-rational over K, rather than rational.

REMARK. In [Sa1, Cor. 5.4], Saltman proves that a generic G-extension S/R over an infinite field K can be chosen such that S is free as an R-module. It is obvious from the above that it can in fact be chosen to have a normal basis consisting of units: $K(\mathbf{t})/K(\mathbf{t})^G$ has one, and it will work for U/T just as well by localising in a suitable t. The lifting of U/T to S/R preserves a normal basis (and units), and we have the result.

Versal extensions. Let K be an infinite field and G a finite group acting on a family $\mathbf{t} = (t_\sigma)_{\sigma \in G}$ by regular action.

DEFINITION 5.2.4. A *versal* G-extension over K is a G-extension U/T of finitely generated K-algebras with the following property: If S/L is a G-extension of a field L containing K, there is a K-algebra homomorphism $\varphi\colon U \to L$ such that $U \otimes_\varphi L/L \simeq S/L$ as G-extensions.

NOTE. This concept is inspired by the versal polynomials used in [B&R1].

Thus, a generic extension is versal, and so is the extension U/T introduced in the proof of Theorem 5.2.3. However, versal extensions is a much weaker concept than generic extensions, as demonstrated by the fact that they always exist:

We construct U/T inside $K(\mathbf{t})/K(\mathbf{t})^G$: Let

$$d = \prod_{i<j} (t_i - t_j)^2 \in K[\mathbf{e}]$$

be the discriminant. Then

$$U/T = K[\mathbf{t}, 1/d]/K[\mathbf{t}, 1/d]^G$$

is a versal extension for G over K. (And $K[\mathbf{t}, 1/d]^G$, being the integral closure of $K[\mathbf{e}, 1/d]$ in $K(\mathbf{t})^G$, *is* a finitely generated K-algebra. Here, $\mathbf{e} = (e_1, \dots, e_n)$ are the elementary symmetric symbols.)

EXAMPLE. Let $\Delta = \prod_{i<j}(t_i - t_j)$ be the different. Then a versal A_n-extension is given by $K[\mathbf{t}, 1/\Delta]/K[\mathbf{e}, 1/\Delta]$.

As before, we can localise U/T in an arbitrary element in $T \setminus (0)$ and still have a versal extension. Thus, any finitely many elements in $K(\mathbf{t})$ can be assumed contained in U.

Now, let $P(\mathbf{s}, X) \in K(\mathbf{s})[X]$ be a generic G-polynomial with splitting field $\mathbb{M}$ over $K(\mathbf{s})$, and let $R = K[\mathbf{s}, 1/d]$ where d is a least common denominator for the coefficients in $P(\mathbf{s}, X)$. Let S be the ring generated over R by the roots of $P(\mathbf{s}, X)$. As $P(\mathbf{s}, X)$ is generic, $K(\mathbf{t})$ is the splitting field over $K(\mathbf{t})^G$ of some specialisation $P(\mathbf{a}, X)$, and we can get a G-equivariant homomorphism $\varphi\colon S \to K(\mathbf{t})$ taking $\mathbf{s}$ to $\mathbf{a}$ by (if necessary) modifying our identification of G with $\operatorname{Aut}_R S$. We may assume $\varphi(S) \subseteq U$, and by adding indeterminates to $\mathbf{s}$, we make $\varphi\colon R \to T$ onto. Thus, $K(\mathbf{t})$ is the quotient field of $\varphi(S)$.

Localising R in $\mathfrak{p} = \ker\varphi \cap R$ and S in $\mathfrak{m} = \ker\varphi$ gives us a homomorphism $\varphi'\colon S_{\mathfrak{m}} \to K(\mathbf{t})$ mapping $R_{\mathfrak{p}}$ onto $K(\mathbf{t})^G$. Clearly, $\varphi'(S_{\mathfrak{m}})/K(\mathbf{t})^G$ is integral, meaning that $\varphi'(S_{\mathfrak{m}})$ must be a field, and since it contains $\varphi(S)$ it is be all of $K(\mathbf{t})$. Thus, $\varphi'\colon S_{\mathfrak{m}} \to K(\mathbf{t})$ is onto.

As $\mathfrak{m}$ is the only maximal ideal in $S_{\mathfrak{m}}$, it is easy to check that $S_{\mathfrak{m}}/R_{\mathfrak{p}}$ is Galois with group G, and the Definition is trivial to check: Let $\sigma \in G \setminus 1$, and pick $s \in S$ such that $\sigma\bar{s} \neq \bar{s}$ in $K(\mathbf{t})$. Then $\sigma s - s \notin \mathfrak{m}$.

It follows that $S[1/s]/R[1/s]$ is Galois for some $s \in R \setminus \mathfrak{p}$, and since this extension specialises to the versal extension $U[1/\varphi(s)]/T[1/\varphi(s)]$, it is generic.

This proves the converse of Proposition 5.1.8, giving us

THEOREM 5.2.5. *Let K be an infinite field and G a finite group. Then there is a generic G-extension over K if and only if there is a generic G-polynomial over K.*

REMARK. The main result of DeMeyer's paper [DM] is that the existence of a generic extension (over an infinite field) is equivalent to the existence of a 'descent-generic' polynomial as defined in Chapter 2. Since we know that 'descent-generic' is the same as generic, we could of course get Theorem 5.2.5 by invoking DeMeyer's result.

In analogy with Proposition 1.1.5 in Chapter 1 above, we also get

PROPOSITION 5.2.6. *Let K be an infinite field and G a finite group. A G-extension S/R, where R is a localised polynomial ring over K, is generic if and only if every G-extension of* fields *containing K is a specialisation.*

5.3. Cyclic Groups of Odd Order

Following [Sa1, §2] we will now establish the existence of generic C_q-extensions, when q is odd. By Proposition 5.1.6, we may assume $q = p^n$ for an odd prime p, and since we are primarily interested in fields of characteristic 0, we will assume all fields to be infinite of characteristic $\neq p$:[3]

Let K be our ground field, and let ζ be a primitive q^{th} root of unity. Letting $d = [K(\mu_q) : K]$, we have $C_d = \mathrm{Gal}(K(\mu_q)/K)$ generated by $\kappa\colon \zeta \mapsto \zeta^e$, where $e \in \mathbb{Z}$ has order d modulo q. We can choose e to have order pd modulo pq, i.e., $p \nmid (e^d - 1)/q$.

By Proposition 1.1.5 from Chapter 1, we need only consider extension fields L of K for which $[L(\mu_q) : L] = d$. Since our construction will depend only on d, this allows us to simply work over K.

We define a map Φ by

$$\Phi(x) = x^{e^{d-1}} \kappa x^{e^{d-2}} \cdots \kappa^{d-1} x.$$

Whenever κ extends from $K(\mu_q)$ to a $K(\mu_q)$-algebra R', Φ is defined on R'.

LEMMA 5.3.1. *Let S/K be a Galois algebra with group C_q, and let $S_q = S \otimes_K K(\mu_q)$. Then $S_q = K(\mu_q)[\theta]$ for a $\theta \in S_q$ with $\theta^q = \Phi(b)$, $b \in K(\mu_q)^*$.*

PROOF. S_q/K is a Galois algebra with group $C_d \times C_q$, and $S_q/K(\mu_q)$ is a Galois extension with group C_q. By Hilbert 90, we have $S_q = K(\mu_q)[\alpha]$ for an α with $\alpha^q = a \in K(\mu_q)^*$. Also, the generator for C_q can be chosen as $\sigma\colon \alpha \mapsto \zeta\,\alpha$.

Since $\kappa\sigma = \sigma\kappa$, we must have $\kappa\alpha = z\alpha^e$ for some $z \in K(\mu_q)^*$, and hence $\alpha = \kappa^d\alpha = \Phi(z)a^{(e^d-1)/q}\alpha$ or $a^{(e^d-1)/q} = \Phi(z^{-1})$. We picked $(e^d - 1)/q$ to be prime to q, and so we get $S_q = K(\mu_q)[\theta]$ for some suitable power b of z^{-1}. □

Now, let $\mathbf{y} = (y_1, \ldots, y_d)$ be a set of indeterminates, and let $x_1 = y_1 + y_2\zeta + \cdots + y_d\zeta^{d-1}$ be a 'generic element' of $K(\mu_q)$. Define $x_i = \kappa^i x_1$ for $i = 1, \ldots, d$. Then $\mathbf{x} = (x_1, \ldots, x_d)$ is algebraically independent, and $x = x_1 \cdots x_d \in K[\mathbf{y}]$. Let $R = K[\mathbf{y}, 1/x]$ and $R_q = K(\mu_q)[\mathbf{y}, 1/x] = K(\mu_q)[\mathbf{x}, 1/x]$. Clearly, R_q is the scalar extension of R to $K(\mu_q)$.

Next, let $S_q = R_q[\theta]$, where $\theta^q = \Phi(x_1)$. Then κ extends to S_q by $\kappa\theta = x_1^{-(e^d-1)/q}\theta^e$, giving us a $C_d \times C_q$-extension S_q/R. Let $S = S_q^{C_d}$.

THEOREM 5.3.2. *S/R is a generic C_q-extension over K.*

PROOF. First of all, *S/R is* a Galois extension with group C_q, and R has the required form.

Now, let T/K be a Galois algebra with group C_q. We let $T_q = T \otimes_K K(\mu_q)$. Then $T_q/K(\mu_q)$ is a Galois extension with group C_q, and so $T_q = K(\mu_q)[\theta]$, where $\theta = \Phi(b)$, $b \in K(\mu_q)^*$.

We define $\varphi'\colon R_q \to K(\mu_q)$ by $\varphi(x_i) = \kappa^{i-1}b$. Then φ' respects the C_d-action, and so induces a specialisation $\varphi\colon R \to L$.

[3]For fields of characteristic p, we have Gaschütz' result, mentioned in Chapter 2 and proved in section 5.6 below, as well as Witt vectors.

Also, $T_q \simeq S_q \otimes_{\varphi'} K(\mu_q)$ as C_q-extensions of $K(\mu_q)$. Thus, it becomes an isomorphism of $C_q \times C_d$-extensions of K. In particular, $T/L \simeq (S_q \otimes_{\varphi'} K(\mu_q))^{C_d}/K(\mu_q)$ as C_q-extensions, and since $S \otimes_\varphi L$ maps into $(S_q \otimes_{\varphi'} K(\mu_q))^{C_d}$, we must have $T/K \simeq S \otimes_\varphi K/K$. □

COROLLARY 5.3.3. *There is a generic polynomial for C_q-extensions over K.*

In order to find generic polynomials as in the proof of Proposition 5.1.8, we need to find generators for S over R. Now, $\mathrm{Tr}_{S_q/S}\colon S_q \to S$ is surjective, and S_q/R is generated (freely) by $\{\zeta_i\theta^j \mid i = 0, \dots, d-1,\ j = 0, \dots, q-1\}$. Hence, S/R is generated by $\{\mathrm{Tr}_{S_q/S}(\zeta^i\theta^j) \mid i = 0, \dots, d-1,\ j = 0, \dots, q-1\}$. Some of these elements are conjugate, giving the same minimal polynomial. Others have degree $< q$, and can thus be disregarded. In fact, we see the following:

Let $\alpha = \mathrm{Tr}_{S_q/S}(\zeta^i\theta^j)$. If $p \nmid j$, $\zeta^i\theta^j$ is conjugate to θ^j in S_q/R_q, and so α is conjugate to $\mathrm{Tr}_{S_q/S}(\theta^j)$ in S/R. If $p \mid j$, we have $\zeta^i\theta^j \in R_q[\theta^p]$, i.e., α is contained in the $C_{p^{n-1}}$-subextension of S/R, and does not contribute significantly.

All in all: We need only consider α when $i = 0$ and $p \nmid j$.

Now, suppose M/K to be a C_q-extension of fields. Then we obtain a specialisation $\varphi\colon R \to K$ by $\varphi(x_1) = b$, where $M_q = M \otimes_K K(\mu_q) = K(\mu_q)[\beta]$, $\beta^q = \Phi(b)$. For some j prime to p, we must then have α specialising to a primitive element for M/K. Replacing β by β^j and φ by $x_1 \mapsto b^j$, we get another specialisation, in which this primitive element is the image of $\mathrm{Tr}_{S_q/S}(\theta)$.

Hence, we only have to look at α for $i = 0$ and $j = 1$. In other words:

PROPOSITION 5.3.4. *The minimal polynomial for*

$$\mathrm{Tr}_{S_q/S}(\theta) = \sum_{i=0}^{d-1} \kappa^i\theta$$

over $K(y_1, \dots, y_d)$ has degree q and is a generic polynomial for C_q-extensions over K.

Generic polynomials for cyclic groups of odd order were first constructed by G. W. Smith in [SmG, 1991].

Since we know exactly how κ and C_q act on θ and the x_i's, the construction above allows us to produce generic polynomials.

EXAMPLE. Consider the simplest case, $q = 3$, and assume $\zeta \notin K^*$: Then $\Phi(x_1) = x_1^2x_2$. We can replace this element by x_2/x_1, since x_1 is a unit. Then

$$\alpha = \sqrt[3]{x_2/x_1} + \sqrt[3]{x_1/x_2},$$

and the minimal polynomial is $X^3 - 3X - (x_1^2 + x_2^2)/x_1x_2$. Letting

$$x_1 = y_1 + y_2\zeta \quad \text{and} \quad x_2 = y_1 + y_2\zeta^2,$$

we get the generic polynomial

$$f(y_1, y_2, X) = X^3 - 3X + \frac{y_2^2 - 2y_1^2 + 2y_1y_2}{y_1^2 + y_2^2 - y_1y_2} \in K(y_1, y_2)[X].$$

Alternatively, we can let

$$x_1 = y_1 + y_2(\zeta - 1/\zeta) \quad \text{and} \quad x_2 = y_1 - y_2(\zeta - 1/\zeta)$$

and note that we may assume $y_2 = 1$ (since modifying x_1 by an element from $K(\mu_3)^*$ or by $\zeta - 1/\zeta$ will only change $\Phi(x_1)$ by a third power), giving us a generic polynomial

$$g(y, X) = X^3 - 3X - 2\frac{y^2 - 3}{y^2 + 3} \in K(y)[X].$$

Generic polynomials over the rational numbers. For use in Chapter 7 we will now take a closer look at the case $K = \mathbb{Q}$. Here, $d = p^{n-1}(p-1)$ and as e we can chose any generator for $\mathbb{Z}/p^2$.

In [SmG], Smith produces generic polynomials for C_q-extensions (over any field of characteristic $\neq p$) with only $d/2$ parameters. Over $\mathbb{Q}$, this is easy to achieve: In our construction above,

$$x_1 = y_1 + y_2\zeta + \cdots + y_d\zeta^{d-1}$$

is — as mentioned – a 'general element' in K_q. But we are only interested in $\Phi(x_1)$ up to a q^{th} power, and this allows us to modify x_1. In fact, we note that $\Phi(x)$ is, up to a q^{th} power, a product of powers of the conjugates of $\kappa^{d/2}x/x$, since the exponents of $\kappa^i x$ and $\kappa^{i+d/2}x$ add up to 0 modulo q. Thus, changing x_1 by a factor invariant under $\kappa^{d/2}$ will not change the extension we obtain. Also, since $\zeta - 1/\zeta$ changes its sign under $\kappa^{d/2}$, we have $\Phi(\zeta - 1/\zeta) = \pm 1$, which is a q^{th} power. All in all, we see that we can let

$$x_1 = y_1 + y_2(\zeta + 1/\zeta) + \cdots + y_{d/2}(\zeta + 1/\zeta)^{d/2-1} + (\zeta - 1/\zeta)$$

and still get everything by specialising.

This proves

THEOREM 5.3.5. (SMITH) *There is a generic C_q-polynomial over $\mathbb{Q}$ with $d/2$ parameters.*

REMARKS. (1) The construction in [SmG] extends the results from characteristic 0 to characteristic $\neq p$ by taking the cyclotomic extension to be $K_q = K[X]/(\Phi_q(X))$, where $\Phi_q(X) \in \mathbb{Z}[X]$ is the q^{th} cyclotomic polynomial. In this way, it becomes possible to do the calculations as if the field has characteristic 0.

(2) For $q = p$ a prime, an alternative construction (with $p - 1$ over $\mathbb{Q}$) of a generic C_p-polynomial is given in [Na].

The generic extensions constructed above have a very nice property: They possess normal bases. By a *normal basis* for a Galois extension S/R we mean an R-basis for S of the form $(\sigma\alpha)_{\sigma\in G}$ for a $\alpha \in S$. We wish to construct a normal basis for S/R, where S/R is the generic C_q-extension given above. We can do this by producing a κ-invariant normal basis for S_q/R_q. (For a more comprehensive treatment of normal bases of cyclic extensions, including descent, see [Gr, Ch. I].)

First, we note that an element $\alpha = \sum_{i=0}^{q-1} a_i\theta^i$ generates a normal basis for S_q/R_q if $a_i \in R_q^*$ for all i. This is obvious, since the matrix transforming the basis $(1, \theta, \ldots, \theta^{q-1})$ into $(\sigma\alpha)_{\sigma\in C_q}$ is invertible.

We claim that the a_i's can be chosen such that $\alpha \in S$:

Clearly, we can replace the basis $(1, \theta, \dots, \theta^{q-1})$ by a basis made up of

$$\begin{aligned}
&1,\\
&\quad \theta, \kappa\theta, \dots, \kappa^{d-1}\theta,\\
&\qquad \theta^p, \kappa\theta^p, \dots, \kappa^{d/p-1}\theta^p,\\
&\qquad\quad \dots,\\
&\qquad\qquad \theta^{p^{n-1}}, \kappa\theta^{p^{n-1}}, \dots, \kappa^{d/p^{n-1}-1}\theta^{p^{n-1}},
\end{aligned}$$

since we get all the exponents $0, 1, \dots, q-1$ of θ. Representing α in this basis, the condition $\kappa\alpha = \alpha$ translates as

$$\begin{aligned}
\alpha =& a_0 +\\
& a_1\theta + \kappa a_1 \kappa\theta + \dots + \kappa^{d-1} a_1 \kappa^{d-1}\theta +\\
& a_p\theta^p + \kappa a_p \kappa\theta^p + \dots + \kappa^{d/p-1} a_p \kappa^{d/p-1}\theta^p + \dots
\end{aligned}$$

where $a_0 \in R$, and $\kappa^{d/p^i} a_{p^i} \kappa^{d/p^i}\theta^{p^i} = a_{p^i}\theta^{p^i}$ for $i = 0, \dots, n-1$.

The element $\kappa^{d/p^i}\theta^{p^i}/\theta^{p^i}$ is in R'_q (since e has order d/p^i modulo q/p^i) and has norm 1 with respect to κ^{d/p^i}. Writing

$$\frac{\kappa^{d/p^i}\theta^{p^i}}{\theta^{p^i}} = x_1^{e_1} \cdots x_d^{e_d},$$

this simply means that $e_j + e_{d/p^i+j} + \dots + e_{(p^i-1)d/p^i+j} = 0$ for all $j = 1, \dots, d/p^i$, and we see that we can let

$$a_{p^i} = \prod_{j=1}^{d/p^i} \prod_{k=0}^{p^i-1} x_{kd/p^i+j}^{-(e_j + e_{d/p^i+j} + \dots + e_{kd/p^i+j})}.$$

Of course, we can modify a_{p^i} by a power of $x_1 \cdots x_d$ if we want to. (For instance, to make α integral over $\mathbb{Q}[y_1, \dots, y_d]$.)

Clearly, any specialisation of the generic extension S/R preserves the normal basis. In particular, the specialisation in $d/2$ parameters given above.

NOTE. It is not hard to see that every generic extension (over an infinite field) can be modified to have a normal basis: Let S/R be generic for G over K. This just means that it specialises to $K(\mathbf{t})/K(\mathbf{t})^G$ through a Galois homomorphism $\varphi\colon S \to K(\mathbf{t})$. Localising S and R in $\mathfrak{m} = \ker\varphi$ and $\mathfrak{p} = \mathfrak{m} \cap R$ gives us a Galois extension $S_{\mathfrak{m}}/R_{\mathfrak{p}}$ of local rings, and it is standard that $S_{\mathfrak{m}}$ (being finitely generated projective over $R_{\mathfrak{p}}$) is then free, and that any pre-images of a basis for $S_{\mathfrak{m}}/\mathfrak{m}$ over $R_{\mathfrak{p}}/\mathfrak{p}$ will be a basis. Thus, we can get a normal basis for $S_{\mathfrak{m}}/R_{\mathfrak{p}}$, and this will work for $S[1/s]/R[1/s]$ too, for a suitable $s \in R \setminus \mathfrak{p}$. Since K is infinite, $S[1/s]/R[1/s]$ is generic for G over K as well.

Thus, a generic extension can be localised to have a normal basis, cf. [Sa1, Cor. 5.4] (where it is proved that it can be localised to be free).

REMARK. In [Sa1], Saltman mentions some so-called 'Grunwald-Wang style' results. While we do not intend to give a comprehensive treatment of this subject,

we will nevertheless indicate what it is about, using the special case of odd-order cyclic groups over algebraic number fields:

Let K be an algebraic number field, and let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be r distinct finite primes in K. Also, let n be an odd number, and let there, for all $i = 1, \dots, r$, be given a cyclic extension $M_i/K_{\mathfrak{p}_i}$ of degree $d_i \mid n$, where $K_{\mathfrak{p}_i}$ is the localisation of K in $\mathfrak{p}_i$. By Proposition 1.1.8 in Chapter 1, these extensions are all obtained by specialising a generic C_n-polynomial $p(\mathbf{s}, X) \in K(\mathbf{s})[X]$ over $K_{\mathfrak{p}_i}$. For convenience, we add a prime $\mathfrak{p}_{r+1}$ and let $M_{r+1}/K_{\mathfrak{p}_{r+1}}$ be of degree n. By Krasner's Lemma and the Weak Approximation Theorem [Ja2, 9.2 p. 563], we may assume that the specialisation is in fact over K, and that it is the same for all $i = 1, \dots, r+1$. It follows that the splitting field M of this specialisation over K is a C_n-extension, and that it localises to the prescribed extensions in $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

The conclusion is: There exists a cyclic extension of K of degree n with prescribed ramification in any finitely many given finite primes.

5.4. Regular Cyclic 2-Extensions and Ikeda's Theorem

By Proposition 3.3.8 in Chapter 3 above and Corollary 5.3.3 above, there exists regular C_q-extensions over any field of characteristic $\neq p$, when $q = p^n$ is a power of the odd prime p.[4] Also, as remarked in the beginning of section 5.3, generic, and hence regular, C_q-extensions exists in characteristic p as well.

This leaves us with the case of C_q-extensions in characteristic $\neq 2$, when $q = 2^n$. Here, generic extensions do not necessarily exist, and so we will be content with simply constructing regular extensions. To this end we will use the following result, communicated to the authors by A. Yakovlev in St. Petersburg:

Lemma 5.4.1. *Let K be a field in characteristic $\neq 2$, and let $a \in K^* \setminus (K^*)^2$ be a norm in the cyclotomic extension $K(\mu_q)/K$, $q = 2^n$. Then $K(\sqrt{a})/K$ can be embedded in a cyclic extension of degree q.*

Remark. Note that a sum of two $2^{(n-1)\,\text{th}}$ powers in K is a norm in $K(\mu_q)/K$. Thus, we get a generalisation of the result from Theorem 2.2.5 in Chapter 2 that $K(\sqrt{a})/K$ can be embedded in a C_4-extension if a is a sum of two squares. (Another special case, $n = 3$, is easily deduced from Theorem 6.4.1 in Chapter 6.)

Proof of Lemma 5.4.1. Let ζ be a primitive q^{th} root of unity. For $\kappa \in \mathrm{Gal}(K(\mu_q)/K)$ we let $e_\kappa \in \mathbb{Z}$ be given by $\kappa\zeta = \zeta^{e_\kappa}$.

By assumption, $a = \mathrm{N}_{K(\mu_q)/K}(z)$ for a $z \in K(\mu_q)^*$. Let $b = \prod_\kappa \kappa^{-1} z^{e_\kappa}$. Then a and b are quadratically equivalent in $K(\mu_q)$, and if we let $S = K(\mu_q)[\omega]$, where $\omega^q = b$, we can extend an element $\lambda \in \mathrm{Gal}(K(\mu_q)/K)$ to S by

$$\lambda\omega = \prod_\kappa \kappa^{-1} z^{(e_{\kappa\lambda} - e_\kappa e_\lambda)/q}\, \omega^{e_\lambda}.$$

In this way, S/K becomes Galois with group $C_q \times \mathrm{Gal}(K(\mu_q)/K)$, and so it contains a C_q-subextension $L/K = S^{\mathrm{Gal}(K(\mu_q)/K)}/K$. The quadratic subextension of

[4] Since a regular extension over $\mathbb{F}_\ell(t)$ is regular over $\mathbb{F}_\ell$ as well, we need not assume K infinite.

$S/K(\mu_q)$ is $K(\mu_q)[\omega^{q/2}]$, and since $\sqrt{a} = \prod_\kappa \kappa^{-1} z^{(1-e_\kappa)/2}\,\omega^{q/2}$ is G_q-invariant, the quadratic subextension of L/K is $K(\sqrt{a})/K$. In particular, L is a field by the Remark on p. 91. □

It is now clear how to produce a regular C_q-extension: The regular quadratic extension $K(t, \sqrt{1+t^{2^{n-1}}})/K(t)$ is embeddable in a C_q-extension. This C_q-extension is then necessarily also regular.

EXAMPLE. Over $\mathbb{Q}(t)$, the polynomial

$$X^8 - 4X^6 + 2\frac{4t^2+1}{t^4+1}X^4 - 4\frac{t^2(t^2+1)}{(t^4+1)^2}X^2 + \frac{t^4}{(t^4+1)^3}$$

gives a regular C_8-extension with quadratic subextension

$$\mathbb{Q}(t, \sqrt{1+t^4})/\mathbb{Q}(t).$$

(And a regular M_{16}-extension over $\mathbb{Q}(t^2)$, where $M_{16} = C_8 \rtimes C_2$ with C_2 acting by taking fifth powers.)

Thus, we can conclude that regular cyclic extensions of prime power degree exist over any field, from which we immediately get

PROPOSITION 5.4.2. *Let K be a field and A a finite abelian group. Then there is a regular A-extension $\mathbb{M}/K(\mathbf{t})$ over K.*

Another consequence of Lemma 5.4.1 is the following result, due to Whaples ([Wh], and later Kuyk and Lenstra in [K&L]):

PROPOSITION 5.4.3. *If the field K has a C_4-extension, it has C_{2^n}-extensions for all $n \in \mathbb{N}$ (and in fact a pro-cyclic 2-extension).*

PROOF. If K has characteristic 2, the result follows by using Witt vectors [Ja2, 8.10–11], and if K contains the $2^{n\,\text{th}}$ roots of unity for all n, it is obvious. (In both cases, a C_2-extension is sufficient.) If the field $K(\mu_{2^\infty})$ obtained from K by adjoining the $2^{n\,\text{th}}$ roots of unity for all n is an infinite extension, it contains the cyclic extensions we seek. This leaves only one case: K has characteristic $\neq 2$, and $K(\mu_{2^\infty})/K$ is a non-trivial finite extension. It is then easy to see that $K(\mu_{2^\infty}) = K(i)$, where $i = \sqrt{-1}$, and Whaples' result follows from Lemma 5.4.1, since the assumption is that $N_{K(i)/K}(K(i)^*)$ contains a non-square in K^*, and this is then trivially a norm in $K(\mu_{2^n})/K$ for all n. (In the case of the pro-cyclic 2-extensions, we must look to the proof of Lemma 5.4.1, and note that we can use the same b for all n.) □

REMARK. Let us also note the following: By Saltman's Theorem 5.1.10 above, an affimative answer to the Noether Problem over an infinite field implies the existence of a generic extension. The opposite implication does *not* hold, since there is a generic C_{47}-extension over $\mathbb{Q}$, even though Swan [Swn1] proved that C_{47} does not satisfy the Noether Problem over $\mathbb{Q}$.

By Theorem 5.2.5, the existence of a generic extension over an infinite field is equivalent to the existence of a generic polynomial.

By Proposition 3.3.8 in Chapter 3, the existence of a generic G-polynomial implies the existence of a regular G-extension. Again, the opposite implication

fails, as shown above, since the is no generic C_8-polynomial over $\mathbb{Q}$, but certainly a regular C_8-extension.

Now, let K be a Hilbertian field, and let $\mathbb{M}/K(\mathbf{t})$, $\mathbf{t} = (t_1, \dots, t_r)$, be a regular A-extension over K, where A is a finite abelian group. Also, let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and assume that G acts on A. Consider the problem of embedding L/K along the projection $\pi\colon A \rtimes G \to G$. We wish to prove that this embedding problem is solvable:

We consider $n = |G|$ copies of the A-extension $\mathbb{M}L/L(\mathbf{t})$, and denote them $\mathbb{M}_1/L(\mathbf{t}_1)$, $\dots$, $\mathbb{M}_n/L(\mathbf{t}_n)$. We can then form the composite $N = \mathbb{M}_1 \cdots \mathbb{M}_n$ over $L(\mathbf{t}_1, \dots, \mathbf{t}_n)$ to get a regular A^n-extension.

Let G act transitively on $\{1, \dots, n\}$ and let $\sigma \in G$. If $\sigma i = j$, we have an isomorphism $L(\mathbf{t}_i) \simeq L(\mathbf{t}_j)$ given by

$$\sigma(at_{ik}) = \sigma a\, t_{jk}, \quad a \in L,\ k = 1, \dots, r.$$

This isomorphism extends to $\sigma\colon \mathbb{M}_i \simeq \mathbb{M}_j$, and we get G acting on N.

Since G acts semi-linearly on the L-vector space of linear forms in $L[\mathbf{t}_1, \dots, \mathbf{t}_n]$, there is a G-invariant basis $\mathbf{s} = (s_1, \dots, s_{rn})$ by the Invariant Basis Lemma, and we see that $L(\mathbf{t}_1, \dots, \mathbf{t}_n)^G = K(\mathbf{s})$.

It is now clear that $N/K(\mathbf{s})$ is an $A \wr G$-extension, where $A \wr G$ is the *wreath product*, cf. [Hu, I.§15]: $A \wr G = A^n \rtimes G$, where $\sigma \in G$ acts on $(a_\rho)_{\rho \in G} \in A^n$ by $\sigma(a_\rho)_\rho = (a_{\sigma^{-1}\rho})_\rho$.[5] Since $A \wr G$ maps onto $A \rtimes G$ by

$$\epsilon\colon [(a_\rho)_\rho, \sigma] \mapsto (\sum_\rho \rho a_\rho, \sigma),$$

there is an $A \rtimes G$-subextension containing $L(\mathbf{s})/K(\mathbf{s})$ as its G-subextension.

K is Hilbertian, and so, by Lemma 3.3.9 in Chapter 3, there is an $A \rtimes G$-extension M/K containing L/K as its G-subextension.

By Proposition 5.4.2 above, there *is* a regular A-extension of K, and so we have

THEOREM 5.4.4. (IKEDA) *Let K be a Hilbertian field, and let L/K be an Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Also, let A be a finite abelian group, and assume that G acts on A. Then there is an $A \rtimes G$-extension of K having L/K as its G-subextension.*

REMARKS. (1) In [Ik, 1960], Ikeda proves the following: If K is an algebraic number field, L/K a G-extension, and $\pi\colon E \to G$ an epimorphism of finite groups with $\ker\pi$ abelian, then L/K can be embedded in a *field* extension M/K along π if it can be embedded in a *Galois algebra* extension along π. This (with K replaced by a Hilbertian field) is obviously equivalent to the statement of the Theorem above.

(2) Ikeda's Theorem is a statement about split-exact embedding problems over Hilbertian fields: If it has abelian kernel, it is solvable. It seems reasonable to conjecture that the following, more general, statement holds: If it has nilpotent kernel, it is solvable. Over algebraic number fields, this is known to be true by a theorem of Shafarevich (cf. [Sha] or [IL&F, Thm. 5.5.4]). Faddeyev's Theorem

[5] For convenience, we index the coordinates in A^n by G instead of by $\{1, \dots, n\}$.

(Theorem 6.1.11 in Chapter 6 below) is an example of a split-exact embedding problem with nilpotent non-abelian kernel being solvable over any Hilbertian field. (Of course, Corollary 3.3.13 is an example of a split-exact embedding problem with — for $n \geq 5$ – simple kernel being solvable over Hilbertian fields.)

(3) It is clear that what we actually proved is the following: Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and assume that G acts on the finite abelian group A. Then the split-exact embedding problem given by L/K and $A \rtimes G \twoheadrightarrow G$ has a *parametric solution*. Here, a parametric solution, as defined in [M&M2, Ch. IV], to the embedding problem given by a Galois extension L/K (with Galois group G) and an epimorphism $\pi\colon E \to G$ is a solution $\mathbb{M}/K(\mathbf{t})$ to the embedding problem given by $L(\mathbf{t})/K(\mathbf{t})$ and π for some set $\mathbf{t} = (t_1, \ldots, t_r)$ of indeterminates, such that $\mathbb{M}/L(\mathbf{t})$ is regular over L. This result is due to Uchida [U]. (Note that the use of the term 'parametric' here is not in accordance with our use of it in 'parametric polynomial'. For our purposes, a parametric solution should be something that specialised to all actual solutions.)

5.5. Dihedral Groups

We looked at the dihedral groups D_4 and D_5 in of Chapter 2. We will now consider generic polynomials for dihedral groups in greater generality.

Definition 5.5.1. Let $n \in \mathbb{N}$. The *dihedral* group of degree n is the group D_n generated by elements σ and τ with relations $\sigma^n = \tau^2 = 1$ and $\tau\sigma = \sigma^{n-1}\tau$.

If A is a finite abelian group, the *generalised dihedral* group D_A is the semi-direct product $A \rtimes C_2$, where C_2 operates on A by inversion.

If $A \simeq C_{a_1} \times \cdots \times C_{a_r}$, we will also denote D_A by $D_{a_1 \times \cdots \times a_r}$.

Remarks. (1) By Furtwängler [Fu], the Noether Problem holds true for D_p when $p = 3$, 5, 7 or 11. This, in particular, implies that there exist generic polynomials over $\mathbb{Q}$ with the Galois group D_p. As we shall see below, generic polynomials in fact exist for D_q for all odd numbers q.

(2) D_n is the simplest non-abelian group. Geometrically, D_n is the symmetry group of the regular n-gon.

(3) It is quite easy to describe D_n-extensions over fields containing the primitive n^{th} roots of unity: $X^{2n} + sX^n + t^n$ is generic. However, it is far from obvious how to descend to, say, $\mathbb{Q}$.

Dihedral groups of odd prime power degree. In [Sa1, §3], Saltman proves various results concerning generic extensions for semi-direct products, most notably wreath products. In this section we adapt these results to produce generic extensions — and hence generic polynomials — over $\mathbb{Q}$ for dihedral groups of degree q, where $q = p^n$ is an odd prime power. The more general result will be covered in section 7.2 of Chapter 7 below.

We start by making the following observation: $C_q \times D_q \simeq C_q \wr C_2$, and the factor C_q on the left corresponds to the C_2-invariant subgroup N of $C_q \times C_q$ on the right. (Here, $C_q \wr C_2$ denotes the wreath product, cf. section 5.4 above.

So, whenever we have a $C_q \wr C_2$-extension S/K, we get (canonically) a D_q-subextension S^N/K. On the other hand, if S'/K is a D_q-extension, $S/K = K^q \otimes_K S'/K$ is a $C_q \wr C_2$-extension by Theorem 4.2.9 in Chapter 4, and $S^N = S'$.

Thus, we can study $C_q \wr C_2$-extensions in the assurance that we will get all D_q-extensions in the process.[6] This is a clear advantage, since $C_q \wr C_2$ is easier to handle than D_q.

Now, assume the following: S/R is a generic C_q-extension over $\mathbb{Q}$, σ generates the group $C_q = \operatorname{Aut}_R S$, and $R = \mathbb{Q}[\mathbf{y}, 1/y]$, where $\mathbf{y} = (y_1, \dots, y_d)$ are indeterminates and $y \in \mathbb{Q}[\mathbf{y}] \setminus 0$.

We let $R_1 = \mathbb{Q}[\mathbf{s}, \mathbf{t}, u, 1/su]$, where $\mathbf{s} = (s_1, \dots, s_d)$, $\mathbf{t} = (t_1, \dots, t_d)$ and u are indeterminates, and $s \in \mathbb{Q}[\mathbf{s}, \mathbf{t}, u]$ is given by

$$s = y(s_1 + t_1\sqrt{u}, \dots, s_d + t_d\sqrt{u})y(s_1 - t_1\sqrt{u}, \dots, s_d - t_d\sqrt{u}).$$

Also, we let $R_2 = \mathbb{Q}[\mathbf{s}, \mathbf{t}, \sqrt{u}, 1/su]$. Then R_2/R_1 is a generic C_2-extension over $\mathbb{Q}$. We denote the generator for $\operatorname{Aut}_{R_1} R_2$ by κ.

Next, we define homomorphisms $\varphi_1, \varphi_2 \colon R \to R_2$ by

$$\varphi_1(y_i) = s_i + t_i\sqrt{u} \quad \text{and} \quad \varphi_2(y_i) = s_i - t_i\sqrt{u}.$$

This gives us specialisations $S_1 = S \otimes_{\varphi_1} R_2$ and $S_2 = S \otimes_{\varphi_2} R_2$, that will be C_q-extensions of R_2 with generators σ_1 and σ_2. We can then extend κ to an R_1-isomorphism $S_1 \simeq S_2$ by $\kappa(s \otimes r_2) = s \otimes \kappa r_2$. This works both ways to give us $\kappa^2 = 1$ and $\kappa\sigma_1 = \sigma_2\kappa$. Thus, we have κ acting on $T = S_1 \otimes_{R_2} S_2$. It is almost obvious that T/R_1 is a $C_q \wr C_2$-extension, and we claim that it is in fact generic:

Let U/K be a $C_q \wr C_2$-extension in characteristic 0. Then we have $U = T_1 \otimes_L T_2$, where L/K is the quadratic subextension, and T_1/L and T_2/L are conjugate C_q-extensions. Now, $L = K[\bar{u}]$ for some $\bar{u}^2 = a \in K^*$, and T_1/L is obtained by specialising S/R with respect to a map $y_i \mapsto a_i + b_i\bar{u}$. The map $\psi \colon R_2 \to L$, given by

$$\psi \colon \sqrt{u} \mapsto \bar{u}, \quad s_i \mapsto a_i, \quad t_i \mapsto b_i,$$

will then give T_1/L by specialisation as well. Also, since $\kappa S_1 = S_2$ and $\kappa T_1 = T_2$, the same specialisation give us T_2/L from S_2/R_2, and hence U/L from T/R_2. Letting $\varphi = \psi|_{R_1}$, this means that $T \otimes_\varphi K \simeq U$.

It follows from this and the remarks above that T^N/R_1 is generic for D_q-extensions over $\mathbb{Q}$.

Now, generic C_q-extensions are described in detail in section 5.3 above, where we established that they can be constructed to have normal bases: There is an element $\alpha \in S$ such that $\alpha, \sigma\alpha, \dots, \sigma^{q-1}\alpha$ is a basis for S/R. Looking at T/R_1 above, this means that there are elements β_1 and $\beta_2 = \kappa\beta_1$ in T, such that $\beta_i, \sigma_i\beta_i, \dots, \sigma_i^{q-1}\beta_i$ is a basis for S_i/R_2, and hence such that $\{\sigma_1^i\beta_1 \otimes \sigma_2^j\beta_2 \mid 0 \le i, j < q\}$ is a basis for T/R_2.

The trace $\operatorname{Tr}_{T/T^N} \colon T \to T^N$ is surjective and R_2-linear, and so the traces of the elements $\sigma_1^i\beta_1 \otimes \sigma_2^j\beta_2$ generate T^N over R_2. Since there are only q distinct

[6] Provided, of course, that we look at Galois *algebras*, and not just fields.

traces $\alpha_i = \sum_{j=0}^{q-1} \sigma_1^j \beta_1 \otimes \sigma_2^{i+j} \beta_2$, these elements form a basis for T^N/R_2. Also, as they are conjugate, it is a normal basis.

Let

$$f(\mathbf{s}, \mathbf{t}, u, X) = \prod_{i=0}^{q-1} (X - \alpha_i).$$

Then $f \in \mathbb{Q}(\mathbf{s}, \mathbf{t}, u)[X]$, since α_0 is κ-invariant. As T^N/R_1 is a generic D_q-extension, we have the following: For every D_q-extension L/K in characteristic 0, there is a specialisation of f over K with splitting field L over the quadratic subextension of L/K. This immediately implies that L is in fact the splitting field over K of the specialised polynomial, and we conclude that f is generic for D_q-extensions over $\mathbb{Q}$.

PROPOSITION 5.5.2. *A generic polynomial for D_q-extensions over $\mathbb{Q}$ exists and can be explicitly constructed.*

In fact, assume that an element $\beta = \sum_{i=0}^{q-1} a_i \theta^i$ generating a normal basis for S/R has been found as described in section 5.3, where a_i is a rational monomial in $x_1, \ldots, x_d$. Then the construction is follows:

As above, $q = p^n$, $d = p^{n-1}(p-1)$ and e generates $\mathbb{Z}/q$. We introduce indeterminates u, $\mathbf{s} = (s_1, \ldots, s_d)$ and $\mathbf{t} = (t_1, \ldots, t_d)$. In $\mathbb{Q}(\mathbf{s}, \mathbf{t}, \sqrt{u})$ we let new 'indeterminates' $\mathbf{x}_1 = (x_{11}, \ldots, x_{1d})$ and $\mathbf{x}_2 = (x_{21}, \ldots, x_{2d})$ be given by

$$s_j + t_j\sqrt{u} = \sum_{i=1}^{d} \zeta^{(i-1)e^{j-1}} x_{1i} \quad \text{and} \quad s_j - t_j\sqrt{u} = \sum_{i=1}^{d} \zeta^{(i-1)e^{j-1}} x_{2i},$$

where $\zeta = \exp(2\pi i/q)$. Next, we let

$$\theta_1 = \sqrt[q]{x_{11}^{e^{d-1}} x_{12}^{e^{d-2}} \cdots x_{1d}} \quad \text{and} \quad \theta_2 = \sqrt[q]{x_{21}^{e^{d-1}} x_{22}^{e^{d-2}} \cdots x_{2d}}.$$

With

$$\beta_1 = a_0(\mathbf{x}_1) + a_1(\mathbf{x}_1)\theta_1 + \cdots + a_{q-1}(\mathbf{x}_1)\theta_1^{q-1},$$
$$\beta_2 = a_0(\mathbf{x}_2) + a_1(\mathbf{x}_2)\theta_2 + \cdots + a_{q-1}(\mathbf{x}_2)\theta_2^{q-1},$$

the generic polynomial is

$$f(\mathbf{s}, \mathbf{t}, u, X) = \prod_{i=0}^{q-1} (X - \sum_{j=0}^{q-1} \sigma_1^i \beta_1 \, \sigma_2^{i+j} \beta_2),$$

where σ_1 and σ_2 are given by $\sigma_1\theta_1 = \zeta\theta_1$, $\sigma_1\theta_2 = \theta_2$, $\sigma_2\theta_1 = \theta_1$ and $\sigma_2\theta_2 = \zeta\theta_2$.

EXAMPLE. Look at the simplest case, $q = 3$. Using the simplifications from the example in section 5.3, we find that a generic D_3-polynomial over $\mathbb{Q}$ is given by

$$f(s_1, s_2, t_1, t_2, u, X) = X^3 - 9X^2 + \frac{324(s_1t_2 - s_2t_1)^2 u}{S^2 - T^2 u},$$

with parameters s_1, s_2, t_1, t_2 and u, and with

$$S = s_1^2 + s_1s_2 + s_2^2 + u(t_1^2 + t_1t_2 + t_2^2),$$
$$T = 2s_1t_1 + s_1t_2 + s_2t_1 + 2s_2t_2.$$

Of course, this polynomial is more complicated than the $X^3 + tX + t$ given in section 2.1 of Chapter 2. However, it allows us to 'control' the quadratic subextension, since this is given by u. For example, letting $s_1 = s_2 = t_2 = 1$ and $u = t_1 = -1$ and scaling X, we get a polynomial $X^3 - 3X^2 - 12$ with Galois group D_3, such that the splitting field has quadratic subextension $\mathbb{Q}(i)/\mathbb{Q}$.

By scaling X it is easy to see that $X^3 + X^2 + t$ is generic for D_3-extensions over $\mathbb{Q}$. From this we can recover $X^3 + tX + t$ by inverting t and changing indeterminate.

Remarks. This construction immediately gives various additional results:

(1) Let $q_1, \dots, q_r$ be powers of odd (not necessarily distinct) primes, and let $f_1(\mathbf{s}_1, \mathbf{t}_1, u, X), \dots, f_r(\mathbf{s}_r, \mathbf{t}_r, u, X)$ be the corresponding generic polynomials as constructed above. Since a $D_{q_1 \times \dots \times q_r}$-extension is the composite of D_{q_1}-, …, D_{q_r}-extensions with the same quadratic subextension, it is clear that

$$f_1(\mathbf{s}_1, \mathbf{t}_1, u, X) \cdots f_r(\mathbf{s}_r, \mathbf{t}_r, u, X) \in \mathbb{Q}(\mathbf{s}_1, \dots, \mathbf{s}_r, \mathbf{t}_1, \dots, \mathbf{t}_r, u)[X]$$

is generic for $D_{q_1 \times \dots \times q_r}$-extensions over $\mathbb{Q}$. In particular, this allows for construction of generic D_n-polynomials for all odd numbers n, since $D_{q \times q'} = D_{qq'}$ when q and q' are mutually prime.

(2) Let n be an odd number, and assume that $f(\mathbf{s}, \mathbf{t}, u, X) \in \mathbb{Q}(\mathbf{s}, \mathbf{t}, u)[X]$ is a generic D_n-polynomial as above. Then

$$f(\mathbf{s}, \mathbf{t}, u, X)(X^2 - v)$$

is generic for D_{2n}-extensions, since $D_{2n} = C_2 \times D_n$. Also,

$$f(\mathbf{s}, \mathbf{t}, t' - 1, X)(X^4 - 2s't'X^2 + s'^2t'(t' - 1)) \in \mathbb{Q}(\mathbf{s}, \mathbf{t}, s', t')[X]$$

is generic for D_{4n}-extensions over $\mathbb{Q}$ by Corollary 2.2.8. Finally,

$$f\big(\mathbf{s}, \mathbf{t}, \frac{1 - 2y^2}{1 + x^2 - 2z^2} - 1, X\big)G(x, y, z, r, q, X) \in \mathbb{Q}(\mathbf{s}, \mathbf{t}, r, q, x, y, z)[X]$$

is generic for D_{8n}-extensions, when $G(x, y, z, r, q, X)$ is the generic polynomial from Corollary 6.5.4 in Chapter 6 below.

Thus, the above example makes it possible to describe generic polynomials for $D_{3\times3}$-, D_6-, D_{12}- and D_{24}-extensions.

(3) If we prefer *irreducible* polynomials, we can use Sylvester resultants as in Chapter 2: Suppose that a $D_{q \times q'}$-extension is the composite of D_q- and $D_{q'}$-extensions obtained as splitting fields of $f(X)$ and $g(X)$, respectively. Then

$$h(X) = \mathrm{Res}((-1)^q f(X - Y), g(Y))$$

is an irreducible polynomial of degree qq' with the $D_{q \times q'}$-extension as splitting field, since it has as its roots exactly the sum of the roots of $f(X)$ and $g(X)$. For instance, we get the $D_{3\times3}$-polynomial

$$X^9 - 15X^6 - 87X^3 - 125 \in \mathbb{Q}[X]$$

if we start with the D_3-polynomials $X^3 - 2$ and $X^3 - 3$, cf. [Wil, 5.2]. Similarly, taking

$$f(X) = X^3 - 3X^2 - 12 \quad \text{and} \quad g(X) = X^5 + \frac{1}{4}X + \frac{6}{5},$$

we get a polynomial

$$\begin{aligned} h(X) = X^{15} - 15X^{14} + 90X^{13} - 330X^{12} + \frac{4503}{4}X^{11} - \frac{69753}{20}X^{10} \\ + 7929X^9 - 17604X^8 + \frac{618411}{16}X^7 - \frac{4891281}{80}X^6 \\ + \frac{25155189}{200}X^5 - \frac{6693669}{40}X^4 + \frac{7649897}{320}X^3 - \frac{60891747}{320}X^2 \\ + \frac{1186983}{100}X - \frac{578469219}{2000} \in \mathbb{Q}[X] \end{aligned}$$

with Galois group D_{15} over $\mathbb{Q}$. And with

$$f(X) = X^3 - 9X^2 - \frac{2268}{43}$$

and

$$g(X) = X^7 - 7X^6 - 7X^5 - 7X^4 - 1$$

we can produce a (decidedly unpleasant looking) D_{21}-polynomial with corresponding quadratic extension $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$. We will, however, refrain from actually *doing* that.

As the examples demonstrate, a reducible polynomial is likely to be much more convenient than an irreducible polynomial. This carries over to generic polynomials, of course.

The Hashimoto-Miyake construction. The construction given above is very general, but also quite involved. In contrast, Hashimoto and Miyake [H&M] gave a very elegant description of generic D_n-polynomials for odd n, using only a single parameter. Unfortunately, it is not done over $\mathbb{Q}$, but over $\mathbb{Q}(\cos\frac{2\pi}{n})$, and this restriction is essential for the argument.[7]

Their construction is based on the following observation, cf. Chapter 2: Let $\omega = 2\cos\frac{2\pi}{n}$, where n is odd. Let ζ be a corresponding primitive n^{th} root of unity, i.e., $\omega = \zeta + 1/\zeta$. Then we get a linear representation $D_n \hookrightarrow \mathrm{GL}_2(\mathbb{Q}(\omega))$ by

$$\sigma \mapsto \mathbf{S} = \begin{pmatrix} 0 & -1 \\ 1 & \omega \end{pmatrix}, \qquad \tau \mapsto \mathbf{T} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and the induced projective representation $D_n \to \mathrm{PGL}_2(\mathbb{Q}(\omega))$ remains injective.

Remark. This is where we need n to be odd. If n is even, we get $D_{n/2} \hookrightarrow \mathrm{PGL}_2(K)$. However, by the Remark on p. 23 in Chapter 1, it is always possible to find a generic polynomial with two parameters.

For any field K, the projective linear group $\mathrm{PGL}_2(K)$ acts on the function field $K(X)$ by

$$\mathbf{A}X = \frac{aX + c}{bX + d} \quad \text{for} \quad \mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and this gives us the entire automorphism group $\mathrm{Aut}_K\, K(X)$, cf. [Ja2, 8.14].

[7] And, as we shall see in Chapter 8, for the result.

Thus, for $K \supseteq \mathbb{Q}(\omega)$, we have D_n acting on $K(X)$ by

$$\sigma X = \frac{1}{\omega - X} \quad \text{and} \quad \tau X = \frac{1}{X},$$

and by Lüroth's Theorem we have a D_n-extension $K(X)/K(U)$ for some $U \in K(X)$. This D_n-extension is 'very general' by

LEMMA 5.5.3. *Let M/K be a D_n-extension of a field K containing $\mathbb{Q}(\omega)$. Then $M = K(x)$ for an $x \in M^*$ with*

$$\sigma x = \frac{1}{\omega - x} \quad \textit{and} \quad \tau x = \frac{1}{x}.$$

PROOF. By Proposition 1.1.1 in Chapter 1, there exists $u, v \in M$, linearly independent over K, such that

$$\sigma u = v, \quad \sigma v = -u + \omega v, \quad \tau u = v \quad \text{and} \quad \tau v = u.$$

Letting $x = u/v$, we get $x \notin K$ and

$$\sigma x = \frac{1}{\omega - x}, \quad \tau x = \frac{1}{x}.$$

If $M = K(x)$, we are through. Otherwise, there is a $\rho \in D_n \setminus 1$ such that $\rho x = x$. Since D_n acts on x by fractional linear action corresponding to the matrix representation, we have

$$x = \rho x = \frac{a'x + b'}{c'x + d'}$$

for suitable $a', b', c', d' \in K$, and hence x satisfies a non-trivial equation of degree ≤ 2 over K. Since $x \notin K$, this means that $K(x)/K$ is the quadratic subextension of M/K, i.e.,

$$\sigma x = x \quad \text{or} \quad x(\omega - x) = 1,$$

i.e., $x = \zeta$ or $x = 1/\zeta$.

Thus, we are in the following situation: $K(\zeta)/K$ is the quadratic subextension of M/K. It follows easily that $M = K(\zeta, \sqrt[n]{a})$ for some $a \in K$, such that σ and τ are given by

$$\begin{aligned} \sigma\colon &\quad \sqrt[n]{a} \mapsto \zeta \cdot \sqrt[n]{a}, \quad \zeta \mapsto \zeta, \\ \tau\colon &\quad \sqrt[n]{a} \mapsto \sqrt[n]{a}, \qquad \zeta \mapsto 1/\zeta. \end{aligned}$$

Let

$$u = (1 + 1/\zeta)\sqrt[n]{a} + \frac{1+\zeta}{\sqrt[n]{a}} \quad \text{and} \quad v = (1+\zeta)\sqrt[n]{a} + \frac{1 + 1/\zeta}{\sqrt[n]{a}}.$$

Then u and v are linearly independent over $K(\zeta)$ and

$$\sigma u = v, \quad \sigma v = -u + \omega v, \quad \tau u = v \quad \text{and} \quad \tau v = u.$$

Hence, we can let $x = u/v$ and get the desired element, since $x \notin K(\zeta)$. □

From this it should be clear that a generic polynomial can be gotten from the extension $K(X)/K(U)$.

Regarding our D_n-extension M/K with $K \supseteq \mathbb{Q}(\omega)$, we notice that

$$\mathbf{S} = \begin{pmatrix} 1 & 1 \\ \zeta & 1/\zeta \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & 1/\zeta \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \zeta & 1/\zeta \end{pmatrix}^{-1},$$

from which it follows that

$$\mathbf{S}^i = \begin{pmatrix} -\xi_{i-1} & \xi_i \\ -\xi_i & \xi_{i+1} \end{pmatrix},$$

where $\xi_i = (\zeta^i - 1/\zeta^i)/(\zeta - 1/\zeta) \in K$. (If we let $\omega_i = \zeta^i + 1/\zeta^i = 2\cos\frac{2\pi i}{n}$, we can rewrite ξ_i as $\xi_i = \omega_{i-1} + \omega_{i-3} + \ldots$.) We let

$$V = \sum_{i=0}^{n-1} \sigma^i X = \sum_{i=0}^{n-1} \frac{-\xi_{i-1}X + \xi_i}{-\xi_i X + \xi_{i+1}} = \frac{P(X)}{Q(X)}$$

with

$$P(X) = \sum_{i=0}^{n-1} (-\xi_{i-1}X + \xi_i) \prod_{j \neq i} (-\xi_j X + \xi_{j+1})$$

and

$$Q(X) = \prod_{i=0}^{n-1} (-\xi_i X + \xi_{i+1}) = X \prod_{i=1}^{n-2} (-\xi_i X + \xi_{i+1}).$$

It is easily seen that the polynomials $-\xi_i X + \xi_{i+1}$, $i = 0, \ldots, n-1$, are mutually prime, and hence so are $P(X)$ and $Q(X)$. Since $\deg Q(X) = n - 1$, we must have $\deg P(X) = n$ and $K(X)^{\langle\sigma\rangle} = K(V)$.

Next, we note that

$$X^n Q(1/X) = X \prod_{i=1}^{n-2} (-\xi_i + \xi_{i+1} X) = Q(X),$$

since $\xi_i = -\xi_{n-i}$. Thus,

$$U = V(X)V(1/X) = \frac{P(X)P(1/X)}{Q(X)Q(1/X)} = \frac{X^n P(X)P(1/X)}{Q(X)^2}$$

is not a constant, and by Lüroth's Theorem we have

$$K(X)^{D_n} = K(V)^{\langle\tau\rangle} = K(U).$$

On the other hand,

$$\begin{aligned} V(X) + V(1/X) &= \mathrm{Tr}_{K(X)/K(V)}(X) + \mathrm{Tr}_{K(X)/K(V)}(1/X) \\ &= \mathrm{Tr}_{K(X)/K(V)}(\sigma^{-1}X + 1/X) = \mathrm{Tr}_{K(X)/K(V)}(\omega) = n\omega \end{aligned}$$

is a constant, meaning that

$$\frac{P(X)^2}{Q(X)^2} - n\omega\frac{P(X)}{Q(X)} + \frac{X^n P(X)P(1/X)}{Q(X)^2} = 0.$$

Hence,

$$X^n P(1/X) = n\omega Q(X) - P(X)$$

and

$$U = \frac{P(X)[n\omega Q(X) - P(X)]}{Q(X)^2}.$$

Let $\eta = \prod_{i=1}^{n-1} \xi_i$. Then

$$P(X) - n\zeta Q(X) = \eta(X - \zeta)^n,$$

which follows by noting that

$$P(X) - n\zeta Q(X) = (X - \zeta) \sum_{i=0}^{n-1} \zeta^i \prod_{j \neq i} (-\xi_j X + \xi_{j+1})$$

and that

$$\sum_{i=0}^{n-1} \zeta^i \prod_{j \neq i} (-\xi_j X + \xi_{j+1}) = \eta(X - \zeta)^{n-1}.$$

(The latter is easily seen, since the left- and right-hand sides are polynomials of degree $n - 1$, have the same leading coefficient η, and coincide at the points ξ_{i+1}/ξ_i, $i = 1, \ldots, n - 1$.)

Similarly,

$$P(X) - n\zeta^{-1} Q(X) = \eta(X - 1/\zeta)^n,$$

and so

$$P(X)^2 - n\omega P(X)Q(X) + n^2 Q(X)^2 = \eta^2 (X^2 - \omega X + 1)^n.$$

Letting $s = X + 1/X - \omega$ and $t = U - n^2$, we get $K(t) = K(U)$ and $K(s) = K(X)^{\langle \tau \rangle}$, as well as

$$\begin{aligned} 0 &= P(X)^2 - n\omega P(X)Q(X) + UQ(X)^2 \\ &= P(X)^2 - n\omega P(X)Q(X) + n^2 Q(X)^2 + tQ(X)^2 \\ &= \eta^2 (X^2 - \omega X + 1)^n + tQ(X)^2, \end{aligned}$$

and, after division by X^n, we obtain

$$\eta^2 s^n + tQ(X)Q(1/X) = 0.$$

As

$$\begin{aligned} Q(X)Q(1/X) &= \prod_{i=1}^{n-2} (-\xi_i X + \xi_{i+1})(-\xi_i \frac{1}{X} + \xi_{i+1}) \\ &= \prod_{i=1}^{n-2} (\xi_i^2 + \xi_{i+1}^2 - \xi_i \xi_{i+1} \omega - \xi_i \xi_{i+1} s) = \prod_{i=1}^{n-2} (1 - \xi_i \xi_{i+1} s), \end{aligned}$$

we conclude that the minimal polynomial for s over $K(t)$ is

$$F(t, Y) = Y^n + t\eta^{-2} \prod_{i=1}^{n-2} (1 - \xi_i \xi_{i+1} Y) \in K(t)[Y].$$

By Lemma 5.5.3, this polynomial is generic for D_n-extensions over $\mathbb{Q}(\omega)$.

Now, a specialisation of $F(t,Y)$ to give a D_n-extension cannot be at $t=0$, and so we can look at

$$G(t,Y) = tY^n F(\eta^2/t, 1/Y) = \prod_{i=0}^{n-1}(Y-\xi_i\xi_{i+1}) + t \in K(t)[Y]$$

instead. Thus, we have proved

THEOREM 5.5.4. (HASHIMOTO & MIYAKE) *For odd n, the polynomial*

$$G(t,Y) = \prod_{i=0}^{n-1}(Y-\xi_i\xi_{i+1}) + t$$

is generic for D_n-extensions over $\mathbb{Q}(\omega)$.

EXAMPLES. (1) For $n=3$, we get $G(t,Y) = Y^3+Y^2+t$, cf. the example in section 5.5 above.

(2) For $n=5$, we get $G(t,Y) = Y^5+(1-3\omega)Y^4+(3-5\omega)Y^3+(2-3\omega)Y^2+t$.

In [H&M], the polynomials are computed for $n=7$, 9 and 11 as well.

REMARK. It is clear that cyclic polynomials can be constructed in a analogous manner, cf. Exercise 5.13 below. See also [Mi] and [Ri]. Assuming $2\cos\frac{2\pi}{n}$ or $e^{2\pi i/n}$ to be an element of K, generic polynomials have been constructed for various cyclic and meta-cyclic groups by Rikuna and Hashimoto.

5.6. p-Groups in characteristic p

As mentioned several times already, it was proved by Gaschütz, in his paper [Ga] from 1959, that a Linear Noether Problem for a p-group over a field of prime characteristic p always have an affirmative answer. Thus, if the field is infinite we get generic polynomials by Proposition 1.1.3 in Chapter 1.

Gaschütz' result is an obvious consequence of the following Lemma, which is a slight generalisation of Satz 2 in [Ga], together with the easily proven fact that for a field K of characteristic p any p-subgroup of $\mathrm{GL}_n(K)$ can, by conjugation, be brought to consist of upper triangular matrices. (Exercise 5.14 below.) A further generalisation of Gaschütz' result is proved in [Miy], cf. also Exercise 5.15 below.

LEMMA 5.6.1. *Let K be an arbitrary field and G a finite group, and assume that G acts faithfully on a rational function field $K(\mathbf{x}) = L(x_1,\dots,x_n)$ such that $\sigma K = K$ and $\sigma x_i - x_i \in K(x_1,\dots,x_{i-1})$ for all $\sigma \in G$ and all $i = 1,\dots,n$. Then the extension $K(\mathbf{x})^G/K^G$ of fixed fields is again rational.*

PROOF. The Lemma follows by induction from the case $n=1$. Thus, we let G act on $K(x)$ with $\sigma K = K$ and $\sigma x - x = u_\sigma \in K$ for $\sigma \in G$.

Consider first the case where G acts faithfully on K. Then $\sigma \mapsto u_\sigma = \sigma x - x$ is an additive crossed homomorphism $G \to K$, and by the additive Hilbert 90 (Lemma A.1.2(a) in Appendix A) there exists $u \in K$ with $\sigma x - x = \sigma u - u$. We then have $x-u \in K(x)^G$ and thus

$$K(x)^G = K(x-u)^G = K^G(x-u).$$

In the case where G does *not* act faithfully on K, we look at the subgroup

$$N = \{\sigma \in G \mid \sigma|_K = 1_K\}$$

of elements acting trivially on K. Clearly, N is normal in G. Also, $\sigma \mapsto u_\sigma$ is a homomorphism from N into K, and as it is necessarily injective, we conclude that K has prime characteristic p and that N is an elementary abelian p-group.

Now, the polynomial

$$h(X) = \prod_{\sigma \in N} (X - u_\sigma) \in K[X]$$

is clearly vectorial, cf. the Example of p. 19 in Chapter 1. Furthermore, since $\sigma u_\rho = u_{\sigma\rho\sigma^{-1}}$ for $\sigma \in G$ and $\rho \in N$, we get that $h(X) \in L^G[X]$, and thus that

$$\sigma h(x) = h(\sigma x) = h(x) + h(u_\sigma) \text{ for all } \sigma \in G.$$

It follows that we can look at the G/N-action on $K(x)^N = K(h(x))$ instead, bringing us back to the situation considered above. □

This immediately demonstrates the existence of generic extensions and generic polynomials for p-groups over *infinite* fields of characteristic p. We will now proceed to give a general construction resulting in substantially fewer parameters: For a group of order p^n, Gaschütz' result could be used to infer the existence of a generic polynomial with p^n parameters. We will, however, prove that no more than n are needed.

Constructing the polynomials. In order to carry out the construction, we will need the observations about Galois extensions in prime characteristic made in section A.1 of Appendix A. We will retain the notations introduced in Appendix A in what follows.

First of all, we note the following, cf. [Wi1]: If K is a field of prime characteristic p and G is a p-group, we can construct a G-extension of K starting from a $G/\Phi(G)$-extension, where $\Phi(G)$ is the Frattini group, by using a composition series

$$G_0 = 1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{r-1} \lhd G_r = \Phi(G)$$

of $\Phi(G)$ with each G_i normal in G: All the group extensions

$$0 \to \mathbb{F}_p \to G/G_{i-1} \to G/G_i \to 1, \quad i = 1, \ldots, r,$$

are non-split, and the corresponding embedding problems therefore solvable.

Moreover, at each step the element θ_ω we adjoin can be found in an 'algorithmic' way using the results from Appendix A about additive crossed homomorphisms, factor systems and elements with trace 1.

We will now produce a generic G-extension in characteristic p, and to this end we will make the following

Assumption: Our ground field K is $\mathbb{F}_p(u)$.

For non-cyclic groups this is no restriction, since a finite field have only cyclic extensions anyway, and we just get u as an additional parameter in a generic polynomial. We will consider cyclic groups separately below.

Elementary abelian groups. We start our construction by considering the case where G is elementary abelian: $G \simeq C_p^r$. To this end we pick an injective group homomorphism $\varphi\colon C_p^r \hookrightarrow K$ and let C_p^r act on the function field $K(t)$ by $\sigma t = t + \varphi(\sigma)$. The polynomial

$$h(X) = \prod_{\sigma \in C_p^r} (X - \varphi(\sigma))$$

is vectorial, cf. Chapter 2, meaning that the minimal polynomial for t over $K(t)^{C_p^r}$ is

$$h(X - t) = h(X) - h(t),$$

and hence that $K(t)^{C_p^r} = K(h(t))$. We let $s = h(t)$. Then $K[t]/K[s]$ is a generic C_p^r-extension, and $g(s, X) = h(X) - s$ is generic for C_p^r over K: If M/L is a C_p^r-extension with $L \supseteq K$, the map $\varphi\colon C_p^r \to K \subseteq M$ is a crossed homomorphism, and so we have $\sigma\omega = \omega + \varphi(\sigma)$ for some $\omega \in M$. Then $M = L(\omega)$, the specialisation $t \mapsto \omega$ is equivariant, and the minimal polynomial for ω over L is $g(h(\omega), X)$.

NOTE. As for getting an element of trace 1 inside $K[t]/K[s]$, we proceed as follows: The trace of t^k, $0 \leq k < p^r$, is

$$\mathrm{Tr}_{K[t]/K[s]}(t^k) = \sum_{\sigma \in C_p^r} (t + \varphi(\sigma))^k = \sum_{\sigma \in C_p^r} \varphi(\sigma)^k,$$

i.e., the k^{th} Newton power sum q_k of the roots of $h(X)$. Since

$$h(X) = X^{p^r} + a_{r-1}X^{p^{r-1}} + \cdots + a_1 X^p + a_0 X,$$

most of the elementary symmetric symbols $s_1, \ldots, s_{p^r}$ are zero, with $s_{p^r - p^{r-1}}$, $s_{p^r - p^{r-2}}, \ldots, s_{p^r - p}, s_{p^r - 1}$ being the only possible exceptions. (Here, $s_{p^r-1} = a_0$ *is* non-zero, since $h(X)$ does not have multiple roots.) From the recursive formula

$$q_n - s_1 q_{n-1} + \cdots + (-1)^{n-1} q_1 s_{n-1} + (-1)^n n s_n = 0, \quad 1 \leq n < p^r,$$

for power sums (cf. e.g. [Lo1, Exc. 15.24] or [Ja1, §2.13 Exc. 3]) we then see that all the q_k's are zero, until we get to $k = p^r - 1$, where we have

$$q_{p^r-1} + (-1)^{p^r-1}(p^r - 1)s_{p^r-1} = 0,$$

i.e., $q_{p^r-1} = s_{p^r-1} = a_0$. Hence, an element of trace 1 is t^{p^r-1}/a_0.

General p-groups. Next, assume that G is obtained from a non-split group extension

$$0 \to \mathbb{F}_p \to G \to H \to 1,$$

and that we have already produced a generic extension

$$K[\mathbf{t}]/K[\mathbf{s}] = K[t_1, \ldots, t_r]/K[s_1, \ldots, s_r]$$

for H, together with an element z of trace 1. As in Appendix A, we get an additive crossed homomorphism from the factor system, and hence an $\omega \in K[t]$ such that the G-extensions containing $K(\mathbf{t})/K(\mathbf{s})$ are $K(\mathbf{t}, \theta_{r+\omega})/K(\mathbf{s})$, $r \in K(\mathbf{s})$. We then get our generic G-extension as $K[\mathbf{t}, \theta_{s_{r+1}+\omega}]/K(\mathbf{s}, s_{r+1})$ and a new element of trace 1 as $-z\theta_{s_{r+1}+\omega}^{p-1}$.

This is in fact a generic G-extension: If M/L is a G-extension with $L \supseteq K$, we can specialise $K[\mathbf{t}]/K[\mathbf{s}]$ to get the H-subextension. Since the construction of ω respects G-homomorphisms, we then get M by some specialisation of s_{r+1}. We then let $t_{r+1} = \theta_{s_{r+1}+\omega}$. (That our extension is in fact Galois follows from Exercise 4.4 in Chapter 4.)

As for producing a generic polynomial, we can of course simply invoke Proposition 5.1.8. However, we can do better: Whenever we specialise $K[\mathbf{t}]/K[\mathbf{s}]$ to get some specific G-extension M/L, we can do it as indicated above, by specialising the s_i's one at a time. In doing that, we have some freedom in our choice, since the specialisation of s_i can be changed by adding $\wp a$ for any $a \in L$, $\wp$ being the Witt vector map defined below in the section on cyclic groups. (Except of course for s_1, where $h(a)$ can be added.) Since the field L is infinite, this implies that the specialisation can be chosen in such a way that any prescribed non-zero polynomial in $K[\mathbf{s}]$ maps to a non-zero element in L. This specialisation can then of course be extended to the localisation of $K[\mathbf{s}]$ in the kernel. From this we easily see that we can choose the specialisation to ensure that any given primitive element for $K(\mathbf{t})/K(\mathbf{s})$ has a well-defined specialisation in M, and that this specialisation is again a primitive element. Consequently, we have

PROPOSITION 5.6.2. *Let G be a finite p-group, and let $K(\mathbf{t})/K(\mathbf{s})$ be the G-extension constructed above. Any monic polynomial $P(\mathbf{s}, X) \in K(\mathbf{s})[X]$ with splitting field $K(\mathbf{t})$ is then generic for G over $K = \mathbb{F}_p(u)$. If G is non-cyclic, it is also generic over $\mathbb{F}_p$ when we consider u as a parameter.*

The number of parameters (over K) is $e + 1$, if $|\Phi(G)| = e$, which can be thought of as 'logarithmically better' than the number $p^n = |G|$ provided by Gaschütz' result.

REMARK. An alternative proof of this Proposition is to prove that a specialisation of $K[\mathbf{t}]/K[\mathbf{s}]$ giving the Noether Extension $K(\mathbf{x})/K(\mathbf{x})^G$ can be chosen such that the images of the s_i's are algebraically independent, i.e., we can embed $K(\mathbf{t})/K(\mathbf{s})$ into $K(\mathbf{x})/K(\mathbf{x})^G$. The result then follows from Kemper and Mattig's result in Proposition 1.1.7 of Chapter 1.

Cyclic groups. If the group is cyclic, i.e., $\simeq C_{p^n}$, we cannot be certain that the polynomial produced above is generic over $\mathbb{F}_p$. In this case, however, there is the classical theory of *Witt vectors*, cf. [Ja2, §§8.10–8.11] or [Wi2] (the original paper by Witt from 1937).

We will assume the basic theory of Witt vectors known, and will denote the ring of n-dimensional Witt vectors over a field L by $W_n(L)$. Also, we let $\wp\colon W_n(L) \to W_n(L)$ be the map

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

We note that $\mathbf{a} = (a_0, \dots, a_{n-1}) \in W_n(L)$ is invertible if an only if $a_0 \neq 0$, from which it easily follows $W_n(M)/W_n(K)$ is a Galois extension with group G whenever M/K is. Also, exactly as for Galois field extensions, we can prove Hilbert 90 and the additive Hilbert 90 (Lemma A.1.2(a) in Appendix A): A

map $f\colon G \to W_n(M)^*$ satisfying $f_{\sigma\tau} = f_\sigma \sigma f_\tau$ has the form

$$f_\sigma = \sigma\mathbf{a}/\mathbf{a}$$

for some $\mathbf{a} \in W_n(M)^*$, and a map $g\colon G \to W_n(M)$ satisfying $g_{\sigma\tau} = g_\sigma + \sigma g_\tau$ has the form

$$g_\sigma = \sigma\mathbf{b} - \mathbf{b}$$

for some $\mathbf{b} \in W_n(M)$.

Now, let M/K be a C_{p^n}-extension in characteristic p, and let σ be a generator for $C_{p^n} = \mathrm{Gal}(M/K)$. Since $1 \in W_n(K)$ has trace 0, there exists, by the above results, an $\mathbf{a} \in W_n(M)$ with $\sigma\mathbf{a} = \mathbf{a} + 1$. It follows immediately that $M = K(\mathbf{a})$ (i.e., $M = K(a_0, \dots, a_{n-1})$). Also, $K(a_i)/K$ has degree p^{i+1} for $i = 0, \dots, n-1$.

To get a generic description, we consider a rational function field $K(\mathbf{t}) = K(t_0, \dots, t_{n-1})$ and define a C_{p^n}-action by $\sigma\colon \mathbf{t} \mapsto \mathbf{t} + 1$. Then $K(\mathbf{t})^{C_{p^n}} = K(\mathbf{s})$ for $\mathbf{s} = \wp\mathbf{t}$, and in fact $K[\mathbf{t}]^{C_{p^n}} = K[\mathbf{s}]$.

Hence, the minimal polynomial for t_{n-1} over $K(\mathbf{s})$ is generic for C_{p^n} in characteristic p.

Thus we have

PROPOSITION 5.6.3. *There is a generic polynomial with n parameters for C_{p^n} over $\mathbb{F}_p$.*

REMARK. The extension $\mathbb{F}_p[\mathbf{t}]/\mathbb{F}_p[\mathbf{s}]$ is in fact generic: In the argument above, we can let M/K be a Galois algebra, and the argument will still hold.

Semi-direct products. The number of parameters in the generic polynomials constructed above is small compared to the group order, and so it is natural to ask whether it is in fact optimal. We are not able to say much about that in general, but we will now proceed to show that at least *some* p-groups allow an even smaller number of parameters:

Let $q = p^n$ be a power of p, and let $a \in (\mathbb{Z}/q)^* = W_n(\mathbb{F}_p)^*$ be an element of multiplicative order $d \mid p^{n-1}(p-1)$. If M/K is a C_d-extension in characteristic p and σ a generator for the Galois group $C_d = \mathrm{Gal}(M/K)$, it is clear that a has norm 1 in $W_n(M)/W_n(K)$, and hence that there exists an $\boldsymbol{\alpha} \in W_n(M)^*$ with $\sigma\boldsymbol{\alpha} = a\,\boldsymbol{\alpha}$. Then $M = K(\boldsymbol{\alpha})$ and $\alpha^d \in W_n(K)$.

REMARK. While $\boldsymbol{\alpha}$ can be considered as a d^{th} root of an element in $W_n(K)$, this is not as useful an observation here as it is in ordinary Kummer theory, since there are in general far too many d^{th} roots of unity in $W_n(K)$. For example, we have $(1, x_1, \dots, x_{n-1})^{p^{n-1}} = 1$ for all $x_1, \dots, x_{n-1} \in K$.

THEOREM 5.6.4. *Let A be a subgroup of $(\mathbb{Z}/q)^*$, and let it act on the rational function field $K(\mathbf{t}) = K(t_0, \dots, t_{n-1})$ by $a\colon \mathbf{t} \mapsto a\,\mathbf{t}$. Then $K(\mathbf{t})^A/K$ is rational.*

PROOF. Clearly, A is the direct product of a p-group and a cyclic group of order $d \mid p-1$.

Consider first the case where $A = C_d$, $d \mid p-1$. Then $A = \langle a \rangle$, where $a = (a, 0, \dots, 0)$, and the action on $K(\mathbf{t})$ is given by $a\colon t_i \mapsto a t_i$. From

$$(\mathbf{t}^d)^{(p^n-1)/d} = \mathbf{t}^{p^n-1} = \mathbf{t}^{-1}(t_0, 0, \dots, 0)^{p^n}$$

we see that $K(\mathbf{t}) = K(\mathbf{t}^d, t_0)$, and hence that $K(\mathbf{t})^{C_d} = K(\mathbf{t}^d)$.

This reduces the general case to that where A is a p-group, i.e., all elements in A are $\equiv 1 \pmod p$. This in particular means that the image of t_i is $t_i + u_i$ for a $u_i \in K(t_0, \dots, t_{i-1})$, and the result follows by Lemma 5.6.1. □

EXAMPLE. Let p be odd, and let $A = \langle 1 + p^{n-1} \rangle$. Then

$$(t_0, \dots, t_{n-1}) \mapsto (t_0, \dots, t_{n-2}, t_{n-1} + t_0^{p^{n-1}}),$$

and so $K(\mathbf{t})^{C_p} = K(t_0, \dots, t_{n-2}, t_{n-1}^p - t_0^{p^{n-1}(p-1)} t_{n-1})$.

Let G be the group

$$G = C_{p^n} \rtimes C_d = \left\langle \sigma, \tau \mid \sigma^{p^n} = \tau^d = 1,\ \tau\sigma = \sigma^a \tau \right\rangle,$$

where $a \in (\mathbb{Z}/q)^*$ has order $d \mid (p-1)p^{n-1}$, and let M/K be a G-extension in characteristic p. Also, let $L = M^{C_{p^n}}$.

Then $M = L(\boldsymbol{\alpha})$ for some $\alpha \in W_n(M)$ with $\sigma\boldsymbol{\alpha} = \boldsymbol{\alpha} + 1$, and by our 'Kummer theory' above we also have $L = K(\boldsymbol{\beta})$ for a $\boldsymbol{\beta} \in W_n(L)^*$ with $\tau\boldsymbol{\beta} = a\,\boldsymbol{\beta}$.

Now, $\tau\boldsymbol{\alpha} \in W_n(M)$ and $\sigma(\tau\boldsymbol{\alpha}) = \tau\sigma^{a^{-1}}\boldsymbol{\alpha} = \tau\boldsymbol{\alpha} + a^{-1}$, meaning that $\tau\boldsymbol{\alpha} = a^{-1}\boldsymbol{\alpha} + \mathbf{x}$ for some $\mathbf{x} \in W_n(L)$.

Since $\tau^d = 1$, we get

$$\boldsymbol{\alpha} = \tau^d\boldsymbol{\alpha} = \tau^{d-1}\mathbf{x} + a^{-1}\tau^{d-2}\mathbf{x} + \cdots + a^{-(d-1)}\mathbf{x} + a^{-d}\boldsymbol{\alpha}$$

or

$$a\,\mathbf{x} + a^2\tau\mathbf{x} + \cdots + a^{d-1}\tau^{d-1}\mathbf{x} = 0.$$

This means that $\mathbf{x}\boldsymbol{\beta}$ has trace 0 in $W_n(L)/W_n(K)$, and so there exists a $\mathbf{y} \in W_n(L)$ with $\tau\mathbf{y} - \mathbf{y} = \mathbf{x}\boldsymbol{\beta}$.

Let $\boldsymbol{\gamma} = \boldsymbol{\alpha} - a\boldsymbol{\beta}^{-1}\mathbf{y}$. Then $\sigma\boldsymbol{\gamma} = \boldsymbol{\gamma} + 1$ and $\tau\boldsymbol{\gamma} = a^{-1}\boldsymbol{\gamma}$.

Thus: $M = K(\boldsymbol{\gamma})$ for a $\boldsymbol{\gamma} \in W_n(M)$ with $\sigma\boldsymbol{\gamma} = \boldsymbol{\gamma} + 1$ and $\tau\boldsymbol{\gamma} = a^{-1}\boldsymbol{\gamma}$.

Also: If we let G act on a rational function field $K(\mathbf{t})$ by $\sigma\mathbf{t} = \mathbf{t} + 1$ and $\tau\mathbf{t} = a^{-1}\mathbf{t}$, we have $K(\mathbf{t})^{C_{p^n}} = K(\wp\mathbf{t})$ and $\tau\wp\mathbf{t} = a^{-1}\wp\mathbf{t}$. Thus, we get an extension $K(\mathbf{t})/K(\mathbf{t})^G$ of rational function fields, and can get an n-parameter generic G-polynomial over K by taking a monic polynomial over $K(\mathbf{t})^G$ with splitting field $K(\mathbf{t})$. (As before, we have sufficient freedom in the choice of $\boldsymbol{\gamma}$, since we can replace it by $\boldsymbol{\gamma} + \mathbf{b}\wp\boldsymbol{\gamma}$ for any Witt vector $\mathbf{b}$ with coefficients in the ground field.)

EXAMPLES. (1) If $d \mid p-1$, we have $\mathbb{F}_p(\mathbf{t})^G = \mathbb{F}_p((\wp\mathbf{t})^d)$ and can get a generic polynomial of degree p^n by taking the minimal polynomial over $\mathbb{F}_p(\mathbf{s}) = \mathbb{F}_p((\wp\mathbf{t})^d)$ for the $(n-1)^{\text{th}}$ coefficient of $\mathbf{t}^d$.

For example, consider the case $q = p$ for p odd, where the group is the Frobenius group $F_{pd} = C_p \rtimes C_d$. Then $s = (t^p - t)^d$, and we are looking for the minimal polynomial $g(s, X)$ of t^d over $\mathbb{F}_p(s)$. As the minimal polynomial for t is

$$f(s, X) = (X^p - X)^d - s,$$

we have

$$g(s, X) = f(s, X^{1/d}) = \sum_{i=0}^{d} \binom{d}{i} (-1)^{d-i} X^{i(p-1)/d+1} - s,$$

and this is a generic F_{pd}-polynomial over $\mathbb{F}_p$.

In particular, we find that $X^p - 2X^{(p+1)/2} + X - s$ is generic for the dihedral group D_p over $\mathbb{F}_p$.

(2) For $p = 2$, we get an n-parameter generic polynomial for the dihedral group D_{2^n} of degree 2^n and order 2^{n+1} when $n \geq 2$.

In the simplest case, $n = 2$, we have

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau \rangle,$$

and we get a D_4-action on $\mathbb{F}_2(s,t)$ by

$$\sigma(s,t) = (s,t) + 1 = (s+1, t+s)$$

and

$$\tau(s,t) = -(s,t) = (s, t+s^2).$$

The fixed field under σ is

$$\mathbb{F}_2(\wp(s,t)) = \mathbb{F}_2(s^2+s, t^2+t+s^2+s^3)$$

and the fixed field under τ is $\mathbb{F}_2(s, t^2+s^2t)$. Thus, we get the fixed field under D_4 to be

$$\begin{aligned}\mathbb{F}_2(s,t)^{D_4} &= \mathbb{F}_2(s^2+s, (t^2+t+s^2+s^3)^2 + (s^2+s)^2(t^2+t+s^2+s^3)) \\ &= \mathbb{F}_2(s^2+s, t^4+t^2+s^2t^2+s^4t^2+s^2t+s^4t+s^5+s^7) \\ &= \mathbb{F}_2(u,v).\end{aligned}$$

The Galois closure of $\mathbb{F}_2(u,v)(t^2+s^2t)$ over $\mathbb{F}_2(u,v)$ is $\mathbb{F}_2(s,t)$, and so the minimal polynomial of t^2+s^2t over $\mathbb{F}_2(u,v)$ is generic for D_4 over $\mathbb{F}_2$ with parameters u and v. This polynomial is

$$\begin{aligned}h(u,v,X) = X^4 + X^3 + u^3X^2 \\ + (u^2+u^3+u^4+v)X + (u^7+u^2v+u^3v+v^2).\end{aligned}$$

The general construction would give a D_4-extension

$$\mathbb{F}_2(s,t,u,\theta_{(s+t)\theta_s+u}, \theta_t)/\mathbb{F}_2(s,t,u),$$

from which we would get a three-parameter polynomial.

Exercises

EXERCISE 5.1. Let S/R be Galois with group G, and assume R to be an integrally closed domain.

(1) Assume that S is a domain with quotient field L. Prove that S is the integral closure of R in L.

(2) Prove that $S = \mathrm{Ind}_H^G(T)$ for some subgroup H of G and a Galois extension T/R of domains with group H.

EXERCISE 5.2. It is well-known from algebraic number theory that any proper finite extension $K/\mathbb{Q}$ has ramified primes. (MINKOWSKI's Theorem.) Use this to prove that the only Galois extension of $\mathbb{Z}$ with respect to a given finite group G is the 'split' extension $\mathrm{Ind}_1^G(\mathbb{Z})/\mathbb{Z} = \mathbb{Z}^{|G|}/\mathbb{Z}$.

EXERCISE 5.3. Let R be an integrally closed domain with quotient field K, let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and let S be the integral closure of R in L. Assume that L is the splitting field over K of the monic polynomial $f(X) \in R[X]$ and that $d = d(f) \neq 0$. Prove that $S[1/d]/R[1/d]$ is a Galois extension with group $\mathrm{Gal}(L/K)$.

EXERCISE 5.4. (1) Assume that all the roots of

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$$

are real, and that $a_0 \neq 0$. Prove that $f(X)$ cannot have two consecutive zero coefficients (i.e., $a_i = a_{i+1} = 0$ for some $i < n$).

(2) Let G be a finite group, and let n be the smallest number for which $G \hookrightarrow S_n$. Let $P(\mathbf{t}, X) \in \mathbb{Q}(\mathbf{t})[X]$ be a generic G-polynomial over $\mathbb{Q}$ of degree n. Prove that $P(\mathbf{t}, X)$ cannot have two consecutive zero coefficients. [Hint: Exercise 3.5 in Chapter 3.]

EXERCISE 5.5. Let L/K be a field extension and t an indeterminate. Prove that L/K is retract-rational if and only if $L(t)/K$ is. [Hint to 'if': Let $\varphi\colon R \to T$ express the retract-rationality of $L(t)/K$. For some $a \in K$, we have $T \subseteq L[t]_{(t-a)}$. Now extend T, such that the specialisation of T in a sits inside T itself.]

EXERCISE 5.6. Let K be an infinite field, and let $E = N \rtimes G$ be a semi-direct product of the finite groups N and G. Prove: If there exists a generic E-polynomial over K, then there exists a generic G-polynomial as well, with the same number of parameters. In particular: For finite groups G and H, there exists a generic $G \times H$-polynomial over K, if and only if there exist generic G- and H-polynomials over K.

EXERCISE 5.7. Prove the equivalent of Exercise 3.5 in Chapter 3 for p-adic fields: Assume that there is a generic G-polynomial over $\mathbb{Q}$, and let p be a prime. Prove the existence of a G-extension of $\mathbb{Q}$ contained in the field $\mathbb{Q}_p$ of p-adic numbers.

EXERCISE 5.8. Let p be a prime, and let K be a field of characteristic $\neq p$ containing the primitive p^{th} roots of unity. Prove: If $a \in K \setminus K^p$ is a norm in the $p^{n\,\text{th}}$ cyclotomic extension, then $K(\sqrt[p]{a})/K$ can be embedded in a C_{p^n}-extension. In particular: Assuming $p \notin K^p$, prove that $K(\sqrt[p]{p})/K$ can be embedded in C_{p^n}-extensions for all $n \in \mathbb{N}$.

EXERCISE 5.9. Let K be a field of characteristic $\neq 2$. Prove that the polynomial

$$X^{2n} + s_{n-1}X^{2(n-1)} + \cdots + s_1X^2 + s_0,$$

with parameters $s_0, \ldots, s_{n-1}$, is generic for $C_2 \wr S_n$ over K.

EXERCISE 5.10. Let A and G be finite groups with A Abelian, and assume that G acts on A by automorphisms. Consider the the wreath product $A \wr G$ as defined in section 5.4, as well as the homomorphism $\epsilon\colon A \wr G \twoheadrightarrow A \rtimes G$ given there.

Prove: If the the group order $|A|$ and $|G|$ have greatest common divisor 1, then ϵ is *split*, i.e., there exists a group homomorphism

$$\iota\colon A \rtimes G \to A \wr G$$

with $\epsilon \circ \iota = 1_{A \rtimes G}$. Conclude that we then have

$$A \wr G \simeq A^{n-1} \rtimes (A \rtimes G)$$

for a suitable action of $A \rtimes G$ on A^{n-1}.

EXERCISE 5.11. Find a generic polynomial $f(s,t,X)$ for D_3 over $\mathbb{Q}$, such that the splitting field over $\mathbb{Q}(s,t)$ contains $\mathbb{Q}(s,\sqrt{t})$.

EXERCISE 5.12. Find a generic $D_{3\times 3}$-polynomial over $\mathbb{Q}$ with two parameters.

EXERCISE 5.13. Let $K = \mathbb{Q}(2\cos\frac{2\pi}{n})$, where n is odd and $\neq 3$. Prove that there is a generic C_n-polynomial over K with one parameter.

EXERCISE 5.14. Let K be field in prime characteristic p, and let $P \subseteq \mathrm{GL}_n(K)$ be the subgroup consisting of upper triangular matrices with 1's in the diagonal.

(1) Prove that every element in P has finite p-power order.

(2) Let G be a finite subgroup of $\mathrm{GL}_n(K)$ of p-power order. Prove that $\sigma G \sigma^{-1} \subseteq P$ for some $\sigma \in \mathrm{GL}_n(K)$. [Hint: First prove that there exists an non-zero G-invariant vector in K^n.]

EXERCISE 5.15. Prove the following results, due to Miyata [Miy]:

(1) Let K be a field and G a finite group, and assume that G acts faithfully on $K(t)$ in such a way that $\sigma K = K$ and σt is a linear polynomial in t for all $\sigma \in G$. Prove that $K(t)^G/K^G$ is rational.

(2) If the finite subgroup G of $\mathrm{GL}_n(K)$ consists of upper triangular matrices, then $K(x_1,\ldots,x_n)^G/K$ is rational.

CHAPTER 6

Solvable Groups I: *p*-Groups

In this chapter, we consider the generic description of some p-groups as Galois groups in characteristic $\neq p$, specifically the dihedral, quasi-dihedral and quaternion groups of order 16, and the Heisenberg groups:

For $n \geq 2$, there are four non-abelian groups of order 2^{n+1} and exponent 2^n, namely

(1) The *dihedral group* D_{2^n} of degree 2^n, given as

$$D_{2^n} = \langle \sigma, \tau \mid \sigma^{2^n} = \tau^2 = 1,\ \tau\sigma = \sigma^{2^n-1}\tau \rangle;$$

(2) The *quasi-dihedral group* QD_{2^n} of degree 2^n, given as

$$QD_{2^n} = \langle u, v \mid u^{2^n} = 1,\ v^2 = u^{2^{n-1}},\ vu = u^{2^{n-1}-1}v \rangle;$$

(3) The *quaternion group* $Q_{2^{n+1}}$ of order 2^{n+1}, given as

$$Q_{2^{n+1}} = \langle x, y \mid x^{2^{n-1}} = 1,\ y^2 = x^{2^{n-2}},\ yx = x^{2^{n-1}-1}y \rangle;\ \text{and}$$

(4) The *modular group* $M_{2^{n+1}}$ of order 2^{n+1}, given as

$$M_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1,\ ba = a^{2^{n-1}+1}b \rangle.$$

We will not be concerned with the modular group, and will look at the others primarily in the case $n = 3$.

All of these groups can be defined in greater generality, cf. the definition of dihedral groups in Chapter 2.

Remarks. (1) The dihedral, quasi-dihedral and modular groups are semi-direct products with the cyclic group C_2 acting on the cyclic group C_{2^n}. The quaternion group Q_{2^n} can be realised as a subgroup of the multiplicative group $\mathbb{H}^*$ of the Hamiltonian quaternions $\mathbb{H}$, i.e., the four-dimensional $\mathbb{R}$-algebra generated by elements i and j with relations

$$i^2 = j^2 = -1, \quad ji = -ij,$$

by letting

$$x = \exp(i\pi/2^{n-2}) = \cos(\pi/2^{n-2}) + i\sin(\pi/2^{n-2}), \quad y = j.$$

In particular, Q_8 can be considered as consisting of the quaternions ± 1, $\pm i$, $\pm j$ and $\pm k$, where $k = ij$. (We will have more to say about quaternion algebras in section 6.1 below.)

(2) The quasi-dihedral group (sometimes called the *semi-dihedral* group) QD_{2^n} is a sort of 'cross-breed' between D_{2^n} and $Q_{2^{n+1}}$: Like D_{2^n}, it is a semi-direct

product, and like $Q_{2^{n+1}}$, it contains Q_{2^n} as a subgroup (generated by u^2 and v). The inclusion $Q_8 \subseteq QD_8$ will prove important later, in section 6.3 below.

For an odd prime p, there are two non-abelian groups of order p^3, namely

(1) The *Heisenberg group*

$$H_{p^3} = \left\langle u, v, w \;\middle|\; \begin{array}{l} u^p = v^p = w^p = 1,\ vu = uvw, \\ wu = uw,\ wv = vw \end{array} \right\rangle;$$

and

(2) The semi-direct product

$$C_{p^2} \rtimes C_p = \langle x, y \mid x^{p^2} = y^p = 1,\ yx = x^{p+1}y \rangle.$$

We will only look at the Heisenberg group. With appropriate modifications, everything we say about H_{p^3} will work for $C_{p^2} \rtimes C_p$ as well. (Making these modifications is left as Exercise 6.10.)

We refer to Blue's Thesis [Blu] for more on generic polynomials for groups of order p^3, p prime.

6.1. Quaternion Groups

We define a *quaternion extension* as a Galois extension with Galois group isomorphic to Q_8.

PROBLEMS. (1) Characterize fields K that admit quaternion extensions.

(2) Find a generic polynomial for quaternion extensions over K.

The characteristic 2 case is covered by the results of section 5.6 of Chapter 5, and so we will assume all fields to have characteristic $\neq 2$.

The main result is

THEOREM 6.1.1. (WITT 1936, [Wi1]) *Let M/K be a V_4-extension, i.e., $M = K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K^*$. Then M/K can be embedded in a quaternion extension if and only if the quadratic forms $aX^2+bY^2+abZ^2$ and $U^2+V^2+W^2$ are equivalent over K. Furthermore, if $\mathbf{P}$ is a 3×3 matrix such that $\det \mathbf{P} = 1/ab$ and*

$$\mathbf{P}^t \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix} \mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

the quaternion extensions containing M/K are

$$K(\sqrt{r(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{a}\sqrt{b})})/K, \quad r \in K^*.$$

The condition $aX^2+bY^2+abZ^2 \sim U^2+V^2+W^2$ is known as *Witt's Criterion*.

REMARK. If, instead of $\mathbf{P}$, we are given a matrix $\mathbf{Q}$ with determinant ab, such that

$$\mathbf{Q}^t\mathbf{Q} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix},$$

we find the quaternion extensions to be

$$K(\sqrt{r(1 + q_{11}/\sqrt{a} + q_{22}/\sqrt{b} + q_{33}/\sqrt{a}\sqrt{b})})/K, \quad r \in K^*.$$

This is clear, since we can let $\mathbf{P} = \mathbf{Q}^{-1}$.

Before the proof proper we need to make a few preliminary observations:

First of all, the Galois group $\mathrm{Gal}(M/K)$ can be identified with the Klein Vierergruppe V_4. Let $\sigma, \tau \in V_4 = \mathrm{Gal}(M/K)$ be given by

$$\begin{aligned} \sigma\colon &\quad \sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}, \\ \tau\colon &\quad \sqrt{a} \mapsto \sqrt{a}, \quad\ \ \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

Suppose that $F/K = M(\sqrt{\omega})/K$, $\omega \in M^*$, is a quaternion extension. By Kummer theory, we then have $\sigma\omega/\omega = x^2$ and $\tau\omega/\omega = y^2$ for some $x, y \in M^*$, and we can extend σ and τ to F by

$$\sigma\sqrt{\omega} = x\sqrt{\omega} \quad \text{and} \quad \tau\sqrt{\omega} = y\sqrt{\omega}.$$

Since these extensions are essentially i and j in Q_8, we must then have

$$x\,\sigma x = -1, \quad y\,\tau y = -1 \quad \text{and} \quad x\,\sigma y = -y\,\tau x$$

(from $i^2 = -1$, $j^2 = -1$ and $ij = -ji$ in Q_8).

Conversely, suppose that we have $x, y, \omega \in M^*$ satisfying these three relations, as well as $\sigma\omega/\omega = x^2$ and $\tau\omega/\omega = y^2$. This ω cannot be a square in M, and the extension

$$F/K = M(\sqrt{\omega})/K$$

is clearly a quaternion extension. By Lemma A.1.1, all the quaternion extensions containing M/K are then $M(\sqrt{r\omega})/K$ for $r \in K^*$.

Finally, if $M(\sqrt{\omega})/K$ is a quaternion extension, $M(\sqrt{\omega})$ and $K(\sqrt{\omega})$ must in fact coincide: Since $\sqrt{\omega}$ changes sign under the element in $\mathrm{Gal}(M(\sqrt{\omega})/K)$ corresponding to -1, this element cannot be in $\mathrm{Gal}(M(\sqrt{\omega})/K(\sqrt{\omega}))$. But the only subgroup of Q_8 not containing -1 is 1.

And now for the proof of Witt's Criterion (including his description of quaternion extensions).[1] Since the two parts, 'if' and 'only if', are proved in significantly different ways, we present them separately:

Sufficiency of Witt's Criterion. Let $\mathbf{E}$ be the 3×3 unit matrix, and let

$$\mathbf{A} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix}.$$

[1] In [Wi1], there is a typographical error in this description: The term 1+ is missing.

We have $\mathbf{P}^t\mathbf{A}\mathbf{P} = \mathbf{E}$ by assumption, and get the additional matrix equations $\mathbf{P}^t\mathbf{A}\mathbf{P} = \mathbf{E}$, $\mathbf{P}^{-1} = \mathbf{P}^t\mathbf{A}$ and $\mathbf{P}\mathbf{P}^t = \mathbf{A}^{-1}$. Looking at the diagonals, we see that

$$\begin{cases} ap_{11}^2 + bp_{21}^2 + abp_{31}^2 = 1, \\ ap_{12}^2 + bp_{22}^2 + abp_{32}^2 = 1, \\ ap_{13}^2 + bp_{23}^2 + abp_{33}^2 = 1, \\ p_{11} = b(p_{22}p_{33} - p_{23}p_{32}), \\ p_{22} = a(p_{11}p_{33} - p_{13}p_{31}), \\ p_{33} = p_{11}p_{22} - p_{12}p_{21}. \\ p_{11}^2 + p_{12}^2 + p_{13}^2 = 1/a, \\ p_{21}^2 + p_{22}^2 + p_{23}^2 = 1/b, \text{ og} \\ p_{31}^2 + p_{32}^2 + p_{33}^2 = 1/ab. \end{cases}$$

We let

$$\omega = 1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{a}\sqrt{b}$$

and

$$x = \sqrt{a}\,\frac{p_{31}\sqrt{b} - p_{13}}{\omega}, \quad y = \sqrt{b}\,\frac{p_{32}\sqrt{a} - p_{23}}{\omega}.$$

Now

$$\begin{aligned} \omega\,\sigma\omega &= (1 + p_{22}\sqrt{b})^2 - a(p_{11} + p_{33}\sqrt{b})^2 \\ &= (1 + bp_{22}^2 - ap_{11}^2 - abp_{33}^2) + 2(p_{22} - ap_{11}p_{33})\sqrt{b} \\ &= (bp_{21}^2 + abp_{31}^2 + bp_{22}^2 - abp_{33}^2) - 2ap_{13}p_{31}\sqrt{b} \\ &= (1 - bp_{23}^2 + abp_{31}^2 - abp_{33}^2) - 2ap_{13}p_{31}\sqrt{b} \\ &= (ap_{13}^2 + abp_{31}^2) - 2ap_{13}p_{31}\sqrt{b} \\ &= a(p_{13} - p_{31}\sqrt{b})^2 = x^2\omega^2, \end{aligned}$$

and similarly

$$\omega\,\tau\omega = y^2\omega^2.$$

It follows that

$$\frac{\sigma\omega}{\omega} = x^2, \quad \frac{\tau\omega}{\omega} = y^2.$$

Furthermore,

$$x\,\sigma x = -1, \quad y\,\tau y = -1,$$

and

$$\begin{aligned}\frac{x\,\sigma y}{y\,\tau x} &= \frac{\sqrt{a}(p_{31}\sqrt{b}-p_{13})\omega^{-1}\sqrt{b}(-p_{32}\sqrt{a}-p_{23})\sigma\omega^{-1}}{\sqrt{b}(p_{32}\sqrt{a}-p_{23})\omega^{-1}\sqrt{a}(-p_{31}\sqrt{b}-p_{13})\tau\omega^{-1}}\\ &= \frac{b(p_{32}\sqrt{a}+p_{23})(p_{32}\sqrt{a}-p_{23})}{a(p_{31}\sqrt{b}+p_{13})(p_{31}\sqrt{b}-p_{13})}\\ &= \frac{abp_{32}^2-bp_{23}^2}{abp_{31}^2-ap_{13}^2}\\ &= \frac{(1-abp_{13}^2-abp_{33}^2)-(1-ap_{13}^2-abp_{33}^2)}{abp_{31}^2-ap_{13}^2} = -1.\end{aligned}$$

Hence, $M(\sqrt{\omega})/K$ is a quaternion extension, as claimed.

REMARK. The argument for sufficiency given above is a slightly modified version of the proof given in [J&Y87]. Specifically, [J&Y87] considers the quadratic form $aX^2+bY^2+1/ab\,Z^2$ instead of $aX^2+bY^2+abZ^2$, and uses a different criterion for embeddability of a biquadratic extension in a quaternion extension: $M(\sqrt{\omega})/K$ is a quaternion extension, if and only if

$$\omega\,\sigma\omega=\alpha^2ab,\quad \omega\,\tau\omega=\beta^2b\quad\text{and}\quad \omega\,\sigma\tau\omega=\gamma^2a$$

for suitable $\alpha\in K(\sqrt{b})^*$, $\beta\in K(\sqrt{a})^*$ and $\gamma\in K(\sqrt{ab})^*$.[2]

Quaternion algebras. For $a,b\in K^*$ the *quaternion algebra*

$$\left(\frac{a,b}{K}\right)$$

is defined as the K-algebra generated by elements i and j with relations

$$i^2=a,\quad j^2=b,\quad ji=-ij.$$

We write $k=ij$. It is easy to see that 1, i, j and k must be linearly independent, and hence that $(a,b/K)$ is a four-dimensional K-algebra.

The quaternion algebra $(a,b/K)$ can always be obtained as a subalgebra of $\mathrm{Mat}_4(K)$ by letting

$$i=\begin{pmatrix}0&a&0&0\\1&0&0&0\\0&0&0&a\\0&0&1&0\end{pmatrix},\quad j=\begin{pmatrix}0&0&b&0\\0&0&0&-b\\1&0&0&0\\0&-1&0&0\end{pmatrix}.$$

We note that in this case the centraliser of $(a,b/K)$ in $\mathrm{Mat}_4(K)$ is generated by the matrices

$$i'=\begin{pmatrix}0&a&0&0\\1&0&0&0\\0&0&0&-a\\0&0&-1&0\end{pmatrix},\quad j'=\begin{pmatrix}0&0&b&0\\0&0&0&b\\1&0&0&0\\0&1&0&0\end{pmatrix},$$

[2]This condition is easily seen to be equivalent to the one used above by letting $\alpha=x\omega/\sqrt{ab}$, $\beta=y\omega/\sqrt{b}$ and $\gamma=x\,\sigma y\,\omega/\sqrt{a}$.

and so is itself isomorphic to $(a, b/K)$. (Sketch of proof: The elements xy, $x = 1, i, j, k$, $y = 1, i', j', k'$, are linearly independent, and so span $\mathrm{Mat}_4(K)$. It is obvious that the only linear combinations commuting with i and j are the linear combinations of $1, i', j', k'$.)

A good example of a quaternion algebra is the Hamiltonian quaternions $\mathbb{H} = (-1, -1/\mathbb{R})$.

For a quaternion $q = x + yi + zj + wk \in (a, b/K)$ we define the *real* and *vector* parts, respectively, by

$$\mathrm{Re}\, q = x \quad \text{and} \quad \mathrm{Vec}\, q = yi + zj + wk.$$

The non-zero elements $q \in \mathrm{Vec}(a, b/K)$ are characterised by the property that $q \notin K$ but $q^2 \in K$.

LEMMA 6.1.2. *If b is a norm in $K(\sqrt{a})/K$, the quaternion algebra $(a, b/K)$ is isomorphic to $\mathrm{Mat}_2(K)$. Otherwise, it is a skew field.*

PROOF. If $a \in (K^*)^2$, b is a norm in $K(\sqrt{a})/K = K/K$, and $(a, b/K) \simeq \mathrm{Mat}_2(K)$ by

$$i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}.$$

Hence, we can assume $a \notin (K^*)^2$.

If $b = \mathrm{N}_{K(\sqrt{a})/K}(x + y\sqrt{a})$ for $x, y \in K$, i.e., $b = x^2 - ay^2$, we can map $(a, b/K)$ into $\mathrm{Mat}_2(K)$ by

$$i \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} x & -ay \\ y & -x \end{pmatrix}.$$

Now, assume that $(a, b/K)$ is not a skew field. Then there exists $q \in (a, b/K)$ such that $K[q]$ is not a field. Since $K[q] = K[\mathrm{Vec}\, q]$, we may assume $\mathrm{Re}\, q = 0$. This means that $q^2 \in K$, and since $K[q]$ is not a field, we must have $q^2 = 0$ or $q^2 \in (K^*)^2$. If $q^2 = c^2$ for some $c \in K^*$, we replace q by $c^{-1}q$ to get $q^2 = 1$. There is then an $r \in \mathrm{Vec}(a, b/K)$ with $rq = -qr$. If $r^2 = 0$, we replace q by r. Otherwise, we replace q by $(1 + q)r$. In any case we end up with $q \neq 0$ in $(a, b/K)$ such that $q^2 = 0$. Write $q = yi + zj + wk$. Then $ay^2 + bz^2 - abw^2 = q^2 = 0$. Multiplication by $-ab$ gives us $(abw)^2 - a(bz)^2 = b(ay)^2$. Since $a \notin (K^*)^2$, we cannot have $y = 0$, and so $(bw/y)^2 - a(bz/ay)^2 = b$, i.e., b is a norm in $K(\sqrt{a})/K$. □

DEFINITION 6.1.3. A quaternion algebra is called *split*, if it is isomorphic to $\mathrm{Mat}_2(K)$. Otherwise, it is called *non-split*.

LEMMA 6.1.4. *If D/K is an n-dimensional division algebra, then D can be embedded into $\mathrm{Mat}_n(K)$ as an algebra, and any two such embeddings are conjugate.*

PROOF. Let $x_1, \ldots, x_n$ be a basis for D/K. For $d \in D$, the map $x \mapsto dx$ is a K-vector space endomorphism on D, and so it is represented by a matrix $\mathbf{A}(d)$ in the basis. This gives us our embedding $d \mapsto \mathbf{A}(d)$.

Now, let $\varphi\colon D \hookrightarrow \mathrm{Mat}_n(K)$ be an arbitrary embedding. Then K^n is a D-vector space by $d\mathbf{v} = \varphi(d)\mathbf{v}$. This D-action is K-linear, and so we must have $\dim_D K^n = 1$. In particular: For $\mathbf{u} \in K^n \setminus \{\mathbf{0}\}$, the vectors $x_1\mathbf{u}, \ldots, x_n\mathbf{u}$

constitute a basis for K^n over K. Let $\mathbf{B}$ be the matrix with i^{th} column $x_i\mathbf{u}$. Then $\mathbf{B}$ is invertible and

$$\mathbf{B}^{-1}\varphi(d)\mathbf{B} = \mathbf{A}(d), \quad d \in D,$$

and so φ is conjugate to $d \mapsto \mathbf{A}(d)$. □

A related result is

LEMMA 6.1.5. *Let $n, N \in \mathbb{N}$. Then $\mathrm{Mat}_n(K)$ can be embedded in $\mathrm{Mat}_N(K)$ as a K-algebra if and only if $n \mid N$. In this case, all embedding are conjugate, and the centraliser of $\mathrm{Mat}_n(K)$ in $\mathrm{Mat}_N(K)$ is isomorphic to $\mathrm{Mat}_{N/n}(K)$.*

PROOF. First, we notice the following: K^n is *irreducible* as an $\mathrm{Mat}_n(K)$-module,[3] i.e., $\{\mathbf{0}\}$ and K^n are the only submodules. Also, as a $\mathrm{Mat}_n(K)$-module, $\mathrm{Mat}_n(K)$ is the direct sum of n submodules $\simeq K^n$, namely the submodules consisting of matrices that are zero outside a specified column. It follows that any $\mathrm{Mat}_n(K)$-module is generated by submodules $\simeq K^n$, and by 'weeding out' we see that every finitely generated $\mathrm{Mat}_n(K)$-module is a direct sum of submodules $\simeq K^n$. In particular, two finitely generated $\mathrm{Mat}_n(K)$-modules are isomorphic if and only if they have the same dimension over K.

Now, let $\varphi\colon \mathrm{Mat}_n(K) \to \mathrm{Mat}_N(K)$ be an embedding. Then K^N becomes a $\mathrm{Mat}_n(K)$-module by $\mathbf{Av} = \varphi(\mathbf{A})\mathbf{v}$, and so $K^N \simeq (K^n)^s$ for some s, i.e., $N = ns$.

Conversely, if $N = ns$, we can embed $\mathrm{Mat}_n(K)$ into $\mathrm{Mat}_N(K)$ by mapping $\mathbf{A} \in \mathrm{Mat}_n(K)$ to the block diagonal matrix with copies of $\mathbf{A}$ down the diagonal, and by considering an $N \times N$ matrix as an $s \times s$ matrix with entries from $\mathrm{Mat}_n(K)$ we see that the centraliser consists of matrices

$$\begin{pmatrix} b_{11}\mathbf{E} & \dots & b_{1s}\mathbf{E} \\ \vdots & \ddots & \vdots \\ b_{s1}\mathbf{E} & \dots & b_{ss}\mathbf{E} \end{pmatrix},$$

where $b_{ij} \in K$ and $\mathbf{E}$ is the $n \times n$ unit matrix. This subalgebra is obviously isomorphic to $\mathrm{Mat}_s(K)$.

Finally, let $\varphi, \psi\colon \mathrm{Mat}_n(K) \to \mathrm{Mat}_N(K)$ be two embeddings. Then K^N is a $\mathrm{Mat}_n(K)$-module by $\mathbf{Av} = \varphi(\mathbf{A})\mathbf{v}$ as well as by $\mathbf{Av} = \psi(\mathbf{A})\mathbf{v}$. These two modules have the same K-dimension and are therefore isomorphic: There exists a group automorphism ε on K^N such that $\varepsilon(\varphi(\mathbf{A})\mathbf{v}) = \psi(\mathbf{A})\varepsilon(\mathbf{v})$ for $\mathbf{A} \in \mathrm{Mat}_n(K)$ and $\mathbf{v} \in K^N$. In particular, ε is K-linear, and thus given by a matrix $\mathbf{B} \in \mathrm{Mat}_N(K)$. It follows that $\psi(\mathbf{A}) = \mathbf{B}\varphi(\mathbf{A})\mathbf{B}^{-1}$. □

Lemma 6.1.5 is not strictly necessary to prove Witt's Criterion, but since we will need it later, we may as well use it here too.

COROLLARY 6.1.6. *Let $(a, b/K)$ be a quaternion algebra. For any embedding of $(a, b/K)$ into $\mathrm{Mat}_4(K)$, the centraliser of $(a, b/K)$ in $\mathrm{Mat}_4(K)$ is isomorphic to $(a, b/K)$ itself.*

Now we are ready to prove

[3] All modules are understood to be unitary left modules.

NECESSITY OF WITT'S CRITERION. Let $x, y \in M^*$ with $x\,\sigma x = y\,\tau y = -1$ and $x\,\sigma y = -y\,\tau x$. We define an embedding $\varphi\colon M \hookrightarrow \mathrm{Mat}_4(K)$ by

$$\sqrt{a} \mapsto \begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \sqrt{b} \mapsto \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(This is the embedding from Lemma 6.1.4 with respect to the basis 1, $\sqrt{a}$, $\sqrt{b}$, $\sqrt{a}\sqrt{b}$.) Also, we define matrices

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \mathbf{V} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

(These are the matrices representing σ and τ is the basis given above.) Then $\mathbf{U}^2 = \mathbf{V}^2 = \mathbf{E}$, where $\mathbf{E}$ is the 4×4 unit matrix, and $\mathbf{UV} = \mathbf{VU}$. Also, $\mathbf{U}\varphi(t) = \varphi(\sigma t)\mathbf{U}$ and $\mathbf{V}\varphi(t) = \varphi(\tau t)\mathbf{V}$ for $t \in M$. Let $\mathbf{U}' = \varphi(x)\mathbf{U}$ and $\mathbf{V}' = \varphi(y)\mathbf{V}$, and consider the subalgebras

$$Q_1 = K[\mathbf{U}', \mathbf{V}'] \quad \text{and} \quad Q_2 = K[\varphi(\sqrt{a})\mathbf{V}', \varphi(\sqrt{b})\mathbf{U}'].$$

Clearly, $Q_1 \simeq (-1, -1/K)$ and $Q_2 \simeq (-a, -b/K)$. Also, Q_1 and Q_2 centralise each other, and are therefore each others centralisers.[4] By Corollary 6.1.6, $Q_1 \simeq Q_2$.

Now, $(-1, -1/K) \simeq (-a, -b/K)$, and this isomorphism will necessarily map $\mathrm{Vec}(-1, -1/K)$ to $\mathrm{Vec}(-a, -b/K)$, and preserve the map $q \mapsto -q^2$. But this map is exactly the quadratic form $U^2 + V^2 + W^2$ on $\mathrm{Vec}(-1, -1/K)$ and $aX^2 + bY^2 + abZ^2$ on $\mathrm{Vec}(-a, -b/K)$. Hence, $U^2 + V^2 + W^2$ and $aX^2 + bY^2 + abZ^2$ are equivalent.

REMARK. As it stands, the proof of necessity of Witt's Criterion given above can be compared to a rabbit pulled from a hat: Where on Earth did it come from? This is because the proof is in fact a 'crude' version of a more sophisticated (and more general) argument from the study of so-called *Brauer type embedding problems*. This more sophisticated argument relies on Brauer group theory and the existence of *obstructions* in the Brauer group to such embedding problems. The problem of embedding a V_4-extension as above in a quaternion extension is of Brauer type, and the obstruction is $(-1, -1)(-a, -b) \in \mathrm{Br}(K)$, where (c, d) is the equivalence class of $(c, d/K)$ in $\mathrm{Br}(K)$ (corresponding to the norm residue symbol $(c, d) \in H^2(K)$). Witt's Criterion then becomes simply a special case.

Brauer type embedding problems are treated in various research papers, such as [GS&S], [Ki] and [Le1, Le2, Le6] (for $p = 2$), [Ma] and [Sw1, Sw2] (for arbitrary p), and [Se1], [Fr], [Cr1, Cr2] and [Le5] (the trace form approach).

For more on quaternion algebras, and their relationship with quadratic forms, we refer to [Lam].

An immediate consequence of Witt's Criterion is

[4] Since the centralisers have dimension 4.

PROPOSITION 6.1.7. *Let $a \in K^* \setminus (K^*)^2$. If $K(\sqrt{a})/K$ is embeddable into a quaternion extension of K, then a is a sum of three squares in K.*

From Witt's Theorem we also get that quaternion extensions come in 'clusters' containing the same biquadratic subextension M/K, and that such a 'cluster' is parametrised by $K^*/(K^* \cap (M^*)^2)$, i.e., by a group of order $\frac{1}{4}[K^* : (K^*)^2]$. From this we easily get

PROPOSITION 6.1.8. *If $K^*/(K^*)^2$ is infinite, the number of quaternion extensions of K is either 0 or ∞. If $K^*/(K^*)^2$ is finite of order ≤ 2, K has no quaternion extensions. If $K^*/(K^*)^2$ is finite of order 2^n, $n \geq 2$, the number of quaternion extensions is a multiple of 2^{n-2}, and at most $2^{n-2}(2^n-1)(2^{n-1}-1)/3$.*

Parametrising quaternion extensions. We will now consider the problem of finding parametrisations of quaternion extensions, in the form of a generic polynomial:.

DEFINITION 6.1.9. The *level* of K, denoted $\ell(K)$, is the smallest natural number n for which -1 is a sum of n squares in K. If -1 is not a sum of squares in K, $\ell(K) = \infty$.

$\ell(K) = \infty$ is equivalent to K being orderable. If the level is finite, it is always a power of 2. This follows easily from the fact that the non-zero sums of 2^n squares in K constitute a subgroup of K^* for all $n \in \mathbb{N}$, cf. [Ja2, Thm. 11.9].

THEOREM 6.1.10. (a) (BUCHT 1910, [Bu]) *Let $a, b \in K^*$ be quadratically independent. Then $M/K = K(\sqrt{a}, \sqrt{b})/K$ is embeddable into a quaternion extension of K, if and only if a and b have the form*

$$a =_2 u = \left(1 + \alpha^2 + \alpha^2\beta^2\right)\left(1 + \beta^2 + \beta^2\gamma^2\right),$$
$$b =_2 v = \left(1 + \beta^2 + \beta^2\gamma^2\right)\left(1 + \gamma^2 + \gamma^2\alpha^2\right),$$

for suitable $\alpha, \beta, \gamma \in K$.[5] *This is* Bucht's Parametrisation.

(b) *For $\ell(K) = 1$, this description can be replaced by*

$$a =_2 1 + s^2,$$
$$b =_2 1 + r^2 + r^2s^2,$$

for suitable $r, s \in K$, and if $\ell(K) = 2$ by

$$a =_2 r, \quad b =_2 s \quad \text{for } r, s \in K^* \text{ with } \quad r + s = -1.$$

REMARK. Let $w = (1 + \gamma^2 + \gamma^2\alpha^2)(1 + \alpha^2 + \alpha^2\beta^2)$ and $\sqrt{w} = \sqrt{u}\sqrt{v}/(1 + \beta^2 + \beta^2\gamma^2)$. Then the quaternion extensions containing $K(\sqrt{u}, \sqrt{v})/K$ are

$$K\left(\sqrt{r\big(1 + \frac{1 - \alpha\beta\gamma}{\sqrt{u}} + \frac{1 - \alpha\beta\gamma}{\sqrt{v}} + \frac{1 - \alpha\beta\gamma}{\sqrt{w}}\big)}\right)/K, \quad r \in K^*,$$

by Witt's Theorem and the proof below. The expression in the square root is invariant under cyclic permutation of α, β and γ.

The parametrisations for $\ell(K) \leq 2$ are less elegant than Bucht's, but they are simpler, and $\ell(K) \leq 2$ covers all fields of (odd) prime characteristic.

[5] See section A.1 in Appendix A for the meaning of '$=_2$'.

PROOF OF THEOREM 6.1.10. 'If': Let

$$\mathbf{Q} = \begin{pmatrix} 1-\alpha\beta\gamma & -(\beta+\alpha\gamma+\beta\gamma^2) & -\alpha(1-\alpha\beta\gamma) \\ \beta(1-\alpha\beta\gamma) & 1-\alpha\beta\gamma & -(\gamma+\alpha\beta+\alpha^2\gamma) \\ \alpha+\beta\gamma+\alpha\beta^2 & \gamma(1-\alpha\beta\gamma) & 1-\alpha\beta\gamma \end{pmatrix}.$$

Then $\det \mathbf{Q} = uvw$ (where w is as in the remark) and

$$\mathbf{Q}^t\mathbf{Q} = \begin{pmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & w \end{pmatrix}.$$

Hence,

$$U^2 + V^2 + W^2 \sim uX'^2 + vY'^2 + wZ'^2 \sim aX^2 + bY^2 + abZ^2,$$

and M/K can be embedded in a quaternion extension. This proves 'if' as well as the claims in the remark.

'Only if': Case (a), $\ell(K) > 2$. If M/K is embeddable in a quaternion extension, we must have some matrix $\mathbf{Q}$ with

$$\mathbf{Q}^t\mathbf{Q} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix}$$

by Witt's Criterion. Permuting the rows of $\mathbf{Q}$ will not change this relation, and so we may assume that the three diagonal elements are all non-zero.[6] Thus, we can write

$$\mathbf{Q} = \begin{pmatrix} q_{11} & -fq_{22} & -\alpha q_{33} \\ \beta q_{11} & q_{22} & -gq_{33} \\ eq_{11} & \gamma q_{22} & q_{33} \end{pmatrix}$$

for suitable $e, f, g, \alpha, \beta, \gamma \in K$. From the orthogonality of the columns of $\mathbf{Q}$, we immediately get

$$-f + \beta + \gamma e = -\alpha - \beta g + e = \alpha f - g + \gamma = 0,$$

or

$$\begin{aligned} e &= \alpha + \beta g, \\ f &= \beta + \gamma e, \\ g &= \gamma + \alpha f, \end{aligned}$$

from which we deduce

$$\begin{aligned} (1-\alpha\beta\gamma)e &= \alpha + \beta\gamma + \alpha\beta^2, \\ (1-\alpha\beta\gamma)f &= \beta + \gamma\alpha + \beta\gamma^2, \\ (1-\alpha\beta\gamma)g &= \gamma + \alpha\beta + \gamma\alpha^2. \end{aligned}$$

If $\alpha\beta\gamma = 1$, we would have

$$0 = e(1-\alpha\beta\gamma)\alpha = \alpha^2 + \alpha\beta\gamma + \alpha^2\beta^2 = 1 + \alpha^2 + \alpha^2\beta^2,$$

[6] Since $\det \mathbf{Q} \neq 0$ and the triples that can become diagonal elements through permuting the rows are exactly the triples that occur in the expansion of the determinant.

contradicting $\ell(K) > 2$. Thus, $\alpha\beta\gamma \neq 1$, and we have

$$\begin{aligned} a &=_2 1 + \beta^2 + e^2 \\ &= 1 + \beta^2 + \frac{(\alpha + \beta\gamma + \alpha\beta^2)^2}{(1 - \alpha\beta\gamma)^2} \\ &= \frac{(1 + \beta^2)(1 - \alpha\beta\gamma) + (\alpha + \beta\gamma + \alpha\beta^2)^2}{(1 - \alpha\beta\gamma)^2} \\ &= \frac{(1 + \alpha^2 + \alpha^2\beta^2)(1 + \beta^2 + \beta^2\gamma^2)}{(1 - \alpha\beta\gamma)^2} =_2 u, \end{aligned}$$

and similarly $b =_2 v$.

Case (b), $\ell(K) = 1$. The equivalence $U^2 + V^2 + W^2 \sim (1 + s^2)X^2 + (1 + r^2 + r^2s^2)Y^2 + (1 + s^2)(1 + r^2 + r^2s^2)Z^2$ is expressed by the matrix

$$\mathbf{Q} = \begin{pmatrix} 1 & -rs & s \\ 0 & 1 & r(1 + s^2) \\ -s & -r & 1 \end{pmatrix}.$$

Conversely, assume M/K embeddable in a quaternion extension. Since -1 is a square, every element in K is a sum of two squares. In particular, $a =_2 1 + s^2$ for some s. Now

$$U^2 + V^2 + W^2 \sim (1 + s^2)U'^2 + (1 + s^2)V'^2 + W'^2,$$

and by the Witt Cancellation Theorem [Ja1, §6.5], we must have $bY^2 + abZ^2 \sim (1 + s^2)V'^2 + W'^2$, i.e., b is represented by $(1 + s^2)V'^2 + W'^2$. Since ab is not a square, we must have $b =_2 r^2(1 + s^2) + 1$ for some r.

This is obviously a special case of Bucht's Parametrisation. ($\alpha = s$, $\beta = 0$, $\gamma = r$.)

Case (c), $\ell(K) = 2$. Write $-1 = x^2 + y^2$, and let $u = (r + 1)/2$, $v = (r - 1)/2$. Then the equivalence $U^2 + V^2 + W^2 \sim rX^2 + sY^2 + rsZ^2$ is expressed by the matrix

$$\mathbf{Q} = \begin{pmatrix} vx & ux + y & ux - ry \\ vy & uy - x & uy + rx \\ u & v & v \end{pmatrix}.$$

Conversely, assume M/K embeddable in a quaternion extension: Since -1 is a sum of two squares, we have

$$\begin{aligned} aX^2 + bY^2 + abZ^2 &\sim U^2 + V^2 + W^2 \\ &\sim U_1^2 - V_1^2 - W_1^2 \\ &\sim aX_1^2 - aY_1^2 - Z_1^2, \end{aligned}$$

and hence $bY^2 + abZ^2 \sim -aY_1^2 - Z_1^2$, meaning that $b = -ax^2 - y^2$ for suitable $x, y \in K$. If $x, y \neq 0$, we can let $r = a(x/y)^2$ and $s = b/y^2$. If $x = 0$, we write $a = u^2 - v^2$ for $u, v \in K^*$, and let $r = a/v^2$ and $s = -(u/v)^2$. If $y = 0$, we write $1/a = u^2 - v^2$ for $u, v \in K^*$, and let $r = au^2$ and $s = -av^2$.

Finally, assume $r, s \in K^*$ quadratically independent with $r + s = -1$. We wish to prove that r and s can then be obtained by Bucht's Parametrisation:

Look at the matrix $\mathbf{Q}$ above. Clearly, vx and v are not 0. Assume for a moment that $uy - x \neq 0$, i.e., $x/y \neq u$. Then we get $\alpha = (ry - ux)/v$, $\beta = y/x$ and $\gamma = v/(uy - x)$ in the argument above for 'only if' and $\ell(K) > 2$. Thus,

$$\alpha\beta\gamma = \frac{(ry - ux)y}{x(uy - x)} = \frac{ry^2 - uxy}{uxy - x^2}.$$

If $\alpha\beta\gamma = 1$, we must have $ry^2 - uxy = uxy - x^2$ or $ry^2 + x^2 - 2uxy = 0$, i.e., $(uy - x)^2 = v^2y^2$, i.e., $uy - x = \pm vy$, i.e., $x/y = u \pm v$. Thus, if we can find $x, y \in K$, such that $x^2 + y^2 = -1$ and $x/y \neq u, r, 1$, we can use the argument from $\ell(K) > 2$. If $x, y \in K$ is one pair with $x^2 + y^2 = -1$, we get all others by letting

$$x' = \frac{x(p^2 - q^2) - 2ypq}{p^2 + q^2},$$
$$y' = \frac{y(p^2 - q^2) + 2xpq}{p^2 + q^2}$$

for $(p, q) \in K \times K$, $(p, q) \neq (0, 0)$. Thus, the possible values for x'/y' are

$$\frac{x'}{y'} = \frac{x(p^2 - q^2) - 2ypq}{y(p^2 - q^2) + 2xpq}.$$

This is a non-constant rational function, since otherwise $x/y = -y/x$, i.e., $x^2 = -y^2$, contradicting $x^2 + y^2 = -1$, and as K is infinite (it has a biquadratic extension), it assumes infinitely many values. In particular, we can avoid the three values u, r and 1. □

Example. Let $K = \mathbb{Q}$, $\alpha = 1$, $\beta = 0$ and $\gamma = 1$. Then $u = 2$, $v = 3$ and $w = 6$, and we get a family

$$\mathbb{Q}\Big(\sqrt{r\big(1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{6}}\big)}\Big)/\mathbb{Q} = \mathbb{Q}\big(\sqrt{r(2 + \sqrt{2})(3 + \sqrt{3})}\big)/\mathbb{Q},$$

of quaternion extensions, when r runs through $\mathbb{Q}^*$. For $r = 1$, this gives us Dedekinds original quaternion extension from 1887, cf. [De].

Remark. As noticed above, Bucht's parametrisation behaves well under cyclic permutation of α, β and γ. Specifically, we get a permutation of

$$u = (1 + \alpha^2 + \alpha^2\beta^2)(1 + \beta^2 + \beta^2\gamma^2),$$
$$v = (1 + \beta^2 + \beta^2\gamma^2)(1 + \gamma^2 + \gamma^2\alpha^2), \text{ and}$$
$$w = (1 + \gamma^2 + \gamma^2\alpha^2)(1 + \alpha^2 + \alpha^2\beta^2),$$

whereas

$$\omega = 1 + \frac{1 - \alpha\beta\gamma}{\sqrt{u}} + \frac{1 - \alpha\beta\gamma}{\sqrt{v}} + \frac{1 - \alpha\beta\gamma}{\sqrt{w}}$$

is left unchanged.

This naturally induces us to consider the case where α, β and γ are in fact conjugate with respect to an automorphism of order 3:

Let L/K be a cyclic extension of degree 3, let σ generate $C_3 = \mathrm{Gal}(M/K)$, and let $\alpha \in L$, $\beta = \sigma\alpha$, $\gamma = \sigma\beta$. If we assume $u \notin L^2$, we immediately get

that u and v are quadratically independent. Also, the biquadratic extension $M = L(\sqrt{u}, \sqrt{v})$ of L is obviously Galois over K, and we can extend σ to M by

$$\sigma\colon \sqrt{u} \mapsto \sqrt{v}, \quad \sqrt{v} \mapsto \sqrt{w} = \frac{\sqrt{u}\sqrt{v}}{1+\beta^2+\beta^2\gamma^2}.$$

From this it is clear that M/K is in fact an A_4-extension. Also, $\sigma\omega = \omega$, and so $F/K = M(\sqrt{\omega})/K$ is Galois, and we can extend σ by $\sigma\sqrt{\omega} = \sqrt{\omega}$. σ then has order 3 in $\mathrm{Gal}(F/K)$, and since it operates non-trivially on $Q_8 = \mathrm{Gal}(F/L)$, we must have

$$\mathrm{Gal}(F/K) \simeq Q_8 \rtimes C_3 \simeq \mathrm{SL}(2,3) = \mathrm{SL}_2(\mathbb{F}_3).$$

Hence, we have obtained an $\mathrm{SL}(2,3)$-extension of K.

Of course, this raises the question of when it is possible to choose $\alpha \in L$ such that $u \in L^* \setminus (L^*)^2$. It should come as no surprise that this can be done over Hilbertian fields:

THEOREM 6.1.11. (FADDEYEV 1945, [Fa]) *If K is Hilbertian, every cyclic extension of degree 3 can be embedded in an $\mathrm{SL}(2,3)$-extension.*

PROOF. First, assume $\mathrm{char}\, K \neq 2$, and let L/K be a cyclic extension of degree 3 as above. Also, let $\xi \in L$ be a primitive element for L/K, i.e., $\xi \in L \setminus K$. Look at the polynomial

$$\begin{aligned} f(s,t,X) = X^2 - (1 + (\xi s + \xi^2 t)^2 + (\xi s + \xi^2 t)^2(\sigma\xi s + \sigma\xi^2 t)^2) \\ \times (1 + (\sigma\xi s + \sigma\xi^2 t)^2 + (\sigma\xi s + \sigma\xi^2 t)^2(\sigma^2\xi s + \sigma^2\xi^2 t)^2) \end{aligned}$$

in $L[s,t,X]$. It is irreducible: We have an L-endomorphism on $L[s,t]$ given by

$$s \mapsto \xi s + \xi^2 t, \quad t \mapsto \sigma\xi s + \sigma\xi^2 t.$$

It is obviously an L-automorphism, and since the polynomial $1 + s^2 + s^2t^2$ is irreducible in $L[s,t]$, the image is irreducible as well. Hence, the two factors in $-f(s,t,0)$ are irreducible. As they are not associated, their product is not a square, and so $f(s,t,X)$ is irreducible.

By Corollary 3.1.6 in Chapter 3, there exists a and b in K with $f(a,b,X)$ irreducible in $L[X]$. We can then let $\alpha = a\xi + b\xi^2$.

If $\mathrm{char}\, K = 2$, we look instead at the polynomial

$$f(t,X) = X^2 - X - t(\xi + \sigma\xi) \in L[t,X].$$

It is clearly irreducible, and so we can find $x \in K$ such that $a = x(\xi + \sigma\xi)$ is not of the form $y^2 - y$, $y \in L$. We now let $b = \sigma a$, and get $\sigma b = a + b$. The biquadratic extension $M = L(\theta_a, \theta_b)$ of L is thus A_4 over K, much as above, and we get a quaternion extension $F = M(\theta_\omega)$ of L by letting $\omega = a\theta_a + (a+b)\theta_b$. This expression is invariant under cyclic permutation of a, b and $a+b$, i.e., under σ, and so F/K is an $\mathrm{SL}(2,3)$-extension, as above. □

The next result gives a generic polynomial for quaternion extensions.

THEOREM 6.1.12. *Let $K(\boldsymbol{\alpha})$ be a function field in the variables $\boldsymbol{\alpha} = (\alpha, \beta, \gamma)$ over K, and let*

$$\begin{aligned} F(\boldsymbol{\alpha}, X) = (X^2-1)^4 &- 2(1-\alpha\beta\gamma)^2 \frac{A+B+C}{ABC}(X^2-1)^2 \\ &- 8\frac{(1-\alpha\beta\gamma)^3}{ABC}(X^2-1) \\ &+ (1-\alpha\beta\gamma)^4 \frac{A^2+B^2+C^2-2AB-2AC-2BC}{A^2B^2C^2} \end{aligned}$$

$\in K(\boldsymbol{\alpha}, X)$, *where*

$$\begin{aligned} A &= 1+\alpha^2+\alpha^2\beta^2, \\ B &= 1+\beta^2+\beta^2\gamma^2, \\ C &= 1+\gamma^2+\gamma^2\alpha^2. \end{aligned}$$

Then:

(a) $\mathrm{Gal}(F(\boldsymbol{\alpha}, X)/K(\boldsymbol{\alpha})) \simeq Q_8$.

(b) *If the specialisations of AB and BC at a point $\boldsymbol{\alpha} \in K \times K \times K$ are non-zero and quadratically independent, the polynomial $r^4 F(\boldsymbol{\alpha}, r^{-1/2}X)$ is irreducible in $K[X]$ for all $r \in K^*$, and the splitting field is a quaternion extension of K.*[7]

(c) *Any quaternion extension of K is obtained by a specialisation as in* (b).

(d) *If $g(X) \in K[X]$ is an irreducible polynomial with Galois group Q_8, then $g(X)$ is Tschirnhaus equivalent*[8] *to some specialisation $r^4 F(\boldsymbol{\alpha}, r^{-1/2}X)$ as in* (b).

PROOF. The assertions (a)–(c) are obvious, since $F(\boldsymbol{\alpha}, X)$ is the minimal polynomial of

$$\sqrt{1 + \frac{1-\alpha\beta\gamma}{\sqrt{AB}} + \frac{1-\alpha\beta\gamma}{\sqrt{BC}} + \frac{1-\alpha\beta\gamma}{\sqrt{CA}}},$$

and this is exactly the expression for a primitive element we found in connection with Bucht's Parametrisation. (Here, $AB = u$, $BC = v$ and $CA = w$.)

(d) $g(X)$ has degree 8. Also, the splitting field of $g(X)$ is the splitting field of a specialisation $f(X) = r^4 F(\boldsymbol{\alpha}, r^{-1/2}X)$ as in (b). In particular, any given root of $g(X)$ is a polynomial of degree < 8 in any given root of $f(X)$, and $g(X)$ is then the corresponding Tschirnhaus transformation of $f(X)$. □

EXAMPLE. Let $K = \mathbb{Q}$, $\alpha = 1$, $\beta = 0$, $\gamma = 1$ and $r = 6$. Then we get

$$(X^2-6)^4 - 72(X^2-6)^2 - 288(X^2-6) - 288 \in \mathbb{Q}[X]$$

as the minimal polynomial for $\sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ over $\mathbb{Q}$. Hence the splitting field is Dedekind's quaternion extension, cf. the example on page 138.

[7] Since $F(\boldsymbol{\alpha}, X)$ is a polynomial in X^2, this expression does in fact give us a polynomial over K.

[8] See the end of this section.

REMARK. In [Grö, 1934], Gröbner proves that the Noether Problem has a positive answer for Q_8 over $\mathbb{Q}$. This is done by considering the four-dimensional linear representation of Q_8, and thus implies the existence of a four-parameter generic polynomial, as above.

We refer the interested reader to the original paper, as it is both short and clear.

We will now briefly consider the generalized quaternion group Q_{2^n}:

PROPOSITION 6.1.13. *Q_{2^n} occurs as a Galois group over $\mathbb{Q}$, and more generally over any Hilbertian field.*

PROOF. If K is Hilbertian, we can realise $C_{2^{n-1}} \rtimes C_4$ (with C_4 acting by inversion) over K by Ikeda's Theorem (Theorem 5.4.4 in Chapter 5), and Q_{2^n} is a surjective image of this group. □

EXAMPLE. (KIMING) Let $n = 4$. Then $\mathbb{Q}(\sqrt{6}, \sqrt{7}, \sqrt{\theta})/\mathbb{Q}$ is a Q_{16}-extension, when

$$\theta = \sqrt{6}\sqrt{7}(41 + 38\sqrt{7})\big(\sqrt{6} - 1 + \frac{\sqrt{6} - \sqrt{7} - 4}{\sqrt{7 + \sqrt{7}}}\big).$$

In [Ki], Kiming considers the problem of constructing extensions with Galois group Q_{16}. Unfortunately, his approach does not lend itself to producing generic polynomials.

PROBLEM. Is there a generic polynomial for Q_{16} over $\mathbb{Q}$, or more generally for Q_{2^n}, $n \geq 4$?

Find explicit polynomials over $\mathbb{Q}$ with Galois group Q_{2^n} for $n \geq 4$.

A criterion for the existence of Q_{32}-extensions is given in [Le3]. In principle, this criterion can be used to construct actual Q_{32}-extensions, but in practice it is decidedly unfriendly.

Tschirnhaus transformations. Let $f(X) \in K[X]$ be a monic polynomial of degree n. A *Tschirnhaus transformation* of $f(X)$ is then a polynomial

$$g(X) = \prod_{i=1}^{n}(X - \varphi(\theta_i)) \in K[X],$$

where $\theta_1, \ldots, \theta_n$ are the roots of $f(X)$, and $\varphi(X) \in K[X]$ is a polynomial of degree $< n$, cf. [We1, IV.§58]. (The trick is expressing the coefficients of $g(X)$ in terms of the coefficients of $f(X)$ and $\varphi(X)$.)

Two polynomials are *Tschirnhaus equivalent*, if they are Tschirnhaus transformations of each other. Of course, that $g(X)$ is a Tschirnhaus transformation of $f(X)$ does not imply that the converse holds, as shown by e.g. $f(X) = X^4 - 2$ and $g(X) = (X^2 - 2)^2$. However, it is clear that we have

PROPOSITION 6.1.14. *Let $f(X)$ and $g(X)$ be monic polynomials in $K[X]$ of the same degree n and with no multiple roots. If $g(X)$ is a Tschirnhaus transformation of $f(X)$, then $f(X)$ is a Tschirnhaus transformation of $g(X)$.*

The proof consists mostly of noting that the Tschirnhaus transformation maps the irreducible factors of $f(X)$ to those of $g(X)$.

For the special case of irreducible polynomials, it is clear that they are Tschirnhaus equivalent if and only if they have isomorphic root fields (a *root field* being the field obtained by adjoining one root of the polynomial), giving us

PROPOSITION 6.1.15. *Let $p(X)$ and $q(X)$ be monic irreducible polynomials in $K[X]$ of the same degree. Then the following conditions are equivalent:*

(i) *$p(X)$ and $q(X)$ are Tschirnhaus equivalent.*
(ii) *The root field of $p(X)$ over K contains a root of $q(X)$.*
(iii) *The root field of $q(X)$ over K contains a root of $p(X)$.*
(iv) *There is a $\varphi(X) \in K[X]$ with $q(X) \mid p(\varphi(X))$.*
(v) *There is a $\psi(X) \in K[X]$ with $p(X) \mid q(\psi(X))$.*
(vi) *$K[X]/(p(X))$ and $K[X]/(q(X))$ are K-isomorphic.*

Obviously, Tschirnhaus equivalent polynomials have the same splitting field. The converse need not hold, although it will often be the case for irreducible separable polynomials for purely group theoretical reasons. (I.e., if the fixed point groups in the Galois group are the only subgroups of the appropriate index.)

EXAMPLES. (1) The polynomials X^4+2 and X^4-2 have the same splitting field over $\mathbb{Q}$, but are not Tschirnhaus equivalent, as their root fields are non-isomorphic.

(2) Consider Brumer's D_5-polynomial

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

from Chapter 2. Since any two subgroups of D_5 of order 2 are conjugate, we get: Any quintic polynomial with Galois group D_5 is Tschirnhaus equivalent to a specialisation of $f(s,t,X)$.

(3) A less trivial example is: The polynomials X^7-7X+3 and $X^7+14X^4-42X^2-21X+9$ are *not* Tschirnhaus equivalent, but have the same splitting field over $\mathbb{Q}$ with $\mathrm{PSL}(2,7)$ as Galois group. This follows from the fact that $\mathrm{PSL}(2,7)$ has non-conjugate subgroups of index 7, and that the root fields of these two polynomials are the fixed fields of two such subgroups.

6.2. The Central Product QC

Let QC be the central product of Q_8 and C_4, i.e.,

$$QC = \left\langle i,j,\rho \;\middle|\; \begin{array}{l} i^2=j^2=\rho^2=-1, \\ ji=-ij,\ \rho i = i\rho,\ \rho j = j\rho \end{array} \right\rangle.$$

The center of QC is cyclic of order 2, generated by -1, and is also the Frattini subgroup. Thus, $QC/Z(QC) \simeq C_2^3$. There are an additional six (non-central) subgroups of order 2, all of them conjugate under the action of $\mathrm{Aut}\, QC$, but falling in three conjugacy classes under the action of QC itself.

We will consider the problem of embedding a C_2^3-extension

$$M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$$

in a QC-extension. As above, we will assume all fields to have characteristic $\neq 2$.

QC contains exactly one subgroup isomorphic to Q_8, and we (arbitrarily) choose to look at QC-extensions F/K containing M/K such that $F/K(\sqrt{c})$ is a quaternion extension. This corresponds to looking at embeddings along $\pi\colon i \mapsto \sigma$, $j \mapsto \tau$, $\rho \mapsto \upsilon$, where $\sigma, \tau, \upsilon \in C_2^3 = \mathrm{Gal}(M/K)$ are given by

$$\begin{aligned}
\sigma\colon &\quad \sqrt{a} \mapsto -\sqrt{a}, &\quad \sqrt{b} \mapsto \sqrt{b}, &\quad \sqrt{c} \mapsto \sqrt{c},\\
\tau\colon &\quad \sqrt{a} \mapsto \sqrt{a}, &\quad \sqrt{b} \mapsto -\sqrt{b}, &\quad \sqrt{c} \mapsto \sqrt{c},\\
\upsilon\colon &\quad \sqrt{a} \mapsto \sqrt{a}, &\quad \sqrt{b} \mapsto \sqrt{b}, &\quad \sqrt{c} \mapsto -\sqrt{c}.
\end{aligned}$$

The result corresponding to Witt's Criterion is

THEOREM 6.2.1. *A C_2^3-extension $M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$ can be embedded in a QC-extension F/K such that $F/K(\sqrt{c})$ is a quaternion extension, if and only if the quadratic forms $aX^2 + bY^2 + abZ^2$ and $U^2 + cV^2 + cW^2$ are equivalent over K. Furthermore, if $\mathbf{P}$ is a 3×3 matrix with $\det \mathbf{P} = c/ab$ and*

$$\mathbf{P}^t \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix} \mathbf{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{pmatrix},$$

the QC-extensions in question are

$$K\left(\sqrt{r\big(1 + p_{11}\sqrt{a} + p_{22}\frac{\sqrt{b}}{\sqrt{c}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}}\big)}, \sqrt{c}\right)/K, \quad r \in K^*.$$

PROOF. First of all: If we have $F/K = M(\sqrt{\omega})/K$ as desired, we get $\sigma\omega/\omega = x^2$, $\tau\omega/\omega = y^2$ and $\upsilon\omega/\omega = z^2$ for $x, y, z \in M^*$ with $x\,\sigma x = y\,\tau y = z\,\upsilon z = -1$, $x\,\sigma y = -y\,\tau x$, $x\,\sigma z = z\,\upsilon x$ and $y\,\tau z = z\,\upsilon y$. And conversely, if we have such $x, y, z, \omega \in M^*$, $M(\sqrt{\omega})/K$ is a QC-extension of the proper type.

Sufficiency: Using matrix equations as in the proof of Witt's Criterion, we prove that we can let

$$\omega = 1 + p_{11}\sqrt{a} + p_{22}\frac{\sqrt{b}}{\sqrt{c}} + p_{33}\frac{\sqrt{a}\sqrt{b}}{\sqrt{c}},$$

$$x = \frac{(p_{13}/\sqrt{c} - p_{31}\sqrt{b})\sqrt{a}}{\omega} \quad \text{and} \quad y = z = \frac{\sqrt{b}(p_{23} - p_{32}\sqrt{a})}{\omega\sqrt{c}}.$$

Necessity: Let x, y and z be derived from an embedding $M/K \subseteq F/K$ as above. We define $\varphi\colon M \hookrightarrow \mathrm{Mat}_8(K)$ to be the embedding given by the basis

$$1, \sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b}, \sqrt{c}, \sqrt{a}\sqrt{c}, \sqrt{b}\sqrt{c}, \sqrt{a}\sqrt{b}\sqrt{c}$$

for M/K, and let $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{W}$ represent σ, τ and υ in the same basis. Then $\mathbf{U}\varphi(t) = \varphi(\sigma t)\mathbf{U}$, $\mathbf{V}\varphi(t) = \varphi(\tau t)\mathbf{V}$ and $\mathbf{W}\varphi(t) = \varphi(\upsilon t)\mathbf{W}$ for $t \in M$. Furthermore, $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{W}$ commute and have square $-\mathbf{E}$, where $\mathbf{E}$ is the 8×8 unit matrix. Let $\mathbf{U}' = \varphi(x)\mathbf{U}$, $\mathbf{V}' = \varphi(y)\mathbf{V}$ and $\mathbf{W}' = \varphi(z)\mathbf{W}$.

Consider the subalgebras

$$Q_1 = K[\varphi(\sqrt{a})\mathbf{V}', \varphi(\sqrt{b})\mathbf{U}'] \simeq \Big(\frac{-a,-b}{K}\Big),$$
$$Q_2 = K[\mathbf{W}', \varphi(\sqrt{c})\mathbf{U}'] \simeq \Big(\frac{-1,-c}{K}\Big) \quad \text{and}$$
$$Q_3 = K[\mathbf{U}', \mathbf{V}'\mathbf{W}'] \simeq \Big(\frac{-1,1}{K}\Big).$$

They centralise each other, and Q_3 is split. By Lemma 6.1.5, the centraliser of Q_3 in $\mathrm{Mat}_8(K)$ is isomorphic to $\mathrm{Mat}_4(K)$, and so we have Q_1 and Q_2 centralising each other inside $\mathrm{Mat}_4(K)$, i.e., $Q_1 \simeq Q_2$ by Corollary 6.1.6. It follows that

$$aX^2 + bY^2 + abZ^2 \sim U^2 + cV^2 + cW^2.$$

□

QC-extensions (with the group named DC instead of QC) are considered in [M&Sm, Cor. 1.3(iv) + Thm. A.2] and [Sw1, Prop. p. 1050]. Both papers provide a description of the extensions. The one given in [Sw1] is similar to Theorem 6.2.1 above.

We can now parametrise QC-extensions in the manner of Bucht:

THEOREM 6.2.2. *A C_2^3-extension $M/K = K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$ can be embedded in a QC-extension F/K such that $F/K(\sqrt{c})$ is a quaternion extension, if and only if*

$$a =_2 u = c(c + \alpha^2 + c\alpha^2\beta^2)(1 + c\beta^2 + c\beta^2\gamma^2) \quad \textit{and}$$
$$b =_2 v = (1 + c\beta^2 + c\beta^2\gamma^2)(c + c\gamma^2 + \gamma^2\alpha^2)$$

for suitable $\alpha, \beta, \gamma \in K$. In this case, the QC-extensions in question are

$$K\bigg(\sqrt{r\big(1 + \frac{c(1-\alpha\beta\gamma)}{\sqrt{u}} + \frac{(1-\alpha\beta\gamma)\sqrt{c}}{\sqrt{v}} + \frac{c(1-\alpha\beta\gamma)\sqrt{c}}{\sqrt{w}}\big)}, \sqrt{c}\bigg)/K$$

for $r \in K^*$, where

$$w = c(c + c\gamma^2 + \gamma^2\alpha^2)(c + \alpha^2 + c\alpha^2\beta^2)$$

and

$$\sqrt{w} = \frac{\sqrt{u}\sqrt{v}}{1 + c\beta^2 + c\beta^2\gamma^2}.$$

PROOF. Let $\mathbf{Q}$ be a 3×3 matrix such that

$$\mathbf{Q}^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{pmatrix} \mathbf{Q} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix}.$$

If $q_{11} = 0$, we replace $\mathbf{Q}$ by $\mathbf{QU}$, where

$$\mathbf{U} = \begin{pmatrix} (cv^2 - u^2)/(u^2 + cv^2) & -2cuv/(u^2 + cv^2) & 0 \\ -2uv/(u^2 + cv^2) & (u^2 - cv^2)/(u^2 + cv^2) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for $u, v \in K^*$ with $u^2 + cv^2 \neq 0$. If q_{22} or q_{33} is zero, we interchange the second and third rows of $\mathbf{Q}$. Thus, we are allowed to assume $q_{11}, q_{22}, q_{33} \neq 0$, and can write

$$\mathbf{Q} = \begin{pmatrix} q_{11} & -fq_{22} & -\alpha q_{33} \\ \beta q_{11} & q_{22} & -gq_{33} \\ eq_{11} & \gamma q_{22} & q_{33} \end{pmatrix}.$$

The argument now proceeds as in the case of Bucht's Parametrisation, with the three cases being (a) $U^2 + cV^2 + cW^2$ anisotropic (i.e., not isotropic), (b) $-c$ square in K, and (c) $U^2 + cV^2 + cW^2$ isotropic, but $-c$ not a square in K. □

COROLLARY 6.2.3. *Let $K(\boldsymbol{\alpha}, c)$ be a function field in the indeterminates $\boldsymbol{\alpha} = (\alpha, \beta, \gamma)$ and c over K, and let*

$$\begin{aligned} G(\boldsymbol{\alpha}, c, X) = (X^2-1)^4 \\ - 2d(1-\alpha\beta\gamma)^2 \frac{A + c^2B + cC}{ABC}(X^2-1)^2 - 8c^3\frac{(1-\alpha\beta\gamma)^3}{ABC}(X^2-1) \\ + c^2(1-\alpha\beta\gamma)^4 \frac{A^2 + c^4B^2 + c^2C^2 - 2c^2AB - 2cAC - 2c^3BC}{A^2B^2C^2} \end{aligned}$$

in $K(\boldsymbol{\alpha}, c, X)$, where

$$\begin{aligned} A &= c(c + \alpha^2 + c\alpha^2\beta^2), \\ B &= 1 + c\beta^2 + c\beta^2\gamma^2, \quad \textit{and} \\ C &= c + c\gamma^2 + \gamma^2\alpha^2. \end{aligned}$$

Then:

(a) *The splitting field of $G(\boldsymbol{\alpha},c,X)$ over $K(\boldsymbol{\alpha},c)$ is a QC-extension of $K(\boldsymbol{\alpha},c)$ and a quaternion extension of $K(\boldsymbol{\alpha}, \sqrt{c})$.*

(b) *If the specialisations of AB, BC and c at a point $(\boldsymbol{a}, c') \in K^3 \times K$ are quadratically independent, the polynomial $r^4G(\boldsymbol{a}, c', r^{-1/2}X)$ is irreducible in $K[X]$ for all $r \in K^*$, and the splitting field is a QC-extension of K and a quaternion extension of $K(\sqrt{c'})$.*

(c) *Any QC-extension of K is obtained by a specialisation as in* (b).

PROOF. $G(\boldsymbol{\alpha}, c, X)$ is the minimal polynomial of

$$\sqrt{1 + \frac{c(1-\alpha\beta\gamma)}{\sqrt{AB}} + \frac{(1-\alpha\beta\gamma)\sqrt{c}}{\sqrt{BC}} + \frac{c(1-\alpha\beta\gamma)\sqrt{c}}{\sqrt{CA}}}$$

over $K(\boldsymbol{\alpha}, c)$. □

REMARK. Any polynomial of degree 8 with QC as Galois group is Tschirnhaus equivalent to a polynomial of the form given in (b) above. This follows from the fact that any two non-central subgroups of QC of order 2 are conjugate under the action of $\operatorname{Aut} QC$. However, as they are not necessarily conjugate under the action of QC itself, it is perfectly possible for two such polynomials to give the same QC-extension *without* being Tschirnhaus equivalent.

EXAMPLE. Let $K = \mathbb{Q}$, $\alpha = 1$, $\beta = 0$, $\gamma = 1$ and $c = 2$, i.e., $u = 6$, $v = 1$ and $w = 5$. Then we get the polynomial

$$G(1,0,1,2,X) = (X^2-1)^4 - \tfrac{8}{3}(X^2-1)^2 - \tfrac{32}{15}(X^2-1) - \tfrac{32}{75} \in \mathbb{Q}[X],$$

which has the root

$$\sqrt{1 + \frac{2}{\sqrt{6}} + \frac{\sqrt{2}}{\sqrt{5}} + \frac{2\sqrt{2}}{\sqrt{30}}} = \sqrt{\tfrac{1}{15}(3+\sqrt{6})(5+\sqrt{10})}.$$

We let $r = 15$ and get

$$\begin{aligned} g(X) &= 15^4 G(1,0,1,2,X/\sqrt{15}) \\ &= (X^2-15)^4 - 600(X^2-15)^2 - 7200(X^2-15) - 21600 \in \mathbb{Q}[X] \end{aligned}$$

as the minimal polynomial for $\sqrt{(3+\sqrt{6})(5+\sqrt{10})}$ over $\mathbb{Q}$. Thus, the splitting field of $g(X)$ over $\mathbb{Q}$ is the QC-extension

$$\mathbb{Q}(\sqrt{(3+\sqrt{6})(5+\sqrt{10})}, \sqrt{2})/\mathbb{Q}.$$

REMARK. It is possible to treat the central product QQ, i.e., the group with generators i, j, i' and j', and relations $i^2 = j^2 = i'^2 = j'^2 = -1$, $ji = -ij$, $j'i' = -i'j'$, $i'i = ii'$, $j'i = ij'$, $i'j = ji'$ and $j'j = jj'$, in a way similar to Q_8 and QC. See [Le6] and [Le7] for details. Another description can be found in [SmT, Thm. 3.1], where the group is named DD.

6.3. The Quasi-Dihedral Group

In this section, we consider the quasi-dihedral group QD_8 of degree 8 as Galois group, and define a *quasi-dihedral extension* as a Galois extension with Galois group isomorphic to QD_8. Again, we will look only at fields of characteristic $\neq 2$.

First, we notice that QD_8 maps onto D_4 by $\pi\colon u \mapsto \sigma$, $v \mapsto \tau$. We know what D_4-extensions look like, and so we will study embeddings along π:

Let $M/K = K(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b})/K$ be a D_4-extension as in Theorem 2.2.7, i.e., $a, b \in K^*$ quadratically independent, $\alpha, \beta \in K$ with $\alpha^2 - a\beta^2 = ab$, and $r \in K^*$ arbitrary. For convenience, we let $\theta = r(\alpha + \beta\sqrt{a})$.

We can identify D_4 with $\mathrm{Gal}(M/K)$ by letting σ and τ in D_4 operate on M by

$$\begin{aligned} \sigma\colon &\quad \sqrt{\theta} \mapsto \frac{\alpha - \beta\sqrt{a}}{\sqrt{a}\sqrt{b}}\sqrt{\theta}, &&\quad \sqrt{b} \mapsto \sqrt{b}, \\ \tau\colon &\quad \sqrt{\theta} \mapsto \sqrt{\theta}, &&\quad \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

To say that $M/K \subseteq F/K$, where F/K is a quasi-dihedral extension containing M/K, is an embedding along π then means that $F/K(\sqrt{a})$ is a quaternion extension, since $Q_8 \simeq \langle u^2, v\rangle \subseteq QD_8$.

THEOREM 6.3.1. *Let $M/K = K(\sqrt{\theta}, \sqrt{b})/K$ be a D_4-extension as above, and assume $\alpha \neq 0$. Then M/K can be embedded in a quasi-dihedral extension along π if and only if the quadratic forms $bX^2 + 2r\alpha Y^2 + 2br\alpha Z^2$ and $aU^2 + 2V^2 + 2aW^2$*

are equivalent over K. Furthermore, if $\mathbf{P}$ is a 3×3 matrix over K with $\det\mathbf{P} = a/br\alpha$ *and*

$$\mathbf{P}^t\begin{pmatrix} b & 0 & 0\\ 0 & 2r\alpha & 0\\ 0 & 0 & 2br\alpha\end{pmatrix}\mathbf{P} = \begin{pmatrix} a & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2a\end{pmatrix},$$

the quasi-dihedral extensions in question are

$$M(\sqrt{s\omega})/K = K(\sqrt{s\omega},\sqrt{a})/K, \quad s\in K^*,$$

where

$$\begin{aligned}\omega = 1 &+ p_{11}\sqrt{b}/\sqrt{a} + \tfrac{1}{2}[p_{22} + p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}]\sqrt{\theta}\\ &+ \tfrac{1}{2}[p_{22} - p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}]\,\frac{\alpha-\beta\sqrt{a}}{\sqrt{a}\sqrt{b}}\sqrt{\theta}.\end{aligned}$$

PROOF. Sufficiency: As stated above, the subgroup of QD_8 generated by u^2 and v is isomorphic to Q_8. Stepping up to $K(\sqrt{a})$ we are thus left with the (easier) problem of embedding the biquadratic extension $M/K(\sqrt{a})$ into a quaternion extension. We have $M = K(\sqrt{a})(\sqrt{\theta},\sigma\sqrt{\theta})$ and $\theta\,\sigma\theta = r^2ab$. Hence, by Witt's Criterion we must find a matrix $\mathbf{S}$ with determinant $1/r^2ab$ expressing the equivalence of $r^2abX^2+\theta Y^2+\sigma\theta Z^2$ and $U^2+V^2+W^2$ over $K(\sqrt{a})$.[9] This is done by letting

$$\mathbf{S} = \begin{pmatrix} 1/r\sqrt{a} & 0 & 0\\ 0 & 1 & \sigma\theta/r\sqrt{a}\\ 0 & 1 & -\theta/r\sqrt{a}\end{pmatrix}\mathbf{P}\begin{pmatrix} 1/\sqrt{a} & 0 & 0\\ 0 & 1/2 & 1/2\\ 0 & 1/2\sqrt{a} & -1/2\sqrt{a}\end{pmatrix}.$$

Hence, a quaternion extension containing $M/K(\sqrt{a})$ is obtained by adjoining $\sqrt{\omega}$, where

$$\begin{aligned}\omega &= 1 + s_{11}r\sqrt{a}\sqrt{b} + s_{22}\sqrt{\theta} + s_{33}\,\sigma\sqrt{\theta}\\ &= 1 + p_{11}\sqrt{b}/\sqrt{a}\\ &\qquad + \tfrac{1}{2}\big[(p_{22}+p_{23}/\sqrt{a}) + (p_{32}+p_{33}/\sqrt{a})\,\sigma\theta/r\sqrt{a}\big]\sqrt{\theta}\\ &\qquad + \tfrac{1}{2}\big[(p_{22}-p_{23}/\sqrt{a}) - (p_{32}-p_{33}/\sqrt{a})\,\theta/r\sqrt{a}\big]\,\sigma\sqrt{\theta}\\ &= 1 + p_{11}\sqrt{b}/\sqrt{a} + \tfrac{1}{2}[p_{22}+p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}]\sqrt{\theta}\\ &\qquad + \tfrac{1}{2}[p_{22}-p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}]\,\sigma\sqrt{\theta}.\end{aligned}$$

To get back down to K, we notice that $\sigma\tau\omega = \omega$, and so $M(\sqrt{\omega})/K$ is Galois. Also, the pre-images of $\sigma\tau$ in $\mathrm{Gal}(M(\sqrt{\omega})/K)$ have order 2, and so the Galois group is the quasi-dihedral group.

Necessity: Let $M/K \subseteq M(\sqrt{\omega})/K$ be an embedding along π. Then we get $x,y\in M^*$ with $\sigma\omega/\omega = x^2$ and $\tau\omega/\omega = y^2$, and it is easily seen that $x\,\sigma x\,\sigma^2x\,\sigma^3x = -1$, $y\,\tau y = -1$ and $x\,\sigma x\,\sigma^2x\,\sigma^3y = y\,\tau x$.

[9] Technically, it should of course be $\theta X^2+\sigma\theta Y^2+r^2abZ^2$ and $U^2+V^2+W^2$. However, permuting the rows and columns of $\mathbf{S}$ cyclically will not change the determinant, and so it makes no difference to us.

We consider the embedding $\varphi\colon M \hookrightarrow \mathrm{Mat}_8(K)$ corresponding to (say) the basis

$$1, \sqrt{a}, \sqrt{\theta}, \sqrt{a}\sqrt{\theta}, \sqrt{b}, \sqrt{a}\sqrt{b}, \sqrt{\theta}\sqrt{b}, \sqrt{a}\sqrt{\theta}, \sqrt{b}$$

for M/K, and let $\mathbf{U}$ and $\mathbf{V}$ in $\mathrm{Mat}_8(K)$ represent σ and τ in the same basis. Then $\mathbf{U}$ and $\mathbf{V}$ generate a subgroup of $\mathrm{GL}_8(K)$ isomorphic to D_4, and $\mathbf{U}\varphi(t) = \varphi(\sigma t)\mathbf{U}$ and $\mathbf{V}\varphi(t) = \varphi(\tau t)\mathbf{V}$ for $t \in M$.

We let $\mathbf{U}' = \varphi(x)\mathbf{U}$ and $\mathbf{V}' = \varphi(y)\mathbf{V}$, and look at the subalgebras

$$Q_1 = K[\varphi(\sqrt{a})\mathbf{U}'^2, \mathbf{U}' + \mathbf{U}'^3] \simeq \Big(\frac{-a,-2}{K}\Big),$$
$$Q_2 = K[\varphi(\sqrt{b})\mathbf{U}'^2, \varphi(\sqrt{\theta})\mathbf{U}' - \varphi(\sigma\sqrt{\theta})\mathbf{U}'^3] \simeq \Big(\frac{-b,-2r\alpha}{K}\Big) \quad \text{and}$$
$$Q_3 = K[\varphi(\sqrt{b}), \mathbf{U}'\mathbf{V}'] \simeq \Big(\frac{b,1}{K}\Big).$$

They centralise each other, and as in the proof of Theorem 6.2.1 we conclude that $Q_1 \simeq Q_2$. □

If $\alpha = 0$, then $-b$ is a square in K^*, and we may assume $b = -1$. Then $M/K = K(\sqrt[4]{r^2a}, i)/K$, $i = \sqrt{-1}$, and replacing a by r^2a, we get a D_4-extension of the form $M/K = K(\sqrt[4]{a}, i)/K$.

THEOREM 6.3.2. *Let $M/K = K(\sqrt[4]{a}, i)/K$ be a D_4-extension as above. Then M/K can be embedded in a quasi-dihedral extension along π, if and only if*

$$\exists p, q \in K\colon p^2 + aq^2 = -2.$$

In this case the quasi-dihedral extensions in question are

$$K(\sqrt{r(1+i)(p+qi\sqrt{a})\,\sqrt[4]{a}}\,, i)/K, \quad r \in K^*.$$

PROOF. We keep the notation from the proof of Theorem 6.3.1.

'If': We let $x = (1-i)/(p+qi\sqrt{a})$, $y = (1+i)/(p+qi\sqrt{a})$ and $\omega = (1+i)(p+qi\sqrt{a})\,\sqrt[4]{a}$.

'Only if': We get Q_1 and Q_3 as before, but

$$[\varphi(\sqrt[4]{a})\mathbf{U}' - \varphi(i\,\sqrt[4]{a})\mathbf{U}'^3]^2 = 0.$$

Thus, the centraliser of Q_1 inside $\mathrm{Mat}_4(K)$ (i.e., inside the centraliser of Q_3) contains a zero divisor and is thus split. The same then holds for Q_1 itself. Hence, -2 is a norm in $K(i\sqrt{a})/K$. □

QD_8 as Galois group is considered in [Ki] and [GS&S].

Now to describe quasi-dihedral extensions and produce a generic polynomial: Let M/K be a D_4-extension. By the proof of Corollary 2.2.8, we may assume

$$M = K(\sqrt{r(a+\sqrt{a})}, \sqrt{b}),$$

where a and $b = a - 1$ in K^* are quadratically independent, and $r \in K^*$ is arbitrary. In the notation introduced above, $\alpha = a$ and $\beta = 1$. In particular,

$\alpha \neq 0$, so by Theorem 6.3.1 we can embed M/K into a quasi-dihedral extension along π, if and only if

$$bX^2 + 2raY^2 + 2rabZ^2 \sim aU^2 + 2V^2 + 2aW^2.$$

Thus, the embedding problem is solvable for *some* $r \in K^*$, if and only if the quadratic form $aU^2 + 2V^2 + 2aW^2$ represents b over K, i.e., if and only if

$$ax^2 + 2y^2 + 2az^2 = b = a - 1$$

for suitable $x, y, z \in K$. Modifying y and z if necessary, we may assume $1 - x^2 - 2z^2 \neq 0$ and hence

$$a = \frac{1 + 2y^2}{1 - x^2 - 2z^2}.$$

Choosing our modified y and z with care, we may assume $ax^2 + 2y^2 \neq 0$ as well. Now,

$$\mathbf{Q}^t \begin{pmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 2a \end{pmatrix} \mathbf{Q} = \begin{pmatrix} b & 0 & 0 \\ 0 & 2a(ax^2 + 2y^2) & 0 \\ 0 & 0 & 2ab(ax^2 + 2y^2) \end{pmatrix}$$

for

$$\mathbf{Q} = \begin{pmatrix} x & -2y & -2axz \\ y & ax & -2ayz \\ z & 0 & ax^2 + 2y^2 \end{pmatrix}.$$

Also, $\det \mathbf{Q} = b(ax^2 + 2y^2)$.

Thus, the embedding problem is solvable for $r = ax^2 + 2y^2$. More generally, it is solvable whenever

$$bX^2 + 2raY^2 + 2rabZ^2 \sim bX'^2 + 2a(ax^2 + 2y^2)Y'^2 + 2ab(ax^2 + 2y^2)Z'^2.$$

By the Witt Cancellation Theorem this is equivalent to

$$2raY^2 + 2rabZ^2 \sim 2a(ax^2 + 2y^2)Y'^2 + 2ab(ax^2 + 2y^2)Z'^2,$$

i.e., to

$$rY^2 + rbZ^2 \sim (ax^2 + 2y^2)(Y'^2 + bZ'^2).$$

Hence, we must have $r = (ax^2 + 2y^2)(p^2 + bq^2)$ for suitable $p, q \in K$. And since we can modify r by a factor from $K^* \cap (K(\sqrt{a}, \sqrt{b})^*)^2$ without changing M, we can let $p = 1$ and $r = (ax^2 + 2y^2)(1 + bq^2)$. Then

$$\mathbf{Q}'^t \begin{pmatrix} a & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2a \end{pmatrix} \mathbf{Q}' = \begin{pmatrix} b & 0 & 0 \\ 0 & 2ra & 0 \\ 0 & 0 & 2rab \end{pmatrix}$$

when

$$\mathbf{Q}' = \mathbf{Q} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -bq \\ 0 & q & 1 \end{pmatrix} = \begin{pmatrix} x & -2(y + aqxz) & 2(bqy - axz) \\ y & a(x - 2qyz) & -a(bqx + 2yz) \\ z & (ax^2 + 2y^2)q & ax^2 + 2y^2 \end{pmatrix},$$

and $\det \mathbf{Q}' = rb$.

To use the construction in Theorem 6.3.1 we need

$$\begin{aligned}\mathbf{P} = \mathbf{Q}'^{-1} &= \begin{pmatrix} 1/b & 0 & 0 \\ 0 & 1/2ra & 0 \\ 0 & 0 & 1/2rab \end{pmatrix} \mathbf{Q}'^{t} \begin{pmatrix} a & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2a \end{pmatrix} \\ &= \begin{pmatrix} ax/b & 2y/b & 2az/b \\ -(y+aqxz)/r & (x-2qyz)/r & (ax^2+2y^2)q/r \\ (bqy-axz)/rb & -(bqx+2yz)/rb & (ax^2+2y^2)/rb \end{pmatrix},\end{aligned}$$

and we get

THEOREM 6.3.3. *A QD_8-extension has the form*

$$K(\sqrt{s\omega}, \sqrt{a})/K, \quad s \in K^*,$$

where

$$a = \frac{1+2y^2}{1-x^2-2z^2}$$

for suitable $x, y, z \in K$, such that a and $b = a-1$ are well-defined and quadratically independent, $ax^2+2y^2 \neq 0$, and

$$\begin{aligned}\omega = 1 &+ \frac{x\sqrt{a}}{\sqrt{b}} \\ &+ \frac{1}{2r}\left[x - 2qyz + \frac{q(ax^2+2y^2)}{\sqrt{a}} + \frac{bqx+2yz}{\sqrt{b}} + \frac{ax^2+2y^2}{\sqrt{a}\sqrt{b}}\right] \times \\ &\qquad \sqrt{r(a+\sqrt{a})} \\ &+ \frac{1}{2r}\left[x - 2qyz - \frac{q(ax^2+2y^2)}{\sqrt{a}} - \frac{bqx+2yz}{\sqrt{b}} + \frac{ax^2+2y^2}{\sqrt{a}\sqrt{b}}\right] \times \\ &\qquad \frac{\sqrt{a}-1}{\sqrt{b}}\sqrt{r(a+\sqrt{a})}\end{aligned}$$

for $q \in K$, such that $r = (ax^2+2y^2)(1+bq^2) \neq 0$.

EXAMPLE. Let $K = \mathbb{Q}$, $x = 0$, $y = 1$, $z = 0$ and $q = 0$. The D_4-extension is then

$$\mathbb{Q}(\sqrt{2(3+\sqrt{3})}, \sqrt{2})/\mathbb{Q} = \mathbb{Q}(\sqrt{3+\sqrt{3}}, \sqrt{2}),$$

and the quasi-dihedral extensions are

$$\mathbb{Q}(\sqrt{s(1+\tfrac{1}{2}[1/\sqrt{2}+1/\sqrt{3}-1/\sqrt{6}]\sqrt{3+\sqrt{3}})}, \sqrt{3})/\mathbb{Q}, \quad s \in \mathbb{Q}^*.$$

COROLLARY 6.3.4. *Let x, y, z, q and s be indeterminates over the field K. Then the polynomial*

$$F(x,y,z,q,s,T) = (T^2-s)^4 + s^2c_2(T^2-s)^2 + s^3c_1(T^2-s) + s^4c_0$$

in $K(x,y,z,q,s,T)$ is a generic polynomial for QD_8-extensions over K, when

$$a = \frac{1+2y^2}{1-x^2-2z^2}, \quad b = a-1, \quad r = (ax^2+2y^2)(1+bq^2),$$
$$h = p_{23} + ap_{32} - p_{33}, \quad k = p_{22} - p_{32} + p_{33},$$
$$\alpha = r(h^2+ak^2+2hk)/4, \quad \beta = r(h^2+ak^2+2ahk)/4a,$$
$$c_2 = -2(ax^2/b + 2\alpha), \quad c_1 = 2rx(p_{23}^2 + abp_{32}^2 - ap_{22}^2 - bp_{33}^2$$
$$-2ap_{22}p_{33} + 2ap_{23}p_{32} - 2p_{23}p_{33} + 2ap_{22}p_{32}),$$
$$c_0 = a^2x^4/b^2 + 2(\alpha^2 + a\beta^2) - 4ax^2\alpha/b - 2(\alpha^2 - a\beta^2)$$

and the p_{ij}'s are the entries in the matrix $\mathbf{P}$ above. Specifically, QD_8-extensions are obtained by specialisations such that a and b are well-defined and quadratically independent, and r and s are $\neq 0$.

PROOF. $f(x,y,z,q,T) = T^4 + c_2T^2 + c_1T + c_0$ is the minimal polynomial for $\omega - 1$, where ω is as in Theorem 6.3.3. It follows that $F(x,y,z,q,s,T)$ is the minimal polynomial for $\sqrt{s\omega}$. □

REMARKS. (1) Let $L/k = k(\sqrt{A},\sqrt{B})/k$ be a $C_2 \times C_2$-extension, and let $\theta = a_1\sqrt{A} + a_2\sqrt{B} + a_3\sqrt{A}\sqrt{B}$, $a_1, a_2, a_3 \in k$, have degree 4. Then the minimal polynomial for θ over k is

$$f(T) = T^4 - 2(a_1^2A + a_2^2B + a_3^2AB)T^2 - 8a_1a_2a_3ABT$$
$$+ (a_1^4A^2 + a_2^4B^2 + a_3^4A^2B^2 - 2a_1^2a_2^2AB - 2a_1^2a_3^2A^2B - 2a_2^2a_3^2AB^2).$$

We notice that the coefficients in degrees 0 and 2 are expressed in terms of $a_1' = a_1^2A$, $a_2' = a_2^2B$ and $a_3' = a_3^2AB$.

In the case of Corollary 6.3.4, we have $L/k = M/K(\sqrt{a})$, $A = b$ and $B = r(a+\sqrt{a})$. Also,

$$a_1 = p_{11}/\sqrt{a},$$
$$a_2 = \tfrac{1}{2}[p_{22} + p_{23}/\sqrt{a} + p_{32}(\sqrt{a}-1) + p_{33}(\sqrt{a}-1)/\sqrt{a}], \quad \text{and}$$
$$a_3 = \tfrac{1}{2}[p_{22}(\sqrt{a}-1)/b - p_{23}(\sqrt{a}-1)/b\sqrt{a} - p_{32} + p_{33}/\sqrt{a}].$$

Calculations in Maple V show that $a_2' = r(1+\sqrt{a})(h+k\sqrt{a})^2/4\sqrt{a} = \alpha + \beta\sqrt{a}$ and a_3' are conjugate in $K(\sqrt{a})/K$. This simplifies the expressions for c_0 and c_2.

(2) Any polynomial of degree 8 with QD_8 as Galois group is Tschirnhaus equivalent to a polynomial of the form given in Corollary 6.3.4. Moreover, two polynomials of degree 8 giving the same QD_8-extension are Tschirnhaus equivalent.

(3) In considering QD_8-extensions built upon a D_4-extension as we have been doing in this section, we may always assume $\alpha \neq 0$: If we have

$$\alpha^2 - a\beta^2 = ab$$

with $\alpha = 0$, we can simply replace α and β by

$$\alpha' = \frac{2\beta}{1/a - 1} \quad \text{and} \quad \beta' = \frac{\beta(1/a + 1)}{1/a - 1}.$$

Consequently, the observations about quadratic forms made above can be formulated more generally as follows: Given a biquadratic extension

$$L/K = K(\sqrt{a}, \sqrt{b})/K,$$

it can be embedded in a QD_8-extension cyclic over $K(\sqrt{b})$, if and only if the quadratic forms

$$X^2 - aY^2 - abZ^2 \quad \text{and} \quad X^2 - 2Y^2 + 2aZ^2 - abW^2$$

are both isotropic over K: The first isotropy guarantees the existence of α and β, and a suitable r is then one for which

$$bX^2 + 2r\alpha Y^2 + 2br\alpha Z^2 \sim aX^2 + 2Y^2 + 2aZ^2.$$

Clearly, such an r exists if and only if

$$aX^2 + 2Y^2 + 2aZ^2 - bW^2$$

is isotropic. But from the first isotropy we deduce

$$aX^2 - bW^2 \sim X^2 - abW^2,$$

and this gives us the second isotropy above.

6.4. The Cyclic Group of Order 8

The quasi-dihedral group QD_8 has exponent 8, and so the embedding of D_4-extensions into quasi-dihedral extensions in section 6.3 also (and incidentially) embeds C_4-extensions in C_8-extensions. With the notation of section 6.3, this happens over $K(\sqrt{b})$.

Looking at the descriptions of C_4- and D_4-extensions in section 2.2 of Chapter 2, we see that C_4-extensions are, loosely speaking, 'degenerate' D_4-extensions, happening when $b = 1$. Thus, we can hope to embed C_4-extensions in C_8-extensions by taking the results of section 6.3 and letting $b = 1$. Again, we restrict our attention to characteristic $\neq 2$.

That this actually works is something of a miracle:

Let $M/K = K(\sqrt{r(\alpha + \beta\sqrt{a})})/K$ be a C_4-extension as in Theorem 2.2.5, i.e., $a \in K^* \setminus (K^*)^2$, $\alpha, \beta \in K$ with $\alpha^2 - a\beta^2 = a$, and $r \in K^*$ arbitrary. Again, we let $\theta = r(\alpha + \beta\sqrt{a})$. As generator for $C_4 = \mathrm{Gal}(M/K)$ we take

$$\sigma\colon \quad \sqrt{\theta} \mapsto \frac{\alpha - \beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

THEOREM 6.4.1. *Let $M/K = K(\sqrt{\theta})/K$ be a C_4-extension as described above, and assume $\alpha \neq 0$. Then M/K can be embedded in a C_8-extension if and only if*

the quadratic forms $X^2+2r\alpha Y^2+2r\alpha Z^2$ *and* $aU^2+2V^2+2aW^2$ *are equivalent over* K. *Furthermore, if* $\mathbf{P}$ *is a* 3×3 *matrix with* $\det\mathbf{P}=a/r\alpha$ *and*

$$\mathbf{P}^t\begin{pmatrix}1&0&0\\0&2r\alpha&0\\0&0&2r\alpha\end{pmatrix}\mathbf{P}=\begin{pmatrix}a&0&0\\0&2&0\\0&0&2a\end{pmatrix},$$

the C_8*-extensions containing* M/K *are*

$$K(\sqrt{s\omega})/K,\quad s\in K^*,$$

where

$$\omega=1+p_{11}/\sqrt{a}+\tfrac{1}{2}[(p_{22}-p_{32})+(p_{23}+p_{33})/\sqrt{a}]\sqrt{\theta}+\\ \tfrac{1}{2}[(p_{22}+p_{32})-(p_{23}-p_{33})/\sqrt{a}]\,\frac{\alpha-\beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

Proof. 'If': Letting

$$\mathbf{S}=\begin{pmatrix}1/r\sqrt{a}&0&0\\0&1&\sigma\theta/r\sqrt{a}\\0&1&-\theta/r\sqrt{a}\end{pmatrix}\mathbf{P}\begin{pmatrix}1/\sqrt{a}&0&0\\0&1/2&1/2\\0&1/2\sqrt{a}&-1/2\sqrt{a}\end{pmatrix},$$

we get

$$\mathbf{S}^t\begin{pmatrix}r^2a&0&0\\0&\theta&0\\0&0&\sigma\theta\end{pmatrix}\mathbf{S}=\mathbf{E}$$

and $\det\mathbf{S}=1/r^2a$. Also,

$$\omega=1+s_{11}r\sqrt{a}+s_{22}\sqrt{\theta}+s_{33}\,\sigma\sqrt{\theta}.$$

Noting that $s_{33}=\sigma s_{22}$, we get

$$\sigma\omega=1-s_{11}r\sqrt{a}-s_{22}\sqrt{\theta}+s_{33}\,\sigma\sqrt{\theta},$$

and by using various equalities (as in the proof of Witt's Criterion), we get

$$\omega\,\sigma\omega=r^2a(s_{12}-s_{21}/\sigma\sqrt{\theta})^2.$$

Hence, $M(\sqrt{\omega})/K$ is Galois. Also,

$$\omega\,\sigma^2\omega=(s_{23}\sqrt{\theta}-s_{32}\,\sigma\sqrt{\theta})^2,$$

and letting

$$x=\frac{s_{23}\sqrt{\theta}-s_{32}\,\sigma\sqrt{\theta}}{\omega}$$

we get $\sigma^2\omega/\omega=x^2$ and $x\,\sigma^2x=-1$. Thus, $M(\sqrt{\omega})/K(\sqrt{a})$ is a C_4-extension, and it follows that $M(\sqrt{\omega})/K$ is a C_8-extension.

'Only if': Let $M(\sqrt{\omega})/K$ be a C_8-extension. Then $\sigma\omega/\omega=x^2$ for some $x\in M^*$, and we see that x has norm -1 in M/K. We define an embedding $\varphi\colon M\hookrightarrow \mathrm{Mat}_4(K)$ by means of some basis, and let $\mathbf{U}\in\mathrm{Mat}_4(K)$ represent σ in

the same basis. Then $\mathbf{U}^4 = 1$ and $\mathbf{U}\varphi(t) = \varphi(\sigma t)\mathbf{U}$ for $t \in M$. Let $\mathbf{U}' = \varphi(x)\mathbf{U}$, and look at the subalgebras

$$Q_1 = K[\varphi(\sqrt{a})\mathbf{U}'^2, \mathbf{U}' + \mathbf{U}'^3] \simeq \Big(\frac{-a,-2}{K}\Big) \quad \text{and}$$
$$Q_2 = K[\mathbf{U}'^2, \varphi(\sqrt{\theta})\mathbf{U}' - \varphi(\sigma\sqrt{\theta})\mathbf{U}'^3] \simeq \Big(\frac{-1,-2r\alpha}{K}\Big)$$

of $\mathrm{Mat}_4(K)$. They centralise each other, and are thus isomorphic. □

EXAMPLE. Let $K = \mathbb{Q}$, $a = 2$, $\alpha = 2$, $\beta = 1$ and $r = 1$, i.e., $M = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. The quadratic forms $X^2 + 4Y^2 + 4Z^2$ and $2U^2 + 2V^2 + 4W^2$ are equivalent over $\mathbb{Q}$, and this equivalence is expressed by the matrix

$$\begin{pmatrix} 1 & -1 & 0 \\ 1/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence, we get

$$\begin{aligned}\omega &= 1 + 1/\sqrt{2} + \sqrt{2+\sqrt{2}}/2 + \sqrt{2+\sqrt{2}}/2\sqrt{2} \\ &= \tfrac{1}{4}(4 + 2\sqrt{2} + 2\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}) \\ &= \tfrac{1}{4}(2+\sqrt{2})(2+\sqrt{2+\sqrt{2}})\end{aligned}$$

and a family

$$\mathbb{Q}(\sqrt{r(2+\sqrt{2+\sqrt{2}})})/\mathbb{Q}, \quad r \in \mathbb{Q}^*,$$

of C_8-extensions.

REMARK. More generally: If $a = 1 + d^4$ (with $d^2 \neq -1$) we can let $\alpha = a/d^2$, $\beta = 1/d^2$ and $r = d^2$ to get $M = K(\sqrt{a+\sqrt{a}})$. Using the matrix

$$\mathbf{P} = \begin{pmatrix} a/(1+d^2) & -2d/(1+d^2) & 0 \\ d/(1+d^2) & 1/(1+d^2) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we get a C_8-extension

$$K\Big(\sqrt{1 + \frac{\sqrt{a}}{1+d^2} + \frac{\sqrt{a+\sqrt{a}}}{1+d^2} + \frac{d^2\sqrt{a+\sqrt{a}}}{(1+d^2)\sqrt{a}}}\Big)/K.$$

This is an explicit special case of Lemma 5.4.1 in Chapter 5.

If $\alpha = 0$, then -1 is a square in K^*, i.e., $i = \sqrt{-1} \in K^*$, and we can assume $M = K(\sqrt[4]{a})$ and $\sigma\sqrt[4]{a} = i\sqrt[4]{a}$. Then

THEOREM 6.4.2. *Assume $i \in K^*$ and let $M/K = K(\sqrt[4]{a})/K$ be a C_4-extension. Then M/K can be embedded in a C_8-extension if and only if*

$$\exists p, q \in K : p^2 - aq^2 = 2,$$

and all the C_8-extensions containing M/K are then

$$K(\sqrt{r(p+q\sqrt{a})\sqrt[4]{a}})/K, \quad r \in K^*.$$

Cyclic extensions of degree 8 are considered in [Ki].

From Theorem 6.4.1 we get that a quadratic extension $K(\sqrt{a})/K$ can be embedded in a C_8-extension, if and only if a is a sum of two squares *and* $a = (1-2y^2)/(x^2+2z^2)$ for some $x, y, z \in K$. As we saw in Chapter 5, these conditions cannot always be combined to provide a generic description of C_8-extensions. It is, of course, perfectly possible to produce an explicit *versal* C_8-extension.

It may perhaps be worth noting that C_8 *does* have the arithmetic lifting property mentioned in Chapter 3: If $a = (1-2y^2)/(x^2+2x^2)$ as above, we can replace a by $\bar{a} = a[1+(t^2-1)^2/(2t)^2]$, where t is an indeterminate, and multiply x and z by $2t/(t^2+1)$. This gives a regular C_8-extension of $K(t)$ specialising to the given one for $t = 1$.

REMARK. As in the case of QD_8-extensions, we can express everything generally in terms of quadratic forms: If $\alpha = 0$, we can again replace α and β by

$$\alpha' = \frac{2\beta}{1/a-1} \quad \text{and} \quad \beta' = \frac{\beta(1/a+1)}{1/a-1}$$

to obtain $\alpha \neq 0$. It follows that a quadratic extension

$$L/K = K(\sqrt{a})/K$$

can be embedded in a C_8-extension if and only if the quadratic forms

$$X^2+Y^2-aZ^2 \quad \text{and} \quad X^2-2Y^2+aZ^2+2aW^2$$

are both isotropic: The first isotropy ensures the existence of α and β, and the second then guarantees the existence of a suitable r.

6.5. The Dihedral Group D_8

In this section, we will look at the dihedral group D_8 of degree 8 as Galois group. D_8 maps onto D_4 by $\pi\colon \sigma \mapsto \sigma$, $\tau \mapsto \tau$, and since we already know what D_4-extensions look like, we will start from there.

As before, we assume all fields to have characteristic $\neq 2$.

THEOREM 6.5.1. *Let $M/K = K(\sqrt{\theta}, \sqrt{b})/K$ be a D_4-extension as in section 6.3, and assume $\alpha \neq 0$. Then M/K can be embedded in a D_8-extension along π if and only if the quadratic forms $bX^2+r\alpha Y^2+br\alpha Z^2$ and $abU^2+2bV^2+2aW^2$ are equivalent over K. Furthermore, if $\mathbf{P}$ is a 3×3 matrix over K with $\det \mathbf{P} = 2a/r\alpha$ and*

$$\mathbf{P}^t \begin{pmatrix} b & 0 & 0 \\ 0 & r\alpha & 0 \\ 0 & 0 & rb\alpha \end{pmatrix} \mathbf{P} = \begin{pmatrix} ab & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 0 & 2b \end{pmatrix},$$

the D_8-extensions in question are

$$K(\sqrt{s\omega}, \sqrt{b})/K, \quad s \in K^*,$$

where

$$\omega = 1 - p_{11}/\sqrt{a} + \tfrac{1}{2}(p_{32} + p_{23}/\sqrt{a})\sqrt{\theta} + \tfrac{1}{2}(p_{22}/b - p_{33}/\sqrt{a})\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}}\sqrt{\theta}.$$

PROOF. 'If': We look first at the problem of embedding $M/K(\sqrt{b})$ in a C_8-extension. $M/K(\sqrt{b})$ has the form required in Theorem 6.4.1, if we replace r, α and β by $r' = r\sqrt{b}$, $\alpha' = \alpha/\sqrt{b}$ and $\beta' = \beta/\sqrt{b}$. Also, letting

$$\mathbf{P}' = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2 & -1/2 \end{pmatrix} \begin{pmatrix} \sqrt{b} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \sqrt{b} \end{pmatrix} \mathbf{P} \begin{pmatrix} 1/\sqrt{b} & 0 & 0 \\ 0 & 1/\sqrt{b} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we get

$$\mathbf{P}'^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2r\alpha & 0 \\ 0 & 0 & 2r\alpha \end{pmatrix} \mathbf{P}' = \begin{pmatrix} a & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2a \end{pmatrix}$$

and $\det \mathbf{P}' = a/r\alpha$. The ω given above is then exactly the one from Theorem 6.4.1, and so $M(\sqrt{\omega})/K(\sqrt{b})$ is C_8. Furthermore, $M(\sqrt{\omega})/K$ is Galois since $\tau\omega = \omega$. The pre-images of τ in $\mathrm{Gal}(M(\sqrt{\omega})/K)$ have order 2, meaning that the Galois group is either D_8 or QD_8.

From the proof of Theorem 6.4.1 we get $\sigma\omega/\omega = x^2$ for

$$x = \frac{r\sqrt{a}\sqrt{b}(s_{12} - s_{21}/\sigma\sqrt{\theta})}{\omega},$$

where

$$\mathbf{S} = \begin{pmatrix} 1/r\sqrt{a}\sqrt{b} & 0 & 0 \\ 0 & 1 & \sigma\theta/r\sqrt{a}\sqrt{b} \\ 0 & 1 & -\theta/r\sqrt{a}\sqrt{b} \end{pmatrix} \mathbf{P} \begin{pmatrix} 1/\sqrt{a} & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2\sqrt{a} & -1/2\sqrt{a} \end{pmatrix}.$$

Now,

$$s_{12} = -\frac{1}{2r\sqrt{a}\sqrt{b}}\big(p_{12} + p_{13}\frac{1}{\sqrt{a}\sqrt{b}}\big), \quad \text{and}$$
$$s_{21} = \frac{1}{2\sqrt{a}}\big[\big(p_{21}\frac{1}{\sqrt{b}} + p_{31}\big) + \big(p_{21}\frac{1}{\sqrt{b}} - p_{31}\big)\frac{\sigma\theta}{r\sqrt{a}\sqrt{b}}\big],$$

and hence

$$\sigma\tau s_{12} = s_{12} \quad \text{and} \quad \sigma\tau s_{21}/\sqrt{\theta} = s_{21}/\sigma\sqrt{\theta},$$

from which we get

$$x\,\sigma\tau x = 1.$$

Thus, the pre-images of $\sigma\tau$ in $\mathrm{Gal}(M(\sqrt{\omega})/K)$ have order 2, and the Galois group is D_8.

'Only if': Let $M/K \subseteq M(\sqrt{\omega})/K$ be an embedding along π, and let $x, y \in M^*$ be given by $\sigma\omega/\omega = x^2$ and $\tau\omega/\omega = y^2$. Look at the embedding $\varphi\colon M \hookrightarrow$

$\mathrm{Mat}_8(K)$ defined by some basis for M/K, and let $\mathbf{U}$ and $\mathbf{V}$ represent σ and τ in the same basis. Let $\mathbf{U}' = \varphi(x)\mathbf{U}$ and $\mathbf{V}' = \varphi(y)\mathbf{V}$. Then the subalgebras

$$\begin{aligned}
Q_1 &= K[\varphi(\sqrt{b}), \mathbf{V}'] \simeq \Big(\frac{b,1}{K}\Big),\\
Q_2 &= K[\varphi(\sqrt{a}\sqrt{b})\mathbf{U}'^2, \varphi(\sqrt{b})(\mathbf{U}' + \mathbf{U}'^3)] \simeq \Big(\frac{-ab,-2b}{K}\Big) \quad \text{and}\\
Q_3 &= K[\varphi(\sqrt{b})\mathbf{U}'^2, \frac{1}{2}\varphi(\sqrt{\theta} - \sigma\sqrt{\theta})\mathbf{U}' - \frac{1}{2}\varphi(\sqrt{\theta} + \sigma\sqrt{\theta})\mathbf{U}'^3]\\
&\simeq \Big(\frac{-b,-r\alpha}{K}\Big)
\end{aligned}$$

centralise each other, and we conclude $Q_2 \simeq Q_3$. □

If $i = \sqrt{-1} \in K^*$, we have

THEOREM 6.5.2. *Let $M/K = K(\sqrt[4]{a}, i)/K$, $a \in K^*$, be a D_4-extension. Then M/K can be embedded in a D_8-extension along π if and only if*

$$\exists p, q \in K : p^2 - aq^2 = 2,$$

and all the D_8-extensions in question are then

$$K(\sqrt{r(p + q\sqrt{a})\sqrt[4]{a}}, i)/K, \quad r \in K^*.$$

D_8 as Galois group is considered in [Ki] and [GS&S]. Also, [Bl2, Thm. 4.6] proves the existence of generic D_8-extensions.

Now, let $M/K = K(\sqrt{r(a + \sqrt{a})}, \sqrt{b})$, $b = a - 1$, be a D_4-extension. M/K can be embedded in a D_8-extension along π for *some* $r \in K^*$, if and only if $abU^2 + 2aV^2 + 2bW^2$ represents b, i.e., if and only if the quadratic form $abU^2 + 2aV^2 + 2bW^2 - bX^2$ is isotropic. Multiplying by $2ab$ and removing square factors, we see that this is equivalent to $2U^2 + bV^2 + aW^2 - 2aX^2$ being isotropic, or to $aU^2 + 2V^2 - 2aX^2$ representing $-b$:

$$ax^2 + 2y^2 - 2az^2 = -b = 1 - a$$

for suitable $x, y, z \in K$. We may assume $1 + x^2 - 2z^2 \neq 0$ and get

$$a = \frac{1 - 2y^2}{1 + x^2 - 2z^2}.$$

Modifying y and z properly, we may assume z and $b + 2y^2$ to be non-zero as well.

Now, returning to the criterion of Theorem 6.5.1,

$$\mathbf{Q}^t \begin{pmatrix} ab & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 0 & 2b \end{pmatrix} \mathbf{Q} = \begin{pmatrix} b & 0 & 0 \\ 0 & a(b + 2y^2) & 0 \\ 0 & 0 & ab(b + 2y^2) \end{pmatrix}$$

for

$$\mathbf{Q} = \begin{pmatrix} y/az & -1 & -xy/z \\ b/2az & y & -bx/2z \\ x/2z & 0 & (b + 2y^2)/2z \end{pmatrix}.$$

Also, $\det \mathbf{Q} = (b + 2y^2)/2$.

Thus, the embedding problem is solvable for $r = b + 2y^2$, and more generally whenever

$$rX^2 + rbY^2 \sim (b + 2y^2)U^2 + b(b + 2y^2)V^2.$$

Hence, we must have $r = (b + 2y^2)(p^2 + bq^2)$ for suitable $p, q \in K$. Again, we can let $p = 1$ and thus $r = (b + 2y^2)(1 + bq^2)$. Then

$$\mathbf{Q}'^t \begin{pmatrix} ab & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 0 & 2b \end{pmatrix} \mathbf{Q}' = \begin{pmatrix} b & 0 & 0 \\ 0 & ra & 0 \\ 0 & 0 & rab \end{pmatrix}$$

when

$$\begin{aligned} \mathbf{Q}' &= \mathbf{Q} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -bq \\ 0 & q & 1 \end{pmatrix} \\ &= \begin{pmatrix} y/az & -(z + qxy)/z & (bqz - xy)/z \\ b/2az & (2yz - bqx)/2z & -(2qyz + x)b/2z \\ x/2z & (b + 2y^2)q/2z & (b + 2y^2)/2z \end{pmatrix}, \end{aligned}$$

and $\det \mathbf{Q}' = r/2$.

To use Theorem 6.5.1, we need

$$\begin{aligned} \mathbf{P} = \mathbf{Q}'^{-1} &= \begin{pmatrix} 1/b & 0 & 0 \\ 0 & 1/ra & 0 \\ 0 & 0 & 1/rab \end{pmatrix} \mathbf{Q}'^t \begin{pmatrix} ab & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 0 & 2b \end{pmatrix} \\ &= \begin{pmatrix} y/z & 1/z & x/z \\ -b(z + qxy)/rz & (2yz - bqx)/rz & (b + 2y^2)bq/raz \\ (bqz - xy)/rz & -(x + 2qyz)/rz & (b + 2y^2)/raz \end{pmatrix}, \end{aligned}$$

and we get

THEOREM 6.5.3. *A D_8-extension has the form*

$$K(\sqrt{s\omega}, \sqrt{b})/K, \quad s \in K^*,$$

where

$$a = \frac{1 - 2y^2}{1 + x^2 - 2z^2}$$

for suitable $x, y, z \in K$, such that a and $b = a - 1$ are well-defined and quadratically independent, z and $b + 2y^2$ are non-zero, and

$$\begin{aligned} \omega = 1 - \frac{y}{z\sqrt{a}} - \frac{2ayz(1 + bq) + ab(1 - q)x + (b + 2y^2)b}{2rabz} \sqrt{r(a + \sqrt{a})} \\ + \frac{b(b + 2y^2)(1 + bq) + a^2(2yz - bqx)}{2rabz\sqrt{a}} \sqrt{r(a + \sqrt{a})} \end{aligned}$$

for $q \in K$, such that $r = (b + 2y^2)(1 + bq^2) \neq 0$.

EXAMPLE. Let $K = \mathbb{Q}$, $x = 0$, $y = 2$, $z = 1$ and $q = 0$. The D_4-extension is then

$$\mathbb{Q}(\sqrt{14(7 + \sqrt{7})}, \sqrt{6})/\mathbb{Q} = \mathbb{Q}(\sqrt{2(7 + \sqrt{7})}, \sqrt{6})/\mathbb{Q},$$

and the family of D_8-extensions is

$$\mathbb{Q}(\sqrt{s(1-3/\sqrt{7}+\tfrac{5}{21}\sqrt{2(7+\sqrt{7})}-\tfrac{2}{3}\sqrt{2(7+\sqrt{7})}/\sqrt{7})},\sqrt{6})/\mathbb{Q},$$

for $s \in \mathbb{Q}^*$.

Considering x, y, z, q and s as indeterminates, we get our generic polynomial for D_8-extensions:

COROLLARY 6.5.4. *Let x, y, z, q and s be indeterminates over the field K. Then the polynomial*

$$G(x,y,z,q,s,T) = (T^2-s)^4 + s^2d_2(T^2-s)^2 + s^3d_1(T^2-s) + s^4d_0$$

in $K(x,y,z,q,s,T)$ is a generic polynomial for D_8-extensions, when

$$a = \frac{1-2y^2}{1+x^2-2z^2}, \quad b = a-1, \quad r = (b+2y^2)(1+bq^2),$$
$$\alpha = -y/az, \quad \beta = -(2ayz(1+bq)+ab(1-q)x+(b+2y^2)b)/2rabz,$$
$$\gamma = (b(b+2y^2)(1+bq)+a^2(2yz-bqx))/2ra^2bz,$$
$$d_2 = -2a(\alpha^2+r\beta^2+ra\gamma^2+2r\beta\gamma),$$
$$d_1 = -4ra\alpha(\beta^2+a\gamma^2+2a\beta\gamma) \quad \textit{and}$$
$$d_0 = a(a\alpha^4+r^2b\beta^4+r^2a^2b\gamma^4-2ra\alpha^2\beta^2-2ra^2\alpha^2\gamma^2$$
$$-2r^2ab\beta^2\gamma^2+2r^2a\beta^3\gamma-4r\alpha^2\beta\gamma).$$

Specifically, D_8-extensions are obtained by specialisations such that a and b are well-defined and quadratically independent, and r and s are $\neq 0$.

PROOF. $g(x,y,z,q,T) = T^4 + d_2T^2 + d_1T + d_0$ is the minimal polynomial for $\omega - 1$, where ω is as in Theorem 6.5.3. □

REMARKS. (1) If $L/k = k(\sqrt{r(a+\sqrt{a})})/k$, where $a = 1+c^2$, is a C_4-extension, the minimal polynomial for an element

$$\theta = \alpha\sqrt{a} + \beta\sqrt{r(a+\sqrt{a})} + \gamma\sqrt{a}\sqrt{r(a+\sqrt{a})} \in L$$

of degree 4 is

$$f(T) = T^4 - 2a(\alpha^2+r\beta^2+ra\gamma^2+2r\beta\gamma)T^2$$
$$-4ra\alpha(\beta^2+a\gamma^2+2a\beta\gamma)T + a(a\alpha^2+r^2c^2\beta^4+r^2c^2a^2\gamma^4$$
$$-2ra\alpha^2\beta^2-2ra^2\alpha^2\gamma^2-2r^2c^2a\beta^2\gamma^2+2r^2a\beta^3\gamma-4r\alpha^2\beta\gamma).$$

In the case of Theorem 6.5.4, we let $\theta = \omega - 1$, $L/k = M/K(\sqrt{b})$ and $c = \sqrt{b}$.

(2) In terms of quadratic forms, we get: A biquadratic extension

$$L/K = K(\sqrt{a},\sqrt{b})/K$$

can be embedded in a D_8-extension cyclic over $K(\sqrt{b})$, if and only if the quadratic forms

$$X^2 - aY^2 - abZ^2 \quad \text{and} \quad X^2 - aY^2 + 2aZ^2 + 2bW^2$$

are both isotropic over K: From the first isotropy we get

$$-bX^2 + baY^2 \sim X^2 - aY^2,$$

and together with Theorem 6.5.1 this gives us the second isotropy.

Dihedral groups of higher degree. Concerning D_{2^n}-extensions of $\mathbb{Q}$ we mention the following result due to Geyer and Jensen [G&J], obtained by using the theory of ring class fields:

For any imaginary quadratic number field Ω there exists a unique tower of Galois extensions of $\mathbb{Q}$:

$$\mathbb{Q} \subset \Omega = M_1 \subset M_2 \subset M_3 \subset M_4 \subset \cdots$$

such that $\mathrm{Gal}(M_n/\mathbb{Q}) = D_{2^{n-1}}$ for all n (with the convention that $D_1 = C_2$ and $D_2 = V_4$), and M_n/Ω is cyclic. The union $\cup_{n=1}^{\infty} M_n$ is then a 'pro-dihedral' extension of $\mathbb{Q}$.

For $\Omega = \mathbb{Q}(\sqrt{-1})$ the first layers of this tower are the following:

$$\begin{aligned}
M_2 &= \mathbb{Q}(\sqrt{-1}, \sqrt{2}),\\
M_3 &= \mathbb{Q}(\sqrt{-1}, \sqrt[4]{2}),\\
M_4 &= \mathbb{Q}(\sqrt{-1}, \sqrt[8]{2}\sqrt{2+\sqrt{2}}\,),\\
M_5 &= \mathbb{Q}(\sqrt{-1}, \sqrt[16]{2}\sqrt[4]{1+\sqrt{2}}\,) \quad \text{and}\\
M_6 &= \mathbb{Q}(\sqrt{-1}, \sqrt[8]{-32-24\sqrt{2}+30\sqrt[4]{2}+18(\sqrt[4]{2})^3})
\end{aligned}$$

(i.e., the splitting field of $X^{32} + 128X^{24} - 480X^{16} + 4352X^8 - 32$ over $\mathbb{Q}$).[10]

As for the verification, we note that M_n is characterised by being the unique $D_{2^{n-1}}$-extension of $\mathbb{Q}$ which is cyclic over $\mathbb{Q}(\sqrt{-1})$ and unramified outside 2. The verification for M_2, M_3, M_4 and M_5 are straightforward, while M_6 needs some comments: Put

$$\begin{aligned}
\beta &= \sqrt[16]{2}\sqrt[4]{1+\sqrt{2}}\,,\\
\alpha &= -32-24\sqrt{2}+30\sqrt[4]{2}+18(\sqrt[4]{2})^3
\end{aligned}$$

and $i = \sqrt{-1}$. Then $M_6 = \mathbb{Q}(i, \sqrt[8]{\alpha})$. Obviously, M_6 contains the field $\mathbb{Q}(i, \sqrt[4]{2}) = M_3$. Let σ be the automorphism of $\mathrm{Gal}(M_3/\mathbb{Q})$ for which

$$\sigma(\sqrt[4]{2}) = i \cdot \sqrt[4]{2} \quad \text{and} \quad \sigma(i) = i.$$

Then $\sigma(\alpha) = \alpha^{-3}\gamma^8$ where

$$\gamma = -1 + \frac{3}{2}(\sqrt[4]{2})^3 i + \sqrt[4]{2}\,i + 2i - \frac{1}{2}(\sqrt[4]{2})^3 + 2\sqrt{2}\,i.$$

Hence there is a unique extension $\bar{\sigma}$ of σ to M_6 for which $\bar{\sigma}(\sqrt[8]{\alpha}) = \gamma/(\sqrt[8]{\alpha})^3$ where $\bar{\sigma}$ turns out to have order 32. Finally, if τ denote complex conjugation, by computation with MAPLE, one finds that $\tau\sigma\tau = \sigma^{-1}$. Hence $\mathrm{Gal}(M_6/\mathbb{Q}) = D_{32}$ and $\mathrm{Gal}(M_6/\Omega) = C_{32}$. Finally, the field discriminant of M_6 is a power of 2.

[10]The authors are grateful to J. Klüners/KASH for constructing an explicit polynomial.

The above sequence of dihedral extensions gives rise to a sequence of quasi-dihedral extensions as well. Indeed, the pull-back $C_4 \leftthreetimes D_{2^{n-1}}$ with respect to the epimorphism $D_{2^{n-1}} \twoheadrightarrow C_2$ with kernel $D_{2^{n-2}}$ has $QD_{2^{n-1}}$ as a quotient. Since $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a C_4-extension of $\mathbb{Q}$ containing $\sqrt{2}$, each $M_n(\sqrt{2+\sqrt{2}})$ is a $C_4 \leftthreetimes D_{2^{n-1}}$-extension of $\mathbb{Q}$ containing a $QD_{2^{n-1}}$-subextension. For $n = 4$, 5 and 6, one finds that

$$\begin{aligned}
&\mathbb{Q}(\sqrt{-1}, \sqrt[8]{2})/\mathbb{Q} && \text{is a } QD_8\text{-extension,}\\
&\mathbb{Q}(\sqrt{-1}, \beta\sqrt{1+\sqrt{2}})/\mathbb{Q} && \text{is a } QD_{16}\text{-extension, and}\\
&\mathbb{Q}(\sqrt{-1}, \sqrt[8]{\alpha}\sqrt{2+\sqrt{2}})/\mathbb{Q} && \text{is a } QD_{32}\text{-extension.}
\end{aligned}$$

Moreover, for $n > 2$ the fields produced in this way are $QD_{2^{n-2}}$-extensions of $\mathbb{Q}(\sqrt{-2})$.

6.6. Heisenberg Groups

Let p be an odd prime. Then the *Heisenberg group* of degree p, as defined previously, is the non-abelian group H_{p^3} of order p^3 and exponent p. It can be realised as the subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$ consisting of upper triangular matrices with 1's in the diagonal.

Let σ and τ be generators for $C_p \times C_p$. Then H_{p^3} maps onto $C_p \times C_p$ by $\pi\colon u \mapsto \sigma$, $v \mapsto \tau$, and we can consider H_{p^3}-extensions by looking at embeddings along π.

We assume all fields to have characteristic $\neq p$.

The case $\boldsymbol{\mu_p \subseteq K^*}$. If the primitive p^{th} roots of unity μ_p are contained in K^*, we have no difficulty describing $C_p \times C_p$-extensions: They have the form

$$M/K = K(\sqrt[p]{a}, \sqrt[p]{b})/K,$$

where $a, b \in K^*$ are *p-independent*, i.e., the classes of a and b are linearly independent in the $\mathbb{F}_p$-vector space $K^*/(K^*)^p$. We pick a primitive p^{th} root of unity ζ, and define σ and τ in $C_p \times C_p = \mathrm{Gal}(M/K)$ by

$$\begin{aligned}
\sigma\colon &\quad \sqrt[p]{a} \mapsto \zeta\sqrt[p]{a}, &\quad \sqrt[p]{b} \mapsto \sqrt[p]{b},\\
\tau\colon &\quad \sqrt[p]{a} \mapsto \sqrt[p]{a}, &\quad \sqrt[p]{b} \mapsto \zeta\sqrt[p]{b}.
\end{aligned}$$

THEOREM 6.6.1. [Ma, Cor. p. 523 & Thm. 3(A)] *Let M/K be a $C_p \times C_p$-extension as above. Then M/K can be embedded into an H_{p^3}-extension along π if and only if b is a norm in $K(\sqrt[p]{a})/K$. Furthermore, if $b = \mathrm{N}_{K(\sqrt[p]{a})/K}(z)$ for a $z \in K(\sqrt[p]{a})$, the embeddings along π are $M/K \subseteq K(\sqrt[p]{r\omega}, \sqrt[p]{b})/K$ for $r \in K^*$, where $\omega = z^{p-1}\,\sigma z^{p-2} \cdots \sigma^{p-2} z$.*

PROOF. First, let $M/K \subseteq F/K$ be an embedding along π. The fixed field F^v inside F is a C_p-extension of $K(\sqrt[p]{a})$, and so

$$F^v = K(\sqrt[p]{a}, \sqrt[p]{\omega}) = K(\sqrt[p]{\omega})$$

for some $\omega \in K(\sqrt[p]{a})^*$. Moreover,

$$F = M(\sqrt[p]{\omega}) = K(\sqrt[p]{\omega}, \sqrt[p]{b}).$$

We may assume $w\sqrt[p]{\omega} = \zeta\sqrt[p]{\omega}$. Let $x = u\sqrt[p]{\omega}/\sqrt[p]{\omega} \in M^*$. Then

$$x\,\sigma x \cdots \sigma^{p-1}x = 1$$

(since $u^p = 1$) and $\tau x = \zeta\, x$ (since $vu = uvw$). Let $z = \sqrt[p]{b}/x$. Then $z \in K(\sqrt[p]{a})^*$ and $\mathrm{N}_{K(\sqrt[p]{a})/K}(z) = b$. Hence, b is a norm in $K(\sqrt[p]{a})/K$.

Conversely, assume $b = \mathrm{N}_{K(\sqrt[p]{a})/K}(z)$ for some $z \in K(\sqrt[p]{a})$, and let

$$x = \sqrt[p]{b}/z, \quad \omega = z^{p-1}\,\sigma z^{p-2} \cdots \sigma^{p-2}z.$$

Then

$$x\,\sigma x \cdots \sigma^{p-1}x = 1, \quad \tau x = \zeta\, x, \quad \frac{\sigma\omega}{\omega} = x^p \quad \text{and} \quad \tau\omega = \omega.$$

It follows that $M(\sqrt[p]{\omega})/K$ is Galois, and since ω is clearly not a p^{th} power in M, it is an extension of degree p^3. We extend σ and τ to $M(\sqrt[p]{\omega})$ by

$$\bar\sigma\sqrt[p]{\omega} = x\sqrt[p]{\omega}, \quad \bar\tau\sqrt[p]{\omega} = \sqrt[p]{\omega}.$$

Then $\mathrm{Gal}(M(\sqrt[p]{\omega})/K) \simeq E$ by $\bar\sigma \mapsto u$ and $\bar\tau \mapsto v$. □

From this, a construction of H_{p^3}-extensions is obvious:

COROLLARY 6.6.2. *An H_{p^3}-extension of K has the form*

$$K(\sqrt[p]{r\,z^{p-1}\,\sigma z^{p-2}\cdots\sigma^{p-2}z}, \sqrt[p]{\mathrm{N}_{K(\sqrt[p]{a})/K}(z)})/K, \quad r \in K^*,$$

where $a \in K^* \setminus (K^*)^p$, and $z \in K(\sqrt[p]{a})/K$ is chosen such that a and $\mathrm{N}_{K(\sqrt[p]{a})/K}(z)$ are p-independent in K^*.

The general case. Now, let K be an arbitrary field of characteristic $\neq p$. Then $K(\mu_p)/K$ is cyclic of degree $d = [K(\mu_p):K] \mid p-1$. Let κ be a generator for $\mathrm{Gal}(K(\mu_p)/K)$. We pick an arbitrary, but fixed, primitive p^{th} root of unity ζ, and get $\kappa\zeta = \zeta^e$ for an $e \in \mathbb{Z} \setminus p\mathbb{Z}$.

LEMMA 6.6.3. *Let $\omega \in K(\mu_p)^* \setminus (K(\mu_p)^*)^p$. Then*

(a) *$K(\mu_p, \sqrt[p]{\omega})/K$ is cyclic, if and only if $\kappa\omega/\omega^e \in (K(\mu_p)^*)^p$; and*
(b) [Mo, Thm. 4.3(2.2)] *in that case, the subextension of degree p is $K(\alpha)/K$, where $\alpha = \sum_{i=0}^{d-1} \bar\kappa^i(\sqrt[p]{\omega})$ and $\bar\kappa$ is the unique extension of κ to $K(\mu_p, \sqrt[p]{\omega})$ of order d.*

PROOF. (a) By Kummer Theory, $K(\mu_p, \sqrt[p]{\omega})/K$ is a Galois extension if and only if $\kappa\omega/\omega^j = x^p$ for some $j \in \{1, \dots, p-1\}$ and some $x \in K(\mu_p)^*$. We lift κ to $K(\mu_p, \sqrt[p]{\omega})$ by

$$\kappa\sqrt[p]{\omega} = x\sqrt[p]{\omega},$$

and let $\lambda \in \mathrm{Gal}(K(\mu_p, \sqrt[p]{\omega})/K(\mu_p))$ be given by

$$\lambda\sqrt[p]{\omega} = \zeta\sqrt[p]{\omega}.$$

Then κ and λ generate $\mathrm{Gal}(K(\mu_p, \sqrt[p]{\omega})/K)$, and it is cyclic if and only if $\kappa\lambda = \lambda\kappa$, i.e., if and only if $j \equiv e \pmod p$.

(b) The subextension of degree p is $K' = K(\mu_p, \sqrt[p]{\omega})^{\bar\kappa}$. Clearly, $\alpha \in K'$. Also, $\alpha \notin K(\mu_p)$, since $\sqrt[p]{\omega}$, $(\sqrt[p]{\omega})^e$, $\dots$, $(\sqrt[p]{\omega})^{e^{d-1}}$ are linearly independent over $K(\mu_p)$. Hence, $\alpha \notin K$, and so α generates K'/K. □

Next, let M/K be a p-extension with Galois group $G = \mathrm{Gal}(M/K)$. Then $M(\mu_p)/K(\mu_p)$ is a G-extension as well, and we can identify the groups $\mathrm{Gal}(M/K)$ and $\mathrm{Gal}(M(\mu_p)/K(\mu_p))$, as well as $\mathrm{Gal}(M(\mu_p)/M)$ and $\mathrm{Gal}(K(\mu_p)/K)$.

We define the map $\Phi\colon M(\mu_p) \to M(\mu_p)$ by

$$\Phi(x) = x^{e^{d-1}} \kappa x^{e^{d-2}} \cdots \kappa^{d-1} x, \quad x \in M(\mu_p).$$

Let $\pi\colon E \to G$ be a non-split epimorphism with kernel of order p, and assume that $M(\mu_p)/K(\mu_p) \subseteq M(\mu_p, \sqrt[p]{\beta})/K(\mu_p)$ is an embedding along π for some $\beta \in M(\mu_p)^*$. Then $\sigma\beta/\beta = x_\sigma^p$ for $\sigma \in G$ and suitable $x_\sigma \in M(\mu_p)^*$, and we can extend σ to $M(\mu_p, \sqrt[p]{\beta})$ by

$$\bar\sigma \sqrt[p]{\beta} = x_\sigma \sqrt[p]{\beta}.$$

We note that

$$\bar\sigma\bar\tau\overline{\sigma\tau}^{-1} \sqrt[p]{\beta}/\sqrt[p]{\beta} = x_\sigma\, \sigma x_\tau\, x_{\sigma\tau}^{-1} \in \mu_p, \quad \sigma, \tau \in G.$$

Letting $\omega = \Phi(\beta)$ and $y_\sigma = \Phi(x_\sigma)$, we clearly get $\sigma\omega/\omega = y_\sigma^p$. Moreover, $\kappa\omega/\omega^e = (\beta^{-(e^d-1)/p})^p$, and so $M(\mu_p, \sqrt[p]{\omega})/K$ is Galois.

Now, if $\omega = \xi^p$ for a $\xi \in M(\mu_p)^*$, we must have $\sigma\xi/\xi = \zeta_\sigma\, y_\sigma$ for a $\zeta_\sigma \in \mu_p$, and thus

$$(x_\sigma\, \sigma x_\tau\, x_{\sigma\tau})^{de^{d-1}} = y_\sigma\, \sigma y_\tau\, y_{\sigma\tau}^{-1} = \zeta_\sigma^{-1}\, \zeta_\tau^{-1}\, \zeta_{\sigma\tau}^{-1}.$$

It follows that

$$x_\sigma\, \sigma x_\tau\, x_{\sigma\tau}^{-1} = \eta_\sigma^{-1}\, \eta_\tau^{-1}\, \eta_{\sigma\tau}$$

for $\eta_\rho \in \mu_p$. But then, by picking $\eta_\sigma\, x_\sigma$ instead of x_σ, we get $\bar\sigma\bar\tau = \overline{\sigma\tau}$, contradicting our assumption that π is non-split. Thus, ω is not a p^{th} power in $M(\mu_p)$.

We extend σ to $M(\mu_p, \sqrt[p]{\omega})$ by

$$\hat\sigma \sqrt[p]{\omega} = y_\sigma \sqrt[p]{\omega},$$

and let $\lambda \in \mathrm{Gal}(M(\mu_p, \sqrt[p]{\beta})/M(\mu_p))$ and $\lambda' \in \mathrm{Gal}(M(\mu_p, \sqrt[p]{\omega})/M(\mu_p))$ be given by

$$\lambda \sqrt[p]{\beta} = \zeta \sqrt[p]{\beta} \quad \text{and} \quad \lambda' \sqrt[p]{\omega} = \zeta \sqrt[p]{\omega}.$$

Then we get an isomorphism

$$\mathrm{Gal}(M(\mu_p, \sqrt[p]{\beta})/K(\mu_p)) \simeq \mathrm{Gal}(M(\sqrt[p]{\omega})/K(\mu_p))$$

by

$$\bar\sigma \mapsto \hat\sigma \quad \text{and} \quad \lambda \mapsto \lambda'^{de^{d-1}}.$$

Thus, $M(\mu_p)/K(\mu_p) \subseteq M(\mu_p, \sqrt[p]{\omega})/K(\mu_p)$ is an embedding along π as well. Also, since $\kappa\omega/\omega^e \in (M(\mu_p)^*)^p$, $\mathrm{Gal}(M(\mu_p, \sqrt[p]{\omega})/M)$ is cyclic, and so

$$\mathrm{Gal}(M(\mu_p, \sqrt[p]{\omega})/K(\mu_p)) = E \times C_d,$$

where $E = \mathrm{Gal}(M(\sqrt[p]{\omega})/K(\mu_p))$ and C_d is generated by the unique pre-image $\bar\kappa$ of κ of order d. This pre-image is given by $\bar\kappa \sqrt[p]{\omega} = \beta^{-(e^d-1)/p}(\sqrt[p]{\omega})^e$.

This gives us the better part of

THEOREM 6.6.4. *Let M/K be a p-extension with Galois group $G = \mathrm{Gal}(M/K)$ and let $\pi\colon E \to G$ be a non-split epimorphism with kernel of order p. If*

$$M(\mu_p)/K(\mu_p) \subseteq M(\mu_p, \sqrt[p]{\beta})/K(\mu_p),$$

with $\beta \in M(\mu_p)^*$, is an embedding along π, so is $M/K \subseteq M(\alpha)/K$, where

$$\omega = \Phi(\beta), \quad \bar{\kappa}\sqrt[p]{\omega} = \beta^{-(e^d-1)/p}\sqrt[p]{\omega}, \quad \textit{and} \quad \alpha = \sum_{i=0}^{d-1} \bar{\kappa}^i \sqrt[p]{\omega},$$

and all *embeddings of M/K along π are obtained in this way by replacing β with $r\beta$ for $r \in K(\mu_p)^*$.*

PROOF. Most of the theorem is already proved or follows from Lemma 6.6.3. We only need to prove that we do in fact get all embeddings:

Let $M/K \subseteq F/K$ be an embedding along π. Then $F(\mu_p)/K(\mu_p)$ is an embedding along π too, and hence $F(\mu_p) = M(\mu_p, \sqrt[p]{r\beta})$ for some $r \in K(\mu_p)^*$. Since $F(\mu_p)/M$ is cyclic, we must have $\kappa(r\beta)/(r\beta)^e \in (M(\mu_p)^*)^p$, from which it follows that $\Phi(r\beta)$ is p-equivalent to $(r\beta)^{de^{d-1}}$. Thus, $F(\mu_p) = M(\mu_p, \sqrt[p]{\overline{\Phi(r\beta)}})$, and we get F/K as above. □

COROLLARY 6.6.5. *M/K can be embedded along π if and only if $M(\mu_p)/K(\mu_p)$ can.*

REMARK. If E is a cyclic p-group, Theorem 6.6.4 is contained in [Al, IX.§7]. If E is non-abelian of order p^3 (such as the Heisenberg group), it is contained in [Bt, Th. 4]. More generally, [Mo] deals with the case where G is an abelian p-group.

COROLLARY 6.6.6. *There exists a generic polynomial of degree p^2 with $d(p+2)$ parameters for H_{p^3}-extensions over K.*

PROOF. Given an H_{p^3}-extension M/K, $M(\mu_p)/K(\mu_p)$ is an H_{p^3}-extension as in the previous section. From Lemma 6.6.3 we then get that we may assume $a = \Phi(\alpha)$ and $b = \Phi(\mathrm{N}_{K(\mu_p, \sqrt[p]{a})/K(\mu_p)}(y))$ for some

$$\alpha = \sum_{i=0}^{d-1} \alpha_i \zeta^i \in K(\mu_p)^*$$

and

$$y = \sum_{i,j} y_{ij} \zeta^i (\sqrt[p]{a})^j \in K(\mu_p, \sqrt[p]{a})^*.$$

M is the splitting field of the minimal polynomial for $\sum_{i=0}^{d-1} \bar{\kappa}^i(\sqrt[p]{\omega})$ over K, and in the description of ω we additionally get an element $r = \sum_{i=0}^{d-1} r_i\zeta^i \in K(\mu_p)^*$. Considering the α_i's, y_{ij}'s and r_i's as indeterminates, we have a parametric polynomial for H_{p^3} over K. It is generic by Proposition 1.1.5 in Chapter 1, since the construction depends only on the degree of the p^{th} cyclotomic field. □

EXAMPLE. We look at $p = 3$. If $\mu_3 \not\subseteq K^*$, we must have $d = e = 2$, and we see that we can let $\Phi(x) = \kappa x/x$. With α, y and r as above, we get

$$\omega = \frac{\kappa(ry^2\sigma y)}{ry^2\sigma y},$$

and so $\bar{\kappa}\sqrt[3]{\omega} = 1/\sqrt[3]{\omega}$. Now, if $f(X) \in K[X]$ is the minimal polynomial for $\omega + 1/\omega$ over K, $f(X^3 - 3X)$ is the minimal polynomial for $\sqrt[3]{\omega} + 1/\sqrt[3]{\omega}$, and so the generic polynomial is

$$(X^3 - 3X - \gamma)(X^3 - 3X - \sigma\gamma)(X^3 - 3X - \sigma^2\gamma),$$

where

$$\gamma = \frac{r^2y^4\sigma y^2 + \kappa(r^2y^4\sigma y^2)}{ry^2\sigma y\,\kappa(ry^2\sigma y)}.$$

As an example, consider $K = \mathbb{Q}$ and $\zeta = e^{2\pi i/3}$, and let $a = \zeta$. Then $\mathbb{Q}(\mu_3, \sqrt[3]{a})$ is the ninth cyclotomic field $\mathbb{Q}(\mu_9)$, and we can let $\sqrt[3]{a} = \upsilon = e^{2\pi i/9}$. Next, we let $y = \upsilon + 2$, and get

$$\beta = y\,\sigma y\,\sigma^2 y = \zeta + 8$$

and

$$b = \frac{\kappa\beta}{\beta} = \frac{2 - 3\zeta}{3 - 2\zeta}.$$

The numerator and denominator of b both have norm 19 in $\mathbb{Q}(\mu_3)/\mathbb{Q}$ and are thus irreducible in $\mathbb{Z}[\zeta]$. Also, they are not associated, and so b is not associated to a third power in $\mathbb{Q}(\mu_3)$. It follows that b is not a third power in $\mathbb{Q}(\mu_9)$.

Consequently, the $C_3 \times C_3$-extension $\mathbb{Q}(\mu_3, \sqrt[3]{a}, \sqrt[3]{b})/\mathbb{Q}(\mu_3)$ can be embedded into an H_{27}-extension. More precisely, computer calculations give us an H_{27}-polynomial

$$(X^3 - 3X)^3 - \frac{3 \cdot 307}{19^2}(X^3 - 3X)^2 + \frac{3 \cdot 3079}{19^3}(X^3 - 3X) - \frac{541}{19^3}$$

over $\mathbb{Q}$.

For larger primes (i.e. > 3), the generic H_{p^3}-polynomial constructed will of course be much more unwieldy. However, the construction *can* be used to produce specific example, as for H_{27} above. For example, we can get an H_{125}-extension of $\mathbb{Q}$ by

$$\alpha = e^{2\pi i/5} \quad \text{and} \quad y = 1 - e^{2\pi i/25} + e^{4\pi i/25}.$$

The corresponding minimal polynomial has been computed by the authors, but as the coefficients are astronomical, there is little point in including it here.

Exercises

EXERCISE 6.1. Prove that the semi-direct product $C_3 \rtimes C_4$, considered in Exercise 2.7 in Chapter 2, and the special linear group $\mathrm{SL}(2,3) = \mathrm{SL}_2(\mathbb{F}_3)$ are both subgroups of $\mathbb{H}^*$.

EXERCISE 6.2. Let K be a field of characteristic $\neq 2$, and let $K(\sqrt{b})/K$ be a quadratic extension. Let $K(\sqrt{b})_{2^n}$ denote the $2^{n\,\text{th}}$ cyclotomic field over $K(\sqrt{b})$. Assume that a is a norm in $K(\sqrt{b})_{2^n}/K$, but not a square or b times a square in K. Prove that $K(\sqrt{a},\sqrt{b})/K$ can be embedded in a D_{2^n}-, a QD_{2^n}- and an $M_{2^{n+1}}$-extension, all cyclic over $K(\sqrt{b})$. [Hint: Proceed in analogy with the proof of Lemma 5.4.1 in Chapter 5.]

EXERCISE 6.3. (1) Let M/K be a Galois extension with cyclic Galois group $\mathrm{Gal}(M/K) = C_n$ of order n, and let σ be a generator for C_n. Also, let $a \in M^*$. Define a K-algebra $\Gamma = (M, \sigma, a)$ as follows: Γ is an n-dimensional M-vectorspace with basis $1, u, u^2, \ldots, u^{n-1}$, and the multiplication is given by $ux = \sigma x\, u$ for $x \in M$, and $u^n = a$. Prove that Γ *is* a K-algebra, and that it is a simple ring (i.e., has no non-trivial two-sided ideals) with center K. Γ is called a *cyclic algebra*. [Hint: Let θ be a primitive element for M/K. Then $\gamma \mapsto \gamma\theta$ is an M-linear map on Γ (with M acting from the left) and the basis elements are eigenvectors with distinct eigenvalues. This remains true in a factor ring.]

(2) Note that quaternion algebras are cyclic.

(3) Use Artin-Wedderburn's Theorem about the structure of simple Artinian rings (see e.g. [Ja2, 4.4 p. 203]) to prove: If $n = p$ is a prime, then a cyclic algebra (M, σ, a) is either a skew field or isomorphic to $\mathrm{Mat}_p(K)$.

(4) Prove that (M, σ, a) is isomorphic to $\mathrm{Mat}_n(K)$ if and only if a is a norm in M/K.

(5) Let $\theta = 2\cos\frac{2\pi}{7}$. Then θ is algebraic over $\mathbb{Q}$ of degree 3, with minimal polynomial X^3+X^2-2X-1, and $\mathbb{Q}(\theta)/\mathbb{Q}$ is cyclic of degree 3 with $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ generated by $\sigma\colon \theta \mapsto \theta^2-2$. Prove that 2 is not a norm in $\mathbb{Q}(\theta)/\mathbb{Q}$, and conclude that $(\mathbb{Q}(\theta), \sigma, 2)$ is a skew field of dimension 9 over $\mathbb{Q}$. (This is the standard example of a skew field other than $\mathbb{H}$.)

EXERCISE 6.4. Let K be a Hilbertian field of characteristic $\neq 2$, and let $a \in K^* \setminus (K^*)^2$. Prove that $K(\sqrt{a})$ can be embedded into a quaternion extension of K if and only if a is a sum of three squares in K.

EXERCISE 6.5. Let K be a field of characteristic $\neq 2$. Find the quaternion extensions of $K(t)$ containing $K(t)(\sqrt{t^2+1}, \sqrt{t^2+2})$ and prove that they are regular.

EXERCISE 6.6. Assume that the field K has a quaternion extension. Prove that it has a D_4- and a C_4-extension as well.

EXERCISE 6.7. Prove or disprove the following: There exists a D_8-polynomial $f(X) = X^8+a_7X^7+\cdots+a_1X+a_0 \in \mathbb{Z}[X]$, such that $\bar{f}(X) \in \mathbb{F}_2[X]$ is irreducible.

EXERCISE 6.8. (1) Let L/K be a C_4-extension in characteristic $\neq 2$, and let $b \in K^* \setminus (L^*)^2$. Prove that the $C_4 \times C_2$-extension $L(\sqrt{b})/K$ can be embedded in an M_{16}-extension cyclic over $K(\sqrt{b})$ if and only if $-b^2$ is a norm in L/K. Then find the M_{16}-extensions in question. [Hint: If $-b^2 = \mathrm{N}_{L/K}(z)$ then z^2/b has norm 1. Use Hilbert 90 to find an ω.]

(2) Assume $L = K(\sqrt{a+\sqrt{a}\,})$ where $a = 1+b^2$. Find an M_{16}-extension containing $L(\sqrt{b})/K$.

EXERCISE 6.9. List all the groups of order 16. [Hint: There are fourteen.] For which of them can the question of the existence of generic polynomials over $\mathbb{Q}$ be answered with the results at your disposal? [Hint: All but two. But see [Le8, Thm. 6] for M_{16}.]

EXERCISE 6.10. Let p be an odd prime, and consider the other non-abelian group $C_{p^2} \rtimes C_p$ of order p^3. Demonstrate the existence of a generic polynomial for this group over any field of characteristic $\neq p$, and give an explicit example of a $C_9 \rtimes C_3$-polynomial over $\mathbb{Q}$. [Hint: With slight modifications, it can be done as for the Heisenberg group.]

CHAPTER 7

Solvable Groups II: Frobenius Groups

We continue our treatment of solvable groups as Galois groups by considering dihedral groups and Frobenius groups. In a more general setting, we consider wreath products and semi-direct products. In particular, we discuss a theorem of Saltman — already referred to in Chapter 5 — on the existence of generic polynomials for wreath products and semi-direct products under certain conditions. Applying Saltman's results to the case of Frobenius groups $F_{p\ell}$, we give a necessary and sufficient condition for the existence of generic polynomials over $\mathbb{Q}$.

7.1. Preliminaries

DEFINITION 7.1.1. Let p be a prime. A *Frobenius group* of degree p is a transitive subgroup G of the symmetric group S_p such that

$$G_i = \{\sigma \in G \mid \sigma i = i\} \neq 1$$

for $i = 1, \ldots, p$, but $G_i \cap G_j = 1$ for $i \neq j$.

The precise structure of a Frobenius group of prime degree is given in the following result by Galois:

LEMMA 7.1.2. [Hu, II.§3 Satz 3.6] *Let G be a transitive subgroup of S_p of order $> p$, where $p \geq 5$. Then the following conditions are all equivalent:*

(a) *G has a unique p-Sylow subgroup.*
(b) *G is solvable.*
(c) *G can be identified with a subgroup of the group of affine transformations on $\mathbb{F}_p$.*
(d) *G is a Frobenius group of degree p.*

REMARKS. (1) An affine transformation $\mathbb{F}_p \to \mathbb{F}_p$ is a map of the form $x \mapsto ax + b$, where $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. Thus, it can be considered as the semi-direct product $\mathbb{F}_p \rtimes \mathbb{F}_p^*$. It follows that a Frobenius group of degree p is a semi-direct product $\mathbb{F}_p \rtimes H$, where H is a non-trivial subgroup of $\mathbb{F}_p^* \simeq C_{p-1}$. If H has order ℓ, we denote this Frobenius group by $F_{p\ell}$.

(2) Frobenius groups are solvable, and hence realisable as Galois groups over $\mathbb{Q}$ by Shafarevich's Theorem. Alternatively, they can be obtained by Ikeda's Theorem (section 5.4 in Chapter 5).

(3) As a permutation group of degree p, $F_{p\ell}$ is 1- but not 2-transitive for $\ell < p - 1$. (BURNSIDE, [Pa, Thm. 7.3]) Conversely, if G is a 1- but not 2-transitive subgroup of S_p, then $G = F_{p\ell}$ for $\ell < p-1$. (ZASSENHAUS, [Za] or [Pa,

Thm. 20.3]) On the other hand, $F_{p(p-1)}$ is sharply 2-transitive, and furthermore the only sharply 2-transitive subgroup of S_p.

(4) Let $f(X) \in K[X]$ be irreducible of degree p, and let M be the splitting field of $f(X)$ over K. An immediate consequence of Lemma 7.1.2 is then that $\mathrm{Gal}(f/K)$ is solvable, if and only if M is generated over K by (any) two roots α and β of $f(X)$. An obviuos question is then: Can we describe the other roots in terms of α and β?

(5) In analogy with the Weber sextic resolvent of Chapter 2, it is possible to define a resolvent for polynomials of degree p such that the polynomial has solvable Galois group if and only if the resolvent has a rational root. Unfortunately, this resolvent will have degree $(p-2)!$, making it unsuited for actual computations.

We notice in particular that the dihedral group D_p is a Frobenius group of degree p. So, although dihedral groups are not in general Frobenius in the sense of the above definition, we will nevertheless treat them here.[1]

Characterising dihedral polynomials. Now we shall give characterization theorems for monic irreducible integral polynomials of odd degree $n \geq 3$ with dihedral (and generalized dihedral) Galois groups over a field K of characteristic 0.

First we consider dihedral groups D_p of prime degree p. Let p be a prime ≥ 3. Embedding D_p into S_p, we may represent the two generators σ and τ by the following cycles:

$$\sigma = (1\,2\,3\ldots p) \text{ and } \tau = (1)(2\,p)(3\,p-1)\ldots(\tfrac{1}{2}(p+1)\,\tfrac{1}{2}(p+3)).$$

The sign of τ is $(-1)^{(p-1)/2}$, and so $D_p \subseteq A_p$ if and only if $p \equiv 1 \pmod 4$.

Let $f(X)$ be a monic polynomial over K of degree p. We give a characterization for $f(X)$ to have $\mathrm{Gal}(f/K) \simeq D_p$. Before stating our theorem, we recall the linear resolvent polynomial $R(x_1 + x_2, f)(X)$ introduced in Chapter 2.

Let $f(X) \in K[X]$ be an irreducible polynomial of degree $p \geq 3$ and let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be p roots of $f(X)$ (over K). Then the $p_2 = \binom{p}{2}$ elements $\alpha_i + \alpha_j, 1 \leq i < j \leq p$ are all distinct. Let

$$P_{p_2}(X) = R(x_1 + x_2, f)(X) = \prod_{1 \leq i < j \leq p} (X - (\alpha_i + \alpha_j)) \in K[X].$$

THEOREM 7.1.3. *Let $f(X) \in K[X]$ be a monic irreducible polynomial of odd prime degree p. Assume that $\mathrm{Gal}(f/K) \neq C_p$. Then $\mathrm{Gal}(f/K) \simeq D_p$, if and only if the resolvent polynomial $P_{p_2}(X)$ decomposes into the product of $(p-1)/2$ distinct irreducible polynomials of degree p over K.*

REMARK. Let q be a prime such that $p = 2q + 1$ is also a prime, e.g., $p = 5, 7, 11, 23, \ldots$. Let $\Phi_p(X)$ be the p^{th} cyclotomic polynomial. The Galois group

[1] The definition of Frobenius groups given in [Hu, V.§8] *does* include dihedral groups, however. We note that, by [Sn], all Frobenius groups, as defined in Huppert, are Galois groups over $\mathbb{Q}$.

$\mathrm{Gal}(\Phi_p/\mathbb{Q}) \simeq \mathbb{F}_p^*$. Dividing $\Phi_p(X)$ by $X^{(p-1)/2} = X^q$, we have

$$X^p + X^{p-1} + \cdots + X + 1 + \frac{1}{X} + \frac{1}{X^2} + \cdots + \frac{1}{X^p} = 0.$$

Put $Y = X + 1/X$. Then this equation can be rewritten as

$$Y^q + a_{q-1}Y^{q-1} + \cdots + a_1 Y + 1 = 0.$$

The Galois group of this polynomial over $\mathbb{Q}$ is C_q.

PROOF OF THEOREM 7.1.3. The dihedral group D_p acts on the set $\{\alpha_i+\alpha_j \mid i \le i < j \le p\}$ of roots of $P_{p_2}(X)$ with $(p-1)/2$ orbits, all of length p, and with multiplicity 2 in the sense that the stabilizer of $\alpha_i+\alpha_j$ is of order 2 for any pair.

In terms of factorization of the polynomial $P_{p_2}(X)$, this says that $P_{p_2}(X)$ factors into a product of $(p-1)/2$ distinct irreducible polynomials of degree p over K.

The above property of D_p can be explained geometrically: We identify the roots of $f(X)$ with the vertices of the regular p-gon, and the sums $\alpha_i + \alpha_j$ with the corresponding edges and diagonals. There are altogether $p(p-1)/2$ such lines. The group D_p is the symmetry group of the regular p-gon, and so it acts on the set of $p(p-1)/2$ lines intransitively with $(p-1)/2$ orbits of length p and multiplicity 2. C_p also acts intransitively on the lines with $(p-1)/2$ orbits of length p, but with multiplicity 1.

Now for sufficiency: $\mathrm{Gal}(f/K)$ is a transitive subgroup of S_p, and it is an easy consequence of our condition that it has order at most $2p$: Considering the roots of $f(X)$ as the corners of a regular p-gon, the roots of the resolvent corresponds to sides and diagonals. Since the factors have degree p, we see in particular that the Galois group permutes the sides, i.e., preserves 'neighbours' among the roots. This immediately limits the Galois group to consist only of rotations and reflections. Since $\mathrm{Gal}(f/K) \neq C_p$, we have the result. □

EXAMPLES. We produce polynomials over $\mathbb{Q}$ having only real roots with Galois group D_p: Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial of degree p and let M denote its splitting field over $\mathbb{Q}$. By Galois' Lemma, $\mathrm{Gal}(f/\mathbb{Q})$ is solvable if and only if M is generated by two roots of $f(X)$. Thus, if $f(X)$ has two real roots and $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_p$, then it has p real roots.

(1) Let $f(X) = X^5+X^4-5X^3-4X^2+3X+1$ (resp. $X^5+X^4-6X^3-5X^2+3X+1$). Then $f(X)$ has five real roots and $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_5$. The quadratic subfield contained in M is $\mathbb{Q}(\sqrt{401})$ (resp. $\mathbb{Q}(\sqrt{817})$) with class number 5. Also,

$$\begin{aligned} P_{10}(X) &= X^{10} + 4X^9 - 9X^8 - 45X^7 + 6X^6 + \\ &\qquad 129X^5 + 48X^4 - 93X^3 - 31X^2 + 14X + 3 \\ &= (X^5 + 2X^4 - 6X^3 - 15X^2 - 8X - 1) \\ &\qquad \times (X^5 + 2X^4 - 7X^3 - 4X^2 + 10X - 3), \end{aligned}$$

resp.

$$\begin{aligned} P_{10}(X) &= X^{10} + 4X^9 - 12X^8 - 55X^7 + 26X^6 + \\ &\qquad 207X^5 + 45X^4 - 208X^3 - 71X^2 + 27X + 5 \\ &= (X^5 + 2X^4 - 9X^3 - 6X^2 + 18X - 5) \\ &\qquad \times (X^5 + 2X^4 - 7X^3 - 17X^2 - 9X - 1) \end{aligned}$$

(2) Let $f(X) = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1$. Then $f(X)$ has exactly one real root and $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_7$. The polynomial $P_{21}(X)$ factors as follows:

$$\begin{aligned} P_{21}(X) &= (X^7 - 2X^6 + 4X^4 + 12X^2 - 27X + 13) \\ &\qquad \times (X^7 - 2X^6 - 2X^5 + 8X^4 - 8X^2 + 5X - 1) \\ &\qquad \times (X^7 - 2X^6 - 4X^4 - 2X^2 + X - 1). \end{aligned}$$

A generalization (over $\mathbb{Q}$) of Theorem 7.1.3 is due to Williamson [Wil]:

THEOREM 7.1.4. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible odd degree polynomial over $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_n$ be its roots in the splitting field M over $\mathbb{Q}$.*
(A) *Suppose that* $\mathrm{Gal}(f/\mathbb{Q})$ *is dihedral of order $2n$, and let K denote the quadratic subfield of M. Then the following assertions hold:*

(a) *$f(X)$ is irreducible over K (i.e.,* $\mathrm{Gal}(M/K)$ *permutes the roots α_i transitively and the splitting field of $f(X)$ has degree n over K).*
(b) *$K = \mathbb{Q}(\sqrt{-d})$, where d is the constant coefficient of any monic irreducible factor $p(X)$ of the resolvent $R(x_1 - x_2, f)(X)$. Further, $p(X)$ is an even polynomial, i.e., a polynomial in X^2.*
(c) *If $p \nmid d(f)$ remains inert in K, then $p\mathcal{O}_K$ splits completely in M: $p\mathcal{O}_M = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. The decomposition fields for the primes $\mathfrak{p}_i$ in $M/\mathbb{Q}$ are distinct. The polynomial $f(X)$ factors into a linear polynomial times a product of $(n-1)/2$ irreducible quadratic polynomials modulo p.*

(B) *Conversely, suppose that*

(i) *The monic irreducible factors of $R(x_1 - x_2, f)(X)$ are even polynomials and the field $K = \mathbb{Q}(\sqrt{-d})$, where $-d$ is the constant coefficient of some monic irreducible factor of $R(x_1 - x_2, f)(X)$, is quadratic over $\mathbb{Q}$ and is independent of the choice of irreducible factor,*
(ii) *The polynomial $f(X)$ is irreducible over K and the splitting field of $f(X)$ over K has degree n, and*
(iii) *for some prime $p \nmid d(f)$ which remains inert in K, $f(X)$ factors into a linear polynomial times a product of $(n-1)/2$ irreducible quadratic polynomials modulo p.*

Then $\mathrm{Gal}(f/\mathbb{Q})$ *is a generalized dihedral group of order $2n$ and K is the unique quadratic subfield of M.*

If condition (II)(i) *fails, then* $\mathrm{Gal}(f/\mathbb{Q})$ *cannot be dihedral of order $2n$. If condition* (II)(i) *holds, but* (II)(ii) *or* (II)(iii) *fails for any prime $p \nmid d(f)$ which remains inert in K, then* $\mathrm{Gal}(f/\mathbb{Q})$ *likewise cannot be dihedral of order $2n$.*

EXAMPLE. Let $\zeta = \exp(2\pi i/3)$, and let $L/\mathbb{Q} = \mathbb{Q}(\zeta, \sqrt[3]{a})/\mathbb{Q}$, $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^3$. Clearly, $L/\mathbb{Q}$ is a D_3-extension, and we can let $\sigma, \tau \in D_3 = \mathrm{Gal}(L/\mathbb{Q})$ be given by

$$\begin{aligned} \sigma\colon &\quad \sqrt[3]{a} \mapsto \zeta\sqrt[3]{a}, \quad \zeta \mapsto \zeta, \\ \tau\colon &\quad \sqrt[3]{a} \mapsto \sqrt[3]{a}, \quad \zeta \mapsto \zeta^2. \end{aligned}$$

If $L/\mathbb{Q}$ can be embedded in a D_9-extension, $L/\mathbb{Q}(\zeta)$ can be embedded in a C_9-extension. Conversely, if $L(\sqrt[3]{\beta})/\mathbb{Q}(\zeta)$ is a C_9-extension, it is easily seen that $L(\sqrt[3]{\beta\,\tau\beta})/\mathbb{Q}$ is a D_9-extension.

Classically, a C_3-extension $L/K = K(\sqrt[3]{a})/K$ over a field K containing a primitive third root of unity ζ can be embedded in a C_9-extension, if and only if ζ is a norm in L/K. And if $\zeta = \mathrm{N}_{L/K}(x)$, we can let $\beta = \sigma x\,\sigma^2 x^2\sqrt[3]{a}$ to get a C_9-extension $L(\sqrt[3]{\beta})/K$, cf. [Ma].

Thus, $L/\mathbb{Q}$ can be embedded in a D_9-extension, if and only if ζ is a norm in $L/\mathbb{Q}(\zeta)$, and in that case we can find such a D_9-extension explicitly. More to the point, we can find a polynomial of degree 9 with this D_9-extension as splitting field, namely $f(X^3)$, where $f(X)$ is the minimal polynomial for $\beta\,\tau\beta$ over $\mathbb{Q}$. ($\beta\,\tau\beta$ has degree 3 over $\mathbb{Q}$, since it is τ-invariant.)

For example: Let $a = 3$ and $L = \mathbb{Q}(\zeta, \sqrt[3]{3})$. Then we can let $x = 1 + \sqrt[3]{3} + (1-\zeta)/\sqrt[3]{3}$ and get that the polynomial

$$g(X) = X^9 - 27X^6 + 675X^3 - 9 \in \mathbb{Q}[X]$$

has Galois group D_9, and that the splitting field contains L.

7.2. Wreath Products and Semi-Direct Products

Frobenius groups are semi-direct products, and can thus in some cases be described generically by the same method employed for dihedral groups in section 5.5 of Chapter 5. As mentioned there, this method is due to Saltman, in [Sa1, §3].

The main result is

THEOREM 7.2.1. (SALTMAN) *Let K be an infinite field, and let N and G be finite groups. If there exist generic extensions for both N and G over K, then there exists a generic $N \wr G$-extension over K as well.*

This of course immediately implies the analogous result for generic *polynomials*: If we have generic N- and G-polynomials over the infinite field K, there exists a generic $N \wr G$-polynomial as well.

PROOF. Let S/R and U/T be the generic G- and N-extensions, respectively. Then $R = K[\mathbf{s}, 1/s] = K[s_1, \ldots, s_m, 1/s]$ and $T = K[\mathbf{t}, 1/t] = K[t_1, \ldots, t_n, 1/t]$.

By the results of Chapter 5, we are allowed to assume that S/R has a normal basis $(\sigma\theta)_{\sigma\in G}$, and that the determinant $|\sigma\tau\theta|_{\sigma,\tau\in G}$ is a unit in S.

Now, we adjoin to S and R a number of additional indeterminates $\mathbf{T} = (t_{\sigma,i})_{\sigma\in G,\ 1\le i\le n}$. Over S, we immediately replace these with $\mathbf{U} = (u_{\sigma,i})_{\sigma,i}$,

where

$$u_{\sigma,i} = \sum_{\rho \in G} \sigma\rho\theta\, t_{\rho,i}.$$

If we let G act trivially on $\mathbf{T}$, we then get $\sigma u_{\tau,i} = u_{\sigma\tau,i}$ and $S[\mathbf{U}] = S[\mathbf{T}]$. The element

$$u = \prod_{\sigma \in G} t(u_{\sigma,1} \cdots u_{\sigma,n})$$

is non-zero in $K[\mathbf{T}]$, and the extension $S[\mathbf{U}, 1/u]/R[\mathbf{U}, 1/u]$ is clearly generic for G over K.

For $\sigma \in G$, we have a homomorphism $\varphi_\sigma \colon T \to S[\mathbf{U}, 1/u]$, given by

$$\varphi_\sigma \colon t_i \mapsto u_{\sigma,i},$$

and get a corresponding tensor product

$$U_\sigma = U \otimes_{\varphi_\sigma} S[\mathbf{U}, 1/u].$$

Obviously, $U_\sigma/S[\mathbf{U}, 1/u]$ is an N-extension. Consequently,

$$W/S[\mathbf{U}, 1/u] = \big(\bigotimes_{\sigma \in G} U_\sigma\big)/S[\mathbf{U}, 1/u]$$

is an N^d-extension, when the tensor product is taken over $S[\mathbf{U}, 1/u]$, and $d = |G|$.

Moreover, $W/R[\mathbf{T}, 1/u]$ is a generic $N \wr G$-extension:

First of all, $W/R[\mathbf{T}, 1/u]$ *is* an $N \wr G$-extension, since $\sigma \in G$ maps the ρ^{th} set of u's to the $\sigma\rho^{\text{th}}$, and this action clearly extends to the tensor product W as a corresponding permutation of the tensor factors.

Second, it is generic: Let M/K be an $N \wr G$-extension,[2] and let L/K be the G-subextension.

Some specialisation $\varphi\colon R \to K$ gives us L as $S \otimes_\varphi K$. But this same specialisation, extended to $R[\mathbf{T}, 1/u]$, produces $W \otimes_\varphi K$, which is simply the tensor product of d copies of a generic N-extension over L, naturally conjugate with respect to G. Specialise one of them to get one of the N-subextensions of M/L, and extend this specialisation by conjugation. This specialisation of $\mathbf{U}$ over L becomes a specialisation of $\mathbf{T}$ over K, and we have established genericity. □

From Exercise 5.10 and Proposition 5.1.7 in Chapter 5, we then get

Corollary 7.2.2. (Saltman) *Let K be an infinite field, and let A and G be finite groups with A Abelian. Assume that there exist generic A- and G-polynomials over K. Also assume that G acts on A by automorphisms, and that the group orders $|A|$ and $|G|$ have greatest common divisor 1. Then there exists a generic $A \rtimes G$-polynomial over K.*

Conversely (and also from Proposition 5.1.7 in Chapter 5), we have that a generic $A \rtimes G$-extension implies the existence of a generic G-extension.

In the case of Frobenius groups over $\mathbb{Q}$, this gives us

[2]The precise structure of K has played no role in the construction of W, so we need not bother with the general 'ground field containing K' rule.

THEOREM 7.2.3. *Let p be an odd prime, and let $\ell \mid p-1$. Then there exists a generic $F_{p\ell}$-polynomial over $\mathbb{Q}$, if and only if $8 \nmid \ell$.*

Of course, any actual *construction* of these polynomials, following the algorithm implicit in the proof of Theorem 7.2.1, is hopelessly involved. We invite the reader to consider the structure of a generic F_{21}-extension.

7.3. Frobenius Groups

Now, following [BJ&Y], we will look at $F_{p\ell}$-polynomials over a field K of characteristic 0 with the help of resolvent polynomials as defined in Chapter 2.

The resolvent polynomials we will use are

$$P_{p_2}(X) = R(x_1 + x_2, f), \quad p_2 = \binom{p}{2} = \frac{p(p-1)}{2},$$

and

$$P_{p_3}(X) = R(x_1 + x_2 + x_3, f), \quad p_3 = \binom{p}{3} = \frac{p(p-1)(p-2)}{6},$$

where $f(X) \in K[X]$ is an irreducible polynomial of prime degree $p \geq 5$.

We note that $F_{p\ell}$ is contained in A_p if and only if $(p-1)/\ell$ is even, if and only if $F_{p\ell} \subseteq F_{p(p-1)/2}$.

LEMMA 7.3.1. *Let p be a prime > 5, and let G be a 2- but not 3-transitive subgroup of S_p distinct from $F_{p(p-1)}$. If $p = 11$, then $G = \mathrm{PSL}(2, 11)$. Otherwise, $p = (q^n - 1)/(q-1)$ for some prime power q and some prime n, and $\mathrm{PSL}(n, q) \subseteq G \subseteq \mathrm{P\Gamma L}(n, q)$. In any case, $G \subseteq A_p$.*

Here, $\mathrm{P\Gamma L}(n, q)$ is the projective group of *semi-linear* maps on $\mathbb{F}_q^n$, i.e., group automorphisms $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $\varphi(a\mathbf{v}) = \varepsilon(a)\varphi(\mathbf{v})$ for some automorphism ε on $\mathbb{F}_q$. It clearly acts on the $(n-1)$-dimensional projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$ with p elements.

PROOF. It is proved by Feit in [Fe] that the first part follows from the classification of finite simple groups. We will leave it at that.

As for the second part: The projective special linear groups are simple, and thus contained in A_p, since otherwise $G \cap A_p$ would be a normal subgroup of index 2. Next, $\mathrm{P\Gamma L}(n, q)$ is generated by $\mathrm{PSL}(n, q)$ and the coordinate-wise application of the Frobenius automorphism on $\mathbb{F}_q$. This latter map is easily seen to be even, unless $p = 5$. □

THEOREM 7.3.2. *Let $f(X) \in K[X]$ be a monic irreducible polynomial of prime degree $p \geq 5$.*

(a) *Let $\ell \mid p-1$, and assume ℓ odd (resp. even). Then a necessary condition for $\mathrm{Gal}(f/K) \simeq F_{p\ell}$ is that $P_{p_2}(X)$ factors into a product of $(p-1)/2\ell$ (resp. $(p-1)/\ell$) distinct irreducible polynomials of degree $p\ell$ (resp. $p\ell/2$) over K.*

(b) *Conversely, suppose that $P_{p_2}(X)$ has a non-trivial factor. Then $G \simeq F_{p\ell}$ for an $\ell \mid p-1$, and the irreducible factors of $P_{p_2}(X)$ all have degree $p\ell$ (if ℓ is odd) or $p\ell/2$ (if ℓ is even).*

PROOF. (a) Assume $\mathrm{Gal}(f/K) \simeq F_{p\ell}$. Then the orbit of an unordered pair $\{i,j\}$, $i \neq j$, in $\mathbb{F}_p$ under $\mathrm{Gal}(f/K)$-action has order $p\ell$ (resp. $p\ell/2$), since the transformation $x \mapsto -x$ is not (resp. is) in $F_{p\ell}$.

(b) If $P_{p_2}(X)$ has a non-trivial factor, then $\mathrm{Gal}(f/K)$ is solvable, and so $\simeq F_{p\ell}$ for some $\ell \mid p-1$. If ℓ is odd, the orbit of a root of $P_{p_2}(X)$ has order $p\ell$, otherwise it has order $p\ell/2$. □

Clearly, this theorem does not allow us to distinguish between the groups $F_{p\ell}$ and $F_{p2\ell}$, ℓ odd. Also, if $P_{p_2}(X)$ is irreducible, the Galois group may be $F_{p(p-1)}$, $F_{p(p-1)/2}$ or insolvable.

PROPOSITION 7.3.3. *Let p be a prime > 5, and let $f(x) \in K[x]$ be an irreducible polynomial of degree p. Assume that $d(f) \notin (K^*)^2$, and that $P_{p_2}(X)$ is irreducible. Then* $\mathrm{Gal}(f/K) \simeq F_{p(p-1)}$ *if and only if $P_{p_3}(X)$ is reducible. In this case, $P_{p_3}(X)$ factors as follows:*

(a) *If $p \equiv 1 \pmod 3$, then $P_{p_3}(x)$ is a product of a monic irreducible polynomial of degree $p(p-1)/2$, a monic irreducible polynomial of degree $p(p-1)/3$, and $(p-7)/6$ distinct monic irreducible polynomials of degree $p(p-1)$ over K.*
(b) *If $p \equiv 2 \pmod 3$, then $P_{p_3}(x)$ is a product of a monic irreducible polynomial of degree $p(p-1)/2$ and $(p-5)/6$ distinct monic irreducible polynomials of degree $p(p-1)$ over K.*

PROOF. 'Only if' is clear. 'If': $\mathrm{Gal}(f/K)$ is 2- but not 3-transitive. Hence, it is either $F_{p(p-1)}$ or a projective group. However, the projective groups are contained in A_p.

As for the factorisation of $P_{p_3}(X)$: Every orbit of three-element sets $\{i,j,k\}$ in $\mathbb{F}_p$ under $F_{p(p-1)}$-action contains an element $\{0,1,a\}$, $a \neq 0,1$. The orbit of $\{0,1,-1\}$ has order $p(p-1)/2$ elements. The orbit of $\{0,1,(1+\sqrt{-3})/2\}$ (if there is one) has $p(p-1)/3$ elements. All others have $p(p-1)$ elements. □

PROPOSITION 7.3.4. *Let p be a prime > 5, and let $f(X) \in K[X]$ be irreducible of degree p. Then* $\mathrm{Gal}(f/K) \simeq F_{p(p-1)/2}$ *if and only if $d(f) \in (K^*)^2$ and $P_{p_3}(X)$ is reducible over K with the maximal degree of an irreducible factor being $p(p-1)/2$. (Alternatively, if and only if $P_{p_3}(X)$ has at least three irreducible factors.) In that case, we have the following:*

(a) *If $p \equiv 1 \pmod{12}$, then $P_{p_3}(x)$ is a product of two distinct monic irreducible polynomials of degree $p(p-1)/4$, two distinct monic irreducible polynomials of degree $p(p-1)/6$ and $(p-7)/3$ distinct monic irreducible polynomials of degree $p(p-1)/2$ over K.*
(b) *If $p \equiv 5 \pmod{12}$, then $P_{p_3}(x)$ is a product of two distinct monic irreducible polynomials of degree $p(p-1)/4$ and $(p-5)/3$ distinct monic irreducible polynomials of degree $p(p-1)/2$ over K.*
(c) *If $p \equiv 7 \pmod{12}$, then $P_{p_3}(x)$ is a product of two distinct monic irreducible polynomials of degree $p(p-1)/6$ and $(p-4)/3$ distinct monic irreducible polynomials of degree $p(p-1)/2$ over K.*

(d) *If* $p \equiv 11 \pmod{12}$, *then* $P_{p_3}(x)$ *is a product of* $(p-2)/3$ *distinct monic irreducible polynomials of degree* $p(p-1)/2$ *over* K.

PROOF. 'Only if' is clear from (a)–(d), proved below. 'If': Assume $\mathrm{Gal}(f/K)$ insolvable. Since it is not 3-transitive, we have either $\mathrm{Gal}(f/K) = \mathrm{PSL}(2,11)$ (and $p = 11$), in which case Theorem 2.7.2(b) gives the result, or $\mathrm{Gal}(f/K) \supseteq \mathrm{PSL}(n,q)$ for suitable n and q with $p = (q^n-1)/(q-1)$. If $n \geq 3$, there are two orbits of $\mathrm{PSL}(n,q)$ on the roots of $P_{p_3}(X)$, corresponding to lines and triangles in $\mathbb{P}^{n-1}(\mathbb{F}_q)$, and one of these orbits must have $> p(p-1)/2$ elements, except when $p = 7$, $q = 2$, $n = 3$, where Theorem 2.5.3(b) applies. If $n = 2$, there is only one orbit.

(a) and (b): We look at the action of $F_{p(p-1)/2}$ on three-element sets in $\mathbb{F}_p$. Considering sets of the form $\{0, 1, a\}$, there is one orbit of length $p(p-1)/4$ (containing $\{0, 1, -1\}$) and (in some cases) one of length $p(p-1)/6$ (containing $\{0, 1, (1+\sqrt{-3})/2\}$). The rest all have length $p(p-1)/2$.

Now, $F_{p(p-1)}$ permutes the $F_{p(p-1)/2}$-orbits, and since there are no $F_{p(p-1)}$-orbits of length $p(p-1)/4$ or $p(p-1)/6$, we see that there must be twice as many of each as counted above. All other orbits must be of length $p(p-1)/2$.

(c) and (d): Each orbit of three-element sets in $\mathbb{F}_p$ under $F_{p(p-1)/2}$-action contains a set $\{0, 1, a\}$. The orbits of $\{0, 1, (1+\sqrt{-3})/2\}$ and $\{0, 1, (1+\sqrt{-3})/2\}$ (if they exist) each have length $p(p-1)/6$. All other orbits have length $p(p-1)/2$. □

THEOREM 7.3.5. *Let* p *be a prime* > 5, *and let* $f(X) \in K[X]$ *be a monic irreducible polynomial of degree* p. *Then* $\mathrm{Gal}(f/K)$ *is solvable if and only if* $d(f)$ *is a square* (*resp. not a square*) *and either* $P_{p_2}(X)$ *is reducible in* $K[X]$ *or* $P_{p_2}(X)$ *remains irreducible over* K *but* $P_{p_3}(X)$ *factors into a product of at least three* (*resp. two*) *distinct irreducible polynomials over* K.

PROOF. If $P_{p_2}(X)$ is reducible, then G must be solvable. Thus, it remains only to prove the following two statements: (1) If G is solvable, $d(f)$ is a square and $P_{p_2}(X)$ is irreducible, then $P_{p_3}(X)$ has at least three irreducible factors. (2) If $P_{p_2}(X)$ is irreducible and $P_{p_3}(X)$ is reducible (with at least three factors for $d(f) \in (K^*)^2$), then G is solvable.

(1) From the assumption, we get that $G = F_{p(p-1)/2}$ and that $p \equiv 3 \pmod 4$. For $p > 8$, the number of roots of P_{p_3} divided by the order of G is > 2, so there is at least three orbits. For $p = 7$, we look at F_{21}'s action on sets of three elements in $\mathbb{F}_7$: The set $\{0, 1, 3\}$ is mapped to itself by $x \mapsto 2x+1$, which is in F_{21}. Thus, there is an orbit with seven elements, and so at least three orbits.

(2) From the (proofs of the) previous theorems, we see that $P_{p_3}(X)$ is irreducible unless $\mathrm{Gal}(f/K)$ is either solvable, equal to $\mathrm{PSL}(2,11)$, or contained between $\mathrm{PSL}(n,q)$ and $\mathrm{P\Gamma L}(n,q)$ for suitable n and q. In the latter two cases, we have square discriminant, but only two factors. □

And immediate consequence of this, and hence ultimately of the classification of finite simple groups, is

COROLLARY 7.3.6. *Let p be a prime ≥ 13, and let $f(X) \in K[X]$ be monic and irreducible of degree p. Then* $\mathrm{Gal}(f/K)$ *is solvable if and only if $P_{p_3}(X)$ is reducible with at least three irrreducible factors.*

Now we shall construct $F_{p\ell}$-extensions of $\mathbb{Q}$:

Let p be an odd prime, and let e be a primitive root modulo p, i.e., $\mathbb{F}_p^* = \langle \bar{e} \rangle$. Also, let $\zeta = e^{2\pi i/p}$. Then $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is generated by κ, where $\kappa\zeta = \zeta^e$.

For $\ell \mid p-1$, we consider the C_ℓ-subextension $L/\mathbb{Q}$ of $\mathbb{Q}(\mu_p)/\mathbb{Q}$. By Ikeda's Theorem (section 5.4 of Chapter 5), $L/\mathbb{Q}$ can be embedded in an $F_{p\ell}$-extension $M/\mathbb{Q}$.

Clearly, $\mathrm{Gal}(M/\mathbb{Q}) \simeq C_p \rtimes C_{p-1}$, where $\kappa \in C_{p-1}$ acts on $\sigma \in C_p$ by

$$\kappa\sigma\kappa^{-1} = \sigma^f \quad \text{for} \quad f \equiv e^{(p-1)/\ell} \pmod{p}$$

(or any other element f of order ℓ modulo p).

$M(\mu_p) = \mathbb{Q}(\mu_p, \sqrt[p]{\omega})$ for some $\omega \in \mathbb{Q}(\mu_p)^* \setminus (\mathbb{Q}(\mu_p)^*)^p$ with $\sigma(\sqrt[p]{\omega}) = \zeta \sqrt[p]{\omega}$. It is then clear that

$$\kappa(\sqrt[p]{\omega}) = x(\sqrt[p]{\omega})^g$$

for an $x \in \mathbb{Q}(\mu_p)^*$ and $g \equiv ef^{\ell-1} \pmod{p}$.

Conversely, if we have an element $\omega \in \mathbb{Q}(\mu_p)^* \setminus (\mathbb{Q}(\mu_p)^*)^p$ with $\kappa\omega/\omega^g \in (\mathbb{Q}(\mu_p)^*)^p$, we get a $C_p \rtimes C_{p-1}$-extension $\mathbb{Q}(\mu_p, \sqrt[p]{\omega})/\mathbb{Q}$.

EXAMPLE. Let $\ell = p-1$. Then we can let $f = e$ and $g = 1$ to get $\kappa(\sqrt[p]{\omega}) = x\sqrt[p]{\omega}$, from which it follows that $\mathrm{N}_{\mathbb{Q}(\mu_p)/\mathbb{Q}}(x) = 1$, and hence that we can let $\omega = a \in \mathbb{Q}^*$. The $F_{p(p-1)}$-extensions of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$ are thus $\mathbb{Q}(\mu_p, \sqrt[p]{a})/\mathbb{Q}$, $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^p$.

Now assume $\ell < p-1$. Replacing g by $g+p$ if necesssary, we obtain $p^2 \nmid g^{p-1} - 1$.

From $\kappa(\sqrt[p]{\omega}) = x(\sqrt[p]{\omega})^g$ we get

$$\sqrt[p]{\omega} = \kappa^{p-1}(\sqrt[p]{\omega}) = \kappa^{p-2}x\,\kappa^{p-3}x^g \cdots \kappa x^{g^{p-3}} x^{g^{p-2}} (\sqrt[p]{\omega})^{g^{p-1}},$$

i.e.,

$$\omega^{-(g^{p-1}-1)/p} = \kappa^{p-2}x\,\kappa^{p-3}x^g \cdots \kappa x^{g^{p-3}} x^{g^{p-2}}.$$

Since $p \nmid (g^{p-1}-1)/p$, we can replace ω to assume

$$\omega = \kappa^{p-2}y\,\kappa^{p-3}y^g \cdots \kappa y^{g^{p-3}} y^{g^{p-2}}$$

for an $y \in \mathbb{Q}(\mu_p)^*$, and

$$\kappa(\sqrt[p]{\omega}) = y^{-(g^{p-1}-1)/p}(\sqrt[p]{\omega})^g.$$

Replacing ω (again) by ω^2, ω^3 or ω^4 if necessary, we have $M = L(\alpha)$ for

$$\alpha = \sum_{i=0}^{(p-1)/\ell - 1} \kappa^{i\ell}(\sqrt[p]{\omega}),$$

thus getting a 'parametrisation' of the $F_{p\ell}$-extensions containing $L/\mathbb{Q}$.

DEFINITION 7.3.7. For $n \in \mathbb{N}$ we define the n^{th} *Chebyshev polynomial* as the polynomial $T_n(X) \in \mathbb{Z}[X]$ of degree n with

$$\cos t = T_n(\cos(t/n)), \quad t \in \mathbb{R}.$$

$T_n(X)$ is easily found using trigonometric identities.

THEOREM 7.3.8. *Let p be a prime $\equiv 3 \pmod 4$, and let $\mathbb{Q}(u,v)$ be the function field over $\mathbb{Q}$ with indeterminates u and v. Put*

$$f(u,v,X) = (u^2+pv^2)^{p/2}\, T_p\Big(\frac{2X}{\sqrt{u^2+pv^2}}\Big) - u(u^2+pv^2)^{(p-1)/2}.$$

Then the following assertions hold:

(a) *$f(u,v,X)$ is irreducible over $\mathbb{Q}(u,v)$.*
(b) *$\mathrm{Gal}(f/\mathbb{Q}(u,v)) \simeq F_{p(p-1)/2}$.*
(c) *For any pair $(u,v) \in \mathbb{Z}^2$ with $p \nmid uv$, (u,v,X) is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{p(p-1)/2}$.*

PROOF. To realize $F_{p(p-1)/2}$ with $p \equiv 3 \pmod 4$, we may take $f = -e$ so that $g = -1$. The problem is then to find an element $\omega \in \mathbb{Q}(\mu_p)^* \setminus (\mathbb{Q}(\mu_p)^*)^p$ such that $\omega\,\kappa\omega = x^p$ for some $x \in \mathbb{Q}(\mu_p)^*$. Now $\mathbb{Q}(\mu_p)$ contains the unique quadratic subfield $\mathbb{Q}(\sqrt{-p})$. Let

$$\omega = \Big(\frac{a^2+pb^2}{4}\Big)^{p/2}(\cos\theta + i\sin\theta)$$

with

$$\cos\theta = \frac{a}{\sqrt{a^2+pb^2}} \quad \text{and} \quad \sin\theta = \frac{b\sqrt{p}}{\sqrt{a^2+pb^2}}.$$

(And $x = (a^2+pb^2)/4$.) Then the real part of $\sqrt[p]{\omega}$ $(= \frac{1}{2}(\sqrt[p]{\omega} + \kappa(\sqrt[p]{\omega})))$ satisfies the equation

$$T_p\Big(\frac{2X}{\sqrt{a^2+pb^2}}\Big) - \frac{a}{\sqrt{a^2+pb^2}} = 0.$$

In fact, let $\alpha = \mathrm{Re}\,\sqrt[p]{\omega}$. Then $\alpha = ((a^2+pb^2)/4)^{1/2}\cos(\theta/p)$ and we have

$$\begin{aligned} T_p\Big(\frac{2}{\sqrt{a^2+pb^2}}\sqrt{\frac{a^2+pb^2}{4}}\cos(\theta/p)\Big) &= T_p\big(\cos(\theta/p)\big) \\ &= \cos\theta = \frac{a}{\sqrt{a^2+pb^2}}. \end{aligned}$$

The polynomial $f(X)$ is (up to a constant factor) the minimal polynomial of α and hence it is irreducible over $\mathbb{Q}$. Thus, $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{p(p-1)/2}$ by construction.

Now we may view a and b as parameters. This gives the assertions (a) and (b).

(c) It is enough to prove that ω is not a p^{th} power in $\mathbb{Q}(\mu_p)$, and in fact that it is not a p^{th} power in $\mathbb{Q}(\sqrt{-p})$. If it were, we would have

$$2^p(a^2+pb^2)^{(p-1)/2}(a+b\sqrt{-p}) = (c+d\sqrt{-p})^p$$

for $c, d \in \mathbb{Z}$ with $c \equiv d \pmod 2$. This, however, is a contradiction, since the coefficient to $\sqrt{-p}$ on the left is not divisible by p, while the one on the right is. □

REMARK. It is clear from the construction that $f(u, v, X)$ is neither generic nor parametric for $F_{p(p-1)/2}$-extensions over $\mathbb{Q}$, since we only get $F_{p(p-1)/2}$-extensions where the cyclic subextension of degree $(p-1)/2$ is the one obtained by adjoining $2\cos(2\pi/p)$.

EXAMPLES. (1) Let $p = 7$. Then a family of polynomials with Galois group F_{21} is given by

$$f(u, v, X) = 64X^7 - 112(u^2 + 7v^2)X^5 + 56(u^2 + 7v^2)^2X^3 - 7(u^2 + 7v^2)^3X - u(u^2 + 7v^2)^3.$$

(2) Let

$$f(X) = X^7 + 14X^6 - 56X^4 + 56X^2 - 16.$$

Then $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{21}$.

(3) Let

$$f(X) = X^{11} - 33X^9 + 396X^7 - 2079X^5 + 4455X^3 - 2673X - 243.$$

Then $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{55}$.

Exercises

EXERCISE 7.1. Let K be an infinite field, and let S/R be a generic extension for the finite group G over K. Assume that G maps to a transitive subgroup of the symmetric group S_n for some n, and let

$$H = \{\sigma \in G \mid \sigma(1) = 1\}.$$

Also, let $\sigma_1, \ldots, \sigma_n \in G$ represent the cosets σH in G.

(1) Prove that we may assume S^H/R to be free, and to possess a basis $\theta_1, \ldots, \theta_n$ such that the determinant $|\sigma_i\theta_j|_{i,j}$ is a unit in S.

(2) Let N be another finite group, and define the *generalised wreath product* with respect to $G \hookrightarrow S_n$ as the semi-direct product

$$N \wr_H G = N^n \rtimes G,$$

where G acts on N^n be

$$\sigma(\nu_1, \ldots, \nu_n) = (\nu_{\sigma^{-1}1}, \ldots, \nu_{\sigma^{-1}n}).$$

Assume the existence of a generic N-extension over K. Prove that there exists a generic $N \wr_H G$-extension. [Hint: This generalises Theorem 7.2.1, and can be proved in much the same way, using (1) above.]

EXERCISE 7.2. Let G be a finite group of order $n = |G|$, and let G act on the Abelian group A by automorphisms. Assume that A is *uniquely divisible* by n, i.e., for all $a \in A$ there exists a unique $b = \frac{1}{n}a \in A$ with $nb = a$. Prove *Maschke's Theorem*, cf. [Ja2, 5.2 p. 253]: Let $B \subseteq A$ be a subgroup of A closed under G's action, and assume that B is a direct summand in A: $A = B \oplus C$ for some subgroup $C \subseteq A$. Then C can be chosen in such a way as to be closed

under G's action as well. [Hint: Take a projection $\pi\colon A \to B$, and modify it to respect the G-action.]

Note that this generalises Exercise 5.10 in Chapter 5, and formulate a corresponding generalisation of Corollary 7.2.2.

EXERCISE 7.3. List all groups of order 24. [Hint: There are fifteen, and S_4 is the only one that does not have a normal Sylow subgroup. (Look at the 3-Sylow subgroups, and map the group to S_4 if there are four of them.) All the others are therefore semi-direct products $C_3 \rtimes E$ or $E \rtimes C_3$, where E is a group of order 8.] Demonstrate that the results at your disposal answer the question of the existence of generic polynomials over $\mathbb{Q}$ for all of these groups except $\mathrm{SL}(2,3) = Q_8 \rtimes C_3$.

EXERCISE 7.4. List all groups of order < 32. Prove that Q_{16} and $\mathrm{SL}(2,3)$ are the only two for which we do not have results proving the existence or non-existence of generic polynomials over $\mathbb{Q}$.

Hilbert class field theory. One way of obtaining explicit integral polynomials with (generalised) dihedral Galois group is by means of Hilbert class fields, and more generally by means of ring class fields of imaginary quadratic number fields. For an extensive treatment, with fuller references, see [K&Y], [C&Y] and [Y&Z], as well as the more recent [Cn2].

For an algebraic number field K, we denote the ring of integers in K by $\mathcal{O}_K$, the discriminant of K by d_K, the *ideal class group* of K by $\mathrm{Pic}(\mathcal{O}_K)$, and the *class number* of K by $h = h_K$. It is well known from algebraic number theory that $\mathrm{Pic}(\mathcal{O}_K)$ is a finite abelian group of order h_K.

To any algebraic number field K we can associate the *Hilbert class field* H. The Hilbert class field is characterised by being the maximal unramified abelian extension of K, cf. [Lo3, Kor. 13.2.8] or [Cox, §5]. In the terminology of [Lo3], H is the class field corresponding to the trivial module $\mathfrak{m} = 1$, and so

$$\mathrm{Gal}(H/K) \simeq \mathrm{Pic}(\mathcal{O}_K).$$

In fact, the isomorphism is induced by the *Artin symbol* as follows: Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and let $\mathfrak{P}$ be an overlying prime in $\mathcal{O}_H$. Then there is a unique element $\sigma = \left(H/K/\mathfrak{p}\right) \in \mathrm{Gal}(H/K)$, called the Artin symbol, satisfying $\sigma x \equiv x^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}}$ for all $x \in \mathcal{O}_H$, where $\mathrm{N}(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}]$, and by homomorphic extension we get a map $\left(H/K/\bullet\right)$ from the ideal group of K to $\mathrm{Gal}(H/K)$, inducing an isomorphism $\mathrm{Pic}(\mathcal{O}_K) \simeq \mathrm{Gal}(H/K)$. See [Cox] or [Lo3, Kap. 7] for details.

It is clear that $H/\mathbb{Q}$ is a Galois extension if $K/\mathbb{Q}$ is, and that we then have

$$\tau\left(\frac{H/K}{\mathfrak{p}}\right)\tau^{-1} = \left(\frac{H/K}{\tau\mathfrak{p}}\right)$$

for $\mathfrak{p}$ in $\mathcal{O}_K$ and $\tau \in \mathrm{Gal}(K/\mathbb{Q})$.

Now, let K be an imaginary quadratic number field, i.e., $K = \mathbb{Q}(\sqrt{-D})$ for a square-free positive integer D. Then $d = d_K$ is either $-D$ or $-4D$, depending

on whether $D \equiv 3 \pmod 4$ or not, and $\mathcal{O}_K = \mathbb{Z}[(d_K + \sqrt{d_K})/2]$. In this case, $H/\mathbb{Q}$ is a generalised dihedral group:

$$\mathrm{Gal}(H/\mathbb{Q}) \simeq D_{\mathrm{Pic}(\mathcal{O}_K)} = \mathrm{Pic}(\mathcal{O}_K) \rtimes C_2.$$

EXERCISE 7.5. Prove this statement about $\mathrm{Gal}(H/\mathbb{Q})$. [Hint: For a non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, we have $\mathfrak{a}\bar{\mathfrak{a}} = [\mathcal{O}_K : \mathfrak{a}]\mathcal{O}_K$ when $\bar{\mathfrak{a}}$ is the complex conjugate ideal.]

It follows that we can produce dihedral extensions on $\mathbb{Q}$ by considering Hilbert class fields of imaginary quadratic number fields. This (being in the Exercises section) is of course only an overview, and we refer to [We3] (as well as [Cox]) for a complete treatment of the basic theory.

More generally, let $\mathcal{O}_K(m)$ be the order in $\mathcal{O}_K$ of conductor $m \in \mathbb{Z}$, i.e. the ring of all integers in K, that are congruent to a rational number modulo m. The class field for the group of principal ideals generated by numbers in the above order is called the *ring class field* for $\mathcal{O}_K(m)$ and has the form $K(j(\alpha))$ for some $\alpha \in \mathcal{O}_K(m)$, where j is the absolute invariant of the modular group ("the elliptic modular j-function"). This class field is Galois over $\mathbb{Q}$ with Galois group a generalized dihedral group. There is an analogue to the classical Kronecker-Weber theorem, according to which every absolute abelian number field is a subfield of a cyclotomic field: Let M be a Galois extension of $\mathbb{Q}$ containing some imaginary quadratic number field K and assume that $\mathrm{Gal}(M/\mathbb{Q})$ is dihedral or generalised dihedral of order $2n$, n odd. Then M is contained in a ring class field $K(j(\alpha))$ for some $\alpha \in K$.

In particular, one obtains all dihedral extensions of order $2n$ that are not totally real, cf. [Je].

EXERCISE 7.6. Consider a quadratic form of the type $(x, y) \mapsto ax^2 + bxy + cy^2$ over $\mathbb{Z}$, i.e., $a, b, c \in \mathbb{Z}$. We denote this form by $[a, b, c]$, and call it *primitive* if $\gcd(a, b, c) = 1$. The *discriminant* of $[a, b, c]$ is $d = b^2 - 4ac$. From the identity

$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - dy^2$$

we see that $[a, b, c]$ is positive definite if $d < 0$ and $a > 0$.

Two forms $[a, b, c]$ and $[A, B, C]$ are said to be *equivalent*, if one can be obtained from the other by a linear transformation with determinant 1, i.e., an element from $\mathrm{SL}_2(\mathbb{Z})$.

Prove the following result, due to GAUSS: The equivalence classes of positive definite primitive quadratic forms $[a, b, c]$ with discriminant d_K correspond bijectively to the elements in $\mathrm{Pic}(\mathcal{O}_K)$ by $[a, b, c] \mapsto \big(a, \frac{1}{2}(-b + \sqrt{d_K})\big)$.

REMARK. A form $[a, b, c]$ is called *reduced*, if $|b| \le a \le c$, and $b \ge 0$ when $|b| = a$ or $a = c$. It can be shown (see e.g. [Cox, Thm. 2.8]) that every positive definite primitive form is equivalent to exactly one reduced form. Using this, it becomes a simple matter, algorithmically speaking, to determine h_K.

Explicit construction of Hilbert class fields. The basic idea is to use singular values of certain modular function. Let $\mathfrak{f}$ be a function defined over the upper half complex plane $\mathfrak{H}$. Suppose that $\mathfrak{f}$ is a modular function for some congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ such that for an imaginary quadratic number

$\tau \in \mathfrak{H}$, $\mathfrak{f}(\tau)$ is an algebraic integer. Let $f(X)$ denote the minimal polynomial of $\mathfrak{f}(\tau)$ over $\mathbb{Q}$ of degree h (the class number of K). Then $f(X)$ is given by

$$f(X) = \prod_{i=1}^{h} (X - \mathfrak{f}(\mathfrak{a}_i))$$

where $\mathrm{Pic}(\mathcal{O}_K) = \{\mathfrak{a}_i \mid i = 1, \cdots, h\}$ and each $\mathfrak{a}_i$ corresponds to a unique imaginary quadratic number $\tau_i \in \mathfrak{H}$. We may call f the *class polynomial* as it depends on the class group $\mathrm{Pic}(\mathcal{O}_K)$. The splitting field of f over $\mathbb{Q}$ defines the Hilbert class field of the imaginary quadratic field $\mathbb{Q}(\tau)$. The Galois group $Gal(f/\mathbb{Q})$ is isomorphic to the generalized dihedral group $D_{\mathrm{Pic}(\mathcal{O}_K)}$.

Algorithms for constructing Hilbert class fields. We now describe a method for constructing class polynomials. The basic idea is to choose a modular function whose singular moduli (that is, values at imaginary quadratic arguments) are concocted to give rise to the 'optimal' class polynomials in the sense that the coefficients are as small as possible.

(A) Traditionally, the elliptic modular j-function, which is a modular function for $\mathrm{PSL}_2(\mathbb{Z})$ was used. Weber computed a number of class polynomials for small discriminates. Kaltofen and Yui [K&Y] pushed the calculations with j-function to discriminants of size ≤ 1000. However, the coefficients of these class polynomials are astronomical, though Gross and Zagier [G&Z] showed that their constant terms and discriminants are so-called 'smooth numbers', i.e., that they factor very highly. In practice, it is not efficient to construct class polynomials using singular moduli of j-function.

(B) The next choice of the modular function that can be used in the construction was Weber modular functions $\mathfrak{f}$, $\mathfrak{f}_1$ and $\mathfrak{f}_2$. The Weber functions are defined as follows:

$$\begin{aligned}
\mathfrak{f}(z) &= q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-1/2}), \\
\mathfrak{f}_1(z) &= q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-1/2}), \quad \text{and} \\
\mathfrak{f}_2(z) &= \sqrt{2}\, q^{1/24} \prod_{n=1}^{\infty} (1 + q^n) = \sqrt{2}\, q^{1/24} \prod_{n=1}^{\infty} (1 - q^{2n-1})^{-1},
\end{aligned}$$

where $q = e^{2\pi i z}$.

These functions are connected with the relations

$$\mathfrak{f}^8(z) = \mathfrak{f}_1^8(z) + \mathfrak{f}_2(z)^8, \quad \mathfrak{f}(z)\mathfrak{f}_1(z)\mathfrak{f}_2(z) = \sqrt{2},$$
$$\mathfrak{f}(z)\mathfrak{f}_2((1+z)/2) = e^{i\pi/24}\sqrt{2} \quad \text{and} \quad \mathfrak{f}_1(z)\mathfrak{f}_2(z/2) = \sqrt{2}.$$

Furthermore, $j(z)$ is related to these functions by the following identities:

$$j(z) = \frac{(\mathfrak{f}^{24}(z) - 16)^3}{\mathfrak{f}^{24}(z)} = \frac{(\mathfrak{f}_1^{24}(z) + 16)^3}{\mathfrak{f}_1^{24}(z)} = \frac{(\mathfrak{f}_2^{24}(z) + 16)^3}{\mathfrak{f}_2^{24}(z)}.$$

This means that $\mathfrak{f}^{24}(z)$, $-\mathfrak{f}_1^{24}(z)$ and $-\mathfrak{f}_2^{24}(z)$ are roots of the equation

$$(X-16)^3 - Xj(z) = 0.$$

These functions were used by Weber, Watson, and Yui and Zagier to produce Hilbert class fields, and class polynomials.

The construction described above for the maximal orders $\mathcal{O}_K$ of imaginary quadratic field K can be extended to orders $\mathcal{O}$ of K, according to the following theorem, which sums up results from Weber [We3], Watson [Wat], and Kaltofen and Yui [K&Y]:

THEOREM. *Let $\mathcal{O}$ be an order of discriminant d in the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d})$, and assume $d \equiv 1 \pmod 4$ and $3 \nmid d_K$. Let h be the class number of $\mathcal{O}$, and $H_d(X)$ the class equation. Put*

$$\tilde{H}_d(X) = X^h H_d\left(\frac{(X-16)^3}{X}\right).$$

Then the following assertions hold:

(a) *$\tilde{H}_d(X)$ is a monic integral polynomial of degree $3h$ over $\mathbb{Q}$,*

(b) *$\tilde{H}_d(X)$ contains an irreducible factor $\tilde{h}_d(X) \in \mathbb{Q}[X]$ of degree h having $2^{12} f^{-24}(\sqrt{d})$ as its root, and*

(c) *if $d \equiv 1 \pmod 8$ and we write $\tilde{h}_d(X) = \prod_{i=1}^h (X - \alpha_i)$, a judicious choice of 24^{th} roots of the α_i's makes the polynomial*

$$h_d(X) = X^h \prod_{i=1}^h \left(\frac{1}{X} - \alpha_i^{1/24}\right)$$

integral and irreducible with the ring class field of $\mathcal{O}$ as splitting field, and hence with Galois group

$$\mathrm{Gal}(h_d/\mathbb{Q}) \simeq D_{\mathrm{Pic}(\mathcal{O})}.$$

EXERCISE 7.7. Prove the above Theorem. [Hint: See the article of Yui and Zagier [Y&Z].]

EXAMPLES. (1) Let $d_K = -127$. Then $h = 5$, and

$$h_{-127}(X) = X^5 - X^4 - 2X^3 + X^2 + 3X - 1.$$

(2) Let $d_K = -191$. Then $h = 13$ and

$$\begin{aligned} h_{-191}(X) = {} & X^{13} - 6X^{12} + 10X^{11} - 16X^{10} + 22X^9 - 19X^8 \\ & + 11X^7 - 5X^6 - X^5 + 5X^4 - 4X^3 + 2X - 1. \end{aligned}$$

(3) Let $d_K = -359$. Then $h = 19$, and

$$\begin{aligned} h_{-359}(X) = {} & X^{19} - 14X^{18} + 59X^{17} - 113X^{16} + 91X^{15} + 19X^{14} \\ & - 90X^{13} + 51X^{12} + 2X^{11} - 5X^{10} + 9X^9 - 30X^8 \\ & + 22X^7 + 7X^6 - 14X^5 + 3X^4 + 2X^3 - 2X^2 + 2X - 1. \end{aligned}$$

(C) At present, the optimal choice for the modular function appears to be the Schertz function [Scz1, Scz2, Scz3, Scz4, Scz5], which is defined in terms of η products as follows: Let $K = \mathbb{Q}(\sqrt{d_K})$ be an imaginary quadratic field over $\mathbb{Q}$. Let $\mathrm{Pic}(\mathcal{O}_K) = \{\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_h\}$. Let $\mathfrak{p}$ and $\mathfrak{q}$ be ideals of K of norm p and q, respectively.

An ideal $\mathfrak{p}$ is *primitive* if $\mathfrak{p}$ is an integral ideal and there is no positive integer $n \geq 2$ for which $\mathfrak{p}/n$ is also integral. A primitive ideal $\mathfrak{p}$ can be written as $\mathfrak{p} = p\mathbb{Z} \oplus \frac{-u+\sqrt{d_K}}{2}\mathbb{Z}$ with $p = \mathrm{N}(\mathfrak{p})$ and $u \in \mathbb{Z}$ determined by $u^2 \equiv D \pmod{4p}$. Assume that

(i) the ideals $\mathfrak{a}_i$ are all primitve,
(ii) the ideals $\mathfrak{p}$ and $\mathfrak{q}$ are primitive non-principal,
(iii) if both classes of $\mathfrak{p}$ and $\mathfrak{q}$ are of order 2 in the class group, these classes are equal,
(iv) for all i, $\mathfrak{pqa}_i$ is primitive, and
(v) e is a positive integer such that $24 \mid e(p-1)(q-1)$.

Define

$$g_{\mathfrak{p},\mathfrak{q},e}(\mathfrak{a}) = \left(\frac{\eta(\tau/p)\eta(\tau/q)}{\eta(\tau/pq)\eta(\tau)}\right)^e,$$

where $\mathfrak{a}_i\mathfrak{pq} = a_i(pq\mathbb{Z} + \frac{-u+\sqrt{d_K}}{2a_i}) = a_i(pq\mathbb{Z} + \tau_i\mathbb{Z})$. Then $g_{\mathfrak{p},\mathfrak{q},e}(\mathfrak{a})$ may replace the singular moduli $j(\mathfrak{a})$, or $\mathfrak{f}(\mathfrak{a})$ in the construction of the Hilbert class field.

Exercise 7.8. Prove the following theorem:

Theorem. (Schertz) *Let*

$$P_{\mathfrak{p},\mathfrak{q},e}(X) = \prod_{i=1,\cdots,h} (X - g_{\mathfrak{p},\mathfrak{q},e}(\mathfrak{a}_i)).$$

Then $P_{\mathfrak{p},\mathfrak{q},e}(X) \in \mathbb{Z}[X]$ is irreducible over K, and $K[X]$, its constant term is ± 1, and its splitting field over $\mathbb{Q}$ is the Hilbert class field of K.

Examples. (1) Let $d_K = -191$. Then

$$P_{\mathfrak{p},\mathfrak{q},e}(X) = X^{13} - 2X^{12} + 4Z^{10} - 5X^9 + X^8 + 5X^7 - 11X^6 + 19X^5 - 22X^4 + 16X^3 - 10X^2 + 6X - 1.$$

(2) Let $d_K = -359$. Then

$$P_{\mathfrak{p},\mathfrak{q},e}(X) = X^{19} - 2X^{18} + 2X^{17} - 2X^{16} - 3X^{15} + 14X^{14} - 7X^{13} - 22X^{12} + 30X^{11} - 9X^{10} + 5X^9 - 2X^8 - 51X^7 + 90X^6 - 19X^5 - 91X^4 + 113X^3 - 59X^2 + 14X - 1.$$

We refer to Cohen, [Cn2, Ch. 6] for further details about Schertz functions and their implementation in GP/Pari.

CHAPTER 8

The Number of Parameters

8.1. Basic Results

One of the questions (D) asked in the Introduction was: Assuming the existence of generic polynomials for the finite group G over the field K, what is the minimal number of parameters required? In some cases, the answer is obvious: $X^2 - t$ is generic for quadratic extensions over any field of characteristic $\neq 2$, and clearly one parameter is the absolute minimum. On the other hand: As we saw in Chapter 2, the polynomial $X^4 - 2s(1+t^2)X^2 + s^2t^2(1+t^2)$ is generic for C_4, and $(X^2 - s)(X^2 - t)$ is generic for V_4 (both in characteristic $\neq 2$ as well). In both cases, we have two parameters. Is this optimal, or is it possible to make do with one? Intuitively, two parameters is 'natural' for V_4: A V_4-extension consists of two quadratic extensions, and how can we hope to 'capture' them both by a single parameter?[1]

It is difficult to establish exact minima in general. However, it *is* possible to give some lower bounds, and we will do so in this section. We start by considering the following question: When is one parameter enough? To this end, we need a preliminary result:

PROPOSITION 8.1.1. (ROQUETTE [Ro], OHM [O]) *Let L/K be a field extension of finite transcendence degree, and let M/K be a subextension of $L(t)/K$ with $\operatorname{tr.deg}_K M \leq \operatorname{tr.deg}_K L$. Then M/K can be embedded in L/K.*

First, a technical lemma:

LEMMA 8.1.2. *Let M/K be a field extension of finite transcendence degree, and let v be a valuation on M with residue field μ, such that v is trivial on K and $\operatorname{tr.deg}_K \mu = \operatorname{tr.deg}_K M$. Then v is trivial.*

PROOF. Let $y_1, \ldots, y_n \in \mathcal{O}_v$, such that $\bar{y}_1, \ldots, \bar{y}_n$ is a transcendence basis for μ/K. Then $y_1, \ldots, y_n$ is a transcendence basis for M/K, and the residue field of $v|_{K(y_1,\ldots,y_n)}$ is $K(\bar{y}_1, \ldots, \bar{y}_n)$. Now, $K[y_1, \ldots, y_n] \subset \mathcal{O}_v$, and $K[y_1, \ldots, y_n] \cap \mathfrak{m}_v = 0$. It follows that $K(y_1, \ldots, y_n) \subseteq \mathcal{O}_v$, i.e., v is trivial on $K(y_1, \ldots, y_n)$. Since $M/K(y_1, \ldots, y_n)$ is algebraic, it follows that v is trivial on M as well. □

PROOF OF PROPOSITION 8.1.1. By extending M inside $L(t)$, we may assume $\operatorname{tr.deg}_K M = \operatorname{tr.deg}_K L$.

[1] Of course, one should be wary of the intuitively obvious. If $\operatorname{char} K = 2$ and $K \neq \mathbb{F}_2$, it *is* in fact possible to find a generic V_4-polynomial with only a single parameter, cf. Chapter 5.)

If L/K is algebraic, the result is clear: L consists exactly of the elements in $L(t)$ that are algebraic over K, and since M/K is algebraic, we must have $M \subseteq L$.

If L/K has transcendence degree $n > 0$, we let $z_1, \dots, z_n$ be a transcendence basis for L/K. Now, $L(t)/M(t)$ is algebraic, and so there exists non-zero polynomials $f_i(t, X) \in M[t, X]$ with $f_i(t, z_i) = 0$. Let S be the set of all the non-zero coefficients in the f_i's as polynomials in t and X, as well as in X alone, i.e., if

$$f_i(t, X) = \sum_j (\sum_k a_{jk} t^k) X^j$$

we include in S all the a_{jk}'s *and* the polynomials $\sum_k a_{jk} t^k$. It is a finite set, and so there are only finitely many $(t - c)$-adic valuations on $M(t)$ for which it is not contained in the group of units. In particular, for $j \gg 0$ we can let $c = z_1^j$. Denote the $(t - c)$-adic valuation by v.

Under the canonical map $\mathcal{O}_v \to L$, the equation $f_i(t, z_i) = 0$ becomes $f_i(c, z_i) = 0$, and since $S \subseteq \mathcal{O}_v^*$, the z_i's satisfy non-zero polynomial equations over $\mu[c]$, where μ is the residue field of M. If we pick j to be larger than the degree (in z_1) of $f_1(t, z_1)$, we see that z_1 is algebraic over μ. Hence, so is $c = z_1^j$, and $\mu[c] = \mu(c)$ is a finite field extension. It follows that L/μ is algebraic, and from the Lemma we get that v is trivial on M, i.e., $M \simeq \mu \subseteq L$. □

NOTE. As mentioned in the Introduction, several examples of unirational but not rational varieties have been constructed over algebraically closed fields, or over $\mathbb{R}$. However, we are mostly interested in the case where the ground field is $\mathbb{Q}$. Here, the first example appears to be the one given by Beauville, Colliot-Thélène, Sansuc and Swinnerton-Dyer in [Be&al], where it is proved that there exists a non-rational subextension of $\mathbb{Q}(x_1, x_2, x_2, x_4, x_5)/\mathbb{Q}$ of transcendence degree 2. (In fact, the subextension considered in [Be&al] is stably rational, but for our purposes this stronger statement is not needed. See also [Oj].) It follows from the above result that in fact there exists a non-rational subextension of $\mathbb{Q}(x, y)/\mathbb{Q}$, thus answering Lüroth's Problem in the negative even for degree 2.

In the Example on p. 57 in Chapter 2 we constructed a non-rational subextension of $\mathbb{Q}(s, t, u)/\mathbb{Q}$.

From Lüroth's Theorem (Theorem 0.3.1 in the Introduction) we now get

COROLLARY 8.1.3. *Let $K(t_1, \dots, t_r)/K = K(\mathbf{t})/K$ be a rational extension, and let L/K be a subextension of transcendence degree* 1. *Then L/K is rational.*

As an immediate consequence of this Corollary, we have

PROPOSITION 8.1.4. *Let K be a field and G a non-trivial finite group. Then a* necessary *condition for the existence of a one-parameter generic polynomial for G over K is that $G \hookrightarrow \mathrm{PGL}_2(K)$.*

PROOF. Let $P(s, X) \in K(s)[X]$ be a one-parameter generic G-polynomial. Also, let G act transitively on a set $\mathbf{t}$ of indeterminates. Then $K(\mathbf{t})$ is the splitting field over $K(\mathbf{t})^G$ of a specialisation $P(t, X)$ of $P(s, X)$. It is clear that t cannot be in K, since $K(\mathbf{t})/K(\mathbf{t})^G$ is not induced by a G-extension of K. Thus, t is transcendental, and the splitting field $\mathbb{M}$ of $P(t, X)$ over $K(t)$ is a G-extension

contained inside $K(\mathbf{t})$. By the Corollary, $\mathbb{M}$ is rational over K: $\mathbb{M} = K(u)$ for some u. Hence, $G \subseteq \mathrm{Aut}_K\, K(u) = \mathrm{PGL}_2(K)$. □

REMARK. It is easy to see that $\mathrm{PGL}_2(\mathbb{Q})$ does not contain any elements of finite order 4, 5 or ≥ 7.[2] Thus, for the groups C_4, D_4, S_4, C_5, D_5, F_{20}, A_5 and S_5, the generic polynomials we have found (with two parameters) are optimal. Similarly for A_4, since this group is not a subgroup of $\mathrm{PGL}_2(\mathbb{Q})$.

EXAMPLES. The Klein Vierergruppe V_4 and the cyclic group C_6 of order 6 are both subgroups of $\mathrm{PGL}_2(\mathbb{Q})$. However, in neither case is there a one-parameter generic polynomial, thus demonstrating that the condition of Proposition 8.1.4 is not sufficient.

(1) Assume $P(s, X) \in \mathbb{Q}(s)[X]$ to be a generic V_4-polynomial, and consider the extension $\mathbb{Q}(x, y)/\mathbb{Q}(x^2, y^2)$. As in the proof above, the splitting field of $P(s, X)$ over $\mathbb{Q}(s)$ has to be rational, i.e., equal to $\mathbb{Q}(t)$ for some t, allowing us to identify V_4 with a subgroup of $\mathrm{PGL}_2(\mathbb{Q})$. Now, every non-trivial element in $\mathrm{PGL}_2(\mathbb{Q})$ is conjugate to one represented by a matrix $\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$, and if the element has order 2, we must have $b = 0$. Thus, by choosing t properly, we may assume that one of the elements in V_4 acts by $t \mapsto a/t$ for a (fixed) $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^2$.

Now, $\mathbb{Q}(x, y)/\mathbb{Q}(x^2, y^2)$ is obtained by specialising $P(s, X)$, and the specialisation is necessarily in a transcendental element. Thus, $\mathbb{Q}(t)/\mathbb{Q}(s)$ can be embedded into $\mathbb{Q}(x, y)/\mathbb{Q}(x^2, y^2)$ (as a V_4-extension). In particular, a is a norm in $\mathbb{Q}(x, y)/L$, where $L/\mathbb{Q}(x^2, y^2)$ is one of the three quadratic subextensions of $\mathbb{Q}(x, y)/\mathbb{Q}(x^2, y^2)$. We may assume $L = \mathbb{Q}(x^2, y)$. But it is clear that a non-square element in $\mathbb{Q}$ is not a norm in $\mathbb{Q}(x, y)/\mathbb{Q}(x^2, y)$. Thus, we have a contradiction, and conclude that V_4 requires two parameters.

(2) Next, suppose $Q(s, X) \in \mathbb{Q}(s)[X]$ to be generic for C_6 over $\mathbb{Q}$. Then, as above, the splitting field is rational over $\mathbb{Q}$, and we write it as $\mathbb{Q}(t)$ for some t. Up to conjugation, there is only one element of order 6 in $\mathrm{PGL}_2(\mathbb{Q})$, represented by $\left(\begin{smallmatrix} 0 & -3 \\ 1 & 3 \end{smallmatrix}\right)$, meaning that we may assume a generator for C_6 to act on $\mathbb{Q}(t)$ by $t \mapsto 1/(3 - 3t)$. It follows that t has norm $-1/27$ in $\mathbb{Q}(t)/\mathbb{Q}(s)$.

Consider now the C_6-extension $\mathbb{Q}(x, y)/\mathbb{Q}(u, v)$, where

$$u = x^2 \quad \text{and} \quad v = \frac{-y^3 + 3y - 1}{y - y^2},$$

cf. section 2.1 in Chapter 2. Then, since $Q(s, X)$ is generic, $\mathbb{Q}(t)/\mathbb{Q}(s)$ embeds into $\mathbb{Q}(x, y)/\mathbb{Q}(u, v)$, implying in particular that $-1/27$ is a norm in the extension $\mathbb{Q}(x, y)/\mathbb{Q}(u, v)$. But then $-1/27$ is also a norm in $\mathbb{Q}(x, v)/\mathbb{Q}(u, v) = \mathbb{Q}(x, v)/\mathbb{Q}(x^2, v)$, in contradiction to the observation in point (1) above. It follows that C_6 does *not* possess a one-parameter generic polynomial over $\mathbb{Q}$, but needs at least two parameters. On the other hand, as with V_4, it is obvious that two parameters are sufficient.

[2]Hint: A matrix $\mathbf{A}$ representing an element of order $n > 1$ must satisfy both its own characteristic equation and $X^n - a$ for suitable $a \in \mathbb{Q}^*$. Thus, the characteristic equation must in fact divide $X^n - a$, and we only have to see that this is not possible for $n = 4$, 9 or p, where p is a prime ≥ 5.

REMARK. It is clear that C_6 *does* possess a one-parameter generic polynomial over the sixth cyclotomic field, namely $X^6 - t$. On the other hand, as we shall see below, it is *never* possible (in characteristic $\neq 2$) to find a one-parameter generic polynomial for V_4.

8.2. Essential Dimension

Following Buhler and Reichstein we now introduce the concept of *essential dimension*. The results in the following are mostly taken from their paper [B&R1], although the arguments given here are different, in that they do not make use of algebraic geometry. See also [B&R2].

DEFINITION 8.2.1. Let M/L be a finite separable extension of fields containing K. If, for an intermediate field L', $K \subseteq L' \subseteq L$, there exists an extension M'/L' of degree $n = [M : L]$ inside M, such that $M = M'L$, we say that M/L is *defined* over L'. Moreover, we define the *essential dimension* of M/L, $\mathrm{ed}_K(M/L)$, to be the minimum of the transcendence degree $\mathrm{tr.deg}_K L'$, when L' runs through all intermediate fields over which M/L is defined.

Clearly, the essential dimension is always finite: M is generated over L by some primitive element θ, and M/L is then defined over the subfield obtained from K by adjoining the coefficients of θ's minimal polynomial over L. And since it is always possible to find a primitive element with trace 0 or 1, we in fact get $\mathrm{ed}_K(M/L) < [M : L]$.

The essential dimension is an expression of the 'complexity' of the extension M/L (over K), in that it gives the number of algebraically independent 'parameters' needed to describe the structure of M/K (in the form of M'/L').

LEMMA 8.2.2. *Let M/L be a G-extension of fields containing K, and let $d = \mathrm{ed}_K(M/L)$. Then there exists a subfield M' of transcendence degree d on which G acts faithfully, and hence the essential dimension of M/L can be obtained from a G-extension M'/L' of subfields.*

PROOF. Pick M''/L'' realising the essential dimension. Then M contains the Galois closure M' of M'' over L'', and we let $L' = M'^G$. Since $M' \supseteq M''$, we have $M = M'L$, and M'/L' gives us the desired G-extension. □

DEFINITION 8.2.3. Let G be a finite group, and let G act regularly on a set $\mathbf{t} = (t_\sigma)_{\sigma \in G}$ of indeterminates. Then we define the *essential dimension* of G over a given field K, $\mathrm{ed}_K G$, to be the essential dimension of $K(\mathbf{t})/K(\mathbf{t})^G$ over K.

EXAMPLES. (1) $\mathrm{ed}_{\mathbb{Q}} 1 = 0$. (This is clear.)

(2) $\mathrm{ed}_{\mathbb{Q}} C_2 = \mathrm{ed}_{\mathbb{Q}} C_3 = \mathrm{ed}_{\mathbb{Q}} S_3 = 1$. (These follow easily from Proposition 8.2.4 below, together with the fact that the trivial group is obviously the *only* group with essential dimension 0.)

(3) We have

$$\mathrm{ed}_{\mathbb{Q}} V_4 = \mathrm{ed}_{\mathbb{Q}} C_4 = \mathrm{ed}_{\mathbb{Q}} D_4 = \mathrm{ed}_{\mathbb{Q}} A_4 = \mathrm{ed}_{\mathbb{Q}} S_4 = 2,$$
$$\mathrm{ed}_{\mathbb{Q}} C_5 = \mathrm{ed}_{\mathbb{Q}} D_5 = \mathrm{ed}_{\mathbb{Q}} F_{20} = \mathrm{ed}_{\mathbb{Q}} A_5 = \mathrm{ed}_{\mathbb{Q}} S_5 = 2,$$
$$\text{as well as} \quad \mathrm{ed}_{\mathbb{Q}} C_6 = 2.$$

(In all cases, an upper bound of 2 follows from Proposition 8.2.4 below, together with the results of Chapter 2. And for all except V_4 and C_6, equality then follows in analogy with the proof of Proposition 8.1.4 above. For V_4 and C_6, more is needed: Either Theorem 8.2.11 below, or Proposition 8.2.8 in conjunction with the arguments of the Examples on p. 189 above.)

PROPOSITION 8.2.4. *Let $P(\mathbf{s}, X) \in K(\mathbf{s})[X] = K(s_1, \ldots, s_n)[X]$ be a generic G-polynomial over K. Then*

$$\operatorname{ed}_K G \leq n.$$

In other words: The essential dimension gives a lower bound on the number of parameters required in a generic polynomial.

PROOF. $K(\mathbf{t})/K(\mathbf{t})^G$ is realised by a specialisation of $P(\mathbf{s}, X)$, say $P(\mathbf{a}, X)$. But then $K(\mathbf{t})/K(\mathbf{t})^G$ is defined over $K(\mathbf{a})$, which has transcendence degree at most n. □

To make proper use of the essential dimension, we need to record a generalisation of Proposition 8.1.1:

PROPOSITION 8.2.5. *Let L/K be a field extension of finite transcendence degree, and let M/L be a G-extension. Extend the action of G to the function field $M(t)$ by $\sigma t = t$ for $\sigma \in G$, and let F be a subfield of $M(t)$ on which G acts faithfully, with $E = F^G$. Assume that* $\operatorname{tr.deg}_K F \leq \operatorname{tr.deg}_K L$. *Then F/E can be embedded in M/L (as a G-extension).*

PROOF. We may assume $\operatorname{tr.deg}_K F = \operatorname{tr.deg}_K L$. The proof of Proposition 8.1.1 gives us a $c \in L$, such that the $(t-c)$-adic valuation v is trivial on E. Clearly, v is defined on $M(t)$, and as such it is trivial on F. Since the canonical map $\mathcal{O}_v \to M$ preserves the G-action, we get F/E embedded in M/L. □

COROLLARY 8.2.6. *Let L/K be a field extension of finite transcendence degree, and let M/L be a G-extension. Then*

$$\operatorname{ed}_K(M(t)/L(t)) = \operatorname{ed}_K(M/L).$$

PROPOSITION 8.2.7. *Let H be a subgroup of G. Then*

$$\operatorname{ed}_K H \leq \operatorname{ed}_K G.$$

PROOF. Let G act regularly on the indeterminates $\mathbf{t} = (t_\sigma)_{\sigma \in G}$, and let H act regularly on the indeterminates $\mathbf{s} = (s_\tau)_{\tau \in H}$. Then $\operatorname{ed}_K(K(\mathbf{t})/K(\mathbf{t})^H) \leq \operatorname{ed}_K G$. Also, $s_\tau \mapsto t_\tau$ gives an embedding of the field $K(\mathbf{s})$ into $K(\mathbf{t})$ that respects the H-action. Thus, $K(\mathbf{s})/K(\mathbf{s})^H \hookrightarrow K(\mathbf{t})/K(\mathbf{t})^H$. By the No-name Lemma (p. 22 in Chapter 1) we get that $K(\mathbf{t})^H/K(\mathbf{s})^H$ is rational, and the Proposition follows from Corollary 8.2.6. □

PROPOSITION 8.2.8. *Let G act faithfully on the finite-dimensional K-vector space V. Then*

$$\operatorname{ed}_K(K(V)/K(V)^G) = \operatorname{ed}_K G.$$

PROOF. Let U be the K-vector space $K[G]$ with regular G-action. Then $K(U \oplus V)/K(U \oplus V)^G$ is obtained from both $K(U)/K(U)^G$ and $K(V)/K(V)^G$ by adjoining indeterminates (the No-name Lemma), and by Corollary 8.2.6 all three extensions have the same essential dimension. □

Hence, $\operatorname{ed}_K G \leq n$ if $G \hookrightarrow \mathrm{GL}_n(K)$.

COROLLARY 8.2.9. $\operatorname{ed}_K(G \times H) \leq \operatorname{ed}_K G + \operatorname{ed}_K H$.

PROOF. Let G and H act regularly on $U = K[G]$ and $V = K[H]$. Then $K(U)/K(U)^G$ and $K(V)/K(V)^H$ both sit inside $K(U \oplus V)$. Let F/E and F'/E' realise $\operatorname{ed}_K G$ and $\operatorname{ed}_K H$. Then $K(U \oplus V)/K(U \oplus V)^{G \times H}$ is defined over EE', and $\operatorname{ed}_K(G \times H) \leq \operatorname{tr.deg}_K EE' = \operatorname{ed}_K G + \operatorname{ed}_K H$. □

REMARK. We do not in general have equality: Over $\mathbb{C}$, any cyclic group has essential dimension 1, regardless of whether it can be written as a direct product of proper subgroups or not.

In analogy with the proof of Proposition 8.2.4 we see that the number of parameters in a generic G-polynomial is bounded below by the essential dimension of *any* G-extension of fields containing K. However, this is no improvement:

PROPOSITION 8.2.10. *Let M/L be a G-extension of fields containing the* infinite *field K. Then*

$$\operatorname{ed}_K(M/L) \leq \operatorname{ed}_K G.$$

PROOF. Let G act regularly on $\mathbf{t} = (t_\sigma)_{\sigma \in G}$. We can find a normal basis $\boldsymbol{\theta} = (\sigma\theta)_{\sigma \in G}$ for M/L, such that any prescribed non-zero polynomial in $t \in K[\mathbf{t}]$ is $\neq 0$ in $\boldsymbol{\theta}$.

Now, let the G-extension F/E inside $K(\mathbf{t})/K(\mathbf{t})^G$ realise the essential dimension, i.e., it has transcendence degree equal to the essential dimension of G over K. F/E has a normal basis $\mathbf{a} = (\sigma a)_{\sigma \in G}$, and we can pick $t \in K[\mathbf{t}]^G \setminus (0)$ such that $K[\mathbf{t}, 1/t]$ contains a, $(\sigma a - a)^{-1}$ for all $\sigma \in G \setminus 1$, and a generating set S for F/K with the following property: S contains a transcendence basis T for F/K, and all the remaining elements of S, as well as a, are integral over $K[T]$. Define a map $\varphi\colon K[\mathbf{t}, 1/t] \to M$ by $t_\sigma \mapsto \sigma\theta$, and extend it to $R = K[\mathbf{t}, 1/t]_{\mathfrak{m}}$ for $\mathfrak{m} = \ker \varphi$. It respects the the G-action, and since $\sigma\varphi a \neq \varphi a$ for $\sigma \neq 1$, G acts faithfully on the field F' generated over K by $\varphi(\mathbf{a})$ and $\varphi(S)$, meaning that M/L is defined over $E' = F'^G$. But clearly $\operatorname{tr.deg}_K E' \leq \operatorname{tr.deg}_K E = \operatorname{ed}_K G$. □

THEOREM 8.2.11. *Let K be a field of characteristic* 0 *containing the primitive p^{th} roots of unity, p prime, and let G be a finite group. Assume that K does not contain the primitive r^{th} roots of unity for any prime $r \neq p$ dividing $|Z(G)|$. Then*

$$\operatorname{ed}_K(G \times C_p) = \operatorname{ed}_K G + 1.$$

PROOF. '$\leq$' is clear from Corollary 8.2.9, since $\operatorname{ed}_K C_p = 1$.

'$\geq$': Let $G \hookrightarrow \mathrm{GL}_K(U)$, and let $\zeta \in K^*$ be a primitive p^{th} root of unity. Then $G \times C_p \hookrightarrow \mathrm{GL}_K(V)$ for $V = U \oplus K$, and $K(V) = K(U)(t)$ for an indeterminate t representing a basis vector in K, with a generator for C_p acting by $t \mapsto \zeta\, t$.

Let the $G \times C_p$-extension F/E inside $K(V)/K(V)^{G\times C_p}$ have transcendence degree equal to $d = \mathrm{ed}_K(G \times C_p)$. Also, let v be the t-adic valuation on $K(V)$. Since $v = v \circ \sigma$ for $\sigma \in G \times C_p$, the residue map $\mathcal{O}_v \to K(U)$ respects the $G \times C_p$-action. It follows that v is non-trivial on F: If not, we would have $F \subseteq \mathcal{O}_v$, and hence get a map $F \hookrightarrow K(U)$ respecting the C_p-action, in contradiction of the fact that C_p acts trivially on $K(U)$ but not on F. Consequently, the residue field F' of $v|_F$ inside $K(U)$ has transcendence degree $\leq d - 1$ by Lemma 8.1.2.

We claim that G acts faithfully on F', and demonstrate this by proving two technical lemmas:

LEMMA 8.2.12. *Let F/K be a field extension, and let v be a discrete valuation on F with residue field F'. Also, let $\sigma \in \mathrm{Aut}_K F$ have finite order not dividing* $\mathrm{char}\, K$*. Assume that v is trivial on K and invariant under σ. Then σ is the identity on F if and only if it induces the identity on both F' and $\mathfrak{m}_v/\mathfrak{m}_v^2$.*

PROOF. 'Only if' is clear. 'If': The assumptions are that $\sigma x - x \in \mathfrak{m}_v$ for all $x \in \mathcal{O}_v$ and that $\sigma x - x \in \mathfrak{m}_v^2$ for all $x \in \mathfrak{m}_v$. It follows by induction that $\sigma x - x \in \mathfrak{m}_v^{n+1}$ for all n and all $x \in \mathfrak{m}_v^n$.

If $\sigma \neq 1_F$, we have some $x \in \mathcal{O}_v$ with $y = \sigma x - x \neq 0$. Let $n = v(y)$. Then $\sigma y - y \in \mathfrak{m}_v^{n+1}$, and it follows that $\sigma^j x \equiv x + jy \pmod{\mathfrak{m}_v^{n+1}}$ for all j. This gives a contradiction for $j = |\sigma|$. Q.E.D.

LEMMA 8.2.13. *Let F/K be a field extension in characteristic* 0*, and let v be a discrete valuation on F with residue field F'. Also, let H be a finite group of K-automorphisms on F, and assume that v is trivial on K and H-invariant. Also assume that K is relatively algebraically closed in F'. Then the inertia group for v (for $\mathfrak{m}_v$) is a central cyclic subgroup of H, isomorphic to a group of roots of unity in K.*

PROOF. Let I be the inertia group. Since I (by definition) acts trivially on F', we get from the previous Lemma that an element $\tau \in I$ is given completely by its action on $\mathfrak{m}_v/\mathfrak{m}_v^2$. As this is a one-dimensional F'-vector space, τ must act as multiplication by a suitable root of unity $\zeta(\tau) \in F'$. We conclude immediately that I is cyclic, and that conjugation with elements from H corresponds to the Galois action on F': For $\tau \in I$ and $\sigma \in H$ we have $\zeta(\sigma\tau\sigma^{-1}) = \sigma\,\zeta(\tau)$. Moreover, since K is assumed relatively algebraically closed in F', we in fact have $\zeta(\tau) \in K$, meaning that conjugation acts trivially: $\zeta(\sigma\tau\sigma^{-1}) = \sigma\,\zeta(\tau) = \zeta(\tau)$. Thus, I is central in H. Q.E.D.

Continuing the proof of Theorem 8.2.11, we assume that G does *not* act faithfully on F'. Then the inertia group I for $v|_F$ contains C_p properly, and by Lemma 8.2.13 it is central cyclic in $G \times C_p$. This is clearly only possible if $I \simeq C_{ph}$ for some $h > 1$ not divisible by p. But Lemma 8.2.13 also gives us that $I \hookrightarrow K^*$, and our assumption about roots of unity in K is exactly that no such h exists. This gives the desired contradiction.

Thus, there exists an element in $I \setminus 1$ acting trivially on $\mathfrak{m}_v/\mathfrak{m}_v^2$. But by Lemma 8.2.12, this element must then act trivially on F, contradicting the faithfulness of G.

All in all: $K(U)/K(U)^G$ is defined over $E' = F'^G$, and so we have $\operatorname{ed}_K G \leq d-1$. □

REMARK. Thus, for instance,

$$\operatorname{ed}_{\mathbb{Q}}(G \times C_2) = \operatorname{ed}_{\mathbb{Q}} G + 1$$

for any finite group G.

Since clearly $\operatorname{ed}_L G \leq \operatorname{ed}_K G$ when $L \supseteq K$, we also get

COROLLARY 8.2.14. *Let K be a field of characteristic 0. Then*

$$\operatorname{ed}_K C_p^n \geq n$$

for all primes p.

This gives an alternative proof of $\operatorname{ed}_{\mathbb{Q}} V_4 = 2$. More generally, we see that

$$\operatorname{ed}_{\mathbb{Q}} C_2^n = \operatorname{ed}_{\mathbb{Q}} C_3^n = n.$$

It follows that C_2, C_3 and S_3 are the *only* finite groups with essential dimension 1 over $\mathbb{Q}$, and hence the only groups admitting one-parameter generic polynomials.

REMARK. In [B&R1], Buhler and Reichstein provides a sketch of an alternative cohomological proof of

$$\operatorname{ed}_{\mathbb{Q}} C_2^n = n$$

due to J.-P. Serre. The argument goes as follows: Quadratic forms in n variables arise from trace forms of multiquadratic extensions. For $r < n$, we have $H^n(K) = 0$ for a field K of transcendency degree r over an algebraically closed field. Since the n^{th} Stiefel-Whitney class for an n-dimensional quadratic form is generically non-zero, it follows that C_2^n must have essential dimension at least n over an algebraically closed field.

Another easy consequence is

COROLLARY 8.2.15. *Let K be a field of characteristic 0. Then*

$$\operatorname{ed}_K S_{n+2} \geq \operatorname{ed}_K S_n + 1$$

for all n. In particular, $\operatorname{ed}_K S_n \geq \lfloor n/2 \rfloor$, where $\lfloor\ \rfloor$ denotes integer part.

Similarly,

$$\operatorname{ed}_K A_{n+4} \geq \operatorname{ed}_K A_n + 2$$

for $n \geq 4$, and so $\operatorname{ed}_K A_n \geq 2\lfloor n/4 \rfloor$.

PROOF. $S_{n+2} \supseteq S_n \times C_2$ and $A_{n+4} \supseteq A_n \times V_4$. Also, $\operatorname{ed}_K S_1 = 0$, $\operatorname{ed}_K S_2 = 1$ and $\operatorname{ed}_K A_4 = 2$. □

To obtain an upper bound for $\operatorname{ed}_K S_n$, we make use of

THEOREM 8.2.16. *Let K be an infinite field, and let $f(X) \in K[X]$ be a monic polynomial with no multiple roots and degree $n \geq 3$. Then $f(X)$ is Tschirnhaus equivalent to a polynomial of the form*

$$g(X) = X^n + a_{n-2}X^{n-2} + \cdots + a_2X^2 + a_1X + a_1 \in K[X],$$

i.e., a polynomial in which the $(n-1)^{\text{th}}$ degree term is 0 and the coefficients in degrees 0 and 1 are equal.

First, we need a technical lemma:

LEMMA 8.2.17. *Let K be an infinite field and let $h(\mathbf{x}) \in K[\mathbf{x}] = K[x_1, \ldots, x_n]$. If the linear polynomial $\ell(\mathbf{x}) \in K[\mathbf{x}] \setminus K$ does not divide $h(\mathbf{x})$, then there is a point $\mathbf{a} \in K^n$ with $\ell(\mathbf{a}) = 0$ and $h(\mathbf{a}) \neq 0$.*

PROOF. We write $\ell(\mathbf{x}) = b_1x_1 + \cdots + b_nx_n + c$, where we may assume $b_1 \neq 0$.

Since $\ell \nmid h$, we have $h \notin \sqrt{(\ell)}$, and so, by the Hilbert Nulstellensatz (in section A.4 of Appendix A below), there is a maximal ideal $\mathfrak{m}$ in $K[\mathbf{x}]$ with $\ell \in \mathfrak{m}$ and $h \notin \mathfrak{m}$. Thus, in $L = K[\mathbf{x}]/\mathfrak{m}$ we have $\ell(\bar{x}_1, \ldots, \bar{x}_n) = 0$ and $h(\bar{x}_1, \ldots, \bar{x}_n) \neq 0$, from which we conclude that $h(-(b_2x_2 + \cdots + b_nx_n + c)/b_1, x_2, \ldots, x_n)$ is not the zero polynomial. Since K is infinite, this means that there is a point in which it is not zero. □

PROOF OF THEOREM 8.2.16. It is of course enough to find a $g(X)$ of the form $X^n + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$ with $a_0, a_1 \neq 0$, since a simple scaling will then give us $a_0 = a_1$:

Let $\theta_1, \ldots, \theta_n$ be the roots of $f(X)$, and let $y_0, \ldots, y_{n-1}$ be indeterminates. We define

$$g(\mathbf{y}, X) = \prod_{i=1}^{n} [X - (y_0 + y_1\theta_i + \cdots + y_{n-1}\theta_i^{n-1})] \in K[\mathbf{y}, X].$$

The coefficient to X^{n-1} in $g(\mathbf{y}, X)$ is

$$\ell(y_0, \ldots, y_{n-1}) = -(ny_0 + c_1y_1 + \cdots + c_{n-1}y_{n-1}),$$

where $c_1, \ldots, c_{n-1} \in K$.

The polynomials $-(x_1 + \cdots + x_n)$ and $h(\mathbf{x}) = e_n(\mathbf{x})e_{n-1}(\mathbf{x})d(\mathbf{x})$ (e_i being the i^{th} elementary symmetric symbol) satisfy the conditions of the Lemma, and since the substitution

$$x_i \mapsto y_0 + y_1\theta_i + \cdots + y_{n-1}\theta_i^{n-1}$$

is invertible (over $K(\theta_1, \ldots, \theta_n)$), so do the polynomials $\ell(\mathbf{y})$ and $h(\{\sum_i y_i\theta_j^i\}_j) \in K[\mathbf{y}]$. Thus, there is a point $\mathbf{a} \in K^n$ where $g(\mathbf{a}, X)$ has no multiple roots, degree-$(n-1)$ coefficient 0 and non-zero constant and first-order terms. □

COROLLARY 8.2.18. *The polynomial*

$$X^n + t_{n-2}X^{n-2} + \cdots + t_2X^2 + t_1X + t_1 \in K(t_1, \ldots, t_{n-2})[X],$$

where $n \geq 3$, is generic for S_n over any infinite field K. In particular, $\operatorname{ed}_{\mathbb{Q}} S_n \leq n - 2$.

In [B&R1, Thm. 6.5], it is proved that in fact $\operatorname{ed}_{\mathbb{Q}} S_n \leq n - 3$ for $n \geq 5$.

Concerning bounds on the essential dimension, we also prove the following simple result:

LEMMA 8.2.19. *Let K be a field and G a finite group. Then*

$$\operatorname{ed}_K G \leq [G : H] \cdot \operatorname{ed}_K H$$

for any *subgroup H of G.*

I.e., $\operatorname{ed}_K G/|G|$ does not grow with G.

PROOF. We let G act regularly on a set $\mathbf{t} = (t_\sigma)_{\sigma\in G}$ of indeterminates. Obviously, H then acts regularly on $\mathbf{t}' = (t_\tau)_{\tau\in H}$, and there exists a subfield F of $K(\mathbf{t}')$ such that $\operatorname{tr.deg}_K F = \operatorname{ed}_K H$ and H acts faithfully on F. Let $F' = \prod_{\sigma\in G} \sigma F$ be the composite in $K(\mathbf{t})$ of the images of F under the G-action. As $\tau F = F$ for $\tau \in H$, and $\sigma F \subseteq K(\sigma\mathbf{t}') = K(\{t_\tau\}_{\tau\in\sigma H})$ for $\sigma \in G$, there must be exactly $[G:H]$ distinct conjugates, with $\sigma F = \sigma' F$ if and $\sigma H = \sigma' H$, and $\sigma F \cap \sigma' F = K$ otherwise.

Now, F' is closed under the G-action, and this action is faithful: Let $\sigma \in G$ act trivially on F'. Then it in particular maps F to itself, and so $\sigma \in H$. But on F, H acts faithfully, meaning that $\sigma = 1$. □

REMARK. Reichstein has extended the notion of essential dimension from finite groups to algebraic groups. See [Re] and [Re&Y].

8.3. Lattices: Better Bounds

Following unpublished work by Buhler and Reichstein [B&R3], we will now describe an upper bound on the essential dimension of certain semi-direct product. In particular, we will improve the upper bound on $\operatorname{ed}_{\mathbb{Q}} C_n$, n odd, obtained in section 5.3, where we proved $\operatorname{ed}_{\mathbb{Q}} C_q \le p^{n-1}(p-1)/2$ for an odd prime power $q = p^n$.

Our goal is to prove

THEOREM 8.3.1. *Let $q = p^n$ be a prime power, and let φ denote the Euler φ-function. Then*

$$\operatorname{ed}_{\mathbb{Q}}(\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*) \le \varphi(p-1)p^{n-1}.$$

REMARKS. (1) In [B&R3], Theorem 8.3.1 (and the more general Proposition 8.3.5 below) is proved only for the cyclic group $\mathbb{Z}/q$ itself, and not for the semi-direct product. Our proof is a modification of Buhler and Reichstein's argument, which can be recovered simply by removing all references to τ below.

(2) For a cyclic group of prime order, the result is due to Hendrik Lenstra.

(3) It is trivial that $\varphi(p-1) \le (p-1)/2$, and unless p is a Fermat prime the inequality is strict. Thus, the Theorem improves the bound on $\operatorname{ed}_{\mathbb{Q}} C_n$ given by Smith's Theorem 5.3.5.

(4) From the Theorem, we get that $\operatorname{ed}_{\mathbb{Q}} C_8$ and $\operatorname{ed}_{\mathbb{Q}} D_8$ are both ≤ 4. This improves the bound of 5 implicit in the descriptions in Chapter 6.

EXAMPLE. Let $q = 7$. We know that $\operatorname{ed}_{\mathbb{Q}} C_7 > 1$, and so

$$\operatorname{ed}_{\mathbb{Q}} C_7 = \operatorname{ed}_{\mathbb{Q}} D_7 = \operatorname{ed}_{\mathbb{Q}} F_{21} = \operatorname{ed}_{\mathbb{Q}} F_{42} = 2.$$

The proof of Theorem 8.3.1 makes use of *multiplicative* group actions on rational function fields, as opposed to the linear actions we have considered above:

Let $\mathcal{L}$ be a *lattice*, i.e., a finitely generated free abelian group. Then the group ring $K[\mathcal{L}]$ is a domain, and if $\ell_1, \dots, \ell_n$ is a basis for $\mathcal{L}$, then $K[\mathcal{L}]$ is the Laurent polynomial ring in indeterminates $x_1, \dots, x_n$ corresponding to $\ell_1, \dots, \ell_n$. In particular, the quotient field $K(\mathcal{L})$ is a rational function field of transcendence degree equal to the rank of $\mathcal{L}$.

If the finite group G acts on $\mathcal{L}$, we call $\mathcal{L}$ a *G-lattice*, and clearly the action extends to $K(\mathcal{L})$. This is a *multiplicative* (or *monomial*) G-action on the function field $K(\mathcal{L})$.

EXAMPLES. (1) Let $C_2 = \langle\sigma\rangle$ act on $\mathbb{Z}$ by $\sigma\colon a \mapsto -a$. This translates to $\tau\colon x \mapsto 1/x$ on $K(x)$.

(2) Let $C_3 = \langle\tau\rangle$ act on $\mathbb{Z}^2$ by $\tau(a,b) = (-b, a-b)$. This translates to $\tau\colon x \mapsto y$, $y \mapsto 1/xy$ on $K(x,y)$, and we recognise this multiplicative action as the one considered in connection with A_4 above.

Multiplicative and linear G-action coincide in the case of a *permutation lattice*, i.e., a G-lattice $\mathcal{P}$ possessing a basis permuted by G. In this case, $K(\mathcal{P}) = K(V)$, where $V = K \otimes_{\mathbb{Z}} \mathcal{P}$.

It should be clear that there is a MULTIPLICATIVE NOETHER PROBLEM: Considering a faithful G-lattice $\mathcal{L}$, is the extension $K(\mathcal{L})^G/K$ rational?–and that an affirmative answer will give rise to generic polynomials in the case where K is infinite, by Proposition 1.1.5 from Chapter 1 and Exercise 8.6(1) below. It should also be clear that this problem has an interesting (i.e., non-trivial) generalisation: If G acts faithfully on both K and $\mathcal{L}$, it acts on $K(\mathcal{L})$ as well, and we can ask if $K(\mathcal{L})^G/K^G$ is rational. Unlike the corresponding question for semi-linear actions, which has an affirmative answer by the Invariant Basis Lemma, examples are known where $K(\mathcal{L})^G/K^G$ is *not* rational. Regarding this problem, we cite the following positive result (from [Vo2, Thm. 2]):

THEOREM 8.3.2. (VOSKRESENSKII) *If* $\operatorname{char} K = 0$ *and G is finite cyclic, the extension $K(\mathcal{L})^G/K^G$ is rational if and only if it is stably rational.*

Returning now to Theorem 8.3.1, we let $q = p^n$ be a power of the prime p and consider a field K of characteristic $\neq p$, such that the q^{th} cyclotomic extension $K(\mu_q)/K$ is cyclic. We denote the degree of $K(\mu_q)/K$ by D. Thus, $D = dp^e$, where $d \mid p-1$ and $e \leq n-1$.

If $f \in \mathbb{Z}$ is a primitive D^{th} root of unity modulo q, the Galois group $G_q = \operatorname{Gal}(K(\mu_q)/K)$ is generated by κ, where $\kappa\zeta = \zeta^f$ for $\zeta \in \mu_q$.

We are interested in the semi-direct product

$$C_q \rtimes C_D = \left\langle \sigma, \tau \mid \sigma^q = \tau^D = 1,\ \tau\sigma = \sigma^f\tau \right\rangle.$$

In order to get a bound on $\operatorname{ed}_K C_q \rtimes C_D$, we need a suitable faithful linear representation over K. We obtain one as follows:

Let $\mathbf{t} = (t_\zeta)_{\zeta\in\mu_q}$ be indeterminates indexed by μ_q, and define an action of $C_q \rtimes C_D$ on the function field $K(\mu_q)(\mathbf{t})$ by

$$\sigma\colon t_\zeta \mapsto \zeta t_\zeta \quad \text{and} \quad \tau\colon t_\zeta \mapsto t_{\kappa\zeta}, \quad \zeta \in \mu_q.$$

This action is defined over $K(\mu_q)$ instead of K, but we will correct that below.

Next, extend G_q's action from $K(\mu_q)$ to $K(\mu_q)(\mathbf{t})$ by

$$\kappa\colon t_\zeta \mapsto t_{\kappa\zeta}, \quad \zeta \in \mu_q.$$

Then difference between κ and τ is then that τ acts trivially on $K(\mu_q)$.

Since

$$\sigma\tau = \tau\sigma^f, \quad \sigma\kappa = \kappa\sigma \quad \text{and} \quad \tau\kappa = \kappa\tau,$$

we have an action of $G_q \times (C_q \rtimes C_D)$ on $K(\mu_q)(\mathbf{t})$, and this action is faithful.

By the Invariant Basis Lemma, the $K(\mu_q)$-vector space generated by $\mathbf{t}$ has a G_q-invariant basis $\mathbf{s} = (s_1, \dots, s_D)$, and $C_q \rtimes C_D$ then acts linearly on $K(\mathbf{s}) = K(\mathbf{t})^{G_q}$.

Consider now the group ring $\mathbb{Z}[\mu_q]$ as a lattice. To avoid confusion, we write the elements in $\mathbb{Z}[\mu_q]$ as $\sum_{\zeta\in\mu_q} a_\zeta e_\zeta$. We then have a G_q-action given by $\kappa\colon e_\zeta \mapsto e_{\kappa\zeta}$. Also, we have a G_q-equivariant map $\lambda\colon \mathbb{Z}[\mu_q] \to \mu_q$ defined by

$$\lambda\Big(\sum_{\zeta\in\mu_q} a_\zeta e_\zeta\Big) = \prod_{\zeta\in\mu_q} \zeta^{a_\zeta}.$$

A G_q-sublattice $\mathcal{L}$ of $\mathbb{Z}[\mu_q]$ is *non-degenerate*, if $\lambda\colon \mathcal{L} \to \mu_q$ is onto.

The key step in establishing Theorem 8.3.1 is the following Lemma:

LEMMA 8.3.3. *Let $\mathcal{L} \subseteq \mathbb{Z}[\mu_q]$ be a non-degenerate G_q-sublattice. Then*

$$\operatorname{ed}_K(C_q \rtimes C_D) \le \operatorname{rank}\mathcal{L}.$$

PROOF. We consider $K(\mu_q)(\mathcal{L})$ as a subfield of $K(\mu_q)(\mathbf{t})$.

For convenience, we denote the monomial $\prod_{\zeta\in\mu_q} t_\zeta^{a_\zeta}$ corresponding to $a = \sum_{\zeta\in\mu_q} a_\zeta e_\zeta$ by t^a, and see that

$$\kappa t^a = \tau t^a = t^{\kappa a} \quad \text{and} \quad \sigma t^a = \lambda(a) t^a.$$

Thus, $K(\mu_q)(\mathcal{L})$ is closed under the $G_q \times (C_q \rtimes C_D)$-action. Moreover, this action is faithful:

Assume that $\chi \in G_q$ and $\rho \in C_q \rtimes C_D$ act identically on $K(\mu_q)(\mathcal{L})$. As $K(\mu_q)(\mathcal{L})$ contains $K(\mu_q)$, where G_q acts faithfully and $C_q \rtimes C_D$ acts trivially, we see that $\chi = 1$, and that therefore ρ acts trivially on $K(\mu_q)(\mathcal{L})$. Write $\rho = \tau^i\sigma^j$ with $0 \le i < q$ and $0 \le j < d$, and pick $a \in \mathcal{L}$ such that $\lambda(a)$ is a primitive q^{th} root of unity. Then

$$\rho(t^a) = \lambda(a)^j t^{\kappa^i a} = t^a,$$

meaning that $j = 0$ and $\rho = \tau^i$. But on the monomials, the C_D-action is faithful, and so $\rho = 1$.

Thus, $C_q \rtimes C_D$ acts faithfully on $K(\mu_q)(\mathcal{L})^{G_q} \subseteq K(\mathbf{s})$. And by construction, $\operatorname{tr.deg}_K K(\mu_q)(\mathcal{L}) = \operatorname{rank}\mathcal{L}$. □

It only remains to find a non-degenerate G_q-sublattice of $\mathbb{Z}[\mu_q]$ of the right rank:

LEMMA 8.3.4. *Let G be a cyclic subgroup of $\operatorname{Aut}\mu_q$ of order $D = dp^e$ as above. Then there exists a non-degenerate G-sublattice of $\mathbb{Z}[\mu_q]$ of rank $\varphi(d)p^e$.*

PROOF. Again, we let f be a primitive D^{th} root of unity, such that a generator κ for G is given by $\kappa\zeta = \zeta^f$ for $\zeta \in \mu_q$.

First we note that f is a primitive d^{th} root of unity modulo p: It has order dividing d, since $f^d \equiv f^D \equiv 1 \pmod p$. And on the other hand, if $f^c \equiv 1 \pmod p$ for some $c \in \{1, \dots, d-1\}$, we get $f^c = 1 + pi$ for an i, and so $f^{cp^{n-1}} \equiv 1 \pmod q$, meaning that D must divide cp^{n-1}, contradicting $0 < c < d$.

Next, we define

$$P(t) = \prod_{j=0}^{e} \Phi_{dp^j}(t) \quad \text{and} \quad Q(t) = \prod_{j=0}^{e} \prod_{\substack{k|d \\ k<d}} \Phi_{kp^j},$$

where $\Phi_m(t)$ is the m^{th} cyclotomic polynomial over $\mathbb{Q}$. Then $P(t)Q(t) = t^D - 1$, and $Q(t)$ consists of all the factors $\Phi_m(t)$ of $t^D - 1$ with $p \nmid \Phi_m(f)$. Thus, $p \nmid Q(f)$. Also, $\deg P(t) = \varphi(d)p^e$.

We can make $\mathbb{Z}[t]/(t^D - 1)$ into a G_q-lattice by letting κ act as multiplication by t. If $\zeta \in \mu_q$ is a primitive q^{th} root of unity, the map

$$\sum_{i=0}^{D-1} a_i t^i \mapsto \sum_{i=0}^{D-1} a_i e_{\kappa^i \zeta}$$

is then a G-equivariant monomorphism from $\mathbb{Z}[t]/(t^D - 1)$ into $\mathbb{Z}[\mu_q]$.

Also, $\mathbb{Z}[t]/(P(t))$ is a G_q-lattice when κ acts as multiplication by t, and $g(t) \mapsto g(t)Q(t)$ is a G-equivariant monomorphism from $\mathbb{Z}[t]/(P(t))$ into $\mathbb{Z}[t]/(t^D - 1)$. We claim that the image of $\mathbb{Z}[t]/(P(t))$ in $\mathbb{Z}[\mu_q]$ is non-degenerate. This proves the Lemma, since clearly $\mathbb{Z}[t]/(P(t))$ has rank equal to $\deg P(t)$.

So, look at the element 1 in $\mathbb{Z}[t]/(P(t))$. It is easy to see that $\lambda(g) = \zeta^{g(f)}$ for any $g \in \mathbb{Z}[t]/(t^D - 1)$ considered as an element in $\mathbb{Z}[\mu_q]$. Thus, the image of $1 \in \mathbb{Z}[t]/(P(t))$ has λ-value $\zeta^{Q(f)}$, and this is a primitive q^{th} root of unity by assumption, making $\mathbb{Z}[t]/(P(t))$ non-degenerate. □

PROPOSITION 8.3.5. *Assume that $K(\mu_q)/K$ is cyclic of degree $D = dp^e$, where $d \mid p-1$ and $e \leq n-1$, and let $G_q = \mathrm{Gal}(K(\mu_q)/K)$ act on C_q by cyclotomic action (i.e., by identifying C_q and μ_q). Then*

$$\mathrm{ed}_K(C_q \rtimes G_q) \leq \varphi(d)p^e.$$

PROOF OF THEOREM 8.3.1. For odd p, the Theorem follows from Proposition 8.3.5. For $p = 2$, we note that $\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*$ has a faithful linear representation over $\mathbb{Q}$ of degree $q/2$, and that we therefore have

$$\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*) \leq q/2.$$

□

REMARKS. (1) Using Corollary 8.2.9, it is of course now a simple matter to bound the essential dimension of any finite abelian group over $\mathbb{Q}$.

(2) Similarly, by using that $D_{m\times n} \hookrightarrow D_m \times D_n$ (with D_2 understood to be C_2), we can bound $\mathrm{ed}_{\mathbb{Q}} D_A$ for any finite abelian group A, and see that the bound obtained is the same as for A itself.

EXAMPLE. Consider the case $q = 7$ over $\mathbb{Q}$. Then, as stated earlier, $\mathrm{ed}_{\mathbb{Q}} C_7 = 2$. Let us go through the argument above in this special case, to see what is actually involved. (We restrict ourselves to C_7 rather than $C_7 \rtimes C_6$ for simplicity. However, remember that κ and τ act identically on the indeterminates.)

We have $D = d = 6$, and can pick $f = 3$. Let $\zeta = e^{2\pi i/7}$ be a primitive 7^{th} root of unity. On the indeterminates $\mathbf{t} = (t_1, t_\zeta, \ldots, t_{\zeta^6})$ we then have σ and κ acting by

$$\sigma\colon t_\eta \mapsto \eta t_\eta \quad \text{and} \quad \kappa\colon t_\eta \mapsto t_{\eta^3} \quad \text{for } \eta \in \mu_7.$$

We get

$$P(t) = t^2 - t + 1 \quad \text{and} \quad Q(t) = t^4 + t^3 - t - 1,$$

from which it follows that the G_7-sublattice $\mathcal{L}$ of $\mathbb{Z}[\mu_7]$ is generated by

$$e_{\zeta^4} + e_{\zeta^6} - e_{\zeta^3} - e_\zeta \quad \text{and} \quad e_{\zeta^5} + e_{\zeta^4} - e_{\zeta^2} - e_{\zeta^3},$$

and hence that

$$\mathbb{Q}(\mu_7)(\mathcal{L}) = \mathbb{Q}(\mu_7)\left(\frac{t_{\zeta^4} t_{\zeta^6}}{t_{\zeta^3} t_\zeta}, \frac{t_{\zeta^5} t_{\zeta^4}}{t_{\zeta^2} t_{\zeta^3}}\right) = \mathbb{Q}(\mu_7)(x, y),$$

with

$$\sigma\colon x \mapsto \zeta^6 x, \quad y \mapsto \zeta^4 y, \quad \text{and} \quad \kappa\colon x \mapsto y, \quad y \mapsto y/x.$$

The essential dimension of C_7 over $\mathbb{Q}$ is then realised (inside $\mathbb{Q}(\mu_7)(\mathbf{t})^{G_7}$) by $\mathbb{Q}(\mu_7)(x,y)^{G_7}/\mathbb{Q}(\mu_7)(x,y)^{G_7 \times C_7}$, and there exists a generic polynomial with two parameters if the fixed field $\mathbb{Q}(\mu_7)(x,y)^{G_7 \times C_7}$ is rational over $\mathbb{Q}$.

It is straightforward to find the fixed field of C_7:

$$\mathbb{Q}(\mu_7)(x,y)^{C_7} = \mathbb{Q}(\mu_7)(x^7, x^4 y) = \mathbb{Q}(\mu_7)(u, v),$$

where

$$\kappa\colon u \mapsto \frac{v^7}{u^4}, \quad v \mapsto \frac{v^5}{u^3}, \quad \text{and} \quad \zeta \mapsto \zeta^3.$$

The question is then: Is $\mathbb{Q}(\mu_7)(u,v)^{G_7}/\mathbb{Q}$ rational? If this is answered (explicitly) in the affirmative, the actual *construction* of a generic C_7-polynomial with two parameters will boil down to linear algebra, cf. the Remark on p. 37.

By Voskresenskii's Theorem 8.3.2 above, $\mathbb{Q}(\mu_7)(u,v)^{G_7}/\mathbb{Q}$ is rational if and only if it is stably rational. We will prove that the extension *is* stably rational, and hence that there exists a two-parameter generic C_7-polynomial over $\mathbb{Q}$. Unfortunately, this result is completely non-constructive. and so we are not able to actually find the polynomial.

Consider a short-exact sequence of G_7-lattices

$$0 \to \mathcal{L}_1 \to \mathcal{L}_2 \to \mathcal{P} \to 0,$$

where G_7 acts faithfully on $\mathcal{L}_1$ and $\mathcal{L}_2$, while $\mathcal{P}$ is a permutation lattice. By Exercise 8.7 below, the extension $\mathbb{Q}(\mu_7)(\mathcal{L}_2)^{G_7}/\mathbb{Q}(\mu_7)(\mathcal{L}_1)^{G_7}$ is rational, and hence $\mathbb{Q}(\mu_7)(\mathcal{L}_1)^{G_7}/\mathbb{Q}$ is stably rational if and only if $\mathbb{Q}(\mu_7)(\mathcal{L}_2)^{G_7}/\mathbb{Q}$ is.

In this case, we start with the lattice $\mathbb{Z}U + \mathbb{Z}V$, where $\kappa U = 7V - 4U$ and $\kappa V = 5V - 3U$. Replacing the basis (U, V) with $(X, Y) = (U - V, 2V - U)$, we get instead $\kappa X = Y$ and $\kappa Y = Y - X$, and so the lattice is just $\mathbb{Z}[t]/(t^2 - t + 1)$ with κ acting as multiplication by t.

Consider the short-exact sequences

$$0 \to \frac{\mathbb{Z}[t]}{(t^2-t+1)} \to \frac{\mathbb{Z}[t]}{(t^2-t+1)(t^3-1)} \to \frac{\mathbb{Z}[t]}{(t^3-1)} \to 0,$$
$$0 \to \frac{\mathbb{Z}[t]}{(t^2-t+1)(t^2+t+1)} \to \frac{\mathbb{Z}[t]}{(t^2-t+1)(t^3-1)} \to \frac{\mathbb{Z}[t]}{(t-1)} \to 0,$$
$$0 \to \frac{\mathbb{Z}[t]}{(t^2-t+1)(t^2+t+1)} \to \frac{\mathbb{Z}[t]}{(t^6-1)} \to \frac{\mathbb{Z}[t]}{(t^2-1)} \to 0.$$

Applying them in order, we 'reduce' our lattice to the permutation lattice $\mathcal{M} = \mathbb{Z}[t]/(t^6-1)$, where the field $\mathbb{Q}(\mu_7)(\mathcal{M})^{G_7}$ is trivially rational over $\mathbb{Q}$ by the Invariant Basis Lemma. Thus, $\mathbb{Q}(\mu_7)(u,v)^{G_7}/\mathbb{Q}$ is rational.

8.4. p-Groups in Characteristic p, Revisited

We now interpret the results of section 5.6 in Chapter 5 in terms of essential dimension:

THEOREM 8.4.1. *Let G be a p-group for some prime p, and let the order of the Frattini subgroup $\Phi(G)$ be p^e. Then*

$$\operatorname{ed}_{\mathbb{F}_p(u)} G \leq e+1,$$

where u is an indeterminate. Moreover,

$$\operatorname{ed}_{\mathbb{F}_p} G \leq e+2$$

if the group G is non-cyclic, whereas

$$\operatorname{ed}_{\mathbb{F}_p} C_{p^n} \leq n.$$

THEOREM 8.4.2. *Let $q = p^n$ be a prime power, and let C_d be a cyclic subgroup of $(\mathbb{Z}/q)^*$. Then*

$$\operatorname{ed}_{\mathbb{F}_p}(\mathbb{Z}/q \rtimes C_d) \leq n.$$

This shows that p-groups (and some related groups) have very low essential dimensions in characteristic p.

As for lower bounds: An elementary Abelian p-group A has essential dimension 1 over K if and only if $|K| \geq |A|$, and otherwise 2. For all other groups, the essential dimension is at least 2 over any field of characteristic p.

8.5. Generic Dimension

The essential dimension gives a bound on the number of parameters needed in a generic polynomial. For completeness' sake, we introduce the concept of *generic dimension*:

DEFINITION 8.5.1. Let K be a field and G a finite group. The *generic dimension* for G over K, written $\operatorname{gd}_K G$, is then the minimal number of parameters in a generic polynomial for G over K, or ∞ if no generic polynomial exists.

We then clearly have

PROPOSITION 8.5.2. $\operatorname{ed}_K G \leq \operatorname{gd}_K G$.

No examples seem to be known of $\operatorname{ed}_K G < \operatorname{gd}_K G$, except of course when $\operatorname{gd}_K G = \infty$. We may therefore propose a

CONJECTURE. If $\mathrm{gd}_K G < \infty$, then $\mathrm{ed}_K G = \mathrm{gd}_K G$.

Notice that many of our upper bounds on essential dimensions are in fact upper bounds on the generic dimension. Thus, for instance

PROPOSITION 8.5.3. *Let K be an infinite field of prime characteristic p, and let G be a p-group with $|\Phi(G)| = p^e$. Then*

$$\mathrm{gd}_K G \leq e + 1.$$

and

PROPOSITION 8.5.4. *For $n > 3$, we have*

$$\lfloor n/2 \rfloor \leq \mathrm{gd}_K S_n \leq n - 2$$

for any field K of characteristic 0.

Also, from Exercise 5.6 in Chapter 5, we get the analogue of Corollary 8.2.9 for generic dimension:

PROPOSITION 8.5.5. *Let K be an infinite field, and let G and H be finite groups. Then*

$$\mathrm{gd}_K G,\, \mathrm{gd}_K H \leq \mathrm{gd}_K(G \times H) \leq \mathrm{gd}_K G + \mathrm{gd}_K H.$$

Note that a result like $\mathrm{gd}_K H \leq \mathrm{gd}_K G$ for $H \subseteq G$ is not generally true (consider e.g. C_8 and D_8 over $\mathbb{Q}$). And it is by no means obvious whether it is true even assuming both generic dimensions to be finite.

For semi-direct products, Exercises 7.1 and 7.2 in Chapter 7, combined with Proposition 5.1.7 from Chapter 5, gives us

PROPOSITION 8.5.6. *Let K be an infinite field, and let G and A be finite groups of mutually prime orders $|G|$ and $|A|$. Moreover, assume that A is Abelian, and that G acts on A as automorphisms. Let $N \subseteq G$ be the kernel of this action. Then*

$$\mathrm{gd}_K(A \rtimes G) \leq \mathrm{gd}_K(G) + [G : N] \cdot \mathrm{gd}_K(A).$$

This is similar to the result of Exercise 8.4 below.

Finally, Lenstra's result (stated in the Introduction and proved in Chapters 2 and 5) can be restated as

THEOREM 8.5.7. (LENSTRA) *For a finite Abelian group A, we have $\mathrm{gd}_{\mathbb{Q}} A = \infty$ if and only if A contains an element of order 8.*

Known bounds. We conclude this section by a brief survey summarizing the present knowledge about the generic dimension over $\mathbb{Q}$ of groups of small degree. For the three groups $\mathrm{PSL}(2,7)$, A_7 and Q_{16}, it is unknown (to the authors) whether the generic dimension is finite or infinite.

(8.5.8) Let G be a transitive subgroup of S_n, where $2 \leq n \leq 7$:

For $n = 2$, we have $G = C_2$, and we know that

$$\mathrm{gd}_{\mathbb{Q}}(C_2) = 1.$$

For $n = 3$, G is either C_3 or S_3, and we have

$$\mathrm{gd}_{\mathbb{Q}}(C_3) = \mathrm{gd}_{\mathbb{Q}}(S_3) = 1.$$

For $n = 4$, G is one of V_4, C_4, D_4, A_4 and S_4, and we have

$$\mathrm{gd}_{\mathbb{Q}}(V_4) = \mathrm{gd}_{\mathbb{Q}}(C_4) = \mathrm{gd}_{\mathbb{Q}}(D_4) = \mathrm{gd}_{\mathbb{Q}}(A_4) = \mathrm{gd}_{\mathbb{Q}}(S_4) = 2.$$

For $n = 5$, G is one of C_5, D_5, F_{20}, A_5 and S_5, and we have

$$\mathrm{gd}_{\mathbb{Q}}(C_5) = \mathrm{gd}_{\mathbb{Q}}(D_5) = \mathrm{gd}_{\mathbb{Q}}(F_{20}) = \mathrm{gd}_{\mathbb{Q}}(A_5) = \mathrm{gd}_{\mathbb{Q}}(S_5) = 2.$$

For $n = 7$, G is one of C_7, D_7, F_{21}, F_{42}, $\mathrm{PSL}(2,7)$, A_7 and S_7, and we have

$$\begin{gathered}\mathrm{gd}_{\mathbb{Q}}(C_7) = 2,\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(D_7) \le 5,\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(F_{21}) \le 7,\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(F_{42}) \le 14,\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(\mathrm{PSL}(2,7)),\ \mathrm{gd}_{\mathbb{Q}}(A_7),\\ 3 \le \mathrm{gd}_{\mathbb{Q}}(S_7) \le 5.\end{gathered}$$

(8.5.9) For the four groups of order 16 and exponent 8, we know that

$$\begin{gathered}2 \le \mathrm{gd}_{\mathbb{Q}}(QD_8),\ \mathrm{gd}_{\mathbb{Q}}(D_8) \le 5,\\ 3 \le \mathrm{gd}_{\mathbb{Q}}(M_{16}) \le 5,\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(Q_{16}).\end{gathered}$$

The result for M_{16} follows from [Le8, Thm. 6] and Exercise 8.9. It is not known whether Q_{16} has a generic polynomial.

(8.5.10) For the groups of order < 24 the generic dimension is finite except for C_8, $C_8 \times C_2$, C_{16} and perhaps Q_{16}. For some individual groups the exact value of the generic dimension is given in Exercise 8.15 below.

(8.5.11) For the groups of order 24, there is only one group for which the question of existence of a generic polynomial is unanswered, namely $\mathrm{SL}(2,3)$. For the remaining groups, the generic dimension is finite, except for C_{24} and the semi-direct product $C_3 \rtimes C_8$.

It is a little laborious, but not fundamentally difficult, to establish bounds on the generic dimensions of 'small' groups, say of order < 32, except of course Q_{16} and $\mathrm{SL}(2,3)$.

(8.5.12) For infinite families of groups, we have already covered S_n in Proposition 8.5.4 above. The alternating groups A_n, $n \ge 6$, satisfy

$$2\lfloor n/4 \rfloor \le \mathrm{gd}_{\mathbb{Q}}(A_n),$$

but it is not known whether generic polynomials exist.

If n is odd with prime factorisation

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

we have

$$\begin{aligned}2 \le \mathrm{gd}_{\mathbb{Q}}(C_n) &\le \frac{1}{2}\big(\varphi(p_1^{e_1}) + \cdots + \varphi(p_r^{e_r}))\big),\\ 2 \le \mathrm{gd}_{\mathbb{Q}}(D_n) &\le 1 + \big(\varphi(p_1^{e_1}) + \cdots + \varphi(p_r^{e_r}))\big).\end{aligned}$$

For highly composite n, these bounds are relatively low.

Exercises

EXERCISE 8.1. (1) Let G be an *infinite* subgroup of $\mathrm{Aut}_K K(x,y)$, where x and y are indeterminates. Prove that $K(x,y)^G/K$ is rational. (In particular, by combining this with the the Remark on p. 23, we get a result by Noether: If G is a subgroup of $\mathrm{GL}_2(K)$, then $K(x,y)^G/K$ is rational.)

(2) Let K be an infinite field. Find $K(x,y)^G$ for $G = \mathrm{SL}_2(K)$ and $\mathrm{GL}_2(K)$ (with linear action), and for $G = \mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z})$ (with monomial action).

EXERCISE 8.2. Let K be an infinite field, and let $G \hookrightarrow \mathrm{GL}_K(V)$ be a faithful linear representation of the finite group G. Prove that there is a generic G-polynomial over K with $\mathrm{ed}_K G$ parameters if and only if the essential dimension can be realised inside $K(V)/K(V)^G$ by a G-extension F/E with E/K rational.

In particular, prove that G has a one-parameter generic polynomial over K if and only if $\mathrm{ed}_K G = 1$.

EXERCISE 8.3. Let L/K be a finite Galois extension. Prove that

$$\mathrm{ed}_K G \leq [L:K] \cdot \mathrm{ed}_L G$$

for *any* finite group G.

EXERCISE 8.4. Let G and N be finite groups, and assume that G acts on N with kernel H. Prove that

$$\mathrm{ed}_K(N \rtimes G) \leq [G:H] \cdot \mathrm{ed}_K N + \mathrm{ed}_K G.$$

QUESTION. Let G be a finite group, and let $N \lhd G$ be a normal subgroup. Is

$$\mathrm{ed}_K(G/N) \leq \mathrm{ed}_K G\,?$$

(At first glance, this looks plausible, and it would give another way of producing lower bounds. For instance, it would imply $\mathrm{ed}_K G \geq n$ whenever G is a p-group minimally generated by n elements, and K is a field of characteristic 0. Unfortunately, it is known to fail for algebraic groups, cf. [Re, Ex. 3.9 + Thm. 9.3], which would indicate that it probably does not work for finite groups either.)

EXERCISE 8.5. By Lemma 8.2.19, we have $\mathrm{ed}_{\mathbb{Q}} S_n \leq 2\,\mathrm{ed}_{\mathbb{Q}} A_n$. Is this an improvement over our previous results?

EXERCISE 8.6. (1) Let G be a finite group. Prove that any G-lattice can be embedded into a permutation G-lattice. [Hint: The proof of Proposition 1.1.4 in Chapter 1.]

(2) Consider the monomial action of $C_4 = \langle\sigma\rangle$ on $\mathbb{Q}(x,y)$ given by $\sigma\colon x \mapsto y \mapsto 1/x$. Prove that $\mathbb{Q}(x,y)^{C_4}/\mathbb{Q}$ is rational. [Hint: Look at $(x-1)/(x+1)$.]

EXERCISE 8.7. Let G be a finite group, and let $\mathcal{M}$ be a G-lattice. Let $\mathcal{L} \subseteq \mathcal{M}$ be a G-sublattice such that G acts faithfully on $\mathcal{L}$, *and* such that the factor group $\mathcal{P}$ is a permutation lattice with the induced G-action. Also, let K be a field with a (not necessarily faithful) G-action. Prove that the extension $K(\mathcal{M})^G/K(\mathcal{L})^G$ is rational. [Hint: The Invariant Basis Theorem applied over $K(\mathcal{L})$.]

EXERCISE 8.8. Prove that $\mathrm{ed}_{\mathbb{Q}} Q_{2^n} \leq 2^{n-1}$ for $n \geq 3$.

EXERCISE 8.9. Prove that $3 \leq \operatorname{ed}_{\mathbb{Q}} M_{2^n} \leq 2^{n-2}$ for $n \geq 4$.

EXERCISE 8.10. Let p be an odd prime, and let H_{p^3} be the Heisenberg group from Chapter 6. Prove that

$$\operatorname{ed}_{\mathbb{Q}} H_{p^3} \leq p^2 - p.$$

EXERCISE 8.11. Let p be a prime, and let P be a group of order p^n. Prove that $\operatorname{ed}_{\mathbb{Q}} P \leq p^{n-1}\varphi(p-1)$.

EXERCISE 8.12. Let the notation be as in section 8.3.

(1) Prove that $K(\mu_q)(\mathcal{L})^{C_q \times G_q}/K$ is rational if and only if the extension $K(\mu_q)(\mathcal{L})^{C_q}/K(\mu_q)$ has a generating transcendence basis consisting of κ-invariant elements.

(2) Prove that the extension $K(\mu_q)(\mathcal{L})^{C_q}/K(\mu_q)$ is always rational, and in fact of the form $K(\mu_q)(\mathcal{L}')$ for a G_q-sublattice $\mathcal{L}'$ of $\mathcal{L}$.

(3) Prove that the lattice $\mathcal{L}'$ from point (2) is isomorphic to $\mathcal{L}$ (as a G_q-lattice) if f can be chosen with $P(f) = q$. Then prove that this is possible for $K = \mathbb{Q}$ and $q = 9$, 11 and 13.

(3) Prove that $\mathbb{Q}(\mu_q)(\mathcal{L})^{G_q}/\mathbb{Q}$ is stably rational for $q = 9$, 11 and 13, and formulate the corresponding existence theorems for generic polynomials.

EXERCISE 8.13. Find a one-parameter generic polynomial for C_3 over $\mathbb{Q}$ using the construction of section 8.3.

EXERCISE 8.14. Let p and q be distinct primes with $p > 3$. Prove that

$$\operatorname{ed}_{\mathbb{Q}(\mu_q)} C_p \geq 2.$$

EXERCISE 8.15. Show that the groups C_{10}, C_{12}, C_{14}, C_{15} and C_{21} all have generic dimension 3 over $\mathbb{Q}$. [Hint: Theorem 8.2.11 applied over $\mathbb{Q}$ or $\mathbb{Q}(\mu_3)$.]

EXERCISE 8.16. Find the essential dimensions over $\mathbb{Q}$ of the dihedral groups D_{15} and D_{21}. [Hint: See Exercise 8.15 above.] Then demonstrate the existence of a generic D_{15}-polynomial over $\mathbb{Q}$ with exactly $\operatorname{ed}_{\mathbb{Q}} D_{15}$ parameters.

EXERCISE 8.17. Consider the semi-direct product $C_3 \rtimes Q_8$, where Q_8 acts non-trivially on C_3. Prove the existence of a five-parameter generic polynomial over $\mathbb{Q}$. [Hint: A $C_3 \rtimes Q_8$-extension is the composite of a Q_8- and an S_3-extension.]

CONJECTURE. $\operatorname{ed}_K D_n = \operatorname{ed}_K C_n$ for any field K of characteristic 0 and any odd number n. (This conjecture is supported by Theorem 8.3.1, and Hashimoto and Miyake's result from Chapter 7.)

OPEN PROBLEM. Colliot-Thélène has given the quotient field K of

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

as an example of an extension of $\mathbb{Q}$ that is unirational but not rational. By Proposition 8.1.1, it can be realised as a subfield of $\mathbb{Q}(s, t)$, and it is clear that $\mathbb{Q}(s, t)/K$ is then a finite extension. Is there a non-rational subextension $L/\mathbb{Q}$ of $\mathbb{Q}(s, t)/\mathbb{Q}$ (possibly isomorphic to $K/\mathbb{Q}$) such that $\mathbb{Q}(s, t)/L$ is a Galois extension? If so, with what Galois group?

APPENDIX A

Technical Results

This appendix contains various results and definitions that are of relevance to the main text but did not fit into it. With the exception of the section on linear disjointness, which depends on the use of tensor products, the sections can be read independently.

A.1. The 'Seen One, Seen Them All' Lemma

If M/K is a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$, and $\pi\colon E \to G$ is an epimorphism[1] of the finite group E onto G, we can ask whether there exists a Galois extension F/K with $M \subseteq F$ and $\mathrm{Gal}(F/K) \simeq E$, such that the restriction map $\mathrm{res}\colon \mathrm{Gal}(F/K) \to G$ corresponds to π, i.e., such that $\mathrm{res} = \pi \circ \varphi$ for a suitable choice of isomorphism $\varphi\colon \mathrm{Gal}(F/K) \simeq E$. This is the (*Galois theoretical*) *embedding problem* given by M/K and π, and in the case of an affirmative answer, we say that F/K is a *solution* to the embedding problem, and that $M/K \subseteq F/K$ is an *embedding along* π.

Clearly, embeddings along epimorphisms allow us to build up Galois extensions step by step.

Now, let p be a prime, and let K be a field of characteristic $\neq p$ containing the primitive p^{th} roots of unity μ_p. Also, let M/K be finite Galois with Galois group $G = \mathrm{Gal}(M/K)$, and let $\pi\colon E \to G$ be an epimorphism with kernel of order p. Then we have

LEMMA A.1.1. *Assume that* $\pi\colon E \to G$ *is* central*, i.e.,* $\ker\pi \subseteq Z(E)$*, and* non-split*, i.e.,* $\ker\pi$ *is not a direct factor of* E*, and let* $M/K \subseteq F/K = M(\sqrt[p]{\omega})/K$*,* $\omega \in M^*$*, be an embedding along* π*. Then all embeddings along* π *are* $M/K \subseteq M(\sqrt[p]{r\omega})/K$ *for* $r \in K^*$*.*[2]

PROOF. Let $r \in K^*$. If $r \in (M^*)^p$, we have $M(\sqrt[p]{r\omega}) = M(\sqrt[p]{\omega})$, and there is nothing to prove. Hence, we may assume $r \notin (M^*)^p$. Then

$$\mathrm{Gal}(M(\sqrt[p]{\omega}, \sqrt[p]{r})/K) = E \times C_p,$$

where

$$E = \mathrm{Gal}(M(\sqrt[p]{\omega}, \sqrt[p]{r})/K(\sqrt[p]{r}))$$

[1] A surjective homomorphism

[2] That is, these are all embeddings along π and every embedding along π has this form. Of course, different r's may give the same embedding.

and

$$C_p = \mathrm{Gal}(M(\sqrt[p]{\omega}, \sqrt[p]{r})/M(\sqrt[p]{\omega})).$$

Let $\zeta \in \mu_p$ be a primitve p^{th} root of unity, and let $\kappa \in E$ and $\kappa' \in C_p$ be given by

$$\kappa \sqrt[p]{\omega} = \zeta \sqrt[p]{\omega} \quad \text{and} \quad \kappa' \sqrt[p]{r} = \zeta^{-1} \sqrt[p]{r},$$

respectively. Then $M(\sqrt[p]{r\omega})$ is the fixed field of $(\kappa, \kappa') \in E \times C_p$. Also, (κ, κ') is central in $E \times C_p$, and so $M(\sqrt[p]{r\omega})/K$ is Galois with Galois group $E \times C_p/\langle(\kappa, \kappa')\rangle$. This group can be identified with E by letting $e \in E$ correspond to the coset of $(e, 1) \in E \times C_p$. Thus, $M/K \subseteq M(\sqrt[p]{r\omega})/K$ is an embedding along π.

Conversely, let $M/K \subseteq M(\sqrt[p]{\lambda})/K$, $\lambda \in M^*$, be an embedding along π. If $M(\sqrt[p]{\omega}) = M(\sqrt[p]{\lambda})$ there is nothing to prove. Hence, assume $M(\sqrt[p]{\omega}) \neq M(\sqrt[p]{\lambda})$. Then $M(\sqrt[p]{\omega}, \sqrt[p]{\lambda})/K$ is Galois with Galois group

$$E \curlywedge E := \{(e, f) \in E \times E \mid e|_M = f|_M\} \simeq E \times C_p,$$

where the factors are $E = \{(e, e) \mid e \in E\}$ and $C_p = \langle(1, \kappa)\rangle$, with κ being a generator for $\mathrm{Gal}(M(\sqrt[p]{\omega}, \sqrt[p]{\lambda})/M(\sqrt[p]{\omega}))$. The fixed field of E is a C_p-extension of K, i.e., $K(\sqrt[p]{r})$ for some $r \in K^*$, and so $M(\sqrt[p]{\lambda}) = M(\sqrt[p]{r^i\omega})$ for some $i \in \{1, \ldots, p-1\}$. □

We will first and foremost use Lemma A.1.1 in the case $p = 2$, where π is necessarily central.

Remarks. (1) The notation $(M^*)^p$ used in the above proof to denote the set of p^{th} powers in M^* will be our standard notation with respect to a field M. Furthermore, for elements a and b in M^*, we say that a and b are *p-equivalent*, written $a =_p b$, if the residue classes $\bar{a}$ and $\bar{b}$ in $M^*/(M^*)^p$ are equal. Also, we say that elements $a_1, \ldots, a_n \in M^*$ are *p-independent*, if the p-equivalence classes are linearly independent in the $\mathbb{F}_p$-vector space $M^*/(M^*)^p$.

If $p = 2$, we say *quadratically equivalent*, *square class* and *quadratically independent* instead of 2-equivalent, 2-equivalence class and 2-independent.

(2) Lemma A.1.1 remains valid if M/K and F/K are assumed to be Galois algebras, cf. section 4.3 in Chapter 4, with the understanding that $M(\sqrt[p]{\omega})$ is then taken to be the ring $M[t]/(t^p - \omega)$. In that case, it is not necessary to assume $\pi\colon E \to G$ non-split.

(3) The embedding problem considered in Lemma A.1.1 is an example of a *Brauer type embedding problem*. Such embedding problems have been extensively studied, most notably for $p = 2$. References can be found in Chapter 6, in particular in the Remark on p. 134.

The characteristic p case. Let M/K be a G-extension in prime characteristic p, and let $\pi\colon E \to G$ be, as in Lemma A.1.1, be central and non-split with $\ker \pi \simeq C_p$. Then the embedding problem given by M/K and $\pi\colon E \to G$ has a solution, and as above we can describe all the solutions if we know one. For use in Chapter 5, we will prove this result here. Our reference is Witt's classical paper [Wi1] from 1936.

We pick an isomorphism $\iota\colon \mathbb{F}_p \simeq \ker \pi$ and get a short-exact sequence

$$0 \to \mathbb{F}_p \underset{\iota}{\longrightarrow} E \underset{\pi}{\longrightarrow} G \to 1. \tag{A.1.1}$$

A map $s\colon G \to E$ with $\pi \circ s = 1_G$ is called a *section* and gives rise to a map $c\colon G \times G \to \mathbb{F}_p$ by

$$\iota(c_{\sigma,\tau}) = s_\sigma s_\tau s_{\sigma\tau}^{-1},$$

cf. [Wei, §5–1]. This map is called a *factor system* and satisfies

$$c_{\rho,\sigma} + c_{\rho\sigma,\tau} = \rho c_{\sigma,\tau} + c_{\rho,\sigma\tau}.$$

(This comes from the associative law in E.) Our assumption about (A.1.1) being non-split is equivalent to saying that s cannot be picked to be a homomorphism.

LEMMA A.1.2. *Suppose that M/K is a Galois extension with Galois group $G = \mathrm{Gal}(M/K)$. Then the following hold, cf.* [Wei, Cor. 3–1–4]*:*

(a) (ADDITIVE HILBERT 90) *Any* additive crossed homomorphism $f\colon G \to M$ *is principal, i.e., a map $f\colon G \to M$ satisfying $f_{\sigma\tau} = f_\sigma + \sigma f_\tau$ has the form $f_\sigma = \sigma a - a$ for some $a \in M$.*

(b) *Any* factor system $c\colon G \times G \to M$ *is split, i.e., any map $c\colon G \times G \to M$ satisfying*

$$c_{\rho,\sigma} + c_{\rho\sigma,\tau} = \rho c_{\sigma,\tau} + c_{\rho,\sigma\tau}$$

has the form

$$c_{\sigma,\tau} = a_\sigma + \sigma a_\tau - a_{\sigma\tau}$$

for some map $a\colon G \to M$.

PROOF. Let $x \in M$ be an element with trace 1.
(a) Let $a = -\sum_{\rho\in G} f_\rho \rho x$.
(b) Let $a_\sigma = \sum_{\rho\in G} c_{\sigma,\rho}\sigma\rho x$. □

REMARKS. (1) It is well-known, and an obvious consequence of point (a) in the Lemma above, that a C_p-extension in characteristic p has the form $K(\theta_a)/K$, where θ_a is a root of the polynomial $X^p - X - a$ (the characteristic p equivalent of a p^{th} root), and as generator of $C_p = \mathrm{Gal}(K(\theta_a)/K)$ is given by $\theta_a \mapsto \theta_a + 1$. Also, the only elements $y \in K(\theta_a)$ for which $y^p - y \in K$ are those of the form $y = h\theta_a + b$, with $h \in \mathbb{F}_p$ and $b \in K$. We denote the Artin-Schreier map $y \mapsto y^p - y$ by $\wp$.

(2) Since we will be using the Lemma to build up p-extension step-wise, we note the following about elements with trace 1: Let M/K be a Galois extension in characteristic p, and let $x \in M$ have trace 1. If $\omega \in M$ is such that $M(\theta_\omega)/K$ is Galois as well, with $\theta_\omega \notin M$, then $-x\theta_\omega^{p-1} \in M(\theta_\omega)$ has trace 1. In particular, if $K(\theta_{a_1}, \ldots, \theta_{a_r})/K$ is a C_p^r-extension, the element $(-1)^r \prod_{i=1}^r \theta_{a_i}^{p-1}$ has trace 1.

Now, returning to our embedding problem from above, we have, by the Lemma, a map $a\colon G \to M$ such that

$$\forall \sigma, \tau \in G\colon c_{\sigma,\tau} = a_\sigma + \sigma a_\tau - a_{\sigma\tau}.$$

Moreover, since $\wp x = 0$ for $x \in \mathbb{F}_p$, the map $\sigma \mapsto \wp a_\sigma$ is an additive crossed homomorphism, meaning that there is an $\omega \in M$ such that

$$\forall \sigma \in G\colon a_\sigma^p - a_\sigma = \sigma\omega - \omega.$$

It is now an easy matter to see that $F/K = M(\theta_\omega)/K$ is a Galois extension with Galois group $\simeq E$. In fact, we can extend $\sigma \in G$ to $\bar{\sigma} \in \mathrm{Gal}(F/K)$ by

$$\bar{\sigma}\colon \theta_\omega \mapsto \theta_\omega + a_\sigma,$$

and get $\bar{\sigma}$ to correspond to the $s_\sigma \in E$ chosen above. Thus, F/K is a solution to the embedding problem given by M/K and $\pi\colon E \to G$.

Similarly, of course, $M(\theta_{r+\omega})/K$ is a solution for all $r \in K$.

On the other hand, by an argument similar to that in the proof of Lemma A.1.1, we see that this gives us *all* solutions to the embedding problem.

EXAMPLE. Consider the quaternion group Q_8 of order 8, as defined in Chapter 6.

In characteristic 2, Q_8-extensions are found as follows: Let $a, b \in K$, such that $K(\theta_a, \theta_b)/K$ is a V_4-extension, and define $\sigma, \tau \in V_4 = \mathrm{Gal}(M/K)$ by

$$\begin{aligned} \sigma\colon &\quad \theta_a \mapsto \theta_a + 1, \quad \theta_b \mapsto \theta_b, \\ \tau\colon &\quad \theta_a \mapsto \theta_a, \qquad\quad \theta_b \mapsto \theta_b + 1. \end{aligned}$$

Now, let

$$\omega = a\theta_a + (a+b)\theta_b, \quad x = \theta_a, \quad \text{and} \quad y = \theta_a + \theta_b.$$

Then

$$\sigma\omega - \omega = a = x^2 - x \quad \text{and} \quad \tau\omega - \omega = y^2 - y.$$

Thus, $F/K = M(\theta_\omega)/K$ is Galois, and since

$$x + \sigma x = y + \tau y = 1 \quad \text{and} \quad x + \sigma y = y + \tau x + 1,$$

we see that F/K has degree 8, and that σ and τ can be extended to F by

$$\sigma\theta_\omega = \theta_\omega + x \quad \text{and} \quad \tau\theta_\omega = \theta_\omega + y.$$

In this way, σ and τ in $\mathrm{Gal}(F/K)$ corresponds to i and j in Q_8, and so F/K is a Q_8-extension.

The Q_8-extensions containing M/K are thus

$$K(\theta_{r+a\theta_a+(a+b)\theta_b})/K, \quad r \in K.$$

(Notice that $\omega = a\theta_a + (a+b)\theta_b$ is invariant under cyclic permutation of a, b and $a+b$.)

A.2. Tensor Products

The basic theory of tensor products is probably known to the reader, and can be found in many algebra textbooks, e.g. [Ja2, 3.7].[3] We include it here only for completeness.

[3]Where the index inexplicably lists it as 'tensor product of molecules'.

Bilinear forms. Let Λ be a ring (not necessarily commutative, but with unit), and let M and N be a right and left Λ-module, respectively. A *bilinear form* $\varphi\colon M \times N \to A$, where A is an abelian group, is then a map with the properties

(i) $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$,
(ii) $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$, and
(iii) $\varphi(m\lambda, n) = \varphi(m, \lambda n)$

for $m, m' \in M$, $n, n' \in N$ and $\lambda \in \Lambda$.

Examples. (1) The maps $(\lambda, n) \mapsto \lambda n$ and $(m, \lambda) \mapsto m\lambda$ are bilinear forms $\Lambda \times N \to N$ and $M \times \Lambda \to M$.

(2) More generally: The maps

$$(\lambda_1, \dots, \lambda_s, n) \mapsto (\lambda_1 n, \dots, \lambda_s n) \quad \text{and} \quad (m, \lambda_1, \dots, \lambda_s) \mapsto (m\lambda_1, \dots, m\lambda_s)$$

are bilinear forms $\Lambda^s \times N \to N^s$ and $M \times \Lambda^s \to M^s$.

The tensor product. Given, as above, Λ-modules M and N, we define a *tensor product* of M and N (over Λ) to be a pair (T, ψ), where T is an abelian group and $\psi\colon M \times N \to T$ is a bilinear form, such that the following condition is satisfied:

Given any bilinear form $\varphi\colon M \times N \to A$, there is a unique group homomorphism $\bar{\varphi}\colon T \to A$ with the property that $\varphi = \bar{\varphi} \circ \psi$. In other words: Bilinear forms from $M \times N$ correspond to group homomorphisms from T.

It is clear that this is a *universal property*, characterising the tensor product up to canonical isomorphism.

As for the *existence* of a tensor product, we proceed as follows: Let $\mathbb{Z}^{(M\times N)}$ be the free abelian group with a basis indexed by the elements of $M \times N$. We denote this basis by $(e_{(m,n)})_{(m,n)\times M\times N}$.

In a tensor product (T, ψ), the images of the elements of $M \times N$ must satisfy the bilinearity conditions (i)–(iii) above. Thus, we take the submodule S of $\mathbb{Z}^{(M\times N)}$ generated by all elements of the forms

$$e_{(m+m',n)} - e_{(m,n)} - e_{m',n},$$
$$e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')} \quad \text{and}$$
$$e_{(m\lambda,n)} - e_{(m,\lambda n)}$$

for $m, m' \in M$, $n, n' \in N$ and $\lambda \in \Lambda$, and let $T = \mathbb{Z}^{(M\times N)}/S$ and $\psi(m, n) = \bar{e}_{(m,n)}$.

(T, ψ) is now in fact a tensor product: ψ is bilinear by construction, and if $\varphi\colon M \times N \to A$ is a bilinear form, we see that the homomorphism from T to A given by $e_{(m,n)} \mapsto \varphi(m, n)$ disappears in S, giving us a well-defined induced map $\bar{\varphi}\colon \bar{e}_{(m,n)} \to \varphi(m, n)$ from T to A. Clearly, $\varphi = \bar{\varphi} \circ \psi$, and $\bar{\varphi}$ is unique with that property.

Thus, tensor products exist and are essentially unique. We will therefore refer to *the* tensor product of M and N, denoted $M \otimes_\Lambda N$, and use the notation $m \otimes n$ for the image of (m, n) in the tensor product.

REMARK. Notice that $M \otimes_\Lambda N$ is generated by the elements $m \otimes n$. This is clear from the construction, but can also be seen using the universal property.

EXAMPLE. From the bilinear map $\Lambda^s \times N \to N^s$ in the previous Example, we get a homomorphism $\Lambda^s \otimes_\Lambda N \to N^s$, given by

$$(\lambda_1, \dots, \lambda_s) \otimes n \mapsto (\lambda_1 n, \dots, \lambda_s n).$$

This is actually an isomorphism: Let $e_1, \dots, e_s$ be the canonical basis for Λ^s, and define a homomorphism $N^s \to \Lambda^s \otimes_\Lambda N$ by

$$(n_1, \dots, n_s) \mapsto e_1 \otimes n_1 + \dots + e_s \otimes n_s.$$

The two maps $\Lambda^s \otimes_\Lambda N \to N^s$ and $N^s \to \Lambda^s \otimes_\Lambda N$ are then each others inverses.

Similarly, $M \otimes_\Lambda \Lambda^s \simeq M^s$.

We leave the proof of the following Proposition as an exercise for the reader:

PROPOSITION A.2.1. (a) $M \otimes_\Lambda (\bigoplus_i N_i) \simeq \bigoplus_i (M \otimes_\Lambda N_i)$ *by* $m \otimes (n_i)_i \mapsto (m \otimes n_i)_i$, *and similarly* $(\bigoplus_j M_j) \otimes_\Lambda N \simeq \bigoplus_j (M_j \otimes_\Lambda N)$.

(b) *If* $f\colon M \to M'$ *and* $g\colon N \to N'$ *are* Λ*-homomorphisms, there is an induced group homomorphism* $f \otimes g\colon M \otimes_\Lambda N \to M' \otimes_\Lambda N'$, *given by* $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

(c) $M \otimes_\Lambda N \simeq N \otimes_{\Lambda^{\mathrm{op}}} M$ *by* $m \otimes n \mapsto n \otimes m$.

The tensor product as a module. Let Γ and Λ be rings. A Γ-Λ-*bimodule* is then an abelian group M equipped with both a left Γ- and a right Λ-module structure, such that

$$\gamma(m\lambda) = (\gamma m)\lambda$$

for $m \in M$, $\gamma \in \Gamma$ and $\lambda \in \Lambda$.

EXAMPLES. (1) If R is a commutative ring, any R-module is trivially an R-R-bimodule.

(2) If K is a field, the vector space $\mathrm{Mat}_{m\times n}(K)$ of $m \times n$ matrices is a $\mathrm{Mat}_m(K)$-$\mathrm{Mat}_n(K)$-bimodule.

If M is a Γ-Λ-bimodule rather then just a right Λ-module, the tensor product $M \otimes_\Lambda N$ gets a left Γ-module structure by

$$\gamma(m \otimes n) = (\gamma m) \otimes n :$$

For given (fixed) $\gamma \in \Gamma$, the map $(m, n) \mapsto (\gamma m) \otimes n$ is a well-defined bilinear form $M \otimes N \to M \otimes_\Lambda N$, and so induces a homomorphism $\gamma\cdot\colon m \otimes n \mapsto (\gamma m) \otimes n$ on $M \otimes_\Lambda N$. It is easily seen that this gives us a module structure.

In the same way, $M \otimes_\Lambda N$ becomes a right Γ-module if N is a Λ-Γ-bimodule.

In particular, $M \otimes_R N$ is an R-module when R is commutative.

PROPOSITION A.2.2. (a) *Assume that* M *is a right* Γ*-module,* N *a* Γ-Λ*-bimodule, and* P *a left* Λ*-module. Then* $M \otimes_\Gamma (N \otimes_\Lambda P) \simeq (M \otimes_\Gamma N) \otimes_\Lambda P$ *by* $m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$.

(b) *If* M *and* M' *are* Γ-Λ*-bimodules, and* $f\colon M \to M'$ *is a bimodule homomorphisms* (*i.e., both a* Γ- *and a* Λ*-homomorphism*), *the induced map* $f \otimes 1\colon M \otimes_\Lambda N \to M' \otimes_\Lambda N$ *is a* Γ*-homomorphism. Similarly from the other side.*

PROOF. Exercise. □

Tensor products of algebras. Let R be a commutative ring. An *R-algebra* is then a ring $\mathfrak{A}$ together with an R-module structure on the additive group $(\mathfrak{A}, +)$, such that

$$r(ab) = (ra)b = a(rb)$$

for $r \in R$ and $a, b \in \mathfrak{A}$. Examples of algebras are matrix rings $\mathrm{Mat}_n(R)$ and field extensions L/K.

If $\mathfrak{A}$ and $\mathfrak{B}$ are R-algebras, we can define a multiplication on the tensor product $\mathfrak{A} \otimes_R \mathfrak{B}$ by

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$$

for $a, a' \in \mathfrak{A}$ and $b, b' \in \mathfrak{B}$. In this way, the tensor product again becomes an R-algebra, and we will always understand it to be an algebra in this way.

EXAMPLE. $\mathrm{Mat}_n(R) \otimes_R \mathfrak{A} \simeq \mathrm{Mat}_n(\mathfrak{A})$. In particular, $\mathrm{Mat}_m(R) \otimes_R \mathrm{Mat}_n(R) \simeq \mathrm{Mat}_{mn}(R)$.

If S is a *commutative* R-algebra, it is also an S-R-bimodule, and consequently the tensor product $S \otimes_R \mathfrak{A}$ becomes an S-algebra by $s(s' \otimes a) = (ss') \otimes a$. In this case, we refer to $S \otimes_R \mathfrak{A}$ as the *scalar extension* of $\mathfrak{A}$ to S.

EXAMPLES. (1) The scalar extension of $R[X]$ to S is $S[X]$.

(2) The scalar extension of $\mathrm{Mat}_n(R)$ to S is $\mathrm{Mat}_n(S)$.

A.3. Linear Disjointness

DEFINITION A.3.1. Let K be a field, and let L/K and M/K be subextensions of a field extension N/K. Then we say that L and M are *linearly disjoint* over K if one of the following two equivalent conditions are satisfied:

(i) Elements in L are linearly independent over M if they are linearly independent over K.

(ii) Elements in M are linearly independent over L if they are linearly independent over K.

That these two conditions *are* equivalent is trivial.

EXAMPLES. (1) If L/K and M/K are finite of mutually prime degrees, they are linearly disjoint.

(2) $K(x)$ and $K(y)$ (inside $K(x, y)$) are linearly disjoint over K.

If L/K is finite, it is easy to produce an extension N/K containing both L/K and a given arbitrary extension M/K. In this case, we have

PROPOSITION A.3.2. *Assume L/K finite. Then L and M are linearly disjoint over K if and only if $L \otimes_K M$ is a field.*

Thus, there is no need to find an N in advance: Just look at $L \otimes_K M$.

PROOF. We consider the map $\ell \otimes m \mapsto \ell m$ from $L \otimes_K M$ to N.

'If': Clearly, the map is injective if $L \otimes_K M$ is a field, and so we may assume $N = L \otimes_K M$. From the Example on p. 212, we now get property (i) in the Definition above.

'Only if': Let $(\ell_i)_i$ be a basis for L/K. Then $(\ell_i \otimes 1)_i$ is a basis for $L \otimes_K M$ over M, *and* $(\ell_i)_i$ is a basis for $LM \subseteq N$ over M. It follows that $L \otimes_K M \simeq LM$, and hence that $L \otimes_K M$ is a field. □

PROPOSITION A.3.3. *Let L/K and M/K be finite Galois extensions. Then L and M are linearly disjoint if and only if $L \cap M = K$.*

This condition is well-defined, since the composite of L and M is unique up to isomorphism.

PROOF. By basic Galois theory, we have $L \cap M = K$ if and only if $[ML : K] = [M : K][L : K]$, if and only if $[ML : L] = [M : K]$, if and only if a basis for M/K is also a basis for ML/L. □

A.4. The Hilbert Nulstellensatz

THE HILBERT NULSTELLENSATZ. *Let K be an arbitrary field, and let $\mathbf{x} = (x_1, \ldots, x_n)$ be indeterminates. Then the following statements hold:*

(a) *A family $f_1, \ldots, f_s$ of polynomials in $K[\mathbf{x}]$ generates a proper ideal if and only if they have a common zero in M^n for some finite field extension M/L.*

(b) *Let $\mathfrak{m}$ be a maximal ideal in $K[\mathbf{x}]$. Then $K[\mathbf{x}]/\mathfrak{m}$ is a finite extension of K.*

(c) *Let $\mathfrak{a} \subseteq K[\mathbf{x}]$ be an ideal. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m},$$

where the $\mathfrak{m}$'s are understood to be maximal ideals.

REMARKS. (1) Normally, the Nulstellensatz is formulated for an algebraically closed field K, and the statements (a) and (b) are then referred to as the *weak* Nulstellensatz, while (c) is the *strong* Nulstellensatz.

(2) A consequence of point (b) in the Nulstellensatz is that a maximal ideal in a polynomial ring $K[\mathbf{x}]$ is given by a tuple $\mathbf{a} = (a_1, \ldots, a_n)$ of elements in an algebraic extension M/K as the polynomials that vanish in $\mathbf{a}$.

PROOF OF THE NULSTELLENSATZ. (a) 'If' is clear. 'Only if' is proved by induction on n, where $n = 1$ is obvious.

We can of course assume that $\mathfrak{m} = (f_1, \ldots, f_s)$ is a maximal ideal in $K[\mathbf{x}]$. There are then two possibilities:

(1) $\mathfrak{m} \cap K[x_1] \neq 0$: Then there is a non-trivial polynomial $\pi(x_1)$ in $\mathfrak{m}$. Let L be the splitting field of $\pi(x_1)$ over K. Since $L[\mathbf{x}]/K[\mathbf{x}]$ is an integral extension, $\mathfrak{m}L[\mathbf{x}]$ is a proper ideal in $L[\mathbf{x}]$ and thus contained in a maximal ideal $\mathfrak{m}'$. Also contained in $\mathfrak{m}'$ is $x_1 - \theta$ for a root $\theta \in L$ of $\pi(x_1)$. It follows that $L[x_2, \ldots, x_n]$ maps surjectively onto $L[\mathbf{x}]/\mathfrak{m}'$, and since $f_1(\theta, x_2, \ldots, x_n), \ldots, f_2(\theta, x_2, \ldots, x_n)$ are in the kernel, they generate a proper ideal in $L[x_2, \ldots, x_n]$. By induction, they have a common zero in a finite extension M of L.

(2) $\mathfrak{m} \cap K[x_1] = 0$: We localise in $K[x_1] \setminus 0$ to get a maximal ideal $(f_1, \ldots, f_s)$ in $K(x_1)[x_2, \ldots . x_n]$. By induction, there is a finite extension $\mathbb{M}/K(x_1)$ in which $f_1, \ldots, f_s$ have a common zero $(x_1, \Theta_2, \ldots, \Theta_n)$. For a suitable $x \in K[x_1]$, the Θ_i's are integral over $K[x_1, 1/x]$. Also, there is a θ algebraic over K with $x(\theta) \neq$

0, giving us a surjection

$$K[x_1, 1/x] \underset{x_1 \mapsto \theta}{\twoheadrightarrow} L = K(\theta)$$

The kernel is a maximal ideal in $K[x_1, 1/x]$, and so is contained in a maximal ideal in the integral closure of $K[x_1, 1/x]$ in $\mathbb{M}$. Call the quotient field M. Then

$$x_1 \mapsto \theta, \quad x_2 \mapsto \bar{\Theta}_2, \quad \ldots, \quad x_n \mapsto \bar{\Theta}_n$$

gives us a homomorphism $K[\mathbf{x}] \to M$ with kernel $\mathfrak{m}$. In particular, the minimal polynomial of θ over K (with respect to x_1) is in $\mathfrak{m}$, contradicting our assumption.

(b) is an immediate consequence of (a), when the f_i's are taken to be generators for $\mathfrak{m}$.

(c) '$\subseteq$' is obvious. Now, let $g \in \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$, and let $\mathfrak{M}$ be a maximal ideal in $K[\mathbf{x}, Y]$ containing $\mathfrak{a}$. Since

$$K \subseteq K[\mathbf{x}]/(\mathfrak{M} \cap K[\mathbf{x}]) \subseteq K[\mathbf{x}, Y]/\mathfrak{M},$$

$K[\mathbf{x}]/(\mathfrak{M} \cap K[\mathbf{x}])$ is a field, and so $\mathfrak{M} \cap K[\mathbf{x}]$ is a maximal ideal in $K[\mathbf{x}]$ containing $\mathfrak{a}$. Thus, $g \in \mathfrak{M} \cap K[\mathbf{x}]$, and hence $g \in \mathfrak{M}$. It follows that no maximal ideal in $K[\mathbf{x}, Y]$ contains both $\mathfrak{a}$ and $1 - gY$. Consequently, there exists polynomials $f_1, \ldots, f_s \in \mathfrak{a}$ and $h_1, \ldots, h_s, h \in K[\mathbf{x}, Y]$, such that

$$h_1 f_1 + \cdots + h_s f_s + h(1 - gY) = 1.$$

Setting $Y = 1/g$, we get

$$h_1(\mathbf{x}, 1/g) f_1(\mathbf{x}) + \cdots + h_s(\mathbf{x}, 1/g) f_s(\mathbf{x}) = 1.$$

Now, $h_i(\mathbf{x}, 1/g) = H_i(\mathbf{x})/g(\mathbf{x})^e$ for some $H_i \in K[\mathbf{x}]$ and some number e, and so

$$H_1 f_1 + \cdots + H_s f_s = g^e,$$

i.e., $g \in \sqrt{\mathfrak{a}}$. □

APPENDIX B

Invariant Theory

In this Appendix we give a brief introduction to classical invariant theory, needed in the proof of Hermite's results concerning quintic polynomials as given in Chapter 2. Our references are [Ol] and [D&C]. We are also indebted to P. Wiggen, whose thesis (*Invariants of Binary Forms and Tschirnhaus Transformations*, Reed College, 1998) contains an exposition of the invariant theory necessary for Hermite's proof.

For convenience, we work over the complex number field $\mathbb{C}$.

B.1. Basic Concepts

We will be concerned with *binary forms*, i.e., homogeneous polynomials

$$P(x,y) = \sum_{i=0}^{n} \binom{n}{i} a_j x^i y^{n-i} \tag{B.1.1}$$

in two indeterminates of some degree n. (Not to be confused with *quadratic* forms, which are homogeneous polynomials of degree 2 in some number n of indeterminates.)

The binomial coefficients in (B.1.1) are included purely for convenience, and have no real bearing on the theory. We refer to Exercise B.3 for a proof of this fact, and to Exercise B.1 and the formula (B.3.2) below for examples of the convenience.

Associated to $P(x,y)$ is a corresponding polynomial

$$P(z) = P(z,1) = \sum_{i=0}^{n} \binom{n}{i} a_i z^i.$$

Whenever we look at $P(z)$, we will keep n in mind and consider it formally to be the degree of $P(z)$, even if $a_n = 0$. This allows the reconstruction of $P(x,y)$ from $P(z)$ by

$$P(x,y) = P(x/y)\, y^n.$$

This situation is somewhat similar to that of Exercise 1.6 in Chapter 1, where $f(X)$ and $g(X)$ did not necessarily have degrees m and n, but required us to specify m and n separately from the polynomials.

Whenever $\alpha \in \mathbb{C}$ is a root of $P(z)$, the linear polynomial $x - \alpha y$ divides $P(x,y)$. And if the actual degree of $P(z)$ is $d < n$, we also get y as a $(n-d)$-fold factor

of $P(x,y)$. These linear factors can be scaled, giving us factorisations of the form

$$P(x,y) = \prod_{i=1}^{n} (y_i x - x_i y). \tag{B.1.2}$$

We will call such a factorisation *normal*. It is of course not unique, except in the usual sense, i.e., up to re-scaling and permuting the factors.

A matrix

$$\mathbf{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

induces an automorphism on $\mathbb{C}[x,y]$ by

$$x \mapsto \alpha x + \beta y, \quad y \mapsto \gamma x + \delta y.$$

Alternatively, it defines a new pair of generating indeterminates

$$\bar{x} = \alpha x + \beta y \quad \text{and} \quad \bar{y} = \gamma x + \delta y,$$

and a corresponding binary form $\bar{P}(\bar{x},\bar{y})$ given by

$$\begin{aligned} \bar{P}(\bar{x},\bar{y}) = P(x,y) &= P\left(\frac{\delta\bar{x} - \beta\bar{y}}{\alpha\delta - \beta\gamma}, \frac{-\gamma\bar{x} + \alpha\bar{y}}{\alpha\delta - \beta\gamma} \right) \\ &= \sum_{i=0}^{n} \binom{n}{i} \bar{a}_i \bar{x}^i \bar{y}^{n-i}. \end{aligned}$$

As for normal factorisations: Applying the transformation factor-wise to (B.1.2), we get

$$\bar{P}(\bar{x},\bar{y}) = \prod_{i=1}^{n} \left(\frac{\gamma x_i + \delta y_i}{\alpha\delta - \beta\gamma} \bar{x} - \frac{\alpha x_i + \beta y_i}{\alpha\delta - \beta\gamma} \bar{y} \right). \tag{B.1.3}$$

NOTE. It is clear that the transformation

$$\mathbf{a} = (a_0, \ldots, a_n) \mapsto \bar{\mathbf{a}} = (\bar{a}_0, \ldots, \bar{a}_n)$$

is linear in $\mathbf{a}$, and from the definition it follows that it is homomorphic in $\mathbf{A}$, i.e., if we denote $\bar{\mathbf{a}}$ by $\mathbf{A}\mathbf{a}$, we have

$$(\mathbf{B}\mathbf{A})\mathbf{a} = \mathbf{B}(\mathbf{A}\mathbf{a}).$$

Thus, the transformation $P(x,y) \mapsto \bar{P}(\bar{x},\bar{y})$ can be considered as a $\mathrm{GL}_2(\mathbb{C})$-action on the vector space $\mathbb{C}^{n+1}$.

For instance, for $n = 2$ we get

$$\begin{aligned} \bar{a}_0 &= \frac{\alpha^2 a_0 - 2\alpha\beta a_1 + \beta^2 a_2}{(\alpha\delta - \beta\gamma)^2}, \\ \bar{a}_1 &= \frac{-\alpha\gamma a_0 + (\alpha\delta + \beta\gamma) a_1 - \beta\delta a_2}{(\alpha\delta - \beta\gamma)^2}, \\ \bar{a}_2 &= \frac{\gamma^2 a_0 - 2\gamma\delta a_1 + \delta^2 a_2}{(\alpha\delta - \beta\gamma)^2}, \end{aligned}$$

meaning that $\mathbf{A}$ acts on $\mathbb{C}^3$ as

$$\hat{\mathbf{A}} = \frac{1}{(\alpha\delta - \beta\gamma)^2} \begin{pmatrix} \alpha^2 & -2\alpha\beta & \beta^2 \\ -\alpha\gamma & \alpha\delta + \beta\gamma & -\beta\delta \\ \gamma^2 & -2\gamma\delta & \delta^2 \end{pmatrix}.$$

This homomorphism from $\mathrm{GL}_2(\mathbb{C})$ into $\mathrm{GL}_3(\mathbb{C})$ has, as we see, a particularly 'algebraic' form: The entries in the image matrix $\hat{\mathbf{A}}$ are rational functions in the entries of the argument matrix $\mathbf{A}$. This is more generally true for any n, of course, and we refer to such representations of a general linear group as *rational*. If the entries are in fact polynomials, we use the term *polynomial* representations.

Projective zeroes. We define the (*complex*) *projective line* $\mathbb{P}^1\mathbb{C}$ as the set of non-zero vectors in $\mathbb{C}^2$ modulo non-zero scalar multiplication, i.e., as the set of lines through the origin in $\mathbb{C}^2$.

The element of $\mathbb{P}^1\mathbb{C}$ containing (or passing through) a point $(a, b) \in \mathbb{C}^2 \setminus \{(0, 0)\}$ is denoted $[a, b]$. We call it a *projective point*, and call $[a, b]$ the *homogeneous coordinates*. The map $a \mapsto [a, 1]$ from $\mathbb{C}$ into $\mathbb{P}^1\mathbb{C}$ covers all of the projective line, except for the one point $\infty = [1, 0]$, referred to as *infinity*. We identify $\mathbb{C}$ with its image in $\mathbb{P}^1\mathbb{C}$, and see that $[a, b] = [a/b, 1]$ if $b \neq 0$.

A binary form

$$P(x, y) = \sum_{i=0}^{n} \binom{n}{i} a_i x^i y^{n-i} \in \mathbb{C}[x, y]$$

has the special property that its non-trivial zeroes (i.e., zeroes other than $(0, 0)$) lie on lines through the origin, and therefore make up projective points. Whenever $[a, b] \in \mathbb{P}^1\mathbb{C}$ is such a *projective zero*, we get a linear factor $bx - ay$ of $P(x, y)$. We can now define the *multiplicity* of a projective zero as the number of times the associated factor divides $P(x, y)$. For an ordinary zero α of $P(z)$, the multiplicity of $[\alpha, 1]$ coincides with the usual multiplicity of α. For ∞, the multiplicity is the difference between the formal and ordinary degrees of $P(z)$. The multiplicities of the projective zeroes therefore add up to n.

The matrix transformation considered above induces a map

$$[x, y] \mapsto [\bar{x}, \bar{y}] = [\alpha x + \beta y, \gamma x + \delta y]$$

on the projective line, which we also denote by

$$z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta}$$

and call a *fractional linear transformation*. (This agrees with the usual division in $\mathbb{C}$, modulo the convention that $a/0 = \infty$ and $a/\infty = 0$ for $a \in \mathbb{C} \setminus \{0\}$.)

Classical invariant theory can be considered as the study of properties of a polynomial $P(z)$ that are unchanged under fractional linear transformations. (See also Exercise B.2.) Note that the ordinary degree of $P(z)$ is *not* such a property, whereas the formal degree is, by definition. Multiplicities of (projective) zeroes *are* preserved.

In the following, we will consider invariant theory in terms of binary forms. We invite the reader to work out the implications for one-parameter polynomials. (Exercise B.10 would be an example.)

B.2. Invariants

Let again $P(x, y) \in \mathbb{C}[x, y]$ be a binary form of degree n. Then we define an *invariant* of $P(x, y)$ to be a function (mostly a polynomial) $I(\mathbf{a}) = I(a_0, \dots, a_n)$ depending on the coefficients of $P(x, y)$, such that

$$I(\mathbf{a}) = \det \mathbf{A}^k \, I(\bar{\mathbf{a}})$$

whenever $\mathbf{A} \in \mathrm{GL}_2(\mathbb{C})$ is as before, and $\bar{\mathbf{a}} = (\bar{a}_0, \dots, \bar{a}_n)$ are the coefficients of the transformed binary form $\bar{P}(\bar{x}, \bar{y})$. We then refer to the exponent k as the *weight* of I, written $k = \operatorname{wt} I$.

Notice that this concept is not really all that interesting if we only look at a single binary form $P(x, y)$. But since the coefficients of $\bar{P}(\bar{x}, \bar{y})$ depend linearly on those of $P(x, y)$, it is understood that we really consider $\mathbf{a}$ and $\bar{\mathbf{a}}$ to be elements of $\mathbb{C}^{n+1}$.

Remark. In what sense is I an invariant? When a group G acts on a set X, the *invariants* are the elements in

$$X^G = \{x \in X \mid \forall \sigma \in G \colon \sigma x = x\}.$$

If G acts on both X and Y, we get a G-action on the set Y^X of maps $X \to Y$ by the so-called *diagonal action*

$$\sigma f \colon x \mapsto \sigma f(\sigma^{-1} x),$$

i.e., by demanding $\sigma f \colon \sigma x \mapsto \sigma f(x)$. In this case, the invariants are also sometimes called *equivariants*. They satisfy

$$\forall \sigma \in G, \ x \in X \colon f(\sigma x) = \sigma f(x).$$

In our case, $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{C}^{n+1}$, and I is a map from $\mathbb{C}^{n+1}$ into $\mathbb{C}$. We thus need to consider possible $\mathrm{GL}_2(\mathbb{C})$-actions on $\mathbb{C}$. These are clearly given by *characters*, i.e., homomorphisms $\chi \colon \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^*$,[1] through

$$\mathbf{A} \colon z \mapsto \chi(\mathbf{A})\, z.$$

We then have that I is a invariant (with respect to χ), if

$$I(\mathbf{A} \cdot \mathbf{a}) = \chi(\mathbf{A}) I(\mathbf{a}).$$

So, what does χ look like? We will restrict our attention to *rational* characters, cf. the Note of p. 218.[2] By [Hu, II Satz 6.10], the commutator subgroup of $\mathrm{GL}_n(\mathbb{C})$ is the special linear group $\mathrm{SL}_n(\mathbb{C})$. (See also Exercise B.5.) In particular, any character $\chi \colon \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^*$ factors through the determinant. Thus, it has the form $\chi = \varphi \circ \det$ for some endomorphism φ on $\mathbb{C}^*$. Since we require χ

[1] Also sometimes referred to as *linear* characters, or characters of *degree* 1.

[2] There are of course many non-rational characters as well, including obvious ones like the conjugate of the determinant.

to be rational, we have a rational function $f(\mathbf{X}) = f(\{x_{ij}\}_{i,j}) \in \mathbb{C}[\mathbf{x}]$, such that $\chi(\mathbf{X}) = f(\mathbf{x})$ when $\mathbf{X} = (x_{ij})_{i,j}$ in the matrix with $(i,j)^{\text{th}}$ entry x_{ij}. From

$$\varphi(x) = \chi \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

we get that φ is a rational function: $\varphi(x) = p(x)/q(x)$ for $p(x), q(x) \in \mathbb{C}[x]$ mutually prime. Since φ is multiplicative, we have

$$p(a)p(x)q(ax) = q(a)q(x)p(ax)$$

for $a \in \mathbb{C}^*$, i.e., $p(x) \mid p(ax)$ and $q(x) \mid q(ax)$, from which we see that $\varphi(x) = x^k$.

Thus, in this case the *only* characters are the powers of the determinant, and our concept of invariant makes sense.

When looking at polynomial invariants, it is clear from the transformation rules that the homogeneous components (in $\mathbf{a}$) are again invariants, of the same weight, and conversely, that adding invariants of the same weight k results in a invariant of weight k.

Regarding homogeneous polynomial invariants, we have

PROPOSITION B.2.1. *Let $I(\mathbf{a})$ be a (non-zero) homogeneous polynomial invariant of degree d and weight k. Then*

$$dn = 2k.$$

PROOF. Consider a scalar matrix

$$\mathbf{A} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}.$$

By Exercise B.6(1), the corresponding transformation is

$$\mathbf{a} \mapsto \bar{\mathbf{a}} = \frac{1}{\alpha^n}\mathbf{a}.$$

From the definition of invariant, we now get

$$I(\mathbf{a}) = \det \mathbf{A}^k \, I(\bar{\mathbf{a}}) = \alpha^{2k-dn} I(\mathbf{a}),$$

since I is homogeneous. But that means $\alpha^{2k-dn} = 1$ for all α, and hence $2k - dn = 0$. □

COROLLARY B.2.2. *Polynomial invariants are homogeneous.*

PROOF. The homogeneous components all have the same degree. □

B.3. Bracket Polynomials

Let once again $P(x,y) \in \mathbb{C}[x,y]$ be a binary form as in (B.1.1), and consider a normal factorisation

$$P(x,y) = \prod_{i=1}^{n}(y_i x - x_i y).$$

As we saw, a transform $\bar{P}(\bar{x},\bar{y})$ of $P(x,y)$ then has an induced normal factorisation

$$\bar{P}(\bar{x},\bar{y}) = \prod_{i=1}^{n}\left(\frac{\gamma x_i + \delta y_i}{\alpha\delta - \beta\gamma}\bar{x} - \frac{\alpha x_i + \beta y_i}{\alpha\delta - \beta\gamma}\bar{y}\right),$$

and we can think of this as giving a transformation

$$(x_i, y_i) \mapsto (\bar{x}_i, \bar{y}_i) = \left(\frac{\alpha x_i + \beta y_i}{\alpha\delta - \beta\gamma}, \frac{\gamma x_i + \delta y_i}{\alpha\delta - \beta\gamma}\right). \tag{B.3.1}$$

We can then look at the determinant

$$[i\,j] = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = x_i y_j - x_j y_i,$$

which almost qualifies as an invariant of weight 1, since

$$\begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = (\alpha\delta - \beta\gamma)\begin{vmatrix} \bar{x}_i & \bar{x}_j \\ \bar{y}_i & \bar{y}_j \end{vmatrix}.$$

Of course, it is not in fact an invariant, since it is not a well-defined function of $\mathbf{a}$.

All we actually know about the x_i's and y_i's is that they satisfy the relations

$$\sum_{\substack{I\subseteq\{1,\dots,n\}\\ |I|=d}} \prod_{i\notin I} x_i \prod_{i\in I} y_i = (-1)^{n-d}\binom{n}{d}a_d, \quad 0 \le d \le n,$$

or more simply put:

$$a_{n-d} = \frac{(-1)^d}{n!}\sum_{\sigma\in S_n} x_{\sigma 1}\cdots x_{\sigma d}\cdot y_{\sigma(d+1)}\cdots y_{\sigma n}, \quad 0 \le d \le n. \tag{B.3.2}$$

Certain polynomials in the x_i's and y_i's can therefore be rewritten as polynomials in $\mathbf{a}$. In particular, we can hope to construct invariants in this way: If the polynomial happens to be homogeneous of degree k, *and* expressible as a polynomial in the $[i\,j]$'s, it will be an invariant of weight $k/2$. We will refer to the $[i\,j]$'s as *brackets*, and to polynomials in the $[i\,j]$'s as *bracket polynomials*.

Example. We can define the *discriminant* of a binary form $P(x,y)$ as

$$d(P) = \prod_{i<j}(y_i x_j - x_j y_j)^2 = \prod_{i<j}[i\,j]^2.$$

This expression is independent of the choice of normal factorisation, and is by construction a bracket polynomial. And it is not hard to see that $d(P)$ is a

polynomial in $\mathbf{a}$: Think of the x_i's and y_i's as indeterminates, and define the a_i's by (B.3.2). Let

$$p(z) = \sum_{i=0}^{n} \binom{n}{i} \frac{a_i}{a_n} z^i.$$

Then $P(x, y) = a_n y^n p(x/y)$, and the zeroes of $p(z)$ are x_i/y_i. Rewriting

$$d(P) = \prod_{i<j} (y_i x_j - x_i y_j)^2 = a_n^{2(n-1)} \prod_{i<j} \big(\frac{x_j}{y_j} - \frac{x_i}{y_i}\big)^2 = a_n^{2(n-1)} d(p),$$

we get the desired result: $d(p)$ is a polynomial in $a_0/a_n, \ldots, a_{n-1}/a_n$, and from the resultant formula in Chapter 1 we get that $d(p)$ has total degree $2(n-1)$ in the coefficients of $p(z)$. Hence, the multiplication by $a_n^{2(n-1)}$ clears the denominators, and gives us a polynomial.

We conclude that the discriminant is an invariant of weight $n(n-1)$, and is homogeneous of degree $2(n-1)$ in the a_i's.

For instance, for $n = 2$ the discriminant is

$$d(P) = 4(a_1^2 - a_0 a_2),$$

and this is an invariant of weight 2.

Note that, like the usual discriminant of a polynomial, $d(P)$ vanishes if and only if $P(x, y)$ has a multiple (projective) zero.

We will look at the abstract question of which polynomials in the polynomial ring $\mathbb{C}[\mathbf{x}, \mathbf{y}] = \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ are polynomials in $\mathbf{a}$, when $\mathbf{a} = (a_0, \ldots, a_n)$ is defined according to (B.3.2):

First of all, since the a_i's are *simultaneously symmetric* in $\mathbf{x}$ and $\mathbf{y}$ (i.e., invariant when the same permutation is applied to both the x_i's and the y_i's), a polynomial in $\mathbb{C}[\mathbf{x}, \mathbf{y}]$ cannot be in $\mathbb{C}[\mathbf{a}]$ unless it is simultaneously symmetric. However, this is not a sufficient condition, simply by reason of the transcendence degrees: $\mathbb{C}(\mathbf{x}, \mathbf{y})^{S_n}$ has transcendence degree $2n$ over $\mathbb{C}$, whereas $\mathbb{C}(\mathbf{a})$ has transcendence degree at most $n + 1$.[3]

Second, we note that $a_0, \ldots, a_n$ are algebraically independent: Up to signs and binomial coefficients, $a_0/a_n, \ldots, a_{n-1}/a_n$ are the elementary symmetric symbols in $x_1/y_1, \ldots, x_n/y_n$, and $a_n = y_1 \cdots y_n$. As $x_1/y_1, \ldots, x_n/y_n, y_1 \cdots y_n$ are trivially algebraically independent, the result follows.

The a_i's are homogeneous (of degree n) as polynomials in $\mathbb{C}[\mathbf{x}, \mathbf{y}]$ and consequently the subalgebra $\mathbb{C}[\mathbf{a}]$ they generate is graded: If we write $f(\mathbf{x}, \mathbf{y}) \in \mathbb{C}[\mathbf{a}]$ as

$$f(\mathbf{x}, \mathbf{y}) = \sum_{i=0}^{m} f_i(\mathbf{x}, \mathbf{y}),$$

where $f_i(\mathbf{x}, \mathbf{y})$ is the homogeneous degree-i component, then $f_i(\mathbf{x}, \mathbf{y}) \in \mathbb{C}[\mathbf{a}]$. Moreover, the a_i's are a very special kind of homogeneous polynomials, in that they are *regular*:

[3] And we are not really interested in the case $n = 1$.

DEFINITION B.3.1. A homogeneous polynomial $f(\mathbf{x},\mathbf{y}) \in \mathbb{C}[\mathbf{x},\mathbf{y}]$ is called *k-regular* if its (non-zero) terms

$$bx_1^{i_1}\cdots x_n^{i_n}\cdot y_1^{j_1}\cdots y_n^{j_n}$$

satisfy $i_d + j_d = k$ for all d.

The degree of a k-regular homogeneous polynomial is of necessity kn.

Clearly, the a_i's are 1-regular, and since the product of a k-regular and an ℓ-regular polynomial is a $(k+\ell)$-regular polynomial, we see that the homogeneous components of an element in $\mathbb{C}[\mathbf{a}]$ must be regular.

PROPOSITION B.3.2. *The elements of $\mathbb{C}[\mathbf{a}]$ are exactly those simultaneously symmetric polynomials in $\mathbb{C}[\mathbf{x},\mathbf{y}]$ for which all the homogeneous components are regular.*

PROOF. We have already seen that the elements in $\mathbb{C}[\mathbf{a}]$ have this form. Conversely, let $f(\mathbf{x},\mathbf{y}) \in \mathbb{C}[\mathbf{x},\mathbf{y}]$ be simultaneously symmetric and k-regular. We write

$$f(\mathbf{x},\mathbf{y}) = (y_1\cdots y_n)^k g\big(\frac{x_1}{y_1},\dots,\frac{x_n}{y_n}\big),$$

where

$$g(\mathbf{z}) = g(z_1,\dots,z_n,1,\dots,1) \in \mathbb{C}[\mathbf{z}]$$

is a symmetric polynomial in the z_i's. Hence, $g(\mathbf{z})$ is a polynomial in the elementary symmetric symbols $\mathbf{e} = (e_1,\dots,e_n)$ of $\mathbf{z}$; it follows that $g(x_1/y_1,\dots,x_n/y_n)$ is a polynomial in $a_0/a_n,\dots,a_{n-1}/a_n$:

$$f(\mathbf{x},\mathbf{y}) = a_n^k h\big(\frac{a_0}{a_n},\dots,\frac{a_{n-1}}{a_n}\big)$$

for some $h(\mathbf{e}) \in \mathbb{C}[\mathbf{e}]$. Since the degree of $g(\mathbf{z})$ in any given z_i is at most k, we see from the standard algorithm for producing $h(\mathbf{e})$, cf. e.g. [Ja1, 2.13], that $h(\mathbf{e})$ has degree at most k. Thus, the factor a_n^k clears the denominators, and $f(\mathbf{x},\mathbf{y})$ is a polynomial in the a_i's. □

COROLLARY B.3.3. *If $f(\mathbf{x},\mathbf{y}) \in \mathbb{C}[\mathbf{x},\mathbf{y}]$ is a simultaneously symmetric and regular bracket polynomial, then it is an invariant.*

The discriminant is an example.

More generally, we can now produce invariants systematically as follows:

(1) In order for a bracket monomial $[i_1\, j_1]\cdots[i_k\, j_k]$ to be regular, it is (of course) necessary and sufficient that the individual terms in the expanded product are regular. These terms have the form

$$\pm\prod_{\ell\in I}(x_{i_\ell}y_{j_\ell})\cdot\prod_{\ell\notin I}(y_{i_\ell}x_{j_\ell})$$

for a subset I of $\{1,\dots,k\}$. A monomial is regular if substituting x_i for y_i throughout results in a power of $x_1\cdots x_n$. In this case, this gives us

$$\pm\prod_{\ell=1}^{k}(x_{i_\ell}x_{j_\ell}),$$

and so we see: The bracket monomial is regular if and only if all numbers $1, \dots, n$ occur in $i_1, \dots, i_k, j_1, \dots, j_k$ an equal number m of times. As a consequence, we must have $mn = 2k$, and the monomial is m-regular.

(2) If a bracket polynomial is regular, we can write it as a homogeneous polynomial in the bracket symbols, such that each monomial term is regular according to (1).[4]

(3) In order to ensure symmetry, we can do the following: Replace the polynomial $f(\mathbf{x}, \mathbf{y})$ under consideration by

$$\frac{1}{n!} \sum_{\sigma \in S_n} f(\sigma \mathbf{x}, \sigma \mathbf{y}).$$

It is clearly simultaneously symmetric, and if $f(\mathbf{x}, \mathbf{y})$ was simultaneously symmetric already, we have changed nothing.

In this way, we can find all bracket invariants of prescribed weight.

EXAMPLE. Let $n = 2$. Then there is (essentially) only one bracket $[1\,2]$, and we see that the only bracket invariants (up to scalar multiples) are the even powers. In other words, the only bracket invariants are

$$(a_1^2 - a_0 a_2)^k, \quad k \geq 0.$$

EXAMPLE. Let $n = 3$. Then we get the even powers of $[1\,2][1\,3][2\,3]$ as the only bracket invariants, i.e.,

$$(3a_1^2 a_2^2 - a_0^2 a_3^2 - 4a_0 a_2^3 - 4a_1^3 a_3 + 6a_0 a_1 a_2 a_3)^k, \quad k \geq 0.$$

The expression in the parentheses is $d(P)/27$.

EXAMPLE. Let $n = 4$. Then a bracket invariant must have even weight. For $k = 2$, there is nothing. For $k = 4$, we get an invariant

$$i = a_0 a_4 - 4a_1 a_3 + 3a_2^2,$$

corresponding to

$$24i = [1\,2]^2[3\,4]^2 + [1\,3]^2[2\,4]^2 + [1\,4]^2[2\,3]^2.$$

For $k = 6$, we get only

$$j = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix} = a_0 a_2 a_4 + 2a_1 a_2 a_3 - a_0 a_3^2 - a_1^2 a_4 - a_2^3,$$

from starting with the bracket monomial $[1\,2]^2[3\,4]^2[1\,3][2\,4]$.

For $k = 8$, the only bracket invariant is i^2, and for $k = 10$ we get simply ij.

For $k = 12$, we immediately get i^3, j^2 and $d(P)$. In fact, i^3 and j^2 generate the space of weight-12 bracket invariants, and a computation shows that

$$i^3 - 27j^2 = \frac{1}{256} d(P).$$

By Proposition B.2.1, the possible weights of invariants for the quartic binary form are the even numbers. From the above, it is clear that we can find invariants of any even weight ≥ 4, just by taking polynomials in i and j.

[4] Of course we are free to add spurious terms like $[i\,j] + [j\,i]$, but why should we?

As the above results indicate, it is true that all invariants for the binary quartic are polynomials in i and j. This is not, however, a trivial result, and we will not prove it.

In principle, we can determine $\mathbb{C}$-bases for the spaces of weight-k bracket invariants for any binary form $P(x, y)$ and any k, using the above procedure together with some linear algebra.

NOTE. Apart from the obvious relation

$$[i\,j] = -[j\,i] \tag{B.3.3}$$

between brackets, there is also an equality

$$[i\,j][k\,\ell] = [i\,\ell][k\,j] + [i\,k][j\,\ell]. \tag{B.3.4}$$

This can be used, for instance, to reduce the number of bracket polynomials needed to produce invariants.

EXAMPLE. For use in Chapter 2, we need to know something about bracket invariants for the binary quintic. Specifically about invariants of weights 5 and 35.

For weight 5, the matter is easily dealt with: We start with a product of five brackets, with each digit $1, \dots, 5$ occuring twice. Up to permutation, this is either

$$[1\,2][2\,3][3\,4][4\,5][5\,1] \quad \text{or} \quad [1\,2]^2[3\,4][4\,5][5\,3].$$

In the first case, the permutation (25)(34) changes the sign of the bracket monomial, and in the second this is accomplished by (45). In either case, the symmetrisation is therefore 0, and there are *no* non-zero bracket invariants of weight 5 (and degree 2).

Beyond that, however, it is convenient to limit the scope of the search before actually starting:

The possible weights of an invariant are the multiples of 5, i.e., $k = 5m$. The degree is then $d = 2m$. A bracket invariant is a linear combination of symmetrisations of bracket monomials of the form

$$[1\,2]^{e_{12}}[1\,3]^{e_{13}}[1\,4]^{e_{14}}[1\,5]^{e_{15}}[2\,3]^{e_{23}}[2\,4]^{e_{24}}[2\,5]^{e_{25}}[3\,4]^{e_{34}}[3\,5]^{e_{35}}[4\,5]^{e_{45}},$$

where the exponents e_{ij} lie between 0 and $2m$, and satisfy the equations

$$\begin{aligned}
2m &= e_{12} + e_{13} + e_{14} + e_{15},\\
2m &= e_{12} + e_{23} + e_{24} + e_{25},\\
2m &= e_{13} + e_{23} + e_{34} + e_{35},\\
2m &= e_{14} + e_{24} + e_{34} + e_{45},\\
2m &= e_{15} + e_{25} + e_{35} + e_{45}.
\end{aligned}$$

(Since each digit must occur in exactly $2m$ brackets.) This system is easily solved, giving us

$$\begin{aligned}
e_{12} &= e_{34} + e_{35} + e_{45} - m,\\
e_{13} &= e_{24} + e_{25} + e_{45} - m,\\
e_{14} &= 2m - e_{24} - e_{34} - e_{45},\\
e_{15} &= 2m - e_{25} - e_{35} - e_{45},\\
e_{23} &= 3m - e_{24} - e_{25} - e_{34} - e_{35} - e_{45}.
\end{aligned}$$

Using the relation (B.3.4), we can reduce to the case where at least two exponents are 0. Permuting, we may therefore assume $e_{35} = e_{45} = 0$ or $e_{24} = e_{35} = 0$.

In the first case, the equations become

$$\begin{aligned}
e_{12} &= e_{34} - m,\\
e_{13} &= e_{24} + e_{25} - m,\\
e_{14} &= 2m - e_{24} - e_{34},\\
e_{15} &= 2m - e_{25},\\
e_{23} &= 3m - e_{24} - e_{25} - e_{34},
\end{aligned}$$

which result in valid sets of exponents for

$$\begin{gathered}
m \le e_{34} \le 2m, \quad 0 \le e_{24} \le 2m - e_{34},\\
\max\{0, m - e_{24}\} \le e_{25} \le \min\{2m, 3m - e_{24} - e_{34}\}.
\end{gathered}$$

For $m = 7$, this gives a total of 204 cases, all of which have symmetrisation 0. (This is best checked by computer.)

In the second case, we get the equations

$$\begin{aligned}
e_{12} &= e_{34} + e_{45} - m,\\
e_{13} &= e_{25} + e_{45} - m,\\
e_{14} &= 2m - e_{34} - e_{45},\\
e_{15} &= 2m - e_{25} - e_{45},\\
e_{23} &= 3m - e_{25} - e_{34} - e_{45},
\end{aligned}$$

and may assume that e_{24} and e_{35} are the *only* exponents equal to 0. The valid exponents are then obtained for

$$\begin{gathered}
1 \le e_{45} \le 2m, \quad \max\{1, m + 1 - e_{45}\} \le e_{34} \le 2m - 1 - e_{45},\\
\max\{1, m + 1 - e_{45}\} \le e_{25} \le \min\{2m - 1 - e_{45}, 3m - 1 - e_{34} - e_{45}\}.
\end{gathered}$$

For $m = 7$, this results in 272 cases, and again all symmetrisations are zero.

Thus, we may conclude that there are *no* weight-35 (degree-14) bracket invariants for the binary quintic.

B.4. The First Fundamental Theorem of Invariant Theory

We are still looking at a binary form $P(x, y)$ of degree n.

THE FIRST FUNDAMENTAL THEOREM. *Let $I(\mathbf{a}) \in \mathbb{C}[\mathbf{a}]$ be a polynomial invariant for $P(x, y)$. Then $I(\mathbf{a})$ is a bracket polynomial when written out in terms of $\mathbf{x}$ and $\mathbf{y}$ according to* (B.3.2).

In other words: The brackets invariants introduced in the previous section are the *only* polynomial invariants for a binary form.

REMARK. The *Second* Fundamental Theorem of Invariant Theory states that (B.3.3) and (B.3.4) gives *all* algebraic dependencies between the bracket symbols $[i\,j]$. These two relations are known as *syzygies*.

In order to prove the First Fundamental Theorem, we need a good deal of preparation.

We start by noting that the transformation (B.3.1) is not really the most natural way to define an action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}^2$: It has

$$\mathbf{A}\colon \mathbf{v} \mapsto \frac{\mathbf{A}\mathbf{v}}{\det \mathbf{A}},$$

where one would expect

$$\mathbf{A}\colon \mathbf{v} \mapsto \mathbf{A}\mathbf{v},$$

i.e.,

$$(x_i, y_i) \mapsto (\hat{x}_i, \hat{y}_i) = (\alpha x_i + \beta y_i, \gamma x_i + \delta y_i).$$

Now, let $I(\mathbf{a})$ be a polynomial invariant of weight k, and write it as a polynomial in $(\mathbf{x}, \mathbf{y})$ by (B.3.2). Then $I(\mathbf{x}, \mathbf{y})$ is homogeneous of degree $2k$ (by Proposition B.2.1), and

$$I(\mathbf{x}, \mathbf{y}) = \det \mathbf{A}^k\, I(\bar{\mathbf{x}}, \bar{\mathbf{y}}) = \det \mathbf{A}^{-k}\, I(\hat{\mathbf{x}}, \hat{\mathbf{y}}),$$

or

$$I(\hat{\mathbf{x}}, \hat{\mathbf{y}}) = \det \mathbf{A}^k\, I(\mathbf{x}, \mathbf{y}). \tag{B.4.1}$$

Conversely, if $I(\mathbf{a}) = I(\mathbf{x}, \mathbf{y})$ satisfies this last relation, then it is in fact an invariant of weight k.

Thus, to prove the Fundamental Theorem we can look at polynomials $I(\mathbf{x}, \mathbf{y})$ satisfying (B.4.1) and demonstrate that they are polynomials in the bracket symbols. This is exactly what we will do.

First, we introduce notation to reflect our new viewpoint: Let $G = \mathrm{GL}_2(\mathbb{C})$.[5] A *linear representation* of G is then an action of G as automorphisms on a finite-dimensional $\mathbb{C}$-vector space V, i.e., a homomorphism $G \to \mathrm{GL}_{\mathbb{C}}(V)$. The *dimension* of the representation is the vector space dimension $\dim_{\mathbb{C}} V$.

A *relative invariant* is a map $f\colon V \to \mathbb{C}$ satisfying

$$f(\sigma v) = \chi(\sigma) f(v), \quad \forall \sigma \in G,\ v \in V,$$

for some character $\chi\colon G \to \mathbb{C}^*$. The character χ is called the *weight* of f.

We will be interested in *polynomial* representations and relative invariants: If $(v_1, \ldots, v_m)$ is a basis for V, the matrix representing the action of $\sigma \in G$ on V

[5] Much of what is said in the following can be done more generally, either for an arbitrary group, or at least for subgroups of $\mathrm{GL}_n(\mathbb{C})$. We invite the reader to make the necessary generalisations.

in this basis should have entries that are polynomials in the entries of σ. Also, the image under f of a vector $v = \sum_i b_i v_i$ should be a polynomial in $b_1, \dots, b_m$.

In particular, from the Remark on p. 220 we get that a character χ is necessarily a (non-negative) power of the determinant map $\det\colon G \to \mathbb{C}^*$. We will therefore speak of a relative invariant as having weight k, when $\chi = \det^k$.

If the polynomials expressing a polynomial representation or relative invariant are all homogeneous of the same degree, we speak of *homogeneous* representations and relative invariants.

The concept of polynomial/homogeneous representations and relative invariants is clearly independent of the choice of basis. In fact, the polynomials involved can be considered as elements of the ring $\mathbb{C}[V^*]$ of polynomial maps on V. (Here, $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is the dual space.)

If G acts on spaces $V_1, \dots, V_r$, a *joint* (or *simultaneous*) relative invariant of weight k is a map $f\colon V_1 \times \cdots \times V_r \to \mathbb{C}$ satisfying

$$f(\sigma v_1, \dots, \sigma v_r) = \det(\sigma)^k f(v_1, \dots, v_r)$$

for all $\sigma \in G$ and all $(v_1, \dots, v_r) \in V_1 \times \cdots \times V_r$. This is the same as a relative invariant $f\colon V \to W$, when G acts entry-wise on $V = V_1 \times \cdots \times V_r$.

We can now offer the first precise formulation of the result we aim to prove:

Fundamental Theorem, v. 2. *Let*

$$I\colon (v_1, \dots, v_n) \mapsto I(v_1, \dots, v_n)$$

be a homogeneous joint relative invariant of weight k and degree d in n vectors $v_1, \dots, v_n$ from $\mathbb{C}^2$. Then $d = 2k$, and I is a linear combination of products of the form

$$|v_{i_1}\, v_{j_1}| \cdots |v_{i_k}\, v_{j_k}|,$$

where $1 \le i_\ell, j_\ell \le n$, and $|v_i\, v_j|$ is the determinant of the 2×2 matrix with columns v_i and v_j.

The Fundamental Theorem as first formulated clearly follows from v. 2, simply by letting

$$v_i = (x_i, y_i),$$

and hence

$$|v_i\, v_j| = [i\, j].$$

But we can reformulate even further:

Let $f(\mathbf{z}) = f(z_1, \dots, z_m)$ be a homogeneous polynomial of degree d, and let $\mathbf{z}_1, \dots, \mathbf{z}_d$ be d sets of m indeterminates. Then we can write

$$f(\lambda_1 \mathbf{z}_1 + \cdots + \lambda_d \mathbf{z}_d) = \sum_{|\mathbf{i}|=d} \boldsymbol{\lambda}^{\mathbf{i}} f_{\mathbf{i}}(\mathbf{z}_1, \dots, \mathbf{z}_d), \tag{B.4.2}$$

where we have used the standard notation for multi-indices: For $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_d)$ and $\mathbf{i} = (i_1, \dots, i_d) \in \mathbb{N}_0^d$ we let $\boldsymbol{\lambda}^{\mathbf{i}} = \lambda_1^{i_1} \cdots \lambda_d^{i_d}$ and $|\mathbf{i}| = i_1 + \cdots + i_d$.

This decomposition is unique, and we can recover $f(\mathbf{z})$ from any $f_{\mathbf{i}}(\mathbf{z}_1, \dots, \mathbf{z}_d)$ by

$$\binom{d}{\mathbf{i}} f(\mathbf{z}) = f_{\mathbf{i}}(\mathbf{z}, \dots, \mathbf{z}),$$

where

$$\binom{d}{\mathbf{i}} = \binom{d}{i_1, \dots, i_d} = \frac{d!}{i_1! \cdots i_d!}$$

is the multinomial coefficient. For: Letting $\mathbf{z}_1 = \cdots = \mathbf{z}_d = \mathbf{z}$, we get

$$\begin{aligned}\sum_{|\mathbf{i}|=d} \boldsymbol{\lambda}^{\mathbf{i}} f_{\mathbf{i}}(\mathbf{z}, \dots, \mathbf{z}) &= f\big((\lambda_1 + \cdots + \lambda_d)\mathbf{z}\big) \\ &= (\lambda_1 + \cdots + \lambda_d)^d f(\mathbf{z}) = \sum_{|\mathbf{i}|=d} \binom{d}{\mathbf{i}} \boldsymbol{\lambda}^{\mathbf{i}} f(\mathbf{z}).\end{aligned}$$

We define the *polarisation* of $f(\mathbf{z})$ as

$$Pf(\mathbf{z}_1, \dots, \mathbf{z}_d) = f_{(1,\dots,1)}(\mathbf{z}_1, \dots, \mathbf{z}_d).$$

From the definition of $f_{\mathbf{i}}(\mathbf{z}_1, \dots, \mathbf{z}_d)$, it is then clear that the polarisation is multilinear and symmetric in $\mathbf{z}_1, \dots, \mathbf{z}_d$, and that we can get $f(\mathbf{z})$ back through

$$f(\mathbf{z}) = \frac{1}{d!} Pf(\mathbf{z}_1, \dots, \mathbf{z}_d).$$

If $f\colon \mathbb{C}^m \to \mathbb{C}$ is a relative invariant, the uniqueness of the decomposition in (B.4.2) ensures that each $f_{\mathbf{i}}(\mathbf{z}_1, \dots, \mathbf{z}_r)$ will be a joint relative invariant on $\mathbb{C}^m \times \cdots \times \mathbb{C}^m$.

Specifically, we have

PROPOSITION B.4.1. *Let $f\colon U \to \mathbb{C}$ be a homogeneous relative invariant of degree d, and let $Pf\colon U^d \to V$ be the polarisation. Then Pf is a multilinear (joint) relative invariant.*

This allows us to reduce v. 2 of the Fundamental Theorem above to

FUNDAMENTAL THEOREM, V. 3. *Let*

$$J\colon (v_1, \dots, v_n) \mapsto J(v_1, \dots, v_n)$$

be a non-zero multilinear joint invariant on $\mathbb{C}^2 \times \cdots \times \mathbb{C}^2$ of weight k. Then $n = 2k$, and $J(v_1, \dots, v_n)$ is a linear combination of expressions

$$|v_{\sigma 1}\, v_{\sigma 2}| \cdots |v_{\sigma(n-1)}\, v_{\sigma n}|$$

for $\sigma \in S_n$.

PROOF OF V. 3 $\Rightarrow$ V. 2: Let $I(v_1, \dots, v_n)$ be a homogeneous joint invariant as in v. 2. We let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{C}^{2n}$ and polarise: If $I(\mathbf{v})$ has degree d, we get a multilinear relative invariant

$$PI(\mathbf{v}_1, \dots, \mathbf{v}_d),$$

where the $\mathbf{v}_i$'s are in $\mathbb{C}^{2n}$, and G's action is given as matrix multiplication on pairs of coordinates (as for $\mathbf{v}$). Write each $\mathbf{v}_i$ as

$$\mathbf{v}_i = \sum_{j=1}^{n} \mathbf{v}_{(i,j)},$$

where $\mathbf{v}_{(i,j)}$ has the same coordinates as $\mathbf{v}_i$ on the $(2j-1)^{\text{th}}$ and $2j^{\text{th}}$ places, and zeroes elsewhere. Then $\mathbf{v}_{(i,j)}$ is effectively an element of $\mathbb{C}^2$, and G acts on it by matrix multiplication. Expand

$$PI(\mathbf{v}_1,\dots,\mathbf{v}_d) = \sum_{1\le j_1,\dots,j_d\le n} PI(\mathbf{v}_{(1,j_1)},\dots,\mathbf{v}_{(d,j_d)}).$$

Each summand is then a multilinear relative invariant over copies of $\mathbb{C}^2$. From v. 3 we get that these summand are linear combinations of product of 2×2 determinants, and when we specialise the polarisation to get our original invariant back, $\mathbf{v}_{(i,j)}$ specialises to v_j, and the determinants to $|v_i\, v_j|$'s. This proves v. 2. □

The hard part is now to prove v. 3.

Semi-simple algebras. The proof of v. 3, as we give it, makes use of some structure theory of finite-dimensional semi-simple algebras over $\mathbb{C}$. We refer to e.g. [Ja2, 3.5 & 4.3–4.4] for more comprehensive accounts, as well as the Appendix in [D&C].

For simplicity, we will assume in this section that all rings are finite-dimensional $\mathbb{C}$-algebras (with units), and that all modules are finitely generated unitary left modules.

Definition B.4.2. Let $\mathfrak{A}$ be an algebra, and let M be a module.

(i) M is called *irreducible*, if $M\neq 0$ and the only submodules are 0 and M.
(ii) M is called *completely reducible*, if M is a direct sum of irreducible submodules.
(iii) $\mathfrak{A}$ is called *simple*, if $\mathfrak{A}\neq 0$ and the only two-sided ideals are 0 and $\mathfrak{A}$.
(iv) $\mathfrak{A}$ is called *semi-simple*, if $\mathfrak{A}$ is a direct sum of simple rings.

Lemma B.4.3. *The following conditions are equivalent for an $\mathfrak{A}$-module M:*

(i) *M is completely reducible.*
(ii) *M is a (not necessarily direct) sum of irreducible submodules.*
(iii) *Every submodule of M is a direct summand.*
(iv) *M is a subdirect product of irreducible modules, i.e., M embeds into a direct product $\prod_i N_i$ of irreducible modules, such that $M\hookrightarrow \prod_i N_i \twoheadrightarrow N_i$ is surjective for all i.*

Moreover, a submodule of a completely reducible module is completely reducible.

Proof. (i) ⇒ (ii) is clear. (ii) ⇒ (iii): Let $M=\sum_i N_i$ wth N_i irreducible. We may assume the sum to be finite, i.e., $M=N_1+\cdots+N_s$. Also, let N be an arbitrary submodule. We can then write $M=N\oplus N_{i_1}\oplus\cdots\oplus N_{i_t}$ by letting i_j be the smallest i with $N_i\nsubseteq N\oplus N_{i_1}\oplus\cdots\oplus N_{i_{j-1}}$.

It follows from this argument that every submodule is completely reducible: Given $N\subseteq M$, we write $M=N\oplus N'$ and get $N\simeq M/N'=\sum_i (N_i+N')/N'$. Since $(N_i+N')/N'\simeq N_i/N_i\cap N'$ is either 0 or irreducible, we have (iii) satisfied for the module N.

(iii) ⇒ (i) is obvious, as is (i) ⇒ (iv).

(iv) $\Rightarrow$ (i): By assumption, we have submodules M_i of M, such that $\bigcap_i M_i = 0$ and M/M_i is irreducible. Since M is finite-dimensional over $\mathbb{C}$, we in fact have a finite intersection $M_1 \cap \cdots \cap M_s = 0$. Thus, M embeds into the completely reducible module $M/M_1 \oplus \cdots \oplus M/M_s$. □

Schur's Lemma. *Let M and N be irreducible $\mathfrak{A}$-modules. Then any module homomorphism $\varphi\colon M \to N$ is either zero or an isomorphism.*

The Density Theorem. *Let M be a completely reducible $\mathfrak{A}$-module. Also, let $\mathfrak{B} = \operatorname{End}_{\mathfrak{A}} M$ and $\mathfrak{C} = \operatorname{End}_{\mathfrak{B}} M$. Then the map*

$$a \mapsto [m \mapsto am]$$

from $\mathfrak{A}$ into $\mathfrak{C}$ is surjective.

Proof. First, we note that an $\mathfrak{A}$-submodule N of M is also a $\mathfrak{C}$-submodule: Write $M = N \oplus N'$, and let $\pi\colon M \to N$ be the corresponding projection. Then $\pi \in \mathfrak{B}$, and for $c \in \mathfrak{C}$ we get $cN = c\pi M = \pi(cM) \subseteq \pi M = N$.

What we need to prove is the following: Given $m_1, \ldots, m_n \in M$ and $c \in \mathfrak{C}$, there is an $a \in \mathfrak{A}$ with $am_i = cm_i$ for all i. This is clearly enough, since M is finitely generated.

Assume first that $n = 1$, and that we therefore have $m \in M$ and $c \in \mathfrak{C}$. By our observation above, $N = \mathfrak{A}m$ is a $\mathfrak{C}$-submodule of M, and so $cm \in N$, i.e., $cm = am$ for some $a \in \mathfrak{A}$.

For an arbitrary n, we first replace M by M^n. An $\mathfrak{A}$-endomorphism on M^n is essentially an $n \times n$ matrix of elements from $\mathfrak{B}$, and the map $(m_1, \ldots, m_n) \mapsto (cm_1, \ldots, cm_n)$ is an $\operatorname{End}_{\mathfrak{A}}(M^n)$-endomorphism on M^n. Thus, by the $n = 1$ case, for any $(m_1, \ldots, m_n) \in M^n$, there exists $a \in \mathfrak{A}$ with $am_i = cm_i$ for all i. □

Corollary B.4.4. *An algebra $\mathfrak{A}$ is simple if and only if $\mathfrak{A} \simeq \operatorname{Mat}_n(\mathbb{C})$ for some n.*

Proof. 'If' is clear. 'Only if': Let M be an irreducible $\mathfrak{A}$-module. By Schur's Lemma, the algebra $\mathfrak{B} = \operatorname{End}_{\mathfrak{A}} M$ is a skew field, and since it is finite-dimensional over $\mathbb{C}$, we have $\mathfrak{B} = \mathbb{C}$. Thus, by the Density Theorem, $\mathfrak{A}$ maps onto $\operatorname{End}_{\mathbb{C}} M \simeq \operatorname{Mat}_n(\mathbb{C})$ (with $n = \dim_{\mathbb{C}} M$). Since $\mathfrak{A}$ is simple, the map is injective, and hence an isomorphism. □

Lemma B.4.5. *Let $\mathfrak{A}$ be simple. Then $\mathfrak{A}$ is completely reducible as an $\mathfrak{A}$-module, and any two irreducible $\mathfrak{A}$-modules are isomorphic.*

Proof. Write $\mathfrak{A} \simeq \operatorname{Mat}_n(\mathbb{C})$, and let $\mathfrak{a}_i$ be the left ideal consisting of matrices that are zero outside of the i^{th} column. Then $\mathfrak{a}_i$ is irreducible, and $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$. If M is an irreducible $\mathfrak{A}$-module, we have $M = \mathfrak{A}m$ for some $m \in M$, and hence $M = \mathfrak{a}_1 m + \cdots + \mathfrak{a}_n m$. For some i, $\mathfrak{a}_i m \neq 0$ and so $\mathfrak{a}_i \simeq \mathfrak{a}_i m = M$. □

Theorem B.4.6. *The following conditions are equivalent for an algebra $\mathfrak{A}$:*

(i) *$\mathfrak{A}$ is semi-simple.*
(ii) *$\mathfrak{A}$ is isomorphic to a direct sum of matrix rings over $\mathbb{C}$.*
(iii) *$\mathfrak{A}$ is completely reducible as an $\mathfrak{A}$-module.*

PROOF. (i) $\Leftrightarrow$ (ii) is obvious, and (i) $\Rightarrow$ (iii) follows from the Lemma.

(iii) $\Rightarrow$ (i): Write $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$, where the $\mathfrak{a}_i$'s are minimal left ideals (and hence irreducible). Then we have

$$\mathfrak{A} \hookrightarrow \operatorname{End}_{\mathbb{C}} \mathfrak{a}_1 \oplus \cdots \oplus \operatorname{End}_{\mathbb{C}} \mathfrak{a}_s$$

by

$$a \mapsto (x \mapsto ax, \ldots, x \mapsto ax).$$

As in the proof of Corollary B.4.4, we see that $\mathfrak{A} \to \operatorname{End}_{\mathbb{C}} \mathfrak{a}_i$ is onto, and hence $\mathfrak{A}$ is a subdirect product of simple rings.

Considering $\mathfrak{A}$ as a module over $\mathfrak{A} \otimes_{\mathbb{C}} \mathfrak{A}^{\mathrm{op}}$ by $(a \otimes b)x = abx$, we see that this means: $\mathfrak{A}$ is completely reducible as an $\mathfrak{A} \otimes_{\mathbb{C}} \mathfrak{A}^{\mathrm{op}}$-module, and is thus a direct sum of irreducible submodules, i.e., a direct sum of simple rings. □

It is clear that the decomposition of a semi-simple algebra as a direct sum of simple rings (so-called *simple components*) is unique. From this again, we get that every module over a semi-simple algebra is completely reducible, and that the decomposition into a direct sum of irreducible submodules is essentially unique. We then speak of *irreducible components*.

The *center*

$$Z(\mathfrak{a}) = \{a \in \mathfrak{A} \mid \forall b \in \mathfrak{A} \colon ab = ba\}$$

of an algebra $\mathfrak{A}$ is a subalgebra, and from the above structure theorem we see that

$$Z(\mathfrak{A}) \simeq \mathbb{C}^d,$$

for a semi-simple algebra $\mathfrak{A}$, where d is the number of simple components. This d is also the number of isomorphism classes of irreducible $\mathfrak{A}$-modules (and/or minimal left ideals in $\mathfrak{A}$).

THE SCHUR COMMUTATOR THEOREM. *Let $N \in \mathbb{N}$, and let $\mathfrak{A}$ be a semi-simple subalgebra of* $\operatorname{Mat}_N(\mathbb{C})$. *Also, let*

$$\mathfrak{B} = C_{\operatorname{Mat}_N(\mathbb{C})}(\mathfrak{A}) = \{b \in \operatorname{Mat}_N(\mathbb{C}) \mid \forall a \in \mathfrak{A} \colon ab = ba\}$$

be $\mathfrak{A}$'s commutator. *Then the following statements hold:*

(a) *If*

$$\mathfrak{A} \simeq \operatorname{Mat}_{m_1}(\mathbb{C}) \oplus \cdots \oplus \operatorname{Mat}_{m_d}(\mathbb{C})$$

is the decomposition of $\mathfrak{A}$ into simple components, and

$$\mathbb{C}^N \simeq (\mathbb{C}^{m_1})^{n_1} \oplus \cdots \oplus (\mathbb{C}^{m_d})^{n_d}$$

is the corresponding decomposition of $\mathbb{C}^N$ into irreducible components, then

$$\mathfrak{B} \simeq \operatorname{Mat}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \operatorname{Mat}_{n_d}(\mathbb{C}).$$

In particular, $\mathfrak{B}$ is semi-simple.

(b) $\mathfrak{A} = C_{\operatorname{Mat}_N(\mathbb{C})}(\mathfrak{B})$.

(c) *If $a \in \mathfrak{A}$ generates a minimal left ideal in $\mathfrak{A}$, then $a\mathbb{C}^N$ is an irreducible $\mathfrak{B}$-submodule of $\mathbb{C}^N$. Furthermore,* every *irreducible $\mathfrak{B}$-submodule of $\mathbb{C}^N$ has the form $a\mathbb{C}^N$ for some $a \in \mathfrak{A}$ generating a minimal left ideal. If a and a' generate isomorphic minimal left ideals in $\mathfrak{A}$, then $a\mathbb{C}^N$ and $a'\mathbb{C}^N$ are isomorphic irreducible $\mathfrak{B}$-modules.*

PROOF. Consider a decomposition of $\mathfrak{A}$ and $\mathbb{C}^N$ as in (a), and pick the 'obvious' basis for $\mathbb{C}^N$ over $\mathbb{C}$, consisting of the vectors corresponding to the canonical bases for $\mathbb{C}^{m_1}, \dots, \mathbb{C}^{m_d}$. In this basis, an element $a \in \mathfrak{A}$ corresponding to a tuple $(\mathbf{A}_1, \dots, \mathbf{A}_d)$ in the decomposition will be represented by the block diagonal matrix

$$\begin{pmatrix} \mathbf{A}_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \mathbf{A}_1 & & & & & & \\ & & & \mathbf{A}_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \mathbf{A}_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & \mathbf{A}_d & \\ & & & & & & & & \ddots \\ & & & & & & & & & \mathbf{A}_d \end{pmatrix},$$

with n_i occurences of the matrix $\mathbf{A}_i$ along the diagonal.

Using block matrix multiplication, it is easy to see that the centraliser of $\mathfrak{A}$ then consists of the matrices

$$\begin{pmatrix} b_{11}^{(1)}\mathbf{E}_1 & \dots & b_{1n_1}^{(1)}\mathbf{E}_1 & & & & & \\ \vdots & \ddots & \vdots & & & & & \\ b_{n_11}^{(1)}\mathbf{E}_1 & \dots & b_{n_1n_1}^{(1)}\mathbf{E}_1 & & & & & \\ & & & \ddots & & & & \\ & & & & b_{11}^{(d)}\mathbf{E}_d & \dots & b_{1n_d}^{(d)}\mathbf{E}_d \\ & & & & \vdots & \ddots & \vdots \\ & & & & b_{n_d1}^{(d)}\mathbf{E}_d & \dots & b_{n_dn_d}^{(d)}\mathbf{E}_d \end{pmatrix},$$

where $\mathbf{E}_i$ is the $n_i \times n_i$ unit matrix, and $b_{ij}^{(k)} \in \mathbb{C}$. The i^{th} block then gives a summand of $\mathfrak{B}$ isomorphic to $\mathrm{Mat}_{n_i}(\mathbb{C})$. This proves (a).

This representation of $\mathfrak{B}$ also demonstrates that $\mathbb{C}^{n_i}$ occurs exactly m_i times in a decomposition of $\mathbb{C}^N$. From (a) it then follows that

$$C_{\mathrm{Mat}_N(\mathbb{C})}(\mathfrak{B}) \simeq \mathfrak{A}.$$

Since $\mathfrak{A}$ is trivially contained in the centraliser of $\mathfrak{B}$, they must therefore be equal. This proves (b).

As for (c): By (b), we may interchange $\mathfrak{A}$ and $\mathfrak{B}$. Also, by a proper choice of basis, we may assume the minimal left ideal of $\mathfrak{B}$ to consist of matrices

with $b_{ij}^{(k)} = 0$ for $j > 1$ or $k > 1$. A generator b is then given by any choice of $(b_{11}^{(1)}, \ldots, b_{n_1 1}^{(1)})$ other than the zero vector, and we see that $b\mathbb{C}^N$ is isomorphic to $\mathbb{C}^{m_1}$ as an $\mathfrak{A}$-module.

Conversely, if we have an irreducible $\mathfrak{A}$-submodule of $\mathbb{C}^N$, we may assume it to consist of all vectors that are zero outside of the first m_1 coordinates, and we can get it by letting $b_{11}^{(1)} = 1$ and letting all other $b_{ij}^{(k)}$'s be zero.

Finally: If a and a' generate isomorphic minimal left ideals in $\mathfrak{A}$, then there exist units p and u in $\mathfrak{A}^*$ with $a' = puap^{-1}$. (This is clear, since we are in effect looking at a matrix ring $\mathrm{Mat}_m(\mathbb{C})$.) Now, multiplication by pu is a $\mathfrak{B}$-automorphism on $\mathbb{C}^N$, and

$$a'\mathbb{C}^N = puap^{-1}\mathbb{C}^N = pua\mathbb{C}^N \simeq a\mathbb{C}^N.$$

This completes the proof of (c). □

An important example (for us) of semi-simple algebras is group rings:

MASCHKE'S THEOREM. *Let G be a finite group. Then the group ring $\mathbb{C}[G]$ is semi-simple.*

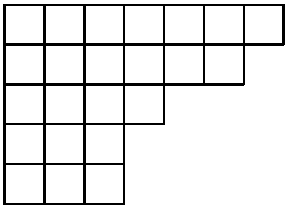
We refer to Exercise 7.2 in Chapter 7 for proof.

The number of simple components in a group ring $\mathbb{C}[G]$ is equal to the number of conjugacy classes in G, since an element $\sum_{\sigma\in G} a_\sigma \sigma$ is central if and only if the coefficients a_σ and a_τ are equal whenever σ and τ are conjugate. This, then, is also the number of non-isomorphic minimal left ideals in $\mathbb{C}[G]$.

Young tableaux. To prove the Fundamental Theorem, we need to know the structure of the minimal left ideals in the group ring $\mathbb{C}[S_d]$. This ring is of course semi-simple by Maschke's Theorem.

To describe the minimal left ideals, we make use of the so-called Young tableaux. Of course, our exposition will be brief and superficial. For a much more thorough account of Young tableaux, we suggest [Ful].

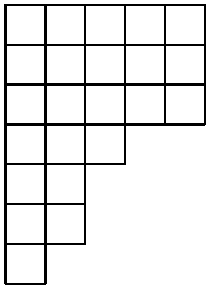
A *Young diagram* λ is a non-increasing sequence of positive integers: $\lambda = (\lambda_1, \ldots, \lambda_r)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$. A Young diagram can be readily visualised in the form



$\lambda = (7, 6, 4, 3, 3)$

A Young diagram is just a partition of the number $d = |\lambda| = \lambda_1 + \cdots + \lambda_r$, which we refer to as the *size* of λ.

From the visualisation, it is clear that a Young diagram 'hides' a second partition of d as well, obtained as the lengths of the columns rather than the rows. In the example above, this second partition would be



$\tilde{\lambda} = (5, 5, 5, 3, 2, 2, 1)$

This 'flipped-over' diagram is called the *conjugate* of λ, written $\tilde{\lambda}$.

The whole point of Young diagrams (from our point of view) is to produce such pairs of related partitions.

Given a Young diagram λ, a *Young tableau* Σ_λ is a family

$$\Sigma_\lambda = (m_{ij} \mid 1 \leq i \leq r,\ 1 \leq j \leq \lambda_i)$$

of distinct integers between 1 and $d = |\lambda|$, corresponding to the boxes in the diagram:

$$\begin{array}{llll} m_{11} & m_{12} & \dots & m_{1\lambda_1} \\ m_{21} & \dots & m_{2\lambda_2} & \\ \vdots & & & \\ m_{r1} & \dots & m_{r\lambda_r} & \end{array}$$

In other words: We have distributed the numbers $1, \dots, d$ in the diagram.

The symmetric group S_d acts (regularly) on the set of tableaux corresponding to a single diagram λ by acting on the entries: $\sigma(m_{ij})_{i,j} = (\sigma m_{i,j})_{i,j}$ for $\sigma \in S_d$.

Corresponding to a tableaux Σ_λ, we get two subgroups $\mathcal{R}(\Sigma_\lambda)$ and $\mathcal{C}(\Sigma_\lambda)$ of S_d, consisting of those permutations preserving the rows, resp. the columns, of Σ_λ. Thus, $\mathcal{R}(\Sigma_\lambda)$ contains those elements of S_d with orbits inside

$$\{m_{1,1}, \dots, m_{1\lambda_1}\},\ \ \{m_{21}, \dots, m_{2\lambda_2}\},\ \ \dots,$$

and similarly for $\mathcal{C}(\Sigma_\lambda)$.

It is obvious that

$$\mathcal{R}(\Sigma_\lambda) \cap \mathcal{C}(\Sigma_\lambda) = 1,$$

and that we have

$$\mathcal{R}(\sigma\Sigma_\lambda) = \sigma\mathcal{R}(\Sigma_\lambda)\sigma^{-1}, \quad \mathcal{C}(\sigma\Sigma_\lambda) = \sigma\mathcal{C}(\Sigma_\lambda)\sigma^{-1}$$

for $\sigma \in S_d$.

In particular, the decomposition of an element in the product set

$$\mathcal{R}(\Sigma_\lambda)\mathcal{C}(\Sigma_\lambda) = \{\rho\kappa \mid \rho \in \mathcal{R}(\Sigma_\lambda),\ \kappa \in \mathcal{C}(\Sigma_\lambda)\}$$

is unique.

LEMMA B.4.7. (VON NEUMANN) *Let Σ_λ and Σ'_λ be two Young tableaux corresponding to the same Young diagram λ, and assume that no two integers occur*

in the same row of Σ_λ *and the same column of* Σ'_λ*. Then there exist* $\rho \in \mathcal{R}(\Sigma_\lambda)$ *and* $\kappa \in \mathcal{C}(\Sigma_\lambda)$ *with*

$$\rho\kappa\Sigma_\lambda = \Sigma'_\lambda.$$

PROOF. The elements in the first row of Σ_λ must all be in different columns of Σ'_λ, meaning that there exists $\kappa_1 \in \mathcal{C}(\Sigma'_\lambda)$ such that Σ_λ and $\kappa_1\Sigma'_\lambda$ have the same elements in the first row. Forgetting about the first rows, we repeat the process, and eventually get a $\kappa' \in \mathcal{C}(\Sigma'_\lambda)$ such that Σ_λ and $\kappa'\Sigma'_\lambda$ have the same elements in each row. In other words:

$$\rho\Sigma_\lambda = \kappa'\Sigma'_\lambda$$

for some $\rho \in \mathcal{R}(\Sigma_\lambda)$. Now,

$$\kappa'^{-1} \in \kappa'\mathcal{C}(\Sigma'_\lambda)\kappa'^{-1} = \mathcal{C}(\kappa'\Sigma'_\lambda) = \mathcal{C}(\rho\Sigma_\lambda) = \rho\mathcal{C}(\Sigma_\lambda)\rho^{-1},$$

and so $\kappa = \rho^{-1}\kappa'^{-1}\rho \in \mathcal{C}(\Sigma_\lambda)$. Since

$$\Sigma'_\lambda = \kappa'^{-1}\rho\Sigma_\lambda = \rho\kappa\Sigma_\lambda,$$

we have the result. □

REMARK. If λ and μ are *different* Young diagrams of the same size d, we may assume $\lambda > \mu$ in lexicographic ordering. Any Young tableaux Σ_λ and Σ'_μ must then necessarily have the property that some pair of integers occur in the same row of Σ_λ and in the same column of Σ'_μ. (Since at the very latest they must exist in the first row of Σ_λ that is longer than the corresponding row of Σ'_μ.)

COROLLARY B.4.8. *If* $\sigma \in S_d \setminus \mathcal{R}(\Sigma_\lambda)\mathcal{C}(\sigma_\lambda)$ *then there exists a transposition* $\tau \in \mathcal{R}(\Sigma_\lambda)$ *with* $\sigma^{-1}\tau\sigma \in \mathcal{C}(\Sigma_\lambda)$.

PROOF. By von Neumann's Lemma there must be integers i and j found in the same row of Σ_λ and in the same column of $\Sigma'_\lambda = \sigma\Sigma_\lambda$. Let $\tau = (ij)$. Then $\tau \in \mathcal{R}(\Sigma'_\lambda) = \sigma\mathcal{R}(\Sigma_\lambda)\sigma^{-1}$, i.e., $\sigma^{-1}\tau\sigma \in \mathcal{C}(\Sigma_\lambda)$. □

Given Σ_λ, we now let

$$\alpha_\lambda = \sum_{\rho\in\mathcal{R}(\Sigma_\lambda)} \rho,$$
$$\beta_\lambda = \sum_{\kappa\in\mathcal{C}(\Sigma_\lambda)} \operatorname{sign}(\kappa)\,\kappa$$

in $\mathbb{C}[S_d]$, where $\operatorname{sign}(\kappa)$ is the sign of the permutation κ.

Picking another tableau corresponding to λ just means applying a conjugation to α_λ and β_λ.

Since no terms in the product can cancel each other out, it is clear that

$$\gamma_\lambda = \alpha_\lambda\beta_\lambda \neq 0.$$

Also,

$$\rho\alpha_\lambda = \alpha_\lambda\rho = \alpha_\lambda \quad \text{for} \quad \rho \in \mathcal{R}(\Sigma_\lambda)$$

and

$$\kappa\beta_\lambda = \beta_\lambda\kappa = \operatorname{sign}(\kappa)\,\beta_\lambda \quad \text{for} \quad \kappa \in \mathcal{C}(\Sigma_\lambda).$$

THEOREM B.4.9. *The left ideals $\mathbb{C}[S_d]\gamma_\lambda$ in $\mathbb{C}[S_d]$ are minimal, and every minimal left ideal in $\mathbb{C}[S_d]$ is isomorphic to $\mathbb{C}[S_d]\gamma_\lambda$ for a unique Young diagram λ.*

PROOF. First of all: The number of isomorphism classes of minimal left ideals is equal to the number of conjugacy classes in S_d. Elements in S_d are conjugate if and only if they have the same cycle type. And a cycle type corresponds to a Young diagram in which there is a row of length e for every e-cycle. Thus, the number of isomorphism classes is equal to the number of Young diagrams.

Since we know that the isomorphism class of $\mathbb{C}[S_d]\gamma_\lambda$ depends only on the diagram λ, and not on any particular tableaux, we only need to prove

(a) $\mathbb{C}[S_d]\gamma_\lambda$ is a minimal left ideal, and
(b) if λ and μ are different Young diagrams of size d, the ideals $\mathbb{C}[S_d]\gamma_\lambda$ and $\mathbb{C}[S_d]\gamma_\mu$ are not isomorphic.

(a) Let $\mathfrak{a}$ be a minimal left ideal contained in $\mathbb{C}[S_d]\gamma_\lambda$. Then

$$\gamma_\lambda\mathfrak{a} \subseteq \gamma_\lambda\mathbb{C}[S_d]\gamma_\lambda \subseteq \alpha_\lambda\mathbb{C}[S_d]\beta_\lambda.$$

We prove below that $\alpha_\lambda\mathbb{C}[S_d]\beta_\lambda = \mathbb{C}\gamma_\lambda$. Hence, $\gamma_\lambda\mathfrak{a}$ is zero- or one-dimensional over $\mathbb{C}$. Now, since $\mathfrak{a}$ is a minimal left ideal in a semi-simple algebra, we have $\mathfrak{a}^2 \neq 0$ (in fact one-dimensional), and as $\gamma_\lambda\mathfrak{a} \supseteq \mathfrak{a}^2$, we have $\gamma_\lambda\mathfrak{a} = \mathbb{C}\gamma_\lambda$, and hence $\mathbb{C}[S_d]\gamma_\lambda = \mathbb{C}[S_d]\gamma_\lambda\mathfrak{a} \subseteq \mathfrak{a}$, i.e., $\mathfrak{a} = \mathbb{C}[S_d]\gamma_\lambda$.

(b) Assume $\lambda > \mu$ in lexicographic ordering. We prove below that $\alpha_\lambda x\beta_\mu = 0$ for all $x \in \mathbb{C}[S_d]$. It follows that $\mathbb{C}[S_d]\gamma_\lambda \cdot \mathbb{C}[S_d]\gamma_\mu = 0$, and hence that $\mathbb{C}[S_d]\gamma_\lambda$ and $\mathbb{C}[S_d]\gamma_\mu$ are not isomorphic.

It now remains to prove that $\alpha_\lambda\mathbb{C}[S_d]\beta_\lambda = \mathbb{C}\gamma_\lambda$ and that $\alpha_\lambda\mathbb{C}[S_d]\beta_\mu = 0$ for $\lambda > \mu$:

Let $\sigma \in S_d$. If $\sigma = \rho\kappa$ for $\rho \in \mathcal{R}(\Sigma_\lambda)$ and $\kappa \in \mathcal{C}(\Sigma_\lambda)$, we have $\alpha_\lambda\sigma\beta_\lambda = \operatorname{sign}(\kappa)\,\gamma_\lambda$. Otherwise, pick a transposition $\tau \in \mathcal{R}(\Sigma_\lambda)$ with $\sigma^{-1}\tau\sigma \in \mathcal{C}(\Sigma_\lambda)$ and write

$$\alpha_\lambda\sigma\beta_\lambda = -\alpha_\lambda\sigma(\sigma^{-1}\tau\sigma)\beta_\lambda = -\alpha_\lambda\sigma\beta_\lambda,$$

i.e., $\alpha_\lambda\sigma\beta_\lambda = 0$. This proves the first claim.

Next, let again $\sigma \in S_d$. By the Remark following von Neumann's Lemma, there must then be integers i and j in the same row of Σ_λ and the same column of $\sigma\Sigma'_\mu$. Let $\tau = (ij)$. Then $\tau \in \mathcal{R}(\Sigma_\lambda) \cap \mathcal{C}(\sigma\Sigma'_\mu)$, and so

$$\alpha_\lambda(\sigma\beta_\mu\sigma^{-1}) = -\alpha_\lambda\tau(\sigma\beta_\mu\sigma^{-1}) = -\alpha_\lambda(\sigma\beta_\mu\sigma^{-1}),$$

i.e., $\alpha_\lambda\sigma\beta_\mu = 0$. This proves the second claim. □

Homogeneous representations. Let $\rho\colon G = \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ be a homogeneous linear representation of degree d, and let $U = \mathbb{C}^2$. Also, let $e_1 = (1,0), e_2 = (0,1)$ be the standard basis for U.

For a multi-index $\mathbf{i} = (i_1, \ldots, i_d) \in I^d = \{1,2\}^d$ we let

$$e_{\mathbf{i}} = e_{i_1} \otimes \cdots \otimes e_{i_d}.$$

The $e_{\mathbf{i}}$'s then form a basis for the 2^d-dimensional space

$$U^{\otimes d} = U \otimes_{\mathbb{C}} \cdots \otimes_{\mathbb{C}} U.$$

The symmetric group S_d acts on multi-indices by

$$\sigma(i_1, \ldots, i_d) = (i_{\sigma^{-1}1}, \ldots, i_{\sigma^{-1}d}),$$

and hence on $U^{\otimes d}$ by

$$\sigma e_{\mathbf{i}} = e_{\sigma\mathbf{i}}.$$

It follows that we have the group ring $\mathbb{C}[S_d]$ mapping to the endomorphism ring $\mathrm{End}_{\mathbb{C}}(U^{\otimes d})$. We now define the algebra $\mathfrak{A}_d$ as

$$\mathfrak{A}_d = C_{\mathrm{End}_{\mathbb{C}}(U^{\otimes d})}(\mathbb{C}[S_d]),$$

i.e., as the commutator of this image: The elements in $\mathfrak{A}_d$ are exactly those endomorphisms φ on $U^{\otimes d}$ for which

$$\sigma \circ \varphi = \varphi \circ \sigma, \quad \forall \sigma \in S_d.$$

Since $\mathbb{C}[S_d]$ is semi-simple by Maschke's Theorem, it now follows from Schur's Commutator Theorem that $\mathfrak{A}_d$ is as well.

In particular, any finitely generated $\mathfrak{A}_d$-module is a direct sum of irreducible submodules, and this decomposition is essentially unique.

Given a matrix

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},$$

we get an element $\mathbf{B}^{\otimes d}$ in $\mathfrak{A}_d$ by

$$\mathbf{B}^{\otimes d} \colon e_{i_1} \otimes \cdots \otimes e_{i_d} \mapsto (\mathbf{B}e_{i_1}) \otimes \cdots \otimes (\mathbf{B}e_{i_d}).$$

With respect to the basis $(e_{\mathbf{i}})_{\mathbf{i} \in I^d}$ for $U^{\otimes d}$, $\mathbf{B}^{\otimes d}$ is represented by the matrix

$$(B_{\mathbf{ij}})_{\mathbf{i},\mathbf{j}} = (b_{i_1 j_1} \cdots b_{i_d j_d})_{\mathbf{i},\mathbf{j}}.$$

We note that $B_{\mathbf{ij}} = B_{\sigma\mathbf{i},\sigma\mathbf{j}}$ for $\sigma \in S_d$. It is easy to see that this property characterises the elements of $\mathfrak{A}_d$:

Let $\mathbf{C} = (C_{\mathbf{ij}})_{\mathbf{i},\mathbf{j}}$ be in $\mathrm{End}_{\mathbb{C}}(U^{\otimes d})$. Then $\mathbf{C} \in \mathfrak{A}_d$ if and only if $C_{\mathbf{ij}} = C_{\sigma\mathbf{i},\sigma\mathbf{j}}$ for all $\sigma \in S_d$.

THEOREM B.4.10. *A homogeneous representation*

$$\rho \colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$$

of degree d factors in a unique way through a homomorphism

$$\bar{\rho} \colon \mathfrak{A}_d \to \mathrm{Mat}_n(\mathbb{C}).$$

PROOF. A homomorphism $\bar{\rho} \colon \mathfrak{A}_d \to \mathrm{Mat}_n(\mathbb{C})$ induces a representation by

$$\rho \colon \mathbf{B} \mapsto \bar{\rho}(\mathbf{B}^{\otimes d}).$$

Conversely, let ρ be given:

The different maps $\mathbf{B} \mapsto B_{\mathbf{ij}} = b_{i_1 j_1} \cdots b_{i_d j_d}$ are linearly independent over $\mathbb{C}$, and two such maps are different if and only if they cannot be mapped to each other by simultanous permutations of the two multi-indices $\mathbf{i}$ and $\mathbf{j}$.

Thus, we can write the $k\ell^{\text{th}}$ component of $\rho(\mathbf{B})$ uniquely in the form

$$\rho_{k\ell}(\mathbf{B}) = \sum_{\mathbf{i},\mathbf{j}} c_{k,\ell,\mathbf{i},\mathbf{j}} B_{\mathbf{ij}}$$

by requiring

$$c_{k,\ell,\sigma\mathbf{i},\sigma\mathbf{j}} = c_{k,\ell,\mathbf{i},\mathbf{j}}, \quad \sigma \in S_d.$$

Another way of saying this is that the subspace of $\mathfrak{A}_d$ generated by the image (under $-^{\otimes d}$) of $\mathrm{Mat}_2(\mathbb{C})$ has orthogonal complement 0 with respect to the inner product

$$(c_{\mathbf{ij}})_{\mathbf{i},\mathbf{j}}(d_{\mathbf{ij}})_{\mathbf{i},\mathbf{j}} = \sum_{\mathbf{i},\mathbf{j}} c_{\mathbf{ij}} d_{\mathbf{ij}},$$

from which we get that the image of $\mathrm{Mat}_2(\mathbb{C})$ actually generates $\mathfrak{A}_d$, cf. Exercise B.19.

We can therefore define $\bar{\rho}$ by

$$\bar{\rho}_{k\ell}(\mathbf{X}) = \sum_{\mathbf{i},\mathbf{j}} c_{k,\ell,\mathbf{i},\mathbf{j}} X_{\mathbf{ij}}$$

for $\mathbf{X} = (x_{\mathbf{ij}})_{\mathbf{i},\mathbf{j}}$, and conclude that it preserves matrix products: By construction, $\bar{\rho}(\mathbf{X})\bar{\rho}(\mathbf{Y}) = \bar{\rho}(\mathbf{XY})$ when $\mathbf{X}$ and $\mathbf{Y}$ are in the image of $\mathrm{GL}_2(\mathbb{C})$. This can be expressed in terms of a family of polynomial equalities in the 2×2 matrix entries, that hold whenever the matrices have non-zero determinants. Then, trivially, they hold for arbitrary determinants, meaning that we can take $\mathbf{X}$ and $\mathbf{Y}$ in the image of $\mathrm{Mat}_2(\mathbb{C})$. These images generate $\mathfrak{A}_d$, and so the map is multiplicative for all $\mathbf{X}, \mathbf{Y} \in \mathfrak{A}_d$. □

From the definition of $\bar{\rho}$, it is clear that $\mathfrak{A}_d$-submodules of $\mathbb{C}^n$ are $\mathbb{C}[\mathrm{GL}_2(\mathbb{C})]$-submodules as well, and vice versa. Thus, we get

Corollary B.4.11. *If $\rho\colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ is a homogeneous representation, then $\mathbb{C}^n$ is a completely reducible $\mathbb{C}[\mathrm{GL}_2(\mathbb{C})]$-module.*

In particular: If $I(v_1, \ldots, v_d)$ is a non-zero multilinear relative invariant on U^d of weigh $k \geq 0$, then we get an induced linear relative invariant $I'\colon U^{\otimes d} \to \mathbb{C}$, i.e., an $\mathfrak{A}_d$-homomorphism. Consequently, $\mathbb{C}$ (with $\mathrm{GL}_2(\mathbb{C})$ acting through $\det^k$) is a direct summand of $U^{\otimes d}$, and I' is a projection.

It is thus of interest for us to find the $\mathfrak{A}_d$-submodules of $U^{\otimes d}$ of dimension 1 (over $\mathbb{C}$). Such a submodule is of course irreducible.

By the results of the section on Young tableaux, irreducible $\mathfrak{A}_d$-modules have the form $\gamma_\lambda U^{\otimes d}$, where

$$\gamma_\lambda = \alpha_\lambda \beta_\lambda = \Big(\sum_{\rho \in \mathcal{R}(\Sigma_\lambda)} \rho \Big) \Big(\sum_{\kappa \in \mathcal{C}(\Sigma_\lambda)} \mathrm{sign}(\kappa)\, \kappa \Big)$$

for some Young tableau Σ_λ of size d. Since the map $\mathbb{C}[S_d] \to \mathrm{End}_{\mathbb{C}}(U^{\otimes d})$ is not necessarily injective, we may get that some of the $\gamma_\lambda U^{\otimes d}$'s are 0. However, if $\gamma_\lambda U^{\otimes d}$ is non-zero, it *is* irreducible.

Since $\gamma_\lambda U^{\otimes d}$ is independent of the choice of tableau (up to isomorphism), we will denote it simply by W_λ, and refer to it as a *Weyl module*.

The particular tableau we will use to describe W_λ is the following: Let the conjugate diagram be $\mu = \tilde{\lambda} = (\mu_1, \dots, \mu_s)$, and fill in λ column by column:

$$\begin{array}{cccc} 1 & \mu_1+1 & \dots & d+1-\mu_s \\ 2 & \vdots & & \vdots \\ \vdots & & & d \\ \mu_1-1 & \mu_1+\mu_2 & & \\ \mu_1 & & & \end{array}$$

A 'typical' element in $U^{\otimes d}$ is a tensor product

$$u = u_1 \otimes \cdots \otimes u_d, \quad u_i \in U,$$

and to determine how γ_λ acts on it, we 'decompose' it as

$$u = w_1 \otimes \cdots \otimes w_s, \quad \text{where} \quad w_i = u_{\mu_1+\cdots+\mu_{i-1}+1} \otimes \cdots \otimes u_{\mu_1+\cdots+\mu_i},$$

i.e., w_i contains the u_j's corresponding to the i^{th} column of our tableau.

We first consider the action of β_λ on v: Any $\kappa \in \mathcal{C}(\Sigma_\lambda)$ can be written uniquely as

$$\kappa = \kappa_1 \cdots \kappa_s,$$

where κ_i acts only on the i^{th} column. We then have

$$\begin{aligned} \beta_\lambda u &= \sum_{\kappa_1,\dots,\kappa_s} (\operatorname{sign}(\kappa_1)\,\kappa_1 w_1) \otimes \cdots \otimes (\operatorname{sign}(\kappa_s)\,\kappa_s w_s) \\ &= \big(\sum_{\kappa_1} \operatorname{sign}(\kappa_1)\,\kappa_1 w_1\big) \otimes \cdots \otimes \big(\sum_{\kappa_s} \operatorname{sign}(\kappa_s)\,\kappa_s w_s\big). \end{aligned}$$

The expressions in the last line are called *anti-symmetrisations*: If S_n acts on the n^{th} tensor power $V^{\otimes n}$ of a vector space V by

$$\sigma(v_1 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}1} \otimes \cdots \otimes v_{\sigma^{-1}n},$$

the anti-symmetrisation is the map

$$a\colon v_1 \otimes \cdots \otimes v_n \mapsto \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, v_{\sigma^{-1}1} \otimes \cdots \otimes v_{\sigma^{-1}n}. \tag{B.4.3}$$

We leave it to the reader (in Exercise B.20) to verify that the anti-symmetrisation satisfies the following two properties:

$$a(v_1 \otimes \cdots \otimes v_n) = 0 \quad \text{if } \dim_{\mathbb{C}} V < n, \tag{B.4.4}$$

and

$$a(v_1 \otimes \cdots \otimes v_n) = |v_1 \dots v_n|\, a(e_1 \otimes \cdots \otimes e_n) \quad \text{if } \dim_{\mathbb{C}} V = n, \tag{B.4.5}$$

where $e_1, \dots, e_n$ is a basis for V, and $|v_1 \dots v_n|$ is the determinant with i^{th} column consisting of the coordinates of v_i in that basis.

It is now clear that $W_\lambda = 0$ if the first column of λ has length > 2.

THEOREM B.4.12. *The Weyl module W_λ is one-dimensional if and only if all columns of λ have length 2 (i.e., if d is even and $\lambda = (d/2, d/2)$).*

PROOF. 'If': With notation as above, we have

$$\beta_\lambda u = |v_1\, v_2| \cdots |v_{d-1}\, v_d| \cdot a(e_1 \otimes e_2) \otimes \cdots \otimes a(e_{d-1} \otimes e_d).$$

Expanding the tensor part of this expression shows us that the term

$$e_1 \otimes e_2 \otimes e_1 \otimes e_2 \otimes \cdots \otimes e_1 \otimes e_2$$

only shows up once. This term is invariant under the action of $\mathcal{R}(\Sigma_\lambda)$ since $\mathcal{R}(\Sigma_\lambda)$ permutes the odd- and even-numbered coordinates in the tensor separately. In particular, in the expansion of

$$\alpha_\lambda a(e_1 \otimes e_2) \otimes \cdots \otimes a(e_{d-1} \otimes e_d)$$

we get that one term $(d/2)!^2$ times, with nothing to cancel it out. Thus, the expression is not zero, and we see that $W_{(d/2,d/2)}$ is one-dimensional.

Also, we note that

$$\gamma_\lambda(\mathbf{A}v_1 \otimes \cdots \otimes \mathbf{A}v_d) = \det \mathbf{A}^{d/2}\, \gamma_\lambda(v_1 \otimes \cdots \otimes v_d)$$

for $\mathbf{A} \in \mathrm{GL}_2(\mathbb{C})$, meaning that $\mathrm{GL}_2(\mathbb{C})$ acts on $W_{(d/2,d/2)}$ as multiplication by $\det^{d/2}$.

'Only if': We already know that $W_\lambda = 0$ if λ has a column of length > 2. Hence, we may assume all columns to have length at most 2, with at least one column of length 1. Our diagram is therefore

$$\begin{array}{cccccccc} 1 & 3 & \dots & 2h-1 & 2h+1 & \dots & d-1 & d \\ 2 & 4 & \dots & 2h & & & & \end{array}$$

for some h with $0 \le h < d/2$. We now consider two u's, namely

$$u_1 = \overbrace{(e_1 \otimes e_2) \otimes \cdots \otimes (e_1 \otimes e_2)}^{h \text{ times}} \otimes e_1 \otimes \cdots \otimes e_1,$$
$$u_2 = (e_2 \otimes e_1) \otimes \cdots \otimes (e_2 \otimes e_1) \otimes e_2 \otimes \cdots \otimes e_2.$$

In $\beta_\lambda u_i$, the term u_i itself occurs exactly once, and is not cancelled out by any other term. Also, it is $\mathcal{R}(\Sigma_\lambda)$-invariant. Consequently,

$$\gamma_\lambda u_i = 2^h u_i + (\text{other terms}) \neq 0.$$

Also, $\gamma_\lambda u_1$ and $\gamma_\lambda u_2$ have no tensor terms in common, since all tensor terms in $\gamma_\lambda u_i$ has h entries equal to e_i, and $d - h > h$ entries equal to e_{2-i}.

Consequently, $\gamma_\lambda u_1$ and $\gamma_\lambda u_2$ are linearly independent, and W_λ has dimension at least 2. □

Proof of the Fundamental Theorem (v. 3). Let $J(v_1, \dots, v_n)$ be a non-zero multilinear joint invariant on U^n. We replace J by the induced linear invariant $\bar{J}$ on $U^{\otimes n}$.

In $\mathbb{C}[S_d]$, we can write

$$1 = \sum_{i=1}^{m} c_i,$$

where the c_i's generate minimal left ideals. Correspondingly, we get

$$v = \sum_{i=1}^{m} c_i v$$

for $v \in U^{\otimes n}$, and therefore

$$J(v_1, \ldots, v_n) = \bar{J}(v_1 \otimes \cdots \otimes v_n) = \sum_{i=1}^{m} \bar{J}(c_i(v_1 \otimes \cdots \otimes v_n)).$$

Now, $\bar{J}$'s restriction to $c_i U^{\otimes n}$ is zero by Schur's Lemma, unless $c_i U^{\otimes n}$ has dimension 1, i.e., unless $c_i \mathbb{C}[S_d]$ is isomorphic to $\gamma_{(n/2,n/2)}\mathbb{C}[S_d]$. Thus, n must be even.

If $c_i \mathbb{C}[S_d] \simeq \gamma_{(n/2,n/2)}\mathbb{C}[S_d]$, we have

$$c_i = pu\gamma_{(n/2,n/2)}p^{-1}$$

for units p and u in $\mathbb{C}[S_d]^*$. Write

$$p^{-1} = \sum_{\sigma \in S_d} q_\sigma \sigma.$$

Then

$$\begin{aligned}
\bar{J}(c_i(v_1 \otimes \cdots \otimes v_n)) &= \bar{J}(pu\gamma_{(n/2,n/2)}p^{-1}(v_1 \otimes \cdots \otimes v_n)) \\
&= \bar{J}(pu\gamma_{(n/2,n/2)} \sum_{\sigma \in S_d} q_\sigma \sigma(v_1 \otimes \cdots \otimes v_n)) \\
&= \sum_{\sigma \in S_d} q_\sigma \bar{J}(pu\gamma_{(n/2,n/2)}(v_{\sigma^{-1}1} \otimes \cdots \otimes v_{\sigma^{-1}n})) \\
&= \sum_{\sigma \in S_d} q_\sigma r_\sigma |v_{\sigma^{-1}1}\, v_{\sigma^{-1}2}| \cdots |v_{\sigma^{-1}(n-1)}\, v_{\sigma^{-1}n}|,
\end{aligned}$$

where

$$r_\sigma = \bar{J}(pu\gamma_{(n/2,n/2)}(e_{\sigma^{-1}1} \otimes \cdots \otimes e_{\sigma^{-1}n})).$$

This completes the proof, since J is then a linear combination of determinant products. □

A few remarks on dimension. Let $\mathrm{GL}_2(\mathbb{C})$ act on $V = \mathbb{C}^{n+1}$ via a binary form $P(x, y)$. Then $\mathrm{GL}_2(\mathbb{C})$ of course also acts on the polynomial ring $\mathbb{C}[V]$, and on the homogeneous degree-d part V_d of $\mathbb{C}[V]$.

This action of $\mathrm{GL}_2(\mathbb{C})$ is not homogeneous according to our definition, but that is not important: By Exercise B.6, it becomes homogeneous of degree nd if we multiply it by the nd^{th} power of the determinant. This multiplication does not change the submodules in any way, and so we have:

RESULT B.4.13. *V_d is completely reducible as a $\mathbb{C}[\mathrm{GL}_2(\mathbb{C})]$-module, and decomposes into a direct sum of Weyl modules W_λ, where $|\lambda| = nd$.*

The subspace of V_d consisting of invariants is of course also completely reducible and a direct sum of Weyl modules. Since $\mathrm{GL}_2(\mathbb{C})$ acts on this subspace (with the corrected homogeneous action) as multiplication by the $(nd/2)^{\text{th}}$ power

of the determinant, and as this is also the action on $W_{(nd/2,nd/2)}$, we immediately get

PROPOSITION B.4.14. *The invariant subspace of V_d is exactly the part generated by the irreducible components $\simeq W_{(nd/2,nd/2)}$. In particular, the dimension of the space of weight-$(nd/2)$ invariants equals the multiplicity of the irreducible component $W_{(nd/2,nd/2)}$ in V_d.*

This is the beginning of the dimension theory for invariants, which results in combinatorial formulas for the dimension of invariant spaces. In this way, the results on binary quintics in the Example on p. 226 can be established in a less make-shift manner. We refer to the literature, e.g. [St], for details.

Exercises

EXERCISE B.1. Let $P(x,y)$ be a binary form of degree n. Describe $\frac{\partial}{\partial x}P(x,y)$ and $\frac{\partial}{\partial y}P(x,y)$ as binary forms of degree $n-1$.

EXERCISE B.2. Let $P(x,y)$ be a binary form of degree n, and let $\bar{P}(\bar{x},\bar{y})$ be the transform. Describe the transformed one-parameter polynomial $\bar{P}(\bar{z})$ in terms of $P(z)$, and vice versa.

EXERCISE B.3. Let $\zeta_0,\dots,\zeta_n$ be non-zero complex numbers, and consider binary forms of the form

$$Q(x,y)=\sum_{i=0}^{n}\zeta_i a_i x^i y^{n-i}.$$

Define an action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}^{n+1}$ in this case, and determine how it relates to the action considered in the text.

EXERCISE B.4. Look at the homomorphism $\mathbf{A}\mapsto\hat{\mathbf{A}}$ from $\mathrm{GL}_2(\mathbb{C})$ into $\mathrm{GL}_3(\mathbb{C})$ as given on p. 219.

(1) Prove that $\det\hat{\mathbf{A}}=\det\mathbf{A}^{-3}$.

(2) Prove that $\mathbf{A}\mapsto\det\mathbf{A}\cdot\hat{\mathbf{A}}$ gives a map $\mathrm{PGL}_2(\mathbb{C})\hookrightarrow\mathrm{SL}_3(\mathbb{C})$.

EXERCISE B.5. Let K be field with more than three elements. Prove that the commutator subgroup $\mathrm{GL}_2(K)'$ of $\mathrm{GL}_2(K)$ is the special linear group $\mathrm{SL}_2(K)$. [Hint: Compute various commutators between diagonal matrices, row operation matrices and $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$.]

EXERCISE B.6. Consider the action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}^{n+1}$ for an arbitrary n. Let $\hat{\mathbf{A}}\in\mathrm{GL}_n(\mathbb{C})$ be the matrix expressing the transformation $\mathbf{a}\mapsto\bar{\mathbf{a}}$ corresponding to $\mathbf{A}\in\mathrm{GL}_2(\mathbb{C})$.

(1) Prove that the entries in $\hat{\mathbf{A}}$ are homogeneous rational functions of degree $-n$, with denominator $\det\mathbf{A}^n$. Find explicit expressions for the entries in the first and last rows of $\hat{\mathbf{A}}$. Write down $\hat{\mathbf{A}}$ when $\mathbf{A}$ is a diagonal matrix.

(2) Prove that $\det\hat{\mathbf{A}}=\det\mathbf{A}^{-n(n+1)/2}$. [Hint: $\mathbf{A}\mapsto\det\hat{\mathbf{A}}$ is a rational character.]

(3) Find the kernel of $\mathbf{A}\mapsto\hat{\mathbf{A}}$.

EXERCISE B.7. How does the discriminant of a binary form $P(x,y)$ relate to the discriminant of the associated polynomial $P(z)$?

EXERCISE B.8. Check by direct computation that the discriminant for a binary form of degree 2 is an invariant of weight 2.

EXERCISE B.9. Let $P(x, y)$ be a binary form of degree n. Prove that $d(P)/n^n$ is a polynomial in $\mathbb{Z}[\mathbf{a}]$.

EXERCISE B.10. Let $p(z) = z^4 + 4a_3z^3 + 6a_2z^2 + 4a_1z + a_0$ be a monic quartic polynomial (i.e., $a_4 = 1$), and consider the invariants i and j from the Example on p. 225. Prove that $p(z)$ has a root of multiplicity ≥ 3, if and only if $i = j = 0$. [Hint: Assuming $i = j = 0$, first prove that $p(z)$ has a root of multiplicity ≥ 2. Perform a fractional linear transformation to make 0 that root.]

EXERCISE B.11. Let i and j in $\mathbb{C}[a_0, \ldots, a_4]$ be the invariants for the binary quartic defined in the Example on p. 225. Prove that i and j are algebraically independent over $\mathbb{C}$.

EXERCISE B.12. Evaluate the invariant

$$[1\,2][1\,3][2\,4][3\,4] + [1\,3][2\,3][1\,4][2\,4] + [2\,3][2\,1][3\,4][1\,4]$$

for the binary quartic. [Hint: (B.3.4)]

EXERCISE B.13. Verify by direct computation that

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_6 \end{vmatrix}$$

is an invariant for the binary sextic. [Hint: A computer algebra package might be useful here.] Suggest a generalisation.

EXERCISE B.14. Let $P(x, y)$ be a binary form of degree n.

(1) Assume n even. Prove that there are no non-zero bracket invariants of weight $n/2$, but that there are non-zero polynomial invariants of weight n. [Hint: Sums of squares.]

(2) Assume n odd. Prove that there are no non-zero bracket invariants of weight n, but that there are non-zero polynomial invariants of weight $2n$.

EXERCISE B.15. Let V be the space of symmetric 2×2 matrices over $\mathbb{C}$, and let $\mathrm{GL}_2(\mathbb{C})$ acts on V by ${}^{\sigma}\mathbf{A} = \sigma\mathbf{A}\sigma^t$. Prove that $\det\colon V \to \mathbb{C}$ is a relative invariant of weight 2.

EXERCISE B.16. Recall the definition of (m, n)-resultant from Exercise 1.6 of Chapter 1, and define the *resultant* of two binary forms $P_1(x, y)$ and $P_2(x, y)$ of degrees m and n to be

$$\mathrm{Res}(P_1, P_2) = \mathrm{Res}_{(m,n)}(P_1(z), P_2(z)).$$

(1) Let

$$P_1(x, y) = \prod_{i=1}^{m}(y_i x - x_i y) \quad \text{and} \quad P_2(x, y) = \prod_{j=1}^{n}(v_j x - u_j y)$$

be normal factorisations. Prove that

$$\mathrm{Res}(P_1, P_2) = \prod_{i,j}(v_j x_i - u_j y_i).$$

(2) Prove that $\operatorname{Res}(P_1, P_2)$ is a joint invariant for $P_1(x, y)$ and $P_2(x, y)$ of weight mn.

EXERCISE B.17. Describe the simple components of $\mathbb{C}[A]$, when A is finite abelian.

EXERCISE B.18. Let D_4 be the dihedral group of degree 4, cf. Chapter 2, and let Q_8 be the quaternion group of order 8, cf. Chapter 6. Prove that $\mathbb{C}[D_4] \simeq \mathbb{C}[Q_8]$.

EXERCISE B.19. Let K be a field and V a finite-dimensional K-vector space. An *inner product* on V is a bilinear map $B\colon V \times V \to K$ satisfying

$$B(v, w) = B(w, v), \quad v, w \in V.$$

The *orthogonal complement* of a subspace U of V is

$$U^{\perp} = \{v \in V \mid \forall u \in U\colon B(u, v) = 0\}.$$

(1) Prove that $U^{\perp}$ is a subspace of V.

(2) Assume $U \cap U^{\perp} = 0$. Prove that $V = U \oplus U^{\perp}$. [Hint: Use the inner product to produce a short-exact sequence

$$0 \to U^{\perp} \to V \to U^* \to 0,$$

where $U^* = \operatorname{Hom}_K(U, K)$ is the dual space.]

(3) Assume $U^{\perp} = 0$. Conclude that $U = V$.

EXERCISE B.20. Consider the anti-symmetrisation map as defined in (B.4.3). Prove properties (B.4.4) and (B.4.5). [Hint: Compose a with a permutation. Then let the v_i's be basis vectors.] Conclude that the image of a is one-dimensional when $n = \dim_{\mathbb{C}} V$.

Bibliography

[Ab] S. S. Abhyankar, *Galois embeddings for linear groups*, Trans. Amer. Math. Soc. **352** (2000), 3881–3912.

[Al] A. A. Albert, *Modern Higher Algebra*, Cambridge University Press, 1938.

[Ar&M] M. Artin & D. Mumford, *Some elementary examples of unirational varieties which are not rational*, Proc. London Math. Soc. **25** (1972), 75–95.

[A&M] M. F. Atiyah & I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[Be&al] A. Beauville, J.-P. Colliot-Thélène, J. Sansuc, H. P. F. Swinnerton-Dyer, *Variétés stablement non rationalles*, Ann. Math. **121** (1985), 253–318.

[Be] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?*, J. Algebra **164** (1994), 430–451.

[Bel1] G. V. Belyi, *Galois extensions of a maximal cyclotomic field* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no.2, 267–276, 479.

[Bel2] ———, *On extensions of the maximal cyclotomic field having a given classical Galois group*, J. Reine Angew. Math. **341** (1983), 147–156.

[Bl1] E. V. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra **203** (1998), 12–29.

[Bl2] ———, *Deformations of dihedral 2-group extensions of fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241.

[Blu] M. P. Blue, *Generic Galois extensions for groups of order p^3*, Ph.D. Thesis, University of Texas at Austin, May 2000.

[Bt] G. Brattström, *On p-groups as Galois groups*, Math. Scand. **65** (1989), 165–174.

[BJ&Y] A. A. Bruen, C. U. Jensen & N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory **24** (1986), 305–359.

[Bu] G. Bucht, *Über einige algebraische Körper achten Grades*, Arkiv för Matematik, Astronomi och Fysik **6/30** (1910), 1–36.

[B&R1] J. Buhler & Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica **106** (1997), 159–179.

[B&R2] J. Buhler & Z. Reichstein, *On Tschirnhaus transformations*, Topics in Number Theory (eds. S. D. Ahlgren & al.), Kluwer Academic Publishers, 1999, 127–142.

[B&R3] J. Buhler & Z. Reichstein, *Versal cyclic polynomials*, unpublished manuscript.

[Bs] W. Burnside, *The alternating functions of three and four variables*, Messenger of Math. **37** (1908), 165–166.

[Ca] G. Castelnuovo, *Sulla razionalità delle involuzioni piane*, Math. Ann. **44** (1894), 125–155.

[CH&R] S. U. Chase, D. K. Harrison & A. Rosenberg, *Galois theory and and Galois cohomology of commutative rings*, Mem. AMS **52** (1965), 1–19.

[C&Y] I. Chen & N. Yui, *Singular values of Thompson series*, Groups, difference sets, and the Monster (Columbus, OH, 1993), Ohio State Univ. Math. Res. Inst. Publ. 4, Walter de Gruyter, 1996, 255–326.

[C&G] H. Clemens & P. Griffiths, *The intermediate Jacobian of the cubic threefold*, Ann of Math. **95** (1972), 281-356.

[Cn1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer-Verlag, 1996.

[Cn2] ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics 193, Springer-Verlag 2000.

[C&P] P. E. Conner & R. Perlis, *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics 2, World Scientific Publishing Co., Singapore, 1984.

[Co] D. F. Coray, *Cubic hypersurfaces and a result of Hermite*, Duke J. Math. **54** (1987), 657–670.

[Cox] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley-Interscience, New York, 1989.

[C&M] H. S. M. Coxeter & W. O. J. Moser, *Generators and Relations for Discrete Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 14 (4. ed.), Springer-Verlag, 1984.

[Cr1] T. Crespo, *Explicit contruction of* $\widetilde{A}_n$ *type fields*, J. Algebra **127** (1989), 452–461.

[Cr2] ———, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. **409** (1990), 180–189.

[De] R. Dedekind, *Konstruktion von Quaternionenkörpern*, Gesammelte mathematische Werke, II. Band, Vieweg, Braunschweig, 1931, 376–384.

[DM] F. R. DeMeyer, *Generic Polynomials*, J. Alg. **84** (1983), 441–448.

[D&I] F. DeMeyer & E. Ingraham, *Separable Algebras over Commutative Rings*, Lecture Notes in Mathematics 181, Springer-Verlag, 1971.

[D&C] J. A. Dieudonné & J. B. Carrell, *Invariant Theory—Old and New*, Academic Press, 1971.

[En] F. Enriques, *Sulle irrazionalità da cui può farsi dipendere la risoluzione d'un' equazione algebrica* $f(xyz) = 0$ *con funzioni razionali di due parametri*, Math. Ann. **49** (1897), 1-23.

[EF&M] D. W. Erbach, J. Fischer & J. McKay, *Polynomials with* $\mathrm{PSL}(2,7)$ *as Galois group*, J. Number Theory **11** (1979), 69–75.

[Fa] D. K. Faddeyev, *Constructions of fields of algebraic numbers whose Galois group is a group of quaternion units*, C. R. (Dokl.) Acad. Sci. URSS **47** (1945), 390–392.

[Fn] G. Fano, *Sul sistema* ∞^2 *di rette contenuto in una varietà cubica*, Atti R. Accad. Sci. Torino **39** (1904), 778-792.

[Fe] W. Feit, *Some consequences of the classification of finite simple groups*, AMS Proc. Sympos. in Pure Math. **37** (1980), 175–181.

[F&J] M. D. Fried & M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik 11, Springer-Verlag, 1986.

[Fr] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.

[F&T] A. Fröhlich & M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics 27, Cambridge University Press, 1991.

[Ful] W. Fulton, *Young Tableaux*, London Mathematical Society Student Texts 35, Cambridge University Press, 1997.

[Fu] Ph. Furtwängler, *Über Minimalbasen für Körper rationaler Funktionen*, S. B. Akad. Wiss. Wien **134** (1925), 69–80.

[G&M] G. Garbe & J. L. Mennicke, *Some remarks on the Mathieu groups*, Canad. Math. Bull. **7** (1964), 201–212.

[Ga] W. Gaschütz, *Fixkörper von p-Automorphismengruppen rein-transzendenter Körpererweiteriungen von p-Charakteristik*, Math. Zeitschr. **71** (1959), 466–468.

[G&J] W.-D. Geyer & C. U. Jensen, *Prodihedral groups as Galois groups over number fields*, J. Number Theory **60** (1996), 332–372.

[Gr] C. Greither, *Cyclic Galois Extensions of Commutative Rings*, Lecture Notes in Mathematics 1534, Springer-Verlag, 1992.

[Grö] W. Gröbner, *Minimalbasis der Quaternionengruppe*, Monatshefte f. Math. und Physik **41** (1934), 78–84.

[G&Z] B. Gross & D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[GS&S] H. G. Grundman, T. L. Smith & J. R. Swallow, *Groups of order* 16 *as Galois groups*, Expo. Math. **13** (1995), 289–319.

[Ha] C. R. Hadlock, *Field Theory and its classical Problems*, Carus Mathematical Monographs 19, Mathematical Association of America, 1978.

[Hj] M. Hajja, *The alternating functions of three and of four variables*, Algebras Groups Geom. **6** (1989), 49–54.

[Hr] D. Haran, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137** (1999), 113–126.

[Hrb1] D. Harbater, *Galois coverings of the arithmetic line*, Number Theory: New York, 1984–85, Lecture Notes in Mathematics 1240, Springer-Verlag, 1987, 165–195.

[Hrb2] ———, *Fundamental groups and embedding problems in characteristic p*, Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993), Cotemp. Math. **186** (1995), 353–369.

[H&M] K. Hashimoto & K. Miyake, *Inverse Galois problem for dihedral groups*, Developments in Mathematics **2**, Kluwer Academic Publishers, 1999, 165–181.

[Hs1] H. Hasse, *Invariante Kennzeichnung relativ-abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers*, Abh. Deutsche Akad. Wiss, math.-naturw. Kl. 1947(8), 1–56.

[Hs2] ———, *Existenz und Mannigfältigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers I–III*, Math. Nachr. **1** (1948), 40–61, 213–217, 277–283.

[Hs3] ———, *Vorlesungen über Zahlentheorie*, Grundlehren der mathematischen Wissenschaften 59, Springer-Verlag, 1964.

[He] C. Hermite, *Sur l'invariant de* 18^e *ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation de cinquième degré, extrait de deux lettres de M. Hermite à l'éditeur*, J. Reine Angew. Math. **59** (1861), 304–305.

[Hi] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[Hu] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften 134, Springer-Verlag, 1967.

[Hw] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893), 403–442.

[IR&S] Y. Ihara, K. Ribet & J.-P. Serre (eds.), *Galois Groups over* $\mathbb{Q}$, Mathematical Sciences Research Institute Publications 16, Springer-Verlag, 1987.

[Ik] M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren*, Abh. Math. Sem. Univ. Hamburg **24** (1960), 126–131.

[IL&F] V. V. Ishkhanov, B. B. Lur'e & D. K. Faddeev, *The Embedding Problem in Galois Theory*, Tranlations of Mathematical Monographs 165, American Mathematical Society, 1997.

[I&M] V. A. Iskovskih & Yu. I. Manin, *Three-dimensional quartics and counterexamples to the Lüroth problem* (Russian), Mat. Sb. (N.S.) **86** (**128**) (1971), 140-166.

[Iw] K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. Math. **58** (1953), 126–131.

[Ja1] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, New York, 1985.

[Ja2] ———, *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.

[Je] C. U. Jensen, *Remark on a characterization of certain ring class fields by their absolute Galois group* Proc. Amer. Math. Soc. **14** (1963), 738-741.

[J&Y82] C. U. Jensen & N. Yui, *Polynomials with* D_p *as Galois group*, J. Number Theory **15** (1982), 347–375.

[J&Y87] ———, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, Kinokuniya, Tokyo, 1987, 155–182.

[Jou] P. Joubert, *Sur l'équation du sixième degré*, C. R. Acad. Sc. Paris **64** (1867), 1025–1029.

[K&Y] E. Kaltofen & N. Yui, *Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, Number Theory (New York Seminar 1989–1990), Springer-Verlag, 1991, 149–202.

[Ke1] G. Kemper, *A constructive approach to Noether's Problem*, Manuscripta Math. **90** (1996), 343–363.
[Ke2] ———, *Generic polynomials are descent-generic*, IWR Preprint, Heidelberg, 2000.
[K&M] G. Kemper & G. Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), 569–586.
[K&Mt] G. Kemper & E. Mattig, *Generic polynomials with few parameters*, J. Symbolic Computation **30** (2000), 843–857.
[Ki] I. Kiming, *Explicit classifications of some* 2*-extensions of a field of characteristic different from* 2, Canad. J. Math. **42** (1990), 825–855.
[Kl&M] J. Klüners & G. Malle, *Explicit Galois realization of transitive groups of degree up to* 15, J. Symbolic Computation **30** (2000), 675–716.
[Ko] T. Kondo, *Algebraic number fields with the discriminant equal to that of a quadratic number field* J. Math. Soc. Japan **47** (1995), 31–36.
[Kn] H. Kuniyoshi, *Certain subfields of rational function fields*, Proc. International Symp. on Algebraic Number Theory, Tokyo & Nikko 1955, 241–243.
[Ku] W. Kuyk, *On a theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A **67** (1964), 32–39.
[K&L] W. Kuyk & H. W. Lenstra, Jr., *Abelian extensions of arbitrary fields*, Math. Ann. **216** (1975), 99–104.
[Lam] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
[LaM] S. E. LaMacchia, *Polynomials with Galois group* PSL(2, 7), Comm. Algebra **8** (1980), 983–992.
[La] S. Lang, *Diophantine Geometry*, Wiley-Interscience, New York, 1962.
[Lc] O. Lecacheux, *Construction de polynômes génériques à groupe de Galois résoluble*, Acta Arithm. **86** (1998), 207–216.
[Le1] A. Ledet, *On* 2*-groups as Galois groups*, Canad. J. Math. **47** (1995), 1253–1273.
[Le2] ———, *Subgroups of* $\operatorname{Hol} Q_8$ *as Galois groups*, J. Algebra **181** (1996), 478–506.
[Le3] ———, *Embedding problems with cyclic kernel of order* 4, Israel Jour. Math. **106** (1998), 109–131.
[Le4] ———, *Dihedral extensions in characteristic* 0, C. R. Math. Rep. Canada **21** (1999), 46–52.
[Le5] ———, *On a theorem by Serre*, Proc. Amer. Math. Soc. **128** (2000), 27–29.
[Le6] ———, *Embedding problems and equivalence of quadratic forms*, Math. Scand. **88** (2001), 279–302.
[Le7] ———, *Generic polynomials for* Q_8*-, QC- and QQ-extensions*, J. Alg. **237** (2001), 1–13.
[Le8] ———, *Generic polynomials for quasi-dihedral, dihedral and modular extensions of order* 16, Proc. Amer. Math. Soc. **128** (2000), 2213-2222.
[Le9] ———, *Generic and explicit realisation of small p-groups*, J. Symbolic Computation **30** (2000), 859–865.
[Le10] ———, *Generic extensions and generic polynomials*, J. Symbolic Computation **30** (2000), 867–872.
[Le11] ———, *On the essential dimension of some semi-direct products*, Can. Math. Bull. (to appear).
[Le12] ———, *On p-group in characteristic p*, Preprint, 2001.
[Le13] ———, *Constructing generic polynomials*, Proceedings of the Workshop on Number Theory 2001 (eds. K. Komatsu & K. Hashimoto), Waseda University, Tokyo, 2001, 114–118.
[Len] H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.
[Lo1] F. Lorenz, *Einführung in die Algebra I* (2. ed.), B. I. Wissenschaftsverlag, Mannheim, 1992.
[Lo2] ———, *Einführung in die Algebra II*, B. I. Wissenschaftsverlag, Mannheim, 1990.
[Lo3] ———, *Algebraische Zahlentheorie*, B. I. Wissenschaftsverlag, Mannheim, 1993.

[Lü] J. Lüroth, *Beweis eines Satzes über rationale Curven*, Math. Ann. **9** (1876), 163–165.

[Mae] T. Maeda, *Noether's problem for A_5*, J. Alg. **125** (1989), 418–430.

[M&M1] G. Malle & B. H. Matzat, *Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$*, Math. Ann. **272** (1985), 549–565.

[M&M2] G. Malle & B. H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer-Verlag, 1999.

[Mn] Yu. I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic* (Russian), Nauka, 1972; (English translation) North-Holland, 1986.

[Ma] R. Massy, *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), 508–535.

[M&Z] B. H. Matzat & A. Zeh-Marschke, *Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$*, J. Number Theory **23** (1986), 195–202.

[McC] E. McClintock, *On the resolution of quintic equations*, Amer. J. of Math. **VI** (1884), 301-315.

[McK] J. McKay, *Some remarks on computing Galois groups*, SIAM J. Comput. **8** (1979), 344–347.

[Mes] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$*, J. Alg. **131** (1990), 483–495.

[Mi] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Adv. Stud. Contemp. Math. (Pusan) **1** (1999), 137–142.

[Miy] T. Miyata, *Invariants of certain groups I*, Nagoya Math. J. **41** (1971), 69–73.

[M&Sm] J. Mináč & T. L. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11.

[Mo] S. Monier, *Descente de p-extensions galoisiennes kummériennes*, Math. Scand. **79** (1996), 5–24.

[Na] S. Nakano, *On generic cyclic polynomials of odd prime degree*, Proc. Japan Acad. **76**, Ser. A (2000), 159–162.

[NS&W] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

[Noe] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1916), 221–229.

[O] J. Ohm, *On subfields of rational function fields*, Arch. Math. **42** (1984), 136–138.

[Oj] M. Ojanguren, *The Witt group and the problem of Lüroth*, Dottorato di Ricerca in Matematica, Dipartimento di Matematica dell'Università di Pisa, 1990.

[Ol] P. J. Olver, *Classical Invariant Theory*, London Mathematical Society Student Texts 44, Cambridge University Press, 1999.

[Pa] D. S. Passman, *Permutation Groups*, Benjamin, New York, 1968.

[Pop] F. Pop, *Étale coverings of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture*, Invent. Math. **120** (1995), 555–578.

[Rei] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. *177* (1937), 1–5.

[Re] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), 265–304.

[Re&Y] Z. Reichstein & B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), 1018–1056.

[Ri] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. AMS (to appear).

[RY&Z] G. Roland, N. Yui & D. Zagier, *A parametric family of quintic polynomials with Galois group D_5*, J. Number Theory **15** (1982), 137–142.

[Ro] P. Roquette, *Isomorphisms of generic splitting fields of simple algebras*, J. Reine Angew. Math. **214/215** (1964), 207–226.

[S&Z] S. Saks & A. Zygmund, *Analytic Functions*, Elsevier Publishing Company, Amsterdam, 1971.

[Sa1] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

[Sa2] ———, *Generic structures and field theory*, Contemporary Mathematics 13: Algebraists' Homage — Papers in ring theory and related topics, American Mathematical Society (1982), 127–134.

[Sa3] ———, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71–84.

[Sch] L. Schneps, *On cyclic field extensions of degree* 8, Math. Scand. **71** (1992), 24–30.

[S&L] L. Schneps & P. Lochak, *Geometric Galois Actions* 1–2, London Mathematical Society Lecture Note Series 242–243, Cambridge University Press, 1997.

[Scz1] R. Schertz, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper*, J. Number Theory **34** (1990), 41–53.

[Scz2] ———, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory **39** (1991), 283–326.

[Scz3] ———, *Problèmes de construction en multiplication complexe*, Sém. Théor. Nombres Bordeaux (2) **4** (1992), 239–262.

[Scz4] ———, *Construction of ray class fields by ellliptic units*, J. Théor. Nombres Bordeaux **9** (1997), 383–394.

[Scz5] ———, *Lower powers of elliptic units*, preprint 1999.

[Sco] A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Math. Z. **42** (1937), 161–188.

[Sg1] B. Segre, *Sull' esistenza, sia nel campo razionale che nel campo reale, di involuzioni piane non birazionali*, Rend. Acc. Naz. Lincei, Sc. fis. mat. e nat. (8) **10** (1951), 94-97.

[Sg2] ———, *The rational solutions of homogeneous cubic equations in four variables*, Math. Notae Univ. Rosario, anno II, fasc. 1-2 (1951), 1-68.

[Sei] F. Seidelmann, *Der Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich*, Math. Ann. **78** (1918), 230–233.

[Se1] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comm. Math. Helv. **59** (1984), 651–676.

[Se2] ———, *Topics in Galois Theory*, Research Notes in Mathematics, Jones & Bartlett, 1992.

[Sha] I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group* (russian), Izv. Akad. Nauk SSSR, Ser. Mat. **18** (1954), 525–578.

[Shi] K.-Y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.

[SmG] G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Alg. **19**(12) (1991), 3367–3391.

[SmT] T. L. Smith, *Extra-special groups of order* 32 *as Galois groups*, Canad. J. Math. **46** (1994), 886–896.

[Sn] J. Sonn, $\mathrm{SL}(2,5)$ *and Frobenius Galois groups over* $\mathbb{Q}$, Canad. J. Math. **32** (1980), 281–293.

[S&M] L. Soicher & J. McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[St] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, 1993.

[Sw1] J. R. Swallow, *Solutions to central embedding problems are constructible*, J. Alg. **184** (1996), 1041–1051.

[Sw2] ———, *Central* p*-extensions of* $(p,p,\ldots,p)$*-type Galois groups*, J. Alg. **186** (1996), 277–298.

[Sw3] ———, *Explicit construction of* $\mathrm{PSL}(2,7)$ *fields over* $\mathbb{Q}(t)$ *embeddable in* $\mathrm{SL}(2,7)$ *fields*, Comm. Algebra **24** (1996), 3787–3796.

[Swn1] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158.

[Swn2] ———, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (eds. B. Srinivasan & J. Sally), Springer-Verlag, 1983, 21–40.

[Syl] J. J. Sylvester, *On a general method of determining by mere inspection the derivations from two equations of any degree*, Philosophical Magazine **16** (1840), 132–135.

[Th] J. G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$*, where* $K \subseteq \mathbb{Q}(\mu_n)$, J. Alg. **89** (1984), 437–499.

[U] K. Uchida, *Separably Hilbertian fields*, Kodai Math. J. **3** (1980), 83–95.

[Vö] H. Völklein, *Groups as Galois Groups, an Introduction*, Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, 1996.

[Vo1] V. E. Voskresenskii, *On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field* $\mathbb{Q}(x_1, \ldots, x_n)$ (russian), Izv. Akad. Nauk SSSR ser. Mat. **34** (1970), 366–375. (English translation in Math. USSR-Izv. **8,4** (1970), 371–380.)

[Vo2] ———, *Stably rational algebraic tori*, Les XXième Journées Arithmétiques (Limoges 1997), J. Théor. Nombres Bordeaux **11** (1999), 263–268.

[vdW] B. L. van der Waerden, *Einführung in die Algebraische Geometrie*, Grundlehren der mathematischen Wissenschaften 51, Springer-Verlag, 1939.

[Wa] S. Wang, *A counterexample to Grunwald's theorem*, Ann. of Math. **49**(4) (1948), 1008–1009.

[Wat] G. N. Watson, *Singular moduli* (4), Acta Arith. **1** (1935), 284–323.

[We1] H. Weber, *Lehrbuch der Algebra I*, Chelsea Publishing Company, New York.

[We3] ———, *Lehrbuch der Algebra III*, Chelsea Publishing Company, New York.

[Wei] E. Weiss, *Cohomology of Groups*, Pure and applied mathematics 34, Academic Press, New York, 1969.

[Wh] G. Whaples, *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201–204.

[Wil] C. J. Williamson, *Odd degree polynomials with dihedral Galois groups*, J. Number Theory **34** (1990), 153–173.

[Wi1] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik* p *zu vorgegebener Gruppe der Ordnung* p^f, J. Reine Angew. Math. **174** (1936), 237–245.

[Wi2] ———, *Zyklische Körper und Algebren der Charakteristik* p *vom Grad* p^n, J. Reine Angew. Math. **176** (1937), 126–140.

[Y&Z] N. Yui & D. Zagier, *On the singular values of Weber modular functions*, Math. Comp. **66** (1997), 1645–1662.

[Z] O. Zariski, *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$ *of an algebraic surface*, Illinois J. Math. **2** (1958), 303–315.

[Z&S] O. Zariski & P. Samuel, *Commutative Algebra I*, Graduate Texts in Mathematics 28, Springer-Verlag, 1979.

[Za] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 187–220.

Index