

Springer Monographs in Mathematics

Gunter Malle
B. Heinrich Matzat

Inverse Galois Theory

Second Edition



Springer Monographs in Mathematics

Editors-in-Chief

Isabelle Gallagher, Paris, France
Minhyong Kim, Oxford, UK

Series Editors

Sheldon Axler, San Francisco, USA
Mark Braverman, Toronto, Canada
Maria Chudnovsky, Princeton, USA
Sinan C. Güntürk, New York, USA
Claude Le Bris, Marne la Vallée, France
Pascal Massart, Orsay, France
Alberto Pinto, Porto, Portugal
Gabriella Pinzari, Napoli, Italy
Ken Ribet, Berkeley, USA
René Schilling, Dresden, Germany
Panagiotis Souganidis, Chicago, USA
Endre Süli, Oxford, UK
Shmuel Weinberger, Chicago, USA
Boris Zilber, Oxford, UK

This series publishes advanced monographs giving well-written presentations of the “state-of-the-art” in fields of mathematical research that have acquired the maturity needed for such a treatment. They are sufficiently self-contained to be accessible to more than just the intimate specialists of the subject, and sufficiently comprehensive to remain valuable references for many years. Besides the current state of knowledge in its field, an SMM volume should ideally describe its relevance to and interaction with neighbouring fields of mathematics, and give pointers to future directions of research

More information about this series at <http://www.springer.com/series/3733>

Gunter Malle • B. Heinrich Matzat

Inverse Galois Theory

Second Edition



Springer

Gunter Malle
FB Mathematik
TU Kaiserslautern
Kaiserslautern, Germany

B. Heinrich Matzat
Interdisziplinäres Zentrum für
Wissenschaftliches Rechnen
Universität Heidelberg
Heidelberg, Germany

ISSN 1439-7382 ISSN 2196-9922 (electronic)
Springer Monographs in Mathematics
ISBN 978-3-662-55419-7 ISBN 978-3-662-55420-3 (eBook)
<https://doi.org/10.1007/978-3-662-55420-3>

Library of Congress Control Number: 2017949891

Mathematics Subject Classification (2010): 12F12, 12-XX, 20-XX

© Springer-Verlag GmbH Germany, part of Springer Nature 1999, 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.

The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Preface

Inverse Galois Theory is concerned with the question which finite groups occur as Galois groups over a given field K . In particular this includes the question on the structure and the representations of the absolute Galois group of K and also the question about its finite epimorphic images, the so-called inverse problem of Galois theory. In all these areas important progress was made in the last few years, about which we want to report here.

The first systematic approach to the solution of the inverse problem over the field of rational numbers \mathbb{Q} goes back to Hilbert (1892). Using the irreducibility theorem which he proved for this purpose, he could show that over \mathbb{Q} and more generally over every field finitely generated over \mathbb{Q} there exist infinitely many Galois extensions with the symmetric and the alternating groups S_n and A_n . E. Noether (1918) then stated that the inverse problem for a finite group can be solved with the Hilbert irreducibility theorem if the field of fractions of the ring of invariants of a permutation representation of the group is rational, and that in this case all polynomials with this Galois group can be parametrized. She could verify this condition for permutation groups of small degree, and her student Seidelmann (1918) computed the corresponding parametric polynomials up to degree 4. This line of research was continued for special solvable groups by Breuer, Furtwängler and Gröbner. Unfortunately, not all fields of invariants of finite groups are rational. A first counter example was given by Swan (1969) for the field \mathbb{Q} and by Saltman (1984) for \mathbb{C} .

The next big step was initiated by Scholz (1937) and Reichardt (1937). By solving sufficiently many number theoretic embedding problems they could show that all finite p -groups for odd primes p occur as Galois groups over \mathbb{Q} . This approach culminated in the celebrated solution of the inverse problem of Galois theory for all solvable groups over arbitrary number fields by Šafarevič (1954d, 1989).

The next set of results was furnished by the works of Shih (1974), Fried (1977), Belyi (1979), Matzat (1979, 1984) and Thompson (1984a), in which the concept of rigidity was introduced and investigated. This allows to translate sufficient conditions for the rationality of covers of compact Riemann surfaces with given monodromy group into group theoretic criteria. Thus it is possible with purely group

theoretic considerations to prove the existence of Galois extensions with prescribed Galois group over $\mathbb{Q}(t)$ and, using the Hilbert irreducibility theorem, also over \mathbb{Q} . This approach has proved to be particularly effective in the case of simple and almost simple groups, where the most far reaching results were obtained by Belyi (1979, 1983), Malle (1988b, 1992, 1996) and Reiter (1999).

Another direction of research consists in finding classes of fields for which the inverse problem of Galois theory can be solved completely. By the Riemann existence theorem and the specialization theorem of Grothendieck for the fundamental group this is true for example for algebraic function fields in one variable over algebraically closed fields of characteristic zero; these fields also form the starting point for the rigidity method. The corresponding result in positive characteristic was proved by Harbater (1984). According to a very recent result of Pop (1996) it remains correct if the algebraically closed field of constants is replaced by a sufficiently large field, above which every smooth curve with rational points possesses infinitely many rational points. This result generalizes in particular the case of a PAC (pseudo algebraically closed) field of constants treated earlier by Fried and Völklein (1991). As an application of the latter result Fried and Völklein (1992) and Pop (1996) could show that the absolute Galois group of a countable Hilbertian PAC field is a free profinite group. The same result for function fields in one variable over arbitrary algebraically closed fields of constants has now been proved by Harbater (1995a) and Pop (1995); in characteristic zero this already goes back to Douady (1964).

The aim of this book is to give a consistent and reasonably complete survey of the results obtained in this area, with main emphasis on the rigidity method and its applications. In order to keep the size reasonable we usually have omitted those proofs which are worked out in other books (with the exceptions of the two introductory lecture notes of Matzat (1987) and Serre (1992)). On the other hand we have substantially rewritten a number of results or even given new proofs.

Since the individual chapters all start with their own overview, we will only characterize them briefly. In Chapter I we explain the rigidity method for coverings of the projective line in characteristic zero. We prove the fundamental rationality criteria including the translation technique. As applications we treat the abelian groups, the symmetric and alternating groups S_n and A_n , the 2-dimensional linear groups $L_2(p)$ and $\mathrm{PGL}_2(p)$ as well as the small Mathieu groups M_{11} and M_{12} . This covers the examples of Hilbert (1892) and Shih (1974). At the end we present the explicit calculation of polynomials for some of these groups and give results on the specialization of parameters. This chapter is essentially elementary with complete proofs.

In Chapter II we give a survey on the results obtained by application of the 1-dimensional rigidity method. This includes the almost complete realization of the finite simple groups as Galois groups over $\mathbb{Q}^{\text{ab}}(t)$ and \mathbb{Q}^{ab} in Paragraphs 1 to 5. Here \mathbb{Q}^{ab} denotes the maximal abelian extension field of \mathbb{Q} . In the following Paragraphs 6 to 9 we give a survey of realizations of simple groups over $\mathbb{Q}(t)$ and over \mathbb{Q} . Here the proofs for the linear groups and the sporadic groups are elementary, while for the remaining groups, some knowledge of the Deligne-Lusztig theory of characters of reductive groups is necessary.

In the third chapter we develop the rigidity method for coverings of projective spaces. This covers the approach of Fried (1977). It leads to partial generalizations of the results in Chapter I. Here, though, the concept of rigidity of a braid orbit is not in general sufficient to deduce existence theorems for Galois extensions over $\mathbb{Q}(t)$ and \mathbb{Q} . Usually, further arithmetic conditions like the existence of rational points have to be satisfied. This makes the application considerably harder, as can be seen at the example of the linear and unitary groups treated by Völklein (1993). The second part of this chapter also contains the proof of Fried and Völklein (1991) that over function fields $k(t)$ with a PAC-field of constants k of characteristic zero every finite group occurs as a Galois group. This solves in particular the inverse problem of Galois theory over Hilbertian PAC-fields of characteristic zero.

Chapter IV considers the question of constructing Galois extensions with composite groups from given Galois extensions with simple Galois groups. This leads to embedding problems for arithmetic function fields. In the first part of the chapter we prove simple reduction theorems, and study the range of applicability of the two elementary basic constructions for embedding problems with abelian and with center free kernel. In continuation of the results of Chapter III the developed methods can be used to prove the result of Fried and Völklein that the absolute Galois group of a countable Hilbertian PAC-field of characteristic zero is profinite free. In the second part we study cohomological descriptions of the embedding obstruction. Explicit computation of these obstructions for example gives realizations of the central extensions of the symmetric and alternating groups as Galois groups over $\mathbb{Q}(t)$. This is followed by the investigation of concordant embedding problems in Paragraph 8 and the remaining Hasse obstruction in Paragraph 9. Finally in Paragraph 10 we prove the Theorem of Scholz (1937) and Reichardt (1937) on the realizability of nilpotent groups as Galois groups, more generally over global fields.

In the final Chapter V the methods of ultrametric analysis are used to prove the results of Harbater (1984, 1995a) and Pop (1995, 1996) concerning the inverse problem and more generally the structure of the absolute Galois group for function fields over complete ultrametric fields of constants and, as an application, over algebraically closed fields in positive characteristic. Further, we introduce the notion of large fields and prove the result of Pop (1996) that the absolute Galois group of a countable Hilbertian large field is free profinite. The chapter ends with a short report on the proof by Raynaud (1994) with the extension by Harbater (1994a) of the conjecture of Abhyankar, which characterizes the possible Galois groups over function fields in one variable over algebraically closed fields of constants of positive characteristic with restricted ramification. Unfortunately parts of the proof itself go beyond the scope of this book.

The Appendix contains tables of polynomials with (regular) Galois groups of small permutation rank over \mathbb{Q} and $\mathbb{Q}(t)$.

Finally we mention some topics not covered by this book. First, this concerns the geometric version of the rigidity method for several variables with the construction of Hurwitz schemes following Fried (1977) and Fried and Völklein (1991), which would have led too far away from the field theoretic approach considered here. This aspect is covered in the recent monograph of Völklein (1996). Further, we do not

treat the question of the present state in the Noether problem and more generally the question of generic polynomials. Last but not least this concerns the description of the action of the absolute Galois group or the Grothendieck–Teichmüller group respectively on algebraic fundamental groups, considered by Ihara (1991) et al. (see for example the survey by Nakamura (1997)). This has at present not yet led to new Galois realizations of finite groups.

We want to thank all those which by their cooperation, their criticism and their corrections as well as proposals for improvements have contributed to the present form of the book. In particular these are M. Geck, D. Harbater, M. Jarden, J. Oesterlé, M. v. d. Put, I. R. Šafarevič, L. Schneps, J.-P. Serre, J. Sonn, T. Szamuely, H. Völklein, A. V. Yakovlev, and our colleagues and collaborators R. Dentzer, M. Folkers, H. Geyer, F. Häfner, G. Hiß, G. Kemper, F.-V. Kuhlmann, F. Lübeck, R. Nauheim, F. Pop, U. Porsch, B. Przywara, S. Reiter, and M. Saïdi.

Preface to the Second Edition

Two important new developments have taken place since the appearance of the first edition of this book. The first is the algebraization of the Katz algorithm for (linearly) rigid generating systems of finite groups. The second is the emergence of a modular Galois theory. The latter has led to new construction methods for additive polynomials with given Galois group over fields of positive characteristic. Both methods have their origin in the Galois theory of differential and difference equations.

The algebraic version of the Katz algorithm goes back to Dettweiler and Reiter (2000). It will be presented here with complete proofs which thus replace the long quite involved development in Katz (1996). The chosen presentation follows the later exposition of Dettweiler (2003). This has the advantage of being better adapted to the notation used throughout this book and of leading to somewhat easier formulas in some instances. As an application we will obtain numerous linear groups defined over \mathbb{F}_q , in particular for high prime powers q , as Galois groups of geometric field extensions over $\mathbb{Q}(t)$. This would not be achievable with the simple rigidity method described in Chapter I. The new results are given at the end of Chapter III in Paragraphs 9 and 10. The original Section 9.1 is retained in Paragraph 5 as Section 5.5. The remaining parts of Paragraphs 9 and 10 from the first edition are superimposed by the new results and have thus become superfluous.

Finite Galois extensions N/K in positive characteristic can be generated over K by a finite dimensional \mathbb{F}_q -vector space V , which is moreover stable under the Frobenius operator. Thus such Galois extensions can also be interpreted as solution fields of difference modules over K for the Frobenius operator—Frobenius modules for short—(see van der Put and Singer (1997)). In this way the Galois group

of N/K comes in a natural way equipped with a faithful matrix representation over \mathbb{F}_q , hence with a modular representation. In analogy to the theory of differential modules the containment of the representing matrix of the Frobenius operator in a linear algebraic subgroup of $\mathrm{GL}(V)$ usually leads to a non-trivial upper bound for the Galois group. A corresponding result in characteristic zero is not available. There also exists an algorithm for the computation of Galois groups of additive polynomials, respectively of Frobenius modules. This can be sped up considerably using a modular Dedekind criterion to prove lower bounds. In favorable cases—as they occur in our applications—the upper bound and the lower bound obtained from the modular Dedekind criterion will agree, so that the Galois group can be determined explicitly without having to use the general algorithm for the computation of Galois groups. Moreover it is possible, starting from the representing matrix of the Frobenius operator, to compute directly additive polynomials whose vector space of zeroes generates the solution field of the Frobenius module. With this method for many families of finite groups of Lie type we will construct generating additive polynomials of a very general form with the corresponding Galois group.

Besides the existence of a non-trivial upper bound for the Galois group, modular Galois theory enjoys a further advantage, which has no parallel in characteristic zero due to the missing matrix representation: the field restriction for linear algebraic groups makes it possible to rewrite a representation of a linear group over \mathbb{F}_q into a (larger dimensional) representation over \mathbb{F}_p . Using this it becomes possible for many finite linear groups defined over \mathbb{F}_q , for which there exist geometric Galois extensions N/K with field of constants \mathbb{F}_q , to construct geometric Galois extensions \tilde{N}/\tilde{K} with field of constants \mathbb{F}_p and with the same Galois group. Due to these facts modular Galois theory has developed to a rather attractive, active and independent research area in modular representation theory. The above results are presented in the new Chapter V on Additive Polynomials.

We expect that these two methods will yield geometric Galois realizations of many further groups apart from the ones constructed here. Nevertheless, for a complete solution of the inverse problem of Galois theory most likely further fundamental ideas will have to be conceived.

Apart from the incorporation of the new parts we have also made a number of additions and corrections to the first edition, and have adapted our notation in some parts. Further the tables of example polynomials in the Appendix have been updated and extended. For helpful advice we are indebted in particular to Annette Bachmayr, Michael Dettweiler, Jürgen Klüners, Peter Müller and Stefan Reiter.

Kaiserslautern, Germany
Heidelberg, Germany

G. Malle
B. H. Matzat

Contents

I The Rigidity Method	1
1 The Inverse Galois Problem over $\mathbb{C}(t)$ and $\mathbb{IR}(t)$	2
1.1 The Fundamental Group of the Punctured Riemann Sphere	2
1.2 The Algebraic Variant of the Fundamental Group	3
1.3 Extension by Complex Conjugation	7
1.4 Generalization to Function Fields of Riemann Surfaces	8
2 Arithmetic Fundamental Groups	10
2.1 Descent to Algebraically Closed Subfields	10
2.2 The Fundamental Splitting Sequence	13
2.3 The Action via the Cyclotomic Character	14
2.4 The Theorem of Belyi	16
3 Fields of Definition of Galois Extensions	19
3.1 Cyclic and Projective Descent	19
3.2 Fields of Definition of Geometric Field Extensions	21
3.3 Fields of Definition of Geometric Galois Extensions	22
4 The Rigidity Property	26
4.1 The Hurwitz Classification	26
4.2 The Fixed Field of a Class of Generating Systems	28
4.3 The Basic Rigidity Theorem	29
4.4 Choice of Ramification Points	31
5 Verification of Rigidity	34
5.1 Geometric Galois Extensions over $\mathbb{Q}(t)$ with Abelian Groups	34
5.2 Geometric Galois Extensions over $\mathbb{Q}(t)$ with S_n and A_n	35
5.3 Structure Constants	36
5.4 The Rigidity Criterion of Belyi	40
6 Geometric Automorphisms	43
6.1 Extension of the Algebraic Fundamental Group	43
6.2 The Action of Geometric Automorphisms	45

	6.3	Rigid Orbits	47
	6.4	The Twisted Rigidity Theorem	49
	6.5	Geometric Galois Extensions over $\mathbb{Q}(t)$ with M_{12} and M_{11}	50
7		Rational Translates of Galois Extensions	53
	7.1	Galois Rational Translates	53
	7.2	Rational Translates with Few Ramification Points	54
	7.3	Twisting Rational Translates	57
	7.4	Geometric Galois Extensions over $\mathbb{Q}(t)$ with $L_2(p)$	60
8		Automorphisms of the Galois Group	63
	8.1	Fixed Fields of Coarse Classes of Generating Systems	63
	8.2	Extension of the Galois Group by Outer Automorphisms	65
	8.3	Geometric Extension of the Galois Group by Outer Automorphisms	66
	8.4	Geometric Galois Extensions over $\mathbb{Q}(t)$ with $PGL_2(p)$	68
9		Computation of Polynomials with Prescribed Group	70
	9.1	Decomposition of Prime Divisors in Galois Extensions	70
	9.2	Polynomials with Groups S_n and A_n	72
	9.3	Polynomials with the Group $\text{Aut}(A_6)$ and Related Groups	75
	9.4	Polynomials with the Mathieu Groups M_{12} and M_{11}	78
10		Specialization of Geometric Galois Extensions	82
	10.1	Local Structure Stability	82
	10.2	Reality Questions	83
	10.3	Ramification in Minimal Fields of Definition	86
	10.4	Ramification in Residue Fields	88
II Applications of Rigidity			91
1		The General Linear Groups	93
	1.1	Groups of Lie Type	93
	1.2	Rigidity for $GL_n(q)$	95
	1.3	Galois Realizations for Linear Groups	98
2		Pseudo-Reflection Groups and Belyi Triples	100
	2.1	Groups Generated by Pseudo-Reflections	100
	2.2	An Effective Version of Belyi's Criterion	101
	2.3	Imprimitive and Symmetric Groups	103
	2.4	Invariant Forms	104
3		The Classical Groups	107
	3.1	Rigidity for $GU_n(q)$	107
	3.2	Rigidity for $CSp_{2n}(q)$	108
	3.3	Rigidity for $SO_{2n+1}(q)$	110
	3.4	Rigidity for $CO_{2n}^+(q)$	111
	3.5	Rigidity for $CO_{2n}^-(q)$	115

4	The Exceptional Groups of Rank at Most 2	117
4.1	Divisibility Criteria	117
4.2	Rigidity for the Ree Groups ${}^2G_2(q^2)$	118
4.3	Rigidity for the Groups $G_2(q)$	120
4.4	Rigidity for the Groups ${}^3D_4(q)$	122
4.5	Rigidity for the Groups ${}^2B_2(8)$ and ${}^2F_4(2)'$	124
5	The Exceptional Groups of Large Rank	126
5.1	Results From Deligne–Lusztig Theory	126
5.2	Rigidity for the Groups $F_4(q)$	128
5.3	Rigidity for the Groups $E_6(q)$ and ${}^2E_6(q)$ for odd q	131
5.4	Rigidity for the Groups $E_6(2^{2m+1})$ and ${}^2E_6(2^{2m})$	135
5.5	Rigidity for the Groups $E_7(q)$	137
5.6	The Groups $E_8(q)$	138
6	Galois Realizations of Linear and Unitary Groups over \mathbb{Q}	140
6.1	Extension by the Graph Automorphism	140
6.2	GA-Realizations over \mathbb{Q}^{ab}	143
6.3	GA-Realizations over \mathbb{Q}	144
7	Galois Realizations of Symplectic and Orthogonal Groups over \mathbb{Q}	146
7.1	GA-Realizations of Symplectic Groups over \mathbb{Q}	146
7.2	GA-Realizations of Odd-Dimensional Orthogonal Groups	148
7.3	Even-Dimensional Split Orthogonal Groups	150
7.4	Even-Dimensional Non-split Orthogonal Groups	151
7.5	The 8-Dimensional Split Orthogonal Groups	152
8	Galois Realizations of Exceptional Groups over \mathbb{Q}	155
8.1	GA-Realizations for the Groups $G_2(p)$	155
8.2	The Groups $F_4(p)$	156
8.3	The Groups $E_6(p)$ and ${}^2E_6(p)$	158
8.4	The Groups $E_8(p)$	159
9	The Sporadic Groups	161
9.1	The Mathieu Groups	161
9.2	The Leech Lattice Groups	163
9.3	The Fischer Groups	165
9.4	The Monster Centralizers	166
9.5	The Oddments	169
9.6	Galois Realizations for the Sporadic Groups	172
10	Summary for Simple Groups	173
10.1	Galois Realizations over \mathbb{Q}^{ab}	173
10.2	Galois Realizations over \mathbb{Q}	174
III Action of Braids	177	
1	Braid Groups	179
1.1	The Artin Braid Group	179
1.2	The Hurwitz Braid Group	181

1.3	The Pure Hurwitz Braid Group	183
1.4	The Word Problem	185
2	Profinite Braid Groups	187
2.1	The Hurwitz Braid Group as Galois Group	187
2.2	Inertia Groups	190
2.3	Structure of the Profinite Hurwitz Braid Group	192
2.4	The Fixed Field of the Free Normal Subgroup	193
3	Galois Descent	196
3.1	An Arithmetic Fundamental Group	196
3.2	Hurwitz Classification	197
3.3	The Fixed Field of a Class of Generating Systems	199
3.4	Using the Symmetry Group	200
4	Cyclic Polynomials	203
4.1	Cyclic Polynomials in Several Variables	203
4.2	Cyclic Polynomials in One Variable	207
4.3	Cyclic Artin-Schreier Towers	208
5	Rigid Braid Orbits	211
5.1	The Regularity Criterion	211
5.2	Braid Orbit Genera	213
5.3	A Rationality Criterion for the Pure Braid Group	215
5.4	Rational Translation of Braid Orbits	216
5.5	Groups of Automorphisms as Galois Groups	219
6	Unramified Rational Places	222
6.1	Specialization of the Fundamental Group	222
6.2	The Specialization Theorem	223
6.3	The Theorem of Conway and Parker	225
6.4	The Inverse Galois Problem over PAC-Fields	229
7	Braids and Geometric Automorphisms	231
7.1	Specialization to Two Variables	231
7.2	Action of Geometric Automorphisms	232
7.3	Symmetrized Braid Orbit Genera	235
7.4	A Twisted Braid Orbit Theorem	238
7.5	Geometric Galois Extensions over $\mathbb{Q}(t)$ with M_{24}	240
8	Ramified Rational Places	241
8.1	Decomposition Groups of Ramified Places	241
8.2	Description via the Hurwitz Classification	243
8.3	Braid Cycle Orbits	244
8.4	Prime Divisors of Odd Degree	248
9	The Katz Algorithm	250
9.1	The Convolution Functor	250
9.2	Multiplicativity of Convolution	254
9.3	Linear Rigidity	260
9.4	The Existence Algorithm of Katz	264
9.5	Braid Compatibility	268

10	Applications of the Katz Algorithm	270
10.1	Jordan–Pochhammer Tuples	270
10.2	Linear and Unitary Groups	273
10.3	Symplectic Groups	276
10.4	Orthogonal Groups	279
10.5	Results for Groups in Characteristic Two	283
IV Embedding Problems	285	
1	Geometric Embedding Problems	287
1.1	Hilbertian Fields	287
1.2	Solutions of Embedding Problems	288
1.3	Direct Decomposition of the Kernel	290
1.4	From Improper to Proper Solutions	292
1.5	Fields with Projective Galois Group	294
2	Split Embedding Problems with Abelian Kernel	296
2.1	Wreath Products	296
2.2	Split Extensions with Abelian Kernel	297
2.3	Semiabelian Groups	299
3	Embedding Problems with Centerless Kernel	302
3.1	The Notion of GAR-Realization	302
3.2	Embedding Problems with Characteristically Simple Kernel	303
3.3	Galois Groups of Hilbertian PAC-Fields	306
4	Verification of the GAR-Property	310
4.1	GAR-Realizations in One Variable	310
4.2	Fields of Constants with Trivial Brauer Group	311
4.3	GAR-Realizations in Several Variables	312
4.4	Specialization to GAR-Realizations in Two Variables	314
5	Frattini Embedding Problems	317
5.1	A Decomposition Theorem	317
5.2	The Frattini Embedding Theorem	318
5.3	Centerless Frattini Extensions	321
5.4	Central Frattini Extensions and $2 \cdot A_n$	323
5.5	Central Extensions of A_n	327
6	The Quadratic Trace Form	329
6.1	The Cohomological Embedding Obstruction	329
6.2	The Trace Form	331
6.3	A Criterion of Serre	333
6.4	Central Extensions of S_n	335
7	Brauer Embedding Problems	339
7.1	Regular Solutions of Brauer Embedding Problems	339
7.2	The Horizontal Local-Global Principle	340
7.3	The Vertical Local-Global Principle	343
7.4	Covering Groups of Simple Groups over $\mathbb{Q}^{\text{ab}}(t)$	345

8	Concordant Embedding Problems	347
8.1	The Reduction Theorem of Kochendörffer	347
8.2	The Concordance Condition	350
8.3	Concordance over Local Fields	354
8.4	Concordance over Global Fields	355
9	The Hasse Embedding Obstruction	358
9.1	Kummer Extensions	358
9.2	Definition of the Hasse Obstruction	360
9.3	Translation of the Hasse Obstruction	364
9.4	The Hasse Obstruction for Global Fields	366
10	Nilpotent Galois Groups over Global Fields	372
10.1	Scholz Extensions	372
10.2	Scholz Embedding Problems	375
10.3	The Theorem of Scholz and Reichardt	379
10.4	Nilpotent Galois Groups over Global Function Fields	380
V	Additive Polynomials	383
1	Frobenius Modules	385
1.1	Ordinary Frobenius Modules	385
1.2	Cyclic Frobenius Modules	387
1.3	Galois Groups	390
1.4	Effective Frobenius Modules	392
2	Computation of the Galois Group	394
2.1	An Invariant Theoretic Criterion	394
2.2	Computation of Homogeneous Invariants	397
2.3	Specialization of Relative Resolvents	398
2.4	Linear Tschirnhaus Transformations	400
2.5	The Modular Dedekind Criterion	402
3	Polynomials for Split Groups of Lie Type	406
3.1	Linear Groups SL_{n+1}	406
3.2	Symplectic Groups	410
3.3	Odd-Dimensional Orthogonal Groups	413
3.4	Even-Dimensional Orthogonal Groups $SO_{2n}^+(q)$	416
3.5	The Dickson Groups $G_2(q)$	420
4	Polynomials for Twisted Groups of Lie Type	423
4.1	The Special Unitary Groups $SU_n(q)$	423
4.2	The Orthogonal Groups $SO_{2n}^-(q)$	428
4.3	The Suzuki Groups ${}^2B_2(q^2)$	432
4.4	The Ree Groups ${}^2G_2(q^2)$	434
4.5	The Steinberg Triality Groups ${}^3D_4(q)$	435
5	Field Restriction in Modular Galois Theory	440
5.1	Base Field Reduction	440
5.2	Application to Groups of Lie Type	442
5.3	Explicit Polynomials for $SL_{n+1}(q)$	443

VI Rigid Analytic Methods	447
1 Results from Rigid Analytic Geometry	449
1.1 Tate Algebras	449
1.2 Rigid Analytic Spaces	451
1.3 Analytification of Algebraic Varieties	453
1.4 The GAGA-Principle for $\mathbb{P}^1(k)^{\text{an}}$	455
2 The Inverse Problem over $\mathbb{Q}_p(t)$ and $\overline{\mathbb{F}}_p(t)$	460
2.1 Induced Covers	460
2.2 The Inverse Problem over Complete Ultrametric Fields	462
2.3 The Inverse Problem over $\overline{\mathbb{F}}_p(t)$	463
2.4 The Conjecture of Šafarevič for $\overline{\mathbb{F}}_p(t)$	464
3 Free Quotients of the Fundamental Group	467
3.1 Free Composites of Galois Extensions	467
3.2 Galois Action	469
3.3 A Free Quotient of the Algebraic Fundamental Group	471
4 Large Fields	474
4.1 Existentially Closed Fields	474
4.2 Characterization of Large Fields	475
4.3 Split Embedding Problems over Large Fields	477
4.4 Application to Hilbertian PAC-Fields	479
5 On the Fundamental Group with Restricted Ramification	480
5.1 Projectivity	480
5.2 Embedding Problems with p -Kernel	483
5.3 The Conjecture of Abhyankar for the Affine Line	483
5.4 The General Case of the Conjecture of Abhyankar	485
Appendix: Example Polynomials	491
1 Regular Realizations for Transitive Groups of Degree Less than 12	491
2 Regular Realizations for Nonsolvable Primitive Groups	499
3 Realizations over \mathbb{Q} for Transitive Groups of Degree up to 14	502
References	515
Index	531

I The Rigidity Method

The idea of deducing the realizability of a finite group as Galois group over $\mathbb{Q}(t)$ from the existence of rigid systems of generators as far as we know first appeared implicitly in the appendix to the dissertation of Shih (1974). This concept was subsequently considered independently by Fried (1977), Belyi (1979), Matzat (1979, 1984, 1985a) and later Thompson (1984a) and extended in different directions. In this first chapter we develop the one variable treatment by Belyi, Matzat and Thompson, which in essence relies on the covering theory of the punctured Riemann sphere (resp. $\mathbb{P}^1(\mathbb{C})$) and the classical Riemann existence theorem. (In the third chapter, the multi-variable approach going back to work of Fried will be presented.)

The first five paragraphs lead directly to the Basic Rigidity Theorem including its character theoretic and representation theoretic variants and thus form the main body of this chapter. Other treatments of the main results in this part may be found in the lecture notes of Matzat (1987), Kap. I, as well as in those of Serre (1992), Sect. 7–9.

The next five paragraphs contain further leading results. In the sixth paragraph we study outer automorphisms of the fundamental group originating from embeddings, which are here called geometric automorphisms, in contrast to earlier notation (Matzat (1986, 1987)). These can be employed to derive the Twisted Rigidity Theorem as the currently strongest variant of the Basic Rigidity Theorem. In the next paragraph we introduce the translation technique of Shih (1974) and Malle (1991) and apply it to the groups $L_2(p)$. Paragraph 8 contains the results needed for the realization of automorphism groups of finite groups as Galois groups; the prototype for this embedding theorem can be found in Matzat (1992). Finally in Paragraph 9 we show how to construct generating polynomials for field extensions whose existence was proved with the rigidity method, and in Paragraph 10 we note what can be said about specializations of such polynomials, using the results of Fried and Dèbes (1990) and Beckmann (1989, 1991).

As examples we consider the abelian groups, the groups A_n and S_n , $L_2(p)$ and $PGL_2(p)$, as well as the smallest sporadic groups M_{11} and M_{12} . The second chapter will then contain a systematic study of the results obtainable by the rigidity method in the area of finite almost simple groups.

1 The Inverse Galois Problem over $\mathbb{C}(t)$ and $\mathbb{R}(t)$

The structure of the fundamental group of the punctured Riemann sphere is well known. From its algebraic variant, the classical solution of the inverse problem of Galois theory over $\mathbb{C}(t)$ follows immediately. After extension of the fundamental group by complex conjugation one also derives the solution of the inverse Galois problem over $\mathbb{R}(t)$.

1.1 The Fundamental Group of the Punctured Riemann Sphere

Our starting point is the Riemann sphere $\mathcal{X} := \hat{\mathbb{C}}$. From this, a set of s points $\mathcal{S} := \{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ is removed. For any choice of base point $\mathcal{P}_0 \in \mathcal{X} \setminus \mathcal{S}$ the topological fundamental group $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$ relative to \mathcal{P}_0 is generated by homotopy classes of nonintersecting loops γ_i from \mathcal{P}_0 counterclockwise around \mathcal{P}_i .

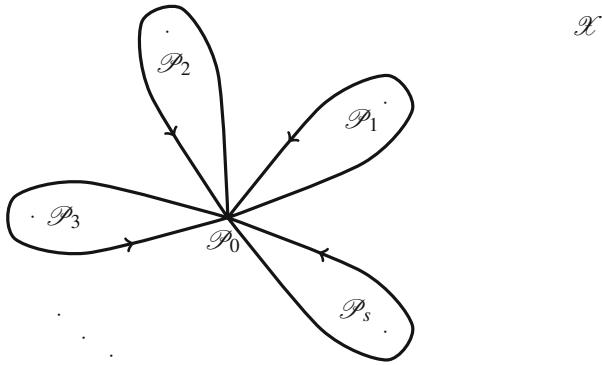


Fig. 1.1 Generators of $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$

The path obtained by concatenation of representatives for the γ_i can clearly be contracted to one point on $\mathcal{X} \setminus \mathcal{S}$, so the generators $\gamma_1, \dots, \gamma_s$ of π_1^{top} satisfy at least the relation $\gamma_1 \cdots \gamma_s = 1$.

Theorem 1.1 (Hurwitz (1891)). *Let \mathcal{S} be a subset of the Riemann sphere $\mathcal{X} = \hat{\mathbb{C}}$ of cardinality s . Then the fundamental group $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$ with respect to any base point $\mathcal{P}_0 \in \mathcal{X} \setminus \mathcal{S}$ has the structure*

$$\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0) = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle. \quad (1.1)$$

A proof of this result can be found for example in Seifert and Threlfall (1934), §47 (see also Stöcker and Zieschang (1988), Aufgabe 5.7.A2).

The only continuous automorphism of the field of complex numbers \mathbb{C} is given by complex conjugation, denoted here by ρ . If the set \mathcal{S} introduced previously and the base point \mathcal{P}_0 remain stable under ρ , i.e., if $\mathcal{S}^\rho = \mathcal{S}$ and $\mathcal{P}_0^\rho = \mathcal{P}_0$, then ρ acts on $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$. Indeed, assume that \mathcal{S} consists of r pairs of complex conjugate points $\mathcal{P}_1, \dots, \mathcal{P}_{2r}$ arranged first by decreasing imaginary part and then by decreasing real part (in case of equality of the imaginary parts), and the real points $\mathcal{P}_{2r+1} < \dots < \mathcal{P}_s$. Choosing the real base point $\mathcal{P}_0 < \mathcal{P}_{2r+1}$ we obtain the following diagram:

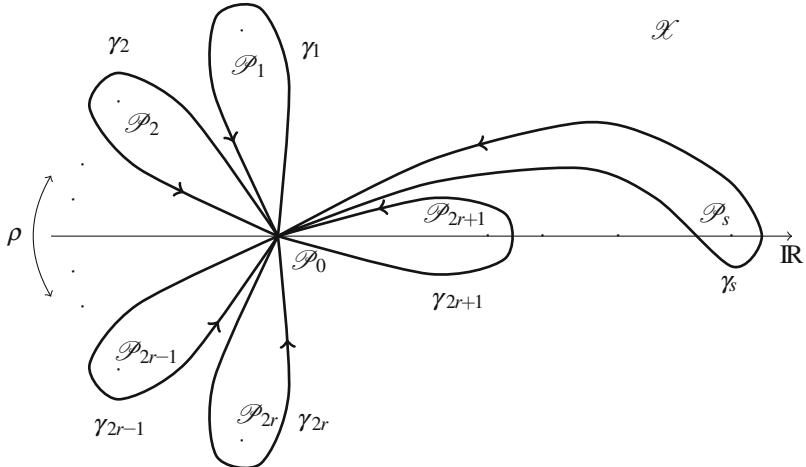


Fig. 1.2 Action of complex conjugation

With this standard arrangement, the homotopy classes of paths γ_i are sent to γ_{2r+1-i}^{-1} for $i = 1, \dots, 2r$, and γ_{2r+j} for $j = 1, \dots, s - 2r$ is mapped to

$$\gamma_{2r+1} \cdots \gamma_{2r+j-1} \gamma_{2r+j}^{-1} \gamma_{2r+j-1}^{-1} \cdots \gamma_{2r+1}^{-1}.$$

This proves the following:

Theorem 1.2 (Hurwitz (1891)). *If the set \mathcal{S} and the base point \mathcal{P}_0 in Theorem 1.1 are stable under complex conjugation ρ , then ρ induces an automorphism of $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$. With the standard arrangement of the base point \mathcal{P}_0 and the points in \mathcal{S} as in Figure 1.2, ρ acts on the generators of $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$ via*

$$(\gamma_1, \dots, \gamma_s)^\rho = (\gamma_{2r}^{-1}, \dots, \gamma_1^{-1}, \gamma_{2r+1}^{-1}, \dots, (\gamma_s^{-1})^{\gamma_{s-1}^{-1} \cdots \gamma_{2r+1}^{-1}}). \quad (1.2)$$

1.2 The Algebraic Variant of the Fundamental Group

The topological fundamental group π_1^{top} has an algebraic analogue π_1^{alg} , for which however the convenient visualization as group of homotopy classes of paths is lost.

Namely, let $K := \mathbb{C}(\mathcal{X})$ be the function field of $\mathcal{X} = \hat{\mathbb{C}}$, or equivalently of the projective line $\mathbb{P}^1(\mathbb{C})$. Then K is isomorphic to the field of rational functions $\mathbb{C}(t)$ over \mathbb{C} . Denote by $\text{IP}(K/\mathbb{C})$ the set of prime divisors or equivalently valuation ideals of the function field K/\mathbb{C} . Then the set $\mathcal{S} \subset \mathcal{X}$ corresponds to the subset \mathbb{S} of primes of K/\mathbb{C} whose valuation ideal has a common zero at one of the points \mathcal{P}_i .

Now let $N_{\mathbb{S}}$ denote the set of all finite Galois extension fields of K , ramified only at prime divisors of \mathbb{S} , in a fixed algebraic closure \hat{K} of K . The union of all $N \in N_{\mathbb{S}}$ forms the maximal extension field $M_{\mathbb{S}}$ of K (in \hat{K}) unramified outside \mathbb{S} . It is again Galois over K , and the (for $|\mathbb{S}| > 1$ finite) Galois group is obtained as the projective limit of the finite Galois groups $\text{Gal}(N/K)$:

$$\text{Gal}(M_{\mathbb{S}}/K) = \varprojlim (\text{Gal}(N/K))_{N \in N_{\mathbb{S}}}. \quad (1.3)$$

This Galois group formally depending on \hat{K} is called the *algebraic fundamental group* of $\mathcal{X} \setminus \mathcal{S}$:

$$\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) = \pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}, \hat{K}) := \text{Gal}(M_{\mathbb{S}}/K). \quad (1.4)$$

For the algebraic fundamental group we get the following profinite version of Riemann's existence theorem:

Theorem 1.3 (Profinite Riemann Existence Theorem). *The algebraic fundamental group $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ is isomorphic to the profinite completion of the topological fundamental group $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$:*

$$\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) \cong \hat{\pi}_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0).$$

Moreover for any choice of the base point \mathcal{P}_0 there exists a monomorphism

$$\iota : \pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0) \longrightarrow \pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}),$$

such that $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ is generated as topological group by the images of the γ_i (where $\iota(\gamma_i)$ is identified with γ_i):

$$\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle. \quad (1.5)$$

Proof. We write $\mathcal{X}^* := \mathcal{X} \setminus \mathcal{S}$. The topological space \mathcal{X}^* is sufficiently connected (in the sense of Stöcker and Zieschang (1988), Def. 6.4.3), so there exists a universal covering

$$u : \hat{\mathcal{X}}^* \rightarrow \mathcal{X}^*,$$

whose group of covering transformations (deck transformations) equipped with the product of mappings is isomorphic to $\pi_1^{\text{top}}(\mathcal{X}^*; \mathcal{P}_0)$:

$$\omega : \text{Deck}(u) \rightarrow \pi_1^{\text{top}}(\mathcal{X}^*; \mathcal{P}_0) \quad (1.6)$$

(see for example loc. cit., Kor. 6.5.5, or Forster (1981), Thm. 5.6). The isomorphism is not canonical and depends on the choice of a point $\hat{\mathcal{P}}_0 \in \hat{\mathcal{X}}^*$ above \mathcal{P}_0 . From the fundamental theorem for coverings of topological surfaces (Stöcker and Zieschang (1988), Satz 6.6.3) it follows that for each finite unramified normal covering

$$p^* : \mathcal{Y}^* \rightarrow \mathcal{X}^*$$

there exists a normal subgroup O of finite index in $\text{Deck}(u)$ such that \mathcal{Y}^* is homeomorphic over \mathcal{X}^* to the orbit space $\hat{\mathcal{X}}^*/O$ (equipped with the quotient topology). Via the canonical map from $\hat{\mathcal{X}}^*$ onto $\hat{\mathcal{X}}^*/O$ we obtain a universal covering

$$v : \hat{\mathcal{X}}^* \rightarrow \mathcal{Y}^* \cong \hat{\mathcal{X}}^*/O$$

of \mathcal{Y}^* with $p^* \circ v = u$ and $\text{Deck}(v) \cong O$. Then we have

$$\text{Deck}(p^*) \cong \text{Deck}(u)/\text{Deck}(v).$$

Now the covering p^* is holomorphic with respect to the lifted analytic structures, so by the Riemann Hebbarkeitssatz it possesses a uniquely determined holomorphic continuation

$$p : \mathcal{Y} \longrightarrow \mathcal{X}$$

on the compactification \mathcal{Y} of \mathcal{Y}^* (see Forster (1981), Thm. 8.4). This continuation is unramified outside \mathcal{S} , and moreover satisfies

$$\text{Deck}(p) \cong \text{Deck}(p^*).$$

The field $N := \mathbb{C}(\mathcal{Y})$ is a Galois extension of $K = \mathbb{C}(\mathcal{X})$, unramified over K outside of the set of prime divisors \mathbb{S} of K/\mathbb{C} belonging to \mathcal{S} . Its degree coincides by the Riemann existence theorem with the number of sheets of the coverings p and p^* . From this it follows that

$$\text{Gal}(N/K) \cong \text{Deck}(p)$$

(with $\text{Gal}(N/K)$ acting on the right), and hence finally

$$\text{Gal}(N/K) \cong \pi_1^{\text{top}}(\mathcal{X}^*; \mathcal{P}_0)/\omega(O) \quad (1.7)$$

with ω from (1.6) (see loc. cit., Thm. 8.12). Conversely, each finite field extension N of K unramified outside \mathbb{S} uniquely determines a compact Riemann surface \mathcal{Y} , which is unramified outside of \mathcal{S} , and with $N = \mathbb{C}(\mathcal{Y})$. Two such extension fields are isomorphic over K precisely when the corresponding Riemann surfaces are homeomorphic over \mathcal{X} (see loc. cit., Thm. 8.3 with Ex. 8.1).

Now let $N_{\mathbb{S}}$ be the set of all finite Galois extensions of K inside \hat{K} unramified outside \mathbb{S} , and denote by \mathcal{O} the set of all normal subgroups of $\text{Deck}(u)$ of finite index. Then $M_{\mathbb{S}} := \bigcup_{N \in N_{\mathbb{S}}} N$ is Galois over K and there exists an isomorphism

$$\begin{aligned} \hat{\omega} : \text{Gal}(M_{\mathbb{S}}/K) &= \varprojlim (\text{Gal}(N/K))_{N \in N_{\mathbb{S}}} \xrightarrow{\sim} \\ &\varprojlim (\pi_1^{\text{top}}(\mathcal{X}^*; \mathcal{P}_0)/\omega(O))_{O \in \mathcal{O}} = \hat{\pi}_1^{\text{top}}(\mathcal{X}^*; \mathcal{P}_0) \end{aligned}$$

since the structural homomorphisms of the respective projective systems commute with the isomorphisms from (1.7). As $\pi_1^{\text{top}}(\mathcal{X}^\circ; \mathcal{P}_0)$ is free of finite rank, hence residually finite (see for example Lyndon and Schupp (1977), Ch. III, Prop. 7.11, with complement on p.195), the canonical homomorphism

$$\hat{\iota} : \pi_1^{\text{top}}(\mathcal{X}^\circ; \mathcal{P}_0) \rightarrow \hat{\pi}_1^{\text{top}}(\mathcal{X}^\circ; \mathcal{P}_0)$$

has trivial kernel (see Serre (1964), §1.1). Hence

$$\iota := \hat{\omega}^{-1} \circ \hat{\iota} : \pi_1^{\text{top}}(\mathcal{X}^\circ; \mathcal{P}_0) \rightarrow \text{Gal}(\mathbf{M}_{\mathbf{S}}/\mathbf{K}) = \pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$$

is a monomorphism with the property (1.5). \square

It remains to study the role of the embedded homotopy classes $\gamma_1, \dots, \gamma_s$ in $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$. This is achieved with:

Theorem 1.4 (Abhyankar (1957)). *The images of the homotopy classes $\gamma_1, \dots, \gamma_s$ in $\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)$ embedded via ι into $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ generate procyclic inertia groups in the Galois group $\text{Gal}(\mathbf{M}_{\mathbf{S}}/\mathbf{K}) = \pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$. More precisely the valuation ideals \mathfrak{P}_i of \mathbf{K}/\mathbb{C} corresponding to $\mathcal{P}_i \in \mathcal{S}$ may be embedded into valuation ideals $\hat{\mathfrak{P}}_i$ of $\mathbf{M}_{\mathbf{S}}/\mathbb{C}$ such that the respective inertia groups satisfy*

$$I(\hat{\mathfrak{P}}_i / \mathfrak{P}_i) = \langle \gamma_i \rangle. \quad (1.8)$$

Proof. We continue to use the notation introduced in the proof of Theorem 1.3 above. In particular, $\hat{\mathcal{P}}_0 \in \hat{\mathcal{X}}^\circ$ denotes the point above \mathcal{P}_0 used in the construction of ω and ι . By the Main Lemma of Covering Theory (see for example Stöcker and Zieschang (1988), Satz 6.22) any path c_i representing the homotopy class γ_i possesses a unique lifting to a path \tilde{c}_i on \mathcal{Y} with $\tilde{c}_i(0) = \hat{\mathcal{P}}_0 := v(\hat{\mathcal{P}}_0)$.

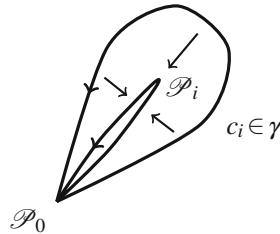


Fig. 1.3 Deformation of c_i

Deforming this path according to Figure 1.3 homotopically in $\mathcal{X}^\circ \cup \{\mathcal{P}_i\}$ yields a double path c_i^* connecting \mathcal{P}_0 and \mathcal{P}_i . Then c_i^* also possesses a lifting \tilde{c}_i^* on \mathcal{Y}

with respect to the extension p of p^* , satisfying $\tilde{c}_i^*(0) = \tilde{\mathcal{P}}_0$. We denote by $\tilde{\mathcal{P}}_i$ the intersection of the fiber $p^{-1}(\mathcal{P}_i)$ with \tilde{c}_i^* , and by d_i the covering transformation of p determined by $d_i(\tilde{\mathcal{P}}_0) = \tilde{c}_i^*(1)$. The points $\tilde{\mathcal{P}}_i$ are now d_i -invariant, and we have $d_1 \circ \dots \circ d_s = \text{Id}$.

Let $\tilde{\mathfrak{P}}_i$ be the valuation ideal of \mathbf{N} defined by $\tilde{\mathcal{P}}_i$, and σ_i the automorphism in $G := \text{Gal}(\mathbf{N}/\mathbf{K})$ induced by $f^{\sigma_i}(\tilde{\mathcal{P}}) := f(d_i(\tilde{\mathcal{P}}))$ for $f \in \mathbf{N}$. As $\tilde{\mathfrak{P}}_i^{\sigma_i} = \tilde{\mathfrak{P}}_i$, the element σ_i is contained in the decomposition group and hence the inertia group $G_I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$. Conversely, if $\sigma \in G_I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$ is given, then the corresponding covering transformation d leaves invariant the point $\tilde{\mathcal{P}}_i \in \mathcal{Y}$. Obviously all such covering transformations are obtained when lifting the powers of γ_i , hence σ_i is a generating element of $G_I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$. The elements $(\sigma_i)_{\mathbf{N} \in \mathbf{N}_{\mathbf{s}}}$ in the projective limit

$$\text{Gal}(\mathbf{M}_{\mathbf{s}}/\mathbf{K}) = \varprojlim (\text{Gal}(\mathbf{N}/\mathbf{K}))_{\mathbf{N} \in \mathbf{N}_{\mathbf{s}}}$$

coincide by construction with the generators $\gamma_i = \iota(\gamma_i)$ of $\text{Gal}(\mathbf{M}_{\mathbf{s}}/\mathbf{K})$ in (1.5). Moreover, with $\hat{\mathfrak{P}}_i := \bigcup_{\mathbf{N} \in \mathbf{N}_{\mathbf{s}}} \tilde{\mathfrak{P}}_i$ we obtain a valuation ideal of $\mathbf{M}_{\mathbf{s}}$ whose inertia group in $\mathbf{M}_{\mathbf{s}}/\mathbf{K}$ is generated as profinite group by $\gamma_i = (\sigma_i)_{\mathbf{N} \in \mathbf{N}_{\mathbf{s}}}$. \square

The previous considerations now easily yield a solution of the inverse problem of Galois theory over the field of rational functions $\mathbb{C}(t)$:

Corollary 1.5. *Every finite group occurs as Galois group over $\mathbb{C}(\mathcal{X}) \cong \mathbb{C}(t)$.*

Proof. Let the finite group G be generated by the elements $\sigma_1, \dots, \sigma_{s-1}, s \geq 2$. Then there exists a continuous epimorphism

$$\psi : \text{Gal}(\mathbf{M}_{\mathbf{s}}/\mathbf{K}) \rightarrow G \quad \text{with} \quad \psi(\gamma_i) = \sigma_i \quad \text{for} \quad i = 1, \dots, s-1$$

(and $\psi(\gamma_s) = (\sigma_1 \cdots \sigma_{s-1})^{-1}$). The fixed field $\mathbf{N} := \mathbf{M}_{\mathbf{s}}^{\ker(\psi)}$ now yields a Galois extension of $\mathbf{K} = \mathbb{C}(\mathcal{X})$ with

$$\text{Gal}(\mathbf{N}/\mathbf{K}) \cong \text{Gal}(\mathbf{M}_{\mathbf{s}}/\mathbf{K}) / \ker(\psi) \cong G. \quad \square$$

1.3 Extension by Complex Conjugation

Under the assumptions of Theorem 1.2 the field $\mathbf{M}_{\mathbf{s}}$ is not only Galois over $\mathbb{C}(t)$, but also over $\mathbb{R}(t)$. More precisely we have:

Theorem 1.6. *Let \mathcal{S} be a finite subset of $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$ invariant under complex conjugation ρ , and let $\mathbf{M}_{\mathbf{s}}/\mathbb{C}(\mathcal{X})$ denote the maximal field extension unramified outside the prime divisors in \mathbf{s} . Then we have*

$$\text{Gal}(\mathbf{M}_{\mathbf{s}}/\mathbb{R}(\mathcal{X})) \cong \pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) \rtimes Z_2. \quad (1.9)$$

If the ramification points, the base point and the homotopy classes of paths are chosen in the standard configuration of Figure 1.2, then the generator ρ of the cyclic

group Z_2 of order 2 acts on the embedded topological generators γ_i of $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ via

$$(\gamma_1, \dots, \gamma_s)^\rho = (\gamma_{2r}^{-1}, \dots, \gamma_1^{-1}, \gamma_{2r+1}^{-1}, \dots, (\gamma_s^{-1})^{\gamma_{s-1}^{-1} \cdots \gamma_{2r+1}^{-1}}). \quad (1.10)$$

Proof. By Theorem 1.2 the complex conjugation map ρ acts on the generators γ_i of the topological fundamental group in the described manner. As the corresponding formula remains valid for the canonical projections of the γ_i in the finite factor groups

$$\pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0)/O \cong \text{Gal}(\mathbf{N}/\mathbb{C}(\mathcal{X})),$$

ρ may be lifted to an automorphism $\hat{\rho}$ of $\mathbf{M}_{\mathbb{S}}/\mathbb{C}(\mathcal{X})$ with $\hat{\mathfrak{P}}_0^{\hat{\rho}} = \hat{\mathfrak{P}}_0$, which moreover acts like ρ on the embedded topological generators γ_i of $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$. Being a generator of the decomposition group of $\hat{\mathfrak{P}}_0/\mathfrak{P}_0$, $\hat{\rho}$ has order 2. Renaming $\hat{\rho}$ to ρ we thus obtain the assertion. \square

We call a finite field extension $N/k(t)$ *geometric*, if k is algebraically closed in N (or equivalently, if N/k is regular). The above structure theorem now yields a solution of the inverse Galois problem for $\text{IR}(t)$ even in the strong form:

Corollary 1.7 (Krull and Neukirch (1971)). *Every finite group occurs as a geometric Galois group over $\text{IR}(t)$.*

Proof. Let G be a finite group, generated by $\sigma_1, \dots, \sigma_r$. For a chosen ρ -invariant subset $\mathcal{S} \subset \mathcal{X}$ in standard configuration with $s = 2r$, due to $\sigma_1 \cdots \sigma_r \sigma_r^{-1} \cdots \sigma_1^{-1} = 1$ there exists a continuous epimorphism

$$\psi : \text{Gal}(\mathbf{M}_{\mathbb{S}}/\mathbb{C}(\mathcal{X})) \rightarrow G \quad \text{with} \quad \psi(\gamma_i) = \begin{cases} \sigma_i & \text{for } i = 1, \dots, r, \\ \sigma_{2r+1-i}^{-1} & \text{for } i = r+1, \dots, 2r. \end{cases}$$

Since moreover $(\sigma_1, \dots, \sigma_r, \sigma_r^{-1}, \dots, \sigma_1^{-1})^\rho = (\sigma_1, \dots, \sigma_r, \sigma_r^{-1}, \dots, \sigma_1^{-1})$ by Theorem 1.6, $\ker(\psi)$ is ρ -invariant. Hence the semidirect product $\ker(\psi) \rtimes \langle \rho \rangle$ is a normal open subgroup of $\text{Gal}(\mathbf{M}_{\mathbb{S}}/\text{IR}(\mathcal{X}))$ whose fixed field \mathbf{N} over $\text{IR}(\mathcal{X}) \cong \text{IR}(t)$ is Galois, and we have

$$\begin{aligned} \text{Gal}(\mathbf{N}/\text{IR}(\mathcal{X})) &\cong \text{Gal}(\mathbf{M}_{\mathbb{S}}/\text{IR}(\mathcal{X}))/(\ker(\psi) \rtimes \langle \rho \rangle) \\ &\cong \text{Gal}(\mathbf{M}_{\mathbb{S}}/\mathbb{C}(\mathcal{X}))/\ker(\psi) \cong G. \end{aligned}$$

Moreover IR is algebraically closed in \mathbf{N} , hence the extension $\mathbf{N}/\text{IR}(\mathcal{X})$ is geometric. \square

1.4 Generalization to Function Fields of Riemann Surfaces

The previous considerations apply to the special case of coverings of the Riemann sphere. If instead we start from an arbitrary compact Riemann surface \mathcal{X}

of genus g , then for $\mathcal{S} = \{\mathcal{P}_1, \dots, \mathcal{P}_s\} \subset \mathcal{X}$ the fundamental group of $\mathcal{X} \setminus \mathcal{S}$ with respect to a base point $\mathcal{P}_0 \in \mathcal{X} \setminus \mathcal{S}$ has the form

$$\begin{aligned} \pi_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0) = \\ \langle \alpha_1, \beta_1, \dots, \alpha_g, \beta_g, \gamma_1, \dots, \gamma_s \mid \alpha_1 \beta_1 \alpha_1^{-1} \beta_1^{-1} \cdots \alpha_g \beta_g \alpha_g^{-1} \beta_g^{-1} \gamma_1 \cdots \gamma_s = 1 \rangle. \end{aligned}$$

Following the same procedure as in Section 1.2 we then obtain the algebraic fundamental group, defined as the Galois group of the maximal field extension $M_{\mathcal{S}}/\mathbb{C}(\mathcal{X})$ unramified outside \mathcal{S} , up to an isomorphism by profinite completion

$$\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) \cong \hat{\pi}_1^{\text{top}}(\mathcal{X} \setminus \mathcal{S}; \mathcal{P}_0).$$

Via the embedding of π_1^{top} into $\hat{\pi}_1^{\text{top}}$ and the above isomorphism we can again identify the generators γ_i with generators of procyclic inertia groups of $M_{\mathcal{S}}/\mathbb{C}(\mathcal{X})$.

At least for $s \geq 1$ these more general fundamental groups are again free, hence as in Section 1.2 we obtain the solution of the inverse problem of Galois theory over all function fields of compact Riemann surfaces.

For a detailed account the reader is referred to the lecture notes Matzat (1987) and Serre (1992).

2 Arithmetic Fundamental Groups

In the previous paragraph, the structure of the fundamental group of the punctured Riemann sphere over the complex numbers was determined. With the Weil Rationality Criterion the results may be transferred to the punctured projective line $\mathbb{P}^1(\bar{\mathbb{Q}})^\circ$ over the field of all algebraic numbers $\bar{\mathbb{Q}}$. If the ramification locus is defined over \mathbb{Q} , the corresponding field extension will be invariant under the absolute Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of \mathbb{Q} . This yields a splitting group extension, called the *arithmetic fundamental group*, where the elements of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ act as outer automorphisms on the algebraic fundamental group $\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{\mathbb{Q}})^\circ)$.

2.1 Descent to Algebraically Closed Subfields

The results on the algebraic fundamental group of the punctured Riemann sphere resp. of $\mathbb{P}^1(\mathbb{C})^\circ = \mathbb{P}^1(\mathbb{C}) \setminus \mathcal{S}$ can be transferred to arbitrary algebraically closed fields \bar{k} of characteristic zero. We give the complete proof only for the case of algebraically closed subfields of \mathbb{C} . For the general case we refer the reader to Grothendieck (1971), Exp. XIII, Cor. 2.12 (see also Popp (1970), §11), or van den Dries and Ribenboim (1979).

Proposition 2.1. *Let \bar{k} be an algebraically closed subfield of \mathbb{C} , $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$, $\mathcal{X}(\bar{k}) = \mathbb{P}^1(\bar{k})$, $\mathcal{S} = \{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ a finite subset of $\mathcal{X}(\bar{k})$ and $\mathbb{S} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ the set of valuation ideals of $\bar{k}(\mathcal{X}) \cong \bar{k}(t)$ corresponding to \mathcal{S} . Then for every finite field extension $N/\mathbb{C}(t)$ unramified outside \mathbb{S} there exists precisely one function field \bar{N}/\bar{k} which is geometric over $k(t)$ and with $\bar{N}\mathbb{C} := \bar{N} \otimes_{\bar{k}} \mathbb{C} = N$.*

Proof. Let first $N/\mathbb{C}(t)$ be a finite field extension unramified outside \mathbb{S} . Further let Δ be the group of \bar{k} -automorphisms of \mathbb{C} and $\hat{\Delta}$ the group of those extensions of elements of Δ to an algebraic closure $\overline{\mathbb{C}(t)}$ of $\mathbb{C}(t)$ which fix $\bar{k}(t)$ pointwise. Then we have $\mathbb{C}^\Delta = \bar{k}$ and $\overline{\mathbb{C}(t)}^{\hat{\Delta}} = \bar{k}(t)$. For each $\hat{\delta} \in \hat{\Delta}$ the field extension $N^{\hat{\delta}}/\mathbb{C}(t)$ is unramified outside \mathbb{S} since $\mathcal{S} \subseteq \mathbb{P}^1(\bar{k})$, so it is a subfield of $M_{\mathbb{S}}$ in (1.3) of degree $[N^{\hat{\delta}} : \mathbb{C}(t)] = [N : \mathbb{C}(t)]$. We saw that the algebraic fundamental group

$$\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) = \text{Gal}(M_{\mathbb{S}}/\mathbb{C}(t))$$

is a finitely generated profinite group, so the number of normal subgroups of finite index is finite. Therefore also the set $\{N^{\hat{\delta}} \mid \hat{\delta} \in \hat{\Delta}\}$ is finite. So the stabilizer

$$\tilde{\Delta} := \{\hat{\delta} \in \hat{\Delta} \mid N^{\hat{\delta}} = N\}$$

of N in $\hat{\Delta}$ has finite index in $\hat{\Delta}$ and $\mathbb{C}(t)^{\tilde{\Delta}}/\bar{k}(t)$ is a finite extension of constants. Since \bar{k} was assumed to be algebraically closed we thus get $\mathbb{C}(t)^{\tilde{\Delta}} = \bar{k}(t)$ respectively $\mathbb{C}^{\tilde{\Delta}} = \bar{k}$.

Now let $a \in \mathcal{X}(\bar{k}) \setminus \mathcal{S}$, \mathfrak{P}_a the corresponding valuation ideal in $\bar{k}(t)$, $\tilde{\mathfrak{P}}_a$ an extension of \mathfrak{P}_a to \mathbf{N}/\mathbb{C} and

$$\tilde{\Delta}_a := \{\tilde{\delta} \in \tilde{\Delta} \mid \tilde{\mathfrak{P}}_a^{\tilde{\delta}} = \tilde{\mathfrak{P}}_a\}$$

the stabilizer of $\tilde{\mathfrak{P}}_a$. Since $\mathbf{N}/\mathbb{C}(t)$ is finite, the same is true for the number of extensions of \mathfrak{P}_a to \mathbf{N}/\mathbb{C} and hence also for the index $(\tilde{\Delta} : \tilde{\Delta}_a)$, which implies $\mathbb{C}^{\tilde{\Delta}_a} = \bar{k}$ as above.

By the theorem of Riemann-Roch (see Forster (1981), Thm. 16.9, for example) \mathbf{N} contains non-constant functions with a as the only pole. If m denotes the smallest occurring order of pole at a , the linear space

$$\mathcal{L}(\tilde{\mathfrak{P}}_a^m) = \{x \in \mathbf{N} \mid \text{ord}_{\tilde{\mathfrak{P}}_a}(x) \geq -m\}$$

has dimension 2 over \mathbb{C} and is generated by 1 and some $z \in \mathbf{N}$ with $\text{ord}_{\tilde{\mathfrak{P}}_a}(z) = -m$: $\mathcal{L}(\tilde{\mathfrak{P}}_a^m) = \mathbb{C} + \mathbb{C}z$. Since $\tilde{\mathfrak{P}}_a$ splits completely in $N/\mathbb{C}(t)$, the function z even has to generate $\mathbf{N}/\mathbb{C}(t)$, i.e., we have $\mathbf{N} = \mathbb{C}(t, z)$.

The completion $\hat{\mathbf{N}}_a$ of \mathbf{N} with respect to $\tilde{\mathfrak{P}}_a$ coincides with the completion of $\mathbb{C}(t)$ with respect to the numerator divisor of $(t-a)$, hence equals the field of formal power series $\hat{\mathbf{N}}_a = \mathbb{C}((t-a))$. In particular every $x \in \mathcal{L}(\tilde{\mathfrak{P}}_a^m)$ can be written in the form

$$x = \sum_{i \geq -m} a_i (t-a)^i \quad \text{with } a_i \in \mathbb{C}$$

in $\hat{\mathbf{N}}_a$. Replacing z by a suitable multiple and subtracting a constant we may assume without loss of generality that $a_{-m} = 1$ and $a_0 = 0$ in the above representation for z . The map

$$\lambda : \mathcal{L}(\tilde{\mathfrak{P}}_a^m) \rightarrow \mathbb{C}[X]_m, \quad x \mapsto \sum_{i=0}^m a_{-i} X^i,$$

on the \mathbb{C} -vector space of polynomials of degree at most m is \mathbb{C} -linear, $\tilde{\Delta}_a$ -equivariant and also injective, since \mathbf{N} contains no non-constant functions without poles. Thus every $\tilde{\delta} \in \tilde{\Delta}_a$ satisfies

$$\lambda(z^{\tilde{\delta}}) = X^m + \sum_{i=1}^{m-1} a_{-i}^{\tilde{\delta}} X^i.$$

But we have $z^{\tilde{\delta}} \in \mathcal{L}(\tilde{\mathfrak{P}}_a^m)$, so there exist constants $b, c \in \mathbb{C}$ with $z^{\tilde{\delta}} = bz + c$. Comparison of coefficients yields $a_i^{\tilde{\delta}} = a_i$ for $-m < i < 0$ and hence $z^{\tilde{\delta}} = z$. Consequently z is a $\tilde{\Delta}_a$ -invariant generator of $\mathbf{N}/\mathbb{C}(t)$. But then the coefficients of the minimal polynomial of z over $\mathbb{C}(t)$ must be $\tilde{\Delta}_a$ -invariant, so by the above already lie inside $\bar{k}(t)$. Thus $\bar{k}(t, z)/\bar{k}(t)$ is an extension of degree

$$[\bar{k}(t, z) : \bar{k}(t)] = [\mathbf{N} : \mathbb{C}(t)] \quad \text{with } \mathbb{C}(t, z) = \mathbf{N}$$

and hence geometric over $\bar{k}(t)$. This proves the existence of $\bar{N} := \bar{k}(t, z)$.

Now let $\bar{N}_1 \neq \bar{N}_2$ be two fields geometric over $\bar{k}(t)$ with $\mathbb{C}\bar{N}_1 = \mathbb{C}\bar{N}_2 = N$. Since \bar{N}_1 and $\mathbb{C}(t)$ are linearly disjoint over $\bar{k}(t)$ the composite $\bar{N}_1\bar{N}_2$ inside $\mathbb{C}(t)$ satisfies

$$[\bar{N}_1\bar{N}_2 : \bar{k}(t)] > [\bar{N}_1 : \bar{k}(t)] = [N : \mathbb{C}(t)] = [\mathbb{C}\bar{N}_1\bar{N}_2 : \mathbb{C}(t)],$$

contrary to the fact that a minimal polynomial for a primitive element of $\bar{N}_1\bar{N}_2/\bar{k}(t)$ remains irreducible over $\mathbb{C}(t)$. This shows the uniqueness of \bar{N} . \square

The above Proposition 2.1 contains the main ingredient for the following generalization of Theorems 1.3 and 1.4 for algebraic fundamental groups over algebraically closed subfields of \mathbb{C} .

Theorem 2.2 (Grothendieck (1971)). *Let \bar{k} be an algebraically closed subfield of \mathbb{C} , $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$, $\mathcal{X}(\bar{k}) = \mathbb{P}^1(\bar{k})$, $\mathcal{S} = \{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ a finite subset of $\mathcal{X}(\bar{k})$, $\mathbb{S} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ the set of valuation ideals of $\bar{k}(\mathcal{X})$ corresponding to \mathcal{S} , and $\bar{M}_{\mathbb{S}}$ the maximal algebraic extension field of $\bar{k}(\mathcal{X}) \cong \bar{k}(t)$ unramified outside \mathbb{S} . Then the algebraic fundamental group $\pi_1^{\text{alg}}(\mathcal{X}(\bar{k}) \setminus \mathcal{S}) = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{k}(\mathcal{X}))$ has the form*

$$\pi_1^{\text{alg}}(\mathcal{X}(\bar{k}) \setminus \mathcal{S}) = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle. \quad (2.1)$$

Moreover the elements γ_i , $i = 1, \dots, s$, are generators of inertia groups of valuation ideals $\hat{\mathfrak{P}}_i$ of $\bar{M}_{\mathbb{S}}/\bar{k}$ lying over \mathfrak{P}_i :

$$I(\hat{\mathfrak{P}}_i/\mathfrak{P}_i) = \langle \gamma_i \rangle. \quad (2.2)$$

Proof. Denote by $\bar{N}_{\mathbb{S}}$ ($N_{\mathbb{S}}$ respectively) the set of finite Galois extensions of $\bar{K} := \bar{k}(\mathcal{X})$ (resp. $K := \mathbb{C}(\mathcal{X})$) unramified outside \mathbb{S} . By Proposition 2.1 the map

$$\nu : \bar{N}_{\mathbb{S}} \rightarrow N_{\mathbb{S}}, \quad \bar{N} \mapsto N := \mathbb{C}\bar{N}$$

is bijective. As in addition the intersection and the composition of fields does not lead outside $\bar{N}_{\mathbb{S}}$, ν is an isomorphism of lattices.

The map ν commutes with the canonical epimorphisms of the projective systems $(\text{Gal}(\bar{N}/\bar{K}))_{\bar{N} \in \bar{N}_{\mathbb{S}}}$ and $(\text{Gal}(N/K))_{N \in N_{\mathbb{S}}}$, so the corresponding projective limits are isomorphic:

$$\text{Gal}(\bar{M}_{\mathbb{S}}/\bar{K}) = \varprojlim (\text{Gal}(\bar{N}/\bar{K}))_{\bar{N} \in \bar{N}_{\mathbb{S}}} \cong \varprojlim (\text{Gal}(N/K))_{N \in N_{\mathbb{S}}} = \text{Gal}(\bar{M}_{\mathbb{S}}/K).$$

This completes the proof of the first part.

For $\mathfrak{P} \in \mathbb{S}$ denote by $\hat{\mathfrak{P}}$ the unique extension to K and by $\hat{\mathfrak{P}}_K$ the extension to $M_{\mathbb{S}}$ constructed according to Theorem 1.4. The inertia group of $\hat{\mathfrak{P}} := \hat{\mathfrak{P}}_K|_{\bar{M}_{\mathbb{S}}}$ over \mathfrak{P} consists of the restrictions of all elements in $I(\hat{\mathfrak{P}}_K/\mathfrak{P}_K)$ to $\bar{M}_{\mathbb{S}}$, and we obviously have

$$I(\hat{\mathfrak{P}}/\mathfrak{P}) \cong I(\hat{\mathfrak{P}}_K/\mathfrak{P}_K).$$

This yields the second part of the assertion. \square

Remark. Let \bar{k}^ρ denote the fixed field under complex conjugation of the field $\bar{k} \leq \mathbb{C}$ in Theorem 2.2. Then if $\mathcal{S}^\rho = \mathcal{S}$, we have

$$\mathrm{Gal}(\bar{M}_{\mathbf{S}}/\bar{k}^\rho(\mathcal{X})) \cong \mathrm{Gal}(\bar{M}_{\mathbf{S}}/\bar{k}(\mathcal{X})) \rtimes \langle \rho \rangle \quad \text{with} \quad \rho^2 = 1. \quad (2.3)$$

If moreover the ramification points are arranged in the standard configuration then ρ acts on the generators γ_i of $\mathrm{Gal}(\bar{M}_{\mathbf{S}}/\bar{k}(\mathcal{X}))$ as described by formula (1.10).

The above Theorem and the subsequent Remark lead to the following:

Corollary 2.3. *Every finite group occurs as a geometric Galois group over $\bar{\mathbb{Q}}(t)$ and over $\bar{\mathbb{Q}}^\rho(t)$.*

In particular the inverse Galois problem is solved in the affirmative over all rational function fields $\bar{k}(t)$ with algebraically closed field of constants \bar{k} of characteristic zero.

2.2 The Fundamental Splitting Sequence

From now on and for the rest of this chapter we will always take \bar{k} to be the field of all algebraic numbers $\bar{\mathbb{Q}}$, since this is one of the most interesting cases. In later chapters, more general base fields will also be studied. Denote the corresponding algebraic fundamental group by

$$\Gamma_s := \mathrm{Gal}(\bar{M}_{\mathbf{S}}/\bar{\mathbb{Q}}(\mathcal{X})) = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle. \quad (2.4)$$

Theorem 2.4 (Splitting Theorem). *If the field \bar{k} in Theorem 2.2 is taken to be the field $\bar{\mathbb{Q}}$ of all algebraic numbers, and the set \mathbf{S} is invariant under the absolute Galois group $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of \mathbb{Q} , then $\bar{M}_{\mathbf{S}}$ is Galois over $\mathbb{Q}(\mathcal{X}) \cong \mathbb{Q}(t)$ and we have*

$$\mathrm{Gal}(\bar{M}_{\mathbf{S}}/\mathbb{Q}(t)) \cong \Gamma_s \rtimes \Gamma_{\mathbb{Q}}. \quad (2.5)$$

Proof. Obviously $\bar{M}_{\mathbf{S}}$ is separable and algebraic over $\mathbb{Q}(t)$. By assumption each monomorphism φ from $\bar{M}_{\mathbf{S}}$ into an algebraic closure $\hat{M}_{\mathbf{S}}$ of $\bar{M}_{\mathbf{S}}$ permutes the elements of \mathbf{S} , and as $\bar{M}_{\mathbf{S}}$ is uniquely determined inside $\hat{M}_{\mathbf{S}}$ as the maximal algebraic extension field of $\bar{\mathbb{Q}}(t)$ unramified outside \mathbf{S} , we clearly have $\bar{M}_{\mathbf{S}}^\varphi = \bar{M}_{\mathbf{S}}$ for all such φ . Hence φ is an automorphism of $\bar{M}_{\mathbf{S}}/\mathbb{Q}(t)$, and $\bar{M}_{\mathbf{S}}/\mathbb{Q}(t)$ is Galois, with group $\Gamma := \mathrm{Gal}(\bar{M}_{\mathbf{S}}/\mathbb{Q}(t))$.

Now let $\mathfrak{P} \in \mathrm{IP}(\mathbb{Q}(t)/\mathbb{Q})$ denote a prime divisor of degree one whose extension $\hat{\mathfrak{P}}$ to $\bar{M}_{\mathbf{S}}$ remains unramified, and denote by $\Gamma_D(\hat{\mathfrak{P}}/\mathfrak{P})$ the (profinite) decomposition group of $\hat{\mathfrak{P}}/\mathfrak{P}$ in Γ (for this, see Nagata (1977), Ch. 7.3). As $\hat{\mathfrak{P}}/\mathfrak{P}$ stays inert in $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$ and splits completely in $\bar{M}_{\mathbf{S}}/\bar{\mathbb{Q}}(t)$, $\Gamma_D(\hat{\mathfrak{P}}/\mathfrak{P})$ intersects Γ_s trivially, and $\Gamma_D(\hat{\mathfrak{P}}/\mathfrak{P})$ together with Γ_s generate the full group Γ . Since $\Gamma_s \triangleleft \Gamma$ and $\Gamma_D(\hat{\mathfrak{P}}/\mathfrak{P}) \cong \Gamma_{\mathbb{Q}}$ the assertion now follows. \square

The previous proof also yields an explicit description of complements in the semidirect product (2.5):

Corollary 2.5. *The decomposition groups of unramified prime divisors of degree one are closed complements to $\text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t))$ in $\text{Gal}(\bar{M}_{\mathbb{S}}/\mathbb{Q}(t))$.*

A generalization of Theorem 2.4 to arbitrary *disclosed function fields of one variable* (i.e., function fields of one variable containing a prime divisor of degree 1) over fields of characteristic zero is proved in Matzat (1987), I.§5, Satz 1.

2.3 The Action via the Cyclotomic Character

Unfortunately only very little is known about the action of $\Gamma_{\mathbb{Q}}$ on Γ_s in the sequence (2.5) for $\text{Gal}(\bar{M}_{\mathbb{S}}/\mathbb{Q}(t))$. An explicit knowledge of this action would provide an answer to the inverse problem of Galois theory. (An implicit description follows from the work of Ihara, see for example Ihara (1991), §3.) But at least the conjugacy classes of the images of the generators γ_i of Γ_s can be determined.

Clearly any $\delta \in \Gamma_{\mathbb{Q}}$ sends the n -th root of unity $\zeta_n := e^{2\pi i/n}$ to a primitive power $\zeta_n^{c_n(\delta)}$, with $c_n(\delta) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. This defines a continuous homomorphism

$$c : \Gamma_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}^{\times}, \quad \delta \mapsto c(\delta) := (c_n(\delta))_{n \in \mathbb{N}} \quad (2.6)$$

from $\Gamma_{\mathbb{Q}}$ onto the group of units in the Prüfer ring $\hat{\mathbb{Z}}$ (the profinite completion of \mathbb{Z}). This homomorphism is called the *cyclotomic character* of $\Gamma_{\mathbb{Q}}$. By the Theorem of Kronecker and Weber (see for example Washington (1982), Thm. 14.1), the maximal abelian extension field \mathbb{Q}^{ab} of \mathbb{Q} is generated by the roots of unity. Correspondingly the cyclotomic character induces a canonical isomorphism from the commutator factor group $\Gamma_{\mathbb{Q}}^{\text{ab}}$ onto $\hat{\mathbb{Z}}^{\times}$:

$$\Gamma_{\mathbb{Q}}^{\text{ab}} = \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^{\times}.$$

If we assume that, as in Theorem 2.4, the set \mathbb{S} of prime ideals ramified in $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ is invariant under $\text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)) \cong \Gamma_{\mathbb{Q}}$, then the elements $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ of \mathbb{S} are permuted by $\Gamma_{\mathbb{Q}}$ in the form

$$\delta : \mathbb{S} \longrightarrow \mathbb{S}, \quad \mathfrak{P}_i \mapsto \mathfrak{P}_{(i)\delta} := \mathfrak{P}_i^{\delta}. \quad (2.7)$$

This induces a permutation representation of $\Gamma_{\mathbb{Q}}$ on \mathbb{S} , and hence into the symmetric group S_s .

Theorem 2.6. *Let $\bar{\Delta} \cong \Gamma_{\mathbb{Q}}$ be a closed complement to*

$$\Gamma_s = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle$$

in $\text{Gal}(\bar{M}_{\mathbf{S}}/\mathbb{Q}(t))$ as in Theorem 2.4, and $\bar{\delta} \in \bar{\Delta}$ a lifting of an element $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ to $\bar{M}_{\mathbf{S}}$. Then $\gamma_i^{\bar{\delta}}$ is conjugate in Γ_s to $\gamma_{(i)\delta}^{c(\delta)}$, so the conjugacy class in Γ_s is given by

$$[\gamma_i^{\bar{\delta}}] = [\gamma_{(i)\delta}^{c(\delta)}]. \quad (2.8)$$

Proof. By Theorem 2.2 the γ_i generate inertia subgroups of prime ideals $\hat{\mathfrak{P}}_i$ of $\bar{M}_{\mathbf{S}}$ lying over $\mathfrak{P}_i \in \mathbf{S}$, so we have $I(\hat{\mathfrak{P}}_i/\mathfrak{P}_i) = \langle \gamma_i \rangle$. The extension $\bar{\delta} \in \bar{\Delta}$ of $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ maps $\langle \gamma_i \rangle$ to $\langle \gamma_i^{\bar{\delta}} \rangle$. Now this is the inertia group of $\hat{\mathfrak{P}}_i^{\bar{\delta}}/\mathfrak{P}_i^{\delta}$, and we have $\mathfrak{P}_i^{\delta} = \mathfrak{P}_{(i)\delta}$, so $\gamma_i^{\bar{\delta}}$ is conjugate in Γ_s to a power of $\gamma_{(i)\delta}$, i.e., there exists $d_i(\bar{\delta}) \in \hat{\mathbb{Z}}^\times$ with $[\gamma_i^{\bar{\delta}}] = [\gamma_{(i)\delta}^{d_i(\bar{\delta})}]$. The commutator factor group Γ_s^{ab} is a free abelian profinite group of rank $s-1$ with the two relations $\bar{\gamma}_1 \cdots \bar{\gamma}_s = 1$ and $\bar{\gamma}_1^{d_1(\bar{\delta})} \cdots \bar{\gamma}_s^{d_s(\bar{\delta})} = 1$ for the classes $\bar{\gamma}_i$ of γ_i in Γ_s^{ab} . Hence the $d_i(\bar{\delta})$ coincide for all $i = 1, \dots, s$, and do not depend on the particular choice of extension $\bar{\delta}$ of δ . So

$$d : \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)) \rightarrow \hat{\mathbb{Z}}^\times, \quad \delta \mapsto d(\delta) := d_i(\bar{\delta})$$

is a well defined homomorphism.

For the determination of d we assume that \mathbf{S} contains at least two $\text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ -invariant prime divisors, say $\mathfrak{P}_1, \mathfrak{P}_s$. This can always be guaranteed by enlarging \mathbf{S} . The fixed field $\bar{K}_{\mathbf{S}}^{\text{ab}}$ of Γ_s^{ab} is the maximal abelian extension of \bar{K} unramified outside \mathbf{S} , hence generated by the union of all roots of functions $t_i \in \bar{K}$ with divisor $(t_i) = \mathfrak{P}_i \mathfrak{P}_s^{-1}$ for $i = 1, \dots, s-1$, where by the choice of \mathfrak{P}_1 and \mathfrak{P}_s we may assume $t_1 = t$. Then the fixed field of $\langle \bar{\gamma}_2, \dots, \bar{\gamma}_{s-1} \rangle$ is obtained as

$$\bar{L} := \bigcup_{n \in \mathbb{N}} \bar{K}(z_n) \quad \text{for } z_n \in \hat{K} \text{ with } (z_n)^n = t,$$

where in addition we can require that $(z_{nm})^m = z_n$, for all $n, m \in \mathbb{N}$. In particular with this choice δ possesses an extension $\bar{\delta}$ onto \bar{L} satisfying $z_n^{\bar{\delta}} = z_n$ for all $n \in \mathbb{N}$. The field \bar{L} is $\bar{\gamma} := \bar{\gamma}_1$ -invariant, so the same is true for $\bar{K}(z_n)$, and there exists a primitive n -th root of unity $\tilde{\zeta}_n \in \bar{\mathbb{Q}}$ with $z_n^{\bar{\gamma}} = \tilde{\zeta}_n z_n$. Moreover we have

$$\tilde{\zeta}_n^{c(\delta)} = \tilde{\zeta}_n^{\bar{\delta}} = \frac{z_n^{\bar{\gamma}\bar{\delta}}}{z_n^{\bar{\delta}}} = \frac{(z_n^{\bar{\delta}})^{\bar{\gamma}^{d(\delta)}}}{z_n^{\bar{\delta}}} = \frac{\tilde{\zeta}_n^{d(\delta)} z_n}{z_n} = \tilde{\zeta}_n^{d(\delta)},$$

from which it follows that d coincides with the cyclotomic character. \square

This has the following consequence:

Corollary 2.7. *The action of $\Gamma_{\mathbb{Q}}$ on the commutator factor group Γ_s^{ab} of Γ_s is entirely given in terms of the action through the cyclotomic character c , by the formula*

$$(\bar{\gamma}_1, \dots, \bar{\gamma}_s)^{\delta} = (\bar{\gamma}_{(1)\delta}^{c(\delta)}, \dots, \bar{\gamma}_{(s)\delta}^{c(\delta)}). \quad (2.9)$$

2.4 The Theorem of Belyi

The aim of this section is to show that each $\delta \in \Gamma_{\mathbb{Q}}$ acts as an outer automorphism on the algebraic fundamental group Γ_s . This leads in particular to a representation of the absolute Galois group $\Gamma_{\mathbb{Q}}$ into the group of outer automorphisms of the free profinite group Γ_s .

Proposition 2.8. *Let $\bar{L}/\bar{\mathbb{Q}}$ be an algebraic function field in one variable. Then there exists a function $t \in \bar{L}$ such that at most the support of t and $t - 1$ is ramified in $\bar{L}/\bar{\mathbb{Q}}(t)$.*

Proof. First let $x \in \bar{L}$ be an arbitrary function. Then only finitely many prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_s \in \text{IP}(\bar{\mathbb{Q}}(x)/\bar{\mathbb{Q}})$ are ramified in $\bar{L}/\bar{\mathbb{Q}}(x)$. As $\bar{\mathbb{Q}}$ is algebraically closed, there exists a canonical bijective map from $\mathbb{P}^1(\bar{\mathbb{Q}})$ onto $\text{IP}(\bar{\mathbb{Q}}(x)/\bar{\mathbb{Q}})$, which sends $a \in \bar{\mathbb{Q}}$ to the numerator divisor of $x - a$, and ∞ to the denominator divisor of x . Denote the preimage of $\{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ under this bijection by $\mathcal{S}(x) = \{a_1, \dots, a_s\}$. We first show that there exists a function $y \in \bar{\mathbb{Q}}(x)$ such that the prime divisors of $\bar{\mathbb{Q}}(y)$ ramified in $\bar{L}/\bar{\mathbb{Q}}(y)$ are defined over $\mathbb{Q}(y)$, i.e., such that $\mathcal{S}(y)$ is a subset of $\mathbb{P}^1(\mathbb{Q})$. For this, let

$$d(x) := \max\{[\mathbb{Q}(a) : \mathbb{Q}] \mid a \in \mathcal{S}(x)\}$$

and

$$r(x) := |\{a \in \mathcal{S}(x) \mid [\mathbb{Q}(a) : \mathbb{Q}] = d(x)\}|.$$

If $d(x) = 1$ there is nothing to prove. For $d(x) > 1$ we choose $a^* \in \mathcal{S}(x)$ with $[\mathbb{Q}(a^*) : \mathbb{Q}] = d(x)$. Denote the minimal polynomial of a^* over \mathbb{Q} by $f(X)$, and let $\tilde{x} := f(x)$. Then we obviously have

$$\mathcal{S}(\tilde{x}) \subseteq \{f(a) \mid a \in \mathcal{S}(x)\} \cup \{f(a) \mid f'(a) = 0\} \cup \{\infty\}.$$

For all $a \in \bar{\mathbb{Q}}$ we have the estimate

$$[\mathbb{Q}(f(a)) : \mathbb{Q}] \leq [\mathbb{Q}(a) : \mathbb{Q}] \leq d(x)$$

for the degree $[\mathbb{Q}(f(a)) : \mathbb{Q}]$, and for the zeroes of $f'(X)$ the even better estimate

$$[\mathbb{Q}(f(a)) : \mathbb{Q}] \leq \deg(f') < d(x) \quad \text{for } a \in \bar{\mathbb{Q}} \text{ with } f'(a) = 0$$

holds. So $d(\tilde{x}) \leq d(x)$, and if $d(\tilde{x}) = d(x)$ then $r(\tilde{x}) < r(x)$. By induction in descending lexicographical order for the pair $(d(x), r(x))$ the existence of the required function $y \in \bar{\mathbb{Q}}(x)$ with $\mathcal{S}(y) \subset \mathbb{P}^1(\mathbb{Q})$ follows.

In the second step we reduce the cardinality of $\mathcal{S}(y)$. Since $\text{Aut}(\bar{\mathbb{Q}}(y)/\bar{\mathbb{Q}}) \cong \text{PGL}_2(\bar{\mathbb{Q}})$ acts threefold transitively on $\text{IP}(\bar{\mathbb{Q}}(y)/\bar{\mathbb{Q}})$, the assertion follows immediately from the first step in the case of $|\mathcal{S}(y)| \leq 3$. Otherwise we have $\mathcal{S}(y) \supseteq \{b_1, b_2, b_3, b_4\}$. By the threefold transitivity there exists $\psi \in \text{PGL}_2(\bar{\mathbb{Q}})$ with $\psi(b_1) = \infty, \psi(b_2) = 0, \psi(b_3) = 1$. Then ψ already belongs to $\text{PGL}_2(\mathbb{Q})$. Permutation of b_1, b_2 and b_3 allows to assume that $0 < \psi(b_4) < 1$. Indeed, the transposition (12) leads

to the transformation $\psi(b_4) \mapsto \psi(b_4)^{-1}$, and (23) leads to $\psi(b_4) \mapsto 1 - \psi(b_4)$. Hence there exist positive integers n, m with $\psi(b_4) = n/(n+m)$. Defining

$$g(Y) := \frac{(n+m)^{n+m}}{n^n m^m} Y^n (1-Y)^m$$

we have $g(\psi(b_i)) \in \{0, 1, \infty\}$ for $1 \leq i \leq 4$. But as

$$g'(Y) = \frac{(n+m)^{n+m+1}}{n^n m^m} Y^{n-1} (1-Y)^{m-1} \left(\frac{n}{n+m} - Y \right)$$

it follows that also $g(b) \in \{0, 1, \infty\}$ for all zeroes b of $g'(Y)$. With $\tilde{y} := g(\psi(y))$ we thus find $\mathcal{S}(\tilde{y}) \subset \mathbb{P}^1(\mathbb{Q})$, and by an argument as above $|\mathcal{S}(\tilde{y})| < |\mathcal{S}(y)|$. Consequently, descending induction on $|\mathcal{S}(y)|$ yields a function $t \in \bar{\mathbb{Q}}(y)$ with $\mathcal{S}(t) \subseteq \{0, 1, \infty\}$. \square

Remark. When replacing the function t by $4t(1-t)$ we obtain an extension ramified in three points, with one of the ramification orders equal to 2. Such functions are called *clean Belyi functions* (see Shabat and Voevodsky (1990), 0.2.2).

Proposition 2.8 allows the following characterization of algebraic function fields definable over $\bar{\mathbb{Q}}$:

Theorem 2.9 (Belyi (1979)). *An algebraic function field in one variable L/k of characteristic zero possesses a nonsingular model over $\bar{\mathbb{Q}}$ if and only if L contains a rational subfield $k(t)$ such that no more than three prime divisors in $\mathbb{P}(k(t)/k)$ ramify in $L/k(t)$.*

Proof. If L/k has a model (i.e., a defining equation) over $\bar{\mathbb{Q}}$, then the existence of $k(t) \leq L$ with $|\mathcal{S}(t)| \leq 3$ follows directly from Proposition 2.8. For the proof of the reverse direction we may assume that k is algebraically closed and that $\mathcal{S}(t)$ is contained in $\{0, 1, \infty\}$. A model of L/k involves only finitely many coefficients, so we may further assume that the transcendence degree of $k/\bar{\mathbb{Q}}$ is finite. Hence k may be identified with an algebraically closed subfield of the complex numbers \mathbb{C} . Then the field $\mathbb{C}L$ obtained by extension of constants is a subfield of the maximal algebraic extension $M_s/\mathbb{C}(t)$ unramified outside the support of $t, t-1$. By the Theorem 2.2 of Grothendieck (with $\bar{k} = \bar{\mathbb{Q}}$) $\bar{L} := \mathbb{C}L \cap \bar{M}_s$ is a geometric extension field of $\bar{\mathbb{Q}}(t)$ with $\mathbb{C}\bar{L} = \mathbb{C}L$ and $k\bar{L} = L$. Now the canonical model of $\bar{L}/\bar{\mathbb{Q}}(t)$ constitutes a nonsingular model for $L/k(t)$ with coefficients in $\bar{\mathbb{Q}}$. \square

As a second consequence of Proposition 2.8 we obtain:

Theorem 2.10 (Belyi (1979)). *The action of $\Gamma_{\mathbb{Q}}$ on Γ_s in the arithmetic fundamental group $\text{Gal}(\bar{M}_s/\mathbb{Q}(t))$ gives for $s \geq 3$ a faithful representation of $\Gamma_{\mathbb{Q}}$ into the group of (continuous) outer automorphisms of Γ_s :*

$$R_s : \Gamma_{\mathbb{Q}} \longrightarrow \text{Out}(\Gamma_s). \quad (2.10)$$

Proof. By Corollary 2.5 the representation R_s is given via the action on Γ_s of the decomposition group of a prime divisor of degree one unramified in $\bar{M}_s/\bar{\mathbb{Q}}(t)$. Now let $\tilde{k} \leq \bar{\mathbb{Q}}$ be the fixed field of $\ker(R_s)$ and denote $\tilde{\Gamma} := \text{Gal}(\bar{M}_s/\tilde{k}(t))$. As the center of Γ_s is trivial for $s \geq 3$, we have that

$$\tilde{\Gamma} = \Gamma_s \times \tilde{C},$$

where \tilde{C} denotes the centralizer in $\tilde{\Gamma}$ of Γ_s . Hence the extension of $\tilde{M} := \bar{M}_s^{\tilde{C}}$ over $\tilde{k}(t)$ is regular over \tilde{k} with Galois group isomorphic to Γ_s . The map $\tilde{L} \rightarrow \bar{\mathbb{Q}}\tilde{L}$ sending intermediate fields of $\tilde{M}/\tilde{k}(t)$ to intermediate fields of $\bar{M}_s/\bar{\mathbb{Q}}(t)$ yields an isomorphism between the lattices of intermediate fields, hence every finite subextension of $\bar{M}_s/\bar{\mathbb{Q}}(t)$ is defined by an equation with coefficients in \tilde{k} .

Given $a \in \bar{\mathbb{Q}}$, there exists an elliptic curve \mathcal{E} with invariant $j(\mathcal{E}) = a$ and Weierstraß model defined over $\mathbb{Q}(a)$ (see for example Silverman (1986), Ch. II, Prop. 1.4). As $s \geq 3$ the corresponding function field $\bar{E} := \bar{\mathbb{Q}}(\mathcal{E})$ may be interpreted by Proposition 2.8 as an intermediate field of $\bar{M}_s/\bar{\mathbb{Q}}(t)$. By the above arguments, $\bar{E}/\bar{\mathbb{Q}}(t)$ possesses a model with coefficients in \tilde{k} , which shows $a \in \tilde{k}$. This forces $\tilde{k} = \bar{\mathbb{Q}}$, and the kernel of R_s is trivial. \square

3 Fields of Definition of Galois Extensions

In this paragraph we introduce and characterize fields of definition of field extensions with additional structure of automorphisms. The resulting theorems are fundamental for the rationality criteria in this chapter and in Chapter III.

3.1 Cyclic and Projective Descent

For the moment, let \tilde{N}/\tilde{K} be an arbitrary field extension and \tilde{G} a subgroup of $\text{Aut}(\tilde{N}/\tilde{K})$. A subfield K of \tilde{K} is called a *field of definition* of \tilde{N}/\tilde{K} if there exists a field extension N/K , linearly disjoint from \tilde{K}/K , with $N\tilde{K} = \tilde{N}$. If moreover N is \tilde{G} -invariant, then K is called a *field of definition of \tilde{N}/\tilde{K} with \tilde{G}* , or of $\tilde{N}/_{\tilde{G}}\tilde{K}$ for short. In particular in the latter case $G := \tilde{G}|_N$ is a subgroup of $\text{Aut}(N/K)$ isomorphic to \tilde{G} .

With these notations we have the general result:

Proposition 3.1. *Let \tilde{N}/\tilde{K} be a Galois extension with group G and K a field of definition of \tilde{N}/\tilde{K} over which \tilde{K} is Galois. Then also \tilde{N}/K is Galois, and the Galois group satisfies*

$$\text{Gal}(\tilde{N}/K) \cong \text{Gal}(\tilde{N}/\tilde{K}) \rtimes \text{Gal}(\tilde{K}/K). \quad (3.1)$$

If K is even a field of definition of $\tilde{N}/_{\tilde{G}}\tilde{K}$, we have the stronger direct product decomposition

$$\text{Gal}(\tilde{N}/K) \cong \text{Gal}(\tilde{N}/\tilde{K}) \times \text{Gal}(\tilde{K}/K). \quad (3.2)$$

Proof. Let N/K denote the field extension linearly disjoint from \tilde{K}/K with $N\tilde{K} = \tilde{N}$, which exists by the definition. The automorphisms of \tilde{K}/K may be lifted uniquely to automorphisms of \tilde{N}/N , so \tilde{N}/N is Galois with $\text{Gal}(\tilde{N}/N) \cong \text{Gal}(\tilde{K}/K)$. By assumption the fixed field of the group $\langle \text{Gal}(\tilde{N}/\tilde{K}), \text{Gal}(\tilde{N}/N) \rangle$ coincides with K , so \tilde{N}/K is a Galois extension. As $\text{Gal}(\tilde{N}/\tilde{K}) \cap \text{Gal}(\tilde{N}/N) = 1$, the group $\text{Gal}(\tilde{N}/N)$ yields a complement of $\text{Gal}(\tilde{N}/\tilde{K})$. This proves (3.1). If moreover N/K is Galois, this complement becomes a normal subgroup in $\text{Gal}(\tilde{N}/K)$, and (3.2) follows. \square

If the field extension \tilde{K}/K is cyclic, we have the following weak converse of Proposition 3.1:

Theorem 3.2 (Dew (1992)). *Let \tilde{N}/\tilde{K} be a Galois extension with group G and K a subfield of \tilde{K} . Moreover assume that there exists a field extension K^*/\tilde{K} of degree $\exp(G)$ linearly disjoint from \tilde{N}/\tilde{K} and cyclic over K . Then for the composite $N^* := K^*\tilde{N}$ (inside an algebraic closure of \tilde{K}) and $G^* := \text{Gal}(N^*/K^*) \cong G$ we have*

(a) *If \tilde{N}/K is Galois, then K is a field of definition of N^*/K^* .*

(b) *If moreover all automorphisms of \tilde{N}/K act as inner automorphisms on G , then K is a field of definition of $N^*/_{G^*}K^*$.*

Proof. By assumption, each monomorphism from N^* into an algebraic closure of \tilde{K} fixing K maps \tilde{N} , and hence also N^* , onto itself. Consequently N^*/K is a Galois extension, with group $\Gamma := \text{Gal}(N^*/K)$. Now

$$\text{Gal}(N^*/\tilde{K}) \cong \text{Gal}(\tilde{N}/\tilde{K}) \times \text{Gal}(K^*/\tilde{K}), \quad (3.3)$$

so $\text{Gal}(N^*/\tilde{K})$ has exponent $n := \exp(G)$, and the exponent $\exp(\Gamma)$ is bounded by $m := n \cdot [\tilde{K} : K]$. Now let δ denote a generator of the cyclic group $\Delta := \text{Gal}(K^*/K) \cong Z_m$, and $\tilde{\delta}$ an extension of δ to N^* . Then $\tilde{\delta}$ has order m , and hence generates a complement $\tilde{\Delta}$ of G^* in Γ . The fixed field N of $\tilde{\Delta}$ thus yields a field extension linearly disjoint from K^*/K , satisfying $K^*N = N^*$. This proves (a).

If all elements of $\text{Gal}(\tilde{N}/K)$ act as inner automorphisms on G , the same holds for all elements of Γ in its action on G^* . Hence Γ is generated by G^* and $\mathcal{C}_\Gamma(G^*)$. The fixed field \tilde{L} of $\mathcal{C}_\Gamma(G^*)$ is an extension of K linearly disjoint from K^*/K . As $\tilde{L} \leq \tilde{N}$ by (3.3) it follows that $L := \tilde{K}\tilde{L} \leq \tilde{N}$ with $\text{Gal}(\tilde{N}/L) = \mathcal{L}(G)$. Application of (a) to the Galois extension \tilde{N}/L with subfield \tilde{L} and $L' := K^*L$ yields a complement $\tilde{\Delta}$ to $\mathcal{L}(G^*)$ in $\mathcal{C}_\Gamma(G^*)$. Hence we have $\Gamma = \tilde{\Delta} \times G^*$, the fixed field N of $\tilde{\Delta}$ is Galois over \tilde{K} with group $\text{Gal}(N/K) \cong G^*$, and we have $K^*N = N^*$, which proves (b). \square

Remark. If in the previous theorem $|G|$ and $[\tilde{K} : K]$ are prime to each other, then K is even a field of definition of \tilde{N}/\tilde{K} , $\tilde{N}/_G\tilde{K}$ respectively (since $\tilde{\delta}|_{\tilde{N}} = 1$).

In the case of congruence function fields we obtain from Theorem 3.2 the following optimal result:

Corollary 3.3. *Let $\bar{K}/\bar{\mathbb{F}}_p$ be an algebraic function field in one variable over the algebraic closure of \mathbb{F}_p , and \bar{N}/\bar{K} a finite Galois extension with group G . Then we have:*

(a) *A subfield K of \bar{K} with $\bar{\mathbb{F}}_p K = \bar{K}$ is a field of definition of \bar{N}/\bar{K} if and only if \bar{N}/K is Galois.*

(b) *This subfield is a field of definition of $\bar{N}/_G\bar{K}$ precisely if in addition all elements of $\text{Gal}(\bar{N}/K)$ act as inner automorphisms on G .*

Proof. By Proposition 3.1 it remains to prove that K is a field of definition of \bar{N}/\bar{K} (resp. $\bar{N}/_G\bar{K}$). For this, we may assume without loss of generality that K has a finite field of constants. First we note that there exists at least a field of definition \tilde{K} of $\bar{N}/_G\bar{K}$ with $[\tilde{K} : K] < \infty$. Since \tilde{K} has cyclic extensions of any finite order, we may now apply Theorem 3.2(a) (resp. (b)) to the corresponding Galois extension \tilde{N}/\tilde{K} and the subfield K , and thus obtain the assertion of the corollary. \square

Corollary 3.3 can also be regarded as a special case of the following theorem concerning descent with a projective profinite group (see Section IV.1.5 for further information):

Theorem 3.4. *Let \bar{K}/\bar{k} be an algebraic function field over a separably closed field \bar{k} and \bar{N}/\bar{K} a finite Galois extension with group G . Further let K be a subfield of*

\bar{K} with $\bar{k}K = \bar{K}$ such that $\text{Gal}(\bar{K}/K)$ is a projective profinite group. Then we have:

- (a) K is a field of definition of \bar{N}/\bar{K} if and only if \bar{N}/K is Galois.
- (b) K is a field of definition of $\bar{N}/G\bar{K}$ if and only if in addition all elements of $\text{Gal}(\bar{N}/K)$ act as inner automorphisms on G .

Proof. By Proposition 3.1 we only have to show the if parts of (a) and (b). Since \bar{N}/K is Galois with group $\Gamma := \text{Gal}(\bar{N}/K)$ and with $\Delta := \text{Gal}(\bar{K}/K)$ we get the exact sequence

$$1 \longrightarrow G \longrightarrow \Gamma \longrightarrow \Delta \longrightarrow 1. \quad (3.4)$$

By assumption Δ is a projective profinite group. Therefore (3.4) splits (see for example Fried and Jarden (1986), Remark 20.11) and G has a closed complement $\tilde{\Delta}$ inside Γ . The fixed field \tilde{N} of $\tilde{\Delta}$ is an extension of K which is regular over $k := \bar{k} \cap K$ and with $\bar{k}\tilde{N} = \bar{N}$. This proves (a).

Now assume that in addition each element of Γ acts as inner automorphism on G . Then the fixed field L of the centralizer $\mathcal{C}_\Gamma(G)$ is an extension of K regular over k . Further $\bar{L} := \bar{k}L \leq \bar{N}$ is a subfield of \bar{N} with $\text{Gal}(\bar{N}/\bar{L}) = \mathcal{Z}(G)$. Application of (a) to the Galois extension \bar{N}/\bar{L} and with the subfield L yields a closed complement $\tilde{\Delta}$ of $\mathcal{Z}(G)$ inside $\mathcal{C}_\Gamma(G)$. Hence we have $\Gamma = \tilde{\Delta} \times G$, and the fixed field N of $\tilde{\Delta}$ is Galois over K with group $\text{Gal}(N/K) \cong G$ and satisfies $\bar{k}N = \bar{N}$, proving (b). \square

Remark. The proof of Theorem 3.4 shows that more generally in the case that Γ acts by inner automorphisms on G the obstruction for K to be a field of definition of $\bar{N}/G\bar{K}$ lies inside the cohomology group $H^2(\Delta, \mathcal{Z}(G))$ with trivial action of Δ on $\mathcal{Z}(G)$ (compare also Belyi (1979)).

3.2 Fields of Definition of Geometric Field Extensions

Optimal results as in Theorem 3.4 are not available in general. We therefore first study fields of definition of geometric Galois extensions while neglecting the Galois group.

Theorem 3.5. *Let \bar{K}/\bar{k} be an algebraic function field in one variable with algebraically closed field of constants of characteristic zero, and \bar{N}/\bar{K} a finite Galois extension. Then a disclosed subfield K of \bar{K} with $\bar{k}K = \bar{K}$ is a field of definition for \bar{N}/\bar{K} if and only if \bar{N}/K is Galois.*

Proof. By Proposition 3.1 it remains to prove that a disclosed subfield K of \bar{K} with field of constants k , over which \bar{N} is Galois, is a field of definition for \bar{N}/\bar{K} . By assumption there exists a prime divisor $\mathfrak{P} \in \mathbb{P}(K/k)$ of degree one. For an arbitrary extension $\bar{\mathfrak{P}} \in \mathbb{P}(\bar{N}/\bar{k})$ let \bar{L} denote the inertia field of $\bar{\mathfrak{P}}/\mathfrak{P}$ containing \bar{K} , and $\bar{\mathfrak{Q}} := \bar{\mathfrak{P}}|_{\bar{L}}$. As $\bar{\mathfrak{Q}}/\mathfrak{P}$ is unramified, each prime element $z \in K$ for \mathfrak{P} is also a prime element for $\bar{\mathfrak{Q}}$ in \bar{L} . Consequently the field of formal power series $\bar{k}((z))$ gives the completion of \bar{L} with respect to $\bar{\mathfrak{Q}}$. Denote by e the ramification index of $\bar{\mathfrak{P}}/\bar{\mathfrak{Q}}$

(hence of $\bar{\mathfrak{P}}/\mathfrak{P}$). Then the completion of \bar{N} with respect to $\bar{\mathfrak{P}}$ is obtained as $\bar{k}((y))$ with $y^e = z$. The automorphisms δ in

$$\Delta := \text{Gal}(\bar{K}/K) \cong \text{Gal}(\bar{k}/k)$$

act on the formal power series $f(z) \in \bar{k}[[z]]$ via the coefficients. Hence among the extensions of δ to $\bar{k}((y))$ there exists precisely one, which we call $\hat{\delta}$, satisfying $y^{\hat{\delta}} = y$. The set of restrictions to \bar{N} of these automorphisms

$$\tilde{\Delta} := \{\tilde{\delta} \mid \tilde{\delta} := \hat{\delta}|_{\bar{N}}, \delta \in \Delta\}$$

is a closed subgroup of $\text{Gal}(\bar{N}/K)$ isomorphic to Δ , which moreover forms a complement to $\text{Gal}(\bar{N}/\bar{K})$. Hence the fixed field N of $\tilde{\Delta}$ is a geometric extension field of K with $\bar{K}N = \bar{N}$. We conclude that K is a field of definition of \bar{N}/\bar{K} . \square

Remark. The complement $\tilde{\Delta}$ constructed in the proof is obviously contained in the decomposition group of $\bar{\mathfrak{P}}/\mathfrak{P}$ and it coincides with it in the case that $\bar{\mathfrak{P}}/\mathfrak{P}$ is unramified. The proof shows that in the latter case the assumption of characteristic zero is superfluous.

The theorem has the following immediate consequence:

Corollary 3.6. *If Ψ is a characteristic open subgroup of the Galois group $\Gamma_s = \text{Gal}(\bar{M}_s/\bar{\mathbb{Q}}(t))$ in (2.5), and \bar{N} denotes its fixed field, then $\bar{N}/\bar{\mathbb{Q}}(t)$ is already defined over $\mathbb{Q}(t)$.*

Proof. By the Splitting Theorem 2.4 each $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ may be lifted uniquely to an automorphism $\bar{\delta} \in \text{Gal}(\bar{M}_s/\mathbb{Q}(t))$ in a given complement of Γ_s . As $\Psi^{\bar{\delta}} = \Psi$, $\bar{\delta}$ induces an automorphism $\tilde{\delta}$ of $\bar{N}/\mathbb{Q}(t)$ extending δ , and different extensions of δ to \bar{N} differ only by an automorphism of $\bar{N}/\bar{\mathbb{Q}}(t)$. Hence $\bar{N}/\mathbb{Q}(t)$ is Galois, and the assertion follows immediately from Theorem 3.5. \square

Example 3.1. If in the previous corollary we have $s = 2$, then $\Gamma_2 \cong \hat{\mathbb{Z}}$ is procyclic, and each normal subgroup of Γ_2 is characteristic. In particular for the subfields \bar{N} of $\bar{M}_s/\bar{\mathbb{Q}}(t)$ with $\text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t)) \cong Z_n$ (the cyclic group of order n), the extensions $\bar{N}/\bar{\mathbb{Q}}(t)$ are already defined over $\mathbb{Q}(t)$. \square

Example 3.2. If in Corollary 3.6 the number of generators satisfies $s \geq 3$, and if we take as Ψ the intersection of all kernels of homomorphisms from Γ_s onto a given finite simple group G , then we obtain: For each finite simple group G there exists an integer $n \in \mathbb{N}$ and a Galois extension $\bar{N}/\bar{\mathbb{Q}}(t)$ with $\text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t)) \cong G^n$ which is defined over $\mathbb{Q}(t)$ (not necessarily as Galois extension). \square

3.3 Fields of Definition of Geometric Galois Extensions

The general result of Theorem 3.5 has the disadvantage that the fields of definition characterized there usually do not form fields of definition for the field exten-

sion together with the Galois group. To obtain this stronger conclusion, additional assumptions have to be made, as the following proposition shows.

Proposition 3.7. *Let \bar{N}/\bar{K} be the Galois extension in Theorem 3.5 with Galois group G and (not necessarily disclosed) field of definition K . Then K is also a field of definition of $\bar{N}/_G\bar{K}$ precisely if each element of $\Gamma := \text{Gal}(\bar{N}/K)$ acts as inner automorphism on G and the center of G has a closed complement in the centralizer $\mathcal{C}_\Gamma(G)$.*

Proof. If K is a field of definition for $\bar{N}/_G\bar{K}$, then by Proposition 3.1 the group G possesses a closed complement $\tilde{\Delta}$ in Γ which acts trivially on G . This is at the same time a closed complement for the center $\mathcal{Z}(G)$ of G in $\mathcal{C}_\Gamma(G) = \tilde{\Delta} \times \mathcal{Z}(G)$.

For the proof of the other direction we first note that G together with $\mathcal{C}_\Gamma(G)$ generates all of Γ . Then a closed complement $\tilde{\Delta}$ of $\mathcal{Z}(G)$ in $\mathcal{C}_\Gamma(G)$ also is a direct complement of G in Γ , hence we have $\Gamma = \tilde{\Delta} \times G$. The fixed field N of $\tilde{\Delta}$ now yields a geometric Galois extension N/K with $\bar{K}N = \bar{N}$, and the assertion is proved. \square

Remark. The additional assumption on the complement in Proposition 3.7 will clearly always be satisfied if for example G is abelian, or if G has trivial center.

They are also guaranteed for example in the following case:

Corollary 3.8. *The field of definition K of \bar{N}/\bar{K} in Theorem 3.5 is also a field of definition of $\bar{N}/_G\bar{K}$ if each element of Γ acts as inner automorphism on G and the fixed field of $\mathcal{C}_\Gamma(G)$ is disclosed.*

Proof. Under these assumptions the fixed field L of $\mathcal{C}_\Gamma(G)$ is a disclosed geometric extension field of K . Hence by Theorem 3.5 the group $\text{Gal}(\bar{N}/\bar{k}L) = \mathcal{Z}(G)$ possesses a closed complement in $\text{Gal}(\bar{N}/L) = \mathcal{C}_\Gamma(G)$. \square

The characterizing condition for fields of definition of Galois extensions $\bar{N}/_G\bar{K}$ in Proposition 3.7 is usually quite hard to check for arbitrary groups, so we give here a sufficient condition for its occurrence.

Theorem 3.9. *Let \bar{N}/\bar{K} be the Galois extension of Theorem 3.5 with Galois group G and field of definition K . Moreover assume that each element of $\text{Gal}(\bar{N}/K)$ acts as an inner automorphism on G and that there exists a prime divisor $\mathfrak{P} \in \text{IP}(K/k)$ of degree one satisfying the following normalizer condition*

(N): *The center of G possesses a complement in the normalizer $\mathcal{N}_G(G_I)$ in G of the inertia group G_I of a prime divisor $\bar{\mathfrak{P}} \in \text{IP}(\bar{N}/\bar{k})$ above \mathfrak{P} .*

Then K is also a field of definition for $\bar{N}/_G\bar{K}$.

Proof. By the Remark following Theorem 3.5 the group G possesses a closed complement $\tilde{\Delta}$ in $\Gamma := \text{Gal}(\bar{N}/K)$ contained in the decomposition group of $\bar{\mathfrak{P}}/\mathfrak{P}$. Its fixed field \tilde{N} is a geometric extension field of K with $\bar{K}\tilde{N} = \bar{N}$. Further let

$\tilde{\Delta}^* := \tilde{\Delta} \cap \mathcal{C}_\Gamma(G)$ with fixed field \tilde{N}^* , and K^* be the fixed field of $\langle \tilde{\Delta}^*, G \rangle$. Then \tilde{N}^* is the Galois closure of \tilde{N}/K and a geometric Galois extension of K^* with group $G^* \cong G$. Moreover $H := \text{Gal}(\tilde{N}^*/K)$ is isomorphic to a subgroup of the holomorph $G \rtimes \text{Aut}(G)$ containing G .

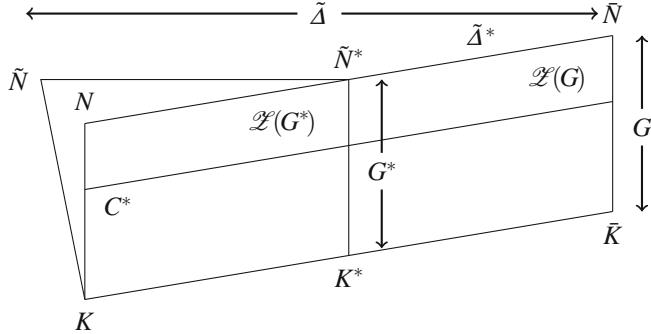


Fig. 3.1 Galois descent using (N)

By construction each element $\tilde{\delta} \in \tilde{\Delta}$ acts on G as an element from $\mathcal{N}_G(G_I)$. Hence each element of $\text{Gal}(\tilde{N}^*/\tilde{N})$ acts on G^* as an element from $\mathcal{N}_{G^*}(G_I^*) \cong \mathcal{N}_G(G_I)$. By a theorem of Jordan (see for example Zassenhaus (1958), Ch. II, §4, Thm. 5), $C^* := \mathcal{C}_H(G^*)$ is isomorphic to a subgroup U of $\mathcal{N}_G(G_I)$ containing $\mathcal{Z}(G)$. By assumption $\mathcal{N}_G(G_I)$ and hence U contains a complement to $\mathcal{Z}(G)$. Hence $\mathcal{Z}(G^*)$ also possesses a complement in C^* . The fixed field N of this complement now constitutes a geometric and Galois extension field of K with

$$\text{Gal}(N/K) \cong G \quad \text{and} \quad \bar{K}N = \tilde{N}.$$

□

If we allow a cyclotomic extension of constants, then Theorem 3.9 has the following useful variant:

Corollary 3.10. *Assume that instead of (N) the prime divisor \mathfrak{P} in Theorem 3.9 satisfies the centralizer condition*

(C): *The center of G possesses a complement in the centralizer $\mathcal{C}_G(G_I)$.*

Then there exists a finite cyclotomic extension K'/K such that K' is a field of definition for $\tilde{N}/G\tilde{K}$.

Proof. As in the proof of Theorem 3.9 let $\tilde{\Delta}$ denote a closed complement to G in $\Gamma := \text{Gal}(\tilde{N}/K)$ contained in the decomposition group of $\mathfrak{P}/\mathfrak{P}$, and \tilde{N} the corresponding fixed field. Moreover let $\tilde{\Delta}' := \tilde{\Delta} \cap \mathcal{C}_\Gamma(G_I)$, $\tilde{\Delta}^* := \tilde{\Delta} \cap \mathcal{C}_\Gamma(G)$, with \tilde{N}' , \tilde{N}^* the corresponding fixed fields, and K' , K^* be the fixed fields of $\langle \tilde{\Delta}', G \rangle$ resp. $\langle \tilde{\Delta}^*, G \rangle$. Then \tilde{N}^* is the Galois closure of \tilde{N}'/K' . Again $H := \text{Gal}(\tilde{N}^*/K')$ is isomorphic to a subgroup of the holomorph $G \rtimes \text{Aut}(G)$ containing G , and $G^* := \text{Gal}(\tilde{N}^*/K^*) \cong G$.

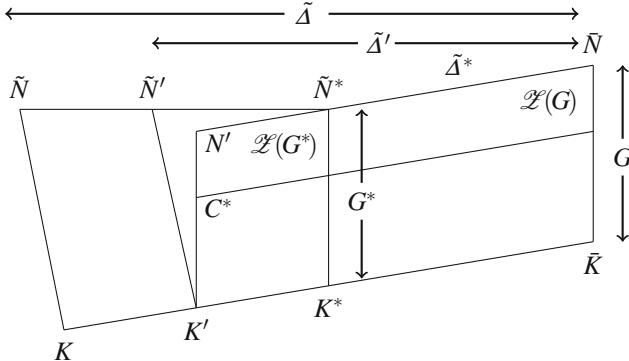


Fig. 3.2 Galois descent using (C)

Replacing now \tilde{N}/K and $\mathcal{N}_G(G_I)$ in the proof of Theorem 3.9 by \tilde{N}'/K' and $\mathcal{C}_G(G_I)$ resp., we get a geometric Galois extension field N' of K' with

$$G' := \text{Gal}(N'/K') \cong G \quad \text{and} \quad \bar{K}N' = \bar{N}.$$

By the choice of $\tilde{\Delta}$ we see that $\tilde{\Delta}/\tilde{\Delta}'$ becomes isomorphic to a subgroup of $\mathcal{N}_G(G_I)/\mathcal{C}_G(G_I)$, hence K'/K is a cyclic extension. As the group $\tilde{\Delta}$ acts on the cyclic group G_I via the cyclotomic character, we indeed have that K'/K is generated by roots of unity, which yields the conclusion. \square

Remark. Theorems 3.5 and 3.9, as well as Corollary 3.10, also hold in positive characteristic with the same proof, if only K/k possesses a prime divisor of degree one not wildly ramified in \tilde{N}/K (satisfying the condition (N) resp. (C) if appropriate).

4 The Rigidity Property

In order to detect small fields of definition for Galois extensions $\bar{N}/\bar{\mathbb{Q}}(t)$ we study here the action of the absolute Galois group of \mathbb{Q} on the subfields of $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ with prescribed Galois group. Here the Hurwitz classification of such fields proves advantageous. As the main result of the discussion we obtain the Basic Rigidity Theorem and its variant for irrational ramification points.

4.1 The Hurwitz Classification

Our starting point is the arithmetic fundamental group in (2.5)

$$\Gamma = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)) \cong \Gamma_s \rtimes \Gamma_{\mathbb{Q}},$$

where $\Gamma_s = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle$ denotes the Galois group of the maximal algebraic Galois extension $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ unramified outside \mathbb{S} , where $|\mathbb{S}| = s$. Each element $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)) \cong \Gamma_{\mathbb{Q}}$ may be lifted uniquely to an automorphism $\tilde{\delta} \in \Gamma$ inside a given closed complement of Γ_s , which then permutes the closed subgroups of Γ_s , hence by Galois correspondence also the intermediate fields of $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$. Now let Ψ be an open normal subgroup of Γ_s with fixed field \bar{N} and

$$G := \text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t)) = \Gamma_s/\Psi.$$

Then both the normal subgroup $\Psi^{\tilde{\delta}}$ and the field $\bar{N}^{\tilde{\delta}}$ are independent of the particular lifting $\tilde{\delta}$ of δ , i.e., of the given complement, and may hence be denoted by Ψ^δ , \bar{N}^δ respectively. We thus obtain

$$\bar{N}^\delta = (\bar{M}_{\mathbb{S}}^\Psi)^\delta = \bar{M}_{\mathbb{S}}^{\Psi^\delta}. \quad (4.1)$$

Now let $\sigma = (\sigma_1, \dots, \sigma_s) \in G^s$ be the image of $\gamma = (\gamma_1, \dots, \gamma_s)$ under the canonical (continuous) homomorphism $\psi : \Gamma_s \rightarrow G$. Then σ is a generating system of G satisfying the product relation $\sigma_1 \cdots \sigma_s = 1$. We call such a system a *generating s-system of G*. The set of all generating s-systems of G is denoted by

$$\Sigma_s(G) := \{\sigma \in G^s \mid \langle \sigma \rangle = G, \sigma_1 \cdots \sigma_s = 1\}. \quad (4.2)$$

For each $\sigma \in \Sigma_s(G)$ there exists precisely one (continuous) $\psi_\sigma \in \text{Hom}(\Gamma_s, G)$ with $\psi_\sigma(\gamma) = \sigma$, the kernel of which constitutes a closed subgroup of Γ_s denoted by $\ker(\sigma)$. Then we have $\ker(\sigma) = \ker(\tau)$ for two generating s-systems $\sigma, \tau \in \Sigma_s(G)$ if and only if there exists $\alpha \in \text{Aut}(G)$ such that $\sigma^\alpha = \tau$.

The set of all intermediate fields of $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ with Galois group isomorphic to G is now denoted by

$$\bar{N}_{\mathbb{S}}(G) := \{\bar{N} \mid \bar{\mathbb{Q}}(t) \leq \bar{N} \leq \bar{M}_{\mathbb{S}}, \text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t)) \cong G\}. \quad (4.3)$$

The above considerations may now be collected as follows:

Theorem 4.1 (Hurwitz Classification). *The fields $\bar{N} \in \bar{\mathbf{N}}_{\mathbf{s}}(G)$ are parameterized by the generating s -system classes $\sigma^{\text{Aut}(G)} \in \Sigma_s(G)/\text{Aut}(G)$; more precisely there exists a bijection*

$$\mathbf{N}_{\mathbf{s}} : \Sigma_s(G)/\text{Aut}(G) \longrightarrow \bar{\mathbf{N}}_{\mathbf{s}}(G), \quad \sigma^{\text{Aut}(G)} \mapsto \bar{N}_{\sigma} := \bar{M}_{\mathbf{s}}^{\ker(\sigma)}. \quad (4.4)$$

The components σ_i of the parameter σ yield generators of inertia groups of prime ideals of $\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t)$ over $\mathfrak{P}_i \in \mathbf{s}$ via

$$\varphi_{\sigma} : G \longrightarrow \text{Gal}(\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t)), \quad \sigma_i \mapsto \psi_{\sigma}^{-1}(\sigma_i) \ker(\sigma). \quad (4.5)$$

Remark. Clearly, $\mathbf{N}_{\mathbf{s}}$ may also be interpreted as a surjective map

$$\mathbf{N}_{\mathbf{s}} : \Sigma_s(G)/\text{Inn}(G) \longrightarrow \bar{\mathbf{N}}_{\mathbf{s}}(G), \quad [\sigma] := \sigma^{\text{Inn}(G)} \mapsto \bar{N}_{\sigma}. \quad (4.6)$$

The group $\Gamma_{\mathbb{Q}}$ respectively more precisely each complement $\tilde{\Gamma}_{\mathbb{Q}}$ of Γ_s in Γ isomorphic to $\Gamma_{\mathbb{Q}}$ now acts on $\text{Hom}(\Gamma_s, G)$ from the right via

$$\text{Hom}(\Gamma_s, G) \times \tilde{\Gamma}_{\mathbb{Q}} \rightarrow \text{Hom}(\Gamma_s, G), \quad (\psi, \tilde{\delta}) \mapsto \psi \cdot \tilde{\delta} \text{ with } (\psi \cdot \tilde{\delta})(\gamma) = \psi(\tilde{\delta} \gamma \tilde{\delta}^{-1}). \quad (4.7)$$

With $\psi_{\sigma, \tilde{\delta}} := \psi_{\sigma} \cdot \tilde{\delta}$ this induces an action of $\tilde{\Gamma}_{\mathbb{Q}}$ on $\Sigma_s(G)$ from the right. This satisfies

$$\Sigma_s(G) \times \tilde{\Gamma}_{\mathbb{Q}} \rightarrow \Sigma_s(G), \quad (\sigma, \tilde{\delta}) \mapsto \sigma \cdot \tilde{\delta} = \sigma^{\tilde{\delta}^{-1}} \text{ with } \sigma^{\tilde{\delta}} := \psi_{\sigma}(\gamma^{\tilde{\delta}}). \quad (4.8)$$

(The definition of $\sigma^{\tilde{\delta}} := \psi_{\sigma}(\gamma^{\tilde{\delta}})$ instead of $\psi_{\sigma}(\gamma^{\tilde{\delta}^{-1}})$ allows an immediate transfer of transformation formulae from γ to σ , see for example Paragraphs 6 and 7 and Ch. III.3.) Taking into account that the image of $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ under $\tilde{\delta} \in \tilde{\Gamma}_{\mathbb{Q}}$ is independent of the particular lifting $\tilde{\delta}$ of $\delta \in \Gamma_{\mathbb{Q}}$, we thus obtain a well-defined action of $\Gamma_{\mathbb{Q}}$ on $\Sigma_s(G)/\text{Inn}(G)$:

$$\Sigma_s(G)/\text{Inn}(G) \times \Gamma_{\mathbb{Q}} \rightarrow \Sigma_s(G)/\text{Inn}(G), \quad ([\sigma], \delta) \mapsto [\sigma]^{\delta^{-1}} := [\sigma^{\tilde{\delta}^{-1}}]. \quad (4.9)$$

With these notations we may conclude:

Proposition 4.2. *With the action of $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ on $\Sigma_s(G)/\text{Inn}(G)$ defined in (4.9) we have*

$$\bar{N}_{\sigma^{\delta}} = (\bar{N}_{\sigma})^{\delta^{-1}}. \quad (4.10)$$

4.2 The Fixed Field of a Class of Generating Systems

In the action of Γ on $\Sigma_s(G)/\text{Inn}(G)$ introduced in (4.9), $\Delta := \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ acts on the classes of generating systems via the cyclotomic character. More precisely we have:

Proposition 4.3. *Let $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$, $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$, and denote by C_i , resp. C_i^δ , the conjugacy class of the i -th component of a representative in $[\sigma]$, resp. $[\sigma]^\delta$. Then we have*

$$C_i^\delta = C_{(i)\delta}^{c(\delta)}. \quad (4.11)$$

Proof. For an extension $\tilde{\delta}$ of δ onto \bar{M}_s , from (4.8) and Theorem 2.6 we have

$$C_i^\delta = [\sigma_i^{\tilde{\delta}}] = [\psi_\sigma(\gamma_i)^{\tilde{\delta}}] = [\psi_\sigma(\gamma_{(i)\delta}^{c(\delta)})] = [\sigma_{(i)\delta}^{c(\delta)}] = C_{(i)\delta}^{c(\delta)}. \quad \square$$

If we assume that the prime divisors $\mathfrak{P} \in \mathbb{S}$ are Δ -invariant, hence defined over $\mathbb{Q}(t)$, then the conjugacy classes $C_i := [\sigma_i] \in \text{Cl}(G)$ belonging to a generating s -system σ are mapped simultaneously onto the conjugacy classes of their $c(\delta)$ -th power: $C_i^\delta = C_i^{c(\delta)}$. This furnishes a transitive permutation representation of Δ on the set of primitive powers

$$\mathbf{C}^* := \{\mathbf{C}^n \mid n \in (\mathbb{Z}/|G|\mathbb{Z})^\times\} \quad (4.12)$$

of the vector $\mathbf{C} = (C_1, \dots, C_s) \in \text{Cl}(G)^s$. Hence the kernel

$$\Delta_{\mathbf{C}} := \{\delta \in \Delta \mid \mathbf{C}^{c(\delta)} = \mathbf{C}\} \quad (4.13)$$

of this permutation representation is a closed subgroup of Δ with index

$$d(\mathbf{C}) := |\mathbf{C}^*|; \quad (4.14)$$

this index will be called the *irrationality degree of \mathbf{C}* .

Proposition 4.4. *Let $\mathbf{C} = (C_1, \dots, C_s) \in \text{Cl}(G)^s$ be a class vector of G . Then the fixed field $\mathbb{Q}_{\mathbf{C}} := \bar{\mathbb{Q}}^{\Delta_{\mathbf{C}}}$ is an abelian number field of degree*

$$[\mathbb{Q}_{\mathbf{C}} : \mathbb{Q}] = d(\mathbf{C}). \quad (4.15)$$

It is generated over \mathbb{Q} by the values of the complex irreducible characters of G on the classes C_1, \dots, C_s :

$$\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\{\chi(C_i) \mid \chi \in \text{Irr}(G), i = 1, \dots, s\}). \quad (4.16)$$

Proof. Since $c(\Delta) = \hat{\mathbb{Z}}^\times$ the factor group

$$\Delta/\Delta_{\mathbf{C}} \cong \text{Gal}(\mathbb{Q}_{\mathbf{C}}/\mathbb{Q})$$

is abelian. Further, as Δ acts transitively on \mathbf{C}^* via c , we have

$$[\mathbb{Q}_C : \mathbb{Q}] = (\Delta : \Delta_C) = d(\mathbf{C}).$$

Equality (4.16) results from the fact that for all conjugacy classes C of G

$$\mathbb{Q}_C = \mathbb{Q}(\{\chi(C) \mid \chi \in \text{Irr}(G)\}),$$

which follows from $\chi^\delta(C) = \chi(C^{c(\delta)})$ (see Huppert (1967), Satz V.13.1). \square

According to Proposition 4.4, a class vector $\mathbf{C} \in \text{Cl}(G)^s$ will be called *rational* if $d(\mathbf{C}) = 1$ and hence $\mathbb{Q}_C = \mathbb{Q}$. For $\mathbf{C} = (C_1, \dots, C_s) \in \text{Cl}(G)^s$ let

$$\Sigma(\mathbf{C}) := \{\sigma \in \Sigma_s(G) \mid \sigma_i \in C_i\} \quad (4.17)$$

with $\Sigma_s(G)$ as in (4.2), and denote by

$$l(\mathbf{C}) := |\Sigma(\mathbf{C}) / \text{Inn}(G)| \quad (4.18)$$

the number of generating s -system classes $[\sigma]$ of G with components $\sigma_i \in C_i$. Following Thompson (1984a) a class vector \mathbf{C} is called *rigid* if $l(\mathbf{C}) = 1$. It is called *rationally rigid* if moreover \mathbf{C} is rational.

As the stabilizer

$$\Delta_\sigma := \{\delta \in \Delta \mid [\sigma]^\delta = [\sigma]\} \quad (4.19)$$

of $[\sigma]$ under the action (4.9) of $\Delta \subseteq \Gamma$ is a closed subgroup of Γ with index at most $l(\mathbf{C})$ in Δ_C , we conclude:

Theorem 4.5. *Let G be a finite group and σ a generating s -system belonging to the class vector \mathbf{C} . If the ramification locus \mathbb{S} of $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ remains pointwise fixed under $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$, then the fixed field K_σ of Δ_σ contains the cyclotomic field \mathbb{Q}_C , and we have*

$$[K_\sigma : \mathbb{Q}_C(t)] \leq l(\mathbf{C}). \quad (4.20)$$

Thus we have $K_\sigma = \mathbb{Q}_C(t)$ if \mathbf{C} is rigid, and if \mathbf{C} is even rationally rigid it follows that $K_\sigma = \mathbb{Q}(t)$.

4.3 The Basic Rigidity Theorem

The fixed field K_σ of a class of generating s -systems $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ often coincides with a field of definition for $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$.

Proposition 4.6. *The field \bar{N}_σ is Galois over K_σ . Moreover the automorphisms of \bar{N}_σ/K_σ act as inner automorphisms on $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$.*

Proof. Let $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/K_\sigma)$ with an extension $\tilde{\delta}$ onto $\bar{M}_\mathbf{S}$. As $[\sigma] = [\sigma]^\delta$ we have by (4.10)

$$\ker(\sigma)^\tilde{\delta} = \ker(\sigma^{\tilde{\delta}^{-1}}) = \ker(\sigma).$$

Hence $\ker(\sigma)$ is normal in $\text{Gal}(\bar{M}_\mathbf{S}/K_\sigma)$ and the fixed field \bar{N}_σ of $\ker(\sigma)$ is Galois over K_σ . By assumption, two generating systems σ and $\sigma^{\tilde{\delta}}$ differ by an inner automorphism of G . Hence there exists a $\tau \in G$ with $\sigma^{\tilde{\delta}} = \sigma^\tau$. So for the images $\varphi(\sigma_i) := \varphi_\sigma(\sigma_i)$ of σ_i in $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$ we obtain by (4.5) and (4.8)

$$\varphi(\sigma)^{\tilde{\delta}} = \psi_\sigma^{-1}(\sigma)^{\tilde{\delta}} \ker(\sigma) = \psi_\sigma^{-1}(\sigma^{\tilde{\delta}}) \ker(\sigma) = \varphi(\sigma^\tau) = \varphi(\sigma)^{\varphi(\tau)}.$$

Thus $\tilde{\delta}$ maps the generating system $\varphi(\sigma)$ of $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$ onto its conjugate $\varphi(\sigma)^{\varphi(\tau)}$ and therefore acts as inner automorphism on $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$. \square

Remark. According to the definition, K_σ is the smallest subfield of $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$ for which the assertions of Proposition 4.6 hold. It is sometimes called *field of moduli*.

Application of Theorem 3.9 and Proposition 4.6 now yields:

Theorem 4.7. *Let G be a finite group in which the center has a complement, and let σ be a generating s -system of G . Then the fixed field K_σ of $[\sigma]$ is a field of definition of $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$.*

Proof. By Proposition 4.6, the extension \bar{N}_σ/K_σ is Galois and each automorphism of \bar{N}_σ/K_σ acts as an inner automorphism on $G = \text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$. Now let k_σ be the algebraic closure of \mathbb{Q} in K_σ and $\mathfrak{P} \in \text{IP}(k_\sigma(t)/k_\sigma)$ a prime divisor of degree one unramified in $\bar{N}_\sigma/k_\sigma(t)$. As the inertia subgroups G_I of prime divisors $\mathfrak{P} \in \text{IP}(\bar{N}_\sigma/\bar{\mathbb{Q}})$ above \mathfrak{P} are trivial, $\mathcal{L}(G)$ possesses a complement in $\mathcal{N}_G(G_I) = G$. Hence \mathfrak{P} satisfies the normalizer condition (N) of Theorem 3.9, and $k_\sigma(t)$ is a field of definition for $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$. In particular there exists a geometric Galois extension $N_\sigma/k_\sigma(t)$ with

$$\text{Gal}(N_\sigma/k_\sigma(t)) \cong G \quad \text{and } \bar{\mathbb{Q}}N_\sigma = \bar{N}_\sigma.$$

\square

In the case that $l(\mathbf{C}) = 1$ this specializes to the Basic Rigidity Theorem:

Theorem 4.8 (Basic Rigidity Theorem). *Let G be a finite group in which the center has a complement, and $\mathbf{C} \in \text{Cl}(G)^s$ a rigid class vector of G . Then for any arbitrarily chosen set \mathbf{S} of s prime divisors $\mathfrak{P}_i \in \text{IP}(\mathbb{Q}_\mathbf{C}(t)/\mathbb{Q}_\mathbf{C})$ of degree one there exists a Galois extension $N/\mathbb{Q}_\mathbf{C}(t)$ unramified outside \mathbf{S} with*

$$\text{Gal}(N/\mathbb{Q}_\mathbf{C}(t)) \cong G$$

such that the inertia groups over the \mathfrak{P}_i are generated by elements $\sigma_i \in C_i$.

If the class vector is rationally rigid, we have $\mathbb{Q}_\mathbf{C} = \mathbb{Q}$.

Proof. By assumption \mathbf{C} is rigid, so there exists a single class of generating s -systems $[\sigma]$ of G in $\Sigma(\mathbf{C})/\text{Inn}(G)$. By the Hurwitz classification (4.4) there exists a Galois extension $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ with group G , unramified outside \mathbf{S} . As $l(\mathbf{C}) = 1$,

$[\sigma]$ remains fixed under Δ_C , and we have $K_\sigma = \mathbb{Q}_C(t)$ by Theorem 4.5. By Theorem 4.7, $\mathbb{Q}_C(t)$ is a field of definition for $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$, hence there exists a geometric Galois extension $N/\mathbb{Q}_C(t)$ with

$$\text{Gal}(N/\mathbb{Q}_C(t)) \cong G \quad \text{and} \quad \bar{\mathbb{Q}}N = \bar{N}_\sigma.$$

The additional assertion on the ramification of $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ and hence also $N/\mathbb{Q}_C(t)$ is contained in Theorem 4.1. Finally, by Proposition 4.4 we have $\mathbb{Q}_C = \mathbb{Q}$ if and only if C is rational. \square

Remark. In the proof of Theorem 4.7, the existence of a complement to the center was only used to deduce the existence of a prime divisor $\mathfrak{P} \in \mathbb{P}(k_\sigma(t)/k_\sigma)$ of degree one satisfying the normalizer condition (N). Theorems 4.7 and 4.8 hence remain valid under this weaker assumption, with the same proof.

4.4 Choice of Ramification Points

Under a suitable choice of the ramification points it may be possible to obtain geometric Galois extensions over $\mathbb{Q}(t)$ even if the corresponding class vector C is not rational. Explicitly checkable criteria for this can be found. For their formulation, we need some more notation.

For $C \in \text{Cl}(G)^s$ let

$$\text{Sym}(C) := \{\omega \in S_s \mid C^\omega \in C^*\} \quad (4.21)$$

with $(C_1, \dots, C_s)^\omega := (C_{1^\omega}, \dots, C_{s^\omega})$ be the *full symmetry group of C* and $V \leq \text{Sym}(C)$ a *symmetry group of C* . For such a V let

$$C^V := \{C^\omega \mid \omega \in V\} \subseteq C^*. \quad (4.22)$$

Furthermore,

$$d^V(C) := |\mathbf{C}^*|/|\mathbf{C}^V| \quad (4.23)$$

is called the *V -symmetrized irrationality degree of C* . According to our definitions we have $d^V(C) = 1$ precisely when $C^V = C^*$. The class vector C is then called *V -symmetric*.

In analogy to (4.13) we now write

$$\Delta_C^V := \{\delta \in \Delta \mid C^{c(\delta)} \in C^V\} \quad (4.24)$$

for the setwise stabilizer of C^V in Δ under its action by exponentiation via the cyclotomic character. The above definitions and Proposition 4.4 now yield

Proposition 4.9. *The fixed field $\mathbb{Q}_C^V := \bar{\mathbb{Q}}^{\Delta_C^V}$ of Δ_C^V is an abelian number field contained in \mathbb{Q}_C , of degree*

$$[\mathbb{Q}_C^V : \mathbb{Q}] = d^V(C). \quad (4.25)$$

In particular we have $\mathbb{Q}_C^V = \mathbb{Q}$ if and only if the class vector C is V -symmetric.

Under the assumption $\$^\Delta = \$$ the group Δ possesses the permutation representation

$$\pi_{\$} : \Delta \longrightarrow S_s, \quad \delta \mapsto \begin{pmatrix} 1 & \dots & s \\ (1)\delta & \dots & (s)\delta \end{pmatrix} \quad (4.26)$$

in the symmetric group S_s . By definition, C^δ then belongs to C^* if and only if $\pi_{\$}(\delta)$ lies in $\text{Sym}(C)$. So no information on the position of the ramification points is lost if we restrict ourselves to $\pi_{\$}(\Delta) \leq \text{Sym}(C)$.

Theorem 4.10. *Let G be a finite group and σ a generating s -system belonging to the class vector C . Further assume that the action (4.26) of $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ on the ramification locus \mathbf{S} of $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ satisfies*

$$V := \pi_{\$}(\Delta) \leq \text{Sym}(C).$$

Then the fixed field K_σ of $[\sigma]$ contains the cyclotomic field \mathbb{Q}_C^V . Moreover if Δ_C^V acts via $\pi := \pi_{\$}$ inversely to the cyclotomic character c on C^V , i.e., if $C^{\pi(\delta)} = C^{c(\delta)^{-1}}$, then

$$[K_\sigma : \mathbb{Q}_C^V(t)] \leq l(C). \quad (4.27)$$

Proof. By Proposition 4.3 we have $C_i^\delta = C_{(i)\delta}^{c(\delta)} = C_i$ and hence $(C^{\pi(\delta)})^{c(\delta)} = C$ for all $\delta \in \Delta_\sigma$. As $C^{\pi(\delta)} \in C^V$ we also have $C^{c(\delta)} \in C^V$, which entails $\delta \in \Delta_C^V$. So we certainly have $K_\sigma \geq \mathbb{Q}_C^V$.

From $C^{\pi(\delta)} = C^{c(\delta)^{-1}}$ we conclude that $C^\delta = C$ for all $\delta \in \Delta_C^V$. Hence the index $(\Delta_C^V : \Delta_\sigma)$ is bounded by the cardinality $l(C)$ of the orbit space $\Sigma(C)/\text{Inn}(G)$. This finally implies (4.27). \square

As a special case of the above result we obtain the following stronger version of the Basic Rigidity Theorem:

Theorem 4.11 (Strong Rigidity Theorem). *Let G be a finite group whose center possesses a complement and with a rigid class vector $C \in \text{Cl}(G)^s$. Furthermore let V be a symmetry group of C with the property that for each $\delta \in \Delta_C^V$ there exists precisely one $\omega \in V$ with $C^{c(\delta)} = C^\omega$. Then there exists a geometric Galois extension $N/\mathbb{Q}_C^V(t)$ with*

$$\text{Gal}(N/\mathbb{Q}_C^V(t)) \cong G. \quad (4.28)$$

If moreover C is V -symmetric, then we have $\mathbb{Q}_C^V = \mathbb{Q}$.

Proof. The set of classes $\{C_1, \dots, C_s\}$ decomposes into orbits under the action of the symmetry group V . For each such orbit \mathbf{B} let

$$\Delta_{\mathbf{B}} := \{\delta \in \Delta_{\mathbf{C}}^V \mid C_i^{c(\delta)} = C_i \text{ for all } C_i \in \mathbf{B}\}.$$

From (4.13) we know that $\Delta_{\mathbf{B}} \geq \Delta_{\mathbf{C}}$, and $\Delta_{\mathbf{B}}/\Delta_{\mathbf{C}}$ acts regularly on \mathbf{B} . Hence the fixed field $\mathbb{Q}_{\mathbf{B}} := \bar{\mathbb{Q}}^{\Delta_{\mathbf{B}}}$ is contained in $\mathbb{Q}_{\mathbf{C}}$ and therefore by Proposition 4.4 an abelian number field with $[\mathbb{Q}_{\mathbf{B}} : \mathbb{Q}_{\mathbf{C}}^V] = |\mathbf{B}|$. Now for an arbitrary class $C_i \in \mathbf{B}$ we choose a primitive element a_i of $\mathbb{Q}_{\mathbf{B}}/\mathbb{Q}_{\mathbf{C}}^V$. For $\delta \in \Delta_{\mathbf{C}}^V$ and the element $\omega \in V$ uniquely determined by δ we define $\mathfrak{P}_{(i)\omega}$ to be the numerator divisor of $(t - a_i^{\delta^{-1}})$. In this way we obtain prime divisors $\mathfrak{P}_j \in \mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$ for all indices j contained in the V -orbit of i . Collect these (without loss of generality pairwise distinct) prime divisors in $\mathbb{S} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$. Then by construction the permutation representation $\pi_{\mathbb{S}}$ from (4.26) satisfies $\pi_{\mathbb{S}}(\delta) = \omega^{-1}$, and hence we have

$$\mathbf{C}^{\delta} = (\mathbf{C}^{\omega^{-1}})^{c(\delta)} = \mathbf{C} \quad \text{for all } \delta \in \Delta_{\mathbf{C}}^V. \quad (4.29)$$

Now let $[\sigma]$ denote the unique generating s -system class in $\Sigma(\mathbf{C})/\text{Inn}(G)$, further \bar{N}_{σ} the field in $\bar{\mathbb{N}}_{\mathbb{S}}(G)$ determined by the Hurwitz classification (4.4), and K_{σ} the fixed field of $[\sigma]$. Then K_{σ} coincides with $\mathbb{Q}_{\mathbf{C}}^V(t)$ by (4.29) and Theorem 4.10. Hence by Theorem 3.9 the field $\mathbb{Q}_{\mathbf{C}}^V(t)$ constitutes a field of definition of $\bar{N}_{\sigma}/_G\bar{\mathbb{Q}}(t)$, and there exists a geometric Galois extension $N/\mathbb{Q}_{\mathbf{C}}^V(t)$ with

$$\text{Gal}(N/\mathbb{Q}_{\mathbf{C}}^V(t)) \cong G \quad \text{and} \quad \bar{\mathbb{Q}}N = \bar{N}_{\sigma}.$$

Further by Proposition 4.9 we have $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$ precisely when the class vector \mathbf{C} is V -symmetric. \square

Remark. As in the proof of the Basic Rigidity Theorem — which here corresponds to the case $V = 1$ — the inertia groups over the ramification points \mathfrak{P}_i are generated by the elements $\sigma_i \in C_i$. The assumptions on ω of Theorem 4.11 then translate to the statement: Each $\delta \in \Delta_{\mathbf{C}}^V$ permutes the components of $\mathbf{C} = (C_1, \dots, C_s)$ via $c(\delta)$ and of $(\mathfrak{P}_1, \dots, \mathfrak{P}_s)$ via $\pi_{\mathbb{S}}$ in the same way, which of course is equivalent to (4.29).

5 Verification of Rigidity

In the first two sections the Basic Rigidity Theorem and its stronger variant are applied to abelian and to symmetric groups. For these, the existence of rigid generating systems may be checked by direct computation. In the next two sections we show how to find rigid class vectors using the character table or a suitable matrix representation of the given group.

5.1 Geometric Galois Extensions over $\mathbb{Q}(t)$ with Abelian Groups

All class vectors \mathbf{C} of abelian groups with $\Sigma(\mathbf{C}) \neq \emptyset$ are automatically rigid, thus these groups present the easiest case. In particular the cyclic groups $Z_n = \langle \sigma \rangle$ obviously possess $\mathbf{C} = (C, C^{-1})$, where $C = \{\sigma\}$, as a natural rigid class vector (compare Example 3.1). But \mathbf{C} is rationally rigid only for $n \leq 2$, since $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\zeta_n)$. If all primitive powers of σ , resp. C , are collected into one class vector $\mathbf{C} = (C^m \mid m \in (\mathbb{Z}/n\mathbb{Z})^\times)$, then we obtain a rigid class vector for any $n \geq 3$, which under a suitable choice of ramification points and symmetry group V yields $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$ and therefore leads to geometric Galois extensions over $\mathbb{Q}(t)$ with group Z_n . This statement can be generalized to arbitrary finite abelian groups as will be shown in the following theorem.

For brevity, let us call a realization of a group H as Galois group $\text{Gal}(N/K)$ a *G-realization of H over k (in r variables)*, if it satisfies the property

(G): N/K is a geometric Galois extension with Galois group H over a rational function field K/k (of transcendence degree r).

(In Serre (1992), 4.1, this property is called Gal_T in the case $k = \mathbb{Q}$.)

Theorem 5.1. *Every finite abelian group possesses a G-realization over \mathbb{Q} .*

Proof. Any finite abelian group G decomposes into a direct product of cyclic groups

$$G = Z_{n_1} \times \cdots \times Z_{n_r},$$

say, where we assume that the n_i are in increasing order. For the first q factors $Z_{n_i} = \langle \sigma_i \rangle$ with $n_i = 2$ the pair (σ_i, σ_i) forms a generating 2-system. For the remaining factors with $n_i \geq 3$ the tuples $(\sigma_i^m \mid m \in (\mathbb{Z}/n_i\mathbb{Z})^\times)$ clearly yield generating $\varphi(n_i)$ -systems, where φ denotes the Euler φ -function. Composing these generating systems we obtain a generating s -system σ of G with $s = q + \sum_{i=1}^r \varphi(n_i)$. As G is abelian, we trivially have $l(\mathbf{C}) = 1$ for the class vector \mathbf{C} containing σ .

Now by construction the components C_1, \dots, C_s of \mathbf{C} consist of full orbits under the exponentiation with $c(\delta)$ for $\delta \in \Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$, so exponentiation induces a permutation representation π of Δ on the classes C_i (trivial on the first $2q$ classes of involutions), and hence on $\{1, \dots, s\}$ with $\ker(\pi) = \Delta_{\mathbf{C}}$. For $V := \text{im}(\pi)$ we then have $\Delta_{\mathbf{C}}^V = \Delta$ due to $\mathbf{C}^V = \mathbf{C}^*$, and $\Delta/\Delta_{\mathbf{C}} \cong V$. Hence for each $\delta \in \Delta$ there exists

a unique $\omega \in V$ satisfying $\mathbf{C}^{c(\delta)} = \mathbf{C}^\omega$. Since moreover the center of an abelian group possesses the trivial group as complement, we may apply the Strong Rigidity Theorem 4.11 to obtain the desired conclusion. \square

Remark. Since it is easy to obtain a G-realization of a direct product from G-realizations of its factors (see also Chapter IV, Corollary 1.7), the assumption that $\mathcal{Z}(G)$ possesses a complement in G may from now on be replaced without loss of generality by the assumption that $\mathcal{Z}(G) = 1$.

5.2 Geometric Galois Extensions over $\mathbb{Q}(t)$ with S_n and A_n

A further example in which the rigidity of class vectors may be shown purely combinatorially is given by the groups S_n . Therefore, let $2A$, $(n-1)A$ and nA denote the conjugacy classes of transpositions, $(n-1)$ -cycles and n -cycles respectively, in the symmetric group S_n on n letters. The results of this section rely on the simple fact:

Proposition 5.2. *The class vector $\mathbf{C} = (2A, (n-1)A, nA)$ of S_n is rationally rigid for $n \geq 2$.*

Proof. All elements of S_n with the same cycle shape are conjugate, so the class vector \mathbf{C} is rational. In case $n = 2$, $\mathbf{C} = (2A, 2A)$ is a rigid class vector of $S_2 = Z_2$. For $n \geq 3$ we have to show that \mathbf{C} contains just one class of generating systems. Let $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in \Sigma(\mathbf{C})$ be such a system. By conjugation with elements from S_n we may assume that $\sigma_3 = (1 \dots n)$. Moreover conjugating $\sigma_1 = (i \ j)$ with a power of σ_3 we get

$$\sigma_3^{i-1} \sigma_1 \sigma_3^{1-i} = (1 \ j+1-i), \quad \sigma_3^{j-1} \sigma_1 \sigma_3^{1-j} = (1 \ i+1-j),$$

so σ_1 can be transformed into the shape $(1k)$ with $2 \leq k \leq n/2 + 1$. But as

$$\sigma_3 \sigma_1 = (1 \dots n)(1k) = (1 \dots k-1)(k \dots n)$$

should lie in $(n-1)A$, it follows that necessarily $k = 2$. So each $\sigma \in \Sigma(\mathbf{C})$ is conjugate to $((12), (2 \dots n)^{-1}, (1 \dots n))$. Moreover it is well known that a primitive subgroup of S_n containing a transposition is already equal to S_n , so this finally shows that $\Sigma(\mathbf{C}) \neq \emptyset$. \square

Using the Basic Rigidity Theorem, Proposition 5.2 now yields the following result, originally proved by Hilbert:

Theorem 5.3 (Hilbert (1892)). *The groups S_n and A_n possess G-realizations over \mathbb{Q} .*

Proof. For the symmetric groups S_n this follows with the Basic Rigidity Theorem 4.8 immediately from Proposition 5.2.

Now let $N/\mathbb{Q}(t)$ denote this Galois extension with $\text{Gal}(N/\mathbb{Q}(t)) = S_n$ for $\mathbf{C} = (2A, (n-1)A, nA)$. Further, let K' be the fixed field of A_n . Either the $(n-1)$ -cycles

or the n -cycles, and hence the inertia groups generated by them, lie already inside the alternating group A_n . Thus, only two prime divisors are ramified in $K'/\mathbb{Q}(t)$, both of order two. Consequently the different $\mathfrak{D}(K'/\mathbb{Q}(t))$ has degree 2. By the Hurwitz genus formula (see for example Lang (1982), Ch. I, Thm. 6.1) this implies

$$g(K') = 1 + 2(g(\mathbb{Q}(t)/\mathbb{Q}) - 1) + \frac{1}{2} \deg(\mathfrak{D}(K'/\mathbb{Q}(t))) = 0.$$

Moreover the ramified prime divisors have degree one in $K'/\mathbb{Q}(t)$, so K'/\mathbb{Q} is a rational function field, say $K' = \mathbb{Q}(t')$ (see Artin (1967), Ch. 16, Thm. 7), and $N/\mathbb{Q}(t')$ is a geometric Galois extension with group A_n . \square

A G -realization $\text{Gal}(N/K)$ over k for a group H with trivial center is called a *GA-realization of H over k* if in addition it has property

- (A): $\text{Gal}(N/K)$ may be embedded into a geometric Galois extension with group $\text{Aut}(H)$ (under identification of H with $\text{Inn}(H)$).

Such realizations will prove particularly useful for the solution of embedding problems with kernel H (compare Chapter IV.3). Since $\text{Aut}(A_n) = S_n$ for $n \neq 6$ we may thus deduce from Theorem 5.3 the following result:

Corollary 5.4. *The groups A_n possess GA-realizations over \mathbb{Q} for $n \neq 6$.*

In general it is extremely difficult to prove rigidity of class vectors as above just from the definition without using further information. In the next section we show how to profit from the knowledge of structure constants, which may be computed from the character table. This method has proved particularly useful for the sporadic groups and the exceptional groups of Lie type (see Chapter II).

5.3 Structure Constants

We first enlarge the set $\Sigma(\mathbf{C})$ of generating s -systems of G in \mathbf{C} to the set

$$\bar{\Sigma}(\mathbf{C}) := \{\sigma \in G^s \mid \sigma_i \in C_i, \sigma_1 \cdots \sigma_s = 1\} \quad (5.1)$$

of not necessarily generating s -systems. The group G also acts on this set by conjugation in the components. The quotient

$$n(\mathbf{C}) := |\bar{\Sigma}(\mathbf{C})| / |\text{Inn}(G)| \quad (5.2)$$

constitutes an estimate for the number of orbits under this action; it will be called the *normalized structure constant of \mathbf{C}* .

Proposition 5.5. *The normalized structure constant of a class vector $\mathbf{C} \in \text{Cl}(G)^s$ of a finite group G is given by*

$$n(\mathbf{C}) = \sum_{[\sigma] \in \bar{\Sigma}(\mathbf{C}) / \text{Inn}(G)} \frac{|\mathcal{L}(G)|}{|\mathcal{C}_G(\langle \sigma_1, \dots, \sigma_s \rangle)|}. \quad (5.3)$$

Proof. The class equation for the action of G on $\bar{\Sigma}(\mathbf{C})$ gives

$$|\bar{\Sigma}(\mathbf{C})| = \sum_{[\sigma] \in \bar{\Sigma}(\mathbf{C}) / \text{Inn}(G)} (G : \mathcal{C}_G(\langle \sigma_1, \dots, \sigma_s \rangle)).$$

The assertion now follows with (5.2). \square

From Proposition 5.5 we immediately get

Corollary 5.6. *For a class vector $\mathbf{C} \in \text{Cl}(G)^s$ of a finite group G we have $l(\mathbf{C}) \leq n(\mathbf{C})$. Moreover equality holds if and only if $\bar{\Sigma}(\mathbf{C}) = \Sigma(\mathbf{C})$.*

For later use we now split up the normalized structure constant into the contribution from the generated subgroups. This leads to the following sum formula:

Proposition 5.7. *For the class vector \mathbf{C} of a finite group G we have*

$$n(\mathbf{C}) = \sum_{[H]: H \leq G} n(\mathbf{C}; H) \quad (5.4)$$

with

$$n(\mathbf{C}; H) = \frac{(H : \mathcal{L}(H))}{(\mathcal{N}_G(H) : \mathcal{L}(G))} \sum_{\mathbf{D} \subseteq \mathbf{C}} l_H(\mathbf{D}). \quad (5.5)$$

Here the sum in (5.4) runs over the conjugacy classes of subgroups of G and in (5.5) over the class vectors of H fusing into \mathbf{C} in G .

Proof. By combining those summands in (5.3) for which $\langle \sigma \rangle$ is conjugate in G to $H \leq G$ we obtain

$$n(\mathbf{C}; H) = \sum_{\substack{[\sigma] \in \bar{\Sigma}(\mathbf{C}) / \text{Inn}(G) \\ [\langle \sigma \rangle] = [H]}} \frac{|\mathcal{L}(G)|}{|\mathcal{C}_G(H)|}.$$

For a class vector \mathbf{D} of H fusing into \mathbf{C} precisely $(\mathcal{N}_G(H) : \mathcal{C}_G(H)) / |\text{Inn}(H)|$ classes of generating systems $\sigma \in \Sigma(\mathbf{D}) / \text{Inn}(H)$ of H fuse into one class $\sigma \in \bar{\Sigma}(\mathbf{C}) / \text{Inn}(G)$. This further implies

$$\begin{aligned} n(\mathbf{C}; H) &= \sum_{\mathbf{D} \subseteq \mathbf{C}} \sum_{[\sigma] \in \Sigma(\mathbf{D}) / \text{Inn}(H)} \frac{|\text{Inn}(H)| |\mathcal{L}(G)|}{(\mathcal{N}_G(H) : \mathcal{C}_G(H)) |\mathcal{C}_G(H)|} \\ &= \sum_{\mathbf{D} \subseteq \mathbf{C}} \frac{(H : \mathcal{L}(H))}{(\mathcal{N}_G(H) : \mathcal{L}(G))} l_H(\mathbf{D}). \end{aligned} \quad \square$$

The normalized structure constant of \mathbf{C} may be computed directly from the values of the complex irreducible characters of G . This offers the possibility of determining the important invariant $l(\mathbf{C})$ from the character tables of G and its subgroups.

Theorem 5.8. *Let $\mathbf{C} = (C_1, \dots, C_s) \in \text{Cl}(G)^s$ be a class vector of a finite group G , where $s \geq 2$. Then we have*

$$n(\mathbf{C}) = |\mathcal{L}(G)| \sum_{\chi \in \text{Irr}(G)} \frac{|G|^{s-2}}{\chi(1)^{s-2}} \prod_{i=1}^s \frac{\chi(\sigma_i)}{|\mathcal{C}_G(\sigma_i)|}, \quad \sigma_i \in C_i. \quad (5.6)$$

Proof. For $\chi \in \text{Irr}(G)$ let $R : G \rightarrow \text{GL}_n(\mathbb{C})$ denote a corresponding matrix representation. By the Schur's Lemma for each $\sigma \in G$ there exists an $\omega(\sigma) \in \mathbb{C}$ satisfying

$$\frac{1}{|G|} \sum_{\rho \in G} R(\sigma^\rho) = \omega(\sigma) I_n, \quad \text{where } \omega(\sigma) = \frac{\chi(\sigma)}{\chi(1)},$$

as follows from the evaluation of traces. Hence for all pairs $(\sigma, \tau) \in G^2$ we have

$$\frac{1}{|G|} \sum_{\rho \in G} R(\sigma^\rho \tau) = \frac{\chi(\sigma)}{\chi(1)} R(\tau).$$

Induction on s now yields

$$\frac{1}{|G|^s} \sum_{\rho \in G^s} R(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s} \tau) = \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^s} R(\tau),$$

and evaluation of traces for $\tau = 1$ then leads to

$$\frac{1}{|G|^s} \sum_{\rho \in G^s} \chi(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s}) = \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-1}}.$$

Now let

$$\epsilon := \frac{1}{|G|} \sum_{\chi \in \text{Irr}(G)} \chi(1) \chi$$

be the characteristic function of the identity in G . Accordingly, multiplying the previous equation by $\chi(1)|G|^{s-1}$ and summing over $\chi \in \text{Irr}(G)$ we hence obtain

$$m(\mathbf{C}) := \sum_{\rho \in G^s} \epsilon(\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s}) = |G|^{s-1} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-2}}.$$

Here $m(\mathbf{C})$ counts the number of solutions $\rho \in G^s$ of $\sigma_1^{\rho_1} \cdots \sigma_s^{\rho_s} = 1$. The normalized structure constant

$$n(\mathbf{C}) = \frac{1}{|\text{Inn}(G)|} |\{\sigma \in \mathbf{C} \mid \sigma_1 \cdots \sigma_s = 1\}|$$

may then be expressed as

$$n(\mathbf{C}) = \frac{m(\mathbf{C})}{|\text{Inn}(G)|} \prod_{i=1}^s |\mathcal{C}_G(\sigma_i)|^{-1}.$$

So indeed we obtain (5.6). \square

In particular Theorem 5.8 leads to the following frequently used criterion for rigid class vectors:

Corollary 5.9. *A class vector $\mathbf{C} \in \text{Cl}(G)^s$ of a finite group G is rigid if the following two conditions are satisfied:*

(1) $G = \langle \sigma_1, \dots, \sigma_s \rangle$ for some $\sigma_i \in C_i$ with $\sigma_1 \cdots \sigma_s = 1$,

$$(2) \quad \sum_{\chi \in \text{Irr}(G)} \frac{\chi(\sigma_1) \cdots \chi(\sigma_s)}{\chi(1)^{s-2}} = \frac{|\mathcal{C}_G(\sigma_1)| \cdots |\mathcal{C}_G(\sigma_s)|}{|G|^{s-2} |\mathcal{Z}(G)|}.$$

Proof. From (2) we get $n(\mathbf{C}) = 1$, and then Condition (1) clearly implies $l(\mathbf{C}) = 1$ by Corollary 5.6. \square

The following example is an application of Theorem 5.8. It shows that rigidity for groups of reasonable size may easily be checked even by hand.

Example 5.1. Let $G = \text{L}_2(8) = \text{SL}_2(8)$ and $\mathbf{C} = (9A, 9B, 9C)$ the class vector consisting of the three classes containing elements of order 9, where $9B = (9A)^2$ and $9C = (9A)^4$, say. Then from the character table of G in the group Atlas (Conway et al. (1985)) one calculates

$$\begin{aligned} n(\mathbf{C}) &= \frac{|G|}{|\mathcal{C}_G(\sigma_1)|^3} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(\sigma_1)\chi(\sigma_2)\chi(\sigma_3)}{\chi(1)} \\ &= \frac{504}{9^3} \left(1 + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} - \frac{1}{8} + 0 + 0 + 0 \right) = 1. \end{aligned}$$

It remains to show that condition (1) in Corollary 5.9 is satisfied. Assuming the contrary, any triple $\sigma \in \mathbf{C}$ with $\sigma_1\sigma_2\sigma_3 = 1$ would generate a proper subgroup of G . The only maximal subgroups of G with order divisible by 9 are dihedral groups D_{18} of order 18, hence we would have $\langle \sigma \rangle = Z_9$. But this implies $\sigma_2 \in \{\sigma_1^2, \sigma_1^7\}$ and $\sigma_3 \in \{\sigma_1^4, \sigma_1^5\}$, contradicting the product relation $\sigma_1\sigma_2\sigma_3 = 1$. Hence $(9A, 9B, 9C)$ is a rigid class vector of $\text{L}_2(8)$.

Now $\mathbb{Q}_{\mathbf{C}}$ is the maximal real subfield of the field of ninth roots of unity. With the choice $V = \langle (123) \rangle$ and a corresponding V -configuration \mathbb{S} we get $\Delta_{\mathbf{C}}^V = \Delta$ and $\Delta/\Delta_{\mathbf{C}} \cong V$, and in particular, V acts regularly on \mathbf{C}^* . Thus for each $\delta \in \Delta$ there exists a unique $\omega \in V$ with $\mathbf{C}^{c(\delta)} = \mathbf{C}^{\omega}$. From the Strong Rigidity Theorem 4.11 now follows the existence of a G -realization of $\text{L}_2(8)$ over \mathbb{Q} . \square

In the next section, we introduce a criterion for rigidity making use of an irreducible matrix representation of G . This has proved extremely helpful in the case of classical groups (see Chapter II).

5.4 The Rigidity Criterion of Belyi

In this section

$$R : G \longrightarrow \mathrm{GL}(V) \cong \mathrm{GL}_n(k), \quad \sigma \mapsto R(\sigma), \quad (5.7)$$

denotes a faithful irreducible representation of the group G into the group of automorphisms of an n -dimensional vector space V over an arbitrary field k . We identify G with its image in $\mathrm{GL}(V)$ under the embedding R ; so in particular we need not distinguish between $1 \in G$ and Id_V . We then have:

Theorem 5.10 (Belyi (1979)). *Let G be a finite group, embedded into $\mathrm{GL}(V) \cong \mathrm{GL}_n(k)$ via the irreducible representation R . Assume that there exist $\sigma_1, \sigma_2 \in G$ with $\langle \sigma_1, \sigma_2 \rangle = G$, and $a \in k^\times$, such that $\sigma_1 - a1$ has rank one. Then all generating 3-systems in $\Sigma([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}])$ are conjugate under $\mathrm{Aut}(G)$. If moreover $\mathcal{N}_{\mathrm{GL}(V)}(G) = G \cdot \mathcal{C}_{\mathrm{GL}(V)}(G)$, then the triple $([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}])$ of conjugacy classes in G is rigid.*

Proof. Let $\tilde{\sigma}_1, \tilde{\sigma}_2 \in G$ be a generating pair of G with $[\tilde{\sigma}_i] = [\sigma_i]$, $i = 1, 2$, and $[\tilde{\sigma}_1 \tilde{\sigma}_2] = [\sigma_1 \sigma_2]$. We have to show that there exists an element $\alpha \in \mathrm{Aut}(G)$ (resp. $\alpha \in G$ in the second case) such that $\tilde{\sigma}_i = \sigma_i^\alpha$ for $i = 1, 2$. By conjugation with a suitable element of G we may assume $\tilde{\sigma}_2 = \sigma_2$, and then α has to centralize σ_2 . Let $\tau := \sigma_1 - a1$ and $\tilde{\tau} := \tilde{\sigma}_1 - a1$ be the elements of rank one. As $\sigma_1 \sigma_2$ and $\tilde{\sigma}_1 \tilde{\sigma}_2 = \tilde{\sigma}_1 \sigma_2$ are conjugate in G , in the field of rational functions $k(t)$ we have

$$\det(\tau \sigma_2 + a \sigma_2 + t1) = \det(\tilde{\tau} \sigma_2 + a \sigma_2 + t1). \quad (5.8)$$

Obviously in $\mathrm{End}(V \otimes_k k((t)))$ we have the identity

$$(a \sigma_2 + t1)^{-1} = \sum_{i=0}^{\infty} (a \sigma_2)^{-i-1} (-t)^i,$$

where $k((t))$ denotes the field of formal power series in t over k . Multiplying (5.8) by $\det(a \sigma_2 + t1)^{-1}$ we further obtain

$$\det(\tau \sigma_2 (a \sigma_2 + t1)^{-1} + 1) = \det(\tilde{\tau} \sigma_2 (a \sigma_2 + t1)^{-1} + 1). \quad (5.9)$$

Let $\psi \in \mathrm{End}(W)$ be an element of rank at most one, where W is an arbitrary vector space over a field. Then consideration of the Jordan normal form immediately shows that $\det(\psi + 1) = \mathrm{tr}(\psi) + 1$. Since the rank of $\tau \sigma_2 (a \sigma_2 + t1)$ is bounded by the rank of τ , which equals 1, this may be applied to (5.9), yielding

$$\mathrm{tr}(a \tau \sum_{i=0}^{\infty} \sigma_2^{-i} (-t)^i) = \mathrm{tr}(a \tilde{\tau} \sum_{i=0}^{\infty} \sigma_2^{-i} (-t)^i),$$

and therefore by comparing coefficients

$$\mathrm{tr}(\tau\sigma_2^i) = \mathrm{tr}(\tilde{\tau}\sigma_2^i) \quad (5.10)$$

for $i < 0$. But since σ_2 has finite order, (5.10) holds for all i .

We now decompose the endomorphism τ of V of rank one into the surjection $\tau_1 : V \rightarrow k$ and the injection $\tau_2 : k \rightarrow V$, so $\tau = \tau_2 \circ \tau_1$. Then $k[\sigma_2]\tau_2(1)$ is σ_2 - and τ -invariant, hence also stabilized by σ_1 . Thus it forms a non-trivial G -invariant subspace of V , which must coincide with V by the irreducibility of G . If we decompose $\tilde{\tau} = \tilde{\tau}_2 \circ \tilde{\tau}_1$ in a similar manner, we get $k[\sigma_2]\tilde{\tau}_2(1) = V$ by the same arguments. In particular, there exists an automorphism α of the $k[\sigma_2]$ -module V , hence an element of $\mathrm{Aut}(V)$ centralizing σ_2 , with $\tilde{\tau}_2 = \tau_2^\alpha$. Thus we get

$$\mathrm{tr}(\tau\sigma_2^i) = \mathrm{tr}(\sigma_2^i\tau) = \mathrm{tr}(\sigma_2^i\tau_2\tau_1) = \mathrm{tr}((\sigma_2^i\tau_2\tau_1)^\alpha) = \mathrm{tr}(\sigma_2^i\tilde{\tau}_2\tau_1^\alpha),$$

and from (5.10) we finally obtain

$$\mathrm{tr}(\sigma_2^i\tilde{\tau}_2(\tau_1^\alpha - \tilde{\tau}_1)) = 0$$

for all integers i . Since we already know $k[\sigma_2]\tilde{\tau}_2(1) = V$, it follows that $\tau_1^\alpha = \tilde{\tau}_1$. Hence $\tau^\alpha = \tilde{\tau}$, $\sigma_1^\alpha = \tilde{\sigma}_1$, so α belongs to $\mathcal{N}_{\mathrm{GL}(V)}(G)$ and is therefore the required element. In the second case we may clearly assume that α already lies in G . \square

Remark. The proof shows that instead of $\mathcal{N}_{\mathrm{GL}(V)}(G) = G \cdot \mathcal{C}_{\mathrm{GL}(V)}(G)$ it suffices to assume in Belyi's rigidity criterion that all $\alpha \in \mathcal{N}_{\mathrm{GL}(V)}(G)$ fixing the conjugacy classes $[\sigma_1]$ and $[\sigma_2]$ already belong to $G \cdot \mathcal{C}_{\mathrm{GL}(V)}(G)$.

As an application of Theorem 5.10 we obtain Hecke's characterization of the field of modular functions of level p (Hecke (1935)).

Example 5.2. It is well known that the special linear group $G := \mathrm{SL}_2(p)$, $p \neq 2$, in its natural matrix representation over IF_p is generated by

$$\sigma_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \sigma_2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$$

(The corresponding matrices over \mathbb{Z} even generate the modular group $\mathrm{SL}_2(\mathbb{Z})$.) Then by Theorem 5.10 all generating 3-systems in $\Sigma([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}])$ are conjugate under $\mathrm{Aut}(G)$. Here $H := G \cdot \mathcal{C}_{\mathrm{GL}(V)}(G) = G \cdot \mathcal{C}(\mathrm{GL}(V))$ has index 2 in $\mathcal{N}_{\mathrm{GL}(V)}(G) = \mathrm{GL}_2(p)$. Thus it is still true that $l(\mathbf{C}) = 1$ for the class vector $\mathbf{C} = ([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}])$, since conjugation by $\alpha \in \mathrm{GL}_2(p) \setminus H$ interchanges the two classes of elements of order p in $\mathrm{SL}_2(p)$, so does not fix $[\sigma_1]$.

Passing from $\mathrm{SL}_2(p)$ to the factor group $\bar{G} := \mathrm{L}_2(p)$ we also obtain $l(\bar{\mathbf{C}}) = 1$ for the image $[\bar{\sigma}] \in \Sigma(\bar{\mathbf{C}})$. Hence the class of generating systems $\bar{\sigma}^{\mathrm{Aut}(\bar{G})}$ is characterized by the element orders p , 3 and 2 of $\bar{\sigma}_1$, $\bar{\sigma}_2$ and $\bar{\sigma}_2^{-1}\bar{\sigma}_1^{-1}$ respectively. Consequently $\bar{N}_{\bar{\sigma}}/\bar{Q}(t)$ is the field of modular functions of level p . The two classes $2A$ and $3A$ are easily seen to be rational, while the class pA is *semirational*, i.e., we

have $pB = (pA)^w$ for any primitive root w modulo p . Thus we have $\mathbb{Q}_C = \mathbb{Q}(\sqrt{p^*})$ with $p^* := (-1)^{(p-1)/2} p$. The Basic Rigidity Theorem now proves that the field of modular functions of level p with its group of automorphism $L_2(p)$ is defined over the field $\mathbb{Q}(\sqrt{p^*}, t)$. \square

The field extensions in the above example will reappear in Paragraph 7. Using rational translates they will be shown to give rise to geometric $L_2(p)$ -extensions over $\mathbb{Q}(t)$ for certain primes p .

6 Geometric Automorphisms

In the rigidity criteria discussed until now, possible fields of definition for Galois extensions are only sought among the intermediate fields of $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$. Smaller fields of definition and hence better results can sometimes be reached by including the *group of geometric automorphisms* $\text{Aut}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$. This allows for all subfields of $\bar{\mathbb{Q}}(t)$ of transcendence degree 1 over \mathbb{Q} to be taken into consideration. The action of geometric automorphisms on the fundamental group can be described explicitly. Thus a numerically verifiable criterion for the existence of fields of definition can be obtained, the so called Twisted Rigidity Theorem. An application of it proves that the small Mathieu groups occur as Galois groups over $\mathbb{Q}(t)$.

6.1 Extension of the Algebraic Fundamental Group

We start again from the algebraic fundamental group

$$\Gamma_s = \text{Gal}(\bar{M}_s/\bar{\mathbb{Q}}(t)) = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle.$$

To extend this group by a group H of geometric automorphisms, we have to require at least that H leaves the set \mathbb{S} stable. Thus we may as well restrict ourselves to considering the group

$$H_{\mathbb{S}} := \{ \eta \in \text{Aut}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}) \mid \mathbb{S}^{\eta} = \mathbb{S} \}. \quad (6.1)$$

Then $H_{\mathbb{S}}$ defines a permutation representation

$$\pi_{\mathbb{S}} : H_{\mathbb{S}} \rightarrow S_s, \quad \eta \mapsto \begin{pmatrix} 1 & \dots & s \\ (1)\eta & \dots & (s)\eta \end{pmatrix}, \quad (6.2)$$

into the symmetric group S_s . For each subgroup V of $\pi_{\mathbb{S}}(H_{\mathbb{S}})$ we obtain an inverse image

$$H_{\mathbb{S}}^V = \{ \eta \in H_{\mathbb{S}} \mid \pi_{\mathbb{S}}(\eta) \in V \}. \quad (6.3)$$

If moreover we assume $s \geq 3$, which by Example 3.1 and Theorem 5.1 is possible without loss of information, then we have:

Proposition 6.1. *For $s \geq 3$ the permutation representation $\pi_{\mathbb{S}}$ of $H_{\mathbb{S}}$ into S_s is faithful. In particular for $V \leq \pi_{\mathbb{S}}(H_{\mathbb{S}})$ we always have*

$$H_{\mathbb{S}}^V \cong V. \quad (6.4)$$

Proof. The assertions in Proposition 6.1 follow from the well known fact that $\text{Aut}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}) \cong \text{PGL}_2(\bar{\mathbb{Q}})$ acts sharply threefold transitively on $\mathbb{P}^1(\bar{\mathbb{Q}})$ and hence on $\mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$. \square

Possible groups of geometric automorphisms $H_{\mathbb{S}}^V$ thus have to be among the finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{Q}})$. The latter are well known from the classical literature:

Theorem 6.2 (Klein (1884)). *Let H be a finite subgroup of $\mathrm{Aut}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}) \cong \mathrm{PGL}_2(\bar{\mathbb{Q}})$. Then we have:*

(a) *H is a finite rotation group, i.e., one of*

$$Z_n, D_n, A_4, S_4, A_5 \quad (n \in \mathbb{N}). \quad (6.5)$$

(b) *At most three prime divisors of $\bar{\mathbb{Q}}(t)^H/\bar{\mathbb{Q}}$ are ramified in $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(t)^H$. The corresponding triples of ramification indices are*

$$(1, n, n), (2, 2, n), (2, 3, 3), (2, 3, 4), (2, 3, 5). \quad (6.6)$$

(c) *The Galois extension $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(t)^H$ is uniquely determined by the three ramification points and the corresponding triple of ramification indices.*

Proof. The Hurwitz genus formula for the field extension $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(t)^H$ with the ramification indices e_1, \dots, e_s forces

$$2(|H| - 1) = \deg(\mathfrak{D}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(t)^H)) = |H| \sum_{i=1}^s \left(1 - \frac{1}{e_i}\right).$$

Interpreting this as a diophantine equation in e_1, \dots, e_s and $|H|$ one first finds that $s \leq 3$ and then that $(e_1, e_2, e_3; |H|)$ can only be one of $(1, n, n; n)$, $(2, 2, n; 2n)$, $(2, 3, 3; 12)$, $(2, 3, 4; 24)$, $(2, 3, 5; 60)$. Thus H is generated by a 3-system

$$(\sigma_1, \sigma_2, \sigma_3) \quad \text{with} \quad \sigma_1^{e_1} = \sigma_2^{e_2} = \sigma_3^{e_3} = 1 \quad \text{and} \quad \sigma_1 \sigma_2 \sigma_3 = 1. \quad (6.7)$$

From these generators and relations an easy calculation, for example with the Todd-Coxeter algorithm, shows that H is one of the groups listed in (a), and moreover that the relations in (6.7) already give a presentation for H .

For (c) it suffices by the Hurwitz classification to prove that in each of the possible groups H there exists precisely one class of generating 3-systems $\sigma^{\mathrm{Aut}(H)}$ of H modulo $\mathrm{Aut}(H)$ with the corresponding element orders. The details for this straightforward calculation are given for example in Matzat (1987), III, §1.3. \square

By the theorem of Lüroth the function field $\bar{\mathbb{Q}}(t)^H/\bar{\mathbb{Q}}$ is rational, say $\bar{\mathbb{Q}}(t)^H = \bar{\mathbb{Q}}(\tilde{t})$. Consequently the above Galois extensions may be identified with Galois extensions inside $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(\tilde{t})$. The following result contains generating s -systems, free up to the product relation, for the corresponding open normal subgroups Ψ of Γ_3 .

Theorem 6.3. *Let $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ be the maximal algebraic Galois extension, unramified outside $\mathbb{S} = \{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$,*

$$\Gamma_3 = \mathrm{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)) = \langle \gamma_1, \gamma_2, \gamma_3 \mid \gamma_1 \gamma_2 \gamma_3 = 1 \rangle,$$

and $\bar{N}_V/\bar{\mathbb{Q}}(t)$ the rational intermediate field of $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ corresponding to the finite rotation group V according to Theorem 6.2. Then for $\Psi_V := \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{N}_V)$ we have:

$$(a) \quad \Psi_{Z_n} = \langle \gamma_1, \gamma_1^{\gamma_2^{-1}}, \dots, \gamma_1^{\gamma_2^{1-n}}, \gamma_2^n, \gamma_3^n \mid \gamma_1 \gamma_1^{\gamma_2^{-1}} \cdots \gamma_3^n = 1 \rangle. \quad (6.8)$$

$$(b) \quad \Psi_{D_n} = \langle \gamma_1^2, (\gamma_1^2)^{\gamma_2^{-1}\gamma_1}, \dots, (\gamma_1^2)^{(\gamma_2^{-1}\gamma_1)^{n-1}}, \gamma_2^2, (\gamma_2^2)^{\gamma_2^{-1}\gamma_3^{-1}\gamma_2}, \dots, \\ (\gamma_2^2)^{(\gamma_2^{-1}\gamma_3^{-1}\gamma_2)^{n-1}}, (\gamma_3^n)^{\gamma_2}, \gamma_3^n \mid \gamma_1^2(\gamma_1^2)^{\gamma_2^{-1}\gamma_1} \cdots \gamma_3^n = 1 \rangle \quad (6.9)$$

(c) For $V = A_4, S_4, A_5$ the group Ψ_V possesses a free generating s -system of length $s = 14, 26, 62$ respectively.

Proof. First let $V = Z_n$. The two prime divisors $\mathfrak{P}_2, \mathfrak{P}_3$ both have ramification order n , so $\Psi_V \cap \langle \gamma_i \rangle$ is generated by γ_i^n for $i = 2, 3$. The prime divisor \mathfrak{P}_1 completely decomposes in $\bar{N}_V/\bar{\mathbb{Q}}(t)$. The inertia groups of prime divisors of \mathfrak{P}_1 in \bar{N}_V are hence obtained by $\langle \gamma_1^\eta \rangle$, where η runs through a full system of representatives of Γ_3/Ψ_V , for example $\eta = \gamma_2^{-i}$ with $i = 0, \dots, n-1$. With this choice the product relation is obviously satisfied. Now Ψ_V , being a subgroup of index n in a free group of rank 2, is also free of rank $r = n+1$, so no further relations exist between these generators, and $(\gamma_1, \gamma_1^{\gamma_2^{-1}}, \dots, \gamma_3^n)$ constitutes a free generating $(n+2)$ -system of Ψ_V . In a completely similar way it is shown that (b) gives a free generating $(2n+2)$ -system of Ψ_V for $V = D_n$. The corresponding free generating s -systems for A_4, S_4 and A_5 are not reproduced here on account of their size. \square

6.2 The Action of Geometric Automorphisms

If $V \leq \pi_{\mathbb{S}}(H_{\mathbb{S}})$ then by definition the geometric automorphisms $\eta \in H_{\mathbb{S}}^V$ extend to automorphisms of $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}$. These act as outer automorphisms on $\Gamma_s = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t))$. Explicit formulae for the images of $[\gamma] = (\gamma_1, \dots, \gamma_s)^{\text{Inn}(\Gamma_s)}$ under this action can easily be derived from Theorem 6.3. This is achieved for $s = 3$ and $s = 4$ in this section.

Theorem 6.4. Let $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ denote the maximal algebraic Galois extension unramified outside $\mathbb{S} = \{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$ with

$$\Gamma_3 = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)) = \langle \gamma_1, \gamma_2, \gamma_3 \mid \gamma_1 \gamma_2 \gamma_3 = 1 \rangle.$$

Then $H_{\mathbb{S}} \cong S_3$ is independent of the choice of \mathbb{S} . For the preimages $\eta_i \in H_{\mathbb{S}}$ of generating elements $\omega_2 = (12)$ and $\omega_3 = (123)$ of S_3 we have:

$$[\gamma_1, \gamma_2, \gamma_3]^{\eta_2} = [\gamma_2, \gamma_1, \gamma_2 \gamma_3 \gamma_2^{-1}], \quad (6.10)$$

$$[\gamma_1, \gamma_2, \gamma_3]^{\eta_3} = [\gamma_2, \gamma_3, \gamma_1]. \quad (6.11)$$

Proof. The isomorphism $H_{\mathbb{S}} \cong S_3$ follows from the threefold transitive action of $\text{Aut}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$ on $\mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$. Now first let $V = \langle \omega_2 \rangle$, $\bar{\mathbb{Q}}(\tilde{t})$ be the fixed field of $H_{\mathbb{S}}^V$ and

$$\tilde{\Gamma}_3 := \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(\tilde{t})) = \langle \tilde{\gamma}_1, \tilde{\gamma}_2, \tilde{\gamma}_3 \mid \tilde{\gamma}_1 \tilde{\gamma}_2 \tilde{\gamma}_3 = 1 \rangle$$

be the Galois group of the maximal algebraic Galois extension unramified outside $\mathfrak{P}_1 := \mathfrak{P}_1|_{\bar{\mathbb{Q}}(\tilde{t})}$, $\mathfrak{P}_2 := \mathfrak{P}_3|_{\bar{\mathbb{Q}}(\tilde{t})}$ and the second prime divisor $\mathfrak{P}_3 \in \mathbb{P}(\bar{\mathbb{Q}}(\tilde{t})/\bar{\mathbb{Q}})$ ramified in $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(\tilde{t})$. According to Theorem 6.3(a) $\bar{\mathbb{Q}}(t)$ is the fixed field of

$$\tilde{\Psi}_V = \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2, \tilde{\gamma}_3^2 \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^2 \tilde{\gamma}_3^2 = 1 \rangle.$$

The prime divisor \mathfrak{P}_3 is unramified in $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$, hence we obtain Γ_3 from $\tilde{\Psi}_V$ by addition of the relation $\tilde{\gamma}_3^2 = 1$:

$$\Gamma_3 \cong \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^2 = 1 \rangle.$$

This allows us to identify $\gamma_1 = \tilde{\gamma}_1$, $\gamma_2 = \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}$ and $\gamma_3 = \tilde{\gamma}_2^2$, and then η_2 is the outer automorphism of Γ_3 induced by $\tilde{\gamma}_3 = \tilde{\gamma}_1 \tilde{\gamma}_2 = \tilde{\gamma}_2^{-1} \tilde{\gamma}_1^{-1}$. Hence we have

$$[\gamma]^{\eta_2} = [\tilde{\gamma}_1^{\tilde{\gamma}_2}, \tilde{\gamma}_1^{\tilde{\gamma}_2^{-2} \tilde{\gamma}_1^{-1}}, (\tilde{\gamma}_2^2)^{\tilde{\gamma}_1^{-1}}] = [\gamma_2^{\gamma_3}, \gamma_1^{\gamma_3^{-1} \gamma_1^{-1}}, \gamma_3^{\gamma_1^{-1}}],$$

which upon conjugation by $\gamma_3^{-1} \gamma_2^{-2}$ yields formula (6.10).

Now let $V = \langle \omega_3 \rangle$, $\bar{\mathbb{Q}}(\tilde{t}) := \bar{\mathbb{Q}}(t)^{H_{\mathbb{S}}^V}$ and $\tilde{\Gamma}_3 = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(\tilde{t}))$ the Galois group of the maximal algebraic Galois extension unramified outside $\mathfrak{P}_1 := \mathfrak{P}_1|_{\bar{\mathbb{Q}}(\tilde{t})}$ and the two prime divisors \mathfrak{P}_2 and \mathfrak{P}_3 ramified in $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(\tilde{t})$. Again by Theorem 6.3(a) we have that $\bar{\mathbb{Q}}(t)$ is the fixed field of

$$\tilde{\Psi}_V = \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2}, \tilde{\gamma}_2^3, \tilde{\gamma}_3^3 \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^3 \tilde{\gamma}_3^3 = 1 \rangle.$$

From this we obtain Γ_3 by addition of the relations $\tilde{\gamma}_2^3 = 1$ and $\tilde{\gamma}_3^3 = 1$, hence

$$\Gamma_3 \cong \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2} \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^3 \tilde{\gamma}_2^{-3} = 1 \rangle.$$

With $\gamma_1 = \tilde{\gamma}_1$, $\gamma_2 = \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}$, $\gamma_3 = \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2}$ and $\eta_3 = \tilde{\gamma}_2^{-1}$ we thus obtain

$$[\gamma]^{\eta_3} = [\tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2}, \tilde{\gamma}_2^3 \tilde{\gamma}_1 \tilde{\gamma}_2^{-3}] = [\gamma_2, \gamma_3, \gamma_1],$$

proving (6.11). \square

In the case $s = 4$ not all subgroups of the symmetric group S_4 occur as images of $H_{\mathbb{S}}$, since \mathbb{S} has to consist of full $H_{\mathbb{S}}$ -orbits, while for example the group S_4 can be seen to have only orbits of lengths 6, 8, 12 and 24 on $\mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$. The remaining possibilities for $s = 4$ are collected in the following theorem. Here the 4-cycle ω_4 is chosen such that together with ω_2 it generates the dihedral group D_4 of order 8.

Theorem 6.5. Let $\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)$ be the maximal Galois extension unramified outside $\mathbb{S} = \{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_4\}$ with

$$\Gamma_4 = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(t)) = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \mid \gamma_1 \gamma_2 \gamma_3 \gamma_4 = 1 \rangle.$$

Then any subgroup V of $\pi_{\mathbb{S}}(H_{\mathbb{S}})$ is conjugate in S_4 to a subgroup of $A_4 = \langle \omega_3, \omega_4^2 \rangle$ or $D_4 = \langle \omega_2, \omega_4 \rangle$ with $\omega_2 = (12)$, $\omega_3 = (123)$ and $\omega_4 = (1324)$. For the preimages $\eta_i \in H_{\mathbb{S}}$ of these generating elements ω_i we have, independently of the choice of \mathbb{S} :

$$[\gamma_1, \gamma_2, \gamma_3, \gamma_4]^{\eta_2} = [\gamma_2, \gamma_3 \gamma_1 \gamma_3^{-1}, \gamma_3, \gamma_1^{-1} \gamma_4 \gamma_1], \quad (6.12)$$

$$[\gamma_1, \gamma_2, \gamma_3, \gamma_4]^{\eta_3} = [\gamma_2, \gamma_3, \gamma_1, \gamma_1^{-1} \gamma_4 \gamma_1], \quad (6.13)$$

$$[\gamma_1, \gamma_2, \gamma_3, \gamma_4]^{\eta_4} = [\gamma_3, \gamma_1^{-1} \gamma_4 \gamma_1, \gamma_2, \gamma_3 \gamma_1 \gamma_3^{-1}]. \quad (6.14)$$

Proof. The proof is entirely analogous to the one for Theorem 6.4, so we restrict ourselves to computing the example with η_4 , which has not been treated in the literature. Let $V = \langle \omega_4 \rangle$, $\bar{\mathbb{Q}}(\tilde{t}) = \bar{\mathbb{Q}}(t)^{H_{\mathbb{S}}^V}$ and $\tilde{\Gamma}_4 = \text{Gal}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}}(\tilde{t}))$ be the Galois group of the maximal algebraic Galois extension unramified outside $\tilde{\mathfrak{P}}_1 := \mathfrak{P}_1|_{\bar{\mathbb{Q}}(\tilde{t})}$ and the two prime divisors $\tilde{\mathfrak{P}}_2, \tilde{\mathfrak{P}}_3$ ramified in $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(\tilde{t})$. Then by Theorem 6.3 the field $\bar{\mathbb{Q}}(t)$ is the fixed field of

$$\tilde{\Gamma}_V = \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2}, \tilde{\gamma}_2^3 \tilde{\gamma}_1 \tilde{\gamma}_2^{-3}, \tilde{\gamma}_2^4, \tilde{\gamma}_3^4 \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^4 \tilde{\gamma}_2^4 = 1 \rangle.$$

The group Γ_4 is obtained from this by addition of the two relations $\tilde{\gamma}_2^4 = 1$ and $\tilde{\gamma}_3^4 = 1$, so we get

$$\Gamma_4 = \langle \tilde{\gamma}_1, \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}, \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^2, \tilde{\gamma}_2^3 \tilde{\gamma}_1 \tilde{\gamma}_2^{-3} \mid (\tilde{\gamma}_1 \tilde{\gamma}_2)^4 \tilde{\gamma}_2^{-4} = 1 \rangle.$$

As $\omega_4 = (1324)$, a good choice of generators is $\gamma_1 = \tilde{\gamma}_1$, $\gamma_3 = \tilde{\gamma}_2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-1}$, $\gamma_3^{-1} \gamma_2 \gamma_3 = \tilde{\gamma}_2^2 \tilde{\gamma}_1 \tilde{\gamma}_2^{-2}$ and $\gamma_4 = \tilde{\gamma}_2^3 \tilde{\gamma}_1 \tilde{\gamma}_2^{-3}$. With $\eta_4 = \tilde{\gamma}_2^{-1}$ we obtain

$$[\gamma_1, \gamma_3, \gamma_2^{\gamma_3}, \gamma_4]^{\eta_4} = [\gamma_3, \gamma_2^{\gamma_3}, \gamma_4, \gamma_1],$$

and hence

$$[\gamma] = [\gamma_3, \gamma_4^{\gamma_1 \gamma_3}, \gamma_2^{\gamma_3}, \gamma_1] = [\gamma_3, \gamma_1^{-1} \gamma_4 \gamma_1, \gamma_2, \gamma_3 \gamma_1 \gamma_3^{-1}]. \quad \square$$

Variants of the proofs of Theorems 6.4 and 6.5, in which the images of embedded homotopy classes of paths are determined topologically, are contained in Matzat (1987), Ch. III, §1, for example.

6.3 Rigid Orbits

Extending $\eta \in H_{\mathbb{S}}$ to $\tilde{\eta} \in \text{Aut}(\bar{M}_{\mathbb{S}}/\bar{\mathbb{Q}})$ we obtain analogously to (4.8) via

$$\Sigma_s(G) \times H_{\mathbb{S}} \rightarrow \Sigma_s(G), \quad (\sigma, \tilde{\eta}) \mapsto \sigma \cdot \tilde{\eta} := \sigma^{\tilde{\eta}^{-1}} \text{ with } \sigma^{\tilde{\eta}} = \psi_{\sigma}(\gamma^{\tilde{\eta}}) \quad (6.15)$$

an action of $\tilde{\eta}$ on $\Sigma_s(G)$, respectively of η on $\Sigma_s(G)/\text{Inn}(G)$. For this we obviously have:

Proposition 6.6. *Let $\mathbf{C} \in \text{Cl}(G)^s$ be a class vector of G and V a symmetry group of \mathbf{C} . Then via (6.15) $H_{\mathbf{s}}^V$ acts on $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$. For the inverse action $[\sigma] \mapsto [\sigma]^\eta$, the formulae for the generating elements $\eta_i \in H_{\mathbf{s}}^V$ carry over unchanged from $[\gamma]$ to $[\sigma] = [\psi_\sigma(\gamma)]$.*

In the case where $H_{\mathbf{s}}^V \cong V$ this action now splits $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ into $H_{\mathbf{s}}^V$ -orbits. Their number shall be denoted by $l^V(\mathbf{C})$. This notation generalizes the previously introduced $l(\mathbf{C}) = l^1(\mathbf{C})$ for the trivial symmetry group 1. The orbits may differ by the type of their stabilizers

$$H_\sigma^V := \{\eta \in H_{\mathbf{s}}^V \mid [\sigma]^\eta = [\sigma]\}. \quad (6.16)$$

For $U \leq H_{\mathbf{s}}^V$ we now define

$$l_U^V(\mathbf{C}) := | \{ [\sigma]^{H_{\mathbf{s}}^V} \mid \sigma \in \Sigma(\mathbf{C}), H_\sigma^V = U^\alpha \text{ for an } \alpha \in \text{Aut}(H_{\mathbf{s}}^V) \} | \quad (6.17)$$

to be the number of such orbits with stabilizer equal to U up to an automorphism of $H_{\mathbf{s}}^V \cong V$. The class equation then yields:

Proposition 6.7. *Let \mathbf{U} be a system of representatives of subgroups of V modulo $\text{Aut}(V)$. Then for each class vector \mathbf{C} of G we have*

$$l^V(\mathbf{C}) = \sum_{U \in \mathbf{U}} l_U^V(\mathbf{C}), \quad l(\mathbf{C}^V) = \sum_{U \in \mathbf{U}} (V : U) l_U^V(\mathbf{C}). \quad (6.18)$$

Those orbits with $l_{H_\sigma^V}^V(\mathbf{C}) = 1$ are characterized inside $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ by their stabilizer H_σ^V . These are of particular interest and will be called *rigid $H_{\mathbf{s}}^V$ -orbits*. In the case where $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ consists of just one single $H_{\mathbf{s}}^V$ -orbit, \mathbf{C} will also be called a *V -rigid class vector*. The next theorem will show that this is a suitable generalization of the rigidity property for a class vector defined in Section 4.2. For this we extend $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ to

$$\Delta_{\mathbf{s}}^V := \langle \Delta, H_{\mathbf{s}}^V \rangle \leq \text{Aut}(\bar{\mathbb{Q}}(t)/\mathbb{Q}), \quad (6.19)$$

and denote the stabilizer of $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ in this group by

$$\Delta_\sigma^V := \{ \delta \in \Delta_{\mathbf{s}}^V \mid [\sigma]^\delta = [\sigma] \} \quad (6.20)$$

analogously to (4.19).

For brevity we call a subset $\mathbb{S} \subseteq \mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$ of cardinality s a *V -configuration* for $V \leq S_s$, if $\pi_{\mathbf{s}}(\Delta)$ is contained in V and if moreover we have $H_{\mathbf{s}}^V \cong V$. According to Theorems 6.4 and 6.5 such configurations exist for example in the case $s = 3$ for all $V \leq S_3$ and in the case $s = 4$ for all $V \leq A_4$ and $V \leq D_4$.

Theorem 6.8. Let $\mathbf{C} \in \text{Cl}(G)^s$ be a class vector of the finite group G , V a symmetry group of \mathbf{C} and \mathbb{S} a V -configuration. Furthermore, for $\sigma \in \Sigma(\mathbf{C})$ let K_σ^V denote the fixed field of Δ_σ^V and k_σ^V the algebraic closure of \mathbb{Q} in K_σ^V . Then we have

$$[k_\sigma^V : \mathbb{Q}_\mathbf{C}^V] \leq l_{H_\sigma^V}^V(\mathbf{C}). \quad (6.21)$$

In particular $K_\sigma^V / \mathbb{Q}_\mathbf{C}^V$ is regular if $[\sigma]^{H_\mathbf{S}^V}$ is rigid.

Proof. According to $\pi_\mathbf{S}(\Delta) \leq V$, for each $\delta \in \Delta_\mathbf{S}^V$ we have $\omega := \pi_\mathbf{S}(\delta) \in V$. Hence for each $\delta \in \Delta_\sigma^V$ we have $\mathbf{C}^{c(\delta)} = \mathbf{C}^{\omega^{-1}} \in \mathbf{C}^V$ since $\mathbf{C}^\delta = \mathbf{C}$, which implies $\delta \in \tilde{\Delta}_\mathbf{C}^V := \langle \Delta_\mathbf{C}^V, H_\mathbf{S}^V \rangle$, with $\Delta_\mathbf{C}^V = \{\delta \in \Delta \mid \mathbf{C}^{c(\delta)} \in \mathbf{C}^V\}$ from (4.24).

Now $H_\mathbf{S}^V$ is normal in $\tilde{\Delta}_\mathbf{C}^V$, so $\delta \in \tilde{\Delta}_\mathbf{C}^V$ maps the class of generating systems $[\sigma] \in \Sigma(\mathbf{C}^V) / \text{Inn}(G)$ onto $[\sigma]^\delta \in \Sigma(\mathbf{C}^V) / \text{Inn}(G)$, where moreover $H_{\sigma^\delta}^V = (H_\sigma^V)^{\delta^{-1}}$ is the image of H_σ^V under an automorphism of $H_\mathbf{S}^V$. Hence with $\tilde{K}_\mathbf{C}^V := \bar{\mathbb{Q}}(t)^{\tilde{\Delta}_\mathbf{C}^V}$ we have

$$[K_\sigma^V : \tilde{K}_\mathbf{C}^V] = (\tilde{\Delta}_\mathbf{C}^V : \Delta_\sigma^V) \leq (H_\mathbf{S}^V : H_\sigma^V) l_{H_\sigma^V}^V(\mathbf{C}).$$

The extension $\tilde{K}_\mathbf{C}^V / \mathbb{Q}_\mathbf{C}^V$ is regular, so as $\bar{\mathbb{Q}} K_\sigma^V = \bar{\mathbb{Q}}(t)^{H_\sigma^V}$ this proves the estimate

$$[k_\sigma^V : \mathbb{Q}_\mathbf{C}^V] = \frac{[K_\sigma^V : \tilde{K}_\mathbf{C}^V]}{[\bar{\mathbb{Q}} K_\sigma^V : \bar{\mathbb{Q}} \tilde{K}_\mathbf{C}^V]} = \frac{(\tilde{\Delta}_\mathbf{C}^V : \Delta_\sigma^V)}{(H_\mathbf{S}^V : H_\sigma^V)} \leq l_{H_\sigma^V}^V(\mathbf{C}).$$

In the case of a rigid $H_\mathbf{S}^V$ -orbit $l_{H_\sigma^V}^V(\mathbf{C})$ equals 1, and so $K_\sigma^V / \mathbb{Q}_\mathbf{C}^V$ is regular. \square

Hence if $[\sigma]$ belongs to a rigid $H_\mathbf{S}^V$ -orbit, the general estimate $[k_\sigma : \mathbb{Q}_\mathbf{C}^V] \leq l(\mathbf{C})$ from Theorem 4.10 may be improved by the much better estimate $[k_\sigma^V : \mathbb{Q}_\mathbf{C}^V] \leq l_{H_\sigma^V}^V(\mathbf{C})$. But unfortunately the corresponding fixed field K_σ^V is not always a rational function field and therefore in general does not allow us to construct Galois extensions over $k_\sigma^V(t)$ and k_σ^V .

6.4 The Twisted Rigidity Theorem

The rationality of K_σ^V / k_σ^V can be guaranteed under a relatively simple additional hypothesis.

Proposition 6.9. The fixed field K_σ^V of Δ_σ^V is a rational function field over k_σ^V if V possesses an orbit of odd length in $\{1, \dots, s\}$.

Proof. The elements $\delta \in \Delta_\sigma^V$ can only permute prime divisors of $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}$ lying in the same $H_\mathbf{S}^V$ -orbit. Thus by the assumption, K_σ^V / k_σ^V possesses a prime divisor of odd degree, and it has genus 0, being a subfield of $\bar{\mathbb{Q}}(t)$. Hence (see Artin (1967), Ch. 16, Thm. 7) K_σ^V / k_σ^V is a rational function field. \square

Remark. In the case $H_\sigma^V \neq 1$ it suffices in Proposition 6.9 to assume that H_σ^V possesses an orbit of odd length on the set of prime divisors in \mathbb{S} restricted to $\bar{K}_\sigma^V := \bar{\mathbb{Q}}(t)^{H_\sigma^V}$.

From Theorem 6.8 we thus obtain the Twisted Rigidity Theorem in the following formulation:

Theorem 6.10 (Twisted Rigidity Theorem). *Let G be a finite group with trivial center, $\mathbf{C} \in \text{Cl}(G)^s$ a class vector with $s \geq 3$ and V a symmetry group of \mathbf{C} having an orbit of odd length and a V -configuration \mathbb{S} . If $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ contains a rigid H_σ^V -orbit, then there exists a geometric Galois extension $N/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ with*

$$\text{Gal}(N/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})) \cong G. \quad (6.22)$$

If moreover the class vector \mathbf{C} is V -symmetric, then we have $\mathbb{Q}_{\mathbf{C}}^V = \bar{\mathbb{Q}}$.

Proof. Let $[\sigma]$ be an element in the rigid H_σ^V -orbit in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ which exists by assumption. Then by Theorem 6.8 and Proposition 6.9 the fixed field K_σ^V is a rational function field over $\mathbb{Q}_{\mathbf{C}}^V$, say $K_\sigma^V = \mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$. As in Proposition 4.6 we obtain that $\bar{N}_\sigma/K_\sigma^V$ is Galois, and each automorphism of $\bar{N}_\sigma/K_\sigma^V$ acts as an inner automorphism on $G = \text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$. Now as $\mathcal{L}(G) = 1$ it follows from Proposition 3.7 that $K_\sigma^V = \mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ constitutes a field of definition of $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$. \square

Remark. In the case $H_\sigma^V = 1$ extension of constants of $N/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ by $\bar{\mathbb{Q}}$ in the Twisted Rigidity Theorem leads to the Galois extension $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$, while in the case $H_\sigma^V \neq 1$ we arrive at a Galois extension $\bar{\mathbb{Q}}N/\bar{\mathbb{Q}}(\tilde{t})$ with $\bar{\mathbb{Q}}N \neq \bar{N}_\sigma$. The translation occurring in this case will be studied in detail in the next paragraph.

In the final section we apply the Twisted Rigidity Theorem to realize the small Mathieu groups as Galois groups.

6.5 Geometric Galois Extensions over $\mathbb{Q}(t)$ with M_{12} and M_{11}

The Mathieu group M_{12} possesses two conjugacy classes $4A$ and $4B$ of elements of order 4, and one, denoted $10A$, of elements of order 10. Here $4A$ denotes the class of double 4-cycles in a given faithful permutation representation π of M_{12} of degree 12. With respect to this same permutation representation the elements of order ten consist of the disjoint product of a 10-cycle and a transposition (Conway et al. (1985)).

Proposition 6.11. *The class vector $\mathbf{C} = (4A, 4A, 10A)$ of M_{12} is rational, and with $V = \langle (12) \rangle$ we have*

$$l(\mathbf{C}) = 2 \quad \text{and} \quad l^V(\mathbf{C}) = 1. \quad (6.23)$$

So the class vector \mathbf{C} is rationally V -rigid.

Proof. The classes $4A$ and $10A$ of M_{12} are rational, so by definition \mathbf{C} is rational class vector (see the Atlas of Conway et al. (1985)). Furthermore, from the character table of M_{12} one calculates the normalized structure constant according to Theorem 5.8

$$\begin{aligned} n(\mathbf{C}) &= \frac{|G|}{|\mathcal{C}_G(\sigma_1)|^2 |\mathcal{C}_G(\sigma_3)|} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(\sigma_1)^2 \chi(\sigma_3)}{\chi(1)} \\ &= \frac{95040}{32^2 10} \left(1 - \frac{9}{11} - \frac{1}{11} + \frac{4}{54} + \frac{4}{66} - \frac{1}{99}\right) = 2. \end{aligned}$$

Now let $\sigma \in \bar{\Sigma}(\mathbf{C})$ and $U := \langle \sigma \rangle$. Then U contains elements of order 10, and according to the list of maximal subgroups of M_{12} in the Group Atlas either we have $U = M_{12}$ or U is contained in one of the two maximal subgroups of M_{12} of type $M_{10} \rtimes Z_2$ or $Z_2 \times S_5$.

The group M_{12} contains two conjugacy classes of maximal subgroups $M_{10} \rtimes Z_2$. Those in the first class act intransitively in the permutation representation π , with orbits of lengths 10 and 2, while those in the second class act transitively. But the relation $\sigma_1 \sigma_2 \sigma_3 = 1$ together with the permutation types $(4)^2(1)^4$ and $(10)(2)$ of the elements σ_1, σ_2 and σ_3 respectively is not compatible with an intransitive action of type $(10)(2)$, so the first possibility can be excluded. Next the outer automorphism group of M_{12} has order 2, and any non-trivial outer automorphism α exchanges the two classes of maximal subgroups $M_{10} \rtimes Z_2$, as well as the conjugacy classes $4A$ and $4B$. In the representation π , the latter class consists of elements of type $(4)^2(2)^2$. Hence by first applying α we may again argue as above with the product relation and the permutation types to exclude the second class of subgroups $M_{10} \rtimes Z_2$ as well.

If U were contained in $Z_2 \times S_5$, then the projection p_1 of U onto the first factor $Z_2 \cong \langle \tau \rangle$ would have to be surjective. Since $p_1(\sigma_3) = \tau$ and $p_1(\sigma_1)p_1(\sigma_2)p_1(\sigma_3) = 1$ this would imply $\{p_1(\sigma_1), p_1(\sigma_2)\} = \{1, \tau\}$. In any case, σ_1 and σ_2 would lie in different conjugacy classes of 4-elements in $Z_2 \times S_5$. The permutation character for such a subgroup shows that it intersects both classes $4A$ and $4B$ of 4-elements in M_{12} . But $Z_2 \times S_5$ has just two classes of 4-elements, so one of these has to fuse into $4B$. Thus by our above observation also one of σ_1, σ_2 would have to lie in class $4B$, contradicting the choice of the class vector $(4A, 4A, 10A)$.

We have now proved that $\bar{\Sigma}(\mathbf{C}) = \Sigma(\mathbf{C})$, which together with Corollary 5.6 yields $l(\mathbf{C}) = n(\mathbf{C}) = 2$. Now assume that $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ is a fixed point under the generating element $\eta_2 \in H_{\mathbf{s}}^V$. Then by (6.10) there exists $\tau \in M_{12}$ with $\sigma^\tau = (\sigma_2, \sigma_1, \sigma_2 \sigma_3 \sigma_2^{-1})$. Since this implies $\sigma_1^{\tau^2} = \sigma_1$ and $\sigma_2^{\tau^2} = \sigma_2$, so that τ centralizes all of M_{12} , we conclude that $\tau^2 = 1$. Setting $\tau_3 := (\tau \sigma_2)^{-1}$ this would mean $\tau_3^2 = (\sigma_2^{-1} \tau^{-1})^2 = \sigma_2^{-1} \sigma_1^{-1} = \sigma_3$, contradicting the fact that M_{12} contains no elements of order 20. Hence the two classes of generating systems in $\Sigma(\mathbf{C})/\text{Inn}(G)$ lie in a single $H_{\mathbf{s}}^V$ -orbit, and we have $l^V(\mathbf{C}) = 1$. \square

The argument for the non-trivial action given at the end of the proof is a special case of the Fixed Point Theorem in Section 7.1. From the above proposition and the

Twisted Rigidity Theorem we already obtain the first half of

Theorem 6.12. *The Mathieu groups M_{12} and M_{11} possess G -realizations over \mathbb{Q} .*

Proof. By Proposition 6.11 and Theorem 6.10 there exists a geometric Galois extension $N/\mathbb{Q}(\tilde{t})$ with $\text{Gal}(N/\mathbb{Q}(\tilde{t})) \cong M_{12}$ belonging to the class vector $(4A, 4A, 10A)$. The permutation representation π introduced at the beginning of this section is induced by the permutation action on the cosets of an (intransitive) maximal subgroup of type M_{11} . Denote the fixed field of such a subgroup by L . Then three prime divisors $\mathfrak{P}_i \in \mathbb{P}(\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}})$ are ramified in $\bar{\mathbb{Q}}L/\bar{\mathbb{Q}}(t)$ (where we have $\bar{\mathbb{Q}}(t) = \bar{\mathbb{Q}}(\tilde{t})$). According to the cycle decompositions for generators of inertia groups $\sigma_1, \sigma_2 \in 4A$ and $\sigma_3 \in 10A$ the ramification behavior of these is given by

$$\mathfrak{P}_i = \mathfrak{Q}_{i,1}^4 \mathfrak{Q}_{i,2}^4 \mathfrak{Q}_{i,3} \mathfrak{Q}_{i,4} \mathfrak{Q}_{i,5} \mathfrak{Q}_{i,6} \quad \text{for } i = 1, 2, \quad \mathfrak{P}_3 = \mathfrak{Q}_{3,1}^{10} \mathfrak{Q}_{3,2}^2. \quad (6.24)$$

(The underlying result will be shown in Section 9.1.) So the different $\mathfrak{D}(\bar{\mathbb{Q}}L/\bar{\mathbb{Q}}(t))$ is of degree 22, and by the Hurwitz genus formula one calculates the genus

$$g(\bar{\mathbb{Q}}L/\bar{\mathbb{Q}}) = 1 - [\bar{\mathbb{Q}}L : \bar{\mathbb{Q}}(t)] + \frac{1}{2} \deg(\mathfrak{D}(\bar{\mathbb{Q}}L/\bar{\mathbb{Q}}(t))) = 0.$$

Hence L/\mathbb{Q} also has genus 0. Since moreover $\mathfrak{Q}_{3,1}$ cannot split in $\bar{\mathbb{Q}}L/L$, its restriction $\mathfrak{Q}_{3,1}|_L$ is a prime divisor of degree 1. This proves that L/\mathbb{Q} is a rational function field, and $\text{Gal}(N/L)$ provides a G -realization of the Mathieu group M_{11} . \square

Remark. By (6.24) the class vector belonging to the geometric M_{11} -extension constructed above, according to the Hurwitz classification, consists of eight components $4A$ and one component $5A$ in M_{11} .

We shall return to the automorphism group $\text{Aut}(M_{12})$ and to the other sporadic groups in Chapter II.9.

7 Rational Translates of Galois Extensions

If a Galois extension $\bar{N}/\bar{\mathbb{Q}}(t)$ is translated via the translation theorem of Galois theory, then in general the corresponding class vector will change. For example, such a translation can sometimes be employed to construct class vectors (resp. orbits) which are rationally rigid with respect to a symmetry group from rigid class vectors (resp. orbits). We give here some theorems to illustrate this phenomenon. These will finally be applied to the linear groups $L_2(p)$.

7.1 Galois Rational Translates

Before treating the general case, we first consider rational translates with a Galois extension. Here rational translate means that the field used for translation is a rational function field. Thanks to this condition, the possible translation fields are those originating from a finite rotation group as classified in Theorem 6.2. The following result can be read off almost immediately from Theorem 6.3.

Proposition 7.1. *Let G be a finite group, $\sigma \in \Sigma_3(G)$, and $\bar{N}_\sigma \in \bar{\mathbf{N}}_{\mathbb{S}}(G)$ the corresponding field extension with group $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t)) \cong G$. Furthermore let $\bar{\mathbb{Q}}(u) = \bar{N}_V \in \bar{\mathbf{N}}_{\mathbb{S}}(V)$ be the rational function field belonging to the finite rotation group V , which we assume to be linearly disjoint from \bar{N}_σ . If now \mathbb{T} denotes the set of prime divisors over \mathbb{S} in $\bar{\mathbb{Q}}(u)$, then we have*

$$\bar{N}_\sigma(u) = \bar{N}_\tau \in \bar{\mathbf{N}}_{\mathbb{T}}(G) \quad \text{with} \quad \tau = \varphi_V(\sigma), \quad (7.1)$$

where φ_V is defined by the free generating s -system $\varphi_V(\gamma)$ of Ψ_V given in Theorem 6.3.

Proof. The proof results from Theorem 6.3 by identifying the initial group G for the Hurwitz classification over $\bar{\mathbb{Q}}(t)$ and over $\bar{\mathbb{Q}}(u)$. We then have

$$\ker(\tau) = \ker(\sigma) \cap \Psi_V. \quad \square$$

Now φ_V maps $\Sigma_3(G)/\text{Inn}(G)$ bijectively onto the subset of V -invariant generating systems in $\Sigma_r(G)$ with $r = |\mathbb{T}|$. This leads to the following generalization of the fixed point theorems in Matzat (1987), III, §2.4:

Theorem 7.2 (Fixed Point Theorem). *Let G be a finite group with trivial center and V a finite rotation group having no common non-trivial factor group with G . Then the map*

$$\varphi_V : \Sigma_3(G)/\text{Inn}(G) \rightarrow \Sigma_r(G)/\text{Inn}(G), \quad [\sigma] \mapsto [\varphi_V(\sigma)], \quad (7.2)$$

defined in (7.1) is injective. The image of φ_V consists precisely of the $H_{\mathbb{T}}^V$ -invariant classes of generating systems $[\tau] \in \Sigma_r(G)/\text{Inn}(G)$.

Proof. Without loss of generality we may assume that $\$$ consists of the support of (t) and $(t-1)$. Now G and V have no non-trivial factor group in common so the fields \bar{N}_σ and \bar{N}_V are necessarily linearly disjoint over $\bar{\mathbb{Q}}(t)$ for all $\sigma \in \Sigma_3(G)$. This implies that $\text{Gal}(\bar{N}_\tau/\bar{\mathbb{Q}}(u)) \cong G$ for $\tau = \varphi_V(\sigma)$ and

$$G_V := \text{Gal}(\bar{N}_\tau/\bar{\mathbb{Q}}(t)) \cong G \times V. \quad (7.3)$$

Since $\mathcal{Z}(G) = 1$, the field \bar{N}_σ is uniquely determined by \bar{N}_τ as the fixed field of $\mathcal{C}_{G_V}(G) \cong V$. So if $\bar{N}_\sigma \neq \bar{N}_{\tilde{\sigma}}$ are different, then we also have $\bar{N}_\tau \neq \bar{N}_{\tilde{\tau}}$. This proves the injectivity of φ_V first on $\Sigma_3(G)/\text{Aut}(G)$, and then since

$$[\varphi_V(\sigma^\alpha)] = [\varphi_V(\sigma)]^\alpha \quad \text{for } \alpha \in \text{Aut}(G) \quad (7.4)$$

also on $\Sigma_3(G)/\text{Inn}(G)$.

By construction, the set \mathbf{T} is a V -configuration. As the extensions of $\eta \in H_{\mathbf{T}}^V = \text{Gal}(\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t))$ act as inner automorphisms on $\text{Gal}(\bar{N}_\tau/\bar{\mathbb{Q}}(u)) \cong G$ by (7.3), the class $[\tau] = [\varphi_V(\sigma)]$ is invariant under $H_{\mathbf{T}}^V$ according to (4.5), and we have $H_\tau^V = H_{\mathbf{T}}^V \cong V$. Conversely, given $\tau \in \Sigma_r(G)$ with $H_\tau^V = H_{\mathbf{T}}^V$, then $\bar{\mathbb{Q}}(t)$ is a field of definition of $\bar{N}_\tau/G\bar{\mathbb{Q}}(u)$. Hence for the corresponding Galois extension $\bar{N}/\bar{\mathbb{Q}}(t)$ with $\bar{N}(u) = \bar{N}_\tau$ there exists by the Hurwitz classification a system $\sigma \in \Sigma_3(G)$ with $\bar{N} = \bar{N}_\sigma$. \square

Remark. Without the assumption on generation in Theorem 7.2, the translation φ_V only maps into $\bar{\Sigma}_r(G)/\text{Inn}(G)$. This generalization will be of use in the next paragraph (see (8.16)).

The previous result also allows the explicit determination of generators for the inertia groups for the Galois extensions constructed in the Twisted Rigidity Theorem.

7.2 Rational Translates with Few Ramification Points

The possibilities for Galois rational translates are rather restricted by Theorem 6.2. But if the assumption that our translation field be Galois is dropped, then a wide variety of field extensions are possible. Guralnick and Thompson (1990) conjectured that apart from cyclic and alternating groups only a finite list of further simple groups can occur as composition factors of the Galois group of the Galois closure of such a field extension $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$. This has been proved by the work of many authors, the last step was given by Frohardt and Magaard (2001). Frohardt et al. (2016) have announced a complete classification of all possible non-alternating and non-cyclic composition factors which comprises 45 further simple groups, including for example all five Mathieu groups.

Here we will here restrict ourselves to translates where the translated Galois extension is ramified in at most 4 points. Such Galois extensions have the advantage that they can be tested on possible symmetries with the help of the formulae

for geometric automorphisms proved in the previous paragraph. Without loss of generality we may moreover restrict ourselves to *primitive translates*, i.e., those extensions $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$ having no proper intermediate field, since all other translates may be composed of these. In the language of Galois groups, this means that the Galois group of the Galois closure \bar{L} of $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$ acts primitively on the cosets of $\text{Gal}(\bar{L}/\bar{\mathbb{Q}}(u))$. All possibilities for such non-Galois rational translates of degree $n \leq 4$ for Galois extensions of genus $g > 1$ are collected in the following theorem.

Theorem 7.3. *For Galois extensions of genus $g > 1$ with at most four ramification points there exist the following primitive and non-Galois rational translates of degree $n \leq 4$:*

(a) *a translation of degree 3 with group S_3 , class vector $\mathbf{C} = (2A, 2A, 3A)$ and*

$$\varphi'_{S_3}(\sigma) = (\sigma_1^2, \sigma_1^{\sigma_2^{-1}\sigma_1}, (\sigma_2^2)^{\sigma_1}, \sigma_2, \sigma_3^3), \quad (7.5)$$

(b) *a translation of degree 4 with group A_4 , class vector $\mathbf{C} = (2B, 3A, 3B)$ and*

$$\varphi'_{A_4}(\sigma) = (\sigma_1^2, (\sigma_1^2)^{\sigma_3^{-1}\sigma_1}, \sigma_2^3, \sigma_2^{\sigma_3^{-2}\sigma_2^2}, (\sigma_3^3)^{\sigma_2^2}, \sigma_3), \quad (7.6)$$

as well as one with $\mathbf{C} = (3A, 3A, 3A)$ and

$$\varphi''_{A_4}(\sigma) = (\sigma_1^3, \sigma_1^{\sigma_2^{-2}}, \sigma_2^3, \sigma_2^{\sigma_3^{-2}}, \sigma_3^3, \sigma_3^{\sigma_1^{-2}}), \quad (7.7)$$

(c) *a translation of degree 4 with group S_4 , class vector $\mathbf{C} = (2A, 3A, 4A)$ and*

$$\varphi'_{S_4}(\sigma) = (\sigma_1^2, \sigma_1^{\sigma_2^{-1}\sigma_1}, \sigma_1^{\sigma_2\sigma_1}, (\sigma_2^3)^{\sigma_3^{-1}\sigma_1}, \sigma_2, \sigma_3^4). \quad (7.8)$$

Here qA denotes the class of q -cycles and $2B$ the class of double transpositions in the symmetric group S_n .

Proof. Clearly only the groups S_3 , A_4 and S_4 possess primitive, faithful, non regular permutation representations of degree $n \leq 4$. The condition $g(\bar{\mathbb{Q}}(u)) = 0$ together with the Hurwitz genus formula then shows that the s prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ ramified in the Galois extension $\bar{N}/\bar{\mathbb{Q}}(t)$ have to split into $(s-2)n+2$ prime divisors \mathfrak{Q}_j in $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$. Since we require that $r \leq 4$, all but four of the \mathfrak{Q}_j have to ramify over $\bar{\mathbb{Q}}(t)$. Consequently the generating s -system for the Galois closure \bar{L} of $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$ in the degree n permutation representation contains elements with altogether at most four fixed points. This restricts the possible class vectors to $\mathbf{C}_a = (2A, 2A, 3A)$ and $\mathbf{C}'_a = (2A, 2A, 2A, 2A)$ for S_3 , $\mathbf{C}_b = (2B, 3A, 3B)$ and $\mathbf{C}'_b = (3A, 3A, 3A)$ for A_4 and $\mathbf{C}_c = (2A, 3A, 4A)$ for S_4 . In the case of the class vector \mathbf{C}'_a , due to $r \leq 4$ precisely four prime divisors are ramified in $\bar{N}(u)/\bar{\mathbb{Q}}(u)$ and in $\bar{N}(u)/\bar{\mathbb{Q}}(t)$, all of order 2, which implies $g(\bar{N}/\bar{\mathbb{Q}}) = 1$. For the remaining class vectors \mathbf{C}_a , \mathbf{C}_b and \mathbf{C}_c , the corresponding Galois extension $\bar{L}/\bar{\mathbb{Q}}(t)$ is uniquely determined by Theorem 6.2(c), and the same holds for \mathbf{C}'_b as well.

In the case of $V = S_3$ with the class vector \mathbf{C}_a , the field $\bar{L} = \bar{N}_V$ (in the notation of Theorem 6.3) possesses three conjugate subfields of degree 3. Among these

we may without loss of generality choose for $\bar{\mathbb{Q}}(u)$ the one for which $\Psi'_{S_3} := \text{Gal}(\bar{M}_S/\bar{\mathbb{Q}}(u))$ contains the inertia group $\langle \gamma_2 \rangle$. This determines Ψ'_{S_3} , which then has the following generating 5-system:

$$\Psi'_{S_3} = \langle \gamma_1^2, \gamma_1^{\gamma_2^{-1}\gamma_1}, (\gamma_2^2)^{\gamma_1}, \gamma_2, \gamma_3^3 \mid (\gamma_1\gamma_2)^3\gamma_3^3 = 1 \rangle.$$

This shows (a). The translation formulae in (b) and (c) are proved in a completely analogous fashion. \square

With these translation maps, classes of generating systems may be distinguished as in the Fixed Point Theorem 7.2 via their stabilizers.

Theorem 7.4. *Let G be a finite group with trivial center and φ a rational translation, whose group does not possess a non-trivial factor group in common with G . Then the map*

$$\varphi : \Sigma_s(G)/\text{Inn}(G) \rightarrow \Sigma_r(G)/\text{Inn}(G), \quad [\sigma] \mapsto [\varphi(\sigma)] \quad (7.9)$$

is injective.

Proof. Let $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$ be the field extension giving rise to the translation, and \bar{L} its Galois closure. By assumption, the translation group $H := \text{Gal}(\bar{L}/\bar{\mathbb{Q}}(t))$ and G do not have a common non-trivial factor group, so $\bar{L}/\bar{\mathbb{Q}}(t)$ is linearly disjoint from each Galois extension $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ with $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$. The composition $\bar{L}\bar{N}_\sigma$ is hence Galois over $\bar{\mathbb{Q}}(t)$ with group

$$G_H := \text{Gal}(\bar{L}\bar{N}_\sigma/\bar{\mathbb{Q}}(t)) \cong G \times H.$$

As in the proof of Theorem 7.2 the Galois extension \bar{N}_σ is uniquely determined by $\bar{L}\bar{N}_\sigma$ and hence also by $\bar{N}_\sigma(u)$ as the fixed field of $\mathcal{C}_{G_H}(G)$ (where here $G = \text{Gal}(\bar{L}\bar{N}_\sigma/\bar{L})$). In particular, if $\bar{N}_\sigma \neq \bar{N}_{\tilde{\sigma}}$ then also $\bar{N}_{\varphi(\sigma)} \neq \bar{N}_{\varphi(\tilde{\sigma})}$. Via the Hurwitz classification, φ is thus seen to be injective on $\Sigma_s(G)/\text{Aut}(G)$, and then as in (7.4) since $[\varphi(\sigma^\alpha)] = [\varphi(\sigma)]^\alpha$ also on $\Sigma_s(G)/\text{Inn}(G)$. \square

This immediately yields the following decomposition for the classes of generating systems in $\Sigma(C)/\text{Inn}(G)$:

Corollary 7.5. *Let $\mathbf{C} \in \text{Cl}(G)^r$ be a class vector of G and $\mathbf{C}_1, \dots, \mathbf{C}_q \in \text{Cl}(G)^s$ those class vectors for which $\Sigma(\mathbf{C}_j)$ contains preimages under the translation φ in (7.9). Then we have a disjoint decomposition*

$$\Sigma(\mathbf{C})/\text{Inn}(G) = \bigcup_{j=1}^q \varphi(\Sigma(\mathbf{C}_j)/\text{Inn}(G)) \cup R, \quad (7.10)$$

where R denotes the set of classes of generating r -systems in $\Sigma(\mathbf{C})/\text{Inn}(G)$ which cannot be obtained by translation with φ .

Such a decomposition can be utilized to obtain improved degree estimates for fields of definition of the corresponding Galois extensions, in a similar way to the decomposition into orbits with different stabilizer in Theorem 6.8. This is illustrated in the following example of a rational Galois translate.

Example 7.1. Let $G = S_8$ and $\mathbf{C} = (10A, 10A, 3B)$ where the classes $10A, 3B$ are characterized by the cycle types $(5, 2, 1), (3^2, 1^2)$ respectively. Then one finds $l(\mathbf{C}) = 15$. Under the action of the geometric automorphisms in H^V with the symmetry group $V = \langle (12) \rangle$, the set $\Sigma(\mathbf{C})/\text{Inn}(G)$ splits into three orbits of length 2 and nine fixed points. In the notation of Section 6.3 we hence have $l_1^V(\mathbf{C}) = 3$ and $l_V^V(\mathbf{C}) = 9$. By the Fixed Point Theorem 7.2 the nine fixed points originate from a translation with φ_{Z_2} , which by Theorems 7.2 and 6.3 has the form

$$\varphi_{Z_2}(\sigma) = (\sigma_1, \sigma_1^{\sigma_2^{-1}}, \sigma_2^2), \quad (7.11)$$

if we let $\sigma_3^2 = 1$, say. The possible preimages are now $\mathbf{C}_1 = (10A, 6A, 2D)$ with $l(\mathbf{C}_1) = 1$, $\mathbf{C}_2 = (10A, 6B, 2C)$ with $l(\mathbf{C}_2) = 7$ and $\mathbf{C}_3 = (10A, 6C, 2D)$ with $l(\mathbf{C}_3) = 1$, where $6A, 6B, 6C$ denote the classes of permutations with types $(6, 1^2), (6, 2)$ resp. $(3^2, 2)$, and $2C, 2D$ those of types $(2^3, 1^2)$ resp. (2^4) . The class vectors \mathbf{C}_1 and \mathbf{C}_3 are rationally rigid, hence the images of the corresponding classes $[\sigma] \in \varphi_{Z_2}(\Sigma(\mathbf{C}_i)/\text{Inn}(G))$ for $i = 1$ and $i = 3$ also remain stable under $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$. Since $\mathcal{L}(S_8) = 1$, the fixed field $K_\sigma = \mathbb{Q}(t)$ for these $[\sigma]$ constitutes a field of definition for $N_\sigma/G\bar{\mathbb{Q}}(t)$. \square

In the above example, Galois extensions $N_\sigma/\bar{\mathbb{Q}}(t)$ with $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ defined over \mathbb{Q} only arise by translation of Galois extensions which themselves are also already defined over $\mathbb{Q}(t)$. To obtain genuinely new Galois extensions in this way, $|R|$ would have to be equal to 1 in Corollary 7.5. However, an example of this phenomenon has yet to be found.

More successfully the rational translation could be used in connection with the Twisted Rigidity Theorem, when the class vector of the translated Galois extension possesses additional symmetries.

7.3 Twisting Rational Translates

A rational translation

$$\varphi : \Sigma_s(G)/\text{Inn}(G) \rightarrow \Sigma_r(G)/\text{Inn}(G), \quad [\sigma] \mapsto [\varphi(\sigma)],$$

in particular also translates the class vectors of a group G , hence it may be coarsened to

$$\varphi : \text{Cl}(G)^s \rightarrow \text{Cl}(G)^r, \quad \mathbf{C} \mapsto \varphi(\mathbf{C}). \quad (7.12)$$

Denote the corresponding field extension by $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(t)$. Then moreover φ associates to the set \mathbb{S} of prime divisors ramified over $\bar{\mathbb{Q}}(t)$ the subset \mathbb{T} of those prime

divisors $\mathfrak{Q} \in \mathbb{P}(\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}})$ over \mathbb{S} which still ramify over $\bar{\mathbb{Q}}(u)$. This will be abbreviated by $\mathbf{T} = \varphi(\mathbb{S})$.

Proposition 7.6. *If the rational translate φ is defined over k , i.e., if it originates from a geometric field extension $k(u)/k(t)$ with $k \subseteq \bar{\mathbb{Q}}$, then for all $\delta \in \text{Gal}(\bar{\mathbb{Q}}(t)/k(t))$ and their extensions $\tilde{\delta} \in \text{Gal}(\bar{\mathbb{Q}}(u)/k(u))$ we have*

$$\tilde{\delta} \circ \varphi = \varphi \circ \delta. \quad (7.13)$$

The prototype of the translation theorems may then be formulated as follows:

Theorem 7.7 (Translation Theorem). *Let G be a finite group with trivial center, $\mathbf{C} \in \text{Cl}(G)^s$ a class vector, φ a rational translation defined over \mathbb{Q} and V a symmetry group of $\varphi(\mathbf{C})$ with an orbit of odd length, with respect to which $\varphi(\mathbb{S})$ forms a V -configuration. If there exists a $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ with*

$$\varphi([\sigma])^\delta \in T := [\varphi(\sigma)]^{H_{\varphi(\mathbb{S})}^V} \quad \text{for all } \delta \in \Delta_{\varphi(\mathbf{C})}^V, \quad (7.14)$$

then there exists a geometric Galois extension $N/\mathbb{Q}_{\varphi(\mathbf{C})}^V(\tilde{u})$ with Galois group

$$\text{Gal}(N/\mathbb{Q}_{\varphi(\mathbf{C})}^V(\tilde{u})) \cong G. \quad (7.15)$$

Here $\mathbb{Q}_{\varphi(\mathbf{C})}^V = \mathbb{Q}$ if $\varphi(\mathbf{C})$ is a V -symmetric class vector.

Proof. Let $\mathbb{Q}(u)/\mathbb{Q}(t)$ be the field extension affording the translation. Further, let $\tau := \varphi(\sigma)$, $\mathbf{D} := \varphi(\mathbf{C})$ and $\mathbf{T} := \varphi(\mathbb{S})$. As \mathbf{T} forms a V -configuration, we have $H := H_{\mathbf{T}}^V \cong V$, and \mathbf{T} remains invariant under $\tilde{\Delta} := \text{Gal}(\bar{\mathbb{Q}}(u)/\mathbb{Q}_{\mathbf{D}}^V(u))$. Thus \mathbf{T} is also stable under $\tilde{\Delta}_{\mathbf{D}}^V := \langle \tilde{\Delta}, H \rangle$.

By assumption we have $\varphi([\sigma])^\delta \in T$ for all $\delta \in \Delta_{\mathbf{D}}^V = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}_{\mathbf{D}}^V(t))$, hence by Proposition 7.6 the image $[\varphi(\sigma)]^{\tilde{\delta}}$ also lies in T for all $\tilde{\delta} \in \tilde{\Delta}$. Consequently T is a $\tilde{\Delta}_{\mathbf{D}}^V$ -invariant H -orbit in $\Sigma(\mathbf{D})/\text{Inn}(G)$. The index of the stabilizer $\tilde{\Delta}_\tau^V$ of $[\tau]$ in $\tilde{\Delta}_{\mathbf{D}}^V$ hence coincides with the index of the corresponding stabilizer in H . This proves that the fixed field K_τ^V of $\tilde{\Delta}_\tau^V$ is regular over $\mathbb{Q}_{\mathbf{D}}^V$.

Since by assumption V possesses an orbit of odd length, Proposition 6.9 proves the existence of $\tilde{u} \in K_\tau^V$ with $K_\tau^V = \mathbb{Q}_{\mathbf{D}}^V(\tilde{u})$. Furthermore, as $\mathcal{X}(G) = 1$ we may conclude from Proposition 3.7 that K_τ^V is a field of definition of $\bar{N}_\tau/G\bar{\mathbb{Q}}(u)$, which completes the proof of the assertion. \square

Remark. If the stabilizer $H_{\varphi(\sigma)}$ in Theorem 7.7 is trivial, then we have moreover $\bar{\mathbb{Q}}N = \bar{N}_{\varphi(\sigma)}$.

If the set $\varphi(\mathbb{S})$ in the Translation Theorem consists of just three prime divisors, the hypotheses on the V -configuration need not be checked thanks to Theorem 6.4, and without loss of generality \mathbb{S} may be assumed to be defined over \mathbb{Q} . In this case

the translation formulae in Theorem 7.3 yield the explicit result:

Corollary 7.8. *Let G be a finite group with trivial center and without factor groups of type S_3 or A_4 . Further let $\mathbf{C} = (C_1, C_2, C_3)$ be a rigid class vector of G , consisting of two rational classes C_1 and C_2 with $C_1^2 = 1$ and $C_2^3 = 1$, and the semirational class C_3 (with primitive power $\bar{C}_3 \neq C_3$). If the corresponding unique classes of generating systems $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$, resp. $[\tau] \in \Sigma(\bar{\mathbf{C}})/\text{Inn}(G)$ satisfy one of*

$$\bar{C}_3 = C_3^2 \text{ and } [\sigma_1, \sigma_3^{\sigma_1 \sigma_3^{-1}}, \sigma_3^2] = [\tau_1, \tau_3^2, \tau_3^{\tau_1 \tau_3}] =: [\varphi(\tau)], \text{ or} \quad (7.16)$$

$$\bar{C}_3 = C_3^3 \text{ and } [\sigma_2, \sigma_3^{\sigma_2 \sigma_3^{-1}}, \sigma_3^3] = [\tau_2, \tau_3^3, \tau_3^{\tau_2 \tau_3^2}] =: [\varphi(\tau)], \quad (7.17)$$

then there exists a geometric Galois extension $N/\mathbb{Q}(\tilde{u})$ with

$$\text{Gal}(N/\mathbb{Q}(\tilde{u})) \cong G \quad \text{and} \quad \bar{\Phi}N = \bar{N}_{\varphi(\sigma)}. \quad (7.18)$$

Proof. Since the class vector \mathbf{C} is semirational and rigid, the orbit of $[\sigma]$ under $\Delta := \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ consists of just $[\sigma]$ itself and $[\tau]$, and we have $\Delta_\sigma = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}_\sigma(t))$.

In the first case, when $\bar{C}_3 = C_3^2$, we choose the rational translation $\varphi := \varphi'_{S_3} \circ \eta'_2$ with φ'_{S_3} from Theorem 7.3(a) and the geometric automorphism η'_2 belonging to $\omega = (23)$. Then since $\sigma_1^2 = 1$ and $\sigma_2^3 = 1$ we get

$$[\varphi(\sigma)] = [\varphi'_{S_3}(\sigma_1, \sigma_2 \sigma_3 \sigma_2^{-1}, \sigma_2)] = [\sigma_1, \sigma_3^2, \sigma_3^{\sigma_1 \sigma_3}]. \quad (7.19)$$

Hence we have $\varphi(\mathbf{C}) = (C_1, \bar{C}_3, C_3)$ and $V := \langle (23) \rangle$ is a subgroup of $\text{Sym}(\varphi(\mathbf{C}))$. The assumption (7.14) in the Translation Theorem is thus satisfied provided that

$$\varphi([\sigma]^\delta) = [\varphi(\sigma)]^{\eta'_2} \quad \text{for} \quad \delta \in \Delta \setminus \Delta_\sigma. \quad (7.20)$$

By (7.19) this is equivalent to

$$\varphi([\tau]) = [\sigma_1, \sigma_3^{\sigma_1 \sigma_3^{-1}}, \sigma_3^2].$$

In the case $\bar{C}_3 = C_3^3$ we choose the rational translation $\varphi = \varphi'_{A_4}$ from Theorem 7.3(b). Then we have

$$[\varphi(\sigma)] = [\varphi'_{A_4}(\sigma_1, \sigma_2, \sigma_3)] = [\sigma_2, \sigma_3^3, \sigma_3^{\sigma_2 \sigma_3^2}]. \quad (7.21)$$

So here we have $\varphi(\mathbf{C}) = (C_2, \bar{C}_3, C_3)$ with $V = \langle (23) \rangle \leq \text{Sym}(\varphi(\mathbf{C}))$ as above. Accordingly the condition (7.14) is equivalent to

$$\varphi([\tau]) = [\sigma_2, \sigma_3^{\sigma_2 \sigma_3^{-1}}, \sigma_3^3].$$

Since in both cases the image class vector $\varphi(\mathbf{C})$ is V -symmetric, we have $\mathbb{Q}_{\varphi(\mathbf{C})}^V = \mathbb{Q}$, and then the assertion follows from Theorem 7.7 together with the subsequent remark. \square

In the next section we study some applications of these new results.

7.4 Geometric Galois Extensions over $\mathbb{Q}(t)$ with $L_2(p)$

Our starting point here is the semirational rigid class vector $(2A, 3A, pA)$ of the projective special linear group $L_2(p)$ introduced in Example 5.2, which characterizes the field of modular functions of level p . From this by rational translation and twisting one may construct geometric $L_2(p)$ -extensions over $\mathbb{Q}(t)$, as was first proved by Shih (1974). The first two parts of the following theorem are applications of Corollary 7.8, while the third part requires a suitable translation of degree 8 for its proof.

Theorem 7.9 (Shih (1974)). *For all primes p satisfying either $(\frac{2}{p}) = -1$, $(\frac{3}{p}) = -1$ or $(\frac{7}{p}) = -1$, the group $L_2(p)$ possesses a G -realization over \mathbb{Q} .*

Proof. According to Example 5.2 the class vector $\mathbf{C} = (2A, 3A, pA)$ of $L_2(p)$ is semirational and rigid. The classes of generating 3-systems in $\Sigma(\mathbf{C})$ and $\Sigma(\tilde{\mathbf{C}})$, where $\tilde{\mathbf{C}} = (2A, 3A, pB)$, are obtained by Example 5.2 as the images of

$$\left[\begin{pmatrix} a+1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right] \quad \text{with} \quad \left(\frac{a}{p} \right) = \pm 1 \quad (7.22)$$

under the canonical epimorphism from $SL_2(p)$ onto $L_2(p)$. (Observe the reverse ordering!) Thus we have $pB = (pA)^a$ if and only if $(\frac{a}{p}) = -1$.

For $a = 2$ and $a = 3$ Corollary 7.8 may now be applied. Indeed it is easily verified that the twisting condition (7.16) resp. (7.17) is satisfied by the two classes of generating systems in (7.22). Therefore there exist geometric Galois extensions $N/\mathbb{Q}(\tilde{u})$ with group $L_2(p)$ for the class vector $(2A, pB, pA)$ when $(\frac{2}{p}) = -1$, respectively for the class vector $(3A, pB, pA)$ when $(\frac{3}{p}) = -1$.

In the case $a = 7$ we employ the rational translation defined by a root field of degree 8 for the field of modular functions of level 7. (A root field for a Galois extension is an intermediate field whose Galois closure coincides with the whole extension.) This is generated by a zero of the equation

$$(u^2 + 5u + 1)^3(u^2 + 13u + 49) - 1728tu = 0 \quad (7.23)$$

(see for example Klein and Fricke (1890), Kap. 7, §4 (3)). The permutation types for the conjugacy classes of the corresponding class vector $(2A, 3A, 7A)$ are (2^4) , $(3^2, 1^2)$ and $(7, 1)$. The translation formula for a class vector $\mathbf{C} = (C_1, C_2, C_3)$ with $\mathbf{C}_1^2 = 1$ and $\mathbf{C}_2^3 = 1$ is then given by

$$\varphi(\sigma) = (\sigma_2, \sigma_2^{\sigma_3^{-2}}, \sigma_3^7, \sigma_3^{\sigma_2\sigma_3^3}) \quad (7.24)$$

(where without loss of generality we have chosen the γ_2 -invariant root field). This shows that $\varphi(\mathbf{C}) = (3A, 3A, pB, pA)$ and $\text{Sym}(\varphi(\mathbf{C})) = \langle(12), (34)\rangle$. Any quadruple of prime divisors consisting of two orbits of length 2 under $\text{Gal}(\bar{\mathbb{Q}}(u)/\mathbb{Q}(u))$ forms at least a $\langle(12)(34)\rangle$ -configuration, hence in particular the above set $\varphi(\mathfrak{S})$. This leads to the symmetry condition

$$[\varphi(\sigma)]^{\eta_4^2} = [\varphi(\tau)], \quad (7.25)$$

where η_4^2 denotes the geometric automorphism in $H_{\varphi(\mathfrak{S})}^V$ belonging to $\omega_4^2 = (12)(34)$ as in Theorem 6.5. Since $\varphi(\mathbf{C})$ is V -symmetric, verification of (7.25) with the two classes of generating systems in (7.22) shows that the fixed field $K_{\varphi(\sigma)}^V$ is regular over \mathbb{Q} .

Now V does not possess an orbit of odd length on $\varphi(\mathfrak{S})$, so the rationality of $K_{\varphi(\sigma)}^V/\mathbb{Q}$ can only be deduced from the explicit knowledge of $\varphi(\mathfrak{S})$, which is implicit in the generating equation (7.23). Ordered according to (7.24) the prime divisors $\mathfrak{Q}_j \in \varphi(\mathfrak{S})$ are given by the divisor equalities

$$(u) = \frac{\mathfrak{Q}_4}{\mathfrak{Q}_3}, \quad (u^2 + 13u + 49) = \frac{\mathfrak{Q}_1\mathfrak{Q}_2}{\mathfrak{Q}_3^2}.$$

In Example 5.2 we saw that $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\sqrt{p^*})$ with $p^* = (-1)^{(p-1)/2}p$. With respect to the new variable $v := \sqrt{p^*} \frac{u-7}{u+7} \in \mathbb{Q}_{\mathbf{C}}(u)$ the product $\mathfrak{Q}_3\mathfrak{Q}_4$ becomes the numerator divisor of $(v^2 + p^*)$, and $\mathfrak{Q}_1\mathfrak{Q}_2$ that of $(v^2 + 27p^*)$. Thus the geometric automorphism η_4^2 maps the function v onto $-v$. Since each automorphism $\delta \in \text{Gal}(\bar{\mathbb{Q}}(u)/\mathbb{Q}(u))$ with non-trivial restriction to $\mathbb{Q}_{\mathbf{C}}(u)/\mathbb{Q}(u)$ maps $[\sigma]$ to $[\tau]$ and hence by Proposition 7.6 also $[\varphi(\sigma)]$ to $[\varphi(\tau)]$, the class $[\varphi(\sigma)]$ is invariant under $\eta_4^2 \circ \delta$. Consequently $K_{\varphi(\sigma)}^V$ is the fixed field of the restriction $\tilde{\delta}$ of $\eta_4^2 \circ \delta$ to $\mathbb{Q}_{\mathbf{C}}(u)$. Since

$$(v - \sqrt{p^*})^{\tilde{\delta}} = (-v - \sqrt{p^*})^{\tilde{\delta}} = (-v + \sqrt{p^*}),$$

the numerator divisor \mathfrak{Q}_3 of $(v - \sqrt{p^*})$ is $\tilde{\delta}$ -invariant. Thus $K_{\varphi(\sigma)}^V$ possesses a prime divisor of degree 1 and is a rational function field, say $K_{\varphi(\sigma)}^V = \mathbb{Q}(\tilde{u})$. Moreover $K_{\varphi(\sigma)}^V$ is a field of definition of $\bar{N}_{\sigma}/\bar{\mathbb{Q}}(u)$ with its Galois group $L_2(p)$ by Proposition 3.7, so the proof of the assertion is also complete in the case $(\frac{7}{p}) = -1$. \square

In the original proof of this result, Shih used Shimura's theory of canonical systems of models instead of the symmetrization of the translation formulae. In contrast to this, the following result can only be proved with the help of the translation theory presented in this chapter. The proof is rather similar to the previous ones, so we just give a rough sketch.

Theorem 7.10. *For primes p with $(\frac{5}{p}) = -1$ the group $L_2(p)$ possesses a G -realization over \mathbb{Q} .*

Sketch of proof. First one verifies that under the hypotheses $(\frac{2}{p}) = 1$, which can be assumed according to Theorem 7.9, the semirational class vector $\mathbf{C} = (2A, 4A, pA)$

of $L_2(p)$ is rigid. With $\bar{\mathbf{C}} = (2A, 4A, pB)$ the classes $[\sigma] \in \Sigma(\mathbf{C})$ and $[\tau] \in \Sigma(\bar{\mathbf{C}})$ of generating 3-systems are the epimorphic images of

$$\left[\begin{pmatrix} 0 & \sqrt{2}/a \\ -a/\sqrt{2} & 0 \end{pmatrix}, \begin{pmatrix} \sqrt{2} & -\sqrt{2}/a \\ a/\sqrt{2} & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \right] \quad \text{with} \quad \left(\frac{a}{p} \right) = \pm 1 \quad (7.26)$$

in $L_2(p)$, where $\sqrt{2}$ denotes a root in \mathbb{F}_p of $X^2 - 2$. As translation one employs the field extension $\mathbb{Q}(u)/\mathbb{Q}(t)$ generated by

$$(u - 1)^4(u^2 - 6u + 25) + 256tu = 0. \quad (7.27)$$

In the Hurwitz classification it belongs to the class vector $(2B, 4A, 5A)$ of the group $\mathrm{PGL}_2(5) \cong S_5$, with components of permutation types (2^3) , $(4, 1^2)$, resp. $(5, 1)$. The translation map for a class vector \mathbf{C} with $C_1^2 = 1$ and $C_2^4 = 1$ is then seen to be given by

$$\varphi(\sigma) = (\sigma_2, \sigma_2^{\sigma_3^{-2}}, \sigma_3^5, \sigma_3^{\sigma_2 \sigma_3^2}). \quad (7.28)$$

Under the assumption $(\frac{5}{p}) = -1$ the image of $\mathbf{C} = (2A, 4A, pA) \in \mathrm{Cl}(L_2(p))^3$ hence equals $\varphi(\mathbf{C}) = (4A, 4A, pB, pA)$. As in the previous proof the set $\varphi(\mathbb{S})$ forms a V -configuration for $V := \langle (12)(34) \rangle = \langle \omega_4^2 \rangle$, and $\varphi(\mathbf{C})$ is V -symmetric. The verification of the symmetry condition

$$[\varphi(\sigma)]^{\eta_4^2} = [\varphi(\tau)] \quad (7.29)$$

is straightforward calculation. This shows that the field of definition $K_{\varphi(\sigma)}^V$ of $\bar{N}_{\varphi(\sigma)}/\bar{\mathbb{Q}}(u)$ is regular over \mathbb{Q} . Finally one checks the rationality as in the previous proof, this time using the new variable $v := \sqrt{p^* \frac{u+5}{u-5}}$. \square

A detailed proof of this theorem, as well as further examples, can be found in Malle (1991). Also in Shih (1978) and Malle (1993a) generating polynomials for the Galois extensions constructed in Theorems 7.9 and 7.10 with group $L_2(p)$ were determined at least for $p \leq 37$. (For $p \leq 29$ see the table in the Appendix A.2.) For that it was useful that the results of Theorem 7.10 possess a translation into the language of modular functions. Indeed, the constructed field extensions may be interpreted as rational models of modular function fields belonging to congruence subgroups inside certain Hecke groups (see Malle (1993a), Section 5).

Remark. According to Theorems 7.9 and 7.10 the groups $L_2(p)$ possess G -realizations over \mathbb{Q} at least for all primes $p < 311$. By Hilbert's irreducibility theorem this remains true for ordinary Galois extensions with group $L_2(p)$ over \mathbb{Q} . By a new result of Zywina (2015) the latter statement has been shown to hold for all primes $p > 3$.

8 Automorphisms of the Galois Group

The fixed fields of a generating system of a group G modulo $\text{Aut}(G)$, or more generally of an intermediate group A between $\text{Inn}(G)$ and $\text{Aut}(G)$ are natural candidates for fields of definition for the field extension obtained from the Hurwitz classification, but not in general with the Galois group. So instead of G , one can sometimes realize the group A , under certain assumptions even as geometric Galois group. With such an extension theorem we may for example embed the $L_2(p)$ -extensions of the last paragraph into geometric $\text{PGL}_2(p)$ -extensions.

8.1 Fixed Fields of Coarse Classes of Generating Systems

In this paragraph, A denotes a group of automorphisms of a finite group G containing $\text{Inn}(G)$, and $\bar{A} := A / \text{Inn}(G)$. The orbit of a class vector $\mathbf{C} \in \text{Cl}(G)^s$ under A is denoted by

$$\mathbf{C}^A := \{\mathbf{C}^\alpha \mid \alpha \in A\}. \quad (8.1)$$

The *full symmetry group* of \mathbf{C}^A is

$$\text{Sym}(\mathbf{C}^A) := \{\omega \in S_s \mid \mathbf{C}^{\omega\alpha} \in \mathbf{C}^*\text{ for some } \alpha \in A\}, \quad (8.2)$$

and any subgroup $V \leq \text{Sym}(\mathbf{C}^A)$ is called a *symmetry group* of \mathbf{C}^A . With respect to such a V we define $H_{\mathbf{S}}^V$ and $\Delta_{\mathbf{S}}^V$ as in (6.3), (6.19) respectively. For the coarse classes of generating systems $\sigma^A \in \Sigma(\mathbf{C}^A)/A$ we thus obtain the fixed groups

$$\Delta_{\sigma^A}^V := \{\delta \in \Delta_{\mathbf{S}}^V \mid \sigma^{\delta A} = \sigma^A\} \quad \text{and} \quad H_{\sigma^A}^V := H_{\mathbf{S}}^V \cap \Delta_{\sigma^A}^V, \quad (8.3)$$

with corresponding fixed fields

$$K_{\sigma^A}^V := \bar{\mathbb{Q}}(t)^{\Delta_{\sigma^A}^V} \quad \text{resp.} \quad \bar{K}_{\sigma^A}^V := \bar{\mathbb{Q}}(t)^{H_{\sigma^A}^V}. \quad (8.4)$$

Theorem 8.1. *If the fixed field $K_{\sigma^A}^V$ of σ^A is a disclosed function field, then it constitutes a field of definition of $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$ (without the group action).*

Proof. As in Proposition 4.6 we note that the field extension $\bar{N}_\sigma/K_{\sigma^A}^V$ is Galois. By Theorem 3.5 the field $K_{\sigma^A}^V$ is hence a field of definition of $\bar{N}_\sigma/\bar{\mathbb{Q}}(t)$, being a disclosed function field. \square

Remark. According to Proposition 6.9 the field $K_{\sigma^A}^V$ is disclosed for example when V possesses an orbit of odd length on \mathbf{S} .

We next give an estimate for the degree of the extension of constants in $K_{\sigma^A}^V/\mathbb{Q}$. Again we first determine the cyclotomic field extension contained in $K_{\sigma^A}^V/\mathbb{Q}$. There-

fore analogously to (4.24) we define the stabilizer of

$$\mathbf{C}^{AV} := \{\mathbf{C}^{\alpha\omega} \mid \alpha \in A, \omega \in V\} \quad (8.5)$$

in $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ under the action via the cyclotomic character as

$$\Delta_{\mathbf{C}}^{AV} := \{\delta \in \Delta \mid \mathbf{C}^{c(\delta)} \in \mathbf{C}^{AV}\}. \quad (8.6)$$

This has index

$$d^{AV}(\mathbf{C}) := (\Delta : \Delta_{\mathbf{C}}^{AV}) = \frac{|\mathbf{C}^*|}{|\mathbf{C}^{AV} \cap \mathbf{C}^*|}, \quad (8.7)$$

which in generalization of (4.23) is called the *AV-symmetrized irrationality degree of \mathbf{C}* . In particular \mathbf{C} is called *AV-symmetric* if $d^{AV}(\mathbf{C}) = 1$. Immediately from the definitions we have:

Proposition 8.2. *The fixed field $\mathbb{Q}_{\mathbf{C}}^{AV} := \bar{\mathbb{Q}}^{\Delta_{\mathbf{C}}^{AV}}$ is an abelian number field contained in $\mathbb{Q}_V \subseteq \mathbb{Q}_{\mathbf{C}}$ with*

$$[\mathbb{Q}_{\mathbf{C}}^{AV} : \mathbb{Q}] = d^{AV}(\mathbf{C}). \quad (8.8)$$

In particular we have $\mathbb{Q}_{\mathbf{C}}^{AV} = \mathbb{Q}$ if the class vector \mathbf{C} is AV-symmetric.

The number of $H_{\mathbf{s}}^V$ -orbits in $\Sigma(\mathbf{C}^{AV})/A$ with given stabilizer $U \leq H_{\mathbf{s}}^V$ up to automorphisms is denoted by

$$l_U^{AV}(\mathbf{C}) := |\{\sigma^{AH_{\mathbf{s}}^V} \mid \sigma \in \Sigma(\mathbf{C}), H_{\sigma A}^V = U^\alpha \text{ for some } \alpha \in \text{Aut}(H_{\mathbf{s}}^V)\}| \quad (8.9)$$

in generalization of (6.17). Correspondingly $\sigma^{AH_{\mathbf{s}}^V}$ is called a *rigid $H_{\mathbf{s}}^V$ -orbit* if $l_U^{AV}(\mathbf{C}) = 1$ for $U = H_{\sigma A}^V$. If $\Sigma(\mathbf{C}^{AV})/A$ consists of a single $H_{\mathbf{s}}^V$ -orbit, the class vector \mathbf{C} itself is called *AV-rigid*. This defines all notations in the following result:

Theorem 8.3. *Let G be a finite group, $\text{Inn}(G) \leq A \leq \text{Aut}(G)$, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$, and $V \leq \text{Sym}(\mathbf{C}^A)$ a symmetry group with respect to which \mathbf{s} forms a V -configuration. Then the fixed field $K_{\sigma A}^V$ of $\sigma^A \in \Sigma(\mathbf{C}^A)/A$ contains $\mathbb{Q}_{\mathbf{C}}^{AV}$. The degree of the algebraic closure $k_{\sigma A}^V$ of \mathbb{Q} in $K_{\sigma A}^V$ can be estimated by*

$$[k_{\sigma A}^V : \mathbb{Q}_{\mathbf{C}}^{AV}] \leq l_U^{AV}(\mathbf{C}) \quad \text{with} \quad U = H_{\sigma A}^V. \quad (8.10)$$

In particular, $K_{\sigma A}^V/\mathbb{Q}_{\mathbf{C}}^{AV}$ is regular if $\sigma^{AH_{\mathbf{s}}^V}$ is rigid.

Proof. The proof is entirely analogous to that of Theorem 6.8: As $\pi_{\mathbf{s}}(\Delta) \leq V$ we have $\mathbf{C}^{c(\delta)} \in \mathbf{C}^{AV}$ for each $\delta \in \Delta_{\sigma A}^V$, which entails $\Delta_{\sigma A}^V \leq \langle \Delta_{\mathbf{C}}^{AV}, H_{\mathbf{s}}^V \rangle =: \tilde{\Delta}_{\mathbf{C}}^{AV}$. If now $\tilde{K}_{\mathbf{C}}^{AV}$ denotes the fixed field of $\tilde{\Delta}_{\mathbf{C}}^{AV}$, then since $H_{\sigma \delta A}^V = (H_{\sigma A}^V)^{\delta^{-1}}$ we have

$$[K_{\sigma A}^V : \tilde{K}_{\mathbf{C}}^{AV}] = (\tilde{\Delta}_{\mathbf{C}}^{AV} : \Delta_{\sigma A}^V) \leq (H_{\mathbf{s}}^V : H_{\sigma A}^V) \cdot l_{H_{\sigma A}^V}^{AV}(\mathbf{C}).$$

Together with (8.4) we then obtain

$$\left[K_{\sigma^A}^V : \mathbb{Q}_C^{AV} \right] = \frac{[K_{\sigma^A}^V : \tilde{K}_C^{AV}]}{[\bar{\mathbb{Q}} K_{\sigma^A}^V : \bar{\mathbb{Q}} \tilde{K}_C^{AV}]} = \frac{(\Delta_C^{AV} : \Delta_{\sigma^A}^V)}{(H_{\mathfrak{s}}^V : H_{\sigma^A}^V)} \leq l_{H_{\sigma^A}^V}^{AV}(\mathbf{C}).$$

By definition the extension $K_{\sigma^A}^V / \mathbb{Q}_C^{AV}$ is regular when $\sigma^{AH_{\mathfrak{s}}^V}$ is rigid. \square

In the case of a trivial symmetry group we obtain the following generalization of Theorem 4.5 from the preceding theorem (where we now omit the superfluous groups from the notation):

Corollary 8.4. *If in Theorem 8.3 we have $V = 1$ so that \mathfrak{s} remains pointwise fixed under $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$, then it follows that*

$$[K_C^A : \mathbb{Q}_C^A(t)] \leq l^A(\mathbf{C}) = \frac{1}{|\bar{A}|} l(\mathbf{C}^A). \quad (8.11)$$

Proof. By the previous results, it only remains to show the equality in (8.11). This follows from

$$|\sigma^A| = |A| = |\bar{A}| \cdot |\text{Inn}(G)| = |\bar{A}| \cdot |[\sigma]| \quad (8.12)$$

and the definition (8.9):

$$l(\mathbf{C}^A) = |\bar{A}| \cdot l^A(\mathbf{C}^A) = |\bar{A}| \cdot l^A(\mathbf{C}). \quad \square$$

Example 8.1. According to Example 5.2 the class vector $\mathbf{C} = (2A, 3A, pA)$ of $L_2(p)$ satisfies $l^A(\mathbf{C}) = 1$. By Theorem 8.1 and Corollary 8.4 the field of modular functions of level p is hence defined over $\mathbb{Q}_C^A(t) = \mathbb{Q}(t)$. Still, since $\mathbb{Q}_C \neq \mathbb{Q}$, this is not true if we include the Galois group. \square

In the next section Galois extensions over $K_{\sigma^A}^V$ with group A will be constructed for which the fixed field of $\text{Inn}(G)$ coincides with K_{σ}^V . In the case $\mathcal{L}(G) = 1$ this leads to an extension of $\text{Gal}(N/K_{\sigma}^V) \cong G$ by $\bar{A} = A/\text{Inn}(G)$ (compare with the Twisted Rigidity Theorem 6.10).

8.2 Extension of the Galois Group by Outer Automorphisms

In this section, we make the general assumption that the group A acts on the $\Delta_{\mathfrak{s}}^V$ -orbit of $[\sigma] = \sigma^{\text{Inn}(G)}$, i.e., that σ^A forms a subset of $[\sigma]^{\Delta_{\mathfrak{s}}^V}$. Then we first have the following general result:

Proposition 8.5. *Let G , A and \mathbf{C} be as in Theorem 8.3, $V \leq \text{Sym}(\mathbf{C}^A)$ and $\sigma \in \Sigma(\mathbf{C}^A)$ with $\sigma^A \subseteq [\sigma]^{\Delta_{\mathfrak{s}}^V}$. Then there exists a Galois extension $N^A/K_{\sigma^A}^V$ with*

$$\text{Gal}(N^A/K_{\sigma^A}^V) \cong A \quad \text{and} \quad \text{Gal}(N^A/K_{\sigma}^V) \cong \text{Inn}(G). \quad (8.13)$$

Here the field extension N^A/K_{σ}^V is geometric.

Proof. It was already seen in the proof of Theorem 8.1 that the extension $\bar{N}_\sigma/K_{\sigma^A}^V$ is Galois. Now let N^A denote the fixed field of the centralizer of $G = \text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$ in this Galois extension. Then due to $\bar{\mathbb{Q}}(t)N^A = \bar{N}_\sigma^{\mathcal{Z}(G)} =: \bar{N}_\sigma^A$ we have

$$\text{Gal}(N^A/K_\sigma^V) \cong \text{Gal}(\bar{N}_\sigma^A/\bar{\mathbb{Q}}(t)) \cong \text{Inn}(G),$$

and in particular N^A/K_σ^V is geometric and Galois. Further $\text{Gal}(N^A/K_{\sigma^A}^V)$ is certainly isomorphic to a subgroup of A . By assumption $\bar{A} = A/\text{Inn}(G)$ acts on the $\Delta_{\mathfrak{s}}^V$ -orbit of $[\sigma]$, which thus according to (8.12) splits under \bar{A} into suborbits of length $|\bar{A}|$. This implies

$$\left[K_\sigma^V : K_{\sigma^A}^V \right] = \left(\Delta_{\sigma^A}^V : \Delta_\sigma^V \right) = |\bar{A}|$$

and hence $\text{Gal}(N^A/K_{\sigma^A}^V) \cong A$. \square

Adding our standard hypotheses this implies the following:

Theorem 8.6. *Let G , A , \mathbf{C} and V be as in Theorem 8.3, where moreover V possesses an orbit of odd length. Assume furthermore that the class vector \mathbf{C} is V -rigid, and that for each $\alpha \in A$ there exists $\delta \in \Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ with $\mathbf{C}^{\alpha V} = \mathbf{C}^{c(\delta)V}$. Then there exists a Galois extension $N^A/\mathbb{Q}_{\mathbf{C}}^{AV}(\tilde{t})$ such that $N^A/\mathbb{Q}_{\mathbf{C}}^V$ is regular and*

$$\text{Gal}(N^A/\mathbb{Q}_{\mathbf{C}}^{AV}(\tilde{t})) \cong A \text{ and } \text{Gal}(N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})) \cong \text{Inn}(G). \quad (8.14)$$

Here we have $\mathbb{Q}_{\mathbf{C}}^{AV} = \mathbb{Q}$ if \mathbf{C} is AV -symmetric.

Proof. The V -rigidity of \mathbf{C} and the assumption that $\mathbf{C}^{AV} \subseteq \mathbf{C}^{\Delta V}$ guarantee that $\Sigma(\mathbf{C}^{\Delta V})/\text{Inn}(G)$ contains a single $\Delta_{\mathfrak{s}}^V$ -orbit. Consequently we have $\sigma^A \subseteq [\sigma]^{\Delta_{\mathfrak{s}}^V}$. By Proposition 8.5 it remains to show that the function field $K_{\sigma^A}^V$ is rational over $\mathbb{Q}_{\mathbf{C}}^{AV}$. But under the above assumptions this follows immediately from Theorems 8.1 and 8.3. \square

Example 8.2. We return to the case of the field $N/\mathbb{Q}_{\mathbf{C}}(t)$ of modular functions of level p already considered in Example 8.1. Here we have $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\sqrt{p^*})$ and $\text{Gal}(N/\mathbb{Q}_{\mathbf{C}}(t)) \cong \text{L}_2(p)$. Since $\mathbf{C}^A = \mathbf{C}^*$ we may conclude from Theorem 8.6 with $V = 1$ that

$$\text{Gal}(N/\mathbb{Q}(t)) \cong \text{PGL}_2(p). \quad \square$$

8.3 Geometric Extension of the Galois Group by Outer Automorphisms

The possibility of extending the Galois group becomes still more interesting when $K_\sigma^V/K_{\sigma^A}^V$ is geometric. For this we get the following criterion:

Theorem 8.7 (Extension Theorem). *Let G , A , \mathbf{C} and V be as in Theorem 8.3, where moreover V possesses an orbit of odd length. Suppose that $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ contains a rigid $H_{\mathbf{s}}^V$ -orbit on which A acts. Then there exists a geometric Galois extension $N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{z})$ with*

$$\text{Gal}(N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{z})) \cong A \quad \text{and} \quad \text{Gal}(N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})) \cong \text{Inn}(G). \quad (8.15)$$

If the class vector \mathbf{C} is V -symmetric, then we have $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$.

Proof. Let $[\sigma]^{H_{\mathbf{s}}^V}$ be the rigid $H_{\mathbf{s}}^V$ -orbit in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$. For this we have $\sigma^A \subseteq [\sigma]^{H_{\mathbf{s}}^V} = [\sigma]^{\Delta_{\mathbf{s}}^V}$ by assumption. Hence by Proposition 8.5 there exists a Galois extension $N^A/K_{\sigma^A}^V$ with group $\text{Gal}(N^A/K_{\sigma^A}^V) \cong A$, in which N^A/K_{σ}^V is geometric. Now since $\sigma^A \subseteq [\sigma]^{H_{\mathbf{s}}^V}$ we have

$$\left[K_{\sigma}^V : K_{\sigma^A}^V \right] = \left(\Delta_{\sigma^A}^V : \Delta_{\sigma}^V \right) = \left(H_{\sigma^A}^V : H_{\sigma}^V \right) = \left[\bar{K}_{\sigma}^V : \bar{K}_{\sigma^A}^V \right],$$

which shows that the extension $K_{\sigma}^V/K_{\sigma^A}^V$ is geometric. Because of the rigidity of the $H_{\mathbf{s}}^V$ -orbit it follows from Theorem 6.8 that $K_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V$ is regular. Hence the same holds for $K_{\sigma^A}^V/\mathbb{Q}_{\mathbf{C}}^V$. Since V possesses an orbit of odd length, Proposition 6.9 shows that first $K_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V$ and then by the Theorem of Lüroth also $K_{\sigma^A}^V/\mathbb{Q}_{\mathbf{C}}^V$ is rational, say $K_{\sigma}^V = \mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ and $K_{\sigma^A}^V/\mathbb{Q}_{\mathbf{C}}^V(\tilde{z})$. This completes the proof. \square

Remark. In the case $\mathcal{Z}(G) = 1$ the Galois extension $N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ in (8.15) coincides with the extension $N/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ constructed in the Twisted Rigidity Theorem 6.10.

With the next example we continue the Example 5.1.

Example 8.3. Let $G = \text{L}_2(8)$ and \mathbf{C} the class vector $(9A, 9B, 9C)$ of G . Since $l(\mathbf{C}) = 1$, $\Sigma(\mathbf{C})/\text{Inn}(G)$ consists of a single class of generating systems $[\sigma] = [\sigma_1, \sigma_2, \sigma_3]$. According to (6.11) its components σ_i are permuted cyclically by $V = \langle (123) \rangle$. On the other hand, $\text{Out}(G) = Z_3$ also permutes the three classes $9A$, $9B$ and $9C$ cyclically. Thus for every V -configuration \mathbf{s} and for $A := \text{Aut}(G) = \Gamma\text{L}_2(8)$ we have $\sigma^A = [\sigma]^{H_{\mathbf{s}}^V}$. In particular, σ^A itself is a rigid $H_{\mathbf{s}}^V$ -orbit. Hence Theorem 8.7 implies the existence of a geometric Galois extension $N/\mathbb{Q}(\tilde{z})$ with

$$\text{Gal}(N/\mathbb{Q}(\tilde{z})) \cong \Gamma\text{L}_2(8).$$

The corresponding class vector is then given by $\tilde{\mathbf{C}} = (9A, 3B, 3C)$. Since the fixed field of $\text{L}_2(8)$ in $N/\mathbb{Q}(\tilde{z})$ is a rational function field, say $\mathbb{Q}(\tilde{t})$, $\text{Gal}(N/\mathbb{Q}(\tilde{t}))$ yields a GA-realization of $\text{L}_2(8)$. \square

If now $\bar{N}^A/\bar{\mathbb{Q}}(\tilde{z})$ denotes the Galois extension with group A obtained from $N^A/\mathbb{Q}_{\mathbf{C}}^V(\tilde{z})$ by extension of constants with $\bar{\mathbb{Q}}$, then the class of generating systems of A parametrizing \bar{N}^A can be deduced from the classifying class of generating systems $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ of $\bar{N}/\bar{\mathbb{Q}}(\tilde{t})$ with the help of the Fixed Point Theorem 7.2.

If $\bar{N}/\bar{\mathbb{Q}}(z)$ is ramified in the r prime divisors of $\mathbf{T} \subseteq \text{IP}(\bar{\mathbb{Q}}(z)/\bar{\mathbb{Q}})$, then $\bar{N}^A \in \mathbf{N}_T(A)$. According to the Hurwitz classification there exists $[\tau] \in \Sigma_r(A)/A$ with $\bar{N}_\tau = \bar{N}^A$. In the case $\mathcal{L}(G) = 1$ one obtains this class using the general translation map

$$\varphi_V : \Sigma_r(A)/A \rightarrow \bar{\Sigma}_s(A)/A, \quad [\tau] \mapsto [\varphi_V(\tau)], \quad (8.16)$$

(see the Remark following Theorem 7.2) as preimage of σ^A . This is a consequence of:

Corollary 8.8. *Let G , A , \mathbf{C} and V be as in Theorem 8.3 and assume $\mathcal{L}(G) = 1$. Then the restriction*

$$\varphi_V^G : \Sigma_r^G(A)/A \rightarrow \Sigma_s(G)/A, \quad \tau^A \mapsto \varphi_V(\tau)^A, \quad (8.17)$$

of the translation map φ_V from (8.16) to the inverse image $\Sigma_r^G(A)/A$ of $\Sigma_s(G)/A$ is injective. The image of φ_V^G consists precisely of those classes of generating systems $\sigma^A \in \Sigma_s(G)/A$ satisfying $\sigma^A \subseteq [\sigma]^{H_\mathbf{s}^V}$.

Proof. By the Fixed Point Theorem 7.2 the field \bar{N}^A is uniquely determined by $\sigma^{\text{Aut}(G)}$, since it can also be obtained by a translation $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}(t)^{H_\sigma^V}$ under which the group remains invariant. Hence the map φ_V^G is injective. The characterization of the image now follows from the proof of the Extension Theorem 8.7. \square

This corollary may also be used to test whether a given G-realization actually is a GA-realization or not.

Example 8.4. Let $N/\mathbb{Q}(t)$ be the Galois extension with the Mathieu group $G = M_{12}$ from Theorem 6.12 for the class vector $\mathbf{C} = (4A, 4A, 10A)$. For $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ and $V = \langle (12) \rangle$ we then have $[\sigma]^{H_\mathbf{s}^V} \subseteq \Sigma(\mathbf{C})/\text{Inn}(G)$. Since the outer automorphisms of M_{12} permute the classes $4A$ and $4B$, the class σ^A is not contained in $[\sigma]^{H_\mathbf{s}^V}$. Consequently, $\text{Gal}(N/\mathbb{Q}(t))$ is not a GA-realization for M_{12} . (But see Theorem II.9.9 for a proper GA-realization of this group.) \square

8.4 Geometric Galois Extensions over $\mathbb{Q}(t)$ with $\text{PGL}_2(p)$

Application of the Extension Theorem 8.7 leads to an embedding of the geometric Galois extension over $\mathbb{Q}(t)$ with groups $L_2(p)$ of the preceding paragraph into one with groups $\text{PGL}_2(p)$. More precisely we have:

Theorem 8.9. *The G-realizations of $L_2(p)$ constructed in Theorems 7.9 and 7.10 are GA-realizations.*

Proof. The proof will only be given for the cases $(\frac{2}{p}) = -1$ and $(\frac{7}{p}) = -1$, the other two being entirely similar.

First let $\text{Gal}(N/\mathbb{Q}(\tilde{u}))$ denote the G-realization of $G = L_2(p)$ over \mathbb{Q} from Theorem 7.9 for $(\frac{2}{p}) = -1$. Then we have $\bar{\mathbb{Q}}N = \bar{N}_{\varphi(\sigma)}$ with $\varphi = \varphi'_{S_3} \circ \eta'_2$ and the

unique class of generating systems $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ for $\mathbf{C} = (2A, 3A, pA)$. Since $\varphi(\mathbf{C}) = (2A, pB, pA)$ we have $\text{Sym}(\varphi(\mathbf{C})^A) = \langle (23) \rangle$ for $A = \text{PGL}_2(p)$. To verify the extension condition $\varphi(\sigma)^A \subseteq [\varphi(\sigma)]^{H_{\mathbf{S}}^V}$ it therefore suffices to show the validity of

$$[\varphi(\sigma)]^\alpha = [\varphi(\sigma)]^\eta \quad \text{with} \quad \eta = \eta'$$

for the outer automorphisms $\alpha \in A$. Due to $[\sigma]^\alpha = [\tau]$ this was already shown in the form of the twisting condition (7.20).

Now let $\text{Gal}(N/\mathbb{Q}(\tilde{u}))$ denote the G-realization of $L_2(p)$ over \mathbb{Q} for $(\frac{7}{p}) = -1$. Then we have $\bar{\mathbb{Q}}N = \bar{N}_{\varphi(\sigma)}$ with φ from (7.24) and $[\sigma]$ as above. We now find $\varphi(\mathbf{C}) = (3A, 3A, pB, pA)$, and $\varphi(\mathbf{S})$ forms a $\langle (12)(34) \rangle$ -configuration. Hence as above we obtain the extension condition for an outer automorphism $\alpha \in A$ from the twisting condition (7.25) proved in Theorem 7.9. \square

For later use we note the following supplementary results:

Corollary 8.10. *The geometric $\text{PGL}_2(p)$ -extensions constructed in Theorem 8.9 belong to the class vectors $(2B, 4A, pA)$ for $(\frac{2}{p}) = -1$, $(2B, 6A, pA)$ for $(\frac{3}{p}) = -1$, $(2B, 2B, 4A, pA)$ for $(\frac{5}{p}) = -1$, and $(2B, 2B, 3A, pA)$ for $(\frac{7}{p}) = -1$. Here all ramified prime divisors of the fixed field have degree 1.*

Proof. This follows immediately from the translation formulae for $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(z)$ with $\bar{\mathbb{Q}}(z) = \bar{\mathbb{Q}}(u)^{H_{\mathbf{S}}^V}$.

If in the case $(\frac{2}{p}) = -1$ the prime divisors ramified in $\bar{N}/\bar{\mathbb{Q}}(t)$ are denoted by $\mathfrak{Q}_2 := \mathfrak{P}_1|_{\bar{\mathbb{Q}}(z)}, \mathfrak{Q}_3 := \mathfrak{P}_2\mathfrak{P}_3|_{\bar{\mathbb{Q}}(z)}$, and if \mathfrak{Q}_1 denotes the second prime divisor ramified in $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(z)$, then the translation formula according to (6.8) for the ramification orders $(2, 2, 1)$ reads

$$\varphi_{Z_2}(\tau) = (\tau_1^2, \tau_2^2, \tau_3^{\tau_2}, \tau_3) = (1, \sigma_1, \sigma_2, \sigma_3). \quad (8.18)$$

Hence we find $\tau_3 = \sigma_3 \in pA, \tau_2 \in 4A$ since $\tau_2^2 = \sigma_1 \in 2A$, and $\tau_1 \in 2B$. In the case $(\frac{3}{p}) = -1$ the class vectors may be determined with the same translation formula. In the two remaining cases one utilizes the translation formula belonging to the ramification orders $(2, 2, 1, 1)$

$$\varphi'_{Z_2}(\tau) = (\tau_1^2, \tau_2^2, \tau_3^{\tau_2}, \tau_3^{\tau_2^{-1}\tau_4^{-1}\tau_2}, \tau_4^{\tau_2}, \tau_4) = (1, 1, \sigma_1, \sigma_2, \sigma_3, \sigma_4). \quad (8.19)$$

Because of the different ramification orders, the residue degrees of the ramified prime divisors are always equal to 1, except possibly the divisors ramified of order 2 in the cases $(\frac{5}{p}) = -1$ and $(\frac{7}{p}) = -1$. But by the proof of Theorem 7.9 in the case $(\frac{7}{p}) = -1$ the fixed field of $L_2(p)$ is $K_{\varphi(\sigma)}^V = \mathbb{Q}(\tilde{v})$ with $\tilde{v} = \sqrt{p^*}v$ (since $\tilde{v}^{\tilde{\delta}} = \tilde{v}$). Now $\eta := \eta_4^2$ satisfies $\tilde{v}^\eta = -\tilde{v}$, so we may take $K_{\varphi(\sigma)^A}^V = \mathbb{Q}(\tilde{z})$ with $\tilde{z} := \tilde{v}^2$. Consequently the divisors in the support of \tilde{z} are the two prime divisors ramified in $N/\mathbb{Q}(\tilde{z})$ of order 2. With the same argument one obtains, that also in the case $(\frac{5}{p}) = -1$ both prime divisors ramified in $N/\mathbb{Q}(\tilde{z})$ with order 2 have degree 1. \square

9 Computation of Polynomials with Prescribed Group

For the geometric field extensions found by the rigidity method, apart from the Galois group also the ramification points and the generators of inertia groups are known via the Hurwitz classification. At least in principle, this enables one to compute generating polynomials for these extensions. The range of calculation is only restricted by the fact that it requires the solution of systems of non-linear algebraic equations in quite a number of unknowns. In this paragraph the necessary calculations are performed for the groups S_n and A_n , including the exceptional case $\text{Aut}(A_6) \cong \text{PGL}_2(9)$, and for the two small Mathieu groups M_{12} and M_{11} .

9.1 Decomposition of Prime Divisors in Galois Extensions

To compute polynomials we require knowledge of the decomposition of the prime divisors ramified in a root field for the extension. We identify the Galois group $\text{Gal}(f)$ of a separable polynomial $f \in K[X]$ with the permutation group on the roots x_1, \dots, x_n of f in a splitting field N , which hence coincides with the image of $\text{Gal}(N/K)$ under the permutation representation

$$\pi_f : \text{Gal}(N/K) \rightarrow S_n, \quad \sigma \mapsto \begin{pmatrix} x_1 & \dots & x_n \\ x_1^\sigma & \dots & x_n^\sigma \end{pmatrix}. \quad (9.1)$$

This is clearly equivalent to the representation of $\text{Gal}(N/K)$ on the cosets of the stabilizer U of the root field $L := K(x_1)$. The decomposition of prime divisors (interpreted as valuation ideals of discrete rank 1 valuations, compare Engler and Prestel (2005), Ch. 2.1) in L/K is then obtained from the following general result:

Theorem 9.1. *Let K be a field with prime divisor \mathfrak{P} , L/K a finite separable field extension, $f \in K[X]$ the minimal polynomial of a primitive element x of L/K and N the splitting field of f over K with Galois group $G = \text{Gal}(N/K)$. Further let $\tilde{\mathfrak{P}}$ be an extension of \mathfrak{P} to N with separable residue field extension. If the set of zeroes $\mathcal{X} = \{x_1, \dots, x_n\}$ of f in N splits into r orbits $\mathcal{X}_1, \dots, \mathcal{X}_r$ under the action of the decomposition group $\pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P}))$, and \mathcal{X}_i splits into f_i orbits of lengths e_i under the action of the inertia group $\pi_f(G_I(\tilde{\mathfrak{P}}/\mathfrak{P}))$, then \mathfrak{P} splits into a product of prime divisors of L as follows:*

$$\mathfrak{P} = \prod_{i=1}^r \mathfrak{Q}_i^{e_i} \quad \text{with residue degrees } d_i = d(\mathfrak{Q}_i/\mathfrak{P}). \quad (9.2)$$

Proof. Let \hat{K}, \hat{N} , denote the completions of K with respect to \mathfrak{P} , respectively of N with respect to $\tilde{\mathfrak{P}}$, and embed f as $\hat{f} \in \hat{K}[X]$ into $\hat{K}[X]$. Then $\text{Gal}(\hat{N}/\hat{K}) \cong G_D(\tilde{\mathfrak{P}}/\mathfrak{P})$ (see for example Serre (1979), Ch. II, §3, Cor. 4), and with appropriate

numbering of the zeroes, also $\text{Gal}(\hat{f}) \leq \text{Gal}(f)$. If \hat{f} now has the prime decomposition

$$\hat{f} = \prod_{i=1}^r \hat{f}_i$$

in $\hat{K}[X]$, then $\text{Gal}(\hat{f})$ acts transitively on each set of zeroes \mathcal{X}_i of \hat{f}_i in \hat{N} , resp. N . So \mathcal{X} splits into r orbits \mathcal{X}_i of lengths $\deg(\hat{f}_i)$ under the action of $\pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P}))$.

The different prime ideals \mathfrak{Q}_i of L lying above \mathfrak{P} correspond bijectively to the prime polynomials \hat{f}_i , and we have

$$\deg(\hat{f}_i) = e(\mathfrak{Q}_i/\mathfrak{P})d(\mathfrak{Q}_i/\mathfrak{P}) = e_i d_i \quad \text{for } i = 1, \dots, r$$

(see loc. cit., Ch. II, Thm. 1 with Cor. 2). Now let $\hat{L}_i \leq \hat{N}$ denote the fields generated over \hat{K} by a zero x of \hat{f}_i , let $\hat{U}_i := \text{Gal}(\hat{N}/\hat{L}_i)$ and \hat{G}/\hat{U}_i a system of representatives of \hat{G} modulo \hat{U}_i . Then we have

$$\hat{f}_i = \prod_{x \in \mathcal{X}_i} (X - x) = \prod_{\hat{\sigma} \in \hat{G}/\hat{U}_i} (X - x^{\hat{\sigma}}) \quad \text{with } x \in \mathcal{X}_i.$$

If now $\hat{\mathfrak{P}}$ denotes the valuation ideal of \hat{K} and $\hat{\mathfrak{Q}}_i$ the one of \hat{L}_i , then the inertia indices satisfy

$$e(\mathfrak{Q}_i/\mathfrak{P}) = e(\hat{\mathfrak{Q}}_i/\hat{\mathfrak{P}}) = (\hat{G}_I : (\hat{U}_i \cap \hat{G}_I))$$

(see loc. cit., Ch. II, Thm. 1 and Ch. I, Prop. 22), where \hat{G}_I denotes the inertia group of \hat{N}/\hat{K} isomorphic to $G_I(\tilde{\mathfrak{P}}/\mathfrak{P})$. Consequently \hat{G}_i and hence also $G_I(\tilde{\mathfrak{P}}/\mathfrak{P})$ decompose the zero set \mathcal{X}_i of \hat{f}_i into orbits of length $e(\mathfrak{Q}_i/\mathfrak{P})$, and this achieves the proof. \square

If instead of the embedding of f into $\hat{K}[X]$ we consider the canonical image \tilde{f} of f in the polynomial ring over the residue field $\tilde{K} := K\mathfrak{P}$, then we obtain the following theorem of Dedekind (see for example Tschebotaröw and Schwerdtfeger (1950), Kap. V, Satz 16):

Theorem 9.2 (Dedekind). *Let K be a field with prime divisor \mathfrak{P} , ring of \mathfrak{P} -integers \mathfrak{O} and residue field $\tilde{K} := \mathfrak{O}/\mathfrak{P}$. Furthermore let $f \in \mathfrak{O}[X]$ be a monic polynomial with discriminant $D(f) \notin \mathfrak{P}$, N the splitting field of f with $G := \text{Gal}(N/K)$, $\tilde{\mathfrak{P}}$ a valuation ideal of N lying above \mathfrak{P} and $\tilde{N} := N\tilde{\mathfrak{P}}$ a separable field extension of \tilde{K} . Then the permutation representation $\pi_{\tilde{f}}$ of $\tilde{G} := \text{Gal}(\tilde{N}/\tilde{K})$ as Galois group of the reduced polynomial $\tilde{f} \in \tilde{K}[X]$ coincides with the restriction to $G_D(\tilde{\mathfrak{P}}/\mathfrak{P})$ of the permutation representation π_f of G :*

$$\pi_{\tilde{f}}(\tilde{G}) = \pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P})). \quad (9.3)$$

Proof. By assumption, \tilde{N}/\tilde{K} is Galois, and the reduction induces a canonical epimorphism

$$\psi : G_D(\tilde{\mathfrak{P}}/\mathfrak{P}) \rightarrow \tilde{G}, \quad \sigma \mapsto \tilde{\sigma} \quad (9.4)$$

(see for example Serre (1979), Ch. I, Prop. 21 with Cor.). Since $f(x)$ is monic and $D(f)$ does not lie in \mathfrak{P} , we have $D(\tilde{f}) = \widehat{D(\tilde{f})} \neq 0$. Hence the polynomial $\tilde{f} \in \tilde{K}[X]$ is separable of degree $\deg(\tilde{f}) = \deg(f)$. Thus each $\sigma \in G_D(\tilde{\mathfrak{P}}/\mathfrak{P})$ acts on the zero set \mathcal{X} of f in N in the same manner as $\tilde{\sigma}$ on the zero set $\tilde{\mathcal{X}}$ of \tilde{f} in \tilde{N} . This implies that $\pi_{\tilde{f}} \circ \psi$ is a faithful permutation representation of $G_D(\tilde{\mathfrak{P}}/\mathfrak{P})$, equivalent to $\pi_f|_{G_D(\tilde{\mathfrak{P}}/\mathfrak{P})}$. \square

In the case that the residue field \tilde{K} is finite, Theorem 9.2 allows us to deduce the permutation types of elements in $\text{Gal}(f)$:

Corollary 9.3 (Dedekind Criterion). *If under the assumptions of Theorem 9.2 the field \tilde{K} is finite, and \tilde{f} splits in $\tilde{K}[X]$ into r prime polynomials \tilde{f}_i then $\text{Gal}(f)$ contains permutations of type $(\deg(\tilde{f}_1), \dots, \deg(\tilde{f}_r))$.*

Proof. In the case of a finite field \tilde{K} , the Galois group $\text{Gal}(\tilde{f})$ is necessarily cyclic. A generating element $\tilde{\sigma}$ of $\text{Gal}(\tilde{f})$ permutes transitively the zeroes of each polynomial $\tilde{f}_i \in \tilde{K}[X]$. Thus by Theorem 9.2 the group $\pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P}))$ is generated by an element of permutation type $(\deg(\tilde{f}_1), \dots, \deg(\tilde{f}_r))$. \square

After these preparations we can now turn to the determination of polynomials, first in the case of S_n and A_n .

9.2 Polynomials with Groups S_n and A_n

The starting point for our construction for S_n is the rationally rigid class vector $\mathbf{C} = (2A, (n-1)A, nA)$ found in Proposition 5.2. We may choose the set \mathbb{S} to consist of the prime divisors in the support of (t) and $(t-1)$,

$$(t) = \frac{\mathfrak{P}_3}{\mathfrak{P}_2}, \quad (t-1) = \frac{\mathfrak{P}_1}{\mathfrak{P}_2}. \quad (9.5)$$

Then by Theorem 5.3 there exists an S_n -extension $N/\mathbb{Q}(t)$ where precisely $\mathfrak{P}_1, \mathfrak{P}_2$ and \mathfrak{P}_3 are ramified, of orders 2, $n-1$ resp. n . Moreover according to the Hurwitz classification we have $\bar{\mathbb{Q}}N = \bar{N}_{\sigma}$, where $[\sigma]$ denotes the unique class of generating systems in $\Sigma(\mathbf{C})/\text{Inn}(G)$. By (4.5) the $\bar{\sigma}_i := \varphi_{\sigma}(\sigma_i)$ then generate inertia groups of prime divisors \mathfrak{P}_i of $\bar{N}_{\sigma}/\bar{\mathbb{Q}}$ lying above \mathfrak{P}_i .

Now let $L = N^{S_{n-1}}$ be a root field of degree n of $N/\mathbb{Q}(t)$, let y be a primitive element of $L/\mathbb{Q}(t)$ with minimal polynomial f . Then the permutation representation given by $\text{Gal}(f)$ is equivalent to the representation of S_n on the cosets of S_{n-1} , and hence to the natural permutation representation of S_n . Consequently the generators of inertia groups have permutation types $(2, 1^{n-2})$, $(n-1, 1)$ and (n) in $\text{Gal}(f)$. Since the inertia groups are normal in the decomposition groups (see Serre (1979), Ch. I, Prop. 20), and the orbits of the normalizers of $\langle \sigma_i \rangle$ in S_n have lengths $(2, n-2)$, $(n-1, 1)$ and (n) , by Theorem 9.1 there exist (not necessarily prime)

divisors $\mathfrak{Q}_{i,j}$ of L/\mathbb{Q} with

$$\mathfrak{P}_1 = \mathfrak{Q}_{1,1}^2 \mathfrak{Q}_{1,2}, \quad \mathfrak{P}_2 = \mathfrak{Q}_{2,1}^{n-1} \mathfrak{Q}_{2,2}, \quad \mathfrak{P}_3 = \mathfrak{Q}_3^n, \quad (9.6)$$

where $\mathfrak{Q}_{1,1}$ has degree $\deg(\mathfrak{Q}_{1,1}) = 1$. Thus the different $\mathfrak{D}(L/\mathbb{Q}(t))$ has degree $2(n-1)$, and the Hurwitz genus formula yields

$$g(L/\mathbb{Q}) = 1 + n(g(\mathbb{Q}(t)) - 1) + \frac{1}{2} \deg(\mathfrak{D}(L/\mathbb{Q}(t))) = 0.$$

Since moreover L/\mathbb{Q} possesses at least the prime divisor \mathfrak{Q}_3 of degree 1, it is a rational function field. An element of L may be determined up to scalar multiples by fixing its divisor. We may hence uniquely define a generating element x of L by the two equations

$$(x) = \frac{\mathfrak{Q}_3}{\mathfrak{Q}_{2,1}} \quad \text{and} \quad (x-1) = \frac{\mathfrak{Q}_{1,1}}{\mathfrak{Q}_{2,1}}. \quad (9.7)$$

The linear space of $\mathfrak{Q}_{2,1}^n$ consists of the polynomial functions in x of degree at most n . So we obtain

$$\frac{\mathfrak{Q}_{2,2}}{\mathfrak{Q}_{2,1}} = (x-a) \quad \text{and} \quad \frac{\mathfrak{Q}_{1,2}}{\mathfrak{Q}_{2,1}^{n-2}} = (b(x)) \quad (9.8)$$

with $a \in \mathbb{Q}^\times$ and a monic polynomial $b(X) \in \mathbb{Q}[X]$ of degree $n-2$.

From (9.5) up to (9.8) we deduce the divisor equalities

$$(t) = \frac{\mathfrak{P}_3}{\mathfrak{P}_2} = \frac{\mathfrak{Q}_3^n}{\mathfrak{Q}_{2,1}^{n-1} \mathfrak{Q}_{2,2}} = \left(\frac{x^n}{x-a} \right),$$

$$(t-1) = \frac{\mathfrak{P}_1}{\mathfrak{P}_2} = \frac{\mathfrak{Q}_{1,1}^2 \mathfrak{Q}_{1,2}}{\mathfrak{Q}_{2,1}^{n-1} \mathfrak{Q}_{2,2}} = \left(\frac{(x-1)^2 b(x)}{x-a} \right).$$

Hence there exist elements $c_0, c_1 \in \mathbb{Q}^\times$ with

$$t(x-a) = c_0 x^n, \quad (t-1)(x-a) = c_1 (x-1)^2 b(x), \quad (9.9)$$

which after elimination of t yields

$$x-a = c_0 x^n - c_1 (x-1)^2 b(x).$$

Since the element x is transcendental over \mathbb{Q} , we find $c_0 = c_1 =: c$, and there remains the polynomial identity

$$h(X) := X^n - \frac{1}{c}(X-a) = (X-1)^2 b(X).$$

The polynomial $h(X)$ has a double zero at 1, which implies

$$h(1) = 1 - \frac{1}{c} + \frac{a}{c} = 0, \quad h'(1) = n - \frac{1}{c} = 0.$$

Substituting the only solution

$$c = \frac{1}{n}, \quad a = \frac{n-1}{n},$$

of this system of linear equations into (9.9), we obtain a relation between x and t which obviously originates from the minimal polynomial of x over $\mathbb{Q}(t)$. This completes the proof of:

Theorem 9.4. *The Galois group of the polynomial*

$$f(t, X) = X^n - t(nX - n + 1) \in \mathbb{Q}(t)[X] \quad (9.10)$$

is the symmetric group S_n . It generates the geometric Galois extension $N/\mathbb{Q}(t)$ in Theorem 5.3 with the choice of \mathfrak{S} according to (9.5).

Remark. Some specializations of t to rational numbers preserving the Galois group of f are given in Example 10.5.

In the proof of Theorem 5.3 it was noticed that the fixed field K' of the alternating group A_n in $N/\mathbb{Q}(t)$ is a rational function field, in which for odd n the prime divisors \mathfrak{P}_1 and \mathfrak{P}_2 ramify and for even n the prime divisors \mathfrak{P}_1 and \mathfrak{P}_3 ramify. Thus the field extensions $K'/\mathbb{Q}(t)$ differ according to the parity of n . Since the calculations in both cases behave identically, we will just give the details in the case of odd n . Then \mathfrak{P}_1 and \mathfrak{P}_2 ramify in $K'/\mathbb{Q}(t)$, say

$$\mathfrak{P}_1 = \mathfrak{Y}_1^2, \quad , \quad \mathfrak{P}_2 = \mathfrak{Y}_2^2, \quad (9.11)$$

and there exists a function $y \in K'$ with divisor $\mathfrak{Y}_1 \mathfrak{Y}_2^{-1}$. The divisor equality

$$(t-1) = \frac{\mathfrak{P}_1}{\mathfrak{P}_2} = \frac{\mathfrak{Y}_1^2}{\mathfrak{Y}_2^2} = (y^2)$$

then proves the existence of $c \in \mathbb{Q}^\times$ satisfying

$$t-1 = cy^2. \quad (9.12)$$

Since y was only determined up to scalar multiples, it remains to find the class of c in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This can be achieved using the discriminant of the polynomial $f(t, X)$ in Theorem 9.4

$$D(f) = \epsilon(n-1)^{n-1} n^n t^{n-1} (1-t) \quad \text{with} \quad \epsilon = (-1)^{n(n-1)/2}, \quad (9.13)$$

which may be computed from the well known formula for the discriminant of a trinomial. Since the zeroes of $f(1+cy^2, X)$ generate the field N over $K' = \mathbb{Q}(y)$ with group A_n , the discriminant of this polynomial must be a square, which implies

$$\frac{1}{2} D(f(1+cy^2, X)) \frac{1}{2} = \epsilon n (1-t) \frac{1}{2} = -\epsilon n c,$$

where $=_2$ means equality up to squares. Consequently we may choose $c = -\epsilon n$, which then completely determines y . From (9.12) we obtain the minimal polynomial

$$g(t, Y) = Y^2 + \frac{1}{\epsilon n}(t-1) \quad (9.14)$$

for y over $\mathbb{Q}(t)$. Together with the corresponding computations in the case of even n we thus obtain:

Theorem 9.5. *The Galois group of the polynomial*

$$f(1 - \epsilon ny^2, X) \in \mathbb{Q}(y)[X] \quad \text{for } n \equiv 1 \pmod{2}, \quad \text{resp.} \quad (9.15)$$

$$f\left(\frac{1}{1 + \epsilon(n-1)y^2}, X\right) \in \mathbb{Q}(y)[X] \quad \text{for } n \equiv 0 \pmod{2} \quad (9.16)$$

with $f(t, X)$ as in (9.10) and $\epsilon := (-1)^{n(n-1)/2}$ is the alternating group A_n . It generates the geometric Galois extension $N/\mathbb{Q}(y)$ with $\mathbb{Q}(y) = K'$ in Theorem 5.3.

Since the calculations in the following examples run along the same lines, we will not give all the details.

9.3 Polynomials with the Group $\text{Aut}(A_6)$ and Related Groups

Apart from the case $n = 6$, the automorphism group of the simple group A_n is just S_n . To complete the list of GA-realizations of alternating groups, we here construct a polynomial with Galois group $\text{Aut}(A_6) \cong \text{PGL}_2(9)$. A suitable class vector can easily be found by hand calculation, using the Group Atlas.

Proposition 9.6. *The class vector $(2B, 4C, 10A)$ of $\text{Aut}(A_6)$ is rationally rigid.*

Proof. From the character table of $\text{Aut}(A_6)$ in the Group Atlas it is immediately verified that the normalized structure constant of the rational class vector $\mathbf{C} = (2B, 4C, 10A)$ equals 1. Now let $\sigma \in \bar{\Sigma}(\mathbf{C})$ and $U := \langle \sigma \rangle$. Since $\sigma_1 \in S_6$ while $\sigma_2, \sigma_3 \notin S_6$, the translation formula for Z_2 with ramification orders $(1, 2, 2)$ using (6.8) yields a generating 4-system

$$\varphi_{Z_2}(\sigma) = (\sigma_1, \sigma_1^{\sigma_2^{-1}}, \sigma_2^2, \sigma_3^2)$$

of $U' := U \cap S_6$. One checks that $\sigma_1 \in 2B$, $\sigma_2 \sigma_1 \sigma_2^{-1} \in 2C$, $\sigma_2^2 \in 2A$ and $\sigma_3^2 \in 5A$, so U' contains elements from all three classes of involutions of S_6 , and elements of order 5. This excludes all proper subgroups of S_6 as candidates for U' , and we conclude $U = \text{Aut}(A_6)$. This implies that $\bar{\Sigma}(\mathbf{C}) = \Sigma(\mathbf{C})$ and hence by Corollary 5.6 that $l(\mathbf{C}) = n(\mathbf{C}) = 1$. \square

Now as in (9.5) choose $\$$ to be the support of (t) and $(t - 1)$, this time with

$$(t) = \frac{\mathfrak{P}_2}{\mathfrak{P}_3}, \quad (t - 1) = \frac{\mathfrak{P}_1}{\mathfrak{P}_3}, \quad (9.17)$$

and let \bar{N}_σ be the field extension in $\mathbf{N}_\sigma(G)$ for $G := \text{Aut}(A_6)$, parametrized by the unique class of generating systems $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$. According to the Basic Rigidity Theorem 4.8, $\bar{N}_\sigma/G\bar{\Phi}(t)$ is defined over $\mathbb{Q}(t)$, whence there exists a geometric Galois extension $N/\mathbb{Q}(t)$ with $\bar{\Phi}N = \bar{N}_\sigma$. Furthermore let L be a root field of $N/\mathbb{Q}(t)$ of degree 10 and y a primitive element of $L/\mathbb{Q}(t)$ with minimal polynomial f . Then $\text{Gal}(f)$ is the image of a permutation representation of $G \cong \text{PGL}_2(9)$ in S_{10} (via its action on the projective line over \mathbb{F}_9), in which elements from the classes $2B$, $4C$ and $10A$ are seen to have permutation types $(2^3, 1^4)$, $(4^2, 1^2)$, (10) respectively. By Theorem 9.1 the \mathfrak{P}_i split in $L/\mathbb{Q}(t)$ as

$$\mathfrak{P}_1 = \mathfrak{Q}_{1,1}^2 \mathfrak{Q}_{1,2}, \quad \mathfrak{P}_2 = \mathfrak{Q}_{2,1}^4 \mathfrak{Q}_{2,2}, \quad \mathfrak{P}_3 = \mathfrak{Q}_3^{10}, \quad (9.18)$$

with $\deg(\mathfrak{Q}_{1,1}) = 3$ and $\deg(\mathfrak{Q}_{2,1}) = 2$. So the different of $L/\mathbb{Q}(t)$ has degree 18, which shows that $g(L/\mathbb{Q}) = 0$. Thus L/\mathbb{Q} is a rational function field, and there exists a unique function $x \in L$ in the linear space of \mathfrak{Q}_3 satisfying

$$\frac{\mathfrak{Q}_{2,1}}{\mathfrak{Q}_3^2} = (x^2 + a), \quad \frac{\mathfrak{Q}_{2,2}}{\mathfrak{Q}_3^2} = (p(x)) = (x^2 + 50x + b), \quad \frac{\mathfrak{Q}_{1,1}}{\mathfrak{Q}_3^3} = (q(x)), \quad \frac{\mathfrak{Q}_{1,2}}{\mathfrak{Q}_3^4} = (r(x)),$$

with $a, b \in \mathbb{Q}$ and monic polynomials $q(X), r(X) \in \mathbb{Q}[X]$ of degree 3, resp. 4. Here for the final determination of x we have used the fact that the trace of $p(X)$ cannot vanish, since otherwise only imprimitive solutions will occur. As above this leads to the divisor equations

$$(t) = \frac{\mathfrak{P}_2}{\mathfrak{P}_3} = \frac{\mathfrak{Q}_{2,1}^4 \mathfrak{Q}_{2,2}}{\mathfrak{Q}_3^{10}} = ((x^2 + a)^4 (x^2 + 50x + b)),$$

$$(t - 1) = \frac{\mathfrak{P}_1}{\mathfrak{P}_3} = \frac{\mathfrak{Q}_{1,1}^2 \mathfrak{Q}_{1,2}}{\mathfrak{Q}_3^{10}} = (q(x)^2 r(x)).$$

So there exist $c_0, c_1 \in \mathbb{Q}^\times$ with

$$c_0 t = (x^2 + a)^4 (x^2 + 50x + b), \quad c_1 (t - 1) = q(x)^2 r(x). \quad (9.19)$$

Eliminating t from this shows $c_0 = c_1 =: c$, and there remains the polynomial identity in $\mathbb{Q}[X]$

$$(X^2 + a)^4 (X^2 + 50X + b) = q(X)^2 r(X) + c. \quad (9.20)$$

Formal differentiation of this with respect to X leads to a second identity, which upon substitution into (9.20) and using that $X^2 + a$ and $q(X)$ are coprime admits

the following splitting:

$$\begin{aligned} 10q(X) &= 8X(X^2 + 50X + b) + (X^2 + a)(2X + 50), \\ 10(X^2 + a)^3 &= 2q'(X)r(X) + q(X)r'(X). \end{aligned} \quad (9.21)$$

Comparison of coefficients now gives a system of non-linear algebraic equations. Only one of its six solutions is rational, with

$$a = -405, \quad b = 945, \quad c = 2^{14}3^{12}5^5, \quad (9.22)$$

which hence leads to the polynomial with group $G = \text{Aut}(A_6)$.

Theorem 9.7. *The Galois group of the polynomial*

$$f(t, X) = (X^2 - 405)^4(X^2 + 50X + 945) - 2^{14}3^{12}5^5t \quad (9.23)$$

is the group $\text{Aut}(A_6) \cong \text{PGL}_2(9)$. It generates a geometric Galois extension $N/\mathbb{Q}(t)$ ramified over $1, 0, \infty$ for the class vector $(2B, 4C, 10A)$.

Obviously the fixed fields K_1, K_2, K_3 of the index two subgroups S_6, M_{10} and $\text{PGL}_2(p)$ in $N/\mathbb{Q}(t)$ are also rational function fields $K_i = \mathbb{Q}(y_i)$, with

$$d_1 y_1^2 = t, \quad d_2 y_2^2 = t - 1, \quad d_3 y_3^2 = \frac{t - 1}{t}, \quad (9.24)$$

for certain $d_i \in \mathbb{Q}^\times$, since $\sigma_1 \in S_6$, $\sigma_2 \in M_{10}$, $\sigma_3 \in \text{PGL}_2(9)$. As $\sigma_2\sigma_1\sigma_2^{-1} \in 2C$, the normalizer of $\sigma_1 \in 2B$ and hence also the decomposition groups of prime divisors of N lying above \mathfrak{P}_1 are already contained in S_6 . So \mathfrak{P}_1 splits in $K_1/\mathbb{Q}(t)$, which according to Theorem 9.1 entails $d_1 =_2 1$. Due to $M_{10} \leq A_{10}$, the class of d_2 modulo squares can again be determined using the discriminant of $f(t, X)$. This is calculated from (9.19) up to (9.21) as

$$\begin{aligned} D(f) &= -\mathcal{N}(f'(t, x)) = -\mathcal{N}(10(x^2 - 405)^3q(x)) \\ &= -10^{10}(-ct)^6(-c(t-1))^3 = 2^{136}3^{108}5^{55}t^6(t-1)^3, \end{aligned} \quad (9.25)$$

where here \mathcal{N} denotes the norm of $L/\mathbb{Q}(t)$. This yields $d_2 =_2 5$. Finally, the composite of the three fields K_i is Galois over $\mathbb{Q}(t)$ with group $Z_2 \times Z_2$, which forces $d_1 d_2 d_3 =_2 1$. So we may choose

$$d_1 = 1 \quad \text{and} \quad d_2 = d_3 = 5. \quad (9.26)$$

Since \mathfrak{P}_1 splits in $K_1/\mathbb{Q}(t)$ and precisely the two prime divisors of \mathfrak{P}_1 in K_1 — these are the numerators of $(y_1 \pm 1)$ — ramify in N^{A_6}/K_1 , the function field $K' := N^{A_6}$ is also rational. A generating equation of K'/K_1 then has the shape

$$dz^2 = \frac{y_1 + 1}{y_1 - 1} \quad \text{with} \quad d = 5, \quad (9.27)$$

since from (9.25) we find as above that $d =_2 5$. In conclusion this leads to:

Corollary 9.8. *Specializing t in the polynomial $f(t, X)$ in Theorem 9.7 to $y_1^2, 1 + 5y_2^2$ resp. $1/(1 - 5y_3^2)$ yields polynomials $f_i(y_i, X) \in \mathbb{Q}(y_i)[X]$ with groups*

$$\text{Gal}(f_1(y_1, X)) \cong S_6, \text{Gal}(f_2(y_2, X)) \cong M_{10}, \text{Gal}(f_3(y_3, X)) \cong PGL_2(9). \quad (9.28)$$

Specialization of t to $\left(\frac{5z^2+1}{5z^2-1}\right)^2$ yields a polynomial $g(z, X) \in \mathbb{Q}(z)[X]$ with

$$\text{Gal}(g(z, X)) \cong A_6. \quad (9.29)$$

The latter gives a GA-realization of A_6 over \mathbb{Q} .

Remark. In a completely similar fashion, GA-realizations over \mathbb{Q} for $L_2(p^2)$ for all $p \equiv \pm 2 \pmod{5}$, $p \neq 2$, may be obtained, by starting from the rationally rigid class vector $\mathbf{C} = (2B, 4C, 10A)$ of the automorphism group $PGL_2(p^2) \cong \text{Aut}(L_2(p^2))$ (see Theorem II.7.7 with Remark).

For future use (see for example Chapter II.6 and II.7) we state the following observation made in the proof of Corollary 9.8 as a special lemma:

Lemma 9.9. *Let $K = k(t)$ be a rational function field of one variable and N/K a geometric Galois extension with group G . Further let H be a normal subgroup of G such that the fixed field N^H/k has genus 0. Now assume that for a generator σ of an inertia group in G over a prime divisor $\mathfrak{P} \in \mathbb{P}(K/k)$ of degree 1 ramified in N/K we have*

$$\mathcal{N}_G(\sigma) \leq \langle H, \sigma \rangle. \quad (9.30)$$

Then N^H/k is a rational function field.

Remark. By Theorem 6.2 the assumption $g(N^H/k) = 0$ is always satisfied if for example G/H is a dihedral group and only three prime divisors $\mathfrak{P} \in \mathbb{P}(K/k)$ are ramified in N^H/K .

9.4 Polynomials with the Mathieu Groups M_{12} and M_{11}

The final example to be given concerns the two smallest sporadic simple groups, namely the Mathieu groups M_{12} and M_{11} . We compute polynomials for the Galois extensions found in Theorem 6.12. Let $N/\mathbb{Q}(\tilde{t})$ denote the geometric Galois extension with $\text{Gal}(N/\mathbb{Q}(\tilde{t})) \cong M_{12}$ for the class vector $\mathbf{C} = (4A, 4A, 10A)$, and L the fixed field of M_{11} . Since this forms a root field of $N/\mathbb{Q}(\tilde{t})$, a polynomial with group M_{12} may be obtained as minimal polynomial of a primitive element of $L/\mathbb{Q}(\tilde{t})$. From Proposition 6.11 we know that $l(\mathbf{C}) = 2$ and $l^V(\mathbf{C}) = 1$ for $V = \langle (12) \rangle$, hence the first two ramified prime divisors \mathfrak{P}_1 and \mathfrak{P}_2 are permuted by $\text{Gal}(\bar{\mathbb{Q}}(\tilde{t})/\mathbb{Q}(\tilde{t}))$, while \mathfrak{P}_3 remains fixed. Now let $k(\tilde{t})$ be the splitting field of \mathfrak{P}_1 in this field extension, of degree 2 over $\mathbb{Q}(\tilde{t})$.

The classes $4A$ and $10A$ have permutation types $(4^2, 1^4)$, $(10, 2)$ in the permutation representation on the cosets of an intransitive M_{11} , so Theorem 9.1 gives the ramification behavior of \mathfrak{P}_i in $kL/k(\tilde{t})$ as

$$\mathfrak{P}_i = \mathfrak{Q}_{i,1}^4 \mathfrak{Q}_{i,2} \quad \text{for } i = 1, 2, \quad \mathfrak{P}_3 = \mathfrak{Q}_{3,1}^{10} \mathfrak{Q}_{3,2}^2, \quad (9.31)$$

with $\deg(\mathfrak{Q}_{i,1}) = 2$ for $i = 1, 2$. Since $\mathfrak{P}_1, \mathfrak{P}_2$ are conjugate in $k(\tilde{t})/\mathbb{Q}(\tilde{t})$, there exists a function $t \in \mathbb{Q}(\tilde{t})$ with

$$\frac{\mathfrak{P}_1}{\mathfrak{P}_3} = (t + a), \quad \frac{\mathfrak{P}_2}{\mathfrak{P}_3} = (t - a), \quad \text{and} \quad a^2 \in \mathbb{Q}. \quad (9.32)$$

Thereby, the divisor (t) of t is uniquely determined. By the proof of Theorem 6.12 the function field L/\mathbb{Q} is rational, hence there exist $x \in L$ and monic polynomials $q, r \in k[X]$ such that

$$\frac{\mathfrak{Q}_{3,2}}{\mathfrak{Q}_{3,1}} = (x), \quad \frac{\mathfrak{Q}_{1,1}}{\mathfrak{Q}_{3,1}^2} = (q(x)), \quad \frac{\mathfrak{Q}_{1,2}}{\mathfrak{Q}_{3,1}^4} = (r(x)). \quad (9.33)$$

Denoting images under the non-trivial automorphism of $k(\tilde{t})/\mathbb{Q}(\tilde{t})$ by a bar, we thus moreover have

$$\frac{\mathfrak{Q}_{2,1}}{\mathfrak{Q}_{3,1}^2} = (\bar{q}(x)), \quad \frac{\mathfrak{Q}_{2,2}}{\mathfrak{Q}_{3,1}^4} = (\bar{r}(x)). \quad (9.34)$$

Together with (9.31) up to (9.34) this implies the divisor equations

$$(t + a) = \frac{\mathfrak{P}_1}{\mathfrak{P}_3} = \frac{\mathfrak{Q}_{1,1}^4 \mathfrak{Q}_{1,2}}{\mathfrak{Q}_{3,1}^{10} \mathfrak{Q}_{3,2}^2} = \left(\frac{q(x)^4 r(x)}{x^2} \right),$$

$$(t - a) = \frac{\mathfrak{P}_2}{\mathfrak{P}_3} = \frac{\mathfrak{Q}_{2,1}^4 \mathfrak{Q}_{2,2}}{\mathfrak{Q}_{3,1}^{10} \mathfrak{Q}_{3,2}^2} = \left(\frac{\bar{q}(x)^4 \bar{r}(x)}{x^2} \right).$$

So there exist $c, \bar{c} \in k^\times$ with

$$c(t + a)x^2 = q(x)^4 r(x), \quad \bar{c}(t - a)x^2 = \bar{q}(x)^4 \bar{r}(x), \quad (9.35)$$

which after elimination of t first forces $c = \bar{c} \in \mathbb{Q}^\times$, and then results in the polynomial identity

$$2acX^2 = q(X)^4 r(X) - \bar{q}(X)^4 \bar{r}(X) \quad (9.36)$$

in $k[X]$. As in the proof of Theorem 9.7, differentiation of this equation, substitution of ac and observing that $q(X)$ and $\bar{q}(X)$ are necessarily coprime now yields

$$10q(X)^3 = 4\bar{q}'(X)\bar{r}(X)X + \bar{q}(X)\bar{r}'(X)X - 2\bar{q}(X)\bar{r}(X) \quad (9.37)$$

and its conjugate in $k[X]/\mathbb{Q}[X]$. By comparison of coefficients we obtain a system of non-linear algebraic equations in the 12 unknown coefficients of q, \bar{q}, r, \bar{r} , to which we may add the requirement $\text{tr}(q\bar{q}) = -6$. The latter finally determines

the function x , which was until now fixed only up to scalar multiples (note that the case $\text{tr}(q\bar{q}) = 0$ leads only to imprimitive field extensions). This system of equations possesses just one pair of conjugate solutions in a quadratic extension field k of \mathbb{Q} , namely in $k = \mathbb{Q}(\sqrt{5})$. With $d := \sqrt{5}$ this is given by

$$\begin{aligned} q(X) &= X^2 + \left(3 + \frac{3}{5}d\right)X - \frac{9}{25}d, \\ r(X) &= X^4 + \left(8 + \frac{12}{5}d\right)X^3 + \left(30 + \frac{336}{25}d\right)X^2 + \left(\frac{216}{5} + \frac{108}{5}d\right)X + \frac{81}{25}. \end{aligned} \quad (9.38)$$

Now t was only fixed up to scalar multiples, so in the equation

$$2ctx^2 = q(x)^4r(x) + \bar{q}(x)^4\bar{r}(x)$$

following from (9.35) we may still replace t by ct since $c \in \mathbb{Q}^\times$. Then x is a zero of the polynomial

$$f(t, X) = \frac{1}{2} \left(q(X)^4r(X) + \bar{q}(X)^4\bar{r}(X) \right) - tX^2.$$

Substituting q and r from (9.38) then yields:

Theorem 9.10. *The following polynomial has Galois group M_{12} over $\mathbb{Q}(t)$:*

$$\begin{aligned} f(t, X) &= X^{12} + 20X^{11} + 162X^{10} + \frac{3348}{5}X^9 + \frac{35559}{5^2}X^8 + \frac{5832}{5}X^7 \\ &\quad - \frac{84564}{5^3}X^6 - \frac{857304}{5^4}X^5 + \frac{807003}{5^5}X^4 + \frac{1810836}{5^5}X^3 \\ &\quad - \frac{511758}{5^6}X^2 + \frac{2125764}{5^7}X + \frac{531441}{5^8} - tX^2. \end{aligned} \quad (9.39)$$

By suitable specialization of t in $f(t, X)$ one easily obtains a polynomial with group M_{11} :

Corollary 9.11. *Writing the polynomial in Theorem 9.10 as $f(t, X) = h(X) - tX^2$, the polynomial*

$$g(x, X) := \frac{x^2h(X) - h(x)X^2}{X - x} \in \mathbb{Q}(x)[X] \quad (9.40)$$

has Galois group M_{11} over $\mathbb{Q}(x)$.

Proof. Let x be a zero of $f(t, X)$ in the splitting field N . Then since $t = h(x)/x^2$ the field N is generated over $\mathbb{Q}(t, x) = \mathbb{Q}(x)$ by a zero of

$$\frac{1}{X - x} \left(h(X) - \frac{h(x)}{x^2}X^2 \right) \in \mathbb{Q}(x)[X]$$

and hence by $g(x, X)$. □

Remark. With the help of Corollary 9.3 one easily finds infinite families of specializations $a, b \in \mathbb{Q}$ such that $\text{Gal}(f(a, X)) \cong M_{12}$ resp. $\text{Gal}(g(b, X)) \cong M_{11}$. For example this is true for all $a \equiv 1 \pmod{66}$ and all $b \equiv 1 \pmod{133}$ (see for example Matzat (1987), IV, §6.4).

A collection of further polynomials for almost simple groups constructed by this method is contained in the Tables in the Appendix A.1 and A.2.

10 Specialization of Geometric Galois Extensions

By the Hilbert irreducibility theorem every polynomial $f(t, X) \in k(t)[X]$ over a number field k possesses infinitely many specializations $t \mapsto a \in k$ with canonically isomorphic Galois group (compare Chapter IV.1). We will now study local properties like reality questions and ramification behavior for Galois extensions obtained in this way.

10.1 Local Structure Stability

By construction, irreducible generating polynomials $f = f(t, X)$ of Galois extensions $\bar{N}/\bar{\mathbb{Q}}(t)$ are defined over a number field k and absolutely irreducible. Hence they remain irreducible if k is replaced by its completion with respect to any valuation. In this section let k denote a complete metric field. If for $a \in k$ the numerator divisor \mathfrak{P} of $(t - a)$ is not contained in the ramification locus \mathbb{S} of $N/k(t)$, then by the Dedekind's Theorem 9.2 for $f_a := f(a, X) \in k[X]$ we have

$$\text{Gal}(f_a) = \pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P})) \cong G_D(\tilde{\mathfrak{P}}/\mathfrak{P}), \quad (10.1)$$

where $\tilde{\mathfrak{P}}$ denotes an extension of \mathfrak{P} to N . Then obviously the absolute Galois group $\Gamma_k = \text{Gal}(\bar{k}/k)$ of k , where \bar{k} denotes a maximal separable extension field of k , acts on the zeroes of f_a and so yields a continuous homomorphism

$$\lambda_a : \Gamma_k \rightarrow \text{Gal}(f_a) = \pi_f(G_D(\tilde{\mathfrak{P}}/\mathfrak{P})) \leq \text{Gal}(f) \cong G \quad (10.2)$$

from Γ_k in $\text{Gal}(f) \cong G$, unique up to inner automorphisms of G . Its kernel consists of the fixed group in Γ_k of the field $N_a := N\tilde{\mathfrak{P}}$ generated by f_a over k . Now let \mathcal{S} denote the set of those $a \in \mathbb{P}^1(k)$ for which the numerator divisor of $(t - a)$ (resp. $(\frac{1}{t})$ when $a = \infty$) lies in \mathbb{S} , and

$$\Lambda := \{\lambda_a \mid a \in \mathbb{P}^1(k) \setminus \mathcal{S}\}. \quad (10.3)$$

Equipping the finite orbit space $\Lambda / \text{Inn}(G)$ with the discrete topology we have:

Theorem 10.1 (Saltman (1982)). *Let k be a complete metric field and $f(t, X) \in k(t)[X]$ an irreducible polynomial. Then the map*

$$\lambda : \mathbb{P}^1(k) \setminus \mathcal{S} \rightarrow \Lambda / \text{Inn}(G), \quad a \mapsto \lambda_a, \quad (10.4)$$

is well defined and continuous; in particular the field extensions N_a/k generated by $f(a, X)$ do not change if the corresponding a are sufficiently close.

Proof. In the case of a complex archimedean valuation the assertion is trivially satisfied since $\Gamma_k = 1$. Since in the case of a real archimedean valuation the zeroes of $f_a := f(a, X) \in k[X]$ depend continuously on a , the decomposition type of f_a can only change when a passes through an element of \mathcal{S} . Finally, in the case of ultrametric valuations, the decomposition type and the coefficients of the factors

of f_a again depend continuously on a by Hensel's Lemma (see for example Artin (1967), Ch. 2, Thm. 5a). For sufficiently close $a, b \in k$ the factors of f_a and f_b generate the same field by Krasner's Lemma (see loc. cit., Ch. 2, Thm. 9), which proves $N_a = N_b$. \square

Example 10.1. In the case $f(t, X) = X^2 - t \in \mathbb{Q}_p(t)[X]$ with $p \neq 2$ the projective line $\mathbb{P}^1(\mathbb{Q}_p) \setminus \{0, \infty\}$ divides up into four open and closed subsets belonging to the four fields $\mathbb{Q}_p(\sqrt{a})$ with $a \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$. \square

In the next section we will first study some applications in the case of real archimedean valuations.

10.2 Reality Questions

Let $\bar{N}/\bar{\mathbb{Q}}(t)$ be a Galois extension which together with its Galois group is defined over a real number field k . With respect to a real archimedean valuation of k , i.e., an embedding of k into \mathbb{R} , by Theorem 10.1 to each connected component \mathcal{O} of $\mathbb{P}^1(k) \setminus \mathcal{S}$ there belongs a well defined conjugacy class of involutions of $G = \text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t))$, whose elements upon specialization of t to $a \in \mathbb{Q}$ take the role of complex conjugation $\rho_a := \rho|_{N_a}$ in the residue fields N_a/k . When G has trivial center, this conjugacy class can be described explicitly without problems. For this let $N_a := N\tilde{\mathfrak{P}}$ be the residue class field of $N/k(t)$ modulo a fixed extension $\tilde{\mathfrak{P}}$ of the numerator divisor $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ of $(t-a)$ and

$$\psi_a : G_D(\tilde{\mathfrak{P}}/\mathfrak{P}) \longrightarrow G_a \quad (10.5)$$

the canonical epimorphism introduced in (9.4). Then we first have:

Proposition 10.2. *The complex conjugation commutes with the epimorphism ψ_a . The action of ρ_a on $G_a = \text{Gal}(N_a/k)$ is given by*

$$\rho_a : G_a \rightarrow G_a, \quad \psi_a(\sigma) \mapsto \psi_a(\sigma^\rho), \quad (10.6)$$

where ρ denotes the complex conjugation in $\bar{\mathbb{Q}}N/k(t)$ from the remark following Theorem 2.2.

Proof. For $\bar{N} := \bar{\mathbb{Q}}N$ we have by Proposition 3.1

$$\Gamma := \text{Gal}(\bar{N}/k(t)) = \text{Gal}(\bar{N}/N) \times \text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t)).$$

Let $\tilde{\mathfrak{P}}$ denote an extension of $\tilde{\mathfrak{P}}$ on \bar{N} and \tilde{N}_D resp. N_D the decomposition fields of $\tilde{\mathfrak{P}}/\mathfrak{P}$ resp. $\tilde{\mathfrak{P}}/\mathfrak{P}$. The corresponding fields of constants are \tilde{k} and k since N_D/k is regular. Using the translation theorem of Galois theory we obtain

$$\text{Gal}(\tilde{k}/k) \cong \text{Gal}(\tilde{N}_D/N_D) \cong \text{Gal}(N/(N \cap N_D)) = G_D(\tilde{\mathfrak{P}}/\mathfrak{P}),$$

which shows that $\tilde{k} = N_a$ and $\text{Gal}(\tilde{k}/k) = G_a$.

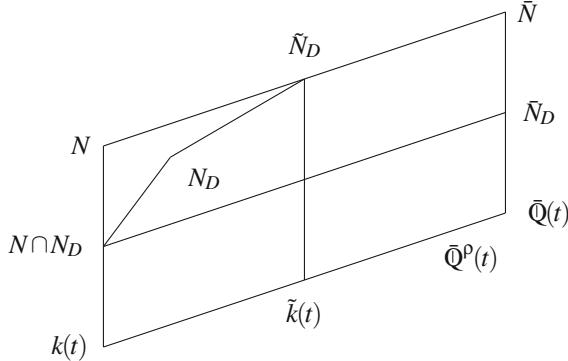


Fig. 10.1 Complex conjugation in residue class fields

Now let ρ be the complex conjugation in $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$ and $\tilde{\rho}$ the unique extension of ρ onto \bar{N} with $\tilde{\mathfrak{P}}^{\tilde{\rho}} = \tilde{\mathfrak{P}}$ (compare with Theorem 1.6 and the Remark after Theorem 2.2). Then $\tilde{\rho}$ has trivial restriction to $N \cap N_D$ and by Theorem 1.6 acts like $\hat{\rho} = \rho$ on $G_D(\tilde{\mathfrak{P}}/\mathfrak{P}) \cong \text{Gal}(\bar{N}/\bar{N}_D)$ with $\bar{N}_D := \bar{\mathbb{Q}}(N \cap N_D)$. Since $\tilde{\rho}|_{\tilde{k}} = \rho|_{\tilde{k}} = \rho_a$ these actions commute with the canonical epimorphism ψ_a . \square

Using Theorem 1.6 we may deduce from this proposition the following result, which in the case of three ramification points originates from Serre (1988):

Theorem 10.3 (Fried and Dèbes (1990)). *Let $N/k(t)$ be a geometric Galois extension with group G over a real number field k , whose ramification locus $\mathcal{S} \subseteq \mathbb{P}^1(\bar{\mathbb{Q}})$ of $\bar{\mathbb{Q}}N = \bar{N}_\sigma$ has the standard form as in Figure 1.2. Assume furthermore that the prime divisor $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ belonging to the base point $a := \mathscr{P}_0$ stays inert in $N/k(t)$. Then the corresponding residue field extension N_a/k is Galois with*

$$G_a := \text{Gal}(N_a/k) \cong G. \quad (10.7)$$

Moreover, the complex conjugation $\rho_a \in G_a$ acts on G_a via

$$\psi_a(\sigma)^{\rho_a} = \psi_a(\sigma^\rho) \quad (10.8)$$

with the canonical epimorphism ψ_a in (10.5) from G onto G_a , and

$$\sigma^\rho = (\sigma_{2r}^{-1}, \dots, \sigma_1^{-1}, \sigma_{2r+1}^{-1}, \dots, (\sigma_s^{-1})^{\sigma_{s-1}^{-1} \cdots \sigma_{2r+1}^{-1}}). \quad (10.9)$$

In the case $\mathcal{Z}(G) = 1$ this uniquely determines the conjugacy class of $\rho_a \in G_a$ depending on $[\sigma]$.

Proof. Let $\tilde{\mathfrak{P}}$ denote the unique extension of \mathfrak{P} onto N . Then we have $G_D(\tilde{\mathfrak{P}}/\mathfrak{P}) \cong G$ and hence (10.7) follows. Now identifying $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$ with $\text{Gal}(N/k(t))$ we obtain the generators σ_i of inertia subgroups of $N/k(t)$ by $\sigma_i = (\varphi_\sigma \circ \psi_\sigma)(\gamma_i)$, with the canonical epimorphisms $\psi_\sigma, \varphi_\sigma$ from the Hurwitz classification (4.5). With this the action of ρ_a on G_a follows directly from Theorem 1.6, using (10.6) and the Remark after Theorem 2.2. Finally in the case $\mathcal{X}(G) = 1$ by (10.8) and (10.9) the action of ρ_a is uniquely determined by ψ_a and σ . Hence the conjugacy class of ρ_a in $G_a \cong G$ is already determined by $[\sigma]$. \square

Remark. Obviously, the field N_a in Theorem 10.3 is real, i.e., a subfield of $\bar{\mathbb{Q}}^\rho$, precisely when $\rho_a = 1$.

By the Structure Stability Theorem 10.1 the conjugacy class of $\rho_a \in G_a$ remains constant as long as the reference point $a \in \mathbb{P}^1(k)$ belonging to \mathfrak{P} varies in the connected component \mathcal{O} of $\mathbb{P}^1(\mathbb{R})$ lying between $a_s := \mathcal{P}_s$ and $a_{2r+1} := \mathcal{P}_{2r+1}$ (compare with Figure 1.2). Otherwise the transformation formulae for the complex conjugation ρ change, and with this in general also the class of ρ_a . But at least the following result holds, which was first proved in the case $s = 3$ by Serre (1992), 8.4.3:

Proposition 10.4. *The conjugacy class of the complex conjugation $\psi_a^{-1}(\rho_a) \in G$ for $a \in \mathbb{P}^1(k)$ remains unchanged when a passes through a point $a_i \in \mathcal{S}$ for which the generator σ_i of the inertia group has odd centralizer order in $\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t))$.*

Proof. We give the proof for the passage from $a \in (a_s, a_{2r+1})$ to $b \in (a_{2r+1}, a_{2r+2})$. The complex conjugation with respect to the base point b satisfies

$$\psi_b(\sigma)^{\rho_b} = \psi_a(\sigma^{\rho\sigma_{2r+1}})$$

and thus

$$\sigma_{2r+1}^{\psi_b^{-1}(\rho_b)} = \sigma_{2r+1}^{-1} = \sigma_{2r+1}^{\psi_a^{-1}(\rho_a)}.$$

So $\tilde{\sigma}_{2r+1} := \psi_a^{-1}(\rho_a)\psi_b^{-1}(\rho_b)$ lies in the centralizer of σ_{2r+1} in G , and thus has odd order $n := o(\tilde{\sigma}_{2r+1})$. The dihedral group

$$\langle \psi_a^{-1}(\rho_a), \psi_b^{-1}(\rho_b) \rangle \cong D_n$$

hence contains a single class of involutions, which proves that $\psi_a^{-1}(\rho_a)$ and $\psi_b^{-1}(\rho_b)$ are conjugate in D_n and so also in G . \square

Remark. If we have $s = 3, r = 0$ and $\mathcal{X}(G) = 1$ in Proposition 10.4, then we even have $\tilde{\sigma}_j = \sigma_j$ for $j = 1, 2, 3$, and it suffices to assume that $o(\sigma_i)$ is odd.

Example 10.2 (Serre (1988)). If the Galois extension $N/G\mathbb{Q}(t)$ with $\mathcal{X}(G) = 1$ and three real ramification points possesses real specializations $N_a/G\mathbb{Q}$, then it follows that $G \cong S_3$. Indeed, if $\rho_a = 1$ for the standard configuration, then by the above remark we have $\sigma_1 = \psi_b^{-1}(\rho_b)$ and $\sigma_3 = \psi_c^{-1}(\rho_c)$ with $b \in (a_1, a_2)$ and $c \in (a_2, a_3)$. Thus G , being generated by two involutions, is isomorphic to a dihedral group D_n .

From this the assertion follows since the class vectors of type $(2, 2, n)$ of D_n are not rational for odd $n > 3$. \square

From Theorem 10.3 we may further deduce:

Corollary 10.5. $\bar{\mathbb{Q}}^\rho(t)$ is a field of definition of $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$ precisely when there exists an involution $\tau \in G$ satisfying $\sigma^\rho = \sigma^\tau$.

Proof. If $\bar{\mathbb{Q}}^\rho(t)$ is a field of definition of $\bar{N}_\sigma/G\bar{\mathbb{Q}}(t)$, then the complex conjugation ρ acts as an inner automorphism on G , and there exists an involution $\tau \in G$ with $\sigma^\rho = \sigma^\tau$. Conversely from the existence of such an involution τ it follows that the fixed field N of $\langle \rho\tau \rangle$ is a geometric Galois extension of $\bar{\mathbb{Q}}^\rho(t)$ with $\bar{\mathbb{Q}}N = \bar{N}_\sigma$. \square

Example 10.3 (Fried and Dèbes (1990)). If in Corollary 10.5 all ramification points are real, then

$$\sigma^\rho = (\sigma_1^{-1}, (\sigma_2^{-1})^{\sigma_1^{-1}}, \dots, (\sigma_s^{-1})^{\sigma_{s-1}^{-1} \cdots \sigma_1^{-1}}) = \sigma^\tau.$$

In particular G is then generated by the involutions

$$\tau_i := \tau\sigma_1 \cdots \sigma_i \quad \text{for } i = 1, \dots, s$$

(with $\tau_s = \tau$). Conversely each generation by involutions $G = \langle \tau_1, \dots, \tau_s \rangle$ with $\tau := \tau_s$, $\sigma_1 := \tau_s\tau_1$ and $\sigma_i := \tau_{i-1}\tau_i$ for $i = 2, \dots, s$ yields the sufficient condition $\sigma^\rho = \sigma^\tau$ for real fields of definition (with respect to the standard configuration in Figure 1.2). \square

For a study of the ramification in the residue class field extensions the reduction of constants has to be utilized. This also yields restrictions on the primes of \mathbb{Q} ramified in minimal fields of definition.

10.3 Ramification in Minimal Fields of Definition

Let \mathfrak{o} denote the valuation ring and \mathfrak{p} the valuation ideal of a valuation of $\bar{\mathbb{Q}}$ extending the p -valuation for some rational prime p . The corresponding residue homomorphism $\kappa : \mathfrak{o} \rightarrow \bar{\mathbb{F}}_p$ can be extended to a place

$$\wp : \mathbb{P}^1(\bar{\mathbb{Q}}) \rightarrow \mathbb{P}^1(\bar{\mathbb{F}}_p), \quad a \mapsto \bar{a}, \tag{10.10}$$

by setting $\wp(a) = \infty$ for $a \notin \mathfrak{o}$. A finite subset $\mathcal{S} \subseteq \mathbb{P}^1(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}} \cup \infty$ is called \wp -stable (or also \mathfrak{p} -stable) if \wp is injective on \mathcal{S} , i.e., if $|\bar{\mathcal{S}}| = |\mathcal{S}|$. With these notations the following theorem holds, which was first proved by Grothendieck (1971), Exp. XIII, Cor. 2.12 (see also Popp (1970), Satz 12.1).

Theorem 10.6 (Grothendieck (1971)). *Let \mathfrak{p} be an extension of (p) onto $\bar{\mathbb{Q}}$ and $\mathcal{S} \subseteq \mathbb{P}^1(\bar{\mathbb{Q}})$ a finite \mathfrak{p} -stable subset. Then the maximal factor groups of p -prime order*

of the algebraic fundamental groups $\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{\mathbb{Q}}) \setminus \mathcal{S})$ and $\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{\mathbb{F}}_p) \setminus \bar{\mathcal{S}})$ are isomorphic via the specialization homomorphism:

$$\pi_1^{(p)}(\mathbb{P}^1(\bar{\mathbb{Q}}) \setminus \mathcal{S}) \cong \pi_1^{(p)}(\mathbb{P}^1(\bar{\mathbb{F}}_p) \setminus \bar{\mathcal{S}}). \quad (10.11)$$

The isomorphism is uniquely determined by \mathfrak{p} up to an inner automorphism.

Thus also the Hurwitz classification of Galois extensions with p -prime order of the Galois group carries over in a canonical way from $\bar{\mathbb{Q}}(t)$ to $\bar{\mathbb{F}}_p(t)$. If $\mathbb{S}, \bar{\mathbb{S}}$ denote the sets of prime divisors in $\bar{\mathbb{Q}}(t)$ resp. $\bar{\mathbb{F}}_p(t)$ corresponding to \mathcal{S} resp. $\bar{\mathcal{S}}$, and $\bar{M}_{\mathbb{S}}^{(p)}, \bar{M}_{\bar{\mathbb{S}}}^{(p)}$ the maximal algebraic Galois extensions unramified outside of \mathbb{S} , resp. $\bar{\mathbb{S}}$, and with degree not divisible by p , then the corresponding Galois groups are isomorphic by Theorem 10.6:

$$\text{Gal}(\bar{M}_{\mathbb{S}}^{(p)} / \bar{\mathbb{Q}}(t)) \cong \text{Gal}(\bar{M}_{\bar{\mathbb{S}}}^{(p)} / \bar{\mathbb{F}}_p(t)). \quad (10.12)$$

In particular the valuation ideal \mathfrak{p}_t of $\bar{\mathbb{Q}}(t)$ corresponding to the t -functional valuation given by \mathfrak{p} with trivial value at t possesses an inert extension $\bar{\mathfrak{p}}_t$ on $\bar{M}_{\mathbb{S}}^{(p)}$.

Corollary 10.7. *Let G be a finite group with p -prime order. Then the map defined by*

$$\bar{N}_{\bar{\mathbb{S}}} : \Sigma_s(G)/\text{Inn}(G) \rightarrow \bar{N}_{\bar{\mathbb{S}}}(G), \quad [\sigma] \mapsto \bar{N}_{\sigma}^{(p)} := (\bar{M}_{\bar{\mathbb{S}}}^{(p)})^{\ker(\sigma)}, \quad (10.13)$$

is surjective and compatible with reduction of constants, i.e., the restriction $\bar{\mathfrak{p}}_t$ of the t -functional extension $\bar{\mathfrak{p}}_t$ of \mathfrak{p} on $\bar{M}_{\mathbb{S}}^{(p)}$ satisfies

$$\bar{N}_{\sigma}^{(p)} = \bar{N}_{\sigma} \bar{\mathfrak{p}}_t. \quad (10.14)$$

From Theorem 10.6 and Corollary 10.7 one may deduce restrictions on the ramification in minimal fields of definition. This is contained in the following important result:

Theorem 10.8 (Beckmann (1989)). *Let G be a finite group, $\sigma \in \Sigma_s(G)$ and $\bar{N}_{\sigma} \in \bar{N}_{\bar{\mathbb{S}}}(G)$ with $\mathbb{S}^{\Delta} = \mathbb{S}$ for $\Delta = \text{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$. Then any prime $p \in \mathbb{P}$ ramified in the field of constants of $k_{\sigma}(t) = \bar{\mathbb{Q}}(t)^{\Delta_{\sigma}}$ either divides the group order $|G|$ or is such that \mathcal{S} is not p -stable.*

Proof. Let p be a prime which does not divide $|G|$ and for which \mathcal{S} is p -stable. In a first step we show that all prime divisors \mathfrak{p} of p are unramified in k_{σ}/k_{σ^A} with $A = \text{Aut}(G)$. For this, let \mathfrak{p}_t be the functional extension of \mathfrak{p} on $k_{\sigma^A}(t)$ and $\bar{\mathfrak{p}}_t$ an extension of \mathfrak{p}_t on \bar{N}_{σ} . Since $\bar{\mathfrak{p}}_t$ remains inert in $\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t)$ by Corollary 10.7, the inertia group Γ_I of $\bar{\mathfrak{p}}_t/\mathfrak{p}_t$ in the Galois extension $\bar{N}_{\sigma}/k_{\sigma^A}(t)$ together with $G = \text{Gal}(\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t))$ generates a subgroup $\tilde{\Gamma}$ of the splitting group Γ_D of $\bar{\mathfrak{p}}_t/\mathfrak{p}_t$. Now Γ_I is normal in Γ_D (see for example Nagata (1977), Thm. 7.3.2), hence Γ_I is also normal in $\tilde{\Gamma}$ with $\Gamma_I \cap G = 1$, which shows that $\tilde{\Gamma} = \Gamma_I \times G$. Hence the fixed field $\tilde{k}(t)$ of $\tilde{\Gamma}$ constitutes a field of definition of $\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t)$ with the property that

$\bar{\mathfrak{p}}_t|_{\tilde{k}}$ is unramified in \tilde{k}/k_{σ^A} . Since any automorphism of $\bar{\mathbb{Q}}(t)/k_{\sigma}(t)$ acts as inner automorphism on G , k_{σ} lies inside \tilde{k} . So all prime divisors of \mathfrak{p} and also of p are unramified in k_{σ}/k_{σ^A} .

In the second step let \bar{N}^* denote the composite of all $\bar{N}_{\sigma}^{\delta}$ for $\delta \in \Delta$, $G^* := \text{Gal}(\bar{N}^*/\bar{\mathbb{Q}}(t))$ and $[\sigma^*]$ the classifying class of generating s -systems of G^* : $\bar{N}^* = \bar{N}_{\sigma^*}$. Since $\bar{N}^*/\bar{\mathbb{Q}}(t)$ is Galois, $\bar{\mathbb{Q}}(t)$ is a field of definition for $\bar{N}^*/\bar{\mathbb{Q}}(t)$ by Theorem 3.5, and we have $k_{(\sigma^*)^A} = \mathbb{Q}$. Further, k_{σ^*} is obtained as the composite of all k_{σ}^{δ} with $\delta \in \Delta$ and thus coincides with the Galois closure of k_{σ}/\mathbb{Q} . Since all prime divisors of $|G^*|$ already divide $|G|$, and \mathcal{S} does not change since $\mathbb{S}^{\Delta} = \mathbb{S}$, we conclude from the first step that p is unramified in k_{σ^*}/\mathbb{Q} and hence a fortiori in k_{σ}/\mathbb{Q} . \square

Remark. If in the case $s = 3$ we choose the ramification locus $\{0, 1, \infty\}$, the assumption of p -stability in Theorem 10.8 is automatically satisfied.

10.4 Ramification in Residue Fields

Let $N/k(t)$ be a geometric Galois extension over a number field k and $\mathfrak{p} \in \mathbb{P}(k)$. We say that $N/k(t)$ has *good reduction modulo \mathfrak{p}* if the t -functional extension $\tilde{\mathfrak{p}}_t$ of \mathfrak{p} on $k(t)$ possesses an inert extension $\bar{\mathfrak{p}}_t$ on $N/k(t)$, such that the residue field extension $N\bar{\mathfrak{p}}_t/k\mathfrak{p}(t)$ is geometric and moreover we have

$$\text{Gal}(N\bar{\mathfrak{p}}_t/k\mathfrak{p}(t)) \cong \text{Gal}(N/k(t)). \quad (10.15)$$

If then the norm of \mathfrak{p} is coprime to the group order, and the ramification locus is \mathfrak{p} -stable, it follows from Corollary 10.7 that

$$\bar{\mathbb{F}}_p(N\bar{\mathfrak{p}}_t) = (\bar{\mathbb{Q}}N)\bar{\mathfrak{p}}_t \quad (10.16)$$

for each extension $\bar{\mathfrak{p}}_t$ of $\tilde{\mathfrak{p}}_t$ onto $\bar{\mathbb{Q}}N$. Conversely we have only the following weaker result, which was first proved by Beckmann (1991), Prop. 2.3, using different methods:

Proposition 10.9. *Let $N/k(t)$ be a geometric Galois extension, whose Galois group has trivial center and p -prime order, and $\mathfrak{p} \in \mathbb{P}(k)$ an extension of (p) , with respect to which the ramification locus $\mathcal{S} \subseteq \mathbb{P}^1(k)$ of $N/k(t)$ is \mathfrak{p} -stable. Then $N/k(t)$ has good reduction modulo \mathfrak{p} .*

Proof. From the \mathfrak{p} -stability of the ramification locus we conclude with Corollary 10.7 that the t -functional valuation ideal \mathfrak{p}_t of $k(t)$ has an extension $\bar{\mathfrak{p}}_t$ onto $\bar{\mathbb{Q}}N$ with

$$\text{Gal}((\bar{\mathbb{Q}}N)\bar{\mathfrak{p}}_t/\bar{\mathbb{F}}_p(t)) \cong \text{Gal}(\bar{\mathbb{Q}}N/\bar{\mathbb{Q}}(t)) \cong \text{Gal}(N/k(t)) = G.$$

Now let $\bar{N} := \bar{\mathbb{Q}}N$, $\Gamma := \text{Gal}(\bar{N}/k(t))$ and Γ_D and Γ_I the splitting group and the inertia group of $\bar{\mathfrak{p}}_t$ in Γ . Since $\bar{\mathfrak{p}}_t$ is inert in $\bar{N}/\bar{\mathbb{Q}}(t)$, Γ_I and $\bar{G} := \text{Gal}(\bar{N}/\bar{\mathbb{Q}}(t))$

generate a subgroup $\tilde{\Gamma}$ of Γ_D . This forces $\Gamma_I \trianglelefteq \tilde{\Gamma}$ and $\Gamma_I \cap \tilde{G} = 1$, from which it follows that $\tilde{\Gamma} = \Gamma_I \times \tilde{G}$. Thus Γ_I is a subgroup of $\mathcal{C}_\Gamma(\tilde{G}) = \text{Gal}(\bar{N}/N)$, and $\tilde{\mathfrak{p}}_t$ does not ramify in $N/k(t)$.

We have $\Gamma_D \geq \tilde{G}$, so the fixed field of Γ_D is an intermediate field of $\bar{\mathbb{Q}}(t)/k(t)$, say $\bar{N}^{\Gamma_D} = k'(t)$, and we set $N' := k'N$. Since Γ_I then also lies in $\text{Gal}(\bar{N}/N')$, $\tilde{\mathfrak{p}}_t$ has relative degree $n := |G|$ in $N'/k'(t)$. Since $\Gamma_D \cap \text{Gal}(\bar{N}/N) = \text{Gal}(\bar{N}/N')$, the relative degree of $\tilde{\mathfrak{p}}_t$ in N'/N is equal to 1. So the restriction $\tilde{\mathfrak{p}}_t$ of $\tilde{\mathfrak{p}}_t$ has residue degree n in $N/k(t)$. This shows that \mathfrak{p}_t is inert in $N/k(t)$, and we have

$$\text{Gal}(N\tilde{\mathfrak{p}}_t/k\mathfrak{p}(t)) \cong \text{Gal}(N/k(t)).$$

It remains to show that $N\tilde{\mathfrak{p}}_t/k\mathfrak{p}$ is regular, i.e., that $\bar{\mathbb{F}}_p(N\tilde{\mathfrak{p}}_t) = (\bar{\mathbb{Q}}N)\tilde{\mathfrak{p}}_t$. If this were not the case, $N\tilde{\mathfrak{p}}_t/k\mathfrak{p}(t)$ and also $N'\tilde{\mathfrak{p}}'_t/k\mathfrak{p}(t)$, with the restriction $\tilde{\mathfrak{p}}'_t$ of $\tilde{\mathfrak{p}}_t$ to N' , would contain a non-trivial extension of constants, which since $\mathcal{Z}(G) = 1$ contradicts the fact that

$$\text{Gal}(\bar{N}\tilde{\mathfrak{p}}_t/N'\tilde{\mathfrak{p}}'_t) \leq \mathcal{C}_{\tilde{\Gamma}}(\text{Gal}(\bar{N}\tilde{\mathfrak{p}}_t/\bar{\mathbb{F}}_p(t)))$$

with $\tilde{\Gamma} := \text{Gal}(\bar{N}\tilde{\mathfrak{p}}_t/k\mathfrak{p}(t))$. □

The assumption $\mathcal{Z}(G) = 1$ in Proposition 10.9 is necessary, as can be seen in the following simple example:

Example 10.4. The Galois extension $N/\mathbb{Q}(t)$ with group Z_2 generated by $x^2 = 3t$ obviously has bad reduction modulo 3, although the prime 3 does not divide the group order, and moreover $\mathcal{S} = \{0, \infty\}$ is 3-stable. □

Under the assumption of good reduction modulo p the ramification in the specialized field extension N_a/k can be described.

Theorem 10.10 (Beckmann (1991)). *Let $N/k(t)$ be a finite geometric Galois extension with group G over $k \leq \bar{\mathbb{Q}}$, where $\bar{\mathbb{Q}}N = \bar{N}_\sigma \in \mathbf{N}_\mathbf{s}(G)$, and with the set $\mathcal{S} = \{a_1, \dots, a_s\} \subseteq \mathbb{P}^1(\bar{\mathbb{Q}})$ of zeroes of the $\mathfrak{P}_i \in \mathbf{S}$. If $N/k(t)$ has good reduction modulo $\mathfrak{p} \in \mathbb{P}(k)$ and \mathcal{S} is \mathfrak{p} -stable, then for $a \in \mathbb{P}^1(k) \setminus \mathcal{S}$ there exists at most one i with $e_i := \text{ord}_\mathfrak{p}(a - a_i) \neq 0$, and the inertia group of an extension $\tilde{\mathfrak{p}}$ of \mathfrak{p} on the residue class field N_a is either trivial or it is generated by the canonical image $\varphi_a(\tau)$ in $G_a = \text{Gal}(N_a/k)$ of an element $\tau \in G$ conjugate to $\sigma_i^{e_i}$ in G .*

The proof would lead us too far astray, so we refer to the original paper Beckmann (1991), Sect. 3. This theorem implies the following weak but explicit version of the Hilbert Irreducibility Theorem:

Corollary 10.11. *In Theorem 10.10 we have $G_a \cong G$, if all $\tau \in \mathbf{C}^\mathbf{e}$ with $\mathbf{e} := (e_1, \dots, e_s)$ generate the group G , where $\mathbf{C} \in \text{Cl}(G)^s$ denotes the class vector of G with $\sigma \in \Sigma(\mathbf{C})$.*

Example 10.5 (Beckmann (1991))). For a prime n we consider the polynomial

$$f(t, X) = X^n - t(nX - n + 1) \in \mathbb{Q}(t)[X]$$

with group S_n from Theorem 9.4. If we specialize the variable t to $a \in \mathbb{Q} \setminus \{0, 1\}$ and if there exists a prime $p > n$ such that $\text{ord}_p(a)$ is prime to n and $\text{ord}_p(a - 1)$ is odd, then $f(a, X) \in \mathbb{Q}[X]$ has Galois group S_n and in particular remains irreducible. This follows with the calculations in (9.2) immediately from Corollary 10.11, since for prime n any group containing an n -cycle is primitive, and a primitive group containing a transposition equals already S_n by a theorem of Jordan. \square

II Applications of Rigidity

It is perhaps astonishing that the rigidity criteria developed in the previous chapter do indeed apply to a wide variety of finite groups, in particular to non-abelian finite simple groups. In fact, it turns out that most of these groups satisfy some form of the rigidity criterion, at least over the field $\mathbb{Q}^{\text{ab}}(t)$.

Assuming the classification of finite simple groups we know that the non-abelian finite simple groups are the alternating groups, the groups of Lie type, and the 26 sporadic simple groups. It was already shown in Theorem I.5.3 that all alternating groups occur as Galois groups over $\mathbb{Q}(t)$. The classical groups of Lie type comprise the linear, unitary, symplectic and various orthogonal groups defined over finite fields \mathbb{F}_q . By construction they all possess a natural matrix representation over \mathbb{F}_q . Belyi (1979, 1983) found an ingenious way to make use of such matrix representations (Theorem I.5.10). His result, which proves that all simple classical groups of Lie type occur as geometric Galois groups over suitable abelian number fields, can be considered as the first major step in realizing nonsolvable groups as Galois groups. A different proof of his results for the classical groups, using the classification of irreducible pseudo-reflection groups, was later given by Walter (1984). We present Belyi's proof for the general linear groups in the first Paragraph. For the other classical groups we avoid the rather heavy computations with Steinberg generators necessary in Belyi's approach and rather follow Walter's approach, making use of a nice effective version of Belyi's criterion due to Völklein (1998).

To treat the exceptional groups of Lie type we have to employ much deeper methods, in particular the Deligne-Lusztig character theory for groups of Lie type and the classification of the finite simple groups. In Paragraphs 4 and 5 the character theoretic form of the rigidity criterion is shown to apply to most of the exceptional groups of Lie type, a result which is due to Malle (1988b, 1992) in good characteristic and to Lübeck and Malle (1998) in bad characteristic different from 2.

The results for Galois realizations of simple groups over $\mathbb{Q}(t)$ at present are far from complete. We present results of Malle (1996) and Reiter (1999) concerning the classical groups in Paragraph 6 and 7, and those of Malle (1988b, 1992) on the exceptional groups of Lie type in Paragraph 8. See also some further results obtained

by different methods in Chapter III.10. While the classical groups can again be treated with the Belyi Criterion, the Deligne-Lusztig theory is needed for the other cases. In this context we also prove some stronger results on realization of groups of automorphisms of classical groups over $\mathbb{Q}^{\text{ab}}(t)$.

Finally, the 26 sporadic groups are covered by ad hoc arguments in the final paragraph. It turns out that all but possibly the Mathieu group M_{23} have GA-realizations even over the field of rational numbers. The proper references for the sporadic groups are given at the beginning of Paragraph 9.

For better reference we collect in Paragraph 10 the G- and GA-realizations proved in this chapter.

1 The General Linear Groups

The first paragraph is devoted to the case of the linear groups, where the calculations are given in some detail. In this case the verification of rigidity comes down to matrix computations, see also Matzat (1987), II.5.2.

Before presenting this elementary proof we first collect some notions and results from the theory of linear algebraic groups. While this theory is not needed for the treatment of the general linear groups in the subsequent sections, it still provides a more natural language for the formulation of certain facts. In the later paragraphs, the remaining series of groups of Lie type will then be considered under this point of view.

1.1 Groups of Lie Type

It is most natural to consider the classical groups from the point of view of algebraic groups. For a short introduction see for example Carter (1985). The details may be found in Steinberg (1967) or Carter (1989).

Let G be a connected reductive algebraic group over the algebraic closure \bar{k} of a finite field $k = \mathbb{F}_q$. Let T be a maximal torus of G , contained in a Borel subgroup B . Then B is the semidirect product of its unipotent radical $U = R_u(B)$ with T . There exists a unique opposite Borel subgroup B^- determined by the property that $B \cap B^- = T$. With its unipotent radical $U^- = R_u(B^-)$ we then have $B^- = U^-T$. Let $\text{Hom}(T, \bar{k}^\times)$ denote the group of algebraic homomorphisms from T to the group of algebraic automorphisms of the additive group of \bar{k} , which is isomorphic to \bar{k}^\times . The minimal non-trivial subgroups of U and U^- normalized by T are connected unipotent algebraic groups of dimension one, isomorphic to the additive group of \bar{k} . The action of T on such a subgroup X defines an element $\alpha \in \text{Hom}(T, \bar{k}^\times)$, a so-called *root*. Distinct subgroups give rise to distinct roots, thus the minimal T -invariant subgroups X of U and U^- may be indexed by roots: $X = X_\alpha \cong \bar{k}$. We write

$$\Phi^\pm(G) := \{\alpha \mid \text{there exists } X \subset U^\pm \text{ with } X = X_\alpha\},$$

for the sets of positive resp. negative roots. For any positive root α , $-\alpha$ is also a root. It can be shown that there exists a surjective homomorphism $\text{SL}_2(\bar{k}) \rightarrow \langle X_\alpha, X_{-\alpha} \rangle$ onto the group generated by the corresponding root subgroups. The preimage of $T \cap \langle X_\alpha, X_{-\alpha} \rangle$ is a maximal torus of $\text{SL}_2(\bar{k})$, hence isomorphic to \bar{k}^\times . This defines an element $\alpha^\vee \in \text{Hom}(\bar{k}^\times, T)$, the *coroot* of α . The sets $\Phi(G) = \Phi^+(G) \cup \Phi^-(G)$ of roots and $\Phi^\vee(G) = \{\alpha^\vee \mid \alpha \in \Phi(G)\}$ of coroots define a root system in $\text{Hom}(T, \bar{k}^\times) \otimes \mathbb{R}$.

Now assume that G is defined over a finite field \mathbb{F}_q and let F be the corresponding Steinberg endomorphism $F : G \rightarrow G$. The group of fixed points $G := G^F$ is a finite group of Lie type. A result of fundamental importance in this area is the following (see for example Steinberg (1968)):

Theorem 1.1 (Lang–Steinberg). *Let \mathbf{G} be a connected algebraic group over an algebraically closed field of positive characteristic and $F : \mathbf{G} \rightarrow \mathbf{G}$ a surjective homomorphism such that \mathbf{G}^F is finite. Then the map*

$$L : \mathbf{G} \rightarrow \mathbf{G}, \quad \sigma \mapsto \sigma^{-1} F(\sigma),$$

is surjective.

As one of the many applications we sketch a proof of the following well-known result which will be of importance in proving generation:

Proposition 1.2. *Let \mathbf{G} be a connected reductive algebraic group, $F : \mathbf{G} \rightarrow \mathbf{G}$ a surjective homomorphism such that \mathbf{G}^F is finite and \mathbf{T} an F -stable maximal torus of \mathbf{G} . Let $\varphi : \tilde{\mathbf{G}} \rightarrow [\mathbf{G}, \mathbf{G}]$ be the simply-connected covering of the derived group of \mathbf{G} (see Borel et al. (1970), E-27). Then $G := \mathbf{G}^F$ is generated by $\varphi(\tilde{\mathbf{G}}^F)$ together with \mathbf{T}^F .*

Indeed, since \mathbf{G} is connected the map $\sigma \mapsto \tilde{\sigma}^{-1} F(\tilde{\sigma})$ (where $\tilde{\sigma} \in \tilde{\mathbf{G}}$ is such that $\varphi(\tilde{\sigma}) = \sigma$) defines an isomorphism of $G/\varphi(\tilde{\mathbf{G}}^F)$ with $\ker(\varphi)/(1 - F)\ker(\varphi)$. Now let $\tilde{\mathbf{T}}$ be the F -stable torus in $\tilde{\mathbf{G}}$ with $\varphi(\tilde{\mathbf{T}}) = \mathbf{T}$. This also contains the central subgroup $\ker(\varphi)$ and is connected. Thus by the same arguments we obtain that $T/(T \cap \varphi(\tilde{\mathbf{G}}^F)) \cong \ker(\varphi)/(1 - F)\ker(\varphi)$, where $T := \mathbf{T}^F$. But then $G/\varphi(\tilde{\mathbf{G}}^F) \cong T/(T \cap \varphi(\tilde{\mathbf{G}}^F))$ as claimed.

The action of F on \mathbf{G} induces an action on the Dynkin diagram of the root system Φ associated to \mathbf{G} . If this action is trivial, we call F an untwisted, otherwise a twisted Steinberg map. If we start from simple simply-connected groups \mathbf{G} of types A_n, B_n, C_n or D_n , then among the resulting finite groups we find all the universal classical groups listed in Table 1.1. The first column gives the Lie notation for $G = \mathbf{G}^F$, the second column identifies these groups with classical matrix groups. The cases of B_2 in characteristic 2 with F inducing the exceptional graph automorphism, and of D_4 with F inducing the triality automorphism will be considered in the section on exceptional groups.

Table 1.1 Classical groups

G		$R(G)$	$\mathcal{N}_{\mathrm{GL}(V)}(R(G))$
$A_n(q)_{sc}$	$\mathrm{SL}_{n+1}(q)$	$n \geq 1$	$\mathrm{SL}_{n+1}(q)$
$B_n(q)_{sc}$	$\mathrm{Spin}_{2n+1}(q)$	$2 \nmid q, n \geq 3$	$\mathrm{O}_{2n+1}(q)$
$C_n(q)_{sc}$	$\mathrm{Sp}_{2n}(q)$	$n \geq 2$	$\mathrm{Sp}_{2n}(q)$
$D_n(q)_{sc}$	$\mathrm{Spin}_{2n}^+(q)$	$n \geq 4$	$\Omega_{2n}^+(q)$
${}^2A_n(q)_{sc}$	$\mathrm{SU}_{n+1}(q)$	$n \geq 2$	$\mathrm{SU}_{n+1}(q)$
${}^2D_n(q)_{sc}$	$\mathrm{Spin}_{2n}^-(q)$	$n \geq 4$	$\Omega_{2n}^-(q)$

Each of the above groups possesses a natural matrix representation R on a vector space V over \mathbb{F}_q (respectively over \mathbb{F}_{q^2} for the unitary groups) whose dimension is given by the lower index in the classical notation for G . This representation $R : G \rightarrow \text{Aut}(V)$ is not necessarily faithful. The image of G under R is given in the fourth column. The last column describes the full normalizer of $R(G)$ in the general linear group on V . This will be needed for the application of Belyi's criterion. The correctness of the entries in the last column will be shown in the subsections treating the individual cases. In the third column we have indicated restrictions on q and n which can be made so as to avoid duplications stemming from generic isomorphisms. Under these restrictions, still all simple classical groups of Lie type occur as a non-abelian composition factor of one of the groups listed (see for example Carter (1989), 11.3 and 14.5).

In the next sections we present the elementary rigidity proof for $\text{GL}_n(q)$ in some detail.

1.2 Rigidity for $\text{GL}_n(q)$

Let $k = \mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is prime. We first prove rigidity for the general linear group $\text{GL}_n(\mathbb{F}_q)$ which, following the usual convention in finite group theory, we will denote by $\text{GL}_n(q)$.

Denote by $\mathbf{G}' = \text{SL}_n(\bar{k})$ the simple, simply connected algebraic group of type A_{n-1} over the algebraic closure \bar{k} of k , so $G' := \mathbf{G}'^F$ is the special linear group over \mathbb{F}_q . The subgroup of diagonal matrices in G' forms a maximal torus T . With respect to a suitable orthonormal basis $\{\epsilon_1, \dots, \epsilon_n\}$ of $\text{Hom}(T, \bar{k}^\times) \otimes \mathbb{R}$ the set of roots is given by

$$\Phi := \{\epsilon_i - \epsilon_j \mid 1 \leq i, j \leq n, i \neq j\}.$$

We identify the root $\epsilon_i - \epsilon_j$ with the ordered pair (i, j) of indices. In the case of $\text{SL}_n(q)$, the root subgroup X_r corresponding to $r = (i, j)$ just consists of the matrices

$$X_{i,j} = \{x_{i,j}(u) := \text{Id} + uI_{i,j} \mid u \in \mathbb{F}_q\},$$

where $I_{i,j}$ denotes the matrix whose only non-zero entry lies at position (i, j) and equals 1.

The following commutator formulae follow immediately from the explicit description of the root subgroups:

$$[x_{i,j}(u), x_{k,l}(v)] = \begin{cases} x_{i,l}(uv) & \text{if } i \neq l, j = k, \\ x_{k,j}(-uv) & \text{if } i = l, j \neq k, \\ 1 & \text{if } i \neq l, j \neq k. \end{cases} \quad (1.1)$$

Next, for $\alpha \in \Phi$ and $u \in \mathbb{F}_q^\times$ let

$$w_\alpha(u) := x_\alpha(u)x_{-\alpha}(-u^{-1})x_\alpha(u), \quad h_\alpha(u) := w_\alpha(u)w_\alpha(1)^{-1}. \quad (1.2)$$

Then the $h_\alpha(u)$ lie in T , the $w_\alpha := w_\alpha(1)$ are contained in $\mathcal{N}_{G'}(T)$ and for $v \in \mathbb{F}_q^\times$ we have

$$w_\alpha(u)x_\alpha(v)w_\alpha(-u) = x_{-\alpha}(-u^{-2}v), \quad (1.3)$$

$$\begin{aligned} w_\alpha x_\beta(u)w_\alpha^{-1} &= x_{w_\alpha(\beta)}(\pm u), \\ h_\alpha(v)^{-1}x_\beta(u)h_\alpha(v) &= x_\beta(v^{-<\beta,\alpha>}u), \end{aligned} \quad (1.4)$$

where $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q^\times$. Here $<\beta, \alpha> := 2(\alpha, \beta)/(\beta, \beta)$, where (α, β) denotes the inner product on the root space.

We denote by $h(v)$ the element $\text{diag}(v, 1, \dots, 1)$ of $\text{GL}_n(q)$. It is easily verified that

$$\begin{aligned} h(v)^{-1}x_{1,i}(u)h(v) &= x_{1,i}(v^{-1}u), & h(v)^{-1}x_{i,1}(u)h(v) &= x_{i,1}(vu) \\ h(v)^{-1}w_{1,i}(u)h(v) &= w_{1,i}(uv^{-1}) \end{aligned} \quad (1.5)$$

for $2 \leq i \leq n$, while $h(v)$ commutes with all $x_{i,i+1}(u)$ for $i > 1$. Due to the different forms of defining relations (1.1), (1.3), we have to distinguish between the rank one case and the general case:

Proposition 1.3. *Let v be a generator of \mathbb{F}_q^\times .*

- (a) *The group $\text{GL}_2(q)$, $q \geq 3$, is generated by $\sigma_1 := h(v)$ and $\sigma_2 := x_{1,2}(1)w_{1,2}$.*
- (b) *The group $\text{GL}_n(q)$, $n \geq 3$, is generated by the elements $\sigma_1 := x_{1,2}(1)$ and $\sigma_2 := w_{n-1,n} \cdots w_{1,2}h(v) = (\prod_{i=1}^{n-1} w_{n-i,n-i+1})h(v)$.*

Proof. Let $H := \langle \sigma_1, \sigma_2 \rangle$.

We first consider (a). There we have

$$\begin{aligned} \sigma_2\sigma_1\sigma_2^{-1} &= x_{1,2}(1)w_{1,2}h(v)w_{1,2}(-1)x_{1,2}(-1) \\ &= x_{1,2}(1)h(v)w_{1,2}(v^{-1})w_{1,2}(-1)x_{1,2}(-1) \quad \text{by (1.5)} \\ &= h(v)x_{1,2}(v^{-1})h_{1,2}(v^{-1})x_{1,2}(-1) \quad \text{by (1.2)} \\ &= h(v)h_{1,2}(v^{-1})x_{1,2}(v-1) \quad \text{by (1.4)}, \end{aligned}$$

so the commutator

$$\begin{aligned} [\sigma_1, \sigma_2\sigma_1\sigma_2^{-1}] &= h(v^{-1})x_{1,2}(1-v)h(v)x_{1,2}(v-1) \\ &= x_{1,2}\left(\frac{1-v}{v}\right)x_{1,2}(v-1) = x_{1,2}(u), \quad \text{where } u := \frac{(v-1)^2}{v} \neq 0, \end{aligned}$$

is contained in H . Conjugating $x_{1,2}(u)$ by powers of σ_1 we obtain

$$\sigma_1^{-i}x_{1,2}(u)\sigma_1^i = h(v^{-i})x_{1,2}(u)h(v^i) = x_{1,2}(v^{-i}u),$$

so by the definition of v all of $X_{1,2}$ is contained in H , whence

$$x_{1,2}(-1)\sigma_2 = w_{1,2} \in H.$$

But $w_{1,2}^{-1}X_{1,2}w_{1,2} = X_{2,1}$ by (1.3), hence also $X_{2,1} \subset H$. It is well known that $\mathrm{SL}_2(q)$ is generated by $X_{1,2}, X_{2,1}$ so the group H contains $\mathrm{SL}_2(q)$, and since $\det(\sigma_1) = v$ we conclude that $H = \mathrm{GL}_2(q)$.

In case (b) we first verify that (1.4) here takes the form

$$\begin{aligned} w_{2,3}(-1)x_{1,2}(1)w_{2,3} &= x_{2,3}(-1)x_{3,2}(1)x_{2,3}(-1)x_{1,2}(1)x_{2,3}(1)x_{3,2}(-1)x_{2,3}(1) \\ &= x_{2,3}(-1)x_{3,2}(1)x_{1,2}(1)x_{1,3}(1)x_{3,2}(-1)x_{2,3}(1) \\ &= x_{2,3}(-1)x_{1,2}(1)x_{1,2}(-1)x_{1,3}(1)x_{2,3}(1) = x_{1,3}(1) \end{aligned}$$

using (1.2) and (1.1), and similarly

$$w_{1,2}(1)x_{1,3}(-1)w_{1,2} = x_{1,2}(-1)x_{2,3}(1)x_{1,3}(1)x_{1,2}(1) = x_{2,3}(1),$$

while all $w_{i,i+1}$ with $i \geq 3$ commute with $x_{1,2}(1)$. With this we obtain

$$\begin{aligned} \sigma_2^{-1}\sigma_1\sigma_2 &= h(v^{-1})w_{1,2}(-1)\cdots w_{n-1,n}(-1)x_{1,2}(1)w_{n-1,n}\cdots w_{1,2}h(v) \\ &= h(v^{-1})w_{1,2}(-1)w_{2,3}(-1)x_{1,2}(1)w_{2,3}w_{1,2}h(v) \\ &= h(v^{-1})w_{1,2}(-1)x_{1,3}(1)w_{1,2}h(v) = h(v^{-1})x_{2,3}(1)h(v) = x_{2,3}(1), \end{aligned}$$

and then inductively

$$\sigma_2^{-i}\sigma_1\sigma_2^i = x_{i+1,i+2}(1) \in H, \quad \text{for } i = 0, \dots, n-2. \quad (1.6)$$

Finally,

$$\begin{aligned} \sigma_2^{-n+1}\sigma_1\sigma_2^{n-1} &= \sigma_2^{-1}x_{n-1,n}(1)\sigma_2 \\ &= h(v^{-1})w_{1,2}(-1)\cdots w_{n-1,n}(-1)x_{n-1,n}(1)w_{n-1,n}\cdots w_{1,2}h(v) \\ &= h(v^{-1})w_{1,2}(-1)\cdots w_{n-2,n-1}(-1)x_{n,n-1}(-1)w_{n-2,n-1}\cdots w_{1,2}h(v) \\ &= h(v^{-1})w_{1,2}(-1)\cdots w_{n-3,n-2}(-1)x_{n,n-2}(1)w_{n-3,n-2}\cdots w_{1,2}h(v) \\ &= \dots = h(v^{-1})x_{n,1}((-1)^n)h(v) = x_{n,1}((-1)^n)v \in H. \end{aligned}$$

Since $x_{n,1}(-v) = x_{n,1}(v)^{-1}$ we certainly have $x_{n,1}(v) \in H$. From the commutator relations (1.1)

$$[x_{1,i}(1), x_{i,i+1}(1)] = x_{1,i+1}(1)$$

we inductively see that $x_{1,i+1}(1) \in H$ for $i = 2, \dots, n-1$, using (1.6). Also, since $n > 2$, for all $u \in \mathbb{F}_q$ we have

$$[x_{1,n}(1), [x_{n,1}(v), x_{1,2}(u)]] = [x_{1,n}(1), x_{n,2}(vu)] = x_{1,2}(vu),$$

so again inductively, starting with $u = 1$, it follows that $X_{1,2} \subset H$. As in (1.6) this forces $X_{i+1,i+2} \subset H$ for $i = 1, \dots, n-2$, and by repeated application of (1.1) all $X_{i,j}$ with $i < j$ are seen to lie in H . Finally

$$[X_{i,n}, x_{n,1}(v)] = X_{i,1}, \quad \text{for } i = 2, \dots, n-1,$$

and (1.1) allows to conclude that indeed all root subgroups are contained in H . Again, since $\mathrm{SL}_n(q)$ is generated by the groups $X_{i,j}$ this shows that $\mathrm{SL}_n(q) \leq H$, and as $\det(\sigma_2) = v$, it then follows that $H = \mathrm{GL}_n(q)$. \square

1.3 Galois Realizations for Linear Groups

Using the Rigidity Criterion of Belyi we obtain the following result from Proposition 1.3:

Theorem 1.4. *The groups $\mathrm{GL}_n(q)$, $q = p^m$, $(n, q) \neq (2, 2)$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\mathrm{ab}}$ for the class vector $([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}])$ with σ_i , $i = 1, 2$, as defined in Proposition 1.3.*

Proof. Obviously the group $G := \mathrm{GL}_n(q)$ acts irreducibly in its natural matrix representation. Moreover the elements σ_1 in Proposition 1.3 all possess an $n - 1$ -dimensional eigenspace for the eigenvalue 1. Hence by the criterion of Belyi (Theorem I.5.10) we have $l([\sigma_1], [\sigma_2], [\sigma_2^{-1}\sigma_1^{-1}]) = 1$ since the condition on the normalizer is trivially satisfied.

For the application of the Basic Rigidity Theorem I.4.8 it remains to check the normalizer condition (N) (see the remark after Theorem I.4.8). Let $N := \mathcal{N}_G(\langle\sigma_1\rangle)$ be the normalizer of the inertia group over the first ramification point, and furthermore let E be the $n - 1$ -dimensional eigenspace for the eigenvalue 1 of σ_1 . Since clearly E is invariant under N , this defines a canonical homomorphism

$$\kappa : N \rightarrow \mathrm{GL}(V/E) \cong \mathrm{GL}_1(q) \cong \mathbb{F}_q^\times,$$

which maps the center $\mathcal{Z}(G)$ surjectively onto \mathbb{F}_q^\times . Hence $\ker(\kappa)$ is a complement to $\mathcal{Z}(G)$ in N , and N satisfies the normalizer condition (N). \square

Remark. The trivial case of the solvable group $\mathrm{GL}_2(2) \cong S_3$ of order six follows for example from Theorem I.5.3.

Passing to suitable subgroups and quotients we obtain:

Corollary 1.5. *The groups $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ and $\mathrm{L}_n(q)$ possess G -realizations over the same fields of definition $k = k(n, q) \leq \mathbb{Q}^{\mathrm{ab}}$ as for $\mathrm{GL}_n(q)$ in Theorem 1.4.*

Proof. Denote by $N/k(t)$ the geometric Galois extension for $\mathrm{GL}_n(q)$ given by Theorem 1.4, and by K' the fixed field of $\mathrm{SL}_n(q)$. So $\mathrm{Gal}(N/K') \cong \mathrm{SL}_n(q)$, and clearly we are done if we can show that K' is a rational function field. The extension $K'/k(t)$ is geometric with

$$\mathrm{Gal}(K'/k(t)) \cong \mathrm{GL}_n(q)/\mathrm{SL}_n(q) \cong \mathbb{F}_q^\times,$$

and ramification occurs at most at the three prime divisors of degree 1 ramified in $N/k(t)$. But for $n = 2$ the element σ_2 already lies in $\mathrm{SL}_n(q)$, while for $n > 2$

we have $\sigma_1 \in \mathrm{SL}_n(q)$. Hence precisely two divisors ramify in $K'/k(t)$. From the Hurwitz genus formula it follows that the ramification is of order $q - 1$ for both of them. Thus the genus $g(K')$ is equal to 0 and the prime divisors lying above the two ramification points have degree one, which proves that K' is rational (see the proof of Theorem I.5.3 for a similar argument).

As $\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/\mathcal{Z}(\mathrm{GL}_n(q))$ and $\mathrm{L}_n(q) = \mathrm{SL}_n(q)/\mathcal{Z}(\mathrm{SL}_n(q))$ are both quotients of groups already realized as geometric Galois groups over k , the remaining assertions follow trivially. \square

Since $\mathrm{Aut}(\mathrm{L}_2(p)) = \mathrm{PGL}_2(p)$ we may also deduce the following:

Corollary 1.6. *For all primes $p > 3$ the groups $\mathrm{L}_2(p)$ possess GA-realizations over \mathbb{Q}^{ab} .*

Remark. The corresponding result for all linear and unitary groups $\mathrm{L}_n(p)$ and $\mathrm{U}_n(p)$ for $n \geq 3$ and primes $p > 2$ will be shown in Corollary 6.6.

This completes the study of linear groups. It should be clear from the above proof that indeed all groups between $\mathrm{GL}_n(q)$ and $\mathrm{L}_n(q)$ may be realized as Galois groups over the original field of definition, i.e., all factor groups of intermediate groups $\mathrm{SL}_n(q) \leq H \leq \mathrm{GL}_n(q)$. In fact, the fixed field of H is rational, being contained in a rational function field of transcendence degree one. In particular this applies to all groups isogenous to $\mathrm{SL}_n(q)$.

Remark. In the papers of Belyi (1979, 1983) all series of classical groups of Lie type are shown to be rigid by using similar methods, the matrix computations being replaced by calculations with Steinberg generators and relators. Since these computations become quite involved in some cases, we prefer to present a more elegant, though less elementary proof which relies on the classification of finite irreducible pseudo-reflection groups.

2 Pseudo-Reflection Groups and Belyi Triples

In order to prove rigidity for the remaining classical groups we first present an elegant effective version of Belyi's criterion, which was proved by Völklein (1998), completing partial results by Malle (1996) and Reiter (1999), and the classification of irreducible pseudo-reflection groups.

2.1 Groups Generated by Pseudo-Reflections

For a finite dimensional vector space V a non-trivial element $\sigma \in \mathrm{GL}(V)$ is called a *pseudo-reflection* if it leaves a hyperplane pointwise fixed. If σ is diagonalizable, so has an eigenvalue $a \neq 1$, then it is called a *homology*. If moreover $a = -1$, then σ is called a *reflection*. The non-diagonalizable pseudo-reflections are also called *transvections*. By their definition pseudo-reflections naturally occur in applications of the Theorem of Belyi. The irreducible linear groups generated by pseudo-reflections are known by work of Wagner (1978, 1980), Kantor (1979) and Zalesskii and Serežkin (1980). We will state their classification, starting with the case of imprimitive groups.

We recall that a linear group $G \leq \mathrm{GL}(V)$ is called a *primitive linear group* if it does not stabilize any non-trivial direct sum decomposition of the underlying vector space V . Let now $m, n > 1$ and $G(m, 1, n)$ be the group of all monomial $n \times n$ -matrices whose entries are m -th roots of unity, of order $m^n n!$. For the following easy result see for example Wagner (1978), Lemma 2.2.

Proposition 2.1. *Let $G \leq \mathrm{GL}_n(q)$ be an irreducible imprimitive linear group generated by pseudo-reflections. Then G is conjugate to a subgroup of $G(m, 1, n)$ for some $m|(q-1)$, the pseudo-reflections in G have order dividing m or 2 and the normalizer in $\mathrm{GL}_n(q)$ of G is again imprimitive unless $n \leq 2$ or $(m, n) \in \{(3, 3), (2, 4)\}$. In the latter cases $|\mathcal{N}_{\mathrm{GL}_n(q)}(G)|$ divides $648(q-1)$ respectively $1152(q-1)$.*

In the primitive case we subdivide the classification according to the type of generating pseudo-reflections.

Theorem 2.2 (Kantor (1979)). *Let $n \geq 4$, $q = p^m$, and H an irreducible subgroup of $\mathrm{SL}_n(q)$ generated by transvections. Then one of the following holds:*

- (a) $H = \mathrm{SL}_n(\tilde{q})$ or $H = \mathrm{Sp}_n(\tilde{q})$ for $\tilde{q}|q$, or
- (b) $H = \mathrm{SU}_n(\tilde{q})$ for $\tilde{q}^2|q$,

or $p = 2$ and one of

- (c) n is even, $H = \mathrm{GO}_n^{(\pm)}(\tilde{q})$ for $\tilde{q}|q$, or
- (d) n is even, $H = S_{n+1}$ or $H = S_{n+2}$, or
- (e) $n = 6$, $H = 3_1.\mathrm{U}_4(3).2_2$, or
- (f) $q \geq 4$ and H is imprimitive.

Theorem 2.3 (Wagner (1978)). *Let $n \geq 3$, $q = p^m$ and H a primitive subgroup of $\mathrm{GL}_n(q)$ generated by non-involutionary homologies. Then one of the following holds:*

- (a) $\mathrm{SL}_n(\tilde{q}) \leq H \leq \mathrm{GL}_n(\tilde{q})$ for $\tilde{q}|q$, or
- (b) $\mathrm{SU}_n(\tilde{q}) \leq H \leq \mathrm{GU}_n(\tilde{q})$ for $\tilde{q}^2|q$,

or $n \leq 4$ and $H \cong \mathrm{GU}_n(2)$. In the latter cases the homologies have order 3.

In the following result we write $W(\mathrm{F}_4), W(\mathrm{H}_4), \dots$ for the Coxeter groups of types $\mathrm{F}_4, \mathrm{H}_4, \dots$ in their natural reflection representation.

Theorem 2.4 (Wagner (1980), Zalesskiĭ and Serežkin (1980)). *Let $n \geq 3$, $q = p^m$ for $p \neq 2$, and H a primitive subgroup of $\mathrm{GL}_n(q)$ generated by reflections. Then one of the following holds:*

- (a) $\mathrm{SL}_n(\tilde{q}) \leq H \leq \mathrm{GL}_n(\tilde{q})$ for $\tilde{q}|q$, or
- (b) $\mathrm{SU}_n(\tilde{q}) \leq H \leq \mathrm{GU}_n(\tilde{q})$ for $\tilde{q}^2|q$, or
- (c) $\Omega_n^{(\pm)}(\tilde{q}) < H \leq \mathrm{GO}_n^{(\pm)}(\tilde{q})$ for $\tilde{q}|q$, or
- (d) $H = S_{n+1}$ and $p \nmid (n+1)$, or $H = S_{n+2}$ and $p|(n+2)$, or
- (e) $n = 3$, $H \in \{A_5 \times 2, L_2(7) \times 2, 3.A_6 \times 2\}$ or $(H, p) = (3.A_7 \times 2, 5)$,
- (f) $n = 4$, $H \in \{W(\mathrm{F}_4), [2^6].S_5, W(\mathrm{H}_4), [2^6].S_6\}$ or $(H, p) = (4.L_3(4).2_2, 3)$,
- (g) $n = 5$, $H = O_5(3) \times 2$,
- (h) $n = 6$, $H \in \{6_1.U_4(3).2_2, W(E_6)\}$,
- (i) $n = 7$, $H = W(E_7) = 2.O_7(2)$,
- (j) $n = 8$, $H = W(E_8) = 2.SO_8^+(2)$.

For the purely group theoretical proofs of these theorems the reader is referred to the original papers.

2.2 An Effective Version of Belyi's Criterion

In this section we present an effective version of the Belyi criterion, which asserts that for certain class vectors of length three the structure constant is in fact non-zero (and thus equal to one by the Theorem I.5.10 of Belyi).

Lemma 2.5. *Let k be a field and $a_1, \dots, a_n, b_1, \dots, b_n \in k^\times$. Then there exist uniquely determined lower (resp. upper) triangular matrices $\sigma, \tau \in \mathrm{GL}_n(k)$ with diagonal entries a_1, \dots, a_n (resp. b_1, \dots, b_n) in this order such that $\sigma^{-1}\tau - \mathrm{Id}$ has identical rows.*

Proof. Let σ be the lower triangular matrix with diagonal entries a_1, \dots, a_n and off-diagonal entries x_{ij} , where $x_{ij} = 0$ if $j > i$. Let ρ denote the matrix such that all rows of $\rho - \mathrm{Id}$ are equal to (y_1, \dots, y_n) . The assertion of the Lemma is now equivalent to the following: there exist unique solutions for the x_{ij}, y_j such that $\sigma\rho$ is upper triangular with diagonal entries b_1, \dots, b_n . This in turn is equivalent to the

unique solvability of the system of equations

$$z_i y_j + x_{ij} = 0, \quad z_i y_i + a_i = b_i, \quad \text{for } 1 \leq i \leq n, 1 \leq j \leq i-1, \quad (2.1)$$

where we have set

$$z_i := a_i + \sum_{l=1}^{i-1} x_{il}. \quad (2.2)$$

This can be solved recursively on i to give the unique solutions

$$y_i = \frac{b_1 \cdots b_{i-1}}{a_1 \cdots a_i} (b_i - a_i), \quad z_i = \frac{a_1 \cdots a_i}{b_1 \cdots b_{i-1}}, \quad x_{ij} = -z_i y_j \quad (2.3)$$

for $1 \leq i \leq n$, $1 \leq j \leq i-1$, where moreover we have

$$1 + \sum_{l=1}^i y_l = \frac{b_1 \cdots b_i}{a_1 \cdots a_i}. \quad (2.4)$$

Indeed, for $i = 1$ this immediately follows from (2.1). So now assume that $i > 1$. Adding up the equations $z_i y_j + x_{ij} = 0$ for $j = 1, \dots, i-1$ we get

$$z_i (y_1 + \dots + y_{i-1}) + z_i - a_i = 0$$

which, using (2.4) inductively, gives the asserted value of z_i . Then the values of y_i and x_{ij} are obtained from (2.1), and (2.4) follows by induction. \square

A triple $(\sigma_1, \sigma_2, \sigma_3)$ of elements $\sigma_i \in \mathrm{GL}_n(k)$ with $\sigma_1 \sigma_2 \sigma_3 = 1$ is called a *Belyi triple* if σ_1 is a pseudo-reflection (i.e., $\mathrm{rk}(\sigma_1 - \mathrm{Id}) = 1$) and the group $\langle \sigma_1, \sigma_2 \rangle$ generated by the triple is an irreducible subgroup of $\mathrm{GL}_n(K)$. We can now state the existence theorem for Belyi triples.

Theorem 2.6 (Völklein (1998)). *Let $f, g \in \mathbb{F}_q[X]$ be coprime monic polynomials of degree n with non-vanishing constant coefficient. Then there exists a Belyi triple $(\sigma_1, \sigma_2, \sigma_3)$ in $\mathrm{GL}_n(q)$ such that the characteristic (and the minimal) polynomial of σ_2^{-1} (resp. σ_3) equals $f(X)$ (resp. $g(X)$).*

Proof. Let $\bar{\mathbb{F}}_q$ be the algebraic closure of \mathbb{F}_q , and denote the zeroes of $f(X)$ (resp. $g(X)$) in $\bar{\mathbb{F}}_q$ by a_1, \dots, a_n (resp. b_1, \dots, b_n). By Lemma 2.5 there exist matrices $\sigma, \tau \in \mathrm{GL}_n(\bar{\mathbb{F}}_q)$ with characteristic polynomials $f(X), g(X)$ respectively such that $\sigma^{-1}\tau - \mathrm{Id}$ has rank 1. Assume that $G := \langle \sigma, \tau \rangle$ is reducible on $V := \bar{\mathbb{F}}_q^n$, with non-trivial G -invariant subspace $0 < W < V$. Since $\mathrm{rk}(\sigma^{-1}\tau - \mathrm{Id}) = 1$ the element $\sigma^{-1}\tau$ acts as identity on W or on V/W . In either case $\sigma = \tau$ on that space, showing that σ and τ have a common eigenvalue, which contradicts our assumption on f, g . Thus $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ with $\sigma_1 := (\sigma^{-1}\tau)^{-1}$, $\sigma_2 := \sigma^{-1}$, $\sigma_3 := \tau$ is a Belyi triple in $\mathrm{GL}_n(\bar{\mathbb{F}}_q)$. The intersection of any eigenspace of σ_2 or σ_3 with the hyperplane of fixed points of σ_1 is a G -invariant subspace. Hence, since G is irreducible, all such eigenspaces are at most 1-dimensional which means that f, g are also the minimal polynomials of σ_2^{-1}, σ_3 .

It remains to descend to the finite field \mathbb{F}_q . Let $F : \mathrm{GL}_n(\bar{\mathbb{F}}_q) \rightarrow \mathrm{GL}_n(\bar{\mathbb{F}}_q)$ be the Frobenius-morphism raising each matrix entry to its q -th power. Then $F(\sigma) = (F(\sigma_1), F(\sigma_2), F(\sigma_3))$ is again a Belyi triple in $\mathrm{GL}_n(\bar{\mathbb{F}}_q)$. Since $f, g \in \mathbb{F}_q[X]$ are F -invariant the elements σ_i and $F(\sigma_i)$ have the same characteristic polynomial for $i = 2, 3$, which equals the minimal polynomial by the above observation. Furthermore, since $\mathrm{rk}(\sigma_1 - \mathrm{Id}) = 1$ it follows that also σ_1 and $F(\sigma_1)$ have the same minimal polynomial. By the theory of Jordan normal forms this shows that σ_i is conjugate to $F(\sigma_i)$ for $i = 1, 2, 3$. By the Theorem I.5.10 of Belyi there exists a $\rho \in \mathrm{GL}_n(\bar{\mathbb{F}}_q)$ with $\sigma_i^\rho = F(\sigma_i)$. But by the Theorem 1.1 of Lang-Steinberg any $\rho \in \mathrm{GL}_n(\bar{\mathbb{F}}_q)$ can be decomposed as $\rho = \gamma F(\gamma)^{-1}$ with a suitable $\gamma \in \mathrm{GL}_n(\bar{\mathbb{F}}_q)$. Then $F(\sigma_i^\gamma) = \sigma_i^\gamma$ is F -invariant for $i = 1, 2, 3$, hence σ^γ is a Belyi triple in $\mathrm{GL}_n(q)$ with the prescribed characteristic polynomials. \square

Remark. The condition in Theorem 2.6 of f, g being coprime is actually necessary and sufficient for the existence of associated Belyi triples, see Völklein (1998).

2.3 Imprimitive and Symmetric Groups

The following result shows that for a wide class of Belyi triples the generated group is primitive.

Proposition 2.7. *Let $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ be a Belyi triple in $\mathrm{GL}_n(q)$ and assume that $G := \langle \sigma \rangle$ is imprimitive with respect to a decomposition $\mathbb{F}_q^n = V_1 \oplus \dots \oplus V_r$ with $r > 1$.*

(a) *If $r < n$ then $\mathrm{tr}(\sigma_2) = \mathrm{tr}(\sigma_3) = 0$, r divides $\gcd(o(\sigma_2), o(\sigma_3))$, the orders of σ_2, σ_3 are bounded above by $r(q^{n/r} - 1)$, and the characteristic polynomials of σ_2, σ_3 are of the form*

$$\prod_{i=1}^r f(\xi^i X), \quad \text{where } \xi^r = 1. \quad (2.5)$$

(b) *If $r = n$ then $G \leq G(q-1, 1, n)$, $o(\sigma_1) = 2$, either σ_2 or σ_3 has order dividing $n(q-1)$ and trace 0 while the other has order at most $n^2(q-1)/4$, and the characteristic polynomials of σ_2, σ_3 are of the form*

$$X^n - c_1, \quad (X^k - c_2)(X^{n-k} - c_3), \quad \text{where } c_1, c_2, c_3 \in \mathbb{F}_q^\times, \quad (2.6)$$

for some $1 \leq k \leq n-1$.

Proof. The G -invariant decomposition $\mathbb{F}_q^n = V_1 \oplus \dots \oplus V_r$ induces a permutation representation $\pi_r : G \rightarrow S_r$ of G into the symmetric group on r letters whose image is transitive (since G acts irreducibly). Since $\mathrm{rk}(\sigma_1 - \mathrm{Id}) = 1$ we necessarily have $\pi_r(\sigma_1) = 1$ in case (a). So both $\pi_r(\sigma_2), \pi_r(\sigma_3)$ are r -cycles, which proves the first part of (a). Moreover the r -th power of σ_i stabilizes each of V_1, \dots, V_r , for $i = 2, 3$. This proves (a).

In case (b) by definition we have $G \leq G(q-1, 1, n) \cong \mathbb{F}_q^\times \wr S_n$. As $\pi_r(G)$ is transitive and $\pi_r(\sigma_1)$ is either the identity or a transposition, at least one of $\pi_r(\sigma_2), \pi_r(\sigma_3)$ must be an n -cycle, so its order divides $n(q-1)$ and its trace vanishes, while the other has at most two orbits. It is clear that elements of $G(q-1, 1, n)$ which map to a permutation of type $(k)(n-k)$ have characteristic polynomial as stated. \square

By similar considerations we can handle symmetric groups as follows:

Proposition 2.8. *Let $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ be a Belyi triple in $\mathrm{GL}_n(q)$ with $\sigma_1^2 = 1$ and assume that $G := \langle \sigma \rangle$ is a symmetric group S_m with $m \in \{n+1, n+2\}$. Then one of $o(\sigma_2), o(\sigma_3)$ is bounded above by m , the other by $m^2/4$.*

Proof. Firstly, as σ_1 is a pseudo-reflection of order 2, it represents a transposition of S_m , $m \in \{n+1, n+2\}$. Thus σ_2, σ_3 both map to permutations with at most two orbits. In fact, since transpositions have odd signature and the product $\sigma_1\sigma_2\sigma_3 = 1$, one of σ_2, σ_3 must be an m -cycle. This proves the assertion. \square

2.4 Invariant Forms

In this section we construct quadratic and bilinear forms invariant under the Belyi triples corresponding to suitable polynomials f, g in Theorem 2.6. This allows an easy recognition of the group generated by σ . For properties of spaces with forms see for example Aschbacher (1986), Ch. 7. We will make use of the following easy fact (see for example Wagner (1978), Lemma 2.1).

Proposition 2.9. *Let $G \leq \mathrm{GL}_n(q)$ be an irreducible subgroup containing a pseudo-reflection. Then G is absolutely irreducible.*

The only case where the existence of invariant forms can not be proved abstractly from Belyi's criterion is that of quadratic forms in characteristic 2. Here Völklein (1998), Lemma 5 and 6, showed that his effective form of Belyi's criterion can be used to write down such forms explicitly (Parts (b) and (c) of the following result). This allows us to distinguish between Belyi triples generating the orthogonal resp. symplectic groups in characteristic 2.

Theorem 2.10. *Let $f, g \in \mathbb{F}_q[X]$ be coprime monic polynomials of degree n with non-vanishing constant coefficient and G the group generated by a Belyi triple constructed from f, g as in Theorem 2.6.*

(a) *Let $n = 2m + 1$ be odd. If the roots in $\bar{\mathbb{F}}_q$ of f and g are of the form*

$$a_1, \dots, a_m, 1, a_m^{-1}, \dots, a_1^{-1}, \quad b_1, \dots, b_m, -1, b_m^{-1}, \dots, b_1^{-1} \quad (2.7)$$

then G leaves invariant a non-degenerate quadratic form.

(b) Let $n = 2m$. If the roots in $\bar{\mathbb{F}}_q$ of f and g are of the form

$$a_1, \dots, a_m, ca_m^{-1}, \dots, ca_1^{-1}, \quad b_1, \dots, b_m, cb_m^{-1}, \dots, cb_1^{-1} \quad (2.8)$$

then G leaves a non-degenerate alternating bilinear form invariant up to scalars.

(c) Let $n = 2m$ and q even. If the roots in $\bar{\mathbb{F}}_q$ of f and g are of the form (2.8) with $c = 1$ then G leaves a non-degenerate quadratic form invariant if and only if one of the a_i or b_i is equal to 1.

(d) Let $n = 2m$ and q odd. If the roots in $\bar{\mathbb{F}}_q$ of f and g are of the form

$$a_1, \dots, a_{m-1}, c, -c, c^2 a_{m-1}^{-1}, \dots, c^2 a_1^{-1}, \quad b_1, \dots, b_m, c^2 b_m^{-1}, \dots, c^2 b_1^{-1} \quad (2.9)$$

then G leaves a non-degenerate quadratic form invariant up to scalars.

Proof. Let σ, τ be the matrices constructed in the proof of Lemma 2.5 with respect to the ordering of the roots as in the statement, and $\rho := \sigma^{-1}\tau$. Let θ be the matrix whose only non-zero entries are y_i in position $(i, n-i+1)$. It is invertible since all y_i are non-zero. An easy calculation then shows that $\theta^{-1}(\rho^t - \text{Id})\theta$ has identical rows. But if $\tilde{\rho} - \text{Id}$ has identical rows for some $\tilde{\rho} \in \text{GL}_n(q)$, this also holds for $\tilde{\rho}^{-1} - \text{Id}$, thus $\theta^{-1}(\rho^{-t} - \text{Id})\theta$ has identical rows. Furthermore, we obtain that $\theta^{-1}\sigma^{-t}\theta$ is lower triangular with diagonal entries $a_n^{-1}, \dots, a_1^{-1}$, and $\theta^{-1}\tau^{-t}\theta$ is upper triangular with diagonal entries $b_n^{-1}, \dots, b_1^{-1}$.

In case (a) it follows from (2.3) that under the condition (2.7) the entries y_i of $\rho - \text{Id}$ satisfy

$$y_{n-i+1} = \frac{b_1 \cdots b_{n-i}}{a_1 \cdots a_{n-i+1}} (b_{n-i+1} - a_{n-i+1}) = \frac{-b_1 \cdots b_{i-1}}{a_1 \cdots a_i} (a_i - b_i) = y_i$$

for $1 \leq i \leq m$. Thus the matrix θ is symmetric and invertible. By the preceding considerations $\sigma' := \theta^{-1}\sigma^{-t}\theta$, $\tau' := \theta^{-1}\tau^{-t}\theta$ are lower (upper) triangular with the same diagonal entries as σ (resp. τ) and the product $(\sigma')^{-1}\tau'$ has identical rows. By the uniqueness assertion in Lemma 2.5 this implies $\sigma' = \sigma$, $\tau' = \tau$, so

$$\sigma^t \theta \sigma = \theta, \quad \tau^t \theta \tau = \theta,$$

i.e., $G := \langle \sigma, \tau \rangle$ leaves invariant the symmetric bilinear form defined by θ since G is absolutely irreducible by Proposition 2.9.

For (b) it follows from (2.3) that the entries y_i of $\rho - \text{Id}$ satisfy $y_i = -y_{n-i+1}$ for $1 \leq i \leq m$. Thus now the matrix θ is skew-symmetric and invertible. Let $\tilde{\sigma} := \sqrt{c}^{-1}\sigma$, $\tilde{\tau} := \sqrt{c}^{-1}\tau$. Then as before the uniqueness part of Lemma 2.5 shows that $\langle \tilde{\sigma}, \tilde{\tau} \rangle \leq \text{GL}_n(\bar{\mathbb{F}}_q)$ leaves invariant the skew-symmetric form $(,)$ defined by θ . But then $\sigma, \tau \in \text{GL}_n(q)$ leave $(,)$ invariant up to scalar multiples.

In (c), let $V = \bar{\mathbb{F}}_q^{2n}$ and $Q : V \rightarrow \bar{\mathbb{F}}_q$ a quadratic form left invariant by G . Then

$$(,)' : V \times V \rightarrow \bar{\mathbb{F}}_q, \quad (v, w)' := Q(v+w) + Q(v) + Q(w),$$

is an alternating bilinear G -invariant form on V , hence by the absolute irreducibility of G (Proposition 2.9) must be equal up to scalars to the form (\cdot, \cdot) defined by the matrix θ from (b). Without loss of generality we may assume that they are actually equal. With respect to the standard basis e_1, \dots, e_n of V we may write

$$\begin{aligned} Q((u_1, \dots, u_n)^t) &= \sum_{i=1}^n u_i^2 Q(e_i) + \sum_{i < j} u_i u_j (e_i, e_j) \\ &= \sum_{i=1}^n u_i^2 Q(e_i) + \sum_{i=1}^m u_i u_{n-i+1} y_i, \end{aligned} \quad (2.10)$$

so Q is determined by the values $Q(e_i)$, $1 \leq i \leq n$. We let $\rho := \sigma^{-1} \tau$. Then

$$Q(\rho(e_i)) = Q(e_i + y_i e_{n+1}) = Q(e_i) + y_i^2 (Q(e_{n+1}) + 1)$$

where we have set $e_{n+1} := e_1 + \dots + e_n$. Thus Q is ρ -invariant only if $Q(e_{n+1}) = 1$.

Furthermore, $(e_i, e_j) = 0$ for $i, j \geq m+1$, so for $i \geq m+1$ we have $Q(\sigma(e_i)) = Q(e_i)$ if and only if

$$(1 + a_i^2) Q(e_i) + \sum_{j=i+1}^n x_{j,i}^2 Q(e_i) = 0.$$

We may assume that $a_i \neq 1$ for $m+1 \leq i \leq n$, so the above has the only solution $Q(e_{m+1}) = \dots = Q(e_n) = 0$. If moreover all roots b_i are different from 1 then similarly we obtain $Q(\tau(e_i)) = Q(e_i)$ for $1 \leq i \leq m$ if and only if $Q(e_1) = \dots = Q(e_m) = 0$. But then $Q(e_{n+1}) = y_1 + \dots + y_m = 1 + b_1 \cdots b_m / (a_1 \cdots a_m) \neq 1$ by (2.4), so Q is not ρ -invariant. This proves the first part of the assertion.

Now assume that $b_m = 1$ and set

$$Q((u_1, \dots, u_n)^t) := u_m^2 \frac{b_1 \cdots b_m}{a_1 \cdots a_m} + \sum_{i=1}^m u_i u_{n-i+1} y_i. \quad (2.11)$$

Since $Q(e_i) = 0$ for $i \geq m+1$ we have that $Q(\sigma(e_i)) = Q(e_i)$ for $i \geq m+1$. Also, $Q(e_{n+1}) = 1$, so Q is ρ -invariant. Finally the definition of Q shows that $Q(\tau^{-1}(e_i)) = Q(e_i)$ for $1 \leq i \leq m$, so

$$\sigma(Q)(e_i) = \tau \rho^{-1}(Q)(e_i) = \tau(Q)(e_i) = Q(\tau^{-1}(e_i)) = Q(e_i)$$

for $1 \leq i \leq m$, hence Q is also σ -invariant, thus G -invariant.

In (d) we show that G leaves a non-degenerate quadratic form invariant if $c = 1$, from which the general assertion follows by considering $\tilde{\sigma} := c^{-1}\sigma$, $\tilde{\tau} := c^{-1}\tau$. Let θ be the $n \times n$ -matrix with only non-zero entries y_i in position $(i, n-i+1)$ for $1 \leq i \leq m-1$, y_m in position $(m, m+1), (m+1, m)$ and $2/z_{m+1}$ in position $(m+1, m+1)$. Then θ is symmetric and invertible. Moreover it is easily checked using (2.3) that $\theta^{-1}(\rho^t - \text{Id})\theta$ has identical rows while $\theta^{-1}\sigma^{-t}\theta$ is lower triangular with diagonal entries $a_1, \dots, a_{m-1}, 1, -1, a_{m-1}^{-1}, \dots, a_1^{-1}$, and $\theta^{-1}\tau^{-t}\theta$ is upper triangular with diagonal entries $b_n^{-1}, \dots, b_1^{-1}$. By the same argument as in (b) this proves that G leaves invariant the non-degenerate quadratic form defined by θ . \square

3 The Classical Groups

In this paragraph we verify rigidity for the remaining classical groups over finite fields, i.e., the unitary, symplectic and orthogonal groups, using the classification of irreducible pseudo-reflection groups.

3.1 Rigidity for $\mathrm{GU}_n(q)$

Let V be a finite dimensional vector space over \mathbb{F}_{q^2} and θ the generator of $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Then on V there exists a unique Hermitian form with respect to θ up to equivalence (see Aschbacher (1986), (21.6.2)). The subgroup of $\mathrm{GL}_n(q^2)$ leaving such a form invariant is called the *general unitary group* $\mathrm{GU}_n(q)$ on V .

Proposition 3.1. *Let $q = p^m$, $n \geq 3$, $a \in \mathbb{F}_{q^2}^\times$ of multiplicative order $q^n - (-1)^n$ and*

$$f(X) := \prod_{i=0}^{n-1} (X - a^{(-q)^i}), \quad g(X) := (X - 1)^n. \quad (3.1)$$

If $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle \sigma \rangle = \mathrm{GU}_n(q)$.

Proof. By definition we have $f, g \in \mathbb{F}_{q^2}[X]$ and f, g are coprime. Thus $G := \langle \sigma \rangle \leq \mathrm{GL}_n(q^2)$ is irreducible. Also, G is not contained in $\mathrm{GL}_n(\tilde{q})$ for any proper subfield $\mathbb{F}_{\tilde{q}}$ of \mathbb{F}_{q^2} since $f \notin \mathbb{F}_{\tilde{q}}[X]$. Let θ be the matrix constructed in the first part of the proof of Theorem 2.10. Then $\tilde{\sigma} := (\theta^{-1}\sigma^{-t}\theta)^q$ is lower triangular with the same diagonal entries as σ (not necessarily in the same order), and similarly for $\tilde{\tau} := (\theta^{-1}\tau^{-t}\theta)^q$. Furthermore $\tilde{\sigma}^{-1}\tilde{\tau} - \mathrm{Id}$ has rank 1. Thus $\tilde{\sigma} := ((\tilde{\sigma}^{-1}\tilde{\tau})^{-1}, \tilde{\sigma}^{-1}, \tilde{\tau})$ is a Belyi triple in $\mathrm{GL}_n(\bar{\mathbb{F}}_q)$ whose elements have the same characteristic polynomials as for the Belyi triple σ . By the Theorem of Belyi $\tilde{\sigma}$ is conjugate to σ by some $\gamma \in \mathrm{GL}_n(\bar{\mathbb{F}}_q)$. Thus

$$\sigma = (\theta\gamma)^{-1}(\sigma^{-t})^q\theta\gamma, \quad \tau = (\theta\gamma)^{-1}(\tau^{-t})^q\theta\gamma$$

and G fixes some non-degenerate Hermitian form. This shows that $G \leq \mathrm{GU}_n(q)$. Since $\sigma_3 \in \mathrm{SL}_n(q^2)$ and the determinant

$$\det(\sigma_2) = \prod_{i=0}^{n-1} a^{(-q)^i} = a^{(q^n - (-1)^n)/(q+1)}$$

of σ_2 has multiplicative order $q + 1$ the pseudo-reflection σ_1 is a homology of order $q + 1$. Since moreover by construction σ_2 is semisimple while σ_3 is unipotent, the group G acts primitively by Proposition 2.7. Hence the normal subgroup H of G generated by the conjugacy class in G of the homology σ_1 acts irreducibly. According to Proposition 2.1 either H is also primitive or $n = q + 1 = 3$. In the

latter case it is easily checked that $G = \mathrm{GU}_3(2)$. In the former case by Theorem 2.3 the only remaining possibility is $G = H = \mathrm{GU}_n(q)$. \square

Thus we obtain:

Theorem 3.2. *The groups $\mathrm{GU}_n(q)$, $q = p^m$, $n \geq 3$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\mathrm{ab}}$ for the class vector $([\sigma_1], [\sigma_2], [\sigma_3])$ defined in Proposition 3.1. The groups $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$ and $\mathrm{U}_n(q)$ possess G -realizations over the same fields of definition.*

Proof. This is a straightforward application of the Belyi criterion to the class vector $\mathbf{C} = ([\sigma_1], [\sigma_2], [\sigma_3])$. The elements in the first class have an $(n - 1)$ -dimensional eigenspace. The normalizer of $G = \mathrm{GU}_n(q)$ in the general linear group $\mathrm{GL}_n(q^2)$ is generated by G and $\mathcal{Z}(\mathrm{GL}_n(q))$, so by Theorem I.5.10 we have $l(\mathbf{C}) = 1$. Let $N := \mathcal{N}_G(\langle \sigma_1 \rangle)$ be the normalizer of the inertia group above the first ramification point, and let E be the 1-eigenspace of σ_1 . As in Theorem 1.4 this defines a canonical homomorphism

$$\kappa : N \rightarrow \mathrm{GU}(V/E) \cong \mathrm{GU}_1(q) \cong \mathbb{F}_{q^2}^\times / \mathbb{F}_q^\times,$$

which maps the center $\mathcal{Z}(G)$ surjectively onto $\mathbb{F}_{q^2}^\times / \mathbb{F}_q^\times$. Hence the kernel $\ker(\kappa)$ is a complement to $\mathcal{Z}(G)$ in N , and N satisfies the normalizer condition (N). Theorem I.4.8 then proves the first part of the assertion.

The descent to the other unitary groups is achieved by the same arguments as in the proof of Corollary 1.5. \square

Remark. In a completely similar fashion it can be shown that $\mathrm{GL}_n(q)$ possesses a G -realizations over abelian number fields by choosing

$$f(X) = \prod_{i=0}^{n-1} (X - a^{q^i}), \quad g(X) = (X - 1)^n,$$

where a is a generator of $\mathbb{F}_{q^n}^\times$, thus giving an alternative proof of Theorems 1.4 and 1.5.

3.2 Rigidity for $\mathrm{CSp}_{2n}(q)$

Let V be an even-dimensional vector space over a finite field \mathbb{F}_q . All non-singular alternating bilinear forms on V are equivalent (see Aschbacher (1986), (21.6.1)). The subgroup of $\mathrm{GL}(V)$ leaving invariant such a form is the *symplectic group* on V , denoted by $\mathrm{Sp}_{2n}(q)$, where $\dim(V) = 2n$. Since $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$ we will assume $n \geq 2$ throughout this section. The symplectic group coincides with the image of the universal Chevalley group of type $C_n(q)_{sc}$ in its natural matrix representation (see Table 1.1). The *conformal symplectic group* $\mathrm{CSp}_{2n}(q)$ is by definition the subgroup of elements of $\mathrm{GL}(V)$ leaving the symplectic form invariant up to scalars.

Proposition 3.3. Let $q = p^m$, $n \geq 2$, $(n, q) \neq (2, 2)$, $a \in \mathbb{F}_{q^{2n}}^\times$ of multiplicative order $(q^n + 1)(q - 1)$, $c := a^{q^n+1}$, and

$$f := \prod_{i=0}^{2n-1} (X - a^{q^i}), \quad g(X) := (X - 1)^n (X - c)^n. \quad (3.2)$$

If $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle \sigma \rangle = \mathrm{CSp}_{2n}(q)$.

Proof. We have $a^{q^n} = ca^{-1}$ for $c = a^{q^n+1} \in \mathbb{F}_q$, so the roots $a, a^q, \dots, a^{q^{2n-1}}$ of $f \in \mathbb{F}_q[X]$ are of the form (2.8). By Theorem 2.10 this implies that $G := \langle \sigma \rangle \leq \mathrm{CSp}_{2n}(q)$. Also, G is not contained in $\mathrm{GL}_{2n}(\tilde{q})$ for any proper subfield $\mathbb{F}_{\tilde{q}}$ of \mathbb{F}_q by the choice of a . As the orders of $\sqrt{c}\sigma_2, \sqrt{c}^{-1}\sigma_3$ are coprime, G is primitive by Proposition 2.7 since $o(\sqrt{c}\sigma_2) = (q^n + 1) > n^2(q - 1)$. Thus the normal subgroup H of G generated by the transvections in G acts irreducibly.

If p is odd then by Theorem 2.2 we have $H \geq \mathrm{Sp}_{2n}(q)$. If $p = 2$ then by Lemma 2.1 either $n = 4$, $H \leq G(2, 1, 4)$, or H is one of the primitive groups listed in Theorem 2.2. Moreover if $H \leq G(2, 1, 4)$ then $|G|$ divides $648(q - 1)$ which is only possible in the excluded case $q = 2$. Furthermore, H is neither an orthogonal group by Theorem 2.10(c), nor a symmetric group by Proposition 2.8. By comparison of orders, $3_1.U_4(3).2_2$ cannot be contained in $\mathrm{Sp}_6(2)$. But for $q \geq 4$ the order of σ_2 is too large.

Finally, since σ_2 multiplies the symplectic form by the generator c of \mathbb{F}_q^\times the group G is the full conformal group $\mathrm{CSp}_{2n}(q)$. \square

Theorem 3.4. The groups $\mathrm{CSp}_{2n}(q)$, $q = p^m$, $(n, q) \neq (2, 2)$, possess G -realizations over abelian number fields $k(n, q)$ for the class vector of σ defined in Proposition 3.3. The groups $\mathrm{Sp}_{2n}(q)$, $\mathrm{PCSp}_{2n}(q)$ and $\mathrm{S}_{2n}(q)$ possess G -realizations over the same fields of definition.

Proof. By construction σ is a Belyi triple. By its definition the group $\mathrm{CSp}_{2n}(q)$ is self-normalizing in $\mathrm{GL}_{2n}(q)$, so the stronger second part of Theorem I.5.10 applies, showing rigidity. The normalizer condition (N) for $\langle \sigma_1 \rangle$ is verified by exactly the same argument as in the proof of Theorem 1.4, using the fact that σ_1 has a $(2n - 1)$ -dimensional eigenspace and that $\mathcal{L}(\mathrm{CSp}_{2n}(q)) \cong \mathbb{F}_q^\times$. Application of Theorem I.4.8 now yields the Galois realization.

The subgroup $\mathrm{Sp}_{2n}(q)$ has a rational fixed field in the Galois extension for $\mathrm{CSp}_{2n}(q)$ by the same arguments as in the proof of Corollary 1.5, so occurs as Galois group over the same field of definition. Finally, the groups $\mathrm{PCSp}_{2n}(q) = \mathrm{CSp}_{2n}(q)/\mathcal{L}(\mathrm{CSp}_{2n}(q))$ and $\mathrm{S}_{2n}(q) = \mathrm{Sp}_{2n}(q)/\mathcal{L}(\mathrm{Sp}_{2n}(q))$ are factor groups, so the remaining assertion is clear. \square

Remark. The group $\mathrm{Sp}_4(2)$ excluded in the Theorem is isomorphic to the symmetric group S_6 on six letters, and hence trivially known to occur as geometric Galois group over $\mathbb{Q}(t)$.

3.3 Rigidity for $\mathrm{SO}_{2n+1}(q)$

Let V be an odd-dimensional vector space over a finite field IF_q of odd order q . All non-degenerate symmetric forms on V are similar (see for example Aschbacher (1986), (21.6.4)). The group leaving such a form invariant is the *orthogonal group*, denoted by $\mathrm{GO}_{2n+1}(q)$, where $\dim(V) = 2n + 1$. The special orthogonal group $\mathrm{SO}_{2n+1}(q)$ consists of the elements of $\mathrm{GO}_{2n+1}(q)$ of determinant 1. In Lie notation, these are the groups $B_n(q)_{\mathrm{ad}}$. The image of the universal Chevalley group $B_n(q)_{sc}$ in this matrix representation is the simple group $O_{2n+1}(q)$, the kernel of the *spinor norm*

$$\mathrm{spin} : \mathrm{SO}_{2n+1}(q) \longrightarrow \mathrm{IF}_q^\times / (\mathrm{IF}_q^\times)^2 \quad (3.3)$$

which is defined as follows: Any $\sigma \in \mathrm{SO}_{2n+1}(q)$ can be written as a product $\sigma = \rho_1 \cdots \rho_r$ of reflections. Let v_i denote an eigenvector of ρ_i for the eigenvalue -1 for $i = 1, \dots, r$. Then $\mathrm{spin}(\sigma) = Q(v_1) \cdots Q(v_r) (\mathrm{IF}_q^\times)^2$ where Q is the quadratic form left invariant by $\mathrm{SO}_{2n+1}(q)$ (see Aschbacher (1986), (22.11)).

Lemma 3.5. *Let q be odd and $\sigma \in G := \mathrm{SO}_{2n+1}(q)$ be of order $q^n + 1$. Then σ generates a (cyclic) maximal torus of G . In particular, $\mathrm{spin}(\sigma) \neq 1$.*

Proof. Let $\mathbf{G} := \mathrm{SO}_{2n+1}(\bar{\mathrm{IF}}_q)$ be defined with respect to the standard quadratic form $Q((x_1, \dots, x_{2n+1})^t) = \sum_{i=1}^{n+1} x_i x_{2n+2-i}$. Up to conjugation all semisimple elements $\tau \in \mathbf{G}$ lie in the diagonal maximal torus of \mathbf{G} . Thus the eigenvalues of τ are of the form $a_1, \dots, a_n, \pm 1, a_n^{-1}, \dots, a_1^{-1}$. If $\tau \in G = \mathrm{SO}_{2n+1}(q)$ then the set of eigenvalues must be defined over IF_q . Thus $q^n + 1$ is the largest possible order of a semisimple element in $\mathrm{SO}_{2n+1}(q)$. Furthermore, if τ is such an element, then the centralizer in G of τ consists only of its powers. Hence $\langle \tau \rangle$ is a maximal abelian subgroup of G consisting of semisimple elements, so it is a maximal torus. The remaining assertion now follows from Proposition 1.2. \square

We shall assume from now on that $n \geq 3$, since otherwise the orthogonal groups are isomorphic to symplectic groups, and these were already considered in the previous section.

Proposition 3.6. *Let q be odd, $n \geq 3$, $a \in \mathrm{IF}_{q^{2n}}^\times$ of multiplicative order $q^n + 1$ and*

$$f(X) := (X - 1) \prod_{i=0}^{2n-1} (X - a^{q^i}), \quad g(X) := (X + 1)^{2n+1}. \quad (3.4)$$

If $\tilde{\sigma} := (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle -\sigma_1, \sigma_2 \rangle = \mathrm{SO}_{2n+1}(q)$.

Proof. We have $a^{q^n} = a^{-1}$, so the roots $a, a^q, \dots, a^{q^{2n-1}}, 1$ of $f \in \mathrm{IF}_q[X]$ are of the form (2.7). By Theorem 2.10 this shows that $\tilde{G} := \langle \tilde{\sigma} \rangle \leq \mathrm{GO}_{2n+1}(q)$. By construction the orders of $\sigma_2, -\sigma_3$ are coprime, hence by Proposition 2.7 the group G acts primitively since $o(\sigma_2) = q^n + 1 > (q - 1)(2n + 1)^2 / 4$. Thus the normal subgroup

H of \tilde{G} generated by the class of the reflection σ_1 in G acts irreducibly. By Proposition 2.1 it even acts primitively whence H is a primitive reflection group contained in $\mathrm{GO}_{2n+1}(q)$. By Theorem 2.4 either $H \geq \mathrm{O}_{2n+1}(q)$ or $H = S_{2n+2}, S_{2n+3}$ or $n = 7$, $H = 2.\mathrm{O}_7(2)$. The symmetric groups can be excluded by Proposition 2.8, while $H = 2.\mathrm{O}_7(2)$ is ruled out by the order of σ_2 . Now σ_1 has determinant -1 and σ_2 lies in $\mathrm{SO}_{2n+1}(q) \setminus \mathrm{O}_{2n+1}(q)$ by Lemma 3.5. Hence $\tilde{G} = \mathrm{GO}_{2n+1}(q)$ and $G = \langle -\sigma_1, \sigma_2 \rangle = \mathrm{SO}_{2n+1}(q)$. \square

Theorem 3.7. *The groups $\mathrm{SO}_{2n+1}(q)$, $q = p^m$ odd, $n \geq 3$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector $([-\sigma_1], [\sigma_2], [-\sigma_3])$ defined in Proposition 3.6. The simple groups $\mathrm{O}_{2n+1}(q)$ possess G -realizations over the same fields of definition.*

Proof. We have seen in Proposition 3.6 that σ is a Belyi triple, so the criterion of Belyi is applicable. By Kleidman and Liebeck (1990), Prop. 2.10.6, the group $\mathrm{SO}_{2n+1}(q)$ acts absolutely irreducibly in its natural representation, so by loc. cit., Cor. 2.10.4, its normalizer in $\mathrm{GL}_{2n+1}(q)$ consists of those matrices leaving the quadratic form invariant up to scalars, and this is the direct product of $\mathrm{SO}_{2n+1}(q)$ with $\mathcal{Z}(\mathrm{GL}_n(q))$. Hence the second condition of Theorem I.5.10 is also satisfied and the result follows from the Basic Rigidity Theorem I.4.8 since $\mathcal{Z}(G) = 1$.

The fixed field of the subgroup $\mathrm{O}_{2n+1}(q)$ of index two in $\mathrm{SO}_{2n+1}(q)$ is rational, which proves the second assertion. \square

3.4 Rigidity for $\mathrm{CO}_{2n}^+(q)$

Let V be an even-dimensional vector space over a finite field \mathbb{F}_q . There exist two types of non-degenerate quadratic forms on V (see Aschbacher (1986), (21.6.3)). The subgroup of $\mathrm{GL}_{2n}(q)$ leaving invariant the quadratic form

$$Q(\mathbf{x}) = \sum_{i=1}^n x_i x_{2n+1-i} \quad (3.5)$$

of maximal Witt index is called the *orthogonal group of plus type* $\mathrm{GO}_{2n}^+(q)$. The *conformal orthogonal group* $\mathrm{CO}_{2n}^+(q)$ consists of those matrices leaving the form invariant up to scalar multiples.

Now first assume that q is odd. The special orthogonal group $\mathrm{SO}_{2n}^+(q)$ is defined as the intersection of $\mathrm{GO}_{2n}^+(q)$ with $\mathrm{SL}_{2n}(q)$. In Lie notation these groups have type D_n . The embeddings of $\mathrm{SO}_{2n}^+(q)$ into $\mathrm{CO}_{2n}^+(q)$ and $\mathrm{GO}_{2n}^+(q)$ give rise to the exact diagram

$$\begin{array}{ccc}
1 & 1 & 1 \\
\downarrow & \downarrow & \downarrow \\
1 \longrightarrow \mathrm{SO}_{2n}^+(q) \hookrightarrow \mathrm{CO}_{2n}^{+\circ}(q) \longrightarrow \mathbb{F}_q^\times \longrightarrow 1 \\
\downarrow & \downarrow & \downarrow \\
1 \longrightarrow \mathrm{GO}_{2n}^+(q) \hookrightarrow \mathrm{CO}_{2n}^+(q) \xrightarrow{\text{mult}} \mathbb{F}_q^\times \longrightarrow 1 & (3.6) \\
\downarrow^{\det} & \downarrow & \downarrow \\
1 \longrightarrow \{\pm 1\} \cong Z_2 \longrightarrow 1 \\
\downarrow & \downarrow & \\
1 & 1 &
\end{array}$$

Here $\mathrm{CO}_{2n}^{+\circ}(q)$ denotes the finite group associated to the connected component of the identity in the conformal orthogonal group over an algebraic closure of \mathbb{F}_q . A generator of the orthogonal group $\mathrm{GO}_{2n}^+(q)$ defined with respect to (3.5) over $\mathrm{SO}_{2n}^+(q)$ is the element

$$\sigma := \begin{pmatrix} 0 & 1 \\ & \mathrm{Id}_{2n-2} \\ 1 & 0 \end{pmatrix} \quad (3.7)$$

which induces the graph automorphism of order two on the diagram D_n . With this the non-split orthogonal group $\mathrm{GO}_{2n}^-(q)$ can be defined as the group of fixed points of the product of the field automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ times σ .

The image of the universal Chevalley group $D_n(q)_{sc}$ in the above matrix representation is the group $\Omega_{2n}^+(q)$, the kernel in $\mathrm{SO}_{2n}^+(q)$ of the spinor norm

$$\mathrm{spin} : \mathrm{SO}_{2n}^+(q) \longrightarrow \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$$

which is defined as in odd dimension. Clearly, the full normalizer of $\Omega_{2n}^+(q)$ in $\mathrm{GL}_{2n}(q)$ is the conformal group $\mathrm{CO}_{2n}^+(q)$. The somewhat complicated connection between various orthogonal groups for odd q is most conveniently depicted in the following exact diagram:

$$\begin{array}{ccc}
1 & 1 & 1 \\
\downarrow & \downarrow & \downarrow \\
1 \rightarrow \mathcal{Z}(\Omega_{2n}^+(q)) \hookrightarrow \mathcal{Z}(\mathrm{SO}_{2n}^+(q)) \xrightarrow{\mathrm{spin}} \pm(\mathbb{F}_q^\times)^2 / (\mathbb{F}_q^\times)^2 \rightarrow 1 \\
\downarrow & \downarrow & \downarrow \\
1 \rightarrow \Omega_{2n}^+(q) \hookrightarrow \mathrm{SO}_{2n}^+(q) \xrightarrow{\mathrm{spin}} \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2 \rightarrow 1 & (3.8) \\
\downarrow & \downarrow & \downarrow \\
1 \rightarrow \mathrm{O}_{2n}^+(q) \hookrightarrow \mathrm{PSO}_{2n}^+(q) \longrightarrow \mathbb{F}_q^\times / \pm(\mathbb{F}_q^\times)^2 \rightarrow 1 \\
\downarrow & \downarrow & \downarrow \\
1 & 1 & 1
\end{array}$$

Here the group $O_{2n}^+(q)$ is simple for $n \geq 3$. In analogy to Lemma 3.5 we have the following result:

Lemma 3.8. *Let $\tau \in G := SO_{2n}^+(q)$ be of order $q^n - 1$. Then τ generates a (cyclic) maximal torus of G . In particular, $\tau \notin \Omega_{2n}^+(q)$.*

The next result of Reiter (1999) allows to distinguish between the two types of orthogonal groups in even dimension.

Lemma 3.9. *Let $\tau \in CO_{2n}^{+o}(q)$ be semisimple with characteristic polynomial $f(X) = \prod_{i=1}^{2n} (X - a_i)$ such that $a_i^2 \neq \text{mult}(\tau)$ for $i = 1, \dots, 2n$. Then $CO_{2n}^{-o}(q)$ does not contain an element with characteristic polynomial $f(X)$.*

Proof. Every semisimple element of the connected algebraic group $G := CO_{2n}^+(\bar{\mathbb{F}}_q)$ lies in a maximal torus, and all maximal tori are conjugate. A particular maximal torus of G is

$$T := \{\text{diag}(t_1, \dots, t_n, ut_n^{-1}, \dots, ut_1^{-1}) \mid u, t_i \in \bar{\mathbb{F}}_q^\times\}$$

(see Digne and Michel (1991), p. 147). From the action of the Weyl group of T it follows that all semisimple elements in T with the same characteristic polynomial are conjugate in G .

Now let $\sigma_1, \sigma_2 \in G$ with characteristic polynomial $f(X)$. By the above we have $\sigma_2 = \sigma_1^\tau$ for some $\tau \in G$. Let $F : G \rightarrow G$ be the standard Frobenius morphism. Assume that $F(\sigma_1) = \sigma_1$ while $F(\sigma_2) = \sigma_2^\sigma$ with σ from (3.7). Then

$$\tau \sigma F(\tau)^{-1} \sigma_1 F(\tau) \sigma^{-1} \tau^{-1} = \sigma_1,$$

so $F(\tau) \sigma^{-1} \tau^{-1} \in \mathcal{C}_{CO_{2n}(\bar{\mathbb{F}}_q)}(\sigma_1)$. Taking determinants (respectively quasi-determinants (3.11) in the case of characteristic 2) shows that $\det(F(\tau) \sigma^{-1} \tau^{-1}) = -1$, so $F(\tau) \sigma^{-1} \tau^{-1} \in CO_{2n}(\bar{\mathbb{F}}_q) \setminus G$. But this gives a contradiction since the centralizer in $CO_{2n}(\bar{\mathbb{F}}_q)$ of a semisimple element satisfying the assumptions of the Lemma is a product of full linear groups, thus it is connected and already contained in G . This proves the assertion. \square

Proposition 3.10. *Let q be odd, $n \geq 4$, a a generator of $\mathbb{F}_{q^n}^\times$, c a generator of \mathbb{F}_q^\times and*

$$f(X) := \prod_{i=0}^{n-1} (X - a^{q^i})(X - ca^{-q^i}), \quad g(X) := (X-1)^{n-1}(X-c)^{n-1}(X^2-c). \tag{3.9}$$

If $\sigma := (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle \sigma \rangle = CO_{2n}^+(q)$.

Proof. We have $f, g \in \mathbb{F}_q[X]$ and the roots of f, g are as in (2.9). Thus $G := \langle \sigma \rangle \leq CO_{2n}^\pm(q)$ by Theorem 2.10. Furthermore, by Lemma 3.9 we have $G \leq CO_{2n}^+(q)$ since $SO_2^+(q^n) \leq SO_{2n}^+(q)$ clearly contains elements with characteristic polynomial

$\prod_{i=0}^{n-1} (X - a^{q^i})(X - a^{-q^i})$. If G acts imprimitively with respect to a decomposition $V_1 \oplus \dots \oplus V_r$ then $r = n$ by Proposition 2.7(a). But we have $o(\sigma_2) = q^n - 1 > n^2(q - 1)$ so by Proposition 2.7(b) the group G acts primitively. Thus the normal subgroup H of G generated by the class of the reflection σ_1 in G acts irreducibly. By Proposition 2.1 it even acts primitively whence H is a primitive reflection group contained in $\mathrm{GO}_{2n}^+(q)$. By Theorem 2.4 either $H > \Omega_{2n}^+(q)$ or $H = S_{2n+1}, S_{2n+2}$ or $n = 8, H = 2.\mathrm{SO}_8^+(2)$. The symmetric groups can be excluded by Proposition 2.8, while $H = 2.\mathrm{SO}_8^+(2)$ is ruled out by the order of σ_2 . Now σ_1 has determinant -1 and σ_2 lies in $\mathrm{SO}_{2n}^+(q) \setminus \Omega_{2n}^+(q)$ by Lemma 3.8. Finally, σ_3 multiplies the form by the generator c of IF_q^\times , so $G = \langle \sigma \rangle = \mathrm{CO}_{2n}^+(q)$. \square

Theorem 3.11. *The groups $\mathrm{CO}_{2n}^+(q)$, $q = p^m$ odd, $n \geq 4$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\text{ab}}(t)$ for the class vector $([\sigma_1], [\sigma_2], [\sigma_3])$ constructed in Proposition 3.10. The groups $\mathrm{GO}_{2n}^+(q), \mathrm{SO}_{2n}^+(q), \mathrm{PSO}_{2n}^+(q), \Omega_{2n}^+(q)$ and $\mathrm{O}_{2n}^+(q)$ possess G -realizations over \mathbb{Q}^{ab} .*

Proof. Let $\mathbf{C} = ([\sigma_1], [\sigma_2], [\sigma_3])$ be the class vector consisting of the conjugacy classes of the elements σ_i defined in Proposition 3.10. Since σ_1 has a $(2n - 1)$ -dimensional eigenspace for the eigenvalue 1 and since, as remarked above, $\mathrm{CO}_{2n}^+(q)$ is self-normalizing in $\mathrm{GL}_{2n}(q)$, we conclude from the Belyi criterion I.5.10 that $l(\mathbf{C}) = 1$ and therefore \mathbf{C} is rigid. The center $Z := \mathcal{Z}(\mathrm{CO}_{2n}^+(q))$ of $\mathrm{CO}_{2n}^+(q)$ consists of the scalar multiples of the identity matrix, hence the argument in the proof of Theorem 1.4 may be used to verify the normalizer condition (N) for the inertia group over σ_1 . The first part of the assertion then follows with Theorem I.4.8.

It remains to achieve the descent to the simple group $\mathrm{O}_{2n}^+(q)$. For this, let \tilde{K} be the fixed field of $\Omega_{2n}^+(q) \cdot Z$ (see the diagrams (3.6) and (3.8)) in the Galois extension $N/k(t)$ for $\mathrm{CO}_{2n}^+(q)$, and

$$H := \mathrm{Gal}(\tilde{K}/k(t)) \cong \mathrm{CO}_{2n}^+(q)/(\Omega_{2n}^+(q) \cdot Z).$$

The first element σ_1 in the class vector is an involution, and the square of the second also lies in $\Omega_{2n}^+(q) \cdot Z$. Hence H has a generating system of elements with orders $(2, 2, k)$, and so is a dihedral group. In particular, \tilde{K} has genus zero by Theorem I.6.2, and since the absolute Galois group of \mathbb{Q}^{ab} is projective (see Serre (1964), Ch. III, §2.4, Ex. 3, or also Theorem IV.1.11(d)), \mathbb{Q}^{ab} is a field of definition of the Galois extension $\mathbb{Q}N/\bar{\mathbb{Q}}K$ by Theorem I.3.4. Thus the group $\Omega_{2n}^+(q) \cdot Z$ has a G -realization over \mathbb{Q}^{ab} . Factoring by its center we obtain the desired realization for the simple group $\mathrm{O}_{2n}^+(q)$.

The fixed fields of $\mathrm{GO}_{2n}^+(q) \cdot Z$ and $\mathrm{SO}_{2n}^+(q) \cdot Z$ are subfields of \tilde{K} , so the preceding arguments also yield Galois extensions for $\mathrm{GO}_{2n}^+(q), \mathrm{SO}_{2n}^+(q)$ and $\mathrm{PSO}_{2n}^+(q)$ over the same field of definition as $\mathrm{O}_{2n}^+(q)$. \square

In even characteristic the relationship between the various types of orthogonal groups becomes much easier. So the four orthogonal groups in diagram (3.8) all coincide, while the diagram (3.6) simplifies to

$$\mathrm{CO}_{2n}^+(2^m) \cong \mathrm{GO}_{2n}^+(2^m) \times \mathrm{IF}_{2^m}^\times. \quad (3.10)$$

The simple group $O_{2n}^+(2^m)$ is now obtained as the kernel of the *quasi-determinant*

$$\text{qdet} : \text{GO}_{2n}^+(2^m) \longrightarrow \{\pm 1\}, \quad \tau \mapsto (-1)^{\text{rk}(\tau-1)} \quad (3.11)$$

(see Conway et al. (1985), p.xii).

Proposition 3.12. *Let $q = 2^m$, $n \geq 4$, a a generator of $\mathbb{F}_{q^n}^\times$ and*

$$f(X) := \prod_{i=0}^{n-1} (X - a^{q^i})(X - a^{-q^i}), \quad g(X) := (X - 1)^{2n}. \quad (3.12)$$

If $\sigma := (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle \sigma \rangle = \text{GO}_{2n}^+(q)$.

The proof is analogous to the one of Proposition 3.10 above, using that an element with minimal polynomial $g(X)$ has quasi-determinant -1 .

Theorem 3.13. *The groups $\text{GO}_{2n}^+(q)$, $q = 2^m$, $n \geq 4$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector $([\sigma_1], [\sigma_2], [\sigma_3])$ defined in Proposition 3.12. The groups $O_{2n}^+(q)$ possess G -realizations over the same field of definition.*

Proof. Since the first element σ_1 of the class vector satisfies the assumptions of Belyi's criterion, we obtain rigidity for the group $\text{GO}_{2n}^+(2^m)$. Since $\text{GO}_{2n}^+(2^m)$ has trivial center the first assertion follows with Theorem I.4.8. The descent to the simple group is possible since $\text{GO}_{2n}^+(q)/O_{2n}^+(q)$ is of order 2. \square

3.5 Rigidity for $\text{CO}_{2n}^-(q)$

We consider the group of non-maximal Witt-index as the subgroup of $\text{GO}_{2n}^+(q^2)$ fixed by the product of the field automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ times the non-trivial graph automorphism of order 2 induced by the element σ defined in (3.7). Thus the *orthogonal group of minus type* $\text{GO}_{2n}^-(q)$ consists of those elements τ in $\text{GO}_{2n}^+(q^2)$ which satisfy $\tau^\sigma = \bar{\tau}$, where $\bar{\cdot}$ denotes the automorphism of $\text{GO}_{2n}^+(q^2)$ raising each matrix entry to its q -th power. The groups $\text{CO}_{2n}^-(q)$ and $\text{SO}_{2n}^-(q)$ are the stabilizers of this automorphism in the corresponding untwisted groups $\text{CO}_{2n}^+(q^2)$ and $\text{SO}_{2n}^+(q^2)$. Taking fixed points we thus obtain the analogues of diagrams (3.6) and (3.8) for the various orthogonal groups of minus type.

Proposition 3.14. *Let $q = p^m$, $n \geq 4$, $a \in \mathbb{F}_{q^{2n}}^\times$ of multiplicative order $(q^n + 1)(q - 1)$, $c := a^{q^n + 1}$, and*

$$f(X) := \prod_{i=0}^{2n-1} (X - a^{q^i}), \quad g(X) := (X - 1)^{n-1}(X - c)^{n-1}(X^2 - c). \quad (3.13)$$

If $\sigma := (\sigma_1, \sigma_2, \sigma_3)$ is a Belyi triple constructed from f, g as in Theorem 2.6 then $G := \langle \sigma \rangle = \text{CO}_{2n}^-(q)$.

Proof. The roots of the polynomials $f, g \in \mathbb{F}_q[X]$ satisfy (2.9) hence $G \leq \text{CO}_{2n}^\pm(q)$. By Lemma 3.9 we even have $G \leq \text{CO}_{2n}^-(q)$ since $\text{SO}_2^-(q^n) \leq \text{SO}_{2n}^-(q)$ contains an element with characteristic polynomial $\prod_{i=0}^{2n-1} (X - a^{q^{i+1}-q^i})$. For the remainder of the argument we may proceed as in the proof of Proposition 3.10 to show that indeed $G = \text{CO}_{2n}^-(q)$, since by definition $\det(\sigma_1) = -1$, σ_2 lies in $\text{SO}_{2n}^-(q) \setminus \Omega_{2n}^-(q)$, and the element σ_3 multiplies the form by the element c of multiplicative order $q - 1$. \square

Theorem 3.15. *The groups $\text{CO}_{2n}^-(q)$, $q = p^m$, $n \geq 4$, possess G -realizations over abelian number fields $k(n, q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector $([\sigma_1], [\sigma_2], [\sigma_3])$ defined in Proposition 3.14. The groups $\text{GO}_{2n}^-(q)$, $\text{SO}_{2n}^-(q)$, $\text{PSO}_{2n}^-(q)$, $\Omega_{2n}^-(q)$ and $\text{O}_{2n}^-(q)$ possess G -realizations over \mathbb{Q}^{ab} .*

Proof. The proof is entirely analogous to those of the preceding results. The Belyi criterion yields $l([\sigma_1], [\sigma_2], [\sigma_3]) = 1$, the normalizer condition (N) is verified as in Theorem 3.2 using the fact that $|\mathcal{L}(\text{CO}_{2n}^-(q))| = q - 1$, and then the Galois realization for $\text{CO}_{2n}^-(q)$ follows from Theorem I.4.8. The other groups are obtained by descent arguments as in the proof of Theorem 3.11 using the corresponding substitutes for the diagrams (3.6) and (3.8) in the twisted case. Again, if q is odd the simple group can only be shown to occur over $\mathbb{Q}^{\text{ab}}(t)$ by using the fact (Theorem IV.1.11(d)) that \mathbb{Q}^{ab} has projective absolute Galois group together with Theorem I.3.4. \square

4 The Exceptional Groups of Rank at Most 2

The exceptional groups of Lie type comprise ten families of finite simple groups derived from the simple exceptional Lie algebras or from classical groups as fixed points under an exceptional automorphism. Unlike the classical groups of Lie type, they do not possess a ‘nice’ matrix representation, and in particular, Belyi’s criterion is not applicable to them. Hence rigidity has to be proved in some other way. Unfortunately, at present no uniform way of treating all exceptional groups of Lie type is known; moreover, it is not even known whether all of them can be realized as Galois groups over $\mathbb{Q}^{\text{ab}}(t)$: the only finite simple groups not known to occur as Galois groups over abelian number fields are among the exceptional groups of Lie type in characteristic 2.

Nevertheless, quite a number of these groups can be covered by the criteria introduced in the previous chapter. The key lies in the character theoretic form of the Rigidity Criterion. The five series of exceptional groups of Lie rank at most two, namely 2B_2 , 2G_2 , G_2 , 3D_4 and 2F_4 , are particularly suited for an application of this criterion. The conjugacy classes of elements, the character tables and the lists of maximal subgroups are explicitly known in all these cases. Moreover, all these results are generic, which is to say that they are almost independent of q . Indeed, the entries in the character tables are polynomials in q , and there exists a fixed number of maximal subgroups, apart from the so-called subfield groups obtained by restricting the field of definition of the relevant group. So basically each series may be treated more or less like one single group; only sometimes the effect of bad characteristic has to be taken into account, forcing a subdivision into several cases.

Thanks to the almost complete knowledge of the small rank groups, only two divisibility criteria are needed in addition. They are presented in the first section.

4.1 Divisibility Criteria

In the application of the character theoretic form of the Basic Rigidity Criterion to a class vector \mathbf{C} of a finite group G , first the structure constant $n(\mathbf{C})$ has to be calculated. Then it remains to prove that a system $\sigma \in \bar{\Sigma}(\mathbf{C})$ generates all of G . This is usually done by showing that $H := \langle \sigma \rangle$ cannot lie in any of the maximal subgroups of G . One easy way to exclude a maximal subgroup M is Lagrange’s theorem, that is, to exhibit a prime divisor of $|H|$ which does not divide the order of M .

The orders of the finite groups of Lie type $G(q)$ can be written as polynomials in $q = p^m$. Let $\phi_r(X)$ denote the r -th cyclotomic polynomial in X , i.e., the polynomial whose roots are the primitive r -th roots of unity, which can be defined recursively by

$$X^r - 1 = \prod_{s|r} \phi_s(X). \quad (4.1)$$

Then, more precisely, the order of $G(q)$ is a product of certain cyclotomic factors $\phi_r(q)$ times a power of q . Factors of this type tend to have large prime divisors. The main result in this direction is due to Zsigmondy (see Huppert and Blackburn (1982), Ch. IX, Thm. 8.3):

Proposition 4.1. *For all positive integers $r \geq 3$ and all primes p there exists a prime divisor l of $p^r - 1$, dividing none of the $p^s - 1$ with $s < r$, except for the case $r = 6$, $p = 2$.*

Such a prime l is called a *primitive prime divisor* of $p^r - 1$. As an easy consequence we get:

Corollary 4.2. *If $\phi_n(p^m)$ with $nm \geq 3$ divides the product $\prod_{i=1}^k (p^{s_i} - 1)$, then there exists an index i with $mn|s_i$, or else $p = 2$ and $mn = 6$.*

Proof. If $(p, mn) \neq (2, 6)$ then there exists a primitive prime divisor l of $p^{mn} - 1$ by Proposition 4.1. Because

$$(p^{mn} - 1) \Big| \phi_n(p^m) \prod_{j=1}^{mn-1} (p^j - 1),$$

l must already divide $\phi_n(p^m)$. Again by the Proposition there now exists an i with $mn \leq s_i$. But $\gcd(p^{mn} - 1, p^s - 1) = p^{\gcd(mn, s)} - 1$, so l can only divide $p^s - 1$ if s is a multiple of mn . \square

A quite different criterion also makes use of the orders of the elements to identify a group generated by a triple of elements. We call a system $(\sigma_1, \sigma_2, \sigma_3)$ of elements with orders $o(\sigma_i)$ an $(o(\sigma_1), o(\sigma_2), o(\sigma_3))$ -triple for short.

Proposition 4.3. *Let $H := \langle \sigma_1, \sigma_2, \sigma_3 \rangle$, where $\sigma_1 \sigma_2 \sigma_3 = 1$, such that the orders $o(\sigma_1)$, $o(\sigma_2)$ and $o(\sigma_3)$ are pairwise coprime. Then H is perfect.*

Proof. Assume H is not perfect. Then the commutator subgroup H' is a proper normal subgroup of H with abelian factor group. In particular there exists a normal subgroup N with factor H/N cyclic of prime order p . This factor H/N must have a generating (m_1, m_2, m_3) -system, where $m_i | o(\sigma_i)$ for $i = 1, 2, 3$. As the three orders $o(\sigma_i)$ are pairwise coprime, at most one of them is divisible by p , so at most one of the m_i is different from 1. The product relation then forces all three to be equal to 1, which contradicts the fact that the images should generate H/N . \square

4.2 Rigidity for the Ree Groups ${}^2G_2(q^2)$

The easiest series to treat among the exceptional groups are the Ree groups ${}^2G_2(q^2)$ in characteristic 3. They are obtained from a simple algebraic group of type G_2 defined over $\bar{\mathbb{F}}_3$ as fixed points under a twisted Frobenius map, and exist only when

$q^2 = 3^{2m+1}$ is an odd power of 3. The group ${}^2G_2(3)$ is isomorphic to the automorphism group $\Gamma L_2(8)$ of $L_2(8)$, while the other groups are simple. The conjugacy classes of elements of $G = {}^2G_2(q^2)$ were determined by Ward (1966), as well as a large portion of the character tables. A complete list of maximal subgroups has been obtained by Kleidman (1988b).

Let \mathbf{C} be a class vector for G consisting of the unique class of involutions C_2 , the class C_3 of 3-elements lying central in a Sylow 3-subgroup (denoted by $[X]$ in Ward (1966)), and C_s , one of the classes containing semisimple elements of order $q^2 - \sqrt{3}q + 1$ (which, despite its appearance, is an integer).

Table 4.1 Character values for ${}^2G_2(3^{2m+1})$

	1	C_2	C_3	C_s
ξ_1	1	1	1	1
ξ_5	$\frac{\sqrt{3}}{6}q(q^2 - 1)(q^2 + \sqrt{3}q + 1)$	$-\frac{1}{2}(q^2 - 1)$	$-\frac{1}{6}(3q^2 + \sqrt{3}q)$	-1
ξ_7	$\frac{\sqrt{3}}{6}q(q^2 - 1)(q^2 + \sqrt{3}q + 1)$	$-\frac{1}{2}(q^2 - 1)$	$-\frac{1}{6}(3q^2 + \sqrt{3}q)$	-1

Proposition 4.4. *The class vector $\mathbf{C} = (C_2, C_3, C_s)$ of ${}^2G_2(3^{2m+1})$, $m \geq 1$, is rigid.*

Proof. We claim that \mathbf{C} satisfies the character theoretic rigidity criterion in Corollary I.5.9. The relevant part of the character table of ${}^2G_2(q^2)$ is reproduced in Table 4.1 with Ward's notation for the characters. It contains the three irreducible characters ξ_1, ξ_5, ξ_7 not vanishing on any of the three classes of \mathbf{C} and thus contributing to the normalized structure constant $n(\mathbf{C})$. Now using $|{}^2G_2(q^2)| = q^6(q^2 - 1) \cdot (q^6 + 1)$, $|\mathcal{C}_G(\sigma_1)| = q^2(q^4 - 1)$, $|\mathcal{C}_G(\sigma_2)| = q^6$ and $|\mathcal{C}_G(\sigma_3)| = q^2 - \sqrt{3}q + 1$, this shows that $n(\mathbf{C}) = 1$.

It remains to check that each $\sigma \in \bar{\Sigma}(\mathbf{C})$ generates all of ${}^2G_2(q^2)$. Let σ be such a system, and set $H := \langle \sigma \rangle$. According to Kleidman (1988b), the isomorphism types of maximal subgroups of ${}^2G_2(q^2)$ for $q^2 > 3$ are as follows:

$$\begin{aligned} &L_2(q^2) \times 2, \quad (2^2 \times D_{\frac{q^2+1}{2}}).3, \quad [q^6].(q^2 - 1), \\ &(q^2 + \sqrt{3}q + 1).6, \quad (q^2 - \sqrt{3}q + 1).6, \\ &{}^2G_2(r^2) \quad \text{for } r^2 = 3^{2k+1} \quad \text{with } (2m+1)/(2k+1) \text{ prime.} \end{aligned}$$

Since the elements σ_i , $i = 1, 2, 3$, have pairwise coprime orders, the group H is perfect by Proposition 4.3. The only nonsolvable maximal subgroups in the list are $L_2(q^2) \times 2$ and the subfield groups ${}^2G_2(r^2)$. But the order of the first is clearly prime to $o(\sigma_3)$. The maximal element order in ${}^2G_2(r^2)$ equals $r^2 + \sqrt{3}r + 1 \leq 2r^2 + 1$, which is smaller than $o(\sigma_3) = q^2 - \sqrt{3}q + 1 \geq 1/2q^2 + 1$ if $r \neq q$. Hence H is not contained in any of the maximal subgroups of ${}^2G_2(q^2)$ and thus coincides with the full group, which proves the assertion. \square

Theorem 4.5. *The groups ${}^2G_2(q^2)$, $q^2 = 3^{2m+1} > 3$, possess G -realizations over \mathbb{Q}^{ab} for the class vector $\mathbf{C} = (C_2, C_3, C_s)$. More precisely, a field of index six in the cyclotomic field $\mathbb{Q}(\zeta_s)$ of $s := (q^2 - \sqrt{3}q + 1)$ -th roots of unity is a field of definition for this Galois extension. The group ${}^2G_2(3)' \cong L_2(8)$ possesses a GA-realization over \mathbb{Q} .*

Proof. This follows from the Basic Rigidity Theorem I.4.8. The precise field of definition can be read off from the character table as described in Proposition I.4.4. Since the first two classes of \mathbf{C} are rational, only the third class contributes to the irrationalities. The GA-realization for $L_2(8)$ was already obtained in Example I.8.3. \square

The same result holds if the class C_s is replaced by one of its powers such that the corresponding element order is a primitive prime divisor in the sense of Zsigmondy. In some cases, this allows to diminish the degree of a field of definition.

4.3 Rigidity for the Groups $G_2(q)$

For the groups $G_2(q)$, $q = p^m$, the character tables were determined by Chang and Ree (1974) in characteristic $p \geq 5$, by Enomoto (1976) in characteristic 3, and by Enomoto and Yamada (1986) in even characteristic. The maximal subgroups were obtained by Cooperstein (1981) for $p = 2$ and by Kleidman (1988b) for $p \geq 3$. It turns out that one may choose a class vector yielding rigidity for almost all groups $G_2(q)$.

For this let C_1^+ be a class of elements of order $q^2 - q + 1$ if $q \equiv 1 \pmod{3}$, and C_1^- (resp. C_1^0), a class of elements of order $q^2 + q + 1$ if $q \equiv -1 \pmod{3}$ (resp. $q \equiv 0 \pmod{3}$). Also let C_2^+ , C_2^0 denote a class of elements of order $q + 1$ with centralizer order $q(q + 1)(q^2 - 1)$ if $q \equiv 1 \pmod{3}$, resp. $q \equiv 0 \pmod{3}$, and C_2^- a class of elements of order $q - 1$ with centralizer order $q(q - 1)(q^2 - 1)$ if $q \equiv -1 \pmod{3}$. Finally let C_3 denote the class of semisimple 3-elements with centralizer order $q^3(q^2 - 1)(q^3 - \varepsilon)$ if $q \equiv \varepsilon = \pm 1 \pmod{3}$, and the unipotent class of 3-elements central in a Sylow 3-subgroup if $3 \nmid q$. Unfortunately the notations for conjugacy classes employed by the different authors vary considerably.

Table 4.2 Conjugacy classes for $G_2(q)$

	CR		$\varepsilon = 0$	EY	
	$\varepsilon = 1$	$\varepsilon = -1$		$\varepsilon = 1$	$\varepsilon = -1$
C_1^ε	h_6	h_3	E_5	E_4	E_3
C_2^ε	h_{2b}	h_{1a}	D_{11}	D_{21}	C_{21}
C_3		k_3	A_2		B_0

Table 4.2 gives a dictionary between our notation and that in the papers of Chang and Ree (1974) (abbreviated CR), of Enomoto (1976) (E) and of Enomoto and Yamada (1986) (EY). From the information given in the literature cited above one verifies that the three classes are nonempty for all $q \neq 2$. The character table of the composite group $G_2(2) \cong U_3(3).2$ is reproduced in the Atlas of finite groups (Conway et al. (1985)), and we shall use the names of conjugacy classes given there for this group.

Proposition 4.6. (a) *The class vector $\mathbf{C} = (C_1^\varepsilon, C_2^\varepsilon, C_3)$ of $G_2(q)$, $2 \neq q = p^m \equiv \varepsilon \pmod{3}$, is rigid.*

(b) *The class vector $\mathbf{C} = (2B, 4D, 12A)$ of $G_2(2)$ is rationally rigid.*

Proof. In the general case (a), the relevant part of the character table is given in Table 4.3 for $q \equiv \varepsilon \pmod{3}$, where $\varepsilon \in \{\pm 1\}$, (here the first column gives the character names in CR, the second one those in EY), and in Table 4.4 for 3 dividing q . (Here the notation for the irreducible characters is taken from Enomoto (1976)). Together with the group order $|G_2(q)| = q^6(q^2 - 1)(q^6 - 1)$ and the centralizer orders given above this yields $n(\mathbf{C}) = 1$.

Table 4.3 Character values for $G_2(q)$, $q \equiv \varepsilon \pmod{3}$

CR	EY	1	C_3	C_2^ε	C_1^ε
χ_{11}	θ_0	1	1	1	1
χ_{12}	θ_5	q^6	εq^3	$-\varepsilon q$	1

Table 4.4 Character values for $G_2(q)$, $q = 3^m$

	1	C_3	C_2^0	C_1^0
θ_0	1	1	1	1
θ_{10}	$\frac{1}{6}q\phi_1^2\phi_6$	$\frac{1}{6}q(2q-1)\phi_1$	ϕ_1	1

Now let $H := \langle \sigma \rangle$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$. The three classes were chosen such that the corresponding element orders are pairwise prime. Hence H is perfect by Proposition 4.3. Moreover we may apply Corollary 4.2 to a primitive prime divisor of the order $o(\sigma_3) = q^2 \pm q + 1$. Note that the exceptions do not occur due to the congruence conditions in the definition of C_1^ε . By Kleidman (1988b) and Cooperstein

(1981) the nonsolvable maximal subgroups of $G_2(q)$ with order divisible by a primitive prime divisor of $o(\sigma_3)$ are

$$\begin{aligned} \mathrm{SL}_3(q):2 &\quad \text{if } q \equiv -1 \pmod{3}, \\ \mathrm{SL}_3(q):2 &\quad \text{if } q \equiv 0 \pmod{3} \quad (\text{two classes}), \\ \mathrm{SU}_3(q):2 &\quad \text{if } q \equiv 1 \pmod{3}, \\ \mathrm{L}_2(13) &\quad \text{if } q = 3 \text{ or } 4. \end{aligned}$$

Let us first assume that $q \equiv 1 \pmod{3}$. Then we have to exclude $\mathrm{SU}_3(q):2$, and for $q = 4$ the $\mathrm{L}_2(13)$. But the latter is easy, since for $q = 4$ elements in C_2^+ have order 5, which does not divide $|\mathrm{L}_2(13)|$. If $H \leq \mathrm{SU}_3(q):2$, then since H is perfect we even have $H \leq \mathrm{SU}_3(q)$. Note that in our case $\mathrm{SU}_3(q) = \mathrm{U}_3(q)$ since $q \equiv 1 \pmod{3}$. It now suffices to show that C_3 does not intersect this subgroup. In $\mathrm{U}_3(q)$ there exists just one class $3A$ of elements of order 3, and from the character table of $\mathrm{U}_3(q)$ in Simpson and Frame (1973) one calculates the normalized structure constant $n(3A, 3A, C_1^+) = q^2 + q + 1$. But in $G_2(q)$ the corresponding structure constant is found to vanish. So indeed $3A$ does not fuse into C_3 , and the result follows for $q \equiv 1 \pmod{3}$. For $q \equiv -1 \pmod{3}$ the proof is entirely similar, with $\mathrm{U}_3(q)$ replaced by $\mathrm{L}_3(q)$.

So let's finally assume $3|q$. In this case, the two classes of maximal subgroups $\mathrm{SL}_3(q)$ are those generated by all long root subgroups, respectively all short root subgroups. Since C_3 is the class of long root elements, its intersection with the second class is empty. The exceptional graph automorphism in characteristic 3 exchanges long and short roots, and it interchanges the two classes of maximal tori in $G_2(q)$ of order $q^2 - 1$. Thus it also interchanges our class $C_2^0 = D_{11}$ with the class denoted by D_{21} in Enomoto (1976). Since $\mathrm{SL}_3(q)$ has just one class of tori of order $q^2 - 1$, it can intersect at most (in fact, precisely) one of D_{11}, D_{21} . From the description of the semisimple classes by Enomoto it now follows that the $\mathrm{SL}_3(q)$ generated by long root elements intersects D_{21} and so the possibility $\mathrm{SL}_3(q)$ is ruled out. If $q = 3$, then by the Atlas the unique 3-class in $\mathrm{L}_2(13)$ fuses into $3D$ of $G_2(3)$, which is not central in a Sylow 3-subgroup. This completes the proof for (a).

For $G = G_2(2)$ in (b) this is a special case of Theorem 6.8(b) due to the exceptional isomorphism $G_2(2) \cong \mathrm{Aut}(\mathrm{U}_3(3))$. \square

Theorem 4.7. *The groups $G_2(q)$, $q = p^m$, possess G -realizations over \mathbb{Q}^{ab} for the class vector \mathbf{C} of Proposition 4.6.*

4.4 Rigidity for the Groups ${}^3\mathrm{D}_4(q)$

The conjugacy classes, the character table and the list of maximal subgroups for ${}^3\mathrm{D}_4(q)$ were determined by Spaltenstein (1982), Deriziotis and Michler (1987) and Kleidman (1988a). We chose the three conjugacy classes $C_1 := [u_1]$, $C_2 := [u_5]$

and $C_3 := [s_{14}]$, where the names of the representative elements are taken from Deriziotis and Michler (1987).

Proposition 4.8. *The class vector $\mathbf{C} = (C_1, C_2, C_3)$ of ${}^3\mathrm{D}_4(q)$, $q = p^m$, is rigid.*

Proof. From the character table in Deriziotis and Michler (1987) one finds that the only irreducible characters not vanishing on any of the three classes in \mathbf{C} are as in Table 4.5. Here the last line stands for a whole family of characters constant on all classes apart from C_3 , and such that the sum of their values on that last class equals -1 (this is indicated by the notation $\{-1\}$ in the table). In particular, since

$$|\mathcal{C}_G(\sigma_1)| = q^{12}(q^6 - 1), \quad |\mathcal{C}_G(\sigma_2)| = q^6, \quad |\mathcal{C}_G(\sigma_3)| = q^4 - q^2 + 1$$

for $\sigma \in \Sigma(\mathbf{C})$, and

$$|{}^3\mathrm{D}_4(q)| = q^{12}(q^2 - 1)(q^6 - 1)(q^8 + q^4 + 1)$$

we obtain the value $n(\mathbf{C}) = 1$ for the normalized structure constant.

Table 4.5 Character values for ${}^3\mathrm{D}_4(q)$

	1	C_1	C_2	C_3
1	1	1	1	1
χ_{14}	$\phi_1^2 \phi_2^2 \phi_3^2 \phi_6^2$	$-\phi_1 \phi_2 \phi_3 \phi_6$	1	$\{-1\}$

Now let $H := \langle \sigma \rangle$. Using the list of maximal subgroups of ${}^3\mathrm{D}_4(q)$ in Kleidman (1988a) and Corollary 4.2 applied to a primitive prime divisor of $o(\sigma_3) = q^4 - q^2 + 1 = \phi_{12}$ one finds that either $H = {}^3\mathrm{D}_4(q)$ or $H \leq \mathcal{N}_G(\langle \sigma_3 \rangle) = (q^4 - q^2 + 1).4$. The elements σ_1 and σ_2 are unipotent, hence have p -power order, so they cannot be contained in the latter subgroup if p is odd. For $p = 2$ one checks that σ_2 has order 4, while σ_1 is an involution. This follows either from the Chevalley commutator formulae, or by considering the element orders in the character table of the group ${}^3\mathrm{D}_4(2)$ over the prime field in the Atlas. If H were in $\mathcal{N}_G(\langle \sigma_3 \rangle)$, then factoring by its cyclic normal subgroup of order $q^4 - q^2 + 1$ reveals that the corresponding factor \tilde{H} would be generated by a $(2, 4)$ -system, which is a contradiction to the product relation. So we have proved $H = {}^3\mathrm{D}_4(q)$ as required. \square

This immediately implies the following result, using that the first two classes in \mathbf{C} are rational, while elements in the third are conjugate to four of their primitive powers:

Theorem 4.9. *The groups ${}^3\mathrm{D}_4(q)$, $q = p^m$, possess G -realizations over \mathbb{Q}^{ab} for the class vector $\mathbf{C} = (C_1, C_2, C_3)$ defined in Proposition 4.8. More precisely, a field of index four in the cyclotomic field $\mathbb{Q}(\zeta_s)$ of $s := (q^4 - q^2 + 1)$ -th roots of unity is a field of definition for this Galois extension.*

4.5 Rigidity for the Groups ${}^2B_2(8)$ and ${}^2F_4(2)'$

In the preceding three sections, we have treated all series of exceptional groups of Lie rank at most two, apart from the Suzuki and Ree groups in characteristic 2, ${}^2B_2(q^2)$ and ${}^2F_4(q^2)$. No Galois realizations for them are known at present, except for the smallest group in each series. In particular for the Suzuki groups ${}^2B_2(2^{2m+1})$ one can check that the Basic Rigidity Criterion does not apply to any class triple \mathbf{C} if m is large.

The Suzuki groups $G = {}^2B_2(2^{2m+1})$ have a very transparent structure. Their character tables and maximal subgroups were determined by Suzuki. Thus all ingredients for the application of the character theoretic rigidity criterion are known. Only six different types of conjugacy classes exist in G . This makes it possible to compute $n(\mathbf{C})$ for all class vectors \mathbf{C} of length three. It turns out that the structure constants are nonconstant polynomials in $q^2 = 2^{2m+1}$, except if \mathbf{C} contains at least two involution classes (and hence $\sigma \in \bar{\Sigma}(\mathbf{C})$ cannot generate G). Furthermore it is not hard to prove that the contributions to $n(\mathbf{C})$ coming from proper subgroups are too small to diminish this growth rate for $l(\mathbf{C})$. From this it follows that the Suzuki groups for large m cannot be realized as Galois groups via the Basic Rigidity Theorem applied to a class triple \mathbf{C} .

However in the smallest simple case ${}^2B_2(8)$, a G -realization may be found (note that ${}^2B_2(2) \cong 5:4$ is solvable). Here the class names are taken from the Atlas.

Theorem 4.10. *The group $\text{Aut}({}^2B_2(8)) = {}^2B_2(8):3$ possesses a G -realization over $\mathbb{Q}(\sqrt{-3})$ for the class vector $\mathbf{C} = (2A, 3A, 15A)$. This yields a GA -realization of ${}^2B_2(8)$ for the class vector $(2A, 2A, 2A, 5A)$.*

Proof. From the Atlas one finds $n(\mathbf{C}) = 1$ in $\text{Aut}({}^2B_2(8))$. The only maximal subgroups of order divisible by 15 are the centralizers of the outer automorphisms, of type ${}^2B_2(2) \times 3 = 5:4 \times 3$. Factoring by the normal Sylow 5-subgroup we would arrive at a $(2, 3, 3)$ -system inside $4 \times 3 \cong Z_{12}$, which is a contradiction. So the generation is clear as well, proving that \mathbf{C} is rigid by Corollary I.5.9. The second assertion follows by descent to the simple subgroup of index 3, similar to the argument proving the Galois realization for A_n from the one of S_n . \square

The situation for the Ree groups ${}^2F_4(2^{2m+1})$ is not much better. Since now there are 52 families of conjugacy classes, a complete study is no longer possible. But all ‘promising’ class triples show a similar behavior to those of the Suzuki groups. Still, the smallest case can again be treated. Here ${}^2F_4(2) \cong \text{Ti}.2$, where $\text{Ti} = {}^2F_4(2)'$ (the Tits group) is a simple group not appearing elsewhere in the classification.

Theorem 4.11. *The group $\text{Ti} = {}^2F_4(2)'$ possesses G -realizations over $\mathbb{Q}(\sqrt{13})$ for the class vectors $\mathbf{C}_1 = (2A, 3A, 13A)$ and $\mathbf{C}_2 = (2A, 5A, 13A)$.*

Proof. From the Atlas character table one verifies that $n(\mathbf{C}_1) = n(\mathbf{C}_2) = 1$. The maximal subgroups of Ti with order divisible by 13 are $L_3(3) \cdot 2$ and $L_2(25) \cdot 2$. Since the group H generated by a triple $\sigma \in \bar{\Sigma}(\mathbf{C})$ is perfect by Proposition 4.3,

only $L_3(3)$ and $L_2(25)$ themselves remain as candidates. But the involution classes in both groups possess centralizer order divisible by 3, hence they must both fuse into $2B$ of G . So the class $2A$ intersects neither of them, and we have $H = G$. This proves rigidity by Corollary I.5.9. The character table reveals that $2A$, $3A$ and $5A$ are rational while $\mathbb{Q}_{13A} = \mathbb{Q}(\sqrt{13})$. \square

The second class vector will again turn up in the Galois realization of the sporadic Rudvalis group Ru.

5 The Exceptional Groups of Large Rank

Apart from those cases treated in the previous paragraph, the character tables of the exceptional groups are not yet completely known. Still, the theory of Deligne and Lusztig on the characters of reductive groups over finite fields furnishes enough information in most cases for the computation of structure constants, if the class vector is chosen carefully enough. Also, no complete lists of maximal subgroups for these groups have been obtained at present. But it is possible to enumerate the maximal subgroups lying above certain cyclic maximal tori (see for example Weigel (1992)), and this will suffice for our purpose.

5.1 Results From Deligne–Lusztig Theory

As in the previous paragraph, and in contrast to the case of classical groups, we shall not work with explicitly given triples of elements, but instead apply the character theoretic form of the Basic Rigidity Theorem. The determination of the structure constant for a chosen class vector requires the knowledge of at least part of the table of complex irreducible characters of G . This is furnished by the Deligne–Lusztig theory of characters of reductive groups over finite fields.

Let \mathbf{G} be a connected reductive algebraic group over the algebraic closure of \mathbb{F}_q , and $F : \mathbf{G} \rightarrow \mathbf{G}$ a Frobenius map. An important tool in the character theory of the groups \mathbf{G}^F are the characters $R_T(\theta)$ which were constructed in the fundamental paper of Deligne and Lusztig (1976). To each F -stable maximal torus T and to each irreducible (hence linear) character θ of $T := T^F$ a generalized character $R_T(\theta)$ can be defined. Two such characters have disjoint sets of constituents if the corresponding pairs (T, θ) and (T', θ') are not *geometrically conjugate*. Since every irreducible character of \mathbf{G}^F appears in some $R_T(\theta)$, this defines a partition of the set $\text{Irr}(\mathbf{G}^F)$ into a disjoint union of *Lusztig series*. However, the $R_T(\theta)$ do not span the whole space of class functions on \mathbf{G}^F , but a very large part of it. Elements in the \mathbb{Q} -span of the $R_T(\theta)$ are called *uniform functions*. Similarly, a conjugacy class C of \mathbf{G}^F is called uniform, if its characteristic function can be expressed as a linear combination of $R_T(\theta)$ s. For semisimple classes we have the following nice result:

Theorem 5.1 (Deligne and Lusztig). *Let \mathbf{G} be a connected reductive group with Frobenius endomorphism $F : \mathbf{G} \rightarrow \mathbf{G}$ and $s \in \mathbf{G}^F$ semisimple.*

- (a) *If $\chi(s) \neq 0$ for $\chi \in \text{Irr}(\mathbf{G}^F)$, then there exist geometrically conjugate pairs $(T, \theta), (T', \theta')$ with $R_T(\theta)(s) \neq 0$ and $(\chi, R_{T'}(\theta')) \neq 0$.*
- (b) *If $R_T(\theta)(s) \neq 0$ then there exists a $g \in \mathbf{G}^F$ with $T^g \leq C_{\mathbf{G}}(s)$.*

The first part follows directly from the fact that semisimple classes are uniform, the second is a consequence of the character formula (see Carter (1985), Prop. 7.5.5, Thm. 7.2.8). This shows that if s has a small centralizer, then only few irreducible characters of \mathbf{G}^F will take non-zero values on s .

In general, the characters $R_T(\theta)$ will themselves be irreducible. Only when θ is not in general position with respect to the Weyl group of T , then $R_T(\theta)$ has norm bigger than one. In particular, this is the case for $\theta = 1$. The irreducible constituents of the $R_T(1)$ are called *unipotent characters*. In Lusztig's classification of the irreducible characters of the groups \mathbf{G}^F they play a crucial role, similar to the role of the unipotent classes in the classification of all conjugacy classes of \mathbf{G}^F . In our applications, apart from the case E_7 , we will only need to know values of unipotent characters.

We give an explicit formula for these at least on semisimple classes. For its formulation, some more notation has to be introduced. For an arbitrary algebraic group H , let H° be the connected component of the identity. Furthermore, for a connected reductive group G let ε_G be the sign associated to G via the relative rank (see Carter (1985), p.199), and for a semisimple element $s \in G^F$, write $\varepsilon_s := \varepsilon_{\mathcal{C}_G^\circ(s)}$. Deligne and Lusztig (1976) proved the following result:

Proposition 5.2. *The value of the unipotent character ρ of the group \mathbf{G}^F on the semisimple element $s \in \mathbf{G}^F$ is given by*

$$\rho(s) = \varepsilon_s |\mathcal{C}_G^\circ(s)^F|_p^{-1} \cdot \sum_{T:s \in T} \varepsilon_T(\rho, R_T(1)). \quad (5.1)$$

The decomposition of the $R_T(1)$ into unipotent characters, and hence the scalar products $(\rho, R_T(1))$, were determined by Lusztig (1980) for exceptional groups.

It is possible to evaluate (5.1) effectively. For this, one can use the fact that all tori T^F containing s lie in $\mathcal{C}_G^\circ(s)^F$ (see Carter (1985), Prop. 3.5.2). By loc. cit., Thm. 3.5.4, $\mathcal{C}_G^\circ(s)$ is a reductive algebraic group itself. So the sum in (5.1) runs precisely over the maximal T^F of $\mathcal{C}_G^\circ(s)^F$. Now the \mathbf{G}^F -conjugacy classes of F -stable maximal tori T of G are parametrized by F -conjugacy classes $[w]_F \subset W(G)$ in the Weyl group. This is indicated by writing T_w for a torus parametrized by $w \in W$. Hence with $C := \mathcal{C}_G^\circ(s)^F$, the C -class $[T_w]$ contains exactly $|C|/|\mathcal{N}_C(T_w)|$ different maximal tori conjugate to T_w . Writing W_0 for the Weyl group of C we therefore have

$$|\mathcal{N}_C(T_w)| = |T_w^F| \cdot (\mathcal{N}_C(T_w) : T_w^F) = |T_w^F| \cdot |\mathcal{C}_{W_0}(w)|,$$

where $\mathcal{C}_{W_0}(w)$ denotes the F -centralizer of w in W_0 . Moreover, for \mathbf{G}^F of untwisted type, define the *almost characters*

$$R_\chi := |W|^{-1} \sum_{w \in W} \chi(w) R_{T_w}(1) \quad \text{for } \chi \in \text{Irr}(W). \quad (5.2)$$

Then (5.1) becomes

Corollary 5.3. *If \mathbf{G}^F is of untwisted type, the value of the unipotent character ρ of the group \mathbf{G}^F on the semisimple element $s \in \mathbf{G}^F$ is given by*

$$\rho(s) = \varepsilon_s |\mathcal{C}_{\mathbf{G}}^\circ(s)^F|_{p'} \cdot \sum_{\chi \in \text{Irr}(W)} (\rho, R_\chi) \cdot \sum_{[w] \subseteq W_0} \varepsilon_{T_w} \frac{\chi(w)}{|\overline{T}_w^F| \cdot |\mathcal{C}_{W_0}(w)|}. \quad (5.3)$$

This looks more complicated than (5.1) but in fact all ingredients in this formula are explicitly known, and the sum may thus be effectively computed for all unipotent characters ρ of \mathbf{G}^F . The multiplicities (ρ, R_χ) are determined by the $(\rho, R_T(1))$ via (5.2). Tables of these numbers are given in Carter (1985), Sect. 13.6.

The theory for the values on arbitrary elements is not yet complete. But for uniform classes, by definition the character values are linear combinations of $R_T(\theta)$, and an analogue of (5.1) holds. It turns out that in these cases it suffices to know the *Green functions* of \mathbf{G}^F , which are defined as the restrictions of the $R_T(\theta)$ to the set of unipotent elements. They do not depend on θ , but only on the \mathbf{G}^F -class of T . Tables of them have been calculated for exceptional groups at least in good characteristic. For details, the reader is referred to the books of Lusztig (1984), Carter (1985) or Digne and Michel (1991).

Important parts of this theory have been generalized to disconnected groups \mathbf{G} by Digne and Michel (1994). This will be useful in the treatment of groups of type E_6 .

5.2 Rigidity for the Groups $F_4(q)$

The character table of the groups $F_4(q)$ is not yet known in general. Only the smallest group $F_4(2)$ has been included in the Atlas. Also, no complete lists of maximal subgroups have been obtained for these groups. There are partial results, in good characteristic, but in general the problem is still open. Through a good choice of class vector, both of the above problems may be circumvented.

The conjugacy classes of elements in $G = F_4(q)$ were determined by Shoji (1974) in characteristic $p \geq 3$, and by Shinoda (1974) for even q . We define C_p to be the class of (unipotent) p -elements in long root subgroups. They are central elements of a Sylow p -subgroup of G , and are characterized by this property if p is odd. This class is called $[x_1]$ in Shoji (1974), and $[x_2]$ in Shinoda (1974).

Furthermore, G contains two families of semisimple classes such that its elements have centralizer type $A_2 + A_1$, one of them having h_{10} as representative in Shoji (1974), the other h_{16} (resp. h_{16}, h_{17} in Shinoda (1974)). We let $C_{q+1} := [h_{16}]$. For odd q this class may also be characterized by the fact that its $(q+1)/2$ -th power is the involution with centralizer structure B_4 . In even characteristic, the two families of classes are interchanged by the exceptional graph automorphism. Finally, choose C_T to contain elements of order $q^4 - q^2 + 1 = \phi_{12}$, generating a Coxeter torus of $F_4(q)$. Representatives for this class are denoted by h_{99}, h_{76} respectively, in loc. cit. For $F_4(2)$, we use the class names from the Atlas.

Proposition 5.4. (a) *The class vector $\mathbf{C} = (C_p, C_{q+1}, C_T)$ of $F_4(q)$, $q = p^m \neq 2$, is rigid.*

(b) *The class vector $\mathbf{C} = (2A, 8A, 17A)$ of $F_4(2)$ is rigid.*

Proof. In (a), the elements in class C_T generate a cyclic maximal torus T of order ϕ_{12} , which is easily seen to be a Hall subgroup of $G = F_4(q)$ by the order formula. In particular all of its non-identity elements are regular. By Theorem 5.1 this means that the only Deligne–Lusztig characters not vanishing on C_T are among the $R_T(\theta)$, θ a linear character of T in general position, and the $R_{T'}(1)$ for arbitrary maximal tori T' . But again by Theorem 5.1 the first take value zero on elements in C_{q+1} , since their centralizer does not contain a conjugate of T for order reasons. It remains to consider the constituents of the $R_{T'}(1)$, hence the 37 unipotent characters of G . For a list of these, see Carter (1985), Sect. 13.9. With Corollary 5.3, their values on C_T may easily be computed, and it turns out that only twelve among them do not vanish on C_T . Next, the same can be done for the semisimple class C_{q+1} . Precisely five unipotent characters are found not to vanish on C_{q+1} and C_T . Their values are given in Table 5.1.

Table 5.1 Character values in $F_4(q)$

	1	C_p	C_{q+1}	C_T
$\phi_{1,0}$	1	1	1	1
$\phi_{1,24}$	q^{24}	0	q^4	1
$B_{2,1}$	$\frac{1}{2}q\phi_1^2\phi_3^2\phi_8$	$-\frac{1}{2}q\phi_1\phi_3(q^4 - q^3 + 1)$	$-\phi_1^2$	1
$B_{2,\epsilon}$	$\frac{1}{2}q^{13}\phi_1^2\phi_3^2\phi_8$	$-\frac{1}{2}q^{13}\phi_1\phi_3$	$-q^2\phi_1^2$	1
$\phi_{6,6''}$	$\frac{1}{12}q^4\phi_3^2\phi_4^2\phi_6^2\phi_8$	$\frac{1}{12}q^4\phi_3\phi_4\phi_6(3q^4 + 2q^2 + 1)$	$-2q\phi_6$	1

It remains to prove the correctness of the values on the unipotent class C_p . It follows from Shoji (1982) in characteristic $p \geq 5$, from Porsch (1993) in characteristic 3 and from Malle (1993c) in characteristic 2 that the class C_p is uniform, and then the values may be computed from the Green functions given in the cited references. The desired structure constant $n(\mathbf{C}) = 1$ now follows from Table 5.1 and the centralizer orders

$$|\mathcal{C}_G(\sigma_1)| = q^{24}(q^2 - 1)(q^4 - 1)(q^6 - 1),$$

$$|\mathcal{C}_G(\sigma_2)| = q^4(q + 1)(q^2 - 1)^2(q^3 + 1), \quad |\mathcal{C}_G(\sigma_3)| = q^4 - q^2 + 1.$$

Next we have to prove generation. For this let $H := \langle \sigma \rangle$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$. Then H contains the maximal torus $T = \langle \sigma_3 \rangle$. Now for $q \geq 4$ the possible overgroups of T in G have been completely classified by Weigel (1992) (see his Table I and Figs. 4 and 5). From the proof given there it follows that this remains true for $q = 3$.

except for a possible additional overgroup $U_3(9)$. But such a group cannot contain H , since in ${}^2A_2(3^2)$ any element of order $4 = q + 1$ has centralizer order divisible by 5, which is not the case for $|\mathcal{C}_G(\sigma_2)|$. Hence for $q \geq 3$ the group H has one of the structures given in loc. cit. Now $\mathcal{N}_G(T) \cong (q^4 - q^2 + 1).12$, which can be ruled out since H is perfect by Proposition 4.3. Thus we are left with the candidates ${}^3D_4(q)$ and $F_4(q)$ for H .

It remains to exclude that $H = {}^3D_4(q)$. First assume that $p \neq 2$. Then by Deriziotis and Michler (1987) H has a single class of involutions C . This would have to fuse into the class C_2 of $\sigma_2^{(q+1)/2}$, which by definition is the one with centralizer structure B_4 in G . Since the normalizer of a torus of order ϕ_{12} has structure $\phi_{12}.4$ in H , H contains a dihedral group $\phi_{12}.2$ with involutions in C_2 . But in G one calculates $n(C_2, C_2, C_T) = 0$ (similarly to the determination of $n(C)$ above), so we obtain a contradiction to the assumption that C fuses into C_2 , and $H = G$ follows for odd q .

If $p = 2$, the groups $F_4(2^m)$ possess exactly two classes of (maximal) subgroups ${}^3D_4(2^m):3$, which are interchanged by the graph automorphism γ (see loc. cit.). We now study the fusion of some classes from these maximal subgroups into the classes C_p and C_{q+1} of G .

By Spaltenstein (1982), ${}^3D_4(2^m)$ contains two classes of involutions, denoted there by A_1 and $3A_1$. Of these, A_1 can only fuse into one of C_2 or C_2^γ , as can be seen from the centralizer orders. On the other hand, elements from $3A_1$ cannot fuse into either C_2 , C_2^γ , since the first are contained in the normalizer of the torus T , but not the second. This can be seen by calculating the corresponding structure constant $n(3A_1, 3A_1, C_T)$ in the group ${}^3D_4(2)$, resp. (C_2, C_2, C_T) in $F_4(2)$, in the Atlas, since representatives for $3A_1$, resp. C_2 , are already defined over \mathbb{F}_2 . Further ${}^3D_4(2^m)$ contains just one class of maximal tori of order $(q+1)(q^3+1)$, while G possesses two, denoted by $C_3 + A_1$ and D_4 in Table 1 of Shinoda (1974), and interchanged by the outer automorphism γ . If both types of tori contained elements conjugate to h_{16} , then both types would also occur in $\mathcal{C}_G(\sigma_2) \cong {}^2A_2(q).A_1(q).(q+1)$. But in the latter group, all tori of that order are conjugate, which yields a contradiction. Hence the element h_{16} lies in one of the two types of tori, the element h_{17} in the other. The above discussion shows that one class of maximal subgroups ${}^3D_4(2^m):3$ of G only contains elements from C_2 and $[h_{17}]$, say, while the other only contains elements from C_2^γ and $[h_{16}] = [h_{17}^\gamma]$. Thus H cannot lie in either of the two, and the proof is complete.

For $G = F_4(2)$, the character table in the Atlas yields $n(C) = 1$. The classes of maximal subgroups of G were enumerated by Norton and Wilson (1989). The only ones with order divisible by 17 are two groups $S_8(2)$. The permutation characters for these subgroups are easily determined to be

$$\chi_1 + \chi_4 + \chi_6 + \chi_{10} + \chi_{12}, \quad \chi_1 + \chi_3 + \chi_6 + \chi_9 + \chi_{11},$$

which both vanish on the class $8A$. (Alternatively, one knows that these $S_8(2)$ are generated by long, resp. short root elements, while the class $8A$ contains products

of root elements for long and short roots.) This completes the proof also in the case $q = 2$. \square

Theorem 5.5. *The groups $F_4(q)$, $q = p^m$, possess G -realizations over abelian number fields $k(q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector \mathbf{C} of Proposition 5.4. For $q = 2$ this yields a G -realization of $F_4(2)$ over $\mathbb{Q}(\sqrt{17})$.*

The rationality assertion for $F_4(2)$ follows from the Atlas table.

Galois realizations over \mathbb{Q} of infinitely many groups $F_4(p)$ for primes p are contained in Paragraph 8.

5.3 Rigidity for the Groups $E_6(q)$ and ${}^2E_6(q)$ for odd q

The circumstances for groups of type E_6 are less favorable than for type F_4 , since here, as in the case of classical groups, they exist in different isogeny types. This entails that the simple group $E_6(q)$ in general is a subgroup of index three in the group of adjoint type $E_6(q)_{\text{ad}}$. Or, if we start from the simply connected group $E_6(q)_{\text{sc}}$, then $E_6(q)$ is obtained by factoring out a center of order three. Both situations turn out to be hostile to the existence of rigid class triples. But the Dynkin diagram of E_6 has a graph automorphism of order two. We will prove G -realizations for the group $E_6(q)_{\text{sc}}:2$, obtained by extending the simply connected group by this graph automorphism, at least in characteristic $p \geq 3$. For $p = 2$ this approach fails, and we will treat this case in the next section.

So first let $G := E_6(q)_{\text{sc}}:2$ be the extension by the graph automorphism of order two of the simply connected group of type E_6 , and assume that $q = p^m$ is odd. Then G may be regarded as the group of fixed points under a Frobenius map F of a disconnected reductive algebraic group. It was shown by Digne and Michel (1994) that the Deligne–Lusztig theory has a nice and straightforward generalization to disconnected groups. So there exist generalized Deligne–Lusztig characters for such groups, indexed by the classes of maximal tori in the centralizer of the graph automorphism. Also, the character formulae given in the first section remain valid, with a suitable interpretation. The decomposition of the generalized Deligne–Lusztig characters in the case of disconnected groups of type E_6 was determined in Malle (1993b), so all ingredients are available to explicitly compute character values also for G .

Let C_2 be the class of the graph automorphism γ in G . Now γ clearly centralizes an $F_4(q)$ and we have $\mathcal{C}_G(\gamma) = F_4(q) \times 2$. If $q \equiv 1 \pmod{3}$ then $E_6(q)_{\text{sc}}$ has a center of order three. Since $\mathcal{Z}(F_4(q)) = 1$, γ acts non-trivially on that center, and G is a group with trivial center. Let u be a unipotent element in $\mathcal{C}_G(\gamma)$ with $|\mathcal{C}_{F_4}(u)| = q^{24}\phi_1^3\phi_2^3\phi_3\phi_4\phi_6$, which hence is central in a Sylow p -subgroup of $F_4(q)$; since $p \neq 2$, the corresponding class is uniquely determined by this property. The element $u\gamma$ then has order $2p$ and centralizer order $2q^{24}\phi_1^3\phi_2^3\phi_3\phi_4\phi_6$ in G . From the list of conjugacy classes in Mizuno (1977) it follows that u must

have centralizer order $q^{36}\phi_1^5\phi_2^3\phi_3^2\phi_4\phi_5\phi_6$ in G , because only that centralizer of a unipotent element contains a subgroup $C_3(q)$ (compare also with the lists in Carter (1985), p.402). Denote the class of $u\gamma$ in G by C_{2p} .

Finally, let T be a maximal torus of G of order $q^6 + q^3 + 1 = \phi_9$, and let C_T be the conjugacy class of a generating element σ_3 in this torus. Then we have $|\mathcal{C}_G(\sigma_3)| = \phi_9$, since the outer automorphism acts fixed point freely on T .

Proposition 5.6. *The class vector $\mathbf{C} = (C_{2p}, C_{2p}, C_T)$ of $E_6(q)_{sc}:2$, $q = p^m$, $p \neq 2$, is rigid.*

Proof. We first calculate the structure constant for \mathbf{C} . If an irreducible character χ of G does not vanish on the class C_T , then clearly the same holds for its restriction to $G' := E_6(q)_{sc}$. Thus we first classify the irreducible characters of the connected group G' not vanishing on C_T . Since $\mathcal{C}_{G'}(\sigma) = T$ for all elements $\sigma \in T$ not lying in $\mathcal{Z}(G')$, these are the constituents of $R_T(\theta)$ and of $R_{T'}(\theta')$, where T' is an arbitrary torus with character θ' of order dividing 3 corresponding to the central elements of G' . Since γ acts non-trivially on $\mathcal{Z}(G')$, those with $\theta' \neq 1$ are not γ -stable. It then follows that none of their constituents extends to G , so they will not contribute to $n(\mathbf{C})$. The irreducible $R_T(\theta)$ are either not γ -stable, or vanish on the class of γ , since the centralizer of γ does not contain T , as follows from the character formula for disconnected groups (see Digne and Michel (1994), Prop. 2.4). Hence it remains to consider the constituents of the $R_{T'}(1)$, the unipotent characters of G' . Nine of them do not vanish on C_T by (5.1). Of these, another two take value zero on the outer *quasi-central* class C_2 , again by the character formula in loc. cit. The remaining seven characters and their values on classes in \mathbf{C} and on the class C_2 , which will be needed in the proof, are given in Table 5.2.

Table 5.2 Character values in $E_6(q)_{sc}:2$

	1	C_2	C_{2p}	C_T
$\phi_{1,0}$	1	1	1	1
$\phi_{20,2}$	$q^2\phi_4\phi_5\phi_8\phi_{12}$	$q\phi_4\phi_8\phi_{12}$	$q(q^6 + q^4 + 1)$	-1
$\phi_{20,20}$	$q^{20}\phi_4\phi_5\phi_8\phi_{12}$	$q^{13}\phi_4\phi_8\phi_{12}$	q^{13}	-1
$\phi_{1,36}$	q^{36}	q^{24}	0	1
$\phi_{90,8}$	$\frac{1}{3}q^7\phi_3^3\phi_5\phi_6^2\phi_8\phi_{12}$	$\frac{1}{3}q^4\phi_3^2\phi_6^2\phi_8\phi_{12}$	$\frac{1}{3}q^4\phi_3\phi_6(2q^4 + 1)$	-1
$E_6[\theta]$	$\frac{1}{3}q^7\phi_1^6\phi_2^4\phi_4^2\phi_5\phi_8$	$\frac{1}{3}q^4\phi_1^4\phi_2^4\phi_4^2\phi_8$	$-\frac{1}{3}q^4\phi_1^3\phi_2^3\phi_4$	-1
$E_6[\theta^2]$	$\frac{1}{3}q^7\phi_1^6\phi_2^4\phi_4^2\phi_5\phi_8$	$\frac{1}{3}q^4\phi_1^4\phi_2^4\phi_4^2\phi_8$	$-\frac{1}{3}q^4\phi_1^3\phi_2^3\phi_4$	-1

Note that each line represents the two extensions of a unipotent character from G' to G . Our notation for the unipotent characters is the same as in Carter (1985), Sect 13.9. Here the entries on the mixed class C_{2p} may again be determined from

the character formula in Digne and Michel (1994). This requires knowledge of the Green functions on C_{2p}^2 , which can be found in Beynon and Spaltenstein (1984) for $p \geq 5$, and in Porsch (1993) for $p = 3$. Note that by Digne and Michel (1994), Props. 2.4 and 4.10, the class C_{2p} is uniform if C_{2p}^2 is uniform, and the latter holds by the criterion of Lusztig (1977) (remark after 2.16). Using the centralizer orders given before, the result $n(\mathbf{C}) = 1$ follows from Table 5.2.

Now let $H := \langle \sigma \rangle$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$ and $\bar{H} := H/(H \cap \mathcal{Z}(G'))$. The element σ_3 generates a maximal torus of G of order $q^6 + q^3 + 1$. By Weigel (1992), Fig. 6, if we can exclude $\bar{H} \leq A_2(q^3):6$ then $\bar{H} = \bar{G}$ follows. We cannot have $\bar{H} = A_2(q^3)$ since otherwise $\bar{H} \cap \bar{G}'$ would be a subgroup of index two in that simple group. On the other hand, \bar{T} is already contained in $A_2(q^3)$, hence \bar{H} has to be an extension of degree 2 of this group. More precisely, this has to be the extension with the graph automorphism. Namely, if q is not a square, $A_2(q^3)$ has only this non-trivial degree 2 extension. If on the other hand $q = r^2$ is a square, then the field automorphism centralizes an $A_2(r^3)$, the graph field automorphism a ${}^2A_2(r^3)$. But neither of these is contained in $\mathcal{C}_G(\sigma_1^p) = F_4(q) \times 2$, as is seen using a primitive prime divisor of $\phi_9(r)$, $\phi_{18}(r)$ respectively.

The particular extension of $A_2(q^3)$ with the graph automorphism is again a disconnected group, and as above, but much easier, the following table of values is obtained:

Table 5.3 Character values in $A_2(q^3):2$

	1	c_2	c_T
χ_3	1	1	1
χ_{21}	$q\phi_2$	0	-1
χ_{111}	q^3	q	1

It contains all characters of $A_2(q^3)$ not vanishing on regular elements in its torus of order $q^6 + q^3 + 1$ and on its unique class c_2 of outer involutions. We find that $n(c_2, c_2, c_T) = 1$ in $A_2(q^3):2$, but from Table 5.2 we see $n(C_2, C_2, C_T) = 0$, which shows that C_2 does not intersect an $A_2(q^3):2$. So finally we have proved that $\bar{H} = \bar{G}$, and since the extension by the center is non-split, also that $H = G$. \square

Application of the Rigidity Criterion yields:

Theorem 5.7. *The groups $E_6(q)_{sc}:2$, $q = p^m$, $p \neq 2$, possess G -realizations over abelian number fields $k(q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector \mathbf{C} of Proposition 5.6.*

By descent from $E_6(q)_{sc}:2$ to $E_6(q)_{sc}$ as in the proof of Corollary 1.5, and then by taking factor groups modulo the center, this immediately gives Galois realizations for the simple groups:

Corollary 5.8. *The groups $E_6(q)_{sc}$, $E_6(q):2$ and $E_6(q)$, q odd, possess G -realizations over the same fields $k(q)$ as for $E_6(q)_{sc}:2$ in Theorem 5.7.*

As a corollary to the proof of Proposition 5.6 we also obtain:

Theorem 5.9. *The groups $E_6(q)_{ad}:2$ and $E_6(q)_{ad}$, q odd, possess G -realizations over \mathbb{Q}^{ab} .*

Proof. The only cases to consider are those where $E_6(q)_{sc} \not\cong E_6(q)_{ad}$, i.e., where $q \equiv 1 \pmod{3}$. Denote by $\tilde{\mathbf{C}}$ the canonical image in $\tilde{G} = E_6(q):2$ of the rigid class vector \mathbf{C} of $G = E_6(q)_{sc}:2$. Here the image \tilde{C}_{2p} of the class C_{2p} is again an outer class, i.e., not contained in $\tilde{G}' = E_6(q)$. The image \tilde{T} of the maximal torus T of G defined above extends to a maximal torus \tilde{T} of $\tilde{G} = E_6(q)_{ad} \cong E_6(q):3$. We denote by \tilde{C}_T the class of a generating element of this cyclic subgroup \tilde{T} of \tilde{G} . Since the unipotent characters of a group of Lie type are classified independently of the isogeny type of the group, precisely the same arguments as in the proof of Proposition 5.6 show that the class vector $\tilde{\mathbf{C}} = (\tilde{C}_{2p}, \tilde{C}_{2p}, \tilde{C}_T)$ of the extension $\tilde{G}:2$ of \tilde{G} by the graph automorphism has structure constant $n(\tilde{\mathbf{C}}) = 1$. Also, the proof of generation remains valid, which yields rigidity of $\tilde{\mathbf{C}}$. Since $\tilde{G}:2/\tilde{G}' \cong S_3$ the descent to all groups above and including $\tilde{G}' = E_6(q)$ is possible by the standard descent argument. \square

Since for $q = p$ the group $E_6(p)_{ad}:2$ is the full automorphism group of the simple group $E_6(p)$, we may conclude from this:

Corollary 5.10. *For $p \neq 2$ the groups $E_6(p)$ possess GA-realizations over \mathbb{Q}^{ab} .*

Remark. Theorem 5.7 realizes $E_6(q)_{sc}:2$ as a Galois group for the class vector $\mathbf{C} = (C_{2p}, C_{2p}, C_T)$. By the Fixed Point Theorem I.7.2, we may obtain a further Galois realization for a class vector $\mathbf{C}' := (C, C_{2p}, C_T)$ of G , with C some class of outer involutions different from C_{2p} . The generating systems contained in $\Sigma(\mathbf{C}')$ arise because the generating triple in \mathbf{C} is a fixed point under the geometric automorphism interchanging the first two (identical) classes. Indeed, the structure constant for \mathbf{C}' may be calculated as in Proposition 5.6, and turns out to be equal to 1. This gives a second proof for the existence of Galois realizations.

The twisted groups ${}^2E_6(q)$ may be treated in an entirely analogous way. The extension by the graph automorphism $G = {}^2E_6(q):2$ also exists for the twisted groups. The classes for \mathbf{C} may be chosen as before, except that we now take C_T to contain generators of a torus of order $\phi_{18} = q^6 - q^3 + 1$. Then the class vector (C_{2p}, C_{2p}, C_T) for G is rigid when q is odd. The proof can be copied word for word from the one for Proposition 5.6, using the relevant part of the character table given in Table 5.4.

It may be noticed that Table 5.4 is obtained from Table 5.2 by simply replacing q by $-q$ everywhere. This observation is explained by the Ennola duality for groups of Lie type.

For generation, we again cite Weigel (1992), Fig. 7, who treats the case $q > 3$. The table for ${}^2A_2(q^3):2$ corresponding to Table 5.3 is again obtained by just replacing q by $-q$, and the arguments go through as above. For $q = 3$, the methods of loc. cit. again lead to the only possibility ${}^2A_2(3^3):2$, for which we proceed as before. We can thus prove:

Theorem 5.11. *The groups ${}^2\mathrm{E}_6(q)_{sc}:2$, $q = p^m$, $p \neq 2$, possess G -realizations over abelian number fields $k(q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector $\mathbf{C} = (C_{2p}, C_{2p}, C_T)$. The groups ${}^2\mathrm{E}_6(q)_{sc}$, ${}^2\mathrm{E}_6(q):2$ and ${}^2\mathrm{E}_6(q)$ possess G -realizations over the same fields $k(q)$.*

Table 5.4 Character values in ${}^2\mathrm{E}_6(q):2$

	1	C_2	C_{2p}	C_T
$\phi_{1,0}$	1	1	1	1
$\phi_{4,1}$	$q^2\phi_4\phi_8\phi_{10}\phi_{12}$	$q\phi_4\phi_8\phi_{12}$	$q(q^6 + q^4 + 1)$	-1
$\phi_{4,13}$	$q^{20}\phi_4\phi_8\phi_{10}\phi_{12}$	$q^{13}\phi_4\phi_8\phi_{12}$	q^{13}	-1
$\phi_{1,24}$	q^{36}	q^{24}	0	1
$\phi_{6,6''}$	$\frac{1}{3}q^7\phi_3^2\phi_6^2\phi_8\phi_{10}\phi_{12}$	$\frac{1}{3}q^4\phi_3^2\phi_6^2\phi_8\phi_{12}$	$\frac{1}{3}q^4\phi_3\phi_6(2q^4 + 1)$	1
$E_6[\theta]$	$\frac{1}{3}q^7\phi_1^4\phi_2^6\phi_4^2\phi_8\phi_{10}$	$\frac{1}{3}q^4\phi_1^4\phi_2^4\phi_4^2\phi_8$	$-\frac{1}{3}q^4\phi_1^3\phi_2^3\phi_4$	1
$E_6[\theta^2]$	$\frac{1}{3}q^7\phi_1^4\phi_2^6\phi_4^2\phi_8\phi_{10}$	$\frac{1}{3}q^4\phi_1^4\phi_2^4\phi_4^2\phi_8$	$-\frac{1}{3}q^4\phi_1^3\phi_2^3\phi_4$	1

As for $\mathrm{E}_6(q)$ we also obtain the result for the adjoint group from the above proof:

Theorem 5.12. *The groups ${}^2\mathrm{E}_6(q)_{ad}:2$ and ${}^2\mathrm{E}_6(q)_{ad}$, q odd, possess G -realizations over \mathbb{Q}^{ab} . For $q = p$ this yields a GA-realization of ${}^2\mathrm{E}_6(p)$, p odd, over \mathbb{Q}^{ab} .*

5.4 Rigidity for the Groups $\mathrm{E}_6(2^{2m+1})$ and ${}^2\mathrm{E}_6(2^{2m})$

The G -realizations given in the previous section needed the assumption $p \neq 2$ already in the definition of the class C_{2p} . It turns out that a rather similar class also exists in characteristic two, but it contains involutions, so that the class vector \mathbf{C} would consist of two involution classes and hence could not contain generating systems for our non-solvable groups.

In characteristic 2, at present rigid class vectors are only known when the adjoint group coincides with the simply connected group, i.e., for $\mathrm{E}_6(2^{2m+1})$ and ${}^2\mathrm{E}_6(2^{2m})$. This result will now be presented. First let $G = \mathrm{E}_6(2^{2m+1})$ where $m \geq 0$. We refer to the list of conjugacy classes of G given by Mizuno (1977). Let $C_2 = [x_1]$ be the class of involutions central in a maximal unipotent subgroup of G , with centralizer order $q^{36}\phi_1^5\phi_2^3\phi_3^2\phi_4\phi_5\phi_6$, $C_8 = [x_{11}]$ the class of unipotent elements with centralizer order $q^{15}\phi_1$, and finally let C_T be our well known class of generators of a torus with order $\phi_9 = q^6 + q^3 + 1$. From the representative element x_{11} given by Mizuno it is easily verified that elements in C_8 indeed have order 8. All three classes exist for all $q = 2^{2m+1}$.

Proposition 5.13. *The class vector $\mathbf{C} = (C_2, C_8, C_T)$ of $E_6(2^{2m+1})$, $m \geq 0$, is rigid.*

Proof. First one determines the irreducible characters not vanishing on the class C_T . As in the proof of Proposition 5.6 these are at most the unipotent characters and the irreducible $R_T(\theta)$. Their values on the semisimple class C_T follow readily with (5.1), while for the determination of those on the unipotent classes C_2 and C_8 we need the Green functions in characteristic 2 calculated in Malle (1993c). There the classes are denoted as $[u_1]$ and $[u_{18}]$, and it is proved that both are uniform. Hence the values can be computed from Table 6 in loc. cit. It turns out that only three unipotent characters take non-zero values on both C_8 and C_T . They are listed in Table 5.5, together with the family of irreducible $R_T(\theta)$. The structure constant $n(\mathbf{C}) = 1$ then follows.

Table 5.5 Character values in $E_6(2^{2m+1})$

	1	C_2	C_8	C_T
$\phi_{1,0}$	1	1	1	1
$\phi_{20,2}$	$q^2\phi_4\phi_5\phi_8\phi_{12}$	$q^2\phi_5$	$q^2\phi_2$	-1
$\phi_{64,4}$	$q^4\phi_2^3\phi_4^2\phi_6^2\phi_8\phi_{12}$	$q^4\phi_2^2\phi_4\phi_5\phi_6(q^3 - q + 1)$	q^4	1
$R_T(\theta)$	$\phi_1^6\phi_2^4\phi_3^3\phi_4^2\phi_5\phi_6^2\phi_8\phi_{12}$	$-\phi_1^5\phi_2^3\phi_3^2\phi_4\phi_5\phi_6\phi_8$	$\phi_1(q^3 - q - 1)$	{-1}

If we let $H := \langle \sigma \rangle$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$, then as in the proof of Proposition 5.6 we see that Weigel (1992), Fig. 6, applies. But none of the proper subgroups listed there contains elements of order 8. This is clear for $SL_3(2^{2m+1})$, since its unipotent classes all have representatives in $SL_3(2) \cong L_2(7)$. But then it also holds for the odd order extension $SL_3(2^{2m+1}).3$. Since all other candidates different from G are contained in the latter, this concludes the proof. \square

Application of the Basic Rigidity Criterion now yields:

Theorem 5.14. *The groups $E_6(2^{2m+1})$, $m \geq 0$, possess G -realizations over abelian number fields for the class vector $\mathbf{C} = (C_2, C_8, C_T)$.*

Again this may immediately be transferred to the twisted groups. Namely, let $G := {}^2E_6(2^{2m})$. Then the simple group again coincides with the one of adjoint type. A classification of unipotent classes for these groups is contained in Malle (1993c), Table 9. Let $C_2 = [u_1]$ be the unipotent class with centralizer order $q^{36}\phi_1^3\phi_2^5\phi_3\phi_4\phi_6^2\phi_{10}$, $C_8 = [u_{18}]$ the class of unipotent elements with centralizer order $q^{15}\phi_2$, and C_T a class of generators for the anisotropic torus of order ϕ_{18} . All three classes exist for all q .

With the same arguments as above, one proves that $\mathbf{C} = (C_2, C_8, C_T)$ for G is rigid. This leads to:

Theorem 5.15. *The groups ${}^2\mathrm{E}_6(2^{2m})$, $m \geq 1$, possess G -realizations over abelian number fields for the class vector $\mathbf{C} = (C_2, C_8, C_T)$.*

5.5 Rigidity for the Groups $E_7(q)$

The hardest case of all exceptional groups occurs for the groups of type E_7 . Since the Euler φ -function of any integer $n \geq 3$ is even, one may deduce that there exist no good maximal tori T in groups of odd rank. Still, instead of a maximal torus we can find a subtorus on which few characters do not vanish. The proofs in this section will not be given in full detail.

Let $G := E_7(q)_{ad}$ with $q = p^n$ the power of an odd prime p . Then the simple group $G' = E_7(q)$ has index 2 in G . The semisimple conjugacy classes of G can be found in Deriziotis (1983) or in Fleischmann and Janiszczak (1993), while the unipotent classes were determined by Mizuno (1980). A class bearing some similarity to the classes C_T used so far is C_T^δ , containing generators of the maximal torus of order $(q - \delta)(q^6 + \delta q^3 + 1)$ with $q \equiv -\delta \pmod{3}$, $\delta \in \{-1, 1\}$. Define C_p to be the unipotent class $4A_1$ in Mizuno (1980) or in Carter (1985), p.403. To assure generation of G , choose the third class so as to contain involutions from $G \setminus G'$. According to Borel et al. (1970), Part F, §§11 and 12, those have centralizer structure A_7 or 2A_7 . More precisely, in the case $q \equiv 1 \pmod{4}$ an involution with centralizer $A_7(q)$ is not contained in G' , and in the case $q \equiv -1 \pmod{4}$ the one with centralizer $A_7(q)$ lies outside G' . For $q \equiv \varepsilon \pmod{4}$, $\varepsilon \in \{1, -1\}$, let the class C_2^ε consist of such elements.

Proposition 5.16. *The class vector $\mathbf{C} = (C_2^\varepsilon, C_p, C_T^\delta)$ of $E_7(q)_{ad}$, $q = p^m$, $p \neq 2$, is rigid.*

Proof. We first classify the Deligne–Lusztig characters $R_{T'}(\theta)$ not vanishing on the third class C_T^δ . This is equivalent to finding the semisimple conjugacy classes in the dual T^* of T . These are easily determined, and we list them in Table 5.6.

Table 5.6 Semisimple classes in T^* .

$o(s)$	# of classes	$\mathcal{C}_{G^*}(s)^*$	# of chars.
1	1	G	76
2	1	G	76
$ q - \delta \neq 1, 2$	$(q - 2 - \delta)/2$	$(q - \delta) \cdot E_6^\delta(q)$	30
$ q - \delta $	$(q - \delta)(q^6 + \delta q^3)/18$	T	1

Here the notation $E_6^\delta(q)$ is shorthand for $E_6(q)$ if $\delta = 1$ and ${}^2E_6(q)$ if $\delta = -1$ (note that for the congruence $q \equiv -\delta \pmod{3}$ the adjoint and the simply connected types

of these groups coincide). The last column indicates how many irreducible characters of G occur as constituents of the $R_{T'}(\theta)$ parametrized by the semisimple element s .

The first two classes yield the extensions to $E_7(q)_{ad} = E_7(q) \cdot 2$ of the 76 unipotent characters of G' . The last family consists of the irreducible $R_T(\theta)$, and they vanish on C_2^ε by Theorem 5.1, since T is not contained in the centralizer of such involutions. The values of the remaining characters on our three classes can be calculated from the Green functions and informations on the Weyl groups of types E_6 , E_7 and A_7 . We omit the cumbersome details, and also the resulting table of values (they are given in Malle (1986), respectively in Lübeck and Malle (1998) for $p \leq 5$). It turns out that indeed $n(\mathbf{C}) = 1$.

For generation we may again turn to Weigel (1992), Fig. 9 and Fig. 10. First assume $\delta = 1$. Then we have to exclude the possibility $(q-1) \cdot E_6(q) \cdot 2$ and the parabolic subgroups of type $Q \cdot (q-1) \cdot E_6(q)$, with the unipotent radical Q . Denote by H the group generated by a triple $\sigma \in \bar{\Sigma}(\mathbf{C})$. In the first case $H \leq (q-1) \cdot E_6(q) \cdot 2$, factoring by the normal subgroup $H \cap E_6(q)$ obviously yields a p' -group, so it has a $(2, 1, 2)$ -system or reduces to the identity. In any case this would imply that $E_6(q)$ contains elements of order $(q-1)\phi_9$, which is not the case since its torus of order ϕ_9 is self-centralizing. Similarly, the second possibility may be excluded, after first factoring out the normal p -subgroup $H \cap Q$.

The same arguments also apply when $\delta = -1$, only here the second possibility doesn't even arise. This completes the proof of generation since C_2^ε was chosen to lie in $E_7(q)_{ad} \setminus E_7(q)$. \square

Theorem 5.17. *The groups $E_7(q)_{ad}$, $q = p^m$, $p \neq 2$, possess G -realizations over abelian number fields $k(q) \leq \mathbb{Q}^{ab}$ for the class vector \mathbf{C} of Proposition 5.16.*

As immediate corollary we find Galois realizations for the simple groups (here C_p , C'_p denote classes of $E_7(q)'_{ad}$ fusing into C_p of $E_7(q)_{ad}$):

Corollary 5.18. *The groups $E_7(q) = E_7(q)'_{ad}$, $q = p^m$, $p \neq 2$, possess G -realizations over the same fields $k(q) \leq \mathbb{Q}^{ab}$ for the class vector $(C_p, C'_p, (C_T^\delta)^2)$ obtained by descent from the $E_7(q)_{ad}$ -realizations in Theorem 5.17.*

5.6 The Groups $E_8(q)$

Let $G := E_8(q)$, $q = p^m$ with $p \geq 3$ odd. There exists a rough classification of the conjugacy classes of G , namely the unipotent classes were found by Mizuno (1980) and the types of semisimple classes by Deriziotis (1983). The Green functions in good characteristic were calculated by Beynon and Spaltenstein (1984) under the assumption that q is large enough; this additional hypotheses was subsequently shown by Lusztig to be unnecessary.

Denote by C_2 the class of involutions of G with centralizer of Lie type D_8 and by C_p the class of unipotent elements with representative z_{189} in Mizuno (1980),

which corresponds to the class denoted $4A_1$ in Beynon and Spaltenstein (1984). Finally, the class C_T will contain generating elements of the cyclic torus of order $\phi_{30} = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$.

Proposition 5.19. *The class vector $\mathbf{C} = (C_2, C_p, C_T)$ of $E_8(q)$, $q = p^m$, $p \geq 3$, is rigid.*

Proof. An element $\sigma_3 \in C_T$ generates a cyclic Hall-subgroup T of $G = E_8(q)$, as follows from the order formula for G . In particular, all elements $\tau \in T \setminus 1$ are regular. By Theorem 5.1(b) this means that among the Deligne–Lusztig characters $R_{T'}(\theta)$, where T' denotes a maximal torus of G , only those where T' is G -conjugate to T or where $\theta = 1$, do not vanish on the elements in C_T . The first ones, with $\theta \neq 1$, are the irreducible Deligne–Lusztig characters for T , the second have as constituents the unipotent characters of G . By Theorem 5.1(a) this implies that we have only to consider the $R_T(\theta)$ and the unipotent characters for a possible contribution to the structure constant $n(\mathbf{C})$.

Now T is self-centralizing and of odd order, so cannot be contained in the centralizer of an involution from class C_2 . Thus the irreducible $R_T(\theta)$ vanish on C_2 . There remain the 166 unipotent characters χ . Their values on the class C_T of regular elements can easily be computed by formula (5.3) and the known character table of the Weyl group $W(E_8)$. It turns out that precisely thirty unipotent characters do not vanish on C_T . So at most these may contribute to $n(\mathbf{C})$. (These thirty characters are the non-exceptional characters in the principal l -block of G for any prime $l > 31$ dividing ϕ_{30} .)

Next comes the more cumbersome step of calculating $\chi(C_2)$ for the remaining thirty unipotent χ , which by Corollary 5.3 requires also knowledge of $W(D_8)$ and its fusion into $W(E_8)$. We omit the details of the straightforward computations. In the end, only 14 of the remaining unipotent characters do not vanish on C_2 . The values of these on the class C_p now follow from the Green functions given in Beynon and Spaltenstein (1984), using the fact that the unipotent class C_p is uniform. These values consist of rather unpleasant polynomials of degree up to 25 in q , which are hence omitted here (see Malle (1986) and Lübeck and Malle (1998) for the tables).

With the centralizer orders

$$|\mathcal{C}_G(\sigma_1)| = q^{56}(q^2 - 1)(q^4 - 1)(q^6 - 1)(q^8 - 1)^2(q^{10} - 1)(q^{12} - 1)(q^{14} - 1),$$

$$|\mathcal{C}_G(\sigma_2)| = q^{100}(q^2 - 1)(q^4 - 1)(q^6 - 1)(q^8 - 1)$$

and $|\mathcal{C}_G(\sigma_3)| = \phi_{30}$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$ one then obtains $n(\mathbf{C}) = 1$.

For the generation, we may employ Weigel (1992), Fig. 11, since H contains the maximal torus T of order ϕ_{30} generated by σ_3 . As the σ_i have pairwise prime orders, H is perfect by Proposition 4.3. It thus cannot lie in $\mathcal{N}_G(T) = \phi_{30}.30$, and hence coincides with G . \square

Theorem 5.20. *The groups $E_8(q)$, $q = p^m$, $p \neq 2$, possess G -realizations over abelian number fields $k(q) \leq \mathbb{Q}^{\text{ab}}$ for the class vector \mathbf{C} of Proposition 5.19.*

Some G -realizations of $E_8(p)$ over \mathbb{Q} are contained in Paragraph 8.

6 Galois Realizations of Linear and Unitary Groups over \mathbb{Q}

When seeking G -realizations over \mathbb{Q} , in addition to rigidity one has to require rationality of the class vectors. This imposes strong restrictions on the element orders in the class triple, which then in turn complicate the proof of generation. In general the conditions obtained in that way do not allow to realize a whole series of groups of Lie type, not even all groups in a series defined over the prime field, but only those where the defining characteristic satisfies some additional number theoretic condition.

Before considering rational realizations, we extend the Galois realizations of Belyi for the linear and unitary groups over \mathbb{Q}^{ab} (Corollary 1.5 and Theorem 3.2) to also include the graph automorphism of order 2, at least if the characteristic of the ground field is odd. Under favorable circumstances this even allows to obtain GA-realizations over \mathbb{Q} .

6.1 Extension by the Graph Automorphism

Before we return to the linear and unitary groups over finite fields we first formulate a kind of converse of the translation theorems.

Proposition 6.1. *Let G be a finite group, $\mathbf{C} = (C_1, C_2, C_3)$ a rigid class vector of G and $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in \Sigma(\mathbf{C})$. Let $Z \leq \mathcal{L}(G)$ be a subgroup of the center of G and denote by \bar{C}_i the images of C_i in G/Z . Then $\bar{\mathbf{C}} := (\bar{C}_1, \bar{C}_2, \bar{C}_3)$ is a rigid class vector of G/Z if for all $\zeta \in Z \cap G'$ there exist $\xi_1, \xi_2, \xi_3 \in Z$ such that $\xi_1 \xi_2 \xi_3 = \zeta^{-1}$ and $\xi_i \sigma_i$ is conjugate to σ_i for $i = 1, 2, 3$.*

Proof. Let $\sigma' = (\sigma'_1, \sigma'_2, \sigma'_3) \in \Sigma(\bar{\mathbf{C}})$. Thus there exist $\xi'_i \in Z$ such that $\xi'_i \sigma'_i$ is conjugate to σ_i and moreover $\zeta := \prod_{i=1}^3 \xi'_i \sigma'_i \in Z$. But we also have $\zeta \in G'$ since $\xi'_i \sigma'_i$ is conjugate to σ_i . By assumption there exist $\xi_i \in Z$ such that

$$\sigma_i \sim \xi_i \sigma_i = \xi_i \xi'_i \sigma'_i$$

and $\xi_1 \xi_2 \xi_3 = \zeta^{-1}$. Thus $(\xi_1 \xi'_1 \sigma'_1, \xi_2 \xi'_2 \sigma'_2, \xi_3 \xi'_3 \sigma'_3) \in \Sigma(\mathbf{C})$, hence it is conjugate to σ . This implies that σ' is conjugate to σ in G/Z . \square

Let G be a finite group, $\mathbf{C} = (C_1, C_2, C_3)$ a rigid class vector of G and γ an automorphism of G of order 2 such that $C_1^\gamma = C_1$, while C_2 and C_3 are interchanged by γ . Let $(\sigma_1, \sigma_2, \sigma_3) \in \Sigma(\mathbf{C})$. Since σ_2^γ and σ_3 are conjugate in G there exists an element $\tau_1 \in G$ with $\sigma_2^{\gamma\tau_1} = \sigma_3$. Clearly a permutation of classes does not change rigidity, so (C_1, C_3, C_2) is also rigid. But this implies that the two triples $(\sigma_1^{\gamma\tau_1}, \sigma_3, \sigma_2^{\gamma\tau_1})$ and $(\sigma_2^{-1}\sigma_1\sigma_2, \sigma_3, \sigma_2)$ are conjugate by an element $\tau_2 \in G$:

$$(\sigma_1, \sigma_2, \sigma_3)^{\gamma\tau_1\tau_2} = (\sigma_1^{\gamma\tau_1}, \sigma_3, \sigma_2^{\gamma\tau_1})^{\tau_2} = (\sigma_2^{-1}\sigma_1\sigma_2, \sigma_3, \sigma_2). \quad (6.1)$$

The element $\rho := \gamma\tau_1\tau_2$ hence satisfies $\sigma_i^{\rho^2} = \sigma_i$ for $i = 2, 3$. Since $\rho^2 \in G$ centralizes the generators σ_1, σ_2, ρ of the semidirect product $\tilde{G} := G.\langle\gamma\rangle$, it lies in $\mathcal{L}(\tilde{G}) \cap G$. The class vector $\tilde{\mathbf{C}} := ([\rho], [\rho\sigma_2^{-1}], [\sigma_2])$ of \tilde{G} thus has the following properties:

$$\langle \rho, \sigma_2 \rangle = \tilde{G}, \quad \rho^2 = \zeta \in \mathcal{L}(\tilde{G}) \cap G, \quad (\rho\sigma_2^{-1})^2 = \zeta\sigma_3^{-1}\sigma_2^{-1} = \zeta\sigma_1. \quad (6.2)$$

In one particular case it is easy to see that $\tilde{\mathbf{C}}$ is rigid:

Corollary 6.2. *Let G be a finite group, $\mathbf{C} = (C_1, C_2, C_3)$ a rigid class vector of G , γ an automorphism of G of order 2 such that $C_1^\gamma = C_1$, $C_2^\gamma = C_3$, and $\tilde{G} = G.\langle\gamma\rangle$ the semidirect product. If $\mathcal{L}(G) = 1$ then there exists a rigid class vector $\tilde{\mathbf{C}} = (\tilde{C}_1, \tilde{C}_2, \tilde{C}_3)$ of \tilde{G} such that \mathbf{C} is the translation image of $\tilde{\mathbf{C}}$ under the passage from \tilde{G} to G , i.e.,*

$$\tilde{C}_1^2 = 1, \quad \tilde{C}_2^2 = C_1, \quad \tilde{C}_3 = C_2 \cup C_3.$$

Proof. Since $\mathcal{L}(G) = 1$ it follows from (6.2) that the class vector $\tilde{\mathbf{C}}$ defined above has \mathbf{C} as its translation image under the passage from \tilde{G} to G . In the notation introduced before let $(\rho', \rho'\sigma_2^{-1}, \sigma_2) \in \Sigma(\tilde{\mathbf{C}})$. Since \mathbf{C} is rigid we may assume after conjugation that $(\rho'\sigma_2^{-1})^2 = \sigma_1$. But then $\rho'\rho'^{-1}$ centralizes the generators of G , so $\rho' = \rho$. Hence $\tilde{\mathbf{C}}$ is rigid. \square

We now specialize to the situation we are most interested in. Let $2 \neq p \in \mathbb{P}$ be an odd prime and q a power of p . Let

$$\gamma : \mathrm{GL}_n(q) \rightarrow \mathrm{GL}_n(q), \quad A \mapsto (A^t)^{-1}, \quad (6.3)$$

be the graph automorphism of $\mathrm{GL}_n(q)$, which sends a matrix to the inverse of its transpose. For $n > 2$ the corresponding semidirect product $\mathrm{GL}_n(q).\langle\gamma\rangle$ is a non-trivial extension of $\mathrm{GL}_n(q)$. If $q = \tilde{q}^2$ is a square then γ normalizes (a suitable conjugate of) the subgroup $\mathrm{GU}_n(\tilde{q}) < \mathrm{GL}_n(q)$, hence gives rise to a semidirect product $\mathrm{GU}_n(\tilde{q}).\langle\gamma\rangle$.

Lemma 6.3. *Let q be odd and $n \geq 4$ be even. Then all involutions in the coset $\gamma \mathrm{GL}_n(\bar{\mathbb{F}}_q)$ are conjugate to $\gamma \cdot \text{antidiag}(1, \dots, 1)$. For the finite groups, $\gamma \mathrm{GL}_n(q)$ and $\gamma \mathrm{GU}_n(q)$ both contain two classes of involutions, with centralizers $\mathrm{GO}_n^+(q)$ and $\mathrm{GO}_n^-(q)$.*

Proof. If $(\gamma\sigma)^2 = 1$ for $\sigma \in \mathrm{GL}_n(k)$ then $\sigma = \sigma^t$. Furthermore, $(\gamma\sigma)^\tau = \gamma\tau^t\sigma\tau$, so the classes of involutions in $\gamma \mathrm{GL}_n(k)$ are in bijection with the equivalence classes of non-degenerate symmetric forms on k^n . If $k = \bar{\mathbb{F}}_q$ there is just one such class, with representative $\gamma \cdot \text{antidiag}(1, \dots, 1)$ (see (3.5)). By definition the centralizer in $\mathrm{GL}_n(k)$ is the orthogonal group $\mathrm{GO}_n(k)$. Since the connected component of this centralizer has index 2, the class splits into two conjugacy classes in the finite groups $\mathrm{GL}_n(q).\langle\gamma\rangle$ or $\mathrm{GU}_n(q).\langle\gamma\rangle$. By (3.5) the centralizers in $\mathrm{GL}_n(q)$ of such involutions are orthogonal group $\mathrm{GO}_{2n}^\pm(q)$. \square

Proposition 6.4. Let $n \geq 3$, q odd, $G \leq \mathrm{GL}_n(q)$ be absolutely irreducible and $\mathbf{C} = (C_1, C_2, C_3)$ a rigid class vector of G . Assume that G is normalized by some $\gamma' \in \mathrm{GL}_n(q)$. γ and $C_1^{\gamma'} = C_1$, while C_2 and C_3 are interchanged by γ' .

(a) If either n is odd or $-C_1$ is a class of transvections, then there exists a rigid class vector $\tilde{\mathbf{C}} = (\tilde{C}_1, \tilde{C}_2, \tilde{C}_3)$ of the group extension $\tilde{G} = G.\langle\gamma'\rangle$ such that \mathbf{C} is the translation image of $\tilde{\mathbf{C}}$ under the passage from \tilde{G} to G , i.e.,

$$\tilde{C}_1^2 = 1, \quad \tilde{C}_2^2 = C_1, \quad \tilde{C}_3 = C_2 \cup C_3.$$

(b) Assume moreover that G contains $\mathrm{SL}_n(q)$ or $\mathrm{SU}_n(\tilde{q})$ with $\tilde{q}^2 = q$ and let $\bar{G} := \pm G/\{\pm 1\}$. If C_1 and $C_2 \cup C_3$ are rational in G , then the image $\tilde{\bar{G}}$ of $\tilde{\mathbf{C}}$ is a rationally rigid class vector of $\bar{G} = \bar{G}.\langle\gamma'\rangle$.

Proof. Let $\sigma \in \Sigma(\mathbf{C})$ and ρ the element constructed above. We first claim that $\rho^2 = 1$. Since G is absolutely irreducible and ρ^2 centralizes the generators σ_1, σ_2, ρ of \tilde{G} , it lies in the center $\{\pm 1\}$ of $\mathrm{GL}_n(q).\langle\gamma\rangle$. The squares of elements from the coset $\gamma \mathrm{GL}_n(q)$ have determinant 1, so for odd n we have $\rho^2 = 1$. If n is even and $\rho^2 = -1$ then $(\rho\sigma_2^{-1})^2 = -\sigma_3^{-1}\sigma_2^{-1} = -\sigma_1$, so the semisimple part of $\rho\sigma_2^{-1}$ is an outer involution centralizing the transvection $-\sigma_1$. By Lemma 6.3, the centralizer of an involution in $\gamma \mathrm{GL}_n(q)$ is an orthogonal group, which gives a contradiction since orthogonal groups in odd characteristic do not contain transvections (see Theorem 2.2). So $\rho^2 = 1$ in all cases, and by (6.2) the class vector $\tilde{\mathbf{C}} := ([\rho], [\rho\sigma_2^{-1}], [\sigma_2])$ of \tilde{G} has the original class vector \mathbf{C} as a translation image in G .

As in the proof of Corollary 6.2, if $(\rho', \rho'\sigma_2^{-1}, \sigma_2) \in \Sigma(\tilde{\mathbf{C}})$ with $(\rho'\sigma_2^{-1})^2 = \sigma_1$ then $\rho'\rho^{-1}$ centralizes G , so $\rho' = a\rho$ for some $a \in \mathcal{Z}(G)$. By assumption $\rho'\sigma_2^{-1} = a\rho\sigma_2^{-1}$ is conjugate to $\rho\sigma_2^{-1}$, so there exists a $\tau \in G$ with $(a\rho\sigma_2^{-1})^\tau = \rho\sigma_2^{-1}$. To show rigidity of $\tilde{\mathbf{C}}$ it suffices to show that $a = b^2$ for some $b \in \mathcal{Z}(G)$ since then $(\rho', \rho'\sigma_2^{-1}, \sigma_2) = (\rho, \rho\sigma_2^{-1}, \sigma_2)^{b^2}$. If n is odd then evaluation of the induced from G to \tilde{G} of the determinant on the previous equality yields that a is a square. For even n note that $(\rho\sigma_2^{-1})^2 = \sigma_1$ by (6.2), hence $\tau \in N := \mathcal{N}_G(\sigma_1)$. By the proof of Theorem 1.4 the center of G has a complement M in N , $N = \mathcal{Z}(G) \times M$, and it can be checked that M remains normal in $\mathcal{N}_{\tilde{G}}(\sigma_1)$. In the factor group $N/M \cong \mathcal{Z}(G)$ two elements are conjugate via the outer automorphism only if they differ by a square. This shows that $a = b^2$ for some $b \in \mathcal{Z}(G)$.

For (b) we note that the classes of the involution ρ and of σ_2 are rational in \tilde{G} by assumption. Furthermore, the image of $\rho\sigma_2^{-1}$ in \tilde{G} has order $2p$, with rational p -part, so it is rational as well. Finally, ρ is conjugate to $-\rho$ by Lemma 6.3 since both are outer involutions with the same centralizer in $\mathrm{GL}_n(q)$. By Proposition 6.1 this shows that $\tilde{\bar{G}}$ remains rigid in \tilde{G} . \square

In the next section we apply the preceding proposition to the case of general linear and unitary groups extended by the graph automorphism.

6.2 GA-Realizations over \mathbb{Q}^{ab}

In odd characteristic the following result extends Belyi's realization of linear and unitary groups as regular Galois groups over \mathbb{Q}^{ab} (Theorems 1.4 and 3.2) by including the outer graph automorphism.

Theorem 6.5. *Let $n \geq 3$, p be an odd prime and $q = p^m$.*

- (a) *The group $\text{PGL}_n(q).(\gamma)$ possesses a G-realization over \mathbb{Q}^{ab} . The fixed field of the simple group $\text{L}_n(q)$ is a rational function field.*
- (b) *The group $\text{PGU}_n(q).(\gamma)$ possesses a G-realization over \mathbb{Q}^{ab} . The fixed field of the simple group $\text{U}_n(q)$ is a rational function field.*

Proof. For (a) assume first that $q \neq 3$. Let $q' := q$ in case (a) respectively $q' := q^2$ in case (b), and

$$f(X) := (X - a)(X - 1)^{n-1} \quad \text{with } a \in \mathbb{F}_{q'}^\times \setminus \{\pm 1, 1-n\}, \quad a^3 \neq 1. \quad (6.4)$$

(Such an a exists since $q' \geq 5$.) By the choice of a the sets of roots of $f(X)$ and $f(-X)$ are disjoint, so by Theorem 2.6 there exists a Belyi triple $\sigma = (-\sigma_1, \sigma_2, -\sigma_3)$ in $\text{GL}_n(q')$ such that σ_2 and σ_3^{-1} both have characteristic polynomial $f(X)$. Moreover by Proposition 2.7 the group $G := \langle \sigma \rangle$ is primitive since f has trace different from 0. Since a suitable p -power of σ_2 is a homology of order larger than 3, G contains either $\text{SU}_n(\tilde{q})$ or $\text{SL}_n(\tilde{q})$ as a normal subgroup by Theorem 2.3.

In case (a) we now choose a to be a generator of the cyclic group \mathbb{F}_q^\times . Since $\text{GU}_n(\tilde{q})$ does not contain an element with minimal polynomial $f(X)$ for any $\tilde{q}|q^2$ we may conclude that $G = \text{GL}_n(q)$ in this case. In case (b) we choose a to be of multiplicative order $q + 1$ in $\mathbb{F}_{q^2}^\times$, so $a^q = a^{-1}$. Then the action of the Frobenius morphism (taking q -th powers) interchanges the classes of σ_2 and σ_3 , while it fixes the class of σ_1 . Since the same is true for γ , the group G is now centralized by a suitable conjugate of the product of the Frobenius map with γ . It thus cannot be a linear group which implies $G = \text{GU}_n(q)$.

If n is odd then $-\sigma_1$ is a reflection and we have $\mathcal{C}_G(\sigma_1) = \text{GL}_1(q) \times \text{GL}_{n-1}(q)$ (respectively $\text{GU}_1(q) \times \text{GU}_{n-1}(q)$ in case (b)) so the center $\mathcal{Z}(G)$ has a complement in the normalizer of $\langle \sigma_1 \rangle$. For n even $-\sigma_1$ is a transvection and the center of G has a complement in the normalizer of $\langle \sigma_1 \rangle$ by the proofs of Theorems 1.4 and 3.2. Thus the Basic Rigidity Theorem I.4.8 yields the existence of a G-realization of G over \mathbb{Q}^{ab} . Furthermore, by Proposition 6.4(a) there exists a rigid class vector $\tilde{\mathbf{C}}$ of $G.(\gamma)$ possessing \mathbf{C} as a translation image. Thus by Proposition 6.4(b) and Theorem I.4.8 there exists a G-realization of the group $G.(\gamma)/\{\pm 1\}$ with trivial center. Trivially this furnishes a G-realization of the factor group $\text{PGL}_n(q).(\gamma)$ (respectively $\text{PGU}_n(q).(\gamma)$ in case (b)) with respect to the canonical image of the class vector $\tilde{\mathbf{C}}$. Furthermore, the fixed field K of the simple group $\text{L}_n(q)$ (resp. $\text{U}_n(q)$) is rational, since the subextension corresponding to K is a dihedral extension ramified at three points with ramification indices $(2, 2, k)$, where $k = \gcd(q-1, n)$ (resp. $k = \gcd(q+1, n)$).

If $q = 3$ in case (a) we start with the polynomial

$$f(X) = (X - 1)^{n-2}(X^2 + X + 2)$$

instead, the roots of the quadratic factor being an 8-th root of unity and its third power. As before there exists a Belyi triple σ . The group $G := \langle \sigma \rangle$ now at least contains a transvection or a reflection, so we may apply Theorems 2.2 or 2.4. In even dimension, the symplectic group may be excluded by the following observation. If σ is a semisimple element in the conformal symplectic group CSp_n over an algebraic closure of \mathbb{F}_q then it has eigenvalues $\{t_1, \dots, t_m, ut_1^{-1}, \dots, ut_m^{-1}\}$ for some $t_i, u \neq 0$ (see Digne and Michel (1991), 15.2, for example). Thus the semisimple part of σ_2 cannot lie inside the normalizer of a symplectic group. The orthogonal groups in odd dimension may again be ruled out by the eigenvalue distribution of the element σ_2 . If G were a symmetric group, then σ_1 would have sign -1 , and σ_2, σ_3 would have to have the same sign. But this is impossible because of the product relation. The four 3 and 5-dimensional exceptional reflection groups do not possess elements of order 8, and in the 7-dimensional group $2.\mathrm{O}_7(2)$ all classes are rational. So G is none of the exceptional cases, and hence contains $\mathrm{SL}_n(3)$ as a normal subgroup. Then the rest of the proof goes through without change. \square

Since $\mathrm{Aut}(\mathrm{L}_n(p)) = \mathrm{PGL}_n(p).\langle \gamma \rangle$ and $\mathrm{Aut}(\mathrm{U}_n(p)) = \mathrm{PGU}_n(p).\langle \gamma \rangle$ for $n \geq 3$, we have the immediate consequence (extending Corollary 1.6):

Corollary 6.6. *Let p be an odd prime. Then the simple groups $\mathrm{L}_n(p)$ and $\mathrm{U}_n(p)$ possess GA-realizations over \mathbb{Q}^{ab} .*

6.3 GA-Realizations over \mathbb{Q}

We now consider cases where the above approach leads to realizations over the field of rational numbers \mathbb{Q} . The element σ_2 used for the Galois realizations in the previous section is semirational only if a has multiplicative order 4 or 6. This leads to:

Theorem 6.7. *Let $n > 2$ be even and $p > 2$.*

(a) *For $\gcd(n, p - 1) = 2$ and either $n \equiv 2 \pmod{4}$ and $p \equiv 5 \pmod{8}$, or $n \equiv 0 \pmod{4}$ and $p \equiv 7 \pmod{12}$, the group $\mathrm{L}_n(p)$ possesses a GA-realization over \mathbb{Q} .*

(b) *For $\gcd(n, p - 1) = 2$ and either $n \equiv 2 \pmod{4}$ and $p \equiv 3 \pmod{8}$, or $n \equiv 0 \pmod{4}$ and $p \equiv 5 \pmod{12}$, the group $\mathrm{U}_n(p)$ possesses a GA-realization over \mathbb{Q} .*

Proof. We first consider case (a). If $p \equiv 1 \pmod{4}$ there exists an element $a \in \mathbb{F}_p$ with $a^2 = -1$. If $p \equiv 1 \pmod{6}$ there exists an element $a \in \mathbb{F}_p$ with $a^3 = -1, a \neq -1$. These are different from ± 1 and $1 - n$. Thus the polynomial $f(X) = (X - a) \cdot (X - 1)^{n-1}$ is as in (6.4) and there exists a Belyi triple $(-\sigma_1, \sigma_2, -\sigma_3)$, where σ_1 is

a transvection and σ_2 is semirational. The arguments in the proof of Theorem 6.5 now give a semirationally rigid class vector \mathbf{C} in $\mathrm{GL}_n(p)$ for a group G containing $\mathrm{SL}_n(p)$. Since under the given congruences a is a non-square in \mathbb{F}_p , the quotient \bar{G} of G by its center is an extension of $\mathrm{L}_n(p)$ of degree 2. Under the assumption $\gcd(n, p-1) = 2$ this coincides with all of $\mathrm{PGL}_n(p)$. By Proposition 6.4 the class vector \mathbf{C} is the translation image of a rigid class vector of $\mathrm{GL}_n(p).\langle\gamma\rangle$, such that after factoring out $\{\pm 1\}$ we obtain a rationally rigid class vector. Taking the quotient modulo the center we obtain a G -realization $N/\mathbb{Q}(t)$ of $\mathrm{PGL}_n(p).\langle\gamma\rangle = \mathrm{Aut}(\mathrm{L}_n(p))$ over \mathbb{Q} . Since the quotient by the simple group $\mathrm{L}_n(p)$ is a four group, we may now apply Lemma I.9.9 to conclude that the fixed field L of the simple group is a rational function field. Indeed, the order of the centralizer of σ_3 in $\mathrm{PGL}_n(p)$ equals the one in $\mathrm{PGL}_n(p).\langle\gamma\rangle$, so the full normalizer of the inertia group of \mathfrak{P}_3 lies already in $\mathrm{PGL}_n(p)$.

In case (b) for $p \equiv 3 \pmod{4}$ there exists $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ with $a^2 = -1$, and for $p \equiv -1 \pmod{6}$ there exists an $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ with $a^3 = -1, a \neq -1$. We can now argue as before, using that a is a non-square precisely under the conditions stated in the Theorem. \square

Remark. The assumption $n \equiv 0 \pmod{4}$ when $p \equiv 7 \pmod{12}$ is necessary in the previous construction, since otherwise the fixed field of the simple group can be shown not to be rational over \mathbb{Q} . In particular the stronger assertion in Malle (1996), Satz 4.8, is not correct.

In odd dimension we obtain a similar result:

Theorem 6.8. *Let n be odd.*

- (a) *For $\gcd(n, p-1) = 1$, $p > 3$ and $p \not\equiv -1 \pmod{12}$ the group $\mathrm{L}_n(p)$ possesses a GA-realization over \mathbb{Q} .*
- (b) *For $\gcd(n, p+1) = 1$, $p > 2$ and $p \not\equiv 1 \pmod{12}$ the group $\mathrm{U}_n(p)$ possesses a GA-realization over \mathbb{Q} .*

Proof. In case (a), if $p \equiv 1 \pmod{4}$ or $p \equiv 1 \pmod{6}$ there exists an element $a \in \mathbb{F}_p$ with $a^2 = -1$ or with $a^3 = -1, a \neq -1$. Again, $f(X) = (X-1)^{n-1}(X-a)$ is as in (6.4) and there exists a semirational Belyi triple $(-\sigma_1, \sigma_2, -\sigma_3)$. The proof now proceeds as the one for Theorem 6.7, except that the condition on a being a non-square is not needed here because $\gcd(n, p-1) = 1$ implies $\mathrm{Aut}(\mathrm{L}_n(p)) = \mathrm{L}_n(p).\langle\gamma\rangle$. Similarly for case (b) there exist suitable elements $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ under the given congruences. \square

Remark. For more general results on realizations of linear and unitary groups covering further congruence classes see Reiter (1999). Linear groups have also been studied by Folkers (1995) starting from rather different class vectors. See also Chapter III.10 for further G -realizations of linear and unitary groups not necessarily over the prime field.

7 Galois Realizations of Symplectic and Orthogonal Groups over \mathbb{Q}

For symplectic and orthogonal groups over the prime field we can apply the techniques of Paragraph 2 to construct Galois realizations over \mathbb{Q} . The results are essentially due to Reiter (1999), in characteristic 2 also to Völklein (1998). In the last section, G-realizations over \mathbb{Q}^{ab} for the groups $O_8^+(q)$ with the exceptional triality graph automorphism are proved, using Lusztig's character theory and the classification of the finite simple groups. For infinitely many primes p this leads to GA-realizations over \mathbb{Q} for the groups $O_8^+(p)$ over the prime field.

7.1 GA-Realizations of Symplectic Groups over \mathbb{Q}

In this section we find Galois realizations over \mathbb{Q} for infinite series of symplectic groups. But first we record a result on rationality of conjugacy classes.

Proposition 7.1. (a) A semisimple element in $\mathrm{SO}_{2n+1}(q)$, $\mathrm{CO}_{2n}^\pm(q)$ or $\mathrm{CSp}_{2n}(q)$ is rational if and only if it is rational considered as element of the corresponding general linear group.

(b) Let σ be an element of $G \in \{\mathrm{SO}_{2n+1}(q), \mathrm{CO}_{2n}^\pm(q), \mathrm{CSp}_{2n}(q)\}$ whose minimal polynomial coincides with its characteristic polynomial and which is rational in the corresponding general linear group. Then σ is rational in G .

A proof can be found in Reiter (1999), Bem. 3.10 and Folg. 3.4. The first part is a consequence of the Theorem of Lang-Steinberg. For the second part it suffices by the first to show that the unipotent part σ_u of σ is rational inside the centralizer of the semisimple part σ_s . This is true since the centralizer of σ_s is a group of classical type, in which σ_u is a regular unipotent element. But the regular unipotent elements in groups of type $\mathrm{SO}_{2n+1}(q)$, $\mathrm{CO}_{2n}^\pm(q)$, $\mathrm{CSp}_{2n}(q)$ are rational.

Theorem 7.2. Let $n \geq 2$. For odd primes $p \not\equiv \pm 1 \pmod{24}$, $p \nmid n$, the symplectic groups $\mathrm{S}_{2n}(p)$ possess GA-realizations over \mathbb{Q} .

Proof. We define

$$f(X) = \begin{cases} (X - a_8)^n (X - a_8^3)^n & \text{if } p \equiv 3 \pmod{8}, \\ (X - 1)^n (X - a_4)^n & \text{if } p \equiv 5 \pmod{8}, \\ (X - 1)^n (X - a_6)^n & \text{if } p \equiv 7 \pmod{12}, \end{cases}$$

where a_i denotes a primitive i -th root of unity in \mathbb{F}_{p^2} . Note that by the chosen congruences we have $f(X) \in \mathbb{F}_p[X]$. Then by Theorem 2.6 there exists a Belyi triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ such that $-\sigma_1$ is a transvection and σ_2, σ_3^{-1} have $f(X)$ as their characteristic polynomial. The group $G := \langle \sigma \rangle$ acts primitively by Proposition 2.7, hence by Proposition 2.1 and Theorem 2.2 we have $\mathrm{Sp}_{2n}(p) \leq G$ or

$\mathrm{SL}_{2n}(p) \trianglelefteq G$. By the criterion of Belyi we obtain $n(\mathbf{C}) = 1$ for the class vector $\mathbf{C} = ([\sigma_1], [\sigma_2], [\sigma_3])$. Now the roots of f are of the form (2.8) for

$$c := \begin{cases} -1 & \text{if } p \equiv 3 \pmod{8}, \\ a_4 & \text{if } p \equiv 5 \pmod{8}, \\ a_6 & \text{if } p \equiv 7 \pmod{12}, \end{cases}$$

so $G \leq \mathrm{CSp}_{2n}(p)$. Furthermore, σ_2 is conjugate to $c\sigma_2^{-1}$ in $\mathrm{GL}_{2n}(p)$. Thus $[\sigma_2]$ is not rational, hence semirational in $\mathrm{CSp}_{2n}(p)$ by Proposition 7.1. Again by the choice of a it follows that $G\mathcal{L}(\mathrm{GL}_{2n}(p)) = \mathrm{CSp}_{2n}(p)$. By the criterion of Belyi this implies $l(\mathbf{C}) = 1$. The normalizer condition is verified as in the proof of Theorem 3.4 and an application of Theorem I.4.8 yields the Galois realization. The factor group of G by $\mathrm{Sp}_{2n}(p)$ is cyclic, so the fixed field of $\mathrm{Sp}_{2n}(p)$ is a rational function field. Taking the quotient by the center gives the assertion.

For primes $p \equiv 5 \pmod{12}$ we choose

$$f(X) := (X - a_{6(p-1)})^n (X - a_{6(p-1)}^p)^n, \quad g(X) := (X^2 - a_{p-1})^n,$$

where again a_i denotes a primitive i -th root of unity in \mathbb{F}_{p^2} . As before the group G generated by a Belyi triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ corresponding to f, g contains the symplectic group and is contained in $\mathrm{CSp}_{2n}(p)$, since the roots of f are of the form (2.8) for $c := a_{6(p-1)}^{5p-7}$. Since σ_3 is conjugate to $-\sigma_3$, the image $\bar{\sigma}$ of σ in $\mathrm{CSp}_{2n}(p)/\mathcal{L}(\mathrm{CSp}_{2n}(p)) = \mathrm{PCSp}_{2n}(p)$ is still rigid by Proposition 6.1. By the choice of σ_2 we have $\bar{G} := \langle \bar{\sigma} \rangle = \mathrm{PCSp}_{2n}(p)$. The images of σ_2, σ_3 in \bar{G} are semirational by Proposition 7.1, so we may argue as above to obtain a GA-realization of $S_{2n}(p)$ over \mathbb{Q} . \square

To conclude this topic we prove a related result in characteristic 2.

Theorem 7.3. *The symplectic groups $S_{2n}(2)$ possess GA-realizations over \mathbb{Q} .*

Proof. For $n = 2$ we have $S_4(2) \cong S_6$ which was treated in Corollary I.9.8. For $n \geq 3$ we choose

$$f(X) := (X^2 + X + 1)^n, \quad g(X) := \phi_5(X)^{(n-3)/2} \phi_7(X),$$

if n is odd, respectively

$$f(X) := (X^2 + X + 1)^{n-3} \phi_9(X), \quad g(X) := \phi_5(X)^{n/2},$$

if n is even, with the cyclotomic polynomials ϕ_5, ϕ_7 and ϕ_9 . Then f, g are coprime of degree $2n$ with non-vanishing constant coefficient. By Theorem 2.6 there exists a corresponding Belyi triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ where σ_1 is a transvection. The group $G := \langle \sigma \rangle \leq \mathrm{GL}_{2n}(2)$ is contained in $\mathrm{Sp}_{2n}(2)$ by Theorem 2.10(b). Furthermore, G is primitive by Proposition 2.7 since σ_2 has trace different from 0. The normal subgroup H of G generated by the conjugates of σ_1 is thus one of the irreducible groups

in Theorem 2.2. In particular H is primitive. The orthogonal groups can be ruled out by Theorem 2.10(c). The minimal polynomials show that H is not a symmetric group. Finally, the order of $S_6(2)$ is not divisible by the order of $3_1.U_4(3).2_2$.

The elements σ_i were chosen such that any primitive power of σ_i has the same eigenvalues as σ_i . Thus σ is rationally rigid by Proposition 7.1. Since for $n \geq 3$ the group $S_{2n}(2)$ coincides with its automorphism group we obtain GA-realizations over \mathbb{Q} . \square

Remark. For further GA-realizations of symplectic groups over \mathbb{Q} see Reiter (1999) and Chapter III.10.

7.2 GA-Realizations of Odd-Dimensional Orthogonal Groups

In odd dimension we obtain Galois realizations of orthogonal groups. These generalize the GA-realization for the class vector $(2B, 4A, pA)$ for $(\frac{2}{p}) = -1$, $(2B, 6A, pA)$ for $(\frac{3}{p}) = -1$ of $L_2(p) \cong O_3(p)$ in Corollary I.8.10 to arbitrary dimensions.

Theorem 7.4. *Let $n \geq 1$. For odd primes $p \not\equiv \pm 1 \pmod{24}$ the odd-dimensional orthogonal groups $O_{2n+1}(p)$ possess GA-realizations over \mathbb{Q} .*

Proof. With a primitive 4-th or 6-th root of unity a in \mathbb{F}_{p^2} we define

$$f(X) := (X-1)^{2n-1}(X-a)(X-a^{-1}), \quad g(X) := (X-1)^{2n+1}.$$

By Theorem 2.6 there exists a Belyi triple $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ such that σ_1 is a reflection and $\sigma_2, -\sigma_3$ have minimal polynomials $f(X), g(X)$. By Theorem 2.10(a) we have $G := \langle \sigma \rangle \leq GO_{2n+1}(p)$. If $2n+1 \not\equiv 0 \pmod{p}$ then $\text{tr}(\sigma_3) \neq 0$ so G is primitive since $p|\sigma_3|/(2n+1)(p-1)$. On the other hand if $p|(2n+1)$ then $\text{tr}(\sigma_2) \neq 0$ so by Proposition 2.7 either G is primitive or it is contained in the monomial subgroup $G(p-1, 1, 2n+1)$. But the latter case is ruled out by the form of $f(X)$. Thus G is primitive and the normal subgroup H of G generated by the class of the reflection σ_1 acts irreducibly. By Proposition 2.1 it even acts primitively whence H is a primitive reflection group contained in $GO_{2n+1}(q)$. The symmetric groups are ruled out by using that $g(X)$ is not the characteristic polynomial of a permutation matrix. In dimension $2n+1 = 3$ the orthogonal group $SO_{2n+1}(p)$ is isomorphic to $\text{PGL}_2(p)$ for which the assertion was shown in Corollary I.8.10. For $2n+1 \geq 5$ the element σ_2 has order $4p$, resp. $6p$, and this rules out the exceptional cases in Theorem 2.4. Hence G must contain the orthogonal group $O_{2n+1}(p)$ as a normal subgroup. By the chosen congruences the semisimple part of σ_2 does not lie in the commutator group of $SO_{2n+1}(p)$, thus we have $G = SO_{2n+1}(p)$.

The element $-\sigma_3$ is regular unipotent and the unipotent part of σ_2 is a regular unipotent element of $SO_{2n-1}(p)$, thus both classes are rational by Carter (1985), Prop. 5.1.7. So $C := ([-\sigma_1], [\sigma_2], [-\sigma_3])$ is a rational class vector, which is rigid by the criterion of Belyi. Since the center of G is trivial, Theorem I.4.8 yields a

Galois realization of $\mathrm{SO}_{2n+1}(p)$ over \mathbb{Q} , which is the full automorphism group of the simple subgroup $\mathrm{O}_{2n+1}(p)$ of index 2. \square

We even obtain GA-realizations over \mathbb{Q} for groups $\mathrm{O}_{2n+1}(p^2)$, generalizing a result of Feit (1984) for $\mathrm{L}_2(p^2) \cong \mathrm{O}_3(p^2)$:

Theorem 7.5. *Let $n \geq 1$.*

(a) *For odd primes p the odd-dimensional orthogonal groups $\mathrm{O}_{2n+1}(p^2)$ possess GA-realizations over \mathbb{Q}^{ab} .*

(b) *For odd primes $p \equiv \pm 2 \pmod{5}$ the odd-dimensional orthogonal groups $\mathrm{O}_{2n+1}(p^2)$ possess GA-realizations over \mathbb{Q} .*

Proof. For (a) let a be a generating element of $\mathbb{F}_{p^4}^\times$, for (b) let $a \in \mathbb{F}_{p^4}^\times$ be of multiplicative order 10. Let

$$f(X) := (X-1)^{2n-1}(X-a)(X-a^{-1}), \quad g(X) := (X-1)^{2n-1}(X-a^p)(X-a^{-p}),$$

so that g is the image of f under the generating automorphism of $\mathbb{F}_{p^2}/\mathbb{F}_p$. Let $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ be a Belyi triple corresponding to this choice of characteristic polynomials according to Theorem 2.6. By Theorem 2.10(a) we have $G := \langle -\sigma_1, \sigma_2 \rangle \leq \mathrm{GO}_{2n+1}(p^2)$. Also, G is not contained in $\mathrm{GL}_{2n+1}(p)$ since f, g are not rational over \mathbb{F}_p by the choice of a . As in the proof of Theorem 7.4 it can then be checked that $G = \mathrm{SO}_{2n+1}(p^2)$.

Now let $F : \mathrm{GL}_{2n+1}(p^2) \rightarrow \mathrm{GL}_{2n+1}(p^2)$ be the Frobenius morphism sending each matrix entry to its p -th power. Replacing G by a suitable conjugate we may assume that it is normalized by F . Then F fixes the class of σ_1 and exchanges the classes of σ_2 and σ_3 . Thus we may apply Corollary 6.2 with the automorphism γ of order 2 induced by F to obtain a rigid class vector $\tilde{\mathbf{C}}$ of $\tilde{G} := \mathrm{SO}_{2n+1}(p^2). \langle \gamma \rangle \cong \mathrm{Aut}(\mathrm{O}_{2n+1}(p^2))$. Since σ_i , $i = 2, 3$, in (b) are semirational, $\tilde{\mathbf{C}}$ is rationally rigid. We next claim that the coset $G\gamma$ contains a single class of involutions, the class of γ . Indeed, assume $(\sigma\gamma)^2 = 1 = \sigma F(\sigma)$. Then by the Theorem 1.1 of Lang-Steinberg there exists $\tau \in \mathrm{SO}_{2n+1}(\bar{\mathbb{F}}_q)$ with $\tau^{-1}F(\tau) = \sigma$, which even lies in G because of

$$F^2(\tau) = F(\tau\sigma) = \tau\sigma F(\sigma) = \tau.$$

But then $\sigma\gamma = \tau^{-1}F(\tau)\gamma = \tau^{-1}\gamma\tau$ is conjugate to γ . Thus the first class of $\tilde{\mathbf{C}}$ is the class of γ . Since $\mathcal{N}_G(\gamma) = \mathcal{C}_G(\gamma) = \mathrm{SO}_{2n+1}(p)$ is contained in $G' = \mathrm{O}_{2n+1}(p^2)$ by definition of the spinor norm (3.3) it follows by Lemma I.9.9 that the G -realization of \tilde{G} is a GA-realization of $\mathrm{O}_{2n+1}(p^2)$. \square

Remark. For other results on GA-realizations of odd-dimensional orthogonal groups see Malle (1996), Satz 6.9, Reiter (1999) and Chapter III.10.

7.3 Even-Dimensional Split Orthogonal Groups

The outer automorphism groups of the split even-dimensional orthogonal groups always have order divisible by 4, so the descent from realizations of the automorphism group to the simple group is more difficult even over the prime field. We first look at the case where $|\text{Out}(\text{O}_{2n}^+(p))| = 4$, i.e., where n is odd and $p \equiv 3 \pmod{4}$. Let $G := \text{PCO}_{2n}^+(p)$ denote the projective conformal split orthogonal group, $G^\circ := \text{PCO}_{2n}^{+\circ}(p)$ the finite group associated to the connected component of the identity in the projective conformal orthogonal group, which is normal of index 2 in G , and $G' := \text{O}_{2n}^+(p)$ the commutator subgroup of G° . Since n is odd, we have $G/G' \cong 2^2$ and G' is simple for all $n \geq 3$.

Theorem 7.6. *Let $n \geq 3$ be odd and p a prime with $p \equiv 3 \pmod{8}$ or $p \equiv 7 \pmod{12}$, $p \nmid n$. Then there exist regular Galois extensions of $\mathbb{Q}(t)$ with groups $\text{PCO}_{2n}^+(p)$, $\text{PSO}_{2n}^+(p)$ and $\text{O}_{2n}^+(p)$. In particular, $\text{O}_{2n}^+(p)$ then possesses a GA-realization over \mathbb{Q} .*

Proof. If $p \equiv 3 \pmod{8}$ then let

$$f(X) := (X^2 - 1)(X - a)^{n-1}(X - a^p)^{n-1}, \quad g(X) := (X^2 + 1)^n, \quad (7.1)$$

with $a \in \mathbb{F}_{p^2}^\times$ of multiplicative order 8, while for $p \equiv 7 \pmod{12}$ let

$$f(X) := (X - 1)^n(X - b)^n, \quad g(X) := (X^2 - b)^n, \quad (7.2)$$

with $b \in \mathbb{F}_p^\times$ of multiplicative order 6. By Theorem 2.10(d) the group $G := \langle \sigma \rangle \leq \text{GL}_{2n}(p)$ generated by a Belyi triple belonging to f, g is a subgroup of $\text{CO}_{2n}^\pm(p)$. By Lemma 3.9 applied to the semisimple part of σ_2 we see that $G \leq \text{CO}_{2n}^+(p)$. The group G is primitive by Proposition 2.8. Now by Lemma 2.1 the subgroup H generated by the conjugates of the reflection σ_1 is among the groups in Theorem 2.4. The symmetric groups can be excluded since $g(X)$ has no eigenvalue 1. The exceptional groups in dimensions 5 and 7 can be excluded by the order of σ_2 . Hence we have that G contains $\Omega_{2n}^+(p)$. By the chosen congruences the element σ_2 generates $\text{CO}_{2n}^{+\circ}(p)$ over $\Omega_{2n}^+(p)$. Since G also contains the reflection σ_1 we obtain that $G = \text{CO}_{2n}^+(p)$. Now σ_3 is conjugate to $-\sigma_3$, so by Proposition 6.1 the image $\bar{\sigma}$ of σ in $\tilde{G} := G/\mathcal{L}(G) \cong \text{PCO}_{2n}^+(p)$ is still rigid. By their distribution of eigenvalues all three elements of $\bar{\sigma}$ are rational in \tilde{G} by Proposition 7.1. We may thus apply the rigidity criterion to obtain a G-realization $N/\mathbb{Q}(t)$ with group $\text{PCO}_{2n}^+(p)$. We may descend to the normal subgroup $\text{O}_{2n}^+(p)$ of index 4 by virtue of Lemma I.9.9 since the centralizer of the reflection σ_1 is contained in the subgroup of order 2 generated over $\text{O}_{2n}^+(p)$ by σ_1 . Thus the Galois realization is a GA-realization of the simple group $\text{O}_{2n}^+(p)$. \square

In the case where n is even or $p \equiv 1 \pmod{4}$ the outer automorphism group of $\text{O}_{2n}^+(p)$ is a dihedral group of order 8.

7.4 Even-Dimensional Non-split Orthogonal Groups

As for the split orthogonal groups we subdivide the cases according to the outer automorphism group of $O_{2n}^-(p)$. If n is even or $p \equiv 1 \pmod{4}$ then $\text{Out}(O_{2n}^-(p))$ is of order 4.

Theorem 7.7. *Let $n \geq 3$ be odd and $p \equiv 5 \pmod{12}$, or $n \geq 6$ be even and $p \equiv 3 \pmod{8}$, or $n \equiv 2 \pmod{4}$ and $p \equiv \pm 2 \pmod{5}$. Then there exist regular Galois extensions of $\mathbb{Q}(t)$ with groups $\text{PCO}_{2n}^-(p)$, $\text{PSO}_{2n}^-(p)$ and $O_{2n}^-(p)$. In particular, $O_{2n}^-(p)$ then possesses a GA-realization over \mathbb{Q} .*

Proof. For n odd, $p \equiv 5 \pmod{12}$ choose

$$f(X) := (X - a_{6(p-1)})^n (X - a_{6(p-1)}^p)^n, \quad g(X) = (X^2 - a_{p-1})^n,$$

for n even, $p \equiv 3 \pmod{8}$ let

$$f(X) := (X^2 - 1)(X - a_8)^{n-1} (X - a_8^3)^{n-1}, \quad g(X) := (X^2 + 1)^{n-1} (X - a_8^5)(X - a_8^7),$$

and for $n \equiv 2 \pmod{4}$, $p \equiv \pm 2 \pmod{5}$, let

$$f(X) = ((X - b)(X - b^p)(X - b^{p^2})(X - b^{p^3}))^{n/2}, \quad g(X) = (X^2 - a_{p-1})^n,$$

with $a_i, b \in \mathbb{F}_{p^4}^\times$ of multiplicative order $i, 10(p-1)$ respectively. We can now argue as in the proof of Theorem 7.6 to verify the assertions of the Theorem. \square

Remark. For $n = 2$ we have $\text{PCO}_4^-(p) \cong \text{PGL}_2(p^2)$, and the GA-realization of $\text{L}_2(p^2)$, $p \neq 2$, $p \equiv \pm 2 \pmod{5}$, obtained above is the one constructed by Feit (1984).

For $n = 3$ Theorem 7.7 yields Galois realizations for the unitary groups $\text{U}_4(p) \cong O_6^-(p)$, $p \equiv 5 \pmod{12}$.

Over the prime field with two elements we obtain complete results:

Theorem 7.8. *For $n \geq 5$ the orthogonal groups $O_{2n}^\pm(2)$ possess GA-realizations over \mathbb{Q} .*

Proof. For the orthogonal groups of plus-type let

$$f(X) := (X - 1)^{2n}, \quad g(X) := \begin{cases} (X^2 + X + 1)^{n-3} \phi_7(X) & \text{if } n \text{ is odd,} \\ (X^2 + X + 1)^n & \text{if } n \text{ is even,} \end{cases}$$

and $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ a Belyi triple corresponding to f, g . By Theorem 2.10(c) the group $G := \langle \sigma \rangle$ is contained in $\text{GO}_{2n}^\pm(2)$. An element with characteristic polynomial $g(X)$ can be found in $O_2^+(4)^{n/2} \leq O_{2n}^+(2)$ if n is even and in $O_2^+(4)^{(n-3)/2} \times O_6^+(2) \leq O_{2n}^+(2)$ if n is odd, thus $G \leq \text{GO}_{2n}^+(2)$ by Lemma 3.9. If n is odd then G is primitive since σ_3 has trace different from 0. If n is even then we are not in

the case (a) of Proposition 2.8. But case (b) cannot occur since $q = 2$. Thus G is primitive and the normal subgroup H of G generated by the transvections conjugate to σ_1 is one of the irreducible groups in Theorem 2.2. The symmetric groups cannot occur by the distribution of eigenvalues of σ_2, σ_3 . Since $n \geq 5$ this only leaves the orthogonal group.

The elements σ_2, σ_3 with minimal polynomials f, g are rational in $\mathrm{GO}_{2n}^-(2)$ by Häfner (1992), Bem. 2.3. Since σ_1 is a transvection of order 2, this shows that σ is a rationally rigid system of generators of $G = \mathrm{GO}_{2n}^+(2)$. The simple group G' has index 2 in G , so the Galois realization for G' is obtained by the standard descent argument. Finally, G is the automorphism group of G' , and the constructed Galois extension gives a GA-realization.

For the non-split group we choose

$$f(X) := (X - 1)^{2n}, \quad g(X) := \begin{cases} (X^2 + X + 1)^n & \text{if } n \text{ is odd,} \\ (X^2 + X + 1)^{n-2} \phi_5(X) & \text{if } n \text{ is even.} \end{cases}$$

Elements with characteristic polynomial $g(X)$ can be found in $\mathrm{O}_2^-(2)^n \leq \mathrm{O}_{2n}^-(2)$ if n is odd, and in $\mathrm{O}_2^-(2)^{n-2} \times \mathrm{O}_4^-(2) \leq \mathrm{O}_{2n}^-(2)$ if n is even, so the group G generated by a Belyi triple σ corresponding to f, g is contained in $\mathrm{GO}_{2n}^-(2)$ by Theorem 2.10(c) and Lemma 3.9. The argument now proceeds as in the split type. \square

Remark. For earlier results on GA-realizations of orthogonal groups over \mathbb{F}_2 see Thompson (1984b) and Häfner (1992), Satz 4.5 and 4.6. Further G-realizations of orthogonal groups will be presented in Chapter III.10.

7.5 The 8-Dimensional Split Orthogonal Groups

Let $G := \mathrm{PCO}_8^+(q). \langle \delta \rangle$, $q = p^m$, be the extension of the projective conformal 8-dimensional split orthogonal group over the finite field \mathbb{F}_q with the triality graph automorphism δ of order 3. Then we have

$$G / \mathrm{O}_8^+(q) \cong \begin{cases} S_4, & \text{if } p > 2, \\ S_3, & \text{if } p = 2. \end{cases}$$

Let C_2 be the class of the graph automorphism γ in G of order 2 with centralizer of type $\mathrm{GO}_7(q) = \mathrm{SO}_7(q) \times 2$. The graph automorphism δ of order 3 centralizes a subgroup of type $\mathrm{G}_2(q)$; let C_3^+ be the class of the product of δ with a (regular) element of order $q^2 + q + 1$ in its centralizer, and analogously C_3^- the class of the product with a (regular) element of order $q^2 - q + 1$. Finally denote by T a γ -invariant maximal torus of the connected component $G^\circ := \mathrm{PCO}_8^+(q)^\circ < G$ of order $(q^2 + 1)^2$. This has the structure of a direct product of two cyclic groups of order $q^2 + 1$. The graph automorphism γ interchanges the two factors, hence there exist elements of order $2(q^2 + 1)$ in the coset $T.\gamma$. Let C_4 be the class of such an

element. The centralizer of $\sigma \in C_4$ in G has order $2(q^2 + 1)q(q^2 - 1)$. Let \mathbf{C}^\pm denote the class vector $\mathbf{C}^\pm := (C_2, C_3^\pm, C_4)$ of G .

Proposition 7.9. *The class vectors \mathbf{C}^\pm of G satisfy $l(\mathbf{C}^\pm) = 1$.*

Proof. We evaluate the formula for the normalized structure constant of \mathbf{C}^\pm . This again requires results from the character theory of disconnected groups. No non-trivial semisimple element of G has centralizer order divisible by both ϕ_3 and ϕ_4 , respectively by ϕ_6 and ϕ_4 . By the character formula in Digne and Michel (1994) this implies that apart from extensions of unipotent characters of G° , no other characters take non-zero values on all three classes of \mathbf{C}^\pm . These extensions are the constituents of the generalized Deligne–Lusztig characters $R_{T,1}$. For disconnected groups of type $D_4:2$ and $D_4:3$, the decomposition of these $R_{T,1}$ into unipotent characters was determined in Malle (1993b), Thms. 6 and 7. From this the decomposition in the case $D_4:S_3$ can immediately be deduced. The values of the extensions of unipotent characters on the three classes of \mathbf{C}^\pm may now be calculated using the character formula in Digne and Michel (1994). One finds that only four unipotent characters give non-zero contributions to $n(\mathbf{C}^\pm)$. Their values are given in Table 7.1. From the definition of the classes C_2, C_3^\pm, C_4 we can read off the centralizer orders $|\mathcal{C}_G(\sigma_1)| = 2q^9(q^2 - 1)(q^4 - 1)(q^6 - 1)$, $|\mathcal{C}_G(\sigma_2)| = 3(q^2 \pm q + 1)$ and $|\mathcal{C}_G(\sigma_3)| = 2q(q^4 - 1)$ for elements $\sigma_i \in C_i^{(\pm)}$. With this information the assertion $n(\mathbf{C}^\pm) = 1$ follows.

Table 7.1 Character values for $O_8^+(q).S_4$

	1	C_2	C_3^+	C_3^-	C_4
$\phi_{4,-}$	1	1	1	1	1
$\phi_{12,1}$	$\frac{1}{2}q^3\phi_2^4\phi_6$	$\frac{1}{2}q^2\phi_2^3\phi_6$	1	.	ϕ_2
ϕ_{cusp}	$\frac{1}{2}q^3\phi_1^4\phi_3$	$-\frac{1}{2}q^2\phi_1^3\phi_3$.	-1	$-\phi_1$
$\phi_{1^4,-}$	q^{12}	q^9	1	1	q

For the proof of generation we make use of the explicit determination of the conjugacy classes of maximal subgroups of groups of type D_4 by Kleidman (1987). Let p_1 and p_2 be primitive prime divisors of $q^2 \pm q + 1$ and $q^2 + 1$ in the sense of Zsigmondy (Proposition 4.1). It can be checked that among the maximal subgroups of G° none of order divisible by both p_1 and p_2 extends to the extension by the group of graph automorphisms. Thus any triple $\sigma \in \bar{\Sigma}(\mathbf{C})$ generates G and the assertion follows from Corollary I.5.9. \square

Theorem 7.10. (a) *The groups $\text{PCO}_8^+(q).\langle \delta \rangle$, $q = p^m$, possess G -realizations over \mathbb{Q}^{ab} . The fixed field of the simple normal subgroup $O_8^+(q)$ is a rational function field.*

(b) *The groups $O_8^+(p)$ possess GA-realizations over \mathbb{Q}^{ab} .*

Proof. By Proposition 7.9 the class vectors \mathbf{C}^\pm of G are rigid. By the Basic Rigidity Theorem I.4.8 this implies the existence of a G -realization $N/\mathbb{Q}^{\text{ab}}(t)$ with group G . The fixed field K of the simple group $O_8^+(q)$ has Galois group S_4 over $\mathbb{Q}^{\text{ab}}(t)$ and class vector $(2, 3, 4)$, if p is odd, respectively group S_3 and class vector $(2, 3, 2)$ if p is even. Thus K has genus 0 and is rational over \mathbb{Q}^{ab} .

In the case $q = p$ we have $G = \text{Aut}(O_8^+(p))$ and assertion (b) follows from the above considerations. \square

Replacing the conjugacy classes C_3^\pm and C_4 by suitable rational classes, we obtain GA-realizations over \mathbb{Q} .

Theorem 7.11. *Let $p \in \mathbb{P}$ with $p \equiv \pm 2 \pmod{5}$ and $p \equiv \pm 2, \pm 3 \pmod{7}$. Then $O_8^+(p)$ possesses a GA-realization over \mathbb{Q} .*

Proof. This is an easy consequence of the proof of Proposition 7.9. If $p \not\equiv \pm 1 \pmod{5}$ then $5|(p^2 + 1)$, and 5 is a primitive prime divisor of $\phi_4(p)$. Furthermore, if $p \not\equiv \pm 1 \pmod{7}$, then 7 divides either $q^2 + q + 1$ or $q^2 - q + 1$ and is a primitive prime divisor of the corresponding cyclotomic polynomial $\phi_3(p)$ or $\phi_6(p)$. Thus if we replace the class C_4 by an analogously defined class C_{10} of elements of order 10, and C_3^\pm by the corresponding class C_{21} of elements of order 21, then by the character formula for unipotent characters extended to the disconnected case (Digne and Michel (1994)) the values in Table 7.1 remain correct for the new classes, hence the normalized structure constant $n(C_2, C_{21}, C_{10})$ also equals 1. In the proof of generation we had only used properties of primitive prime divisors, and since 5 and 7 are such primitive divisors, the generation property also remains true. So under the assumptions of the theorem, the class vector $\mathbf{C} := (C_2, C_{21}, C_{10})$ is also rigid.

Elements of order 5 in T are rational, so the same holds for elements in C_{10} . Further δ is a rational element, and elements of order 7 in the centralizer $G_2(p)$ of δ are rational. Finally this $G_2(p)$ is even contained in the centralizer of an S_3 containing δ , which proves the rationality of C_{21} and the assertion of the Theorem. \square

8 Galois Realizations of Exceptional Groups over \mathbb{Q}

In this paragraph we derive Galois realizations for certain exceptional groups over $\mathbb{Q}(t)$. The methods are rather similar to those employed in the previous paragraph. We first deal with the easier case of $G_2(p)$. In the second section we give a result on tori which are trivial intersection subgroups, which will allow to prove generation also in the cases of the larger groups treated later on.

8.1 GA-Realizations for the Groups $G_2(p)$

The first series of groups we shall consider are the groups of type G_2 defined over the prime field \mathbb{F}_p . It was shown independently by Thompson (unpublished) and by Feit and Fong (1984) that they occur as geometric Galois groups over \mathbb{Q} for all primes $p \geq 5$. While Thompson's proof utilizes generators and relations as in Belyi's treatment of the classical groups (see also Malle (1986), §3.3), Feit and Fong quote the character table and the classification of finite simple groups. We will follow this second approach, which is more akin to the methods for the other exceptional groups.

Let $G = G_2(p)$, $p \geq 5$, and let C_1 be the unique conjugacy class of involutions in G , C_2 the class of long root elements, and C_3 the class of regular unipotent elements. Corresponding elements are denoted by k_2 , u_2 , resp. u_6 in Chang and Ree (1974).

Theorem 8.1. *The groups $G_2(p)$, $p \geq 5$ prime, possess GA-realizations over \mathbb{Q} for the class vector $\mathbf{C} = (C_1, C_2, C_3)$.*

Proof. Since $G = G_2(p)$ has trivial outer automorphism group for primes $p \geq 5$, we are reduced to showing that \mathbf{C} is rationally rigid for G .

First from the character table of G in Chang and Ree (1974) one computes that $n(\mathbf{C}) = 1$ and verifies that all three classes are rational. Note that, contrary to the case of the class vector for $G_2(q)$ used in Proposition 4.6, most families of irreducible characters of G contribute to $n(\mathbf{C})$. This comes from the fact that the only semisimple class C_1 in \mathbf{C} has large centralizer. We omit the list of the relevant eleven character families. They can be found in Feit and Fong (1984).

Now let $H = \langle \sigma \rangle$ for a system $\sigma \in \bar{\Sigma}(\mathbf{C})$. Since the two rational p -elements σ_2 and σ_3 are not conjugate in G , the order of H is divisible at least by p^2 . By the list of maximal subgroups of G in Kleidman (1988b) we are left with the cases

$$[p^5]:\mathrm{GL}_2(p) \text{ (2 classes)}, (\mathrm{SL}_2(p) \circ \mathrm{SL}_2(p)) \cdot 2, \mathrm{SL}_3(p):2, \mathrm{SU}_3(p):2.$$

If H were contained in one of the parabolic subgroups $[p^5]:\mathrm{GL}_2(p)$, then, since it is generated by p -elements, it would already lie in $[p^5]:\mathrm{SL}_2(p)$. But now upon factorization by the normal p -subgroup $H \cap [p^5]$ the image of σ_1 can only be the unique and hence central involution of $\mathrm{SL}_2(p)$. Then by the product relation one of the other two elements orders would also have to be even, which is a contradiction.

The centralizer of an involution $(\mathrm{SL}_2(p) \circ \mathrm{SL}_2(p)) \cdot 2$ does not contain regular unipotent elements, since those have centralizer order p^2 . This rules out the second case, and also the centralizer of a 3-element, which is of type $\mathrm{SL}_3(p)$ when $p \equiv 1 \pmod{3}$, and of type $\mathrm{SU}_3(p)$ otherwise.

Since H is generated by its p -elements, we are left with $H \leq \mathrm{L}_3(p)$ or $H \leq \mathrm{U}_3(p)$, depending on the congruence of $p \pmod{3}$. Both the latter groups possess exactly two classes of p -elements and one involution class. Hence the fusion from either containing H into G is clear. But the corresponding structure constants vanish in both groups. This excludes the last possible maximal subgroups, and the proof is complete. \square

We already constructed a GA-realization for $\mathrm{G}_2(2)' = \mathrm{U}_3(3)$ over \mathbb{Q} in Theorem 6.8(b), so only the case $p = 3$ remains to be treated.

Theorem 8.2. *The group $\mathrm{G}_2(3)$ possesses a GA-realization over \mathbb{Q} for the class vector $(3A, 4C, 6E)$ of its automorphism group $\mathrm{Aut}(\mathrm{G}_2(3)) \cong \mathrm{G}_2(3):2$.*

Proof. From the character table in the Atlas one finds $n(3A, 4C, 6E) = 1$. Now let H be the group generated by a corresponding triple of elements. Since $6E^2 = 3C$, the group H intersects two distinct classes of 3-elements, hence its Sylow 3-subgroup has order at least nine. By the list of maximal subgroups of $\mathrm{Aut}(\mathrm{G}_2(3))$ in the Atlas, it thus lies in one of $[3^6]:D_8$, $\mathrm{L}_2(8):3 \times 2$ or $[2^5].(S_3 \times S_3)$. But H is no subgroup of the first candidate, as can be seen by factoring out the normal Sylow 3-subgroup. Also, the second type of maximal subgroup consists of centralizers of $2B$ -involution, but no element from $3A$ centralizes such an involution. Finally, the maximal subgroup $[2^5].(S_3 \times S_3)$ is the centralizer of a $2A$ -involution, but this now does not centralize $3C$ -elements. Hence all three possibilities are ruled out, and we conclude that $H = G$. Descent of degree two now yields the result for the simple group. \square

8.2 The Groups $\mathrm{F}_4(p)$

Our choice of class vector for $\mathrm{F}_4(p)$ is similar to the one in Section 5.2. The first class C_p again consists of long root elements. For the second class, when $q \equiv -1 \pmod{3}$, we take $C_6 := [h_{16}^{(q+1)/6}]$ containing rational elements of order 6, a power of the class C_{q+1} in Section 5.2. If $q \equiv 1 \pmod{3}$, similar elements of order six are given by $C_6 := [h_{15}^{(q-1)/6}]$.

In Proposition 5.4 we chose C_T to contain a generator of the cyclic torus T . It turns out that it suffices to include an element with order a primitive prime divisor of $|T|$ into the class structure to obtain rigidity. Now T has normalizer $\mathcal{N}_G(T) = T.12$, so any non-identity rational elements in it has order 13. Such elements exist when q is a primitive root modulo 13. Now when $q = p^m$ is a primitive root, the same certainly holds for p , so that our element of order 13 will already be contained in

the group over the prime field $F_4(p)$. We can hence only expect generation when $q = p$. Let C_{13} be the class of an element of order 13 in T .

Theorem 8.3. *For primes $p \equiv 2, 6, 7, 11 \pmod{13}$, $p \geq 19$, the groups $F_4(p)$ have GA-realizations over \mathbb{Q} for the class vector $\mathbf{C} = (C_p, C_6, C_{13})$.*

Proof. First note that the class vector is rational by Shoji (1974). So it suffices to show $l(\mathbf{C}) = 1$. In the case $p \equiv -1 \pmod{3}$, the arguments in Proposition 5.4 to find the nonvanishing characters also work with C_{13} and C_6 . Moreover, elements from C_T and C_{13} , resp. from C_{q+1} and C_6 have conjugate centralizers, so the values of unipotent characters on them are the same by the character formula (5.3). So in this case we immediately get $n(\mathbf{C}) = 1$ from Table 5.1. If $p \equiv 1 \pmod{3}$, similar arguments to those in the proof of Proposition 5.4 also allow the verification of $n(\mathbf{C}) = 1$. The relevant character values are omitted.

But for generation we cannot use Weigel (1992) as above, since there only the overgroups of the whole torus T are classified. Instead we apply Malle and Testerman (2011), Theorem 29.5. Note that $H = \langle \sigma \rangle$ for $\sigma \in \bar{\Sigma}(\mathbf{C})$ is perfect by Proposition 4.3. Corollary 4.2 applied to the primitive prime divisor 13 of $p^4 - p^2 + 1$ excludes the possibilities (ii)–(iv) and this forces H to be simple of Lie type in characteristic p or one of the groups in Liebeck and Seitz (1999), Theorem 2. The following of these have order divisible by 13:

$$L_2(13), L_2(25), L_2(27), L_3(3), L_4(3), {}^2B_2(8), {}^3D_4(2).$$

All of these groups have order only divisible by primes $l \leq 13$, while the order of H is also divisible by $p \geq 19$.

Thus we are left with the groups of Lie type in the same characteristic p . We only need to consider those of Lie rank at most 4, since otherwise they cannot be contained in G . Again since 13 is a primitive prime divisor of $\phi_{12}(p)$, we may apply the divisibility criterion in Corollary 4.2 to the order of candidates $H(p^m)$ in the form

$$\phi_{12}(p) \mid |H(p^m)| \mid |F_4(p)|.$$

Apart from G this leaves the six cases

$$A_1(p^6), A_2(p^4), {}^2A_2(p^2), B_2(p^3), G_2(p^2), {}^3D_4(p).$$

Most of those cannot be contained in G : The centralizer of an element of order 13 has order $(p^6 + 1)/2$ in $A_1(p^6)$, $p^8 + p^4 + 1$ in $A_2(p^4)$ and $p^6 + 1$ in $B_2(p^3)$, but only $p^4 - p^2 + 1$ in G . Also, $G_2(p^2)$ contains a maximal torus of order $p^4 + p^2 + 1$, while there are no elements of that order in G . The remaining two groups ${}^2A_2(p^2)$ and ${}^3D_4(p)$ are excluded precisely as in the proof of Proposition 5.4, and the proof is complete. \square

Using a different class vector Guralnick, Lübeck and Yu (2016) were able to show a more comprehensive result for $F_4(p)$. To state it, let C_2 denote the class of involutions with centralizer of type $C_3 + A_1$, C_{2p} the class of elements of order

$2p$ whose square is a long root element and whose p th power is an involution with centralizer type B_4 , and C_u be the class of regular unipotent elements. All three classes are rational.

Theorem 8.4. *For all primes $p > 3$ the groups $F_4(p)$ have GA-realizations over \mathbb{Q} for the class vector $\mathbf{C} = (C_2, C_{2p}, C_u)$ defined above.*

The proof requires a more detailed analysis involving estimates on character values as well as precise information on subgroups of $F_4(p)$ containing regular unipotent elements.

8.3 The Groups $E_6(p)$ and ${}^2E_6(p)$

Let again $G := E_6(q)_{sc}:2$ be the extension by the graph automorphism of order two of the simply connected group of type E_6 . Define the class C_{2p} as in Section 5.3. This class is rational. Next, we have to find rational elements in the torus of order $q^6 + q^3 + 1 = \phi_9$. Since $|\mathcal{N}_G(T)/T| = 18$, these will necessarily have order 19, and exist when q is the square of a primitive root modulo 19. Let C_{19} denote the class of such elements.

Theorem 8.5. *For primes $p \equiv 4, 5, 6, 9, 16, 17 \pmod{19}$, the group $E_6(p)_{sc}:2$ has a G-realization over \mathbb{Q} for the class vector $\mathbf{C} = (C_{2p}, C_{2p}, C_{19})$.*

Proof. As in the case of $F_4(p)$ it first follows from the Deligne–Lusztig theory of disconnected groups (Digne and Michel (1994)) that the character values on C_T given in Table 5.2 coincide with those on C_{19} . This yields $n(\mathbf{C}) = 1$.

So now let $H = \langle \sigma \rangle$ with $\sigma \in \bar{\Sigma}(\mathbf{C})$, and $\tilde{H} := H/(H \cap \mathcal{Z}(G'))$. For generation, we may proceed as in the case of $F_4(p)$. In particular, by Malle and Testerman (2011), Theorem 29.5, it remains to consider simple groups of Lie type in characteristic p and the groups in Liebeck and Seitz (1999), Theorem 2.

Of the latter, only $L_2(19), J_1$ and J_3 have order divisible by 19. But J_1 possesses a Frobenius subgroup of type $11:10$. By Cohen et al. (1992) such can only exist in G when $p = 31$ resp. $p = 11$. But neither p satisfies the congruences. The only possible case for the occurrence of $L_2(19)$ is for $p = 5$. As H contains outer elements of G , $\overline{H \cap G'}$ is a subgroup of \tilde{H} of index two. If we had $L_2(19) \leq \tilde{H} \leq \text{Aut}(L_2(19)) = L_2(19):2$, then consequently $\tilde{H} = L_2(19):2$. But this is impossible since $L_2(19):2$ does not possess outer elements of order $10 = 2p$. The remaining case $R = J_3$ might only happen for $p \in \{5, 17\}$, as we have $|J_3| = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$. The case $p = 5$ is excluded as above. Finally from the Atlas one finds that the $(34, 34, 19)$ -structure constants of $J_3:2$ are too large to come from (C_{34}, C_{34}, C_{19}) in G .

The groups of Lie type are treated as in the proof of Proposition 8.3. Using Corollary 4.2, only $A_2(p^3)$ remains apart from $E_6(p)$. Now the end of the proof of Proposition 5.6 may be used to exclude that last case, and the assertion follows. \square

Descent to the normal subgroup of index 2, taking factor groups, and using that $\text{Aut}(E_6(p)) = E_6(p):2$ for $p \not\equiv 1 \pmod{3}$ leads to:

Corollary 8.6. *The groups $E_6(p):2$, $E_6(p)_{sc}$ and $E_6(p)$ possess G -realizations over \mathbb{Q} for primes $p \equiv 4, 5, 6, 9, 16, 17 \pmod{19}$. If moreover $p \equiv -1 \pmod{3}$, this yields a GA-realization of $E_6(p)$ over \mathbb{Q} .*

A completely similar treatment is possible for the twisted groups. The choice of classes for the class vector is precisely the same as above, except that now we look for rational elements of order 19 in the torus of order ϕ_{18} , which exist if p is a primitive root mod 19.

Theorem 8.7. *The groups ${}^2E_6(p)_{sc}:2$, ${}^2E_6(p):2$, ${}^2E_6(p)_{sc}$ and ${}^2E_6(p)$ possess G -realizations over \mathbb{Q} for primes $p \equiv 2, 3, 10, 13, 14, 15 \pmod{19}$, $p > 3$, where the class vector for ${}^2E_6(p)_{sc}:2$ is $\mathbf{C} = (C_{2p}, C_{2p}, C_{19})$. If moreover $p \not\equiv -1 \pmod{3}$ this yields a GA-realization of ${}^2E_6(p)$ over \mathbb{Q} .*

Sketch of proof. The structure constant $n(\mathbf{C}) = 1$ follows from Table 5.4. Arguing as in the preceding proof, we only need to consider simple subgroups. We first consider those not of Lie type not in characteristic p , viz. $L_2(19)$, and J_3 . Now the group generated by a triple from \mathbf{C} clearly has order divisible by p , hence p must be one of $p = 2, 3, 5, 19$ for $L_2(19)$ or $p = 2, 3, 5, 17, 19$ for J_3 . None of these primes is allowed in the theorem (note that $\text{PGL}_2(19)$ possesses a $(6, 6, 19)$ generating system, so $p = 3$ has to be excluded at this point). Again, the groups of Lie type in the same characteristic are excluded as usual.

The final assertion follows since $\text{Aut}({}^2E_6(p)) = {}^2E_6(p):2$ for $p \not\equiv -1 \pmod{3}$. \square

Remark. As with $E_6(q)$, we obtain a second Galois realization for the groups in Theorems 8.5, 8.6 and 8.7 from the Fixed Point Theorem I.7.2, belonging to a class vector (C_2, C_{2p}, C_{19}) .

8.4 The Groups $E_8(p)$

Recall the maximal torus T of $E_8(q)$ from Section 5.6. If it contains rational elements, we can hope to obtain Galois realizations over \mathbb{Q} , at least for $E_8(p)$. Since $\mathcal{N}_G(T) = T.30$, rational elements in $T \setminus 1$ necessarily have order 31. Now 31 divides ϕ_{30} precisely when p is a primitive root modulo 31. This happens for roughly every fourth prime. There exists another t.i.-torus in G containing rational elements of order 31, namely the one with order ϕ_{15} . Let C_{31} denote the class of an element of order 31 in $E_8(p)$ when $31 \mid \phi_{15}$ or $31 \mid \phi_{30}$. To ease the notation, write

$$P_1 := \{p \in \mathbb{P} \mid p \equiv 3, 11, 12, 13, 17, 21, 22 \text{ or } 24 \pmod{31}\},$$

$$P_2 := \{p \in \mathbb{P} \mid p \equiv 7, 9, 10, 14, 18, 19, 20 \text{ or } 28 \pmod{31}\},$$

for the set P_i of primes p of multiplicative order $30/i$ modulo 31. Then with the classes C_2 and C_p introduced in Section 5.6 we have:

Theorem 8.8. *The groups $E_8(p)$ have GA-realizations over \mathbb{Q} for primes $p \in P_1 \cup P_2$, $p \geq 7$ for the class vector (C_2, C_p, C_{31}) .*

Note that elements from the third class either lie in the torus of order ϕ_{30} used above, or in one of order ϕ_{15} with rather similar properties. Hence the proof can be completed as the one for $F_4(p)$ in Theorem 8.3, using the list in Liebeck and Seitz (1999) of possible simple subgroups of $E_8(q)$. The details can be found in Malle (1988b).

As in the case of $F_4(p)$ a more comprehensive result is available whose proof relies on more precise discussion of character values and on a knowledge of over-groups of regular unipotent elements. Let C_2 be the class of involutions in $E_8(p)$ with centralizer of type D_8 , C_p the class of unipotent elements of type $4A_1$, and C_u the class of regular unipotent elements. The following is shown in Guralnick and Malle (2014):

Theorem 8.9. *For all primes $p \geq 7$ the groups $E_8(p)$ have GA-realizations over \mathbb{Q} for the class vector $\mathbf{C} = (C_2, C_p, C_u)$ defined above.*

9 The Sporadic Groups

The character theoretic form of the rationality criterion is most suited for application to the sporadic groups. The character tables of all 26 sporadic groups are known (see Conway et al. (1985) and also Breuer, Malle and O'Brien (2016)), and moreover the lists of maximal subgroups are almost complete by the work of a number of authors.

Due to the irregular nature of the sporadic groups, no unified proof of rigidity for them is known. Still, they can be treated in a case by case analysis, and it turns out that with at most the exception of the Mathieu group M_{23} , they all occur as geometric Galois groups over $\mathbb{Q}(t)$. This result is due to Thompson (1984a) for the monster M , to Matzat (1985a) for M_{12} and M_{22} , to Hoyden-Siedersleben (1985) for M_{23} , M_{24} and J_1 , to Matzat and Zeh-Marschke (1986) for M_{11} , to Hunt (1986) for J_2 , Suz, HS, Co_3 , Co_2 , Co_1 , Fi_{23} , Fi'_{24} and Th, to Hoyden-Siedersleben and Matzat (1986) for HN, ON, and to Pahlings (1988, 1989) for McL, He, Fi_{22} , J_3 , Ly, Ru and J_4 . No correct Galois realization for the baby monster B is contained in the literature (note that the structure constant given for B in Hunt (1986) is equal to 3, not 1 as stated).

The proofs appearing in the literature sometimes make extensive use of computer calculations, of character tables for maximal subgroups and their fusion maps. We have tried to present proofs which may be checked just by using the Atlas. Therefore, in addition to the Galois realization for B , new realizations are given for the sporadic groups Suz, Co_3 , Co_2 , He, Fi_{22} , Fi_{23} and Ru in order to get simplified proofs. Nevertheless for the groups B , J_3 and J_4 no easy arguments could be found, and our proofs are sketchy and still rely on a certain amount of computer calculations, most notably in the cases of J_4 and B . Despite considerable efforts the group M_{23} has at present only been realized as Galois group over several quadratic extension fields of \mathbb{Q} .

The sporadic groups may be subdivided into several families of more or less similar groups, as proposed in the Atlas. We follow this subdivision in our proof.

9.1 The Mathieu Groups

The names for the conjugacy classes in the class vectors are taken from the Atlas, as well as all results on character tables, on classes, powermaps and maximal subgroups, if no other source is indicated.

In the proofs we will make frequent use of the following observations. Let $G = \langle \sigma_1, \sigma_2 \rangle$ be generated by a 3-system $\sigma = (\sigma_1, \sigma_2, \sigma_2^{-1}\sigma_1^{-1})$ with element orders (n_1, n_2, n_3) . If $H \triangleleft G$ is a normal subgroup, then clearly G/H is generated by the 3-system $\bar{\sigma}$ of images, with orders (m_1, m_2, m_3) , where $m_i | n_i$, $i = 1, 2, 3$. If G/H has a transparent structure, this may be used to deduce restrictions on possible tuples (n_1, n_2, n_3) for G . One strong application was already given by Proposition 4.3.

Proposition 9.1. (a) *The class vector $(2C, 3A, 12A)$ of $\text{Aut}(M_{12})$ is rationally rigid.*

(b) *The class vector $(2B, 4C, 11A)$ of $\text{Aut}(M_{22})$ is rationally rigid.*

(c) *The class vector $(2A, 3B, 23A)$ of M_{24} is rigid.*

Proof. We use the character theoretic rigidity criterion in Corollary I.5.9 and the tables of complex irreducible characters of the sporadic simple groups G and their automorphism groups $\text{Aut}(G)$ in the Atlas. From these tables the structure constants $n(\mathbf{C})$ for the class vectors above are easily calculated to be equal to 1 in all cases. To be able to apply the Basic Rigidity Theorem I.4.8, we have to prove $l(\mathbf{C}) = 1$. In the case $n(\mathbf{C}) = 1$ this is equivalent to showing that a triple from \mathbf{C} cannot generate a proper subgroup of $\text{Aut}(G)$. Let H denote the subgroup of $\text{Aut}(G)$ generated by a triple of elements from the class vector \mathbf{C} .

In case (a), the squares of elements from class $12A$ lie in class $6A$, so clearly H contains elements from classes $3A$ and $6A$. In the Atlas, the permutation characters for ten of the eleven classes of maximal subgroups of M_{12} are given. From these one checks that none contains elements from both $3A$ and $6A$. So the only remaining possibility is $H \leq M = S_4 \times S_3$. If M has a $(2, 3, 12)$ -system, then the last class has to be the product of the 4-cycles in S_4 times the 3-cycles in S_3 . It then follows that

$$\mathbf{C} \cap M = ((2) \times (1), (3) \times (3), (4) \times (3))$$

in obvious notation. Now M has three classes of elements of order three, $(1) \times (3)$, $(3) \times (1)$ and $(3) \times (3)$, with centralizers in M of orders 72, 18 and 9 respectively. If $n_M(\mathbf{C}) \neq 0$, then clearly the first of the three classes fuses into $3B = (6A)^2$, while the third fuses into $3A$. But now, depending on the fusion of $(3) \times (1)$, the permutation character $\chi = 1_M^G$ takes either the values $\chi(3A) = 12$, $\chi(3B) = 5$, or $\chi(3A) = 18$, $\chi(3B) = 1$. This contradicts the fact that by congruence properties of character values we should have $\chi(3A) \equiv \chi(3B) \pmod{3}$. So $H \not\leq M$, completing the proof for part (a).

In case (b), from the Atlas we see that $\text{PGL}_2(11) = \text{L}_2(11):2$ is the only type of maximal subgroup of $\text{Aut}(G)$ different from G with order divisible by 11. Assume that $H \leq \text{PGL}_2(11)$. The intersection of this maximal subgroup with G is equal to $\text{L}_2(11)$, so elements from the single outer class of involutions of $\text{PGL}_2(11)$ would have to fuse into $2B$. The centralizer order for this class in $\text{PGL}_2(11)$ is divisible by 5, in contrast to the centralizer order for $2B$ in $\text{Aut}(M_{22})$. Thus we have $H \not\leq \text{PGL}_2(11)$ (this can also be seen from the permutation character given in the Atlas), and the result follows.

In the third case, the maximal subgroups of G of order divisible by 23 are M_{23} and $\text{L}_2(23)$. Both of these have just one class of elements of orders 2 and 3. Moreover both contain elements of order 6. Since $(6A)^2 = 3A$, $(6A)^3 = 2A$, while $(6B)^2 = 3B$, $(6B)^3 = 2B$, the classes $2a$, $3a$, from the two maximal subgroups either fuse into $2A$, $3A$, or into $2B$, $3B$; in particular none of the two types intersects both $2A$ and $3B$. This proves that $H = M_{24}$. \square

9.2 The Leech Lattice Groups

The sporadic groups J_2 , Suz , HS , McL , Co_3 , Co_2 and Co_1 are most conveniently described as stabilizers of vectors in the Leech lattice and hence subsumed under the name of Leech lattice groups.

- Proposition 9.2.** (a) *The class vector $(3A, 8C, 14A)$ of $\text{Aut}(J_2)$ is rationally rigid.*
 (b) *The class vector $(2C, 8D, 13A)$ of $\text{Aut}(\text{Suz})$ is rationally rigid.*
 (c) *The class vector $(2C, 5C, 30A)$ of $\text{Aut}(\text{HS})$ is rationally rigid.*
 (d) *The class vector $(3A, 4B, 10B)$ of $\text{Aut}(\text{McL})$ is rationally rigid.*

Proof. This can again be proved with Corollary I.5.9. From the complex character tables one verifies $n(\mathbf{C}) = 1$ in cases (a)–(c) and $n(\mathbf{C}) = 3$ for $\text{Aut}(\text{McL})$. It remains to check generation in the first three cases, while in the last we have to account for a summand of 2 in the structure constant coming from proper subgroups.

The list in the Atlas reveals that only the maximal subgroups $U_3(3):2 \cong G_2(2)$ and $\text{PGL}_2(7) \times 2$ of $\text{Aut}(J_2) = J_2:2$ different from J_2 have order divisible by 7. But $G_2(2)$ does not contain elements of order 14. Assume $H \leq \text{PGL}_2(7) \times 2$. The factor group $H/(H \cap L_2(7))$ is a subgroup of $Z_2 \times Z_2$ and has a $(1, 2, 2)$ -generation (obtained from \mathbf{C}), hence is isomorphic to Z_2 . So we would already have $H \leq \text{PGL}_2(7)$ or $H \leq L_2(7) \times 2$, but the first contains no elements of order 14, the second none of order 8. This excludes the last possible maximal subgroup, proving generation in case (a).

The maximal subgroups of $\text{Aut}(\text{Suz})$ different from Suz of order divisible by 13 are $G_2(4):2$ and $L_2(25):2$. The latter is actually equal to $L_2(25):2_2$, since $L_2(25).2_3$ is non-split, and the outer involutions in $L_2(25):2_1$ centralize an element of order 13. But $L_2(25):2_2$ contains no element of order 8. The permutation character χ of Suz on $G_2(4)$ is well known; in fact, Suz may be constructed as a rank three permutation group with point stabilizer $G_2(4)$. The permutation character of $\text{Aut}(\text{Suz})$ on $G_2(4):2$ may easily be deduced from that. It restricts to Suz as $\chi = \chi_1 + \chi_{780} + \chi_{1001}$, and since it has to take non-negative values, it is exactly given by the sum of the first, the fourth and the fifth irreducible character of $\text{Aut}(G)$ in the Atlas. But this permutation character vanishes on class $8D$, so we have $H = \text{Aut}(\text{Suz})$ and the result follows for part (b).

In case (c), as H contains representatives from the two rational conjugacy classes $5B = (30A)^6$ and $5C$, its order is divisible by at least 25. The only maximal subgroups of $\text{Aut}(\text{HS})$ apart from $G := \text{HS}$ with order divisible by 25 are $U_3(5):2$, $5_+^{1+2}:[2^5]$ and $M = 5:4 \times S_5$. But the first subgroup contains no outer elements, while the order of the second is prime to three. The third one, a direct product of the Frobenius group of order 20 with the symmetric group S_5 , obviously has three conjugacy classes of elements of order five, $C_1 = 1 \times 5$, $C_2 = 5 \times 1$, $C_3 = 5 \times 5$, where we have indicated the projections of these classes onto the two factors of the direct product M . The corresponding centralizer orders in M are 100, 600 and 25, respectively. The first class fuses into $5A$ of G by the description $M = \mathcal{N}(2B, 3A, 5A)$ in the Atlas. The class C_2 has to fuse into $5B$ since that is the only class with centralizer order divisible by three. Now the values of the permutation character $\chi_M^{\text{Aut}(G)}$ on

$1A$ and on $5B$ have to be congruent modulo 5, hence divisible by 5, as immediately follows from consideration of the cycle type of the element of order 5 in this permutation representation. The inclusion $C_2 \subset 5B$ contributes 1 to $\chi_M^{\text{Aut}(G)}(5B)$, so the class C_3 also has to fuse into $5B$ and $M \cap 5C$ is empty. Thus $H \not\leq M$, proving the result for assertion (c).

Excluding the maximal subgroup of $\text{Aut}(\text{McL})$ of order not divisible by 5, we are left with $U_4(3):2_3$, $U_3(5):2$, $3^{1+4}:4S_5$, $3^4:(M_{10} \times 2)$, $L_3(4):2^2$, $2:S_8$, $M_{11} \times 2$ and $(5_+^{1+2}:3:8).2$. Factoring the last group by its normal subgroup of order $3 \cdot 5^3$ it becomes evident that it cannot contain $(3, 4, 10)$ -triples. The subgroup $3^{1+4}:4S_5$ is identified as $\mathcal{N}(3A)$, so the powermap shows that its 5-elements lie in $5A$ of $G := \text{McL}$. But as $(10B)^2 = 5B$ it does not intersect class $10B$. Similarly we have $2:S_8 = \mathcal{N}(2A)$, hence its 5-elements again lie in $5A$. The group $M_{11} \times 2$ centralizes the outer involution $2B$, so its unique class of 3-elements fuses into $3B$ of G . Also, $U_3(5):2$ has outer elements of order six, which hence fuse into $6C$ of G . But the squares of such elements lie in $3B$, and it follows that $3A \cap U_3(5):2 = \emptyset$. Precisely the same argument applies to $L_3(4):2^2$. In any complement of 3^4 in the semidirect product $3^4:(M_{10} \times 2)$ the central involution is outer, hence lies in class $2B$. So again all 3-elements of the complement fuse into $3B$. As this is true for any complement, $3A$ -elements could only lie in the normal subgroup of $3^4:(M_{10} \times 2)$. Factoring by this 3^4 we see that \mathbf{C} cannot contain triples from that maximal subgroup.

We are left with $M = U_4(3):2_3$. Since this group has uniquely determined outer classes $4j$ of 4-elements and $10c$ of elements of order 10, these fuse into $4B$, $10B$ of G , respectively. Further M contains a full Sylow 3-subgroup of G . The class $3A$ of G consists of third powers of elements of order nine and all third powers of elements of order 9 in M fall into $3a$, so the intersection of M with $3A$ is just $3a$. The structure constant for the intersections of \mathbf{C} with M now equals

$$n_M(3a, 4j, 10c) = 2.$$

From the list of maximal subgroups of M it is easily seen that any such triple has to generate all of M , so this maximal subgroup contributes 2 to $n(\mathbf{C})$ by Proposition I.5.7. This yields $l(\mathbf{C}) = n(\mathbf{C}) - 2 = 1$. \square

- Proposition 9.3.** (a) *The class vector $(2A, 5B, 30A)$ of Co_3 is rationally rigid.*
 (b) *The class vector $(2A, 5A, 28A)$ of Co_2 is rationally rigid.*
 (c) *The class vector $(3A, 5C, 13A)$ of Co_1 is rationally rigid.*

Proof. The structure constant for Co_3 is found to be $n(\mathbf{C}) = 7$, while in the other two cases one computes $n(\mathbf{C}) = 1$.

In $G = \text{Co}_3$, the sixth powers of elements from $30A$ lie in class $5A$ of G , so H contains elements from the two rational classes $5A$, $5B$, and its order must be divisible by 25. This rules out all maximal subgroups apart from $\text{McL}:2$, HS and $U_3(5):S_3$. The group HS has no elements of order 30. Clearly H has no factor group S_3 , and $H \leq U_3(5):2$ can be ruled out since $U_3(5)$ does not contain elements of order 15. Finally consider $M = \text{McL}:2$. The class $5a$ of M consists of sixth powers of elements from $30a$ (the unique class of 30-elements in M), so fuses into

$5A$ of G . As the full 5 -part of $|G|$ divides $|M|$, the other class $5b$ of 5 -elements in M must fuse into $5B$. Finally $2a = (30a)^{15}$ in M , so $2a$ fuses into $2A = (30A)^{15}$, and since $2a, 5b$ already lie in the simple group $M' = \text{McL}$, we only have to consider subgroups of McL . The structure constant in M equals

$$n_M(2a, 5b, 30a) = 6.$$

The only maximal subgroup of McL containing elements of order 30 and with order divisible by 25 is a $5_+^{1+2}:3:8$, but clearly the above triple cannot lie in that group. So any of the six triples in M generates M' , which yields a contribution of 6 to $n(\mathbf{C})$ by Proposition I.5.7. Since this was the only maximal subgroup left to consider, we obtain $l(\mathbf{C}) = n(\mathbf{C}) - 6 = 1$.

In part (b), for divisibility reasons only the maximal subgroups $2^{10}:\text{M}_{22}:2$, McL , $2_+^{1+8}:2\text{S}_6(2)$, $\text{HS}:2$, $[2^{11}]:A_8$, $\text{U}_4(3).\text{D}_8$, M_{23} or $\text{U}_6(2):2$ might contain H . Of these, McL , $\text{HS}:2$, M_{23} and $\text{U}_6(2):2$ do not contain elements of order 28. The maximal subgroup $2_+^{1+8}:2\text{S}_6(2)$ is the centralizer in G of $2A$ -involution, and as such does not intersect the class $5A$ as can be seen from the powermap of elements of order 10 in G . Similarly, $[2^{11}]:A_8$ centralizes a $2B$ -involution, but the self-centralizing subgroup generated by an element from $28A$ only contains $2A$ involutions, hence does not lie in $\mathcal{C}_G(2B)$. If H were contained in $\text{U}_4(3).\text{D}_8$, then it would already lie in an extension of $\text{U}_4(3)$ of degree two, as can be seen from $\bar{\mathbf{C}}$ in $H/(H \cap \text{U}_4(3))$. But as $\text{U}_4(3)$ has no elements of order 14, no element in such a degree 2 extension has order 28. Finally assume $H \leq 2^{10}:\text{M}_{22}:2$. We claim that M_{22} contains no $5A$ -elements. Indeed, the Sylow 11-subgroup of G is self-centralizing, with normalizer $11:10$. The maximal subgroup $\text{U}_6(2):2$ contains a subgroup $11:5$. Its elements of order 30 are rational, so they fuse into $30A$ of G . The sixth power of $30A$ is $5B$, showing that the 11-normalizer $11:10$ contains $5B$ -type elements. Now M_{22} also contains $11:5$, hence its single class of elements of order 5 fuses into $5B$, which completes the proof in case (b).

In the third case the maximal subgroups with order divisible by 13 are $3'\text{Suz}:2$ and $(A_4 \times G_2(4)):2$. The centralizer order of $5C$ -elements in G is not divisible by 9, but in $A_4 \times G_2(4)$, all 5 -elements have centralizer order $12 \cdot 300$. The group $3'\text{Suz}:2$ arises as the normalizer $\mathcal{N}(3A)$, but from the powermap of elements of order 15 it follows that $5C$ does not intersect the centralizer $\mathcal{C}(3A)$. Hence we have $H = G$. \square

9.3 The Fischer Groups

- Proposition 9.4.** (a) The class vector $(2D, 5A, 42A)$ of $\text{Aut}(\text{Fi}_{22})$ is rationally rigid.
 (b) The class vector $(2A, 7A, 27A)$ of Fi_{23} is rationally rigid.
 (c) The class vector $(2C, 8D, 29A)$ of $\text{Aut}(\text{Fi}'_{24})$ is rationally rigid.

Proof. For all three groups, the normalized structure constant $n(\mathbf{C})$ equals 1.

In case $G = \text{Fi}_{22}$, among the maximal subgroups of $\text{Aut}(G)$ different from G , only $2'\text{U}_6(2).2$, $\text{G}_2(3):2$, $\text{O}_8^+(2):\text{S}_3 \times 2$, $2^{10}:\text{M}_{22}$, $2^7:\text{S}_6(2)$ and $\text{S}_3 \times \text{U}_4(3).(2^2)_{122}$

have order divisible by 7 (Wilson (2017)). As $2^7 U_6(2)$, $G_2(3)$, M_{22} and $S_6(2)$ do not contain elements of order 21, we are left with the cases $M_1 = O_8^+(2) : S_3 \times 2$ and $M_2 = S_3 \times U_4(3). (2^2)_{122}$. These may be excluded at the same time. For this denote by N_i the simple normal subgroup $O_8^+(2)$, resp. $U_4(3)$ of M_i . If H is contained in M_i , then $H/(H \cap N_i)$ has order at most two, since the second class of C clearly lies inside N_i . So $H \leq N_i \cdot 2$, which contradicts the fact that in neither case the group N_i contains elements of order 21. This completes the proof of (a).

By Wilson (2017), only the maximal subgroups of Fi_{23} isomorphic to $O_8^+(3) : S_3$, $[2^7 3^{12}] \cdot 2S_4$ or $[3^{10}] \cdot (2 \times L_3(3))$ might contain elements of order 27. But the order of the latter two is not divisible by 7. If H were contained in $O_8^+(3) : S_3$, then, as the orders of the three elements in C are coprime, it would already lie in $O_8^+(3)$ by Proposition 4.3. But that group has no elements of order 27. So it follows that $H = G$ for case (b).

By Wilson (2017), the only maximal subgroup of Fi'_{24} of order divisible by 29 is the local subgroup $29 : 14$, which extends to $29 : 28$ in Fi_{24} . Since 8 does not divide its order, we obviously have $H = \text{Aut}(G)$. \square

9.4 The Monster Centralizers

The four sporadic groups He, HN, Th and B occur as centralizers of elements in the monster group M. We treat B and M separately, since at least for M the information on maximal subgroups is still incomplete, although strong restrictions on possible subgroups follow from the classification, and so different methods of proof must be employed.

- Proposition 9.5.** (a) *The class vector $(2C, 3A, 30A)$ of $\text{Aut}(\text{He})$ is rationally rigid.*
 (b) *The class vector $(2C, 5A, 42A)$ of $\text{Aut}(\text{HN})$ is rationally rigid.*
 (c) *The class vector $(2A, 3A, 19A)$ of Th is rationally rigid.*

Proof. For $\text{Aut}(\text{He})$ we have $n(C) = 7/6$, while in the two other cases the structure constant is calculated as $n(C) = 1$.

For $G = \text{He}$, among the maximal subgroups of $\text{Aut}(G)$, only those of type $S_4(4) : 4$, $S_5 \wr 2$, $2^2 \cdot L_3(4) \cdot D_{12}$, $3 : S_7 \times 2$ and $5^2 : 4S_4$ have orders divisible by 5. Of these, $S_4(4) : 4$, $2^2 \cdot L_3(4) \cdot D_{12}$ and $5^2 : 4S_4$ do not contain elements of order 30. For the second of these this follows from its characterization as $\mathcal{N}(2A^2)$: the square of the element of order 30 has odd centralizer order in G , so acts non-trivially on $2A^2$. Thus the cube of the element of order 30 has to centralize the whole four group. But $(30A)^3 = 10B$, and the centralizer of such an element is of order 60 and contains at least one element from $(10B)^2 = 2C$, so cannot contain a $2A^2$, as claimed. Assume that $5^2 : 4S_4$ has elements of order 30. Then an element ρ of order three in the complement $4S_4$ has to centralize some element of order 5 in the elementary abelian normal subgroup 5^2 , hence also the cyclic subgroup generated by this element. This leaves 20 elements in 5^2 , of which obviously ρ has to centralize at least another one. But then we would have $25 \mid |\mathcal{C}_G(\rho)|$, which is not the case.

Next assume $H \leq 3^{\cdot}S_7 \times 2$. Then by factoring out $H \cap 3^{\cdot}A_7$ we see that H already lies inside $3^{\cdot}A_7 \times 2$. The projection of \mathbf{C} onto the second factor now has the type $(2, 1, 2)$, hence it projects as $(2, 3, 15)$ onto $3^{\cdot}A_7$. The relevant structure constants in that group are easily computed and by Proposition I.5.7 contribute at most $1/3 + 1/6$ to $n(\mathbf{C})$, depending on the exact fusion.

We are left with $M = S_5 \wr 2$. Again, if $H \leq M$, then H already lies in a degree 2 extension of $A_5 \times A_5$. Elements of order 30 in the wreath product $S_5 \wr 2$ are easily seen to generate their proper centralizers, and then it follows that a degree two extension containing these must be $S_5 \times A_5$. The projection of \mathbf{C} onto the factors must then equal $(2, 3, 6) \times (2, 3, 5)$, and again we find a structure constant of $1/6$. In conclusion, we have $7/6 \geq l(\mathbf{C}) \geq n(\mathbf{C}) - 4/6 = 3/6$, and this proves $l(\mathbf{C}) = 1$ in case (a).

The maximal subgroups of $\text{Aut}(\text{HN})$ with order divisible by 5 and 7 are of types S_{12} , $4 \cdot \text{HS}.2$ and $5:4 \times \text{U}_3(5):2$. But neither HS nor $\text{U}_3(5)$ does contain elements of order 21, hence the same holds for the second and third maximal subgroup listed above. So we are left with the symmetric group S_{12} . From the character table of S_{12} it may be calculated that the only non-vanishing $(2, 5, 42)$ -structure constants are

$$n(2e, 5b, 42a) = 3 \quad \text{and} \quad n(2f, 5b, 42a) = 51/2.$$

But S_{12} is self normalizing in $\text{Aut}(\text{HN})$, so if indeed one of the two above class vectors would fuse into \mathbf{C} in $\text{Aut}(\text{HN})$, then the structure constant could be at most as large as in $\text{Aut}(\text{HN})$ by Proposition I.5.7. This contradiction rules out $H \leq S_{12}$, proving the result in case (b).

For $G = \text{Th}$, only the maximal subgroups of type $\text{U}_3(8):6$ and $\text{L}_2(19):2$ contain elements of order 19 (Wilson (2017)). But in $\text{L}_2(19)$, the elements of order three are third powers, which is not the case for elements from $3A$ in G . If $H \leq \text{U}_3(8):6$, then we already have $H \leq \text{U}_3(8)$, as H is perfect by Proposition 4.3. The class $3c$ of $\text{U}_3(8)$ has third roots, so it cannot fuse into $3A$ of G . Thus \mathbf{C} would have to be equal to one of $(2a, 3ab, 19abcdef)$. But the corresponding structure constants vanish in $\text{U}_3(8)$, so we have $H = G$, proving part (c). \square

Proposition 9.6. (a) *The class vector $(2C, 3A, 55A)$ of B is rationally rigid.*

(b) *The class vector $(2A, 3B, 29A)$ of M is rationally rigid.*

Proof. For the baby monster B , we proceed as follows: The $(2C, 3A, 55A)$ -structure constant of B equals 1. Using the matrix representation of dimension 4370 of B over \mathbb{F}_2 constructed by himself, R. Wilson verified the existence of a generating triple of elements in the class vector \mathbf{C} . To be more precise, he found three matrices, lying in the respective classes of \mathbf{C} and with product one, such that the orders of some randomly produced elements contained all prime divisors of the group order. Then an easy application of the classification shows that the three elements already have to generate B (see the list of maximal subgroups in Wilson (2017)).

The maximal subgroups of M are not yet known completely, but as in the previous case, we can make use of the classification. The three element orders in \mathbf{C} are pairwise coprime, so H is perfect by Proposition 4.3. Let L denote a top non-abelian

simple composition factor of H . Then the condition $29 \mid |L|$ together with the list of possible simple sections of M in the Atlas shows that $L \in \{L_2(29), L_2(59), \text{Fi}'_{24}\}$ or $L = H = M$. Now the class $2A$ of M consists of $\{3, 4, 5, 6\}$ -transpositions, i.e., of transpositions such that the product of any two has order at most 6. The groups $L_2(29)$ and $L_2(59)$ contain dihedral subgroups of orders 14, 58 respectively, so their unique class of involutions cannot fuse into $2A$. Hence if $H \neq M$, then its top composition factor is isomorphic to the Fischer group Fi'_{24} .

Assume that this is the case. Let S be a minimal normal subgroup of H . Then S is a direct product of isomorphic simple groups. The element of order 29 in H acts on S . If $S = S_1 \times \cdots \times S_r$ were non-abelian, then either $29 \mid |\text{Aut}(S_1)|$, hence $S = L$ by the classification above, or S consists of at least 29 factors, since the element of order 29 has centralizer order $3 \cdot 29$. This is impossible since only the prime 2 occurs with multiplicity more than 20 in $|M|$. If $S = p^r$ is elementary abelian, then again the element of order 29 acts fixed point freely unless $p = 3$ or $p = 29$. Now 2 and 3 are primitive roots mod 29, while 5 has order 14 and 7 has order 7, so since the top composition factor L of H already has a 2-part 2^{21} , the possibility of fixed point free action can be ruled out. Also, $p = 29$ is impossible since 29 divides $|M|$ just once and is already contained in the top composition factor $L = \text{Fi}'_{24}$. We are left with the possibility of a central 3-extension of Fi'_{24} , non-split since H is perfect. This can only be the universal covering group $3'\text{Fi}'_{24}$.

Table 9.1 Character values in M

1A	11A	17A	23AB	29A
196883	16	6	3	2

Table 9.2 Character values in $3'\text{Fi}'_{24}$

	1A	11A	17A	23AB	29A
ψ_1	1	1	1	1	1
ψ_{8671}	8671	3	1	0	0
ψ_{57477}	57477	2	0	0	-1
$\psi_{783} + \bar{\psi}_{783}$	1566	4	2	2	0
$\psi_{64584} + \bar{\psi}_{64584}$	129168	6	2	0	2

To deal with the remaining cases Fi'_{24} and $3'\text{Fi}'_{24}$, we determine the possible restrictions of the smallest non-trivial character χ of degree 196883 of M to the universal covering $3'\text{Fi}'_{24}$. The values of χ on some classes of M are given in Table 9.1. The rational characters of $3'\text{Fi}'_{24}$ of degree at most 196883 with their values on the

corresponding classes are as given in Table 9.2 where the last two are faithful while the first three factor through the simple group. Note that we only have to consider rational characters as constituents of the restriction, since χ is rational. The linear system of equations for the coefficients in the restriction has the unique positive solution

$$\chi|_{3 \cdot \text{Fi}'_{24}} = \psi_1 + \psi_{8671} + \psi_{57477} + (\psi_{783} + \bar{\psi}_{783}) + (\psi_{64584} + \bar{\psi}_{64584}).$$

Now $\chi(3B) = 53$, thus comparison with the character table of $3 \cdot \text{Fi}'_{24}$ shows that only 3-classes above $3b$, $3c$ and $3d$ of Fi'_{24} fuse into $3B$ of M . But the structure constant $n(2a, 3bcd, 29a)$ for these 3-classes turns out to vanish in $3 \cdot \text{Fi}'_{24}$. This eliminates the last possible proper subgroup for case (b) and proves $l(\mathbf{C}) = 1$. \square

9.5 The Oddments

These last six sporadic groups do not fit into any convenient family and were therefore baptized in the Atlas.

- Proposition 9.7.** (a) *The class vector $(2A, 5A, 5B)$ of J_1 is rigid.*
 (b) *The class vector $(2B, 4A, 22A)$ of $\text{Aut}(\text{ON})$ is rationally rigid.*
 (c) *The class vector $(2A, 5A, 14A)$ of Ly is rationally rigid.*
 (d) *The class vector $(2A, 5A, 13A)$ of Ru is rationally rigid.*

Proof. For J_1 we have $n(\mathbf{C}) = 5/2$. The maximal subgroups of J_1 with order divisible by 5 are $11:10$, $D_6 \times D_{10}$, $2 \times A_5$ and $L_2(11)$. Factoring the first one by its normal Sylow 11-subgroup one sees that it cannot contain $(2, 5, 5)$ -systems. The same is true for the second, since all elements of order five are contained in the normal Sylow 5-subgroup. In the third case, as elements of order five only occur in the second factor, we would already have $H \leq A_5$. It is easily seen that no proper subgroup of A_5 has a $(2, 5, 5)$ -system, so in this case $H = A_5$. The corresponding structure constant is equal to 1 in A_5 . The last type of maximal subgroups contains two classes of maximal subgroups A_5 . Each of them contributes 1 to the structure constant $n_{L_2(11)}(2a, 5a, 5b) = 2$ in $L_2(11)$, so the contribution from proper subgroups is precisely the one coming from subgroups isomorphic to A_5 . But the number of classes of such subgroups may be computed from the $(2, 3, 5)$ -structure constant of G , since any $(2, 3, 5)$ -triple generates an alternating group A_5 . We have $n_{J_1}(2A, 3A, 5A) = 3/2$, and if this is subtracted from the normalized structure constant $n(\mathbf{C}) = 5/2$, we get $l(\mathbf{C}) = 1$ in part (a).

In case (b) the structure constant $n(\mathbf{C})$ equals 1. The only maximal subgroups of $\text{Aut}(\text{ON})$ different from ON with order divisible by 11 are of type $J_1 \times 2$. But J_1 , hence $J_1 \times 2$, does not contain elements of order four. So $H = \text{Aut}(\text{ON})$, proving part (b).

For $G = \text{Ly}$ we compute $n(\mathbf{C}) = 3/2$. Only the maximal subgroups $G_2(5)$, $3 \cdot \text{McL}:2$, and $2 \cdot A_{11}$ of G have orders divisible by 7. But $G_2(5)$ contains no elements

of order 14. The maximal subgroup $2^{\circ}A_{11}$ is the centralizer of a $2A$ -element, so it intersects both classes $5A, 5B$ of G non-trivially, as can be seen from the powermap. From the centralizer orders in A_{11} it is clear that $5a$ from $2^{\circ}A_{11}$ fuses into $5A$ of G , while $5b$ fuses into $5B$. The group $2^{\circ}A_{11}$ contains just one class of elements of order 14, namely $14a$, and two of order 2, one of them consisting of the central element, and the other containing the preimages of $2b$ of A_{11} in $2^{\circ}A_{11}$. Clearly the $(2, 5, 14)$ -structure constant involving the central involution of $2^{\circ}A_{11}$ vanishes, while the second is found to be equal to

$$n_{2^{\circ}A_{11}}(2b, 5a, 14a) = 1/6.$$

We finally consider the possibility $H \leq 3^{\circ}\text{McL}:2 =: M$. This group is the centralizer of a $3A$ -element, so also contains elements from both $5A$ and $5B$. Again the two classes $5a, 5b$ of M are seen to fuse into $5A, 5B$ respectively. There exists just one class $14a$ of elements of order 14 in M . Since $5a$ and $14a$ lie in 3°McL , only the inner involution class $2a$ of M can contribute to $n_M(2, 5a, 14a)$. One finds $n_M(2a, 5a, 14a) = 1/2$. By Proposition I.5.7 it is clear that not all of $n(\mathbf{C})$ is accounted for in proper subgroups, so $l(\mathbf{C}) = 1$ follows as claimed.

The $(2b, 5a, 14a)$ -system of $2^{\circ}A_{11}$ actually generates a $2^{\circ}A_8$, with centralizer of order six, which explains the $1/6$. This group also occurs as a maximal subgroup in McL , so the contribution from $2^{\circ}A_{11}$ is also contained in the structure constant $1/2$ for the $3^{\circ}\text{McL}:2$, but this is not relevant for the proof.

For $G = \text{Ru}$ the structure constant for \mathbf{C} equals $n(\mathbf{C}) = 28$, so a contribution of 27 has to be shown to come from proper subgroups. Only the maximal subgroups ${}^2\text{F}_4(2)$, $(2^2 \times {}^2\text{B}_2(8)):3$ and $\text{L}_2(25).2^2$ have order divisible by 5 and 13. Clearly the group $(2^2 \times {}^2\text{B}_2(8)):3$ contains elements of order 15, so its 5-elements fuse into class $5B$ of G , which rules out this maximal subgroup. The two involution classes $2a, 2b$ of ${}^2\text{F}_4(2)$ have centralizer order divisible by $2^{11}, 3$ respectively, so both fuse into $2A$ of G . The elements of order 5 in ${}^2\text{F}_4(2)$ are fourth powers of elements of order 20, so fuse into $5A$ of G . (The fusion could also be deduced from the permutation character given in the Atlas.) Hence the contribution from ${}^2\text{F}_4(2)$ to $n(\mathbf{C})$ equals

$$n(2a, 5a, 13a) + n(2b, 5a, 13a) = 1 + 26 = 27.$$

Finally assume $H \leq \text{L}_2(25).2^2$. Then, since the second and third class in \mathbf{C} contain elements of odd order, clearly $H \leq \text{L}_2(25)$. The relevant structure constant in $\text{L}_2(25).2^2$ is calculated as

$$n(2a, 5ab, 13abcdef) = 3,$$

where we have written $5ab$ for $5a \cup 5b$ and similarly for $13abcdef$. As $27 + 3 > n(\mathbf{C})$ this means by Proposition I.5.7 that either $\text{L}_2(25).2^2$ does not intersect one of the three classes, so contributes 0, or that its normal subgroup $\text{L}_2(25)$ already lies in ${}^2\text{F}_4(2)$, and the contribution was already accounted for in the latter group. In either case we get $l(\mathbf{C}) = 28 - 27 = 1$, and the result in case (d) follows. (Actually, the

second possibility holds, since ${}^2F_4(2)$ has a maximal subgroup $L_2(25):2$, but this is not important for the proof.) \square

For the two Janko groups J_3 and J_4 we have to appeal to computer results to verify rigidity:

Proposition 9.8. (a) *The class vector $(2B, 3B, 8B)$ of $\text{Aut}(J_3)$ is rationally rigid.*
 (b) *The class vector $(2A, 4C, 11A)$ of J_4 is rationally rigid.*

Proof. For the automorphism group $J_3:2$ of the group J_3 one verifies that $n(\mathbf{C}) = 1$ from the Atlas. The group H generated by a triple of elements from \mathbf{C} cannot lie inside the maximal subgroup $L_2(16):4$, since all involutions of the latter lie in the normal subgroup of index two. Also, the possibility $2^{1+4}:S_5$ can be excluded, since by the description in the Atlas, elements of order 3 in that group are of $3A$ -type. Next, the order of $19:18$ is not divisible by 8. Assume that H lies in $(3 \times M_{10}):2$. Then the factor group by the almost central 3 also has a $(2, 3, 8)$ generating system. Now two of the A_6 -cosets of $M_{10}:2$ lie in the outer half of $\text{Aut}(J_3)$, and just one of them contains involutions, while only the other one contains elements of order 8. This contradicts the possibility of a non-zero $(2, 3, 8)$ structure constant for $M_{10}:2$. To deal with the remaining cases, we have to use computer results. The permutation characters for the maximal subgroups $2^4:(3 \times A_5).2$, $L_2(17) \times 2$ and $3^5:8.2$ were calculated by Pahlings (1989). It turns out that none of these groups intersect class $8B$. Finally, the character table of $2^{2+4}:(S_3 \times S_3)$ was also determined in loc. cit., and it proves that the $(2B, 3B, 8B)$ -structure constant of that maximal subgroup vanishes. This rules out the last proper subgroup, thus proving rigidity.

The structure constant for $\mathbf{C} = (2A, 4C, 11A)$ in J_4 equals $3/2$. According to Wilson (2017), among the maximal subgroups of J_4 , only $2^{11}:M_{24}$, $2_+^{1+12} \cdot 3 \cdot M_{22}:2$, $11_+^{1+2}:(5 \times 2S_4)$, $U_3(11)$, $M_{22}:2$, $L_2(32):5$ and $L_2(23):2$ have order divisible by 11. Of these, $11_+^{1+2}:(5 \times 2S_4)$ obviously can not possess a $(2, 4, 11)$ -system. The group $L_2(32):5$ contains no elements of order 4, in $L_2(23):2$ all elements of order 4 are squares, while this is not true for elements of $4C$ in J_4 . In $U_3(11):2$, the outer elements of order 4 have centralizer order divisible by 11, hence cannot fuse into $4C$, while the inner ones are again squares. The elements of order 11 in $M_{22}:2$ are of type $11B$ by loc. cit., Cor. 6.2.2. To exclude $2^{11}:M_{24}$, we note that the possible irreducible constituents (χ_1, \dots, χ_{21} in Atlas-notation) of the permutation character on this maximal subgroup all take nonnegative values on $11B$, hence this subgroup has trivial intersection with $11A$. (This also follows from the aforementioned result in loc. cit.) Finally, to exclude the possibility $2_+^{1+12} \cdot 3 \cdot M_{22}:2$ we have to employ the unpublished character table of that group, which was calculated by B. Fischer (see Pahlings (1988)), together with its fusion into J_4 . It turns out that this subgroup contributes exactly $1/2$ to $n(\mathbf{C})$, leaving $l(\mathbf{C}) = 1$. \square

9.6 Galois Realizations for the Sporadic Groups

Collecting the rigidity results of the previous sections we obtain GA-realizations for most sporadic simple groups:

Theorem 9.9. *All sporadic simple groups G with the possible exception of the Mathieu groups M_{23} and M_{24} possess G -realizations over \mathbb{Q} . A class vector \mathbf{C} of $\text{Aut}(G)$ yielding such a realization is given for each case apart from M_{11} in Propositions 9.1–9.8.*

Both M_{23} and M_{24} occur as geometric Galois groups over $\mathbb{Q}(\sqrt{-23})$.

Proof. The Mathieu group M_{11} was treated in Theorem I.6.12 by descent from M_{12} . Now let G be a sporadic group different from M_{11} , M_{23} , M_{24} and J_1 . Then we have proved rational rigidity for the class vector \mathbf{C} of $\text{Aut}(G)$ in Propositions 9.1–9.8. Since these groups have trivial center, they occur as regular Galois groups over $\mathbb{Q}(t)$ by the Basic Rigidity Theorem I.4.8.

If $G = \text{Aut}(G)$ the assertion of the theorem follows immediately. In all other cases we have $(\text{Aut}(G) : G) = 2$. The class vectors all contain two outer classes, so the fixed field L of G in the $\text{Aut}(G)$ -extension $N/\mathbb{Q}(t)$ is ramified at precisely two places. Thus L is a rational function field $L = \mathbb{Q}(u)$, and $N/\mathbb{Q}(u)$ yields a geometric Galois extension with group G .

If $G = J_1$, then $\mathbf{C} = (2A, 5A, 5B)$ is not rational, since $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\sqrt{5})$. But \mathbf{C} is V -symmetric for $V = \langle(23)\rangle$, and this leads to $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$ in this case as well. By the Strong Rigidity Theorem I.4.11 this guarantees the existence of a geometric Galois extension of $\mathbb{Q}(t)$ with group J_1 .

For $G = M_{24}$, the class vector \mathbf{C} satisfies $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(\sqrt{-23})$, and Theorem I.4.8 implies the assertion for that group. The Mathieu group M_{23} may now be obtained by descent from the Galois realization for M_{24} , much the same way as for M_{11} in the proof of Theorem I.6.12. Namely, let K denote the fixed field of M_{23} in the Galois extension $N/\mathbb{Q}(\sqrt{-23}, t)$ with group M_{24} of degree $[K : \mathbb{Q}(\sqrt{-23}, t)] = 24$ over $\mathbb{Q}(\sqrt{-23}, t)$. The permutation types of elements in the three classes in the permutation representation of degree 24 are $(2)^8(1)^8$, $(3)^8$, $(23)(1)$ respectively. This describes the ramification behavior of the three ramified prime divisors $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ in $K/\mathbb{Q}(\sqrt{-23}, t)$, and from the Hurwitz genus formula it now follows that $g(K) = 0$. Since above \mathfrak{P}_3 there lie prime divisors of degree 1, K is a rational function field $K = \mathbb{Q}(\sqrt{-23}, u)$, and $N/\mathbb{Q}(\sqrt{-23}, u)$ yields the required Galois realization. The class vector belonging to this extension can also be deduced from the permutation types in the same way as for M_{11} in Theorem I.6.12. \square

The stronger assertion for $\text{Aut}(G)$ instead of G is of importance in the context of embedding problems treated in Chapter IV. Indeed, from Theorem 9.9 and the definitions we immediately see:

Corollary 9.10. *The sporadic groups different from M_{23} and M_{24} possess GA-realizations over \mathbb{Q} . The Mathieu groups M_{23} and M_{24} possess GA-realizations over $\mathbb{Q}(\sqrt{-23})$.*

A GA-realization over \mathbb{Q} for M_{24} will be proved in Theorem III.7.12.

10 Summary for Simple Groups

For the convenience of the reader and for future use we collect the G- and GA-realizations for finite simple groups proved in this Chapter.

10.1 Galois Realizations over \mathbb{Q}^{ab}

The picture for G-realizations of simple groups over \mathbb{Q}^{ab} is almost complete:

Theorem 10.1. *The finite simple groups possesses G-realizations over \mathbb{Q}^{ab} except possibly the following exceptional groups of Lie type in characteristic 2:*

$$\begin{aligned} {}^2B_2(2^{2m+1}), m \geq 2, & \quad {}^2F_2(2^{2m+1}), m \geq 1, \quad E_6(2^{2m}), m \geq 0, \\ {}^2E_6(2^{2m+1}), m \geq 0, & \quad E_7(2^m), m \geq 1, \quad E_8(2^m), m \geq 1. \end{aligned}$$

Proof. Theorem I.5.3 proves a G-realization for A_n , $n \geq 5$. A G-realization for $L_n(q)$ is given in Corollary 1.5, for $U_n(q)$ in Theorem 3.2, for $S_{2n}(q)$ in Theorem 3.4, for $O_{2n+1}(q)$ in Theorem 3.7, for $O_{2n}^+(q)$ in Theorems 3.11 and 3.13, and for $O_{2n}^-(q)$ in Theorem 3.15.

For the exceptional groups of Lie type ${}^2G_2(3^{2m+1})$ the G-realization was constructed in Theorem 4.5, for $G_2(q)$ in Theorem 4.7, for ${}^3D_4(q)$ in Theorem 4.9, for ${}^2B_2(8)$ in Theorem 4.10 and for ${}^2F_4(2)'$ in Theorem 4.11. For $F_4(q)$ the result can be found in Theorem 5.5, for $E_6(q)$ with $q \neq 2^{2m}$ in Corollary 5.8 and Theorem 5.14, for ${}^2E_6(q)$ with $q \neq 2^{2m+1}$ in Theorems 5.11 and 5.15, for $E_7(q)$ with odd q in Corollary 5.18, for $E_8(q)$ in Theorem 5.20. Finally the assertion for the sporadic groups is contained in Theorem 9.9. \square

Theorem 10.2. *The following finite simple groups possess GA-realizations over the field \mathbb{Q}^{ab} .*

- (a) *The non-abelian simple alternating groups A_n .*
- (b) *The groups of Lie type $G(p)$ for $2 < p \in \mathbb{P}$ with the possible exception ${}^3D_4(p)$.*
- (c) *The groups $S_{2n}(2)$, $O_{2n}^+(2)$, $O_{2n}^-(2)$.*
- (d) *The sporadic simple groups.*

Proof. The GA-realizations used in the theorem are contained in the following results: Corollaries I.5.4 and I.9.8 prove GA-realizations for A_n for $n \neq 6$ respectively $n = 6$ over \mathbb{Q} and hence over \mathbb{Q}^{ab} .

GA-realizations for the groups $L_n(p)$ and $U_n(p)$ were constructed in Corollary 6.6. Using $\text{Aut}(O_{2n+1}(p)) = SO_{2n+1}(p)$ we obtain GA-realizations of $O_{2n+1}(p)$ over \mathbb{Q}^{ab} from Theorem 3.7. The corresponding result for $S_{2n}(p)$ follows from Theorem 3.4 since $\text{Aut}(S_{2n}(p)) = \text{PCSp}_{2n}(p)$ for $(n, p) \neq (2, 2)$. GA-realizations for $O_{2n}^+(p)$ with $n \geq 5$ are obtained from Theorem 3.11 for $p \neq 2$

and Theorem 3.13 for $p = 2$, since all automorphisms of $O_{2n}^+(p)$ are induced by $\text{CO}_{2n}^+(p)$. The case $O_8^+(p)$ with the exceptional graph automorphism of order 3 was treated in Theorem 7.10(b). Correspondingly, we have a GA-realization for $O_{2n}^-(p)$ and $n \geq 4$ over \mathbb{Q}^{ab} from Theorem 3.15 since here again all automorphisms of $O_{2n}^-(p)$ are induced by $\text{CO}_{2n}^-(p)$. (The graph-field automorphism is already realized inside the conformal group.)

A GA-realization for ${}^2G_2(3) \cong \text{Aut}(L_2(8))$ was obtained in Example I.8.3. Theorems 4.7, 8.1 and 8.2 give GA-realizations for $G_2(p)$, for $F_4(p)$ it follows from Theorem 5.5 since $\text{Out}(F_4(p)) = 1$ for $p \neq 2$. GA-realizations over \mathbb{Q}^{ab} for $E_6(p)$ with odd p and ${}^2E_6(p)$ with odd p were obtained in Corollary 5.10 and Theorem 5.12. The result for $E_7(p)$ follows from Theorem 5.18 because $\text{Aut}(E_7(p)) = E_7(p)_{\text{ad}}$. Finally for $E_8(p)$ the result follows from Theorem 5.20 since $\text{Out}(E_8(p)) = 1$.

By Theorem 9.9 and Corollary 9.10 all sporadic groups apart from M_{23} and M_{24} have GA-realizations over \mathbb{Q} and the latter two exceptions at least over $\mathbb{Q}(\sqrt{-23})$ since their outer automorphism groups are trivial. This completes the proof of the theorem. \square

10.2 Galois Realizations over \mathbb{Q}

Most of the known G-realizations of finite simple groups over \mathbb{Q} are in fact GA-realizations, so we just collect the latter (including a GA-realization for M_{24} which will be proved in Theorem III.7.12):

Theorem 10.3. *The following finite simple groups possess GA-realizations over the field \mathbb{Q} .*

(a) *The non-abelian simple alternating groups A_n .*

(b) *The linear groups $L_n(p)$ for $\gcd(n, p-1) = 1$, $p > 3$ and $p \not\equiv -1 \pmod{12}$, and for $\gcd(n, p-1) = 2$, $n \equiv 2 \pmod{4}$ and $p \equiv 5 \pmod{8}$, or $n \equiv 0 \pmod{4}$ and $p \equiv 7 \pmod{12}$.*

(c) *The unitary groups $U_n(p)$ for $\gcd(n, p+1) = 1$, $p > 2$ and $p \not\equiv 1 \pmod{12}$, and for $\gcd(n, p+1) = 2$, $n \equiv 2 \pmod{4}$ and $p \equiv 3 \pmod{8}$, or $n \equiv 0 \pmod{4}$ and $p \equiv 5 \pmod{12}$.*

(d) *The symplectic groups $S_{2n}(p)$ for odd primes $p \not\equiv \pm 1 \pmod{24}$, $p \nmid n$, or for $p = 2$.*

(e) *The orthogonal groups $O_{2n+1}(p)$ for $n \geq 1$ and odd primes $p \not\equiv \pm 1 \pmod{24}$.*

(f) *The orthogonal groups $O_{2n+1}(p^2)$ for odd primes $p \equiv \pm 2 \pmod{5}$.*

(g) *The orthogonal groups $O_{2n}^+(p)$ for $p = 2$, or for $n \geq 3$ odd and $p \equiv 3 \pmod{8}$ or $p \equiv 7 \pmod{12}$, $p \nmid n$.*

(h) *The orthogonal groups $O_{2n}^-(p)$ for $p = 2$, or for $n \geq 3$ odd and $p \equiv 5 \pmod{12}$, or $n \geq 6$ even and $p \equiv 3 \pmod{8}$, or $n \equiv 2 \pmod{4}$ and $p \equiv \pm 2 \pmod{5}$.*

- (i) *The orthogonal groups $O_8^+(p)$ for $p \equiv \pm 2 \pmod{5}$, $p \equiv \pm 2, \pm 3 \pmod{7}$.*
- (j) *The groups $G_2(p)$.*
- (k) *The groups $F_4(p)$ for $p \geq 5$.*
- (l) *The groups $E_6(p)$ for $p \equiv 4, 5, 6, 9, 16, 17 \pmod{19}$, $p \equiv -1 \pmod{3}$.*
- (m) *The groups ${}^2E_6(p)$ for $p \equiv 2, 3, 10, 13, 14, 15 \pmod{19}$, $p \not\equiv -1 \pmod{3}$, $p > 3$.*
- (n) *The groups $E_8(p)$ for $p \geq 7$.*
- (o) *The sporadic simple groups with the possible exception of M_{23} .*

Proof. This was shown in Corollaries I.5.4 and I.9.8 for the alternating groups. Part (b) is contained in Theorems 6.7(a) and 6.8(a), the assertion (c) is proved in Theorems 6.7(b) and 6.8(b). Part (d) was shown in Theorems 7.2 and 7.3, part (e) in Theorem 7.4, part (f) in Theorem 7.5, part (g) in Theorems 7.6, 7.8 and 7.11, part (h) in Theorems 7.7 and 7.8, part (i) in Theorem 7.11. For the exceptional groups, the result is contained in Theorems 8.1, 8.2 and 6.8 for part (j), in Theorem 8.4 for part (k), in Corollary 8.6 for part (l), in Theorem 8.7 for part (m), in Theorem 8.9 for part (n) and in Corollary 9.10 for the sporadic groups except M_{24} . A GA-realization over \mathbb{Q} for M_{24} will be proved in Theorem III.7.12. \square

GA-realizations for groups $L_2(p^2)$ are implicitly contained in Theorem 10.3(f) because of $L_2(p^2) \cong O_3(p^2)$. The group $L_2(8)$ is handled in Chapter I, Example 8.3.

Further G- and GA-realizations of classical simple groups of Lie type are obtained in the next Chapter III.10, and Chapter IV.4.3, respectively.

III Action of Braids

In this chapter we pursue an approach to the solution of the inverse problem of Galois theory using several variables, which building on ideas of Hurwitz (1891), goes back to results of Fried (1977, 1984) and Fried and Biggers (1982). A variant more suitable for the realization of groups as Galois groups was proposed by Matzat (1989) and subsequently developed in papers of Matzat (1991a) and in geometric context, of Fried and Völklein (1991) (see also the survey article Matzat (1991c)). This version will be presented here.

The advantage of this approach consists in the fact that the rather restrictive group theoretic rigidity criterion in the case of one variable is replaced by a much weaker rigidity condition on braid orbits. But this then only implies the regularity of the field of definition over \mathbb{Q} . The rationality needed for an application of Hilbert's irreducibility theorem must therefore be guaranteed by additional arithmetic conditions.

The first five paragraphs contain the basic material of the chapter developed in the papers mentioned above. In Paragraphs 1 and 2 we collect the necessary group theoretic results on braid groups and braid actions. In Paragraph 3 the rigidity theorems of Chapter I are transferred to Galois realizations of several variables and used to construct cyclic polynomials in Paragraph 4. Paragraph 5 finally contains the basic investigations on the rationality of fields of definition, a result concerning rational translation, and ends with a criterion for GA-realizations in several variables.

In the following three paragraphs we consider questions of specialization and further results. The specialization theorem in Paragraph 6 yields the connection with Chapter I by characterizing Galois realizations in one variable as specializations by unramified rational places of Galois realizations in several variables. This leads in particular to the solution of the inverse problem over Hilbertian PAC-fields of characteristic zero (Fried and Völklein (1991)). In Paragraph 7 we treat the additional use of geometric automorphisms of Matzat (1991a) and in Paragraph 8 the relevance of the decomposition groups, which was first studied in loc. cit. and continued in Matzat (1993). Here the two biggest Mathieu groups serve as illustrating examples.

The last two paragraphs present the Katz algorithm with some applications. Paragraph 9 contains an algebraic version due to Dettweiler and Reiter (2000) of the Katz algorithm for rigid local systems introduced in Katz (1996) with complete proofs. With this it is possible to connect linearly rigid generating systems of linear groups algorithmically with linear rigid systems of GL_n with small n for example over finite fields \mathbb{F}_q . By compatibility with the braid action the same holds for linearly rigid braid orbits. In the applications in Paragraph 10, starting with rationally (braid) rigid generating systems of subgroups of $\mathrm{GL}_1(q)$ or $\mathrm{GL}_2(q)$ we obtain rationally linear (braid) rigid generating systems for many classical linear groups over \mathbb{Q} . This complements the results of Theorem II.10.3 in particular for higher prime powers q .

1 Braid Groups

In this first paragraph we introduce the Artin and the Hurwitz braid groups as fundamental groups and collect some of their properties which will be needed later on. We omit the proofs which can already be found in the monograph of Birman (1975).

1.1 The Artin Braid Group

For an arbitrary topological space \mathcal{X} we call

$$\mathcal{X}_r^{\cdot} := \{(x_1, \dots, x_r) \in \mathcal{X}^r \mid x_i \neq x_j \text{ for } i \neq j\}$$

the r -fold incomplete product of \mathcal{X} . On this the symmetric group S_r acts in a natural way by transformation of coordinates. The orbit space of \mathcal{X}_r^{\cdot} under this action

$$\tilde{\mathcal{X}}_r^{\cdot} := \mathcal{X}_r^{\cdot}/S_r$$

is called the r -fold incomplete symmetric product of \mathcal{X} .

If for \mathcal{X} we choose the affine line $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$ (with the topology of the Euclidean plane), then the fundamental group of \mathcal{X}_r^{\cdot} with respect to the base point $\mathcal{P}_0 = (1, \dots, r) \in \mathcal{X}_r^{\cdot}$ is called the pure (or unpermuted) Artin braid group B_r and the fundamental group of $\tilde{\mathcal{X}}_r^{\cdot}$ with respect to the S_r -orbit $\tilde{\mathcal{P}}_0$ of \mathcal{P}_0 the (full) Artin braid group \tilde{B}_r :

$$B_r := \pi_1^{\text{top}}(\mathbb{A}^1(\mathbb{C})_r^{\cdot}; \mathcal{P}_0), \quad \tilde{B}_r := \pi_1^{\text{top}}(\tilde{\mathbb{A}}^1(\mathbb{C})_r^{\cdot}; \tilde{\mathcal{P}}_0). \quad (1.1)$$

Obviously B_r is a normal subgroup of \tilde{B}_r with $\tilde{B}_r/B_r \cong S_r$.

Every element $\beta \in \tilde{B}_r$ possesses a unique lifting to a path b in \mathcal{X}_r^{\cdot} with $b(0) = \mathcal{P}_0 = (1, \dots, r)$ and $b(1) = (1^\omega, \dots, r^\omega)$ for an $\omega \in S_r$. The coordinate functions of $b(t) = (b_1(t), \dots, b_r(t))$ then form a geometric braid in the sense of Artin (1925). With the elements β_i of \tilde{B}_r depicted in Figure 1.1 we have:

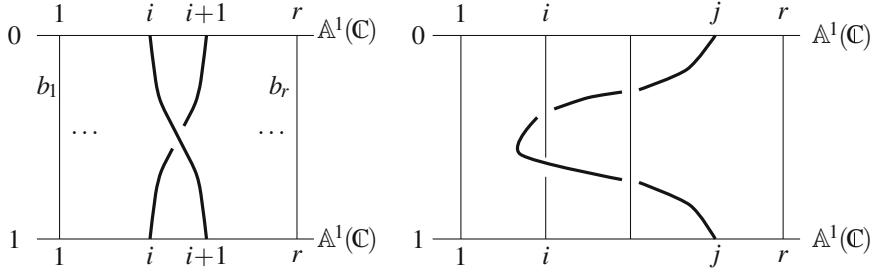
Theorem 1.1 (Artin (1925)). (a) *The full Artin braid group \tilde{B}_r is generated by $\beta_1, \dots, \beta_{r-1}$ subject to the relations*

$$\beta_i \beta_j = \beta_j \beta_i \text{ for } 1 \leq i < j \leq r-1 \text{ and } j \neq i+1,$$

$$\beta_i \beta_{i+1} \beta_i = \beta_{i+1} \beta_i \beta_{i+1} \text{ for } 1 \leq i \leq r-2.$$

(b) *The pure Artin braid group B_r is generated in \tilde{B}_r by the elements*

$$\beta_{ij} := (\beta_i^2)^{\beta_{i+1}^{-1} \cdots \beta_{j-1}^{-1}} = (\beta_{j-1}^2)^{\beta_{j-2} \cdots \beta_i} \text{ for } 1 \leq i < j \leq r.$$

**Fig. 1.1** Artin braids $\beta_i \dots$... and β_{ij}

The proof can be found in Birman (1975), Thm. 1.8 with Lemma 1.8.2, where moreover defining relations are given for the pure Artin braid group (see also Hansen (1989), Appendix 1, for a correction of the braid relations).

From the presentation of \tilde{B}_r in Theorem 1.1 we immediately obtain a canonical epimorphism

$$q_r : \tilde{B}_r \rightarrow S_r, \quad \beta_i \mapsto (i, i+1) \quad (1.2)$$

with $\ker(q_r) = B_r$. Now let

$$\tilde{B}_r^* := q_r^{-1}(S_{r-1}) = \{\beta \in \tilde{B}_r \mid (r)q_r(\beta) = r\} \quad (1.3)$$

denote the preimage of the stabilizer S_{r-1} of r under q_r and

$$F_{r-1} := \langle \gamma_1, \dots, \gamma_{r-1} \rangle \text{ with } \gamma_i := \beta_{ir}. \quad (1.4)$$

Thus we obtain the fundamental structure theorem for the Artin braid group:

Theorem 1.2 (Chow (1948)). *For $r \geq 3$ we have:*

- (a) F_{r-1} is a free normal subgroup of \tilde{B}_r^* of rank $r-1$.
- (b) \tilde{B}_r^* decomposes into a semidirect product of F_{r-1} with \tilde{B}_{r-1} , where the action of the generators $\beta_1, \dots, \beta_{r-2}$ of \tilde{B}_{r-1} on F_{r-1} is given componentwise by

$$(\gamma_1, \dots, \gamma_{r-1})^{\beta_i} = (\gamma_1, \dots, \gamma_{i-1}, \gamma_i \gamma_{i+1} \gamma_i^{-1}, \gamma_i, \gamma_{i+2}, \dots, \gamma_{r-1}). \quad (1.5)$$

The proof of this statement can either be found in the original paper or in the proof of Lemma 1.8.2 and Cor. 1.8.3 in Birman (1975). As a consequence we obtain the following result, which was also proved by Chow (1948) (see also Birman (1975), Cor. 1.8.4):

Corollary 1.3. *For $r \geq 3$ the center of the Artin braid group \tilde{B}_r is the infinite cyclic group generated by $(\beta_1 \cdots \beta_{r-1})^r$.*

Remark. In the case $r = 2$ we have $\tilde{B}_2 = \langle \beta_1 \rangle = \mathcal{Z}(\tilde{B}_2)$.

We defined the Artin braid groups as fundamental groups of the uncomplete symmetric products of \mathbb{C} , respectively of the space of regular orbits under S_r on \mathbb{C}^r . The corresponding construction may be applied to all finite Coxeter groups (see for example Suzuki (1982), Ch. 3, §4, or Aschbacher (1986), §29), and leads to groups having similar properties to the Artin braid group. These have entered the literature under the name of Artin groups (see Brieskorn and Saito (1972)).

1.2 The Hurwitz Braid Group

For the definition of the Artin braid groups the topological space \mathcal{X} was chosen to be the affine line $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$, and the base point $\mathcal{P}_0 = (1, \dots, r)$. If instead we replace it by the projective line $\mathbb{P}^1(\mathbb{C}) = \hat{\mathbb{C}}$ (with the topology of the sphere in 3-dimensional Euclidean space) and again use $\mathcal{P}_0 = (1, \dots, r)$ by identifying the points in $\mathbb{P}^1(\mathbb{C})$ with the elements of $\hat{\mathbb{C}}$, then we obtain the *pure* (or *unpermuted*) *Hurwitz braid group* H_r and the (*full*) *Hurwitz braid group* \tilde{H}_r :

$$H_r := \pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C})_r; \mathcal{P}_0), \quad \tilde{H}_r := \pi_1^{\text{top}}(\tilde{\mathbb{P}}^1(\mathbb{C})_r; \tilde{\mathcal{P}}_0). \quad (1.6)$$

As above these satisfy $H_r \triangleleft \tilde{H}_r$ with $\tilde{H}_r / H_r \cong S_r$ if $\tilde{\mathcal{P}}_0$ is chosen to be the S_r -orbit of \mathcal{P}_0 .

In analogy to the Artin braid group the elements of \tilde{H}_r can be represented as geometric braids, but now between two spheres (see Figure 1.2). The right hand part of Figure 1.2 also shows that in addition to the relations of the Artin braid group, which are called *braid relations*, at least one further relation $\beta_1 \cdots \beta_{r-1} \beta_{r-1} \cdots \beta_1 = 1$ holds in \tilde{H}_r .

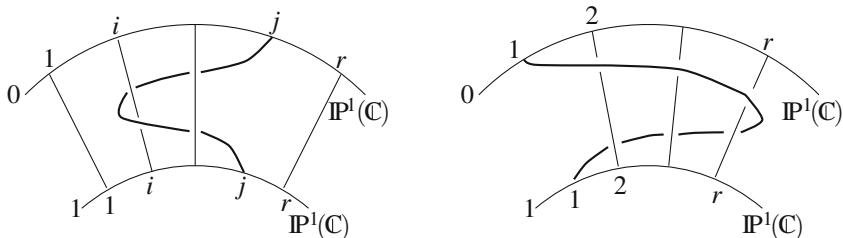


Fig. 1.2 Hurwitz braids $\beta_{ij} \dots$

... and $\beta_1 \cdots \beta_{r-1} \beta_{r-1} \cdots \beta_1$

Theorem 1.4 (Fadell and Van Buskirk (1962)). *Let N_r be the normal subgroup of \tilde{B}_r generated by $\beta_1 \cdots \beta_{r-1} \beta_{r-1} \cdots \beta_1 \in \tilde{B}_r$. Then we have*

$$\tilde{H}_r \cong \tilde{B}_r / N_r \text{ and } H_r \cong B_r / N_r.$$

In particular a presentation of the full Hurwitz braid group resp. the pure Hurwitz braid group is obtained from the one of \tilde{B}_r resp. B_r in Theorem 1.1 by addition of the relation

$$\beta_1 \cdots \beta_{r-1} \beta_{r-1} \cdots \beta_1 = 1. \quad (1.7)$$

Calling (1.7) (which coincides with $\beta_{12} \cdots \beta_{1r} = 1$) or more generally the relations $\beta_{1j} \cdots \beta_{j-1,j} \beta_{j,j+1} \cdots \beta_{jr} = 1$ *sphere relations*, we get the more general

Corollary 1.5. *The normal subgroup N_r of \tilde{B}_r is generated by the sphere relations:*

$$N_r = \langle \beta_{1j} \cdots \beta_{j-1,j} \beta_{j,j+1} \cdots \beta_{jr} \mid 1 < j < r \rangle. \quad (1.8)$$

The proof for these results closely follows the one of Theorem 1.1 (see for example Birman (1975), Thm. 1.11). In contrast, the structure theorem for the Hurwitz braid group corresponding to Theorem 1.2 was not included in the monograph of Birman. For that, in analogy to (1.2)–(1.4), let

$$q_r : \tilde{H}_r \rightarrow S_r, \quad \beta_i \mapsto (i, i+1) \quad (1.9)$$

denote the canonical epimorphism with kernel H_r ,

$$\tilde{H}_r^* := q_r^{-1}(S_{r-1}) = \{\beta \in \tilde{H}_r \mid (r)q_r(\beta) = r\} \quad (1.10)$$

the preimage of S_{r-1} under q_r and

$$G_{r-1} := \langle \gamma_1, \dots, \gamma_{r-1} \rangle \quad \text{with} \quad \gamma_i = \beta_{ir}. \quad (1.11)$$

Theorem 1.6 (Gillette and Van Buskirk (1968)). *For $r \geq 4$ we have:*

- (a) G_{r-1} is a free normal subgroup of \tilde{H}_r^* of rank $r-2$ with the defining relation $\gamma_1 \cdots \gamma_{r-1} = 1$.
- (b) \tilde{H}_r^* is an extension of G_{r-1} by \tilde{H}_{r-1} , where the action of the generators $\beta_1, \dots, \beta_{r-2}$ of \tilde{H}_{r-1} on G_{r-1} is given by the following formula (up to simultaneous conjugation in G_{r-1})

$$[\gamma_1, \dots, \gamma_{r-1}]^{\beta_i} = [\gamma_1, \dots, \gamma_{i-1}, \gamma_i \gamma_{i+1} \gamma_i^{-1}, \gamma_i, \gamma_{i+2}, \dots, \gamma_{r-1}]. \quad (1.12)$$

Proof. The sphere relation for $j = r$ gives

$$\beta_{1r} \cdots \beta_{r-1,r} = \gamma_1 \cdots \gamma_{r-1} = 1. \quad (1.13)$$

Hence a presentation of G_{r-1} is obtained from one of F_{r-1} by addition of the relation (1.13). According to Theorem 1.2(a) the group G_{r-1} is thus free of rank $r-2$.

Being the image of F_{r-1} under the canonical surjection ν from \tilde{B}_r^* onto \tilde{H}_r^* , G_{r-1} is a normal subgroup of \tilde{H}_r^* with factor group isomorphic to $\nu(\tilde{B}_{r-1}) = \tilde{H}_{r-1}$. Since the action of \tilde{B}_{r-1} on F_{r-1} commutes with ν , (1.12) follows from (1.5). \square

Remark. For $r \leq 3$ the Hurwitz braid groups \tilde{H}_r are finite and therefore require a separate treatment. We have

$$\tilde{H}_2 = \langle \beta_1 \mid \beta_1^2 = 1 \rangle \cong Z_2, \quad (1.14)$$

$$\tilde{H}_3 = \langle \beta_1, \beta_1\beta_2 \mid \beta_1^2 = (\beta_1\beta_2\beta_1)^2 = (\beta_1\beta_2)^3 \rangle \cong Z_3 \rtimes Z_4 \quad (1.15)$$

and hence $H_2 = 1$ and $H_3 \cong Z_2$.

With the help of the Schreier transversal

$$\theta_i := \beta_{r-1} \cdots \beta_i \quad \text{for } i = 1, \dots, r$$

of \tilde{H}_r in \tilde{H}_r (resp. \tilde{B}_r in \tilde{B}_r) we obtain, using the Reidemeister rewriting process (see Lyndon and Schupp (1977), Ch. II, Prop. 4.1), the following simple and useful presentation of \tilde{H}_r :

Proposition 1.7. *For $r \geq 3$ the group \tilde{H}_r is generated by $\beta_1, \dots, \beta_{r-2}$. The braid relations of \tilde{B}_{r-1} together with*

$$(\beta_1 \cdots \beta_{r-2})^{2(r-1)} = 1$$

constitute a complete set of defining relations.

A proof for this assertion and for the subsequent Corollary 1.8, which also originates from Gillette and Van Buskirk (1968), is obtained from the proof of Lemma 4.2.3 in Birman (1975).

Corollary 1.8. *For $r \geq 3$ the center of the Hurwitz braid group \tilde{H}_r has order 2 and is generated by*

$$\iota_r := (\beta_1 \cdots \beta_{r-1})^r = (\beta_1 \cdots \beta_{r-2})^{r-1}. \quad (1.16)$$

The factor group $\tilde{H}_r / \mathcal{Z}(\tilde{H}_r)$ is known under the name of *mapping class group* of the r -pointed sphere (see Birman (1975), Thm. 4.5). For later use we mention the following structure result for the first infinite Hurwitz braid group \tilde{H}_4 and for $\tilde{H}_4 / \mathcal{Z}(\tilde{H}_4)$ (see Birman (1975), Lemma 5.4.1 and 5.4.3):

Proposition 1.9. *\tilde{H}_4 has a quaternion group Q_8 of order 8 as normal subgroup with*

$$\tilde{H}_4 / Q_8 = \mathrm{PSL}_2(\mathbb{Z}) \quad \text{for} \quad Q_8 = \langle \beta_1\beta_3^{-1}, (\beta_1\beta_2\beta_3)^2 \rangle. \quad (1.17)$$

The induced group extension of $\tilde{H}_4 / \mathcal{Z}(\tilde{H}_4)$ splits:

$$\tilde{H}_4 / \mathcal{Z}(\tilde{H}_4) \cong Z_2^2 \rtimes \mathrm{PSL}_2(\mathbb{Z}). \quad (1.18)$$

1.3 The Pure Hurwitz Braid Group

The fundamental difference between the structure theorem for the Artin braid group and the Hurwitz braid group lies in the fact that the underlying exact sequence splits in the case of the Artin braid group. This is impossible for the Hurwitz braid group,

since \tilde{H}_r does not even contain subgroups isomorphic to \tilde{H}_{r-1} (see Gillette and Van Buskirk (1968), Thm. 4.12). Nevertheless the corresponding result for the pure Hurwitz braid group remains true. The first proof of this result used mainly topological methods (Fadell (1962)); the purely algebraic proof given here was communicated to us by L. Schneps.

Theorem 1.10 (Fadell and Van Buskirk (1962)). *For $r \geq 4$ the pure Hurwitz braid group H_r is a semidirect product of the free normal subgroup G_{r-1} with H_{r-1} .*

Proof. Since the sphere relation makes it impossible to embed H_{r-1} canonically into H_r , we will denote the elements of B_{r-1} and H_r by β_{ij} and the corresponding elements of B_{r-2} and H_{r-1} by $\tilde{\beta}_{ij}$. Furthermore, we let

$$H_r^* := \langle \beta_{ij} \in H_r \mid 1 \leq i < j \leq r-1, (i, j) \neq (1, 2) \rangle,$$

$$B_{r-1}^* := \langle \beta_{ij} \in B_{r-1} \mid 1 \leq i < j \leq r-1, (i, j) \neq (1, 2) \rangle.$$

According to Corollary 1.5 upon replacing $\beta_{ij} \in H_r^*$ by $\beta_{ij} \in B_{r-1}^*$ the groups H_r^* and B_{r-1}^* then possess identical presentations, which shows

$$H_r^* \cong B_{r-1}^*. \quad (1.19)$$

In particular H_r^* contains no non-trivial elements of finite order by Theorem 1.2. The generator ι_r of the center of H_r then satisfies

$$\iota_r = (\beta_1 \cdots \beta_{r-2})^{r-1} = \beta_{12}(\beta_{13}\beta_{23}) \cdots (\beta_{1,r-1} \cdots \beta_{r-2,r-1}),$$

thus β_{12} lies in the group generated by $\mathcal{Z}(H_r)$ and H_r^* , yielding $H_r = \langle H_r^*, \mathcal{Z}(H_r) \rangle$. As ι_r is of order 2, we moreover have $H_r^* \cap \mathcal{Z}(H_r) = 1$, so that

$$H_r = H_r^* \times \mathcal{Z}(H_r). \quad (1.20)$$

By (1.19) and (1.20) the inclusion $\varphi^* : B_{r-2}^* \rightarrow B_{r-1}^*$ can be extended to a monomorphism

$$\varphi : H_{r-1} \cong B_{r-2}^* \times \mathcal{Z}(H_{r-1}) \rightarrow B_{r-1}^* \times \mathcal{Z}(H_r) \cong H_r$$

by sending the non-trivial central element $\iota_{r-1} = \tilde{\iota}_r$ onto ι_r . Composing φ with the canonical projection

$$\psi : H_r \rightarrow H_{r-1}, \quad \beta \mapsto \tilde{\beta} = \beta G_{r-1}$$

we obtain for $(\tilde{\beta}^*, \tilde{\tau}) \in H_r^* \times \mathcal{Z}(H_r)$ with $\tilde{\beta}^* \in H_{r-1}^*$ and $\tilde{\tau} \in \{\tilde{\iota}_r, 1\}$

$$(\psi \circ \varphi)(\tilde{\beta}^*, \tilde{\tau}) = \psi(\beta^*, \tau) = \beta^* \tau G_{r-1} = \tilde{\beta}^* \tilde{\tau}$$

and thus $\psi \circ \varphi = \text{Id}_{H_{r-1}}$. Consequently we have $G_{r-1} \cap \varphi(H_{r-1}) = 1$ and also $H_r = \langle G_{r-1}, \varphi(H_{r-1}) \rangle$, which finally implies

$$H_r = G_{r-1} \rtimes \varphi(H_{r-1}) \cong G_{r-1} \rtimes H_{r-1}. \quad \square$$

1.4 The Word Problem

For an arbitrary group G let \mathcal{O}_G denote the system of normal subgroups of finite index:

$$\mathcal{O}_G := \{O \triangleleft G \mid (G : O) < \infty\}. \quad (1.21)$$

An arbitrary normal subgroup U of G is called a *thick normal subgroup* if

$$\mathcal{O}_U^G := \{O \cap U \mid O \in \mathcal{O}_G\} \quad (1.22)$$

constitutes a cofinal system in \mathcal{O}_U , i.e., if for any $O \in \mathcal{O}_U$ there exists a $\tilde{O} \in \mathcal{O}_U^G$ with $\tilde{O} \leq O$.

Thick normal subgroups are useful for example for inductive proofs of residual finiteness. Namely, we have the

Proposition 1.11. *If the group G possesses a residually finite thick normal subgroup U with residually finite factor group G/U , then G itself is residually finite.*

Proof. Let

$$K := \bigcap_{O \in \mathcal{O}_G} O.$$

Then since U is residually finite and \mathcal{O}_U^G is cofinal in \mathcal{O}_U we have

$$K \cap U = \bigcap_{O \in \mathcal{O}_G} (O \cap U) = \bigcap_{O_U \in \mathcal{O}_U^G} O_U = 1.$$

Now let $\bar{G} := G/U$ with canonical epimorphism $\kappa : G \rightarrow \bar{G}$, and $\bar{K} := \kappa(K)$. Then for all $\bar{O} \in \mathcal{O}_{\bar{G}}$ the inverse image $\kappa^{-1}(\bar{O})$ is normal in G of finite index and by definition contains K . By the residual finiteness of \bar{G} it now follows that

$$\bar{K} \leq \bigcap_{\bar{O} \in \mathcal{O}_{\bar{G}}} \bar{O} = 1$$

and hence $K \leq U$, which together with $K \cap U = 1$ finally yields $K = 1$. \square

To apply this result to the Hurwitz braid group, one first shows the following result, which also proves useful in a different context.

Proposition 1.12. *The group G_{r-1} is a thick normal subgroup of \tilde{H}_r and therefore also of the pure Hurwitz braid group H_r .*

Proof. Let first $G = H_r$ and $U = G_{r-1}$. Then from Theorem 1.10 we know $G \cong U \rtimes H$ with $H \cong H_{r-1}$. Since U is a finitely generated normal subgroup of G , the group

$$O_U := \bigcap_{\sigma \in G} O^\sigma$$

has finite index in U for any $O \in \mathcal{O}_U$ (Lyndon and Schupp (1977), Ch. IV, Thm. 4.7), and hence is an element of \mathcal{O}_U satisfying $O_U \triangleleft G$. For any $O_H \in \mathcal{O}_H$ the group $\langle O_U, O_H \rangle = O_U \rtimes O_H$ has finite index in G , thus it follows that

$$O_G := \bigcap_{\sigma \in G} (O_U \rtimes O_H)^\sigma \in \mathcal{O}_G$$

with $O_G \cap U = O_U$. We deduce that $O \supseteq O_U \in \mathcal{O}_U^G$, which shows that \mathcal{O}_U^G is a cofinal subsystem of \mathcal{O}_U .

Now G has finite index $(r-1)!$ in $\tilde{G} := \tilde{H}_r$, hence for all $O_U \in \mathcal{O}_U^G$ it follows that

$$\tilde{O} := \bigcap_{\sigma \in \tilde{G}} O_U^\sigma \in \mathcal{O}_{\tilde{U}}^{\tilde{G}}.$$

Thus $\mathcal{O}_{\tilde{U}}^{\tilde{G}}$ also constitutes a cofinal subsystem of \mathcal{O}_U . \square

From Propositions 1.11 and 1.12 we may now deduce the main result of this section.

Theorem 1.13. *The full Hurwitz braid group \tilde{H}_r is a finitely generated residually finite group.*

Proof. The pure Hurwitz braid group H_r is finite for $r \leq 3$ and by Theorem 1.6 for $r \geq 4$ possesses a free normal subgroup G_{r-1} of rank $r-2$ with $H_r/G_{r-1} \cong H_{r-1}$. Being a free group, G_{r-1} is residually finite (see for example Lyndon and Schupp (1977), Ch. III, Prop. 7.11 with supplement on p. 195). By Proposition 1.12, G_{r-1} is hence a residually finite thick normal subgroup of H_r . Thus at least for $r=4$ all assumptions in Proposition 1.11 are satisfied, proving that H_4 is residually finite. Induction on r then proves the result for all $r \geq 4$.

Since $(\tilde{H}_r : H_r) < \infty$, the group H_r is a thick normal subgroup of \tilde{H}_r , which again with Proposition 1.11, now applied to $G = \tilde{H}_r$ and $U = H_r$ entails the residual finiteness of \tilde{H}_r . \square

As a corollary to Theorem 1.13, using a result of McKinsey (Lyndon and Schupp (1977), Ch. IV, Thm. 4.6) we obtain a nice consequence which was first proved by Fadell and Van Buskirk (1962) by different methods:

Corollary 1.14. *The Hurwitz braid group \tilde{H}_r has solvable word problem.*

In a completely analogous way one may prove the solvability of the word problem for the Artin braid groups (compare with Artin (1925, 1947)).

2 Profinite Braid Groups

In analogy to Section I.1.2, the universal covering of the incomplete (symmetric) product of $\mathbb{P}^1(\mathbb{C})$ defines a Galois extension, whose structure reflects that of the Hurwitz braid groups. As in the case of one variable the canonical generators of the braid group play the role of generators of inertia groups.

2.1 The Hurwitz Braid Group as Galois Group

For a field k and an algebraic variety \mathcal{X} let $k(\mathcal{X})$ denote the field of k -valued functions on \mathcal{X} .

Proposition 2.1. *For $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$ we have:*

(a) *The field $\mathbb{C}(\mathcal{X}_r^\circ)$ is purely transcendental over \mathbb{C} of degree r and is generated by the functions*

$$t_i : \mathcal{X}_r^\circ \setminus \mathcal{U}_i \rightarrow \mathbb{C}, \quad (x_1, \dots, x_r) \mapsto x_i \quad \text{for } i = 1, \dots, r,$$

where \mathcal{U}_i denotes the hyperplane defined by $x_i = \infty$.

(b) *The field $\mathbb{C}(\tilde{\mathcal{X}}_r^\circ)$ is purely transcendental over \mathbb{C} of degree r and is generated by the elementary symmetric functions*

$$\tilde{t}_j := \sum_{1 \leq i_1 < \dots < i_j \leq r} t_{i_1} \cdots t_{i_j} \quad \text{for } j = 1, \dots, r.$$

Proof. Since \mathcal{X}_r° is an open and dense subset (with the Zariski topology) of the product \mathcal{X}^r , the function fields of \mathcal{X}_r° and \mathcal{X}^r coincide, i.e., we have

$$\mathbb{C}(\mathcal{X}_r^\circ) = \mathbb{C}(\mathcal{X}^r) = \mathbb{C}(t_1, \dots, t_r).$$

From the definition of the S_r -covering $\mathcal{X}_r^\circ \rightarrow \tilde{\mathcal{X}}_r^\circ$ in Section 1.1 we thus obtain

$$\mathbb{C}(\tilde{\mathcal{X}}_r^\circ) = \mathbb{C}(\tilde{t}_1, \dots, \tilde{t}_r). \quad \square$$

Now let k be an algebraically closed field and \mathcal{X} a quasiprojective normal variety. Then a field extension $L/k(\mathcal{X})$ is called *unramified over \mathcal{X}* , if the normalization \mathcal{Y} of \mathcal{X} in L is unramified over \mathcal{X} . The set of finite extension fields of $K := k(\mathcal{X})$ unramified over \mathcal{X} is closed under composition and taking of the Galois hull (in a given algebraic closure of K). Thus, the union of all such fields forms a maximal extension field M of K unramified over \mathcal{X} , which is moreover Galois over K (see Grothendieck (1971), Exp. I.10, Exp. V.4+8 and Exp. XII.5, or Popp (1970), 1. Vorl.). The corresponding Galois group is then called the *algebraic fundamental group of \mathcal{X}* :

$$\pi_1^{\text{alg}}(\mathcal{X}) := \text{Gal}(M/K).$$

In our case we thus obtain:

Theorem 2.2. *Let M_r be a maximal field extension of $\mathbb{C}(\tilde{\mathbf{t}}) = \mathbb{C}(\tilde{t}_1, \dots, \tilde{t}_r)$ unramified over the r -fold incomplete symmetric product of $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$. Then the Galois group of $M_r/\mathbb{C}(\tilde{\mathbf{t}})$ is isomorphic to the profinite completion of the full Hurwitz braid group \tilde{H}_r :*

$$\text{Gal}(M_r/\mathbb{C}(\tilde{\mathbf{t}})) = \pi_1^{\text{alg}}(\tilde{\mathcal{X}}_r) \cong (\tilde{H}_r)^{\circ}. \quad (2.1)$$

Here $\mathbb{C}(\mathbf{t}) = \mathbb{C}(t_1, \dots, t_r)$ is the fixed field of the profinite completion of the pure Hurwitz braid group:

$$\text{Gal}(M_r/\mathbb{C}(\mathbf{t})) = \pi_1^{\text{alg}}(\mathcal{X}_r) \cong \hat{H}_r. \quad (2.2)$$

Proof. The proof runs entirely along the lines of the proof of Theorem I.1.3, with the only difference that here we have to cite the higher dimensional version of the Riemann Hebbarkeitssatz and the Riemann Existence Theorem.

Obviously $\tilde{\mathcal{X}}_r$ is sufficiently connected (in the sense of Stöcker and Zieschang (1988), Def. 6.4.3). Thus there exists a universal covering

$$u : \hat{\mathcal{X}}_r \longrightarrow \tilde{\mathcal{X}}_r$$

whose group of covering transformations is isomorphic to the fundamental group of $\tilde{\mathcal{X}}_r$ with respect to the base point $\mathcal{P}_0 = (1, \dots, r)$ and hence to the pure Hurwitz braid group via

$$\omega : \text{Deck}(u) \rightarrow \pi_1^{\text{top}}(\tilde{\mathcal{X}}_r; \mathcal{P}_0) = H_r, \quad (2.3)$$

depending on a point $\hat{\mathcal{P}}_0 \in \hat{\mathcal{X}}_r$ with $u(\hat{\mathcal{P}}_0) = \mathcal{P}_0$. From the fundamental theorem for coverings of topological spaces it now follows that for each finite unramified normal covering

$$p^* : \mathcal{Y}_r \longrightarrow \tilde{\mathcal{X}}_r$$

there exists a unique normal subgroup O of finite index in $\text{Deck}(u)$ such that \mathcal{Y}_r is homeomorphic to the orbit space $\hat{\mathcal{X}}_r/O$ (equipped with the quotient topology). Via the canonical map of $\hat{\mathcal{X}}_r$ onto $\hat{\mathcal{X}}_r/O$ we obtain a universal covering

$$v : \hat{\mathcal{X}}_r \longrightarrow \mathcal{Y}_r \cong \hat{\mathcal{X}}_r/O$$

satisfying $p^* \circ v = u$ and $\text{Deck}(v) \cong O$, where moreover

$$\text{Deck}(p^*) \cong \text{Deck}(u)/\text{Deck}(v).$$

By a theorem of Grauert and Remmert (see for example Grothendieck (1971), Exp. XII, Thm. 5.4, or also Popp (1970), 1. Vorl.), the covering p^* possesses a unique continuation

$$p : \mathcal{Y}_r \longrightarrow \mathcal{X}_r$$

to a normal projective manifold \mathcal{Y}_r , in which \mathcal{Y}_r lies dense and for which moreover

$$\text{Deck}(p) \cong \text{Deck}(p^*).$$

The field $N := \mathbb{C}(\mathcal{Y}_r)$ is a Galois extension of $K := \mathbb{C}(t)$ unramified over \mathcal{X}_r° , whose degree equals the number of sheets of the covering p respectively p° by the Grothendieck version of the Riemann existence theorem (Grothendieck (1971), Exp. XII, Thm. 5.1). This implies

$$\mathrm{Gal}(N/K) \cong \mathrm{Deck}(p)$$

(with $\mathrm{Gal}(N/K)$ acting from the right) und hence finally

$$\mathrm{Gal}(N/K) \cong H_r/\omega(O).$$

On the other hand, every finite Galois extension field N of K unramified over \mathcal{X}_r° determines via the normalization of \mathcal{X}_r° in N a normal unramified covering \mathcal{Y}_r° of \mathcal{X}_r° with $\mathbb{C}(\mathcal{Y}_r^\circ) = N$. Thus the above mapping between the set \mathcal{O}_r of normal subgroups of finite index of $\mathrm{Deck}(u)$ and the set N_r of finite Galois extensions of K unramified over \mathcal{X}_r° becomes a Galois correspondence. Since the maximal extension field M_r of K unramified over \mathcal{X}_r° can be regarded as the union of all $N \in N_r$, the Galois group of M_r/K is the projective limit of the Galois groups $\mathrm{Gal}(N/K)$, hence

$$\mathrm{Gal}(M_r/K) \cong \varprojlim (H_r/\omega(O))_{O \in \mathcal{O}_r} = \hat{H}_r.$$

The canonical map $\tilde{q} : \mathcal{X}_r^\circ \rightarrow \tilde{\mathcal{X}}_r^\circ$ is unramified, so $\tilde{u} := \tilde{q} \circ u$ becomes a universal covering of $\tilde{\mathcal{X}}_r^\circ$, which finally proves

$$\mathrm{Gal}(M_r/\tilde{K}) \cong (\tilde{H}_r)^\wedge,$$

where we have set $\tilde{K} := \mathbb{C}(\tilde{t})$. □

In what follows we call the profinite completions of H_r resp. \tilde{H}_r *profinite Hurwitz braid groups*. Lacking a suitable different letter in the Greek alphabet we will again denote them by H_r resp. \tilde{H}_r . This should not give rise to any confusion, since the discrete Hurwitz braid groups will from now on always occur as fundamental groups $\pi_1^{\text{top}}(\mathcal{X}_r^\circ; \mathcal{P}_0)$ or $\pi_1^{\text{top}}(\tilde{\mathcal{X}}_r^\circ; \tilde{\mathcal{P}}_0)$ respectively, for $\mathcal{P}_0 = (1, \dots, r)$. (If necessary they will be distinguished from the profinite groups by using the symbols \check{H}_r or \tilde{H}_r^\vee respectively.)

We see that by Theorem 2.2 the profinite Hurwitz braid groups also satisfy

$$\tilde{H}_r/H_r \cong S_r. \tag{2.4}$$

Furthermore Theorem 1.13 immediately implies (compare Serre (1964), Ch. I, §1.1):

Corollary 2.3. *The canonical map from the (discrete) Hurwitz braid group into the profinite Hurwitz braid group is injective.*

Consequently in what follows, we do not distinguish between the elements of $\pi_1^{\text{top}}(\tilde{\mathcal{X}}_r^\circ; \tilde{\mathcal{P}}_0)$ and their embedded images in \tilde{H}_r (depending on $\tilde{\mathcal{P}}_0$ by (2.3)).

2.2 Inertia Groups

As in the 1-dimensional case the embedded generators β_i of \tilde{H}_r resp. β_{ij} of H_r can be interpreted as generators of inertia groups in $M_r/\mathbb{C}(\tilde{\mathbf{t}})$ resp. $M_r/\mathbb{C}(\mathbf{t})$.

Theorem 2.4. *Let $K = \mathbb{C}(\mathbf{t})$ and \mathfrak{D}_{ij} be the valuation ideal of K defined by $(t_i - t_j)$ in the corresponding local ring. Further let M_r/K be a maximal field extension unramified over $\mathbb{P}^1(\mathbb{C})_r$ with the Galois group $\pi_1^{\text{alg}}(\mathbb{P}^1(\mathbb{C})_r) = H_r$. Then there exists a valuation ideal $\hat{\mathfrak{D}}_{ij}$ of M_r lying above \mathfrak{D}_{ij} such that β_{ij} generates the inertia group of $\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}$:*

$$I(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) = \langle \beta_{ij} \rangle. \quad (2.5)$$

Proof. The notations introduced in the proof of Theorem 2.2 are tacitly used. Further let \mathcal{D}_{ij} be the hyperplane $x_i = x_j$ in \mathcal{X}^r and \mathcal{D}_{ij}^c the complement of the intersections $\mathcal{D}_{ij} \cap \mathcal{D}_{kl}$ for $\{k, l\} \neq \{i, j\}$ in \mathcal{D}_{ij} .

Let $u : \hat{\mathcal{X}}_r \rightarrow \mathcal{X}_r$ be an universal covering of \mathcal{X}_r and $\hat{\mathcal{P}}_0 \in \hat{\mathcal{X}}_r$ the preimage of the base point $\mathcal{P}_0 = (1, \dots, r) \in \mathcal{X}_r$ under u used for (2.3). For a closed path b_{ij} in the homotopy class β_{ij} by the main lemma of covering theory there exists a unique lifting \tilde{b}_{ij} to \mathcal{Y}_r with $\tilde{b}_{ij}(0) = \tilde{\mathcal{P}}_0 := v(\hat{\mathcal{P}}_0)$.

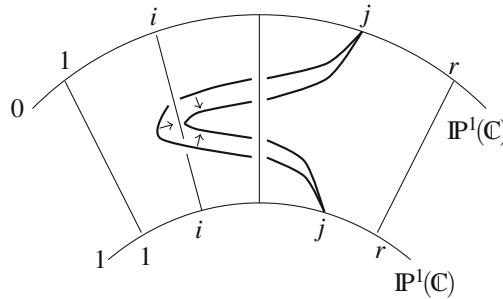


Fig. 2.1 Deformation of b_{ij}

We now deform the path b_{ij} according to Figure 2.1 homotopically in $\mathcal{X}_r \cup \mathcal{D}_{ij}^c$ to a path b_{ij}^* in \mathcal{X}^r , which apart from the intersection point $\mathcal{P}_{ij} = (1, \dots, j-1, i, j+1, \dots, r)$ with \mathcal{D}_{ij} lies completely inside \mathcal{X}_r . Then b_{ij}^* also possesses a lifting \tilde{b}_{ij}^* in \mathcal{Y}_r with respect to the continuation p of p^* . (The preimage $\tilde{\mathcal{P}}_{ij}$ of \mathcal{P}_{ij} is uniquely determined, since the continuation p of p^* is continuous.) Denote the irreducible component of the fiber $p^{-1}(\mathcal{D}_{ij})$ containing $\tilde{\mathcal{P}}_{ij}$ by $\tilde{\mathcal{D}}_{ij}$, and by d_{ij} the covering transformation of p determined by $d_{ij}(\tilde{\mathcal{P}}_0) = \tilde{b}_{ij}(1)$. Then $\tilde{\mathcal{D}}_{ij}$ remains pointwise fixed under d_{ij} due to $d_{ij}(\tilde{\mathcal{P}}_{ij}) = \tilde{\mathcal{P}}_{ij}$.

As a closed submanifold of \mathcal{Y}_r of codimension 1, $\tilde{\mathcal{D}}_{ij}$ defines a discrete ultrametric valuation on N continuing the valuation of K belonging to \mathcal{D}_{ij} . The corresponding valuation ring and valuation ideal are denoted by $\tilde{\mathfrak{O}}_{ij}$ resp. $\tilde{\mathfrak{D}}_{ij}$. For any $f \in \tilde{\mathfrak{O}}_{ij}$

and the automorphism $\sigma_{ij} \in \text{Gal}(\mathbb{N}/\mathbb{K})$ defined by $f^{\sigma_{ij}}(\tilde{\mathcal{P}}) = f(d_{ij}(\tilde{\mathcal{P}}))$ we have $f^{\sigma_{ij}} - f \in \tilde{\mathfrak{D}}_{ij}$, hence the element σ_{ij} is contained in the inertia group of $\tilde{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}$. If conversely σ lies in the inertia group of $\tilde{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}$, then $\tilde{\mathfrak{D}}_{ij}$ belongs to the fixed point manifold of the corresponding covering transformation d of $\mathcal{Y}_r/\mathcal{X}^r$ (see for example Popp (1970), Lemma 1.22 and 1.23). In particular the point $\tilde{\mathcal{P}}_{ij}$ is fixed by d . On the side of the braid group $\check{H}_r = \pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C})_r; \mathcal{P}_0)$ this means that d corresponds to a braid β which becomes trivial by identifying the coordinates i and j of \mathcal{P}_0 along b_{ij}^* (see Figure 2.2). (From the point of view of homotopy groups this procedure describes a deformation of the loops $b \in \beta$ to loops inside \mathfrak{D}_{ij} by moving the base point \mathcal{P}_0 to the base point $\mathcal{P}_{ij} \in \mathfrak{D}_{ij}$ along b_{ij}^* , see also Paragraph 8.1.) This implies that β is a power of β_{ij} . Thus σ_{ij} even generates the inertia group of $\tilde{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}$.

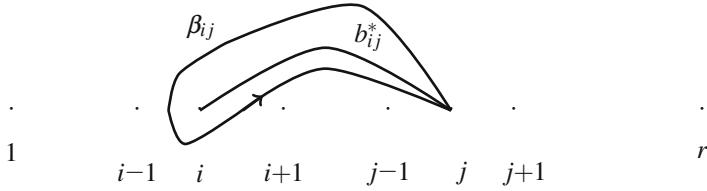


Fig. 2.2 Moving \mathcal{P}_0 to \mathcal{P}_{ij}

By construction we thus have

$$(\sigma_{ij})_{O \in \mathcal{O}_r} = \beta_{ij} \in H_r, \quad \text{and} \quad \hat{\mathfrak{D}}_{ij} := \bigcup_{\mathbb{N} \in \mathbb{N}_r} \tilde{\mathfrak{D}}_{ij}$$

is a valuation ideal of \mathbb{M}_r lying above \mathfrak{D}_{ij} whose inertia group is generated by β_{ij} as a topological group. \square

Theorem 2.4 has the following consequence for the Galois extension $\mathbb{M}_r/\mathbb{C}(\tilde{\mathbf{t}})$:

Corollary 2.5. *Let $\tilde{\mathbb{K}} = \mathbb{C}(\tilde{\mathbf{t}})$ be the field of rational functions of the incomplete symmetric product $\tilde{\mathcal{X}}_r$ of $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$ and $\tilde{\mathfrak{D}}_i$ the valuation ideal of $\tilde{\mathbb{K}}$ contained in the valuation ideal $\mathfrak{D}_{i,i+1}$ of $\mathbb{K} = \mathbb{C}(\mathbf{t})$. Then $\mathbb{M}_r/\tilde{\mathbb{K}}$ is Galois with group $\pi_1^{\text{alg}}(\tilde{\mathcal{X}}_r) = \check{H}_r$, and we have*

$$I(\hat{\mathfrak{D}}_{i,i+1}/\tilde{\mathfrak{D}}_i) = \langle \beta_i \rangle. \tag{2.6}$$

Proof. The Galois group of $\mathbb{M}_r/\tilde{\mathbb{K}}$ had already been determined in Corollary 2.1. By Theorem 2.4 we have

$$I(\hat{\mathfrak{D}}_{i,i+1}/\mathfrak{D}_{i,i+1}) = \langle \beta_i^2 \rangle,$$

hence it only remains to identify the inertia group of $\mathfrak{D}_{i,i+1}/\tilde{\mathfrak{D}}_i$. It consists of those elements of

$$\text{Gal}(\mathbf{K}/\tilde{\mathbf{K}}) \cong S_r = q_r(\tilde{H}_r)$$

whose corresponding covering transformation of \mathcal{X}^r over \mathcal{X}^r/S_r leaves the hyperplane $\mathcal{D}_{i,i+1}$ pointwise fixed, hence of the powers of the transposition $(i, i+1)$. The assertion now follows since $q_r(\beta_i) = (i, i+1)$. \square

Before we study the field extension $\mathbf{M}_r/\mathbb{C}(\tilde{\mathbf{t}})$ in more detail, we prove some further results on the structure of the Hurwitz braid group.

2.3 Structure of the Profinite Hurwitz Braid Group

The key to the following structure theorems lies in the result proved in Proposition 1.12 asserting that G_{r-1} is a thick normal subgroup of the Hurwitz braid group. Namely more generally we have:

Proposition 2.6. *Let G be a finitely generated group and U a thick normal subgroup of G . Then we have:*

- (a) *\hat{U} is a closed normal subgroup of \hat{G} and $\hat{G}/\hat{U} \cong \widehat{G/U}$.*
- (b) *If U possesses a complement H in G , then $\hat{G} \cong \hat{U} \rtimes \hat{H}$.*

Proof. By assumption \hat{U} is not only the projective limit of the groups U/O for $O \in \mathcal{O}_U$ but we also have

$$\hat{U} = \varprojlim (U/\tilde{O})_{\tilde{O} \in \mathcal{O}_U^G}$$

with the \mathcal{O}_U^G defined in (1.22). For any $O \in \mathcal{O}_G$ the exact sequence

$$1 \longrightarrow UO/O \longrightarrow G/O \longrightarrow G/O/UO/O \longrightarrow 1$$

together with the isomorphism theorems immediately implies the exactness of

$$1 \longrightarrow U/(U \cap O) \longrightarrow G/O \longrightarrow G/UO \longrightarrow 1.$$

Since passage to the projective limit is an exact functor (Ribes (1970), Ch. I, Prop. 3.6), we obtain the exact sequence of profinite groups asserted in (a).

Now let H be a complement to U in G . Obviously for each $O \in \mathcal{O}_G$ we have $O_U := O \cap U \in \mathcal{O}_U$ and $O_H := O \cap H \in \mathcal{O}_H$. Since $\mathcal{O}_U \triangleleft G$ the subgroup of G generated by O_U and O_H is a semidirect product of finite index in G , and it follows that

$$\tilde{O} := \bigcap_{\sigma \in G} (O_U \rtimes O_H)^\sigma \in \mathcal{O}_G.$$

If as above we set $\tilde{O}_U := \tilde{O} \cap U$ and $\tilde{O}_H := \tilde{O} \cap H$, then clearly $\tilde{O}_U = O_U$ and $(O_H : \tilde{O}_H) \leq ((O_U \rtimes O_H) : \tilde{O})$. Consequently \tilde{O} coincides with the semidirect

product generated by O_U and \tilde{O}_H . Since \tilde{O} has finite index in G , $\tilde{\mathcal{O}}_G := \{\tilde{O} \mid O \in \mathcal{O}_G\}$ forms a cofinal subsystem of \mathcal{O}_G . For $\tilde{O} \in \tilde{\mathcal{O}}_G$ the split exact sequence

$$1 \longrightarrow U \longrightarrow G \xrightarrow{\quad} H \longrightarrow 1$$

first implies the sequence

$$1 \longrightarrow U\tilde{O}/\tilde{O} \longrightarrow G/\tilde{O} \xrightarrow{\quad} H\tilde{O}/\tilde{O} \longrightarrow 1$$

with $U\tilde{O}/\tilde{O} \cong U/O_U$ and $H\tilde{O}/\tilde{O} \cong H/\tilde{O}_H$. Since

$$(G : \tilde{O}) = (U : O_U)(H : \tilde{O}_H) = (U\tilde{O} : \tilde{O})(H\tilde{O} : \tilde{O})$$

this is exact and clearly also splits. Passage to the projective limit yields the splitting sequence of profinite groups claimed in (b). \square

We denote the profinite completion of G_{r-1} by Γ_{r-1} :

$$\Gamma_{r-1} := \hat{G}_{r-1} = \langle \gamma_1, \dots, \gamma_{r-1} \mid \gamma_1 \cdots \gamma_{r-1} = 1 \rangle. \quad (2.7)$$

Then Theorems 1.6 and 1.10 yield:

Theorem 2.7. *For $r \geq 4$ we have:*

(a) Γ_{r-1} is a closed normal subgroup of $\tilde{H}_r^+ := \{\beta \in \tilde{H}_r \mid q_r(\beta) \in S_{r-1}\}$, free of rank $r-2$, with

$$\tilde{H}_r^+ / \Gamma_{r-1} \cong \tilde{H}_{r-1}. \quad (2.8)$$

The action of the generators $\Gamma_{r-1}\beta_i$ of the factor group isomorphic to \tilde{H}_{r-1}^+ on Γ_{r-1} is given by the formulae in Theorem 1.6.

(b) Γ_{r-1} possesses in H_r a complement isomorphic to H_{r-1} :

$$H_r \cong \Gamma_{r-1} \rtimes H_{r-1}. \quad (2.9)$$

In the next section we investigate the fixed field of Γ_{r-1} .

2.4 The Fixed Field of the Free Normal Subgroup

The following theorem explains inductively the stepwise structure of the Galois extension M_r/K with $K = \mathbb{C}(t)$:

Theorem 2.8. *Let M_r/K for $r \geq 4$ be the field extension described in Theorem 2.2 with $\text{Gal}(M_r/K) = H_r$. Then the fixed field of the free normal subgroup Γ_{r-1} of H_r is the field $M_{r-1}(t_r)$:*

$$M_r^{\Gamma_{r-1}} = M_{r-1}(t_r). \quad (2.10)$$

Moreover M_{r-1} is algebraically closed in M_r .

Proof. Let $\mathcal{X} := \mathbb{P}^1(\mathbb{C})$ and $N := M_r^{\Gamma_{r-1}}$. Since

$$I(\hat{\mathcal{D}}_{ir}/\mathcal{D}_{ir}) = \langle \beta_{ir} \rangle \leq \Gamma_{r-1}$$

the valuation ideals \mathcal{D}_{ir} of K are unramified in N/K for $i = 1, \dots, r-1$. Consequently N/K is unramified even over $\mathcal{X}_{r-1}^\circ \times \mathcal{X}$, which since $\pi_1^{\text{top}}(\mathcal{X}_{r-1}^\circ \times \mathcal{X}; (1, \dots, r)) \cong \pi_1^{\text{top}}(\mathcal{X}_{r-1}^\circ; (1, \dots, r-1))$ implies that N is a subfield of $M_{r-1}(t_r)$ for which moreover

$$\text{Gal}(N/K) \cong H_r/\Gamma_{r-1} \cong H_{r-1} \cong \text{Gal}(M_{r-1}(t_r)/K).$$

Obviously the kernel of the canonical epimorphism from $\text{Gal}(M_{r-1}/K)$ to $\text{Gal}(N/K)$ lies in the intersection of all normal subgroups of finite index and hence equals the trivial group, which forces $N = M_{r-1}(t_r)$.

If L is an intermediate field of M_r/M_{r-1} algebraic over M_{r-1} , then L is algebraic over $\mathbb{C}(t_1, \dots, t_{r-1})$ and unramified over $\mathcal{X}_r^\circ \cap \mathcal{X}^{r-1} = \mathcal{X}_{r-1}^\circ$. Thus it is a subfield of M_{r-1} which finally proves that $L = M_{r-1}$. \square

Descending induction over s then immediately leads to:

Corollary 2.9. *For $3 \leq s \leq r$ the group*

$$\Gamma_s^{(r)} := \langle \beta_{ij} \mid 1 \leq i < j, s < j \leq r \rangle \leq H_r \quad (2.11)$$

is normal in H_r and has fixed field

$$M_r^{\Gamma_s^{(r)}} = M_s(t_{s+1}, \dots, t_r). \quad (2.12)$$

The following description of the field extension M_r/M_{r-1} builds the connection to the 1-dimensional case (compare Theorem I.1.3).

Theorem 2.10. *Let \mathbb{S} be the set of numerator divisors of $(t_i - t_r)$ for $i = 1, \dots, r-1$ and $r \geq 4$ in the divisor group of $M_{r-1}(t_r)/M_{r-1}$. Then M_r is a maximal Galois extension field of $M_{r-1}(t_r)$, regular over M_{r-1} and unramified outside \mathbb{S} . Further M_r is characterized by these properties among the extension fields of $M_{r-1}(t_r)$.*

Proof. By Theorem 2.8 the field extension M_r/M_{r-1} is regular. Further at most the valuation ideals $M_{r-1}\mathcal{D}_{ir}$ of $M_{r-1}(t_r)$ ramify in $M_r/M_{r-1}(t_r)$. These are the numerator divisors of $(t_i - t_r)$ in the divisor group of $M_{r-1}(t_r)/M_{r-1}$. After extension of constants by an algebraic closure \hat{M}_{r-1} of M_{r-1} (in an algebraic closure of K) we obtain a Galois extension $\hat{M}_{r-1}M_r/\hat{M}_{r-1}(t_r)$ with Galois group isomorphic to Γ_{r-1} , unramified outside the set $\hat{\mathbb{S}}$ of extensions of \mathbb{S} to $\hat{M}_{r-1}(t_r)$. Thus $\hat{M}_{r-1}M_r$ is a subfield of the maximal extension field \hat{M}_r of $\hat{M}_{r-1}(t_r)$ unramified outside $\hat{\mathbb{S}}$, whose Galois group over $\hat{M}_{r-1}(t_r)$ is free profinite of rank $r-2$ by Theorem I.1.3. Consequently the Galois extension $\hat{M}_r/\hat{M}_{r-1}M_r$ induces a canonical epimorphism from Γ_{r-1} onto itself, whose kernel lies in the intersection of all open normal subgroups of Γ_{r-1} and hence is trivial. So we have $\hat{M}_{r-1}M_r = \hat{M}_r$, which proves the maximality of M_r .

By what precedes $\hat{M}_r/M_{r-1}(t_r)$ is Galois with

$$\text{Gal}(\hat{M}_r/M_{r-1}(t_r)) = \text{Gal}(\hat{M}_r/M_r) \times \text{Gal}(\hat{M}_r/\hat{M}_{r-1}(t_r)).$$

The center of Γ_{r-1} is trivial, so M_r is characterized inside the whole Galois extension as the fixed field of the centralizer of $\text{Gal}(\hat{M}_r/\hat{M}_{r-1}(t_r))$. \square

Remark. By a similar consideration the first layer in the above tower of fields M_3/K , where $K = \mathbb{C}(t_1, t_2, t_3)$, with group $H_3 \cong Z_2$, can be seen to be

$$M_3 = K(\sqrt{(t_1 - t_2)(t_1 - t_3)(t_2 - t_3)}). \quad (2.13)$$

3 Galois Descent

Using a similar approach to that of the first chapter, we now study the fields of definition of intermediate fields of the Galois extension $M_r/M_{r-1}(t)$ with the free Galois group Γ_{r-1} by means of the Hurwitz classification. Among other results this then leads to variants in several variables of the Basic Rigidity Theorem and the Strong Rigidity Theorem.

3.1 An Arithmetic Fundamental Group

For the descent from \mathbb{C} to $\bar{\mathbb{Q}}$ we need a generalization of Proposition I.2.1 to function fields of several variables. This can be obtained from Weil's rationality criterion for regular extensions of fields of constants (see Weil (1956), Thm. 4). The following variant is proved in the book of Serre (1992), Thm. 6.3.3.

Proposition 3.1. *Let \bar{k} be an algebraically closed subfield of \mathbb{C} , \mathcal{X} an algebraic variety over \bar{k} and $\bar{K} := \bar{k}(\mathcal{X})$ respectively $K := \mathbb{C}(\mathcal{X})$ the function field of \mathcal{X} over \bar{k} , \mathbb{C} respectively. Then for every finite field extension N/K unramified over \mathcal{X} there exists precisely one field extension \bar{N}/\bar{K} unramified over \mathcal{X} and regular over \bar{k} with $\bar{N}\mathbb{C} := \bar{N} \otimes_{\bar{k}} \mathbb{C} = N$.*

Using the steps of the proof of Theorem I.2.2 we thus obtain here:

Theorem 3.2. *Let \bar{M}_r be a maximal extension field of $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ unramified over the r -fold incomplete symmetric product of $\mathcal{X}(\bar{\mathbb{Q}}) = \mathbb{P}^1(\bar{\mathbb{Q}})$. Then the Galois group of $\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ is isomorphic to the profinite Hurwitz braid group:*

$$\text{Gal}(\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}})) = \pi_1^{\text{alg}}(\tilde{\mathcal{X}}_r(\bar{\mathbb{Q}})) \cong \tilde{H}_r. \quad (3.1)$$

Herein $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ is the fixed field of the profinite pure Hurwitz braid group:

$$\text{Gal}(\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}})) = \pi_1^{\text{alg}}(\mathcal{X}_r(\bar{\mathbb{Q}})) \cong H_r. \quad (3.2)$$

Via this isomorphism the interpretation of the generators β_i of \tilde{H}_r resp. β_{ij} of H_r as generators of inertia groups according to Theorem 2.4 and Corollary 2.5 is transported to the field extensions over $\bar{\mathbb{Q}}$.

In the following we will hence identify \tilde{H}_r with $\text{Gal}(\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}}))$ and H_r with $\text{Gal}(\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}}))$.

The Splitting Theorem I.2.4 with Theorem I.2.6 carries over to the present situation in the following form:

Theorem 3.3 (Splitting Theorem). *The maximal extension field \bar{M}_r of $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ unramified over $\mathbb{P}^1(\bar{\mathbb{Q}})$ is Galois over $\mathbb{Q}(\tilde{\mathbf{t}})$ with*

$$\text{Gal}(\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}})) \cong \tilde{H}_r \rtimes \Gamma_{\mathbb{Q}}. \quad (3.3)$$

Herein the absolute Galois group $\Gamma_{\mathbb{Q}}$ of \mathbb{Q} acts on the generators β_i of \tilde{H}_r and β_{ij} of H_r via the cyclotomic character c , i.e., for $\delta \in \Gamma_{\mathbb{Q}}$ we have

$$[\beta_i]^{\delta} = [\beta_i^{c(\delta)}] \quad \text{and} \quad [\beta_{ij}]^{\delta} = [\beta_{ij}^{c(\delta)}]. \quad (3.4)$$

Proof. Obviously the ramification locus $\tilde{\mathcal{X}}_r(\bar{\mathbb{Q}}) \setminus \tilde{\mathcal{X}}_r^+(\bar{\mathbb{Q}})$ of $\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ remains invariant under all automorphisms δ of $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})/\mathbb{Q}(\tilde{\mathbf{t}})$. Now \bar{M}_r is uniquely determined in a fixed algebraic closure of $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ as the maximal extension field of $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$ unramified over $\tilde{\mathcal{X}}_r^+(\bar{\mathbb{Q}})$, so any lifting $\bar{\delta}$ of δ maps \bar{M}_r onto itself. Hence $\bar{\delta}$ is an automorphism of $\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}})$, and $\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}})$ is Galois with group $\tilde{\Gamma}$, say.

Clearly \tilde{H}_r and H_r lie normal in $\tilde{\Gamma}$. Let \mathfrak{P} denote the valuation ideal of $\mathbb{Q}(\tilde{\mathbf{t}})$ of functions vanishing at a point \mathcal{P} of $\tilde{\mathcal{X}}_r^+(\mathbb{Q})$. Then any valuation ideal $\hat{\mathfrak{P}}$ of \bar{M}_r above \mathfrak{P} is unramified in $\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}})$. Since $\hat{\mathfrak{P}}/\mathfrak{P}$ moreover does not decompose in $\bar{\mathbb{Q}}(\tilde{\mathbf{t}})/\mathbb{Q}(\tilde{\mathbf{t}})$, and completely decomposes in $\bar{M}_r/\bar{\mathbb{Q}}(\tilde{\mathbf{t}})$, the decomposition group of $\mathfrak{P}/\mathfrak{P}$ yields a complement to H_r isomorphic to $\Gamma_{\mathbb{Q}}$ in $\Gamma := \text{Gal}(\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}}))$. This then also forms a closed complement to \tilde{H}_r in $\tilde{\Gamma} = \Gamma(\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}}))$.

For the proof of the second assertion we may utilize the proof of Theorem I.2.6. Denote by $M_{r-1}(t_r)$ the fixed field of a complement to H_{r-1} in $\text{Gal}(\bar{M}_{r-1}(t_r)/\mathbb{Q}(\tilde{\mathbf{t}}))$. Then we have

$$\text{Gal}(\bar{M}_r/M_{r-1}(t_r)) \cong \Gamma_{r-1} \rtimes \Gamma_{\mathbb{Q}}.$$

By Theorem 2.10 the extension $\bar{M}_r/\bar{M}_{r-1}(t_r)$ is maximal Galois unramified outside the set \mathbb{S} of numerator divisors \mathfrak{P}_i of $(t_r - t_i)$ for $i = 1, \dots, r-1$ with Galois group Γ_{r-1} . Since $\text{Gal}(\bar{M}_{r-1}(t_r)/M_{r-1}(t_r))$ leaves this set pointwise fixed, the proof of Theorem I.2.6 yields

$$[\beta_{ir}]^{\delta} = [\gamma_i]^{\delta} = [\gamma_i^{c(\delta)}] = [\beta_{ir}^{c(\delta)}].$$

Exchanging the variables t_i we thus obtain the corresponding result for all generators β_{ij} of H_r .

By Corollary 2.5 the braid β_i generates an inertia group over a valuation ideal of $\mathbb{Q}(\tilde{\mathbf{t}})$ in $\tilde{\Gamma}$, so the conjugacy class $[\beta_i]$ is also mapped to a power of itself. Since $\beta_i^2 = \beta_{i,i+1}$ this finally implies $[\beta_i]^{\delta} = [\beta_i^{c(\delta)}]$. \square

As in Chapter I we refer to the Galois groups $\tilde{\Gamma} = \text{Gal}(\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}}))$ and $\Gamma = \text{Gal}(\bar{M}_r/\mathbb{Q}(\tilde{\mathbf{t}}))$ as *arithmetic fundamental groups* (belonging to \tilde{H}_r resp. H_r).

3.2 Hurwitz Classification

Theorem 2.10 and Proposition 3.2 show that with the maximal Galois extension $\bar{M}_r/\bar{M}_{r-1}(t_r)$, unramified outside the set of numerator divisors \mathfrak{P}_i of $(t_r - t_i)$ for $i = 1, \dots, r-1$ in the divisor group of $\bar{M}_{r-1}(t_r)/\bar{M}_{r-1}$ we are in the same situation

as with the Galois extension $\bar{M}_s/\bar{\mathbb{Q}}(t)$ in Chapter I. From now on we always let $s := r - 1$ with $s \geq 3$ and, if necessary, $t := t_r$.

For a finite group G we correspondingly set

$$\bar{\mathbf{N}}_s(G) := \{\bar{N} \mid \bar{M}_s(t) \leq \bar{N} \leq \bar{M}_{s+1}, \text{Gal}(\bar{N}/\bar{M}_s(t)) \cong G\}. \quad (3.5)$$

For $\sigma \in \Sigma_s(G)$ let ψ_σ be the continuous homomorphism from $\Gamma_s = \text{Gal}(\bar{M}_{s+1}/\bar{M}_s(t))$ onto G with kernel $\ker(\sigma)$ defined by $\psi_\sigma(\gamma) = \sigma$ (compare I, (4.2)). Then in complete analogy to Theorem I.4.1 we have:

Theorem 3.4 (Hurwitz Classification). *For $s \geq 3$ the fields $\bar{N} \in \bar{\mathbf{N}}_s(G)$ are parameterized by the classes of generating s -systems $\sigma^{\text{Aut}(G)} \in \Sigma_s(G)/\text{Aut}(G)$. More precisely there exists a bijection*

$$\mathbf{N}_s : \Sigma_s(G)/\text{Aut}(G) \rightarrow \bar{\mathbf{N}}_s(G), \quad \sigma^{\text{Aut}(G)} \mapsto \bar{N}_\sigma := \bar{M}_{s+1}^{\ker(\sigma)}. \quad (3.6)$$

The components σ_i of the parameter σ generate inertia groups of prime ideals of $\bar{N}_\sigma/\bar{M}_s(t)$ over \mathfrak{P}_i via

$$\varphi_\sigma : G \rightarrow \text{Gal}(\bar{N}_\sigma/\bar{M}_s(t)), \quad \sigma_i \mapsto \psi_\sigma^{-1}(\sigma_i) \ker(\sigma). \quad (3.7)$$

Remark. \mathbf{N}_s may also be interpreted as a surjective map

$$\mathbf{N}_s : \Sigma_s(G)/\text{Inn}(G) \rightarrow \bar{\mathbf{N}}_s(G), \quad [\sigma] \mapsto \bar{N}_\sigma. \quad (3.8)$$

Due to $\Gamma_s \triangleleft \tilde{H}_{s+1}^\cdot$ the group Γ_s is not only normal in $\Gamma = \text{Gal}(\bar{M}_{s+1}/\mathbb{Q}(\mathbf{t}))$, but also in

$$\tilde{\Gamma}^\cdot := \text{Gal}(\bar{M}_{s+1}/\mathbb{Q}(\tilde{t}_1, \dots, \tilde{t}_s, t)), \quad (3.9)$$

where the \tilde{t}_i denote the elementary symmetric functions in t_1, \dots, t_s . As in I, (4.8), we now define an action of $\tilde{\Gamma}^\cdot$ on $\Sigma_s(G)$ from the right via

$$\Sigma_s(G) \times \tilde{\Gamma}^\cdot \rightarrow \Sigma_s(G), \quad (\sigma, \tilde{\delta}) \mapsto \sigma \cdot \tilde{\delta} = \sigma^{\tilde{\delta}^{-1}} \text{ with } \sigma^{\tilde{\delta}} = \psi_\sigma(\gamma^{\tilde{\delta}}). \quad (3.10)$$

Then formula (3.4) carries over to the components of the image $\sigma = \psi_\sigma(\gamma)$. As a consequence the actions of $\tilde{\Gamma}^\cdot$ respectively of

$$\tilde{\Delta}_s := \text{Gal}(\bar{M}_s(t)/\mathbb{Q}(\tilde{t}_1, \dots, \tilde{t}_s, t)) \cong \tilde{\Gamma}^\cdot / \Gamma_s \quad (3.11)$$

on $\Sigma_s(G)/\text{Inn}(G)$ and $\bar{\mathbf{N}}_s(G)$ are inverse to each other.

Proposition 3.5. *With the action of $\tilde{\delta} \in \tilde{\Delta}_s$ on $\Sigma_s(G)/\text{Inn}(G)$ defined in (3.10) we have*

$$\bar{N}_{\sigma \cdot \tilde{\delta}} = (\bar{N}_\sigma)^{\tilde{\delta}^{-1}}. \quad (3.12)$$

The proof is exactly the same as the one for Proposition I.4.2.

3.3 The Fixed Field of a Class of Generating Systems

Via the action of $\tilde{\Gamma}_s^*$ on G defined in (3.10) the group $\tilde{\Delta}_s$ acts on the conjugacy classes of G via the cyclotomic character. More precisely we have the following analogue of Proposition I.4.3:

Proposition 3.6. *According to the decomposition of $\tilde{\Delta}_s$ into a semidirect product $\tilde{H}_s \rtimes \Gamma_{\mathbb{Q}}$ write $\tilde{\delta} \in \tilde{\Delta}_s$ as $\beta\delta$ with $\beta \in \tilde{H}_s$. Then $\tilde{\delta} \in \tilde{\Delta}_s$ acts on the set of conjugacy classes C_i of the i -th component of $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ via*

$$C_i^{\tilde{\delta}} = C_{(i)\beta}^{c(\delta)}, \quad (3.13)$$

with the cyclotomic character c and $(i)\beta := (i)q_s(\beta)$.

Proof. By Theorem 1.6 and Corollary 2.3 the generators β_j of \tilde{H}_s act on the generators γ_i of Γ_s and hence according to (3.10) on the generators σ_i of G via

$$[\sigma_1, \dots, \sigma_s]^{\beta_j} = [\sigma_1, \dots, \sigma_{j-1}, \sigma_j \sigma_{j+1} \sigma_j^{-1}, \sigma_j, \sigma_{j+2}, \dots, \sigma_s].$$

Consequently $C_i = [\sigma_i]$ is mapped onto $C_{(i)\beta}$ under $\beta \in \tilde{H}_s$. Using Theorem 3.3 we thus obtain

$$C_i^{\tilde{\delta}} = C_i^{\beta\delta} = C_{(i)\beta}^{\delta} = C_{(i)\beta}^{c(\delta)}. \quad \square$$

If in Proposition 3.6 the element $\tilde{\delta} = \beta\delta$ belongs to the subgroup

$$\Delta_s := \text{Gal}(\bar{M}_s(t)/\mathbb{Q}(t_1, \dots, t_s, t)) = \Gamma/\Gamma_s \quad (3.14)$$

of $\tilde{\Delta}_s$, then we even have $C_i^{\tilde{\delta}} = C_i^{c(\delta)}$ since $H_s = \ker(q_s)$. By (3.13), the stabilizer

$$\Delta_C := \{\delta \in \Delta_s \mid C^{\delta} = C\} \quad (3.15)$$

of the class vector $C = (C_1, \dots, C_s)$ under this action of Δ_s (compare I, (4.13)) is a closed subgroup with fixed field

$$\bar{M}_s(t)^{\Delta_C} = \mathbb{Q}_C(t) \quad (3.16)$$

where \mathbb{Q}_C is the field introduced in Proposition I.4.4.

The fixed field K_{σ} under the closed subgroup

$$\Delta_{\sigma} := \{\delta \in \Delta_s \mid [\sigma]^{\delta} = [\sigma]\} \quad (3.17)$$

for $[\sigma] \in \Sigma(C)/\text{Inn}(G)$ then satisfies the analogue of Theorems I.4.5 and I.4.7:

Theorem 3.7. *Let G be a finite group and $[\sigma]$ a class of generating s -systems of G with $s \geq 3$ belonging to the class vector C .*

(a) The fixed field K_σ of $[\sigma]$ contains the field $\mathbb{Q}_C(\mathbf{t}) = \mathbb{Q}_C(t_1, \dots, t_s, t)$ and we have

$$[K_\sigma : \mathbb{Q}_C(\mathbf{t})] \leq l(\mathbf{C}). \quad (3.18)$$

(b) If $\mathcal{L}(G) = 1$ then there exists a geometric Galois extension N_σ / K_σ with

$$\text{Gal}(N_\sigma / K_\sigma) \cong G \quad \text{and} \quad \bar{M}_s N_\sigma = \bar{N}_\sigma. \quad (3.19)$$

Proof. Assertion (a) follows from

$$(\Delta_C : \Delta_\sigma) \leq |\Sigma(C)/\text{Inn}(G)| = l(\mathbf{C}).$$

According to Proposition I.4.6 the field \bar{N}_σ is Galois over K_σ and the corresponding Galois group acts by inner automorphisms on $\text{Gal}(\bar{N}_\sigma / \bar{M}_s(t)) \cong G$. Thus the field N_σ in part (b) is obtained as the fixed field of the centralizer of $\text{Gal}(\bar{N}_\sigma / \bar{M}_s(t))$ in $\text{Gal}(\bar{N}_\sigma / K_\sigma)$. \square

In the special case $l(\mathbf{C}) = 1$ we recover from Theorem 3.7 a variant of the Basic Rigidity Theorem I.4.8 in several variables:

Corollary 3.8. *Let G be a finite group with trivial center and with a rigid class vector $\mathbf{C} \in \text{Cl}(G)^s$. Then there exists a geometric Galois extension $N / \mathbb{Q}_C(t_1, \dots, t_s, t)$ with group*

$$\text{Gal}(N / \mathbb{Q}_C(\mathbf{t})) \cong G.$$

If moreover C is rationally rigid, then we even have $\mathbb{Q}_C = \mathbb{Q}$.

In the next section we deduce the higher dimensional analogue of the Strong Rigidity Theorem using symmetry groups of \mathbf{C} .

3.4 Using the Symmetry Group

As in Section I.4.4, let V denote a symmetry group of the class vector \mathbf{C} of G and $\mathbf{C}^V = \{\mathbf{C}^\omega \mid \omega \in V\}$. Furthermore, for $\tilde{\delta} = \beta\delta$ according to Proposition 3.6 let

$$\tilde{\Delta}_C^V := \{\tilde{\delta} \in \tilde{\Delta}_s \mid \mathbf{C}^{\tilde{\delta}} \in \mathbf{C}^V\} = \{\tilde{\delta} \in \tilde{\Delta}_s \mid \mathbf{C}^{c(\tilde{\delta})} \in \mathbf{C}^V\}. \quad (3.20)$$

The fixed field of this closed subgroup is the subfield of all V -invariant functions in $\mathbb{Q}_C^V(\mathbf{t}) = \mathbb{Q}_C^V(t_1, \dots, t_s, t)$. We write \mathbf{t}^V for a system of basic invariants of $t_1, \dots, t_s, t = t_{s+1}$ under the action of $V \leq S_s$ (by permutation of the indices), and then obtain

$$\bar{M}_s(t)^{\tilde{\Delta}_C^V} = (\mathbb{Q}_C^V(\mathbf{t}))^V = \mathbb{Q}_C^V(\mathbf{t}^V). \quad (3.21)$$

Here in general $\mathbb{Q}_C^V(\mathbf{t}^V)$ is not rational but only a *unirational function field*, i.e., a subfield of a purely transcendental field with the same field of constants. The fixed

field K_σ^V of the closed subgroup

$$\Delta_\sigma^V := \{\tilde{\delta} \in \tilde{\Delta}_s \mid [\sigma]^{\tilde{\delta}} = [\sigma]\} \quad (3.22)$$

of $\tilde{\Delta}_s$ then satisfies the following generalization of Theorem 3.7 with exactly the same proof:

Theorem 3.9. *Let G be a finite group, $[\sigma]$ a class of generating s -systems with $s \geq 3$ of G with class vector \mathbf{C} and V a symmetry group of \mathbf{C} .*

(a) *The fixed field K_σ^V of $[\sigma]$ contains the field $\mathbb{Q}_C^V(t^V)$, and we have*

$$[K_\sigma^V : \mathbb{Q}_C^V(t^V)] \leq l(\mathbf{C}^V). \quad (3.23)$$

(b) *If $\mathcal{Z}(G) = 1$ then there exists a geometric Galois extension N_σ / K_σ^V with group*

$$\text{Gal}(N_\sigma / K_\sigma^V) \cong G \quad \text{and} \quad \bar{M}_s N_\sigma = \bar{N}_\sigma. \quad (3.24)$$

For the proof of the analogue of the Strong Rigidity Theorem it is easiest to use a semilinear rationality criterion introduced by Speiser (1919) (see also Borel (1991), Ch. AG, §14.2). This will be employed several times in what follows.

Proposition 3.10 (Speiser's Lemma). *Let K/k be an algebraic function field of transcendence degree r and \bar{K}/\bar{k} an extension of constants with a separable algebraic closure \bar{k} of k . If \bar{K}/\bar{k} possesses a linear subspace \bar{U} invariant by $\Delta := \text{Gal}(\bar{K}/K)$ with $\bar{k}(\bar{U}) = \bar{K}$ and $\dim(\bar{U}) = r$, then the fixed point set $U := \bar{U}^\Delta$ is a vector space over k with $K = k(U)$. In particular, K/k is a rational function field and any basis of the vector space U/k yields a transcendence basis of K/k .*

Proof. For $u \in \bar{U}$ the index of the stabilizer Δ_u of u in Δ is finite. The intersection $\tilde{\Delta}$ of the Δ -conjugates of Δ_u is hence a normal subgroup of finite index in Δ , whose fixed field in \bar{K} resp. \bar{k} will be denoted by \tilde{K} resp. \tilde{k} . Let $\sigma_1 = 1, \sigma_2, \dots, \sigma_n$ be the elements of $\Delta/\tilde{\Delta}$ and a_1, \dots, a_n a k -basis of \tilde{k} . Then the

$$v_i := \sum_{j=1}^n a_i^{\sigma_j} u^{\sigma_j} \in \bar{U} \quad \text{for } i = 1, \dots, n \quad (3.25)$$

are Δ -invariant and thus lie in U . From the linear independence of the automorphisms σ_j over \tilde{k} it follows that the matrix $A = (a_i^{\sigma_j})_{ij}$ is invertible in $\tilde{k}^{n \times n}$, with inverse $B = (b_{hi})_{hi}$ say. We calculate that

$$\sum_{i=1}^n b_{1i} v_i = \sum_{i=1}^n \sum_{j=1}^n b_{1i} a_i^{\sigma_j} u^{\sigma_j} = \sum_{j=1}^n \delta_{1j} u^{\sigma_j} = u \quad (3.26)$$

with the Kronecker symbol δ_{ij} is a \tilde{k} -linear combination of elements of U . This implies $\tilde{k} \otimes_k U = \bar{U}$ and thus $K = k(U)$. \square

The analogue of the Strong Rigidity Theorem is now given by:

Theorem 3.11. *Let G be a finite group with trivial center and rigid class vector $\mathbf{C} \in \text{Cl}(G)^s$ where $s \geq 3$. Further let V be a symmetry group of \mathbf{C} with the property that for each $\delta \in \Delta_{\mathbf{C}}^V := \Delta_s \cap \tilde{\Delta}_{\mathbf{C}}^V$ there exists a unique $\omega \in V$ satisfying $\mathbf{C}^{c(\delta)} = \mathbf{C}^\omega$. Then there exists a function field $\mathbb{Q}_{\mathbf{C}}^V(v_1, \dots, v_s, t)$, purely transcendental over $\mathbb{Q}_{\mathbf{C}}^V$, and a geometric Galois extension $N/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{v}, t)$ with group*

$$\text{Gal}(N/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{v}, t)) \cong G.$$

Moreover if \mathbf{C} is V -symmetric, then $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$.

Proof. From rigidity of \mathbf{C} we obtain that $\Sigma(\mathbf{C})/\text{Inn}(G)$ consists of a single class of generating systems $[\sigma]$. This then satisfies

$$\Delta_\sigma^V = \{\delta \in \tilde{\Delta}_{\mathbf{C}}^V \mid \mathbf{C}^\delta = \mathbf{C}\} = \tilde{\Delta}_{\mathbf{C}} \geq \Delta_{\mathbf{C}},$$

which first yields $\mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^V) \leq K_\sigma^V \leq \mathbb{Q}_{\mathbf{C}}(\mathbf{t})$. Since by assumption for each $\delta \in \Delta_{\mathbf{C}}^V$ there exists $\omega \in V$ with $\mathbf{C}^{c(\delta)} = \mathbf{C}^\omega$, the extension $K_\sigma^V/\mathbb{Q}_{\mathbf{C}}^V$ is regular. Moreover, from the uniqueness of ω it follows that $\bar{\mathbb{Q}}K_\sigma^V = \bar{\mathbb{Q}}(\mathbf{t})$. As $\Delta_\sigma^V \leq \tilde{\Delta}_{\mathbf{C}}^V$, any $\delta \in \Delta_\sigma^V = \text{Gal}(\bar{\mathbb{Q}}(\mathbf{t})/K_\sigma^V)$ permutes the transcendence basis t_1, \dots, t_s of $\bar{\mathbb{Q}}(\mathbf{t})/\bar{\mathbb{Q}}(t)$ and hence acts on the $\bar{\mathbb{Q}}$ -vector space $\bar{U} = \bigoplus_{i=1}^s \bar{\mathbb{Q}}t_i$. By Proposition 3.10 the space \bar{U} possesses a basis v_1, \dots, v_s with $v_i \in K_\sigma^V$ which leads to

$$K_\sigma^V = \mathbb{Q}_{\mathbf{C}}^V(\mathbf{v}, t). \quad (3.27)$$

From this the assertion follows with Theorem 3.9(b). \square

In Paragraph 5 the structure of K_σ^V is studied in the nonrigid situation. Before, in the next paragraph we use Theorem 3.11 to construct polynomials with cyclic Galois groups.

4 Cyclic Polynomials

In this paragraph we treat the higher dimensional analogue of the construction of cyclic field extensions from Section I.5.1, as an example. With its help it is possible to compute generating polynomials of geometric cyclic field extensions of degree n over fields of characteristic not dividing n . These results are complemented by the construction of polynomials which over any field of characteristic p generate a cyclic Galois extension of p -power degree. Thus every finite abelian group possesses G-realizations over every field.

4.1 Cyclic Polynomials in Several Variables

Since for $n = 2$ the polynomial

$$f_2(t, X) := X^2 - t \in k(t)[X] \quad (4.1)$$

generates a geometric Z_2 -extension over $k(t)$ for any field k of characteristic different from 2, we will assume until further notice that $n > 2$.

Proposition 4.1. *Let $2 < n \in \mathbb{N}$, $Z_n = \langle \sigma \rangle$ a cyclic group of order n , $\mathbf{C} = ([\sigma]^i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times)$ and $V := (\mathbb{Z}/n\mathbb{Z})^\times$. Then for the generating system $\sigma \in \mathbf{C}$ there exists a geometric Galois extension N_σ/K_σ^V with*

$$\text{Gal}(N_\sigma/K_\sigma^V) \cong Z_n \quad \text{and} \quad K_\sigma^V = \mathbb{Q}(\mathbf{v}, t), \quad (4.2)$$

where $\mathbf{v} = (v_1, \dots, v_{\varphi(n)})$ and t are independent transcendentals over \mathbb{Q} .

Proof. To simplify the formulae we set

$$C_i := [\sigma^i] = \{\sigma^i\}, \quad \text{and} \quad \mathbf{C} = (C_i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times) \quad (4.3)$$

as above. (For groups Z_p with $p \in \mathbb{P}$ this notation coincides with the one used so far.) Since Z_n is abelian, the class vector \mathbf{C} is rigid. By the definition I, (4.12), we have $\mathbf{C}^V = \mathbf{C}^*$, hence \mathbf{C}^V is even V -symmetric with

$$C_i^\delta = C_i^{c(\delta)} \quad \text{where} \quad c(\delta) \in (\mathbb{Z}/n\mathbb{Z})^\times = V.$$

Thus the additional assumption in Theorem 3.11 is satisfied and we have $\mathbb{Q}_C^V = \mathbb{Q}$ and $K_C^V = \mathbb{Q}(\mathbf{v}, t)$.

Since cyclic groups have non-trivial center, Theorem 3.11 does not immediately apply, and it remains to show the existence of a geometric Galois extension N_σ/K_σ^V . But this can easily be verified (compare the 1-dimensional analogue Theorem I.4.11). As in the proof of the Splitting Theorem 3.3 we obtain from the decomposition group of an unramified rational point of $\mathbb{Q}(\mathbf{v}, t)$ a complement to

$\text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(\mathbf{t})) = Z_n$ in $\text{Gal}(\bar{N}_\sigma/\mathbb{Q}(\mathbf{v}, t))$. Since by construction this group acts trivially on Z_n , it is even a direct complement, whose fixed field N_σ is geometric over $\mathbb{Q}(\mathbf{v}, t)$ and Galois with group $\text{Gal}(N_\sigma/\mathbb{Q}(\mathbf{v}, t)) \cong Z_n$. \square

We proceed to compute generating polynomials for $N_\sigma/\mathbb{Q}(\mathbf{v}, t)$. For this we start with the extension of constants $N_\sigma := \mathbb{Q}_C N_\sigma$ of N_σ , with $\mathbb{Q}_C = \mathbb{Q}(\zeta_n)$, over $\mathbb{Q}_C(\mathbf{v}, t) = \mathbb{Q}_C(\mathbf{t})$, where following the notation in (4.3) we write $\mathbf{t} = (\dots, t_i, \dots, t \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times)$. By Kummer theory \tilde{N}_σ is a subfield of $\mathbb{Q}_C(\mathbf{x}, t)$ with $x_i^n = t - t_i$ for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. The correct subfield can now be determined from the ramification structure (4.3), taking (3.12) in Proposition 3.5 into account: We have

$$\tilde{N}_\sigma = \mathbb{Q}_C(\mathbf{t}, y) \quad \text{with} \quad y := \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{r_n(1/i)}, \quad (4.4)$$

where $r_n(1/i)$ denotes the smallest positive representative of the residue class of $1/i$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. By Proposition 4.1 it follows that

$$\text{Gal}(\tilde{N}_\sigma/K_\sigma^V) \cong \text{Gal}(\tilde{N}_\sigma/\mathbb{Q}_C(\mathbf{t})) \times \text{Gal}(\mathbb{Q}_C/\mathbb{Q}) \cong Z_n \times V.$$

It only remains to find a generating element of $\tilde{N}_\sigma/\mathbb{Q}_C(t)$ invariant under V . For this the Lagrangian resolvents

$$u_i := \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} \zeta_n^{ij} y_j \quad \text{for } i = 1, \dots, n \quad \text{with} \quad (4.5)$$

$$y_j := \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{r_n(j/i)} \quad \text{for } j \in (\mathbb{Z}/n\mathbb{Z})^\times, \quad (4.6)$$

are suitable.

Lemma 4.2. *The polynomial*

$$h_n(X) = \sum_{i=1}^n (-1)^i s_i X^{n-i} := \prod_{i=1}^n (X - u_i) \in \mathbb{Q}(\mathbf{y}, t)[X], \quad (4.7)$$

where $\mathbf{y} = (y_j \mid j \in (\mathbb{Z}/n\mathbb{Z})^\times)$ from (4.6), satisfies:

- (a) $h_n(X)$ has coefficients $s_i \in \mathbb{Z}[\mathbf{t}]$.
- (b) $h_n(X)$ is an Eisenstein polynomial with respect to the numerator divisor of $(t - t_i)$ for every $i \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. We denote by

$$q_m := \sum_{i=1}^n u_i^m \quad \text{for } m \in \{1, \dots, n\} \quad (4.8)$$

the m -th power sum of the u_i from (4.5). According to Newton's identities

$$q_m + \sum_{i=1}^{m-1} (-1)^i s_i q_{m-i} + (-1)^m m s_m = 0 \quad \text{for } m = 1, \dots, n \quad (4.9)$$

it suffices for (a) to prove that q_m lies in $\mathbb{Z}[\mathbf{t}]$. This follows by an elementary calculation: We have

$$q_m = \sum_{i=1}^n \left(\sum_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} \zeta_n^{ij} y_j \right)^m = \sum_{\mathbf{j} \in ((\mathbb{Z}/n\mathbb{Z})^\times)^m} \prod_{l=1}^m y_{j_l} \left(\sum_{i=1}^n \prod_{l=1}^m \zeta_n^{ij_l} \right)$$

for $1 \leq m \leq n$. As $\sum_{i=1}^n \zeta_n^{ij}$ equals n for $n|j$ and 0 else, only the terms with $\sum_{l=1}^m j_l \equiv 0 \pmod{n}$ do not vanish in the above sum. These satisfy

$$\prod_{l=1}^m y_{j_l} = \prod_{l=1}^m \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{r_n(j_l/i)} = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{\sum_{l=1}^m r_n(j_l/i)} \in \mathbb{Z}[\mathbf{t}]$$

due to

$$\sum_{l=1}^m r_n(j_l/i) \equiv (\sum_{l=1}^m j_l)/i \equiv 0 \pmod{n} \quad \text{for } i \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

This proves (a). Further this implies that $x_i^n = t - t_i$ divides q_m and according to (4.9) also s_m for $m = 1, \dots, n$.

For (b) it remains to prove that $(t - t_i)$ divides s_n precisely once. Again by (4.9) it suffices to show the corresponding assertion for q_n . The latter follows from the fact that only for the summand $n \prod_{l=1}^n y_{j_l}$ of q_n with $j_l = i$ for $l = 1, \dots, n$ we have

$$\text{ord}_{(t-t_i)} \left(n \prod_{l=1}^n y_{j_l} \right) = \frac{1}{n} \sum_{l=1}^n r_n(j_l/i) = 1. \quad \square$$

By Proposition 4.1 the polynomial $h_n(X) \in \mathbb{Q}(\mathbf{t})[X]$ is not Galois since $\mathbb{Q}(\mathbf{t}) \neq K_\sigma^V$. Instead we have to consider the minimal polynomial of u_1 over K_σ^V . To simplify the formulae we will not employ the transcendence basis of K_σ^V/\mathbb{Q} coming from Speiser's Lemma (Proposition 3.10), but

$$v_j := V_j(\boldsymbol{\zeta}, \mathbf{t})/V(\boldsymbol{\zeta}) \quad \text{for } j = 1, \dots, \varphi(n) \quad (4.10)$$

with the Vandermonde determinant $V(\boldsymbol{\zeta})$ for $\boldsymbol{\zeta} := (\zeta_n^i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times)$ and the determinant $V_j(\boldsymbol{\zeta}, \mathbf{t})$ which is obtained from $V(\boldsymbol{\zeta})$ by replacing the j -th column by the transposed of $(t_i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times)$ (compare Matzat (1987), Kap. IV, §3.1). Then by the Cramer's rule we have the inversion formula

$$t_i = \sum_{j=1}^{\varphi(n)} \zeta_n^{i(j-1)} v_j \quad \text{for } i \in (\mathbb{Z}/n\mathbb{Z})^\times. \quad (4.11)$$

Substituting t_i according to (4.11) in $h_n(\mathbf{t}, X) \in \mathbb{Q}(\mathbf{t})[X]$ from Lemma 4.2 we obtain the polynomial

$$g_n(X) = g_n(\mathbf{v}, t, X) := h_n\left(\sum_{j=1}^{\varphi(n)} \zeta_n^{i(j-1)} v_j, t, X\right) \in \mathbb{Q}(\zeta_n, \mathbf{v}, t)[X] \quad (4.12)$$

with the following properties:

Theorem 4.3. *The polynomial $g_n(X)$ in (4.12) satisfies:*

- (a) $g_n(X)$ has coefficients in $\mathbb{Z}[\mathbf{v}, t]$.
- (b) $g_n(X)$ generates a geometric Galois extension $N_n/\mathbb{Q}(\mathbf{v}, t)$ with the group Z_n .
- (c) The extension $N_n(\zeta_n)/\mathbb{Q}(\zeta_n, \mathbf{v}, t)$ is completely ramified in the numerator divisor \mathfrak{P}_i of $(t - t_i)$ for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ and unramified elsewhere.
- (d) The denominator divisor \mathfrak{P}_∞ of (t) splits completely in $N_n/\mathbb{Q}(\mathbf{v}, t)$.

Proof. Every automorphism ω of $\mathbb{Q}(\zeta_n, \mathbf{t})/\mathbb{Q}(\mathbf{v}, t)$ permutes the t_i and the ζ_n^i for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ in the same way. Obviously these automorphisms can be extended uniquely to a group of automorphisms $\tilde{\omega}$ of $\mathbb{Q}_C(\mathbf{x}, t)/\mathbb{Q}(\mathbf{v}, t)$, which permute the generators x_i also like the ζ_n^i . These extensions $\tilde{\omega}$ act on the y_j from (4.6) via

$$y_j^{\tilde{\omega}} = \left(\prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{r_n(j/i)} \right)^{\tilde{\omega}} = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_{il}^{r_n(j/i)} = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} x_i^{r_n(jl/i)} = y_{jl}$$

with $l \in (\mathbb{Z}/n\mathbb{Z})^\times$ determined by $(\zeta_n^i)^\omega = \zeta_n^{il}$. Thus the restrictions of the $\tilde{\omega}$ to $\tilde{N}_\sigma = \mathbb{Q}(\zeta_n, \mathbf{t}, \mathbf{y})$ form a group $\tilde{V} \cong V$, and the Lagrangian resolvents u_i from (4.5) lie in the fixed field $N_\sigma := \tilde{N}_\sigma^{\tilde{V}}$ of \tilde{V} . In particular $g_n(X)$, being the minimal polynomial of u_i , is contained in $\mathbb{Q}_C(\mathbf{t})^V[X] = \mathbb{Q}(\mathbf{v}, t)[X]$ by Lemma 4.2(a) with coefficients in $\mathbb{Z}[\mathbf{v}, t]$ by (4.11). Further, since

$$\text{Gal}(\tilde{N}_\sigma/\mathbb{Q}(\mathbf{v}, t)) \cong \text{Gal}(\tilde{N}_\sigma/N_\sigma) \times \text{Gal}(\tilde{N}_\sigma/\mathbb{Q}_C(\mathbf{t})) \cong V \times Z_n,$$

g_n is Galois with group Z_n , and the splitting field $N_n := N_\sigma$ of g_n is regular over $\mathbb{Q}(\mathbf{v})$. This proves (a) and (b). According to the choice of the ramification points assertion (c) follows directly from the knowledge of the class vector \mathbf{C} in (4.3).

It remains to show (d), which cannot be deduced from the general theory. For this we replace t by $t' := t^{-1}$ and use n -th roots x'_i of $1 - t't_i$ instead of the generators x_i . Now forming y'_j , u'_i , h'_n and g'_n according to the formulae (4.5)–(4.7) and (4.12) with x_i replaced by x'_i , then the u'_i also generate the Galois extension $N_n/\mathbb{Q}(\mathbf{v}, t)$, and g'_n is the minimal polynomial of the u'_i over $\mathbb{Q}(\mathbf{v}, t') = \mathbb{Q}(\mathbf{v}, t)$. Upon specialization of t' to $\bar{t}' = 0$ the x'_i become the same n -th root of unity for all i due to the compatibility with \tilde{V} , and we have $\bar{y}'_j = 1$ for $j \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus $\bar{u}'_n = \varphi(n)$ is a simple root of the specialized polynomial \tilde{g}'_n . By Theorem I.9.1 the decomposition groups of the corresponding extension $\tilde{\mathfrak{P}}_\infty$ of \mathfrak{P}_∞ and hence of all extensions of \mathfrak{P}_∞ onto N_n are trivial. \square

Corollary 4.4. *The assertions of Theorem 4.3 remain true for the residue class polynomial $\bar{g}_n(X) \in \mathbb{F}_p(\mathbf{v}, t)[X]$ of $g_n(X)$ from (4.12) modulo a prime p not dividing n , with \mathbb{F}_p in place of \mathbb{Z} respectively \mathbb{Q} .*

Proof. It suffices to show that $\bar{g}_n(X)$ stays irreducible. With a primitive n -th root of unity ζ_n over \mathbb{F}_p we have, using (4.10),

$$\bar{g}_n(\dots, V_j(\zeta, \mathbf{t})/V(\zeta), \dots, t, X) = \bar{h}_n(X) \in \mathbb{F}_p(\mathbf{t})[X]$$

with $h_n(X)$ from (4.7). By the proof of Lemma 4.2 the reduction $\bar{h}_n(X)$ is an Eisenstein polynomial with respect to the numerator divisor \mathfrak{P}_i of $(t - t_i)$ and thus irreducible even over $\mathbb{F}_p(\mathbf{t})$. Since \bar{h}_n and \bar{g}_n have the same splitting field over $\mathbb{F}_p(\mathbf{v}, t) = \mathbb{F}_p(\mathbf{t})$, \bar{g}_n is also irreducible over $\mathbb{F}_p(\mathbf{v}, t)$ and a fortiori over $\mathbb{F}_p(\mathbf{v}, t)$. \square

Remark. By specializing $(t - t_i)$ to t_i one obtains from g_n resp. \bar{g}_n the polynomials given by Dentzer (1995a) (see also Smith (1991) for odd prime powers n).

Since the polynomials $g_n(X)$ in $\varphi(n) + 1$ parameters from Theorem 4.3 are hard to compute explicitly, we specialize them to one-variable polynomials in the next section.

4.2 Cyclic Polynomials in One Variable

Specializing the independent variables $\mathbf{v} = (v_1, \dots, v_{\varphi(n)})$ in $g_n(\mathbf{v}, t, X)$ from (4.12) to $(0, 1, 0, \dots, 0)$, we obtain a polynomial

$$f_n(t, X) := g_n(0, 1, 0, \dots, 0, t, X) \in \mathbb{Z}[t, X] \quad (4.13)$$

with the following properties (see for example Dentzer (1995a), Thm. 1):

Theorem 4.5. *The polynomials $f_n(t, X)$ from (4.13) satisfy:*

- (a) $f_n(t, X)$ generates a geometric Galois extension $N_n/\mathbb{Q}(t)$ with group Z_n .
- (b) The extension $N_n(\zeta_n)/\mathbb{Q}(\zeta_n, t)$ is completely ramified in the numerator divisors \mathfrak{P}_i of $(t - \zeta_n^i)$ for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ and unramified elsewhere.
- (c) The denominator divisor \mathfrak{P}_∞ of (t) splits completely in $N_n/\mathbb{Q}(t)$.
- (d) If the prime p does not divide n , then (a)–(c) continue to hold for the reduction $\bar{f}_n(X) \in \mathbb{F}_p[t, X]$ with \mathbb{F}_p in place of \mathbb{Q} .

Proof. By Theorem 4.3 it suffices to show that the specialized polynomials $f_n(X)$ and $\bar{f}_n(X)$ are irreducible and that under the specialization t_i goes to ζ_n^i . The latter follows immediately from (4.11). The irreducibility of f_n and \bar{f}_n is an easy consequence of the fact that f_n and \bar{f}_n are Eisenstein polynomials over $\mathbb{Q}(t)$ respectively over $\mathbb{F}_p(t)$ with respect to the numerator divisors \mathfrak{P}_i of $(t - \zeta_n^i)$. \square

Remark. The polynomials $f_n(t, X)$ generate the cyclic Galois extension over $\mathbb{Q}(t)$ obtained in Theorem I.5.1 with the choice of ζ_n^i for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ as ramification points over $\bar{\Phi}(t)$.

Numerical evaluation of the formula yields:

Corollary 4.6. *With the n -th cyclotomic polynomials $\phi_n = \phi_n(t)$ we have:*

$$\begin{aligned} f_3(t, X) &= X^3 - 3\phi_3 X - (2t + 1)\phi_3, \\ f_4(t, X) &= X^4 - 4\phi_4 X^2 + 4\phi_4, \\ f_5(t, X) &= X^5 - 10\phi_5 X^3 - 5(4t^2 + 2t - 1)\phi_5 X^2 \\ &\quad - 5(3t^3 + 6t^2 + 4t + 2)\phi_1\phi_5 X - (4t^6 + 6t^5 - 5t^4 - 10t^3 - 10t^2 - 9t - 1)\phi_5. \end{aligned}$$

Remark. A list of further cyclic polynomials up to degree 16 can be found in Dentzer (1995a) and up to degree 11, as well as for 16, in the tables of the Appendix.

Theorems 4.3 and 4.5 give constructions of G-realizations of the cyclic group Z_n over all fields of characteristic prime to n . In the next section we treat the case of cyclic groups of p -power order over fields of characteristic p .

4.3 Cyclic Artin-Schreier Towers

Since in contrast to the cyclic Kummer-extensions the Artin-Schreier-extensions exist already without adjunction of suitable roots of unity, the results of this section can be read off from the general theory without crossing by a wreath-product.

Let K first be an arbitrary field of characteristic p and $\mathbb{W}(K)$ the ring of Witt vectors $\mathbf{x} = (x_1, \dots, x_n)$ of length n over K (see Jacobson (1980), Thm. 8.26). Then cyclic extensions of degree p^n over K are classified by the cyclic subgroups of order p^n of the additive group $\mathbb{W}^+(K)$ of $\mathbb{W}(K)$ modulo the subgroup $\{\mathbf{x}^p - \mathbf{x} \mid \mathbf{x} \in \mathbb{W}(K)\}$ (loc. cit., Thm. 8.31). These are generated by the Witt vectors \mathbf{x} with $x_1 \notin \{x^p - x \mid x \in K\}$ (loc. cit., Thm. 8.32). We can thus state the analogue of Theorem 4.3:

Theorem 4.7. *Let $K(\mathbf{t})$, $\mathbf{t} = (t_1, \dots, t_n)$, be a rational function field over a field K of characteristic p . Then the field*

$$N_{p,n} := K(\mathbf{t}, \mathbf{x}), \quad \text{with } \mathbf{x}^p - \mathbf{x} = \mathbf{t}, \tag{4.14}$$

generated by the components $x_i \in \overline{K(\mathbf{t})}$ of a solution \mathbf{x} of $\mathbf{x}^p - \mathbf{x} = \mathbf{t}$ in the Witt ring $\mathbb{W}(\overline{K(\mathbf{t})})$ satisfies:

- (a) $N_{p,n}$ is regular over K and Galois over $K(\mathbf{t})$ with group Z_{p^n} .
- (b) $N_{p,n}/K(\mathbf{t})$ ramifies in the denominator divisors \mathfrak{P}_i of (t_i) with ramification index p^{n+1-i} and is unramified elsewhere.
- (c) The numerator divisor \mathfrak{P}_0 of (t_1) splits completely in $K(\mathbf{t}, x_1)/K(\mathbf{t})$.

Proof. The assertion $\text{Gal}(N_{p,n}/K(\mathbf{t})) \cong Z_{p^n}$ follows immediately from the above since $t_1 \notin \{x^p - x \mid x \in K(\mathbf{t})\}$. The regularity of $N_{p,n}/K$ is a trivial consequence of (b), since a separable extension of constants is unramified.

For part (b) we consider the tower of fields

$$L_0 := K(\mathbf{t}), \quad L_i := L_{i-1}(x_i) \quad \text{with } L_n = N_{p,n}.$$

Here the L_i/L_{i-1} are Artin-Schreier-extensions

$$L_i = L_{i-1}(x_i) \quad \text{with } x_i^p - x_i = h_i(x_1, \dots, x_{i-1}) + t_i \quad (4.15)$$

(Jacobson (1980), Ch. 8.11, Proof of Lemma 2) where $h_i \in K[X_1, \dots, X_{i-1}]$ has constant term 0 (loc. cit., Ch. 8.10, (50)). Hence only the denominator divisor \mathfrak{P}_1 of (t_1) ramifies in $L_1/K(\mathbf{t})$. But now the inertia group of any extension of \mathfrak{P}_1 to $N_{p,n}$ is the full group, so \mathfrak{P}_1 is even completely ramified in $N_{p,n}/K(\mathbf{t})$. In the case $i > 1$, (4.15) implies that in L_i/L_{i-1} apart from the denominator divisors of x_1, \dots, x_{i-1} and thus of t_1, \dots, t_{i-1} precisely the denominator divisor \mathfrak{P}_i of (t_i) ramifies, which is inert in $L_{i-1}/K(\mathbf{t})$, and as above this ramifies completely in $N_{p,n}/L_{i-1}$.

By the Dedekind Criterion (Corollary I.9.3) the numerator divisor \mathfrak{P}_0 of (t_1) splits completely in $L_1/K(\mathbf{t})$. Since its extensions to L_1 remain inert in $N_{p,n}/L_1$ the decomposition group of \mathfrak{P}_0 equals $\text{Gal}(N_{p,n}/L_1) \cong Z_{p^{n-1}}$. \square

Remark. The generating polynomials of $N_{p,n}/K(\mathbf{t})$ are generic polynomials over K in the sense of Saltman (1982) or Jensen, Ledet and Yui (2002). The same holds for the polynomials $g_n(X)$ in Theorem 4.3 for odd prime powers n (see Smith (1991), Thm. 5).

The analogue of Theorem 4.5 is obtained by choosing $K = \mathbb{F}_p(t)$ in Theorem 4.7 and specializing (t_1, \dots, t_n) to $(t, 0, \dots, 0)$:

Corollary 4.8. *Let \mathbf{x} be a solution of $\mathbf{x}^p - \mathbf{x} = (t, 0, \dots, 0)$ in the Witt ring $\mathbb{W}(\overline{\mathbb{F}_p(t)})$. Then the field $N_{p,n}$ generated by the components $x_i \in \overline{\mathbb{F}_p(t)}$ of \mathbf{x} over $\mathbb{F}(t)$ satisfies:*

- (a) $N_{p,n}/\mathbb{F}_p(t)$ is a geometric Galois extension with group Z_{p^n} .
- (b) $N_{p,n}/\mathbb{F}_p(t)$ is completely ramified in the denominator divisor \mathfrak{P}_∞ of (t) and unramified elsewhere.

(c) The numerator divisor \mathfrak{P}_0 of (t) splits completely in $N_{p,n}/\mathbb{F}_p(t)$.

Proof. As $t \notin \{x^p - x \mid x \in \mathbb{F}_p(t)\}$ the specialized field extension $N_{p,n}/\mathbb{F}_p(t)$ possesses the Galois group Z_{p^n} . Thus (a) and (b) follow immediately from Theorem 4.7(a) and (b). By Theorem 4.7(c) the divisor \mathfrak{P}_0 splits completely in $L_1/K(\mathbf{t})$ and the numerator divisor of (x_1) is an extension $\mathfrak{P}_0^{(1)}$ of \mathfrak{P}_0 . Since the constant term of h_1 in (4.15) vanishes, by the Dedekind Criterion (Corollary I.9.3) $\mathfrak{P}_0^{(1)}$ splits completely in L_2/L_1 and the numerator divisor of (x_2) is divisible by an extension $\mathfrak{P}_0^{(2)}$ of $\mathfrak{P}_0^{(1)}$. Induction then yields an unramified prime divisor $\mathfrak{P}_0^{(n)}$ of \mathfrak{P}_0 in $N_{p,n}$ of degree 1 and thus with trivial decomposition group. Hence here \mathfrak{P}_0 even splits completely in $N_{p,n}/K(\mathbf{t})$. \square

We finish the paragraph by giving the two simplest generating polynomials for $N_{p,n}/\mathbb{F}_p(t)$.

Corollary 4.9. *The fields $N_{p,n}/\mathbb{F}_p(t)$ in Corollary 4.8 for $n \leq 2$ by (4.15) are generated by the Artin-Schreier-polynomials*

$$\begin{aligned} f_{p,1}(t, X_1) &= X_1^p - X_1 - t \in \mathbb{F}_p(t)[X_1], \\ f_{p,2}(t, X_2) &= X_2^p - X_2 - \frac{1}{p} \sum_{i=1}^{p-1} (-1)^{p-i} \binom{p}{i} X_1^{ip+p-i} \in \mathbb{F}_p(t, x_1)[X_2], \end{aligned}$$

with a zero x_1 of $f_{p,1}(t, X_1)$ in $\overline{\mathbb{F}_p(t)}$.

A generating polynomial of $N_{p,2}/\mathbb{F}_p(t)$ can be computed from this using the Buchberger algorithm.

Remark. Using Corollary IV.1.7 from the next Chapter it follows from Theorem 4.5 and Corollary 4.8 that every finite abelian group possesses a G-realization over any prime field and hence over any field.

5 Rigid Braid Orbits

In this paragraph we study the question when the fixed field of a class of generating systems is regular over \mathbb{Q} and rational. The first question may be answered by proving rigidity of the corresponding braid orbit, the second by calculation of braid orbit genera. As main result we obtain the Rigid Braid Orbit Theorem, which is then demonstrated on the example of $L_2(25)$. The last two sections contain a translation theorem for braid orbits and a higher dimensional analogue of the Extension Theorem I.8.7.

5.1 The Regularity Criterion

For the action defined in (3.10) of \tilde{H}_s on G and hence also on $\Sigma_s(G)$ we have by Theorem 1.6 with Corollary 2.3:

Proposition 5.1. *Let G be a finite group. Then for $s \geq 3$ the generators β_i of \tilde{H}_s act on $\Sigma_s(G)/\text{Inn}(G)$ via (3.10) as*

$$[\sigma_1, \dots, \sigma_s]^{\beta_i} = [\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1} \sigma_i^{-1}, \sigma_i, \sigma_{i+2}, \dots, \sigma_s]. \quad (5.1)$$

In particular the pure Hurwitz braid group H_s permutes the classes of generating systems in $\Sigma(\mathbf{C})/\text{Inn}(G)$ for each class vector \mathbf{C} of G .

Now let V be a symmetry group of \mathbf{C} . The orbit of $[\sigma] \in \Sigma(\mathbf{C}^V)/\text{Inn}(G)$ under the action (5.1) of

$$H_s^V := \tilde{H}_s \cap \tilde{\Delta}_{\mathbf{C}}^V = \{\beta \in \tilde{H}_s \mid \mathbf{C}^\beta \in \mathbf{C}^V\} \quad (5.2)$$

will from now on be symbolized by

$$B^V(\sigma) := [\sigma]^{H_s^V} \quad (\text{resp. } B(\sigma) \text{ for } V = 1) \quad (5.3)$$

and will be called the V -symmetrized braid orbit of $[\sigma]$. The number of such braid orbits in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ is denoted by

$$h^V(\mathbf{C}^V) := |\Sigma(\mathbf{C}^V)/\text{Inn}(G) H_s^V| \quad (\text{resp. } h(\mathbf{C}) \text{ for } V = 1) \quad (5.4)$$

in analogy to I, (6.18) (resp. I, (4.18) in the case $V = 1$).

For a V -symmetrized braid orbit $B \subseteq \Sigma(\mathbf{C}^V)/\text{Inn}(G)$ let further

$$\Delta_B^V := \{\delta \in \tilde{\Delta}_{\mathbf{C}}^V \mid [\sigma]^\delta \in B \text{ for } [\sigma] \in B\} \quad (5.5)$$

be the stabilizer of the braid orbit. The corresponding fixed field then satisfies:

Proposition 5.2. *The fixed field of the V -symmetrized braid orbit $B = B^V(\sigma)$ of $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ of G has the form*

$$\bar{M}_s(t)^{\Delta_B^V} = k_\sigma^V(\mathbf{t}^V), \quad (5.6)$$

where k_σ^V denotes the algebraic closure of \mathbb{Q} in K_σ^V and \mathbf{t}^V is defined by (3.21).

Proof. Let

$$H_\sigma^V := H_s^V \cap \Delta_\sigma^V \quad (5.7)$$

be the stabilizer of $[\sigma]$ in H_s^V . Then since $H_\sigma^V \leq \Delta_B^V$ the H_s^V -orbit $B^V(\sigma)$ of $[\sigma]$ equals the Δ_B^V -orbit. Since this implies

$$[K_\sigma^V : \bar{M}_s(t)^{\Delta_B^V}] = (\Delta_B^V : \Delta_\sigma^V) = (H_s^V : H_\sigma^V) = [\bar{\mathbb{Q}} K_\sigma^V : \bar{M}_s(t)^{H_s^V}],$$

the algebraic closure of \mathbb{Q} in $\bar{M}_s(t)^{\Delta_B^V}$ coincides with the one in K_σ^V . Now $\Delta_B^V \leq \tilde{\Delta}_C^V$, so by (3.21) $\bar{\mathbb{Q}}_C^V(\mathbf{t}^V)$ is a subfield of $\bar{M}_s(t)^{\Delta_B^V}$. Consequently we also have $k_\sigma^V(\mathbf{t}^V) \leq \bar{M}_s(t)^{\Delta_B^V}$, which, as

$$\bar{\mathbb{Q}} \bar{M}_s(t)^{\Delta_B^V} = \bar{M}_s(t)^{H_s^V} = \bar{\mathbb{Q}}(\mathbf{t}^V)$$

proves (5.6). \square

Proposition 5.2 furnishes an interpretation for the extension of constants in $K_\sigma^V/\bar{\mathbb{Q}}_C^V(\mathbf{t}^V)$ as well as for the purely geometric part. The degree of the latter obviously equals the orbit length $|B^V(\sigma)|$. To obtain a good estimate for the extension of constants we first have to introduce some more notation. In analogy to I, (6.17), for an open subgroup $U \leq H_s^V$ let

$$h_U^V(\mathbf{C}) := |\{B^V(\sigma) \mid \sigma \in \Sigma(\mathbf{C}^V), H_\sigma^V = U^\alpha \text{ for an } \alpha \in \text{Aut}(H_s^V)\}| \quad (5.8)$$

be the number of braid orbits of those $[\sigma] \in \Sigma(\mathbf{C}^V)/\text{Inn}(G)$ whose stabilizer H_σ^V in H_s^V coincides with U up to an automorphism. Those braid orbits $B^V(\sigma)$ with $h_{H_\sigma^V}^V(\mathbf{C}) = 1$ are distinguished by their stabilizers and are called *rigid* H_s^V -orbits.

Furthermore, \mathbf{C} is called a H_s^V -rigid class vector if $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ consists of a single H_s^V -orbit.

Theorem 5.3 (Regularity Theorem). *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$ a class vector of G and V a symmetry group of \mathbf{C} . Also for $\sigma \in \Sigma(\mathbf{C})$ let K_σ^V denote the fixed field of Δ_σ^V and k_σ^V the algebraic closure of \mathbb{Q} in K_σ^V . Then we have*

$$[K_\sigma^V : k_\sigma^V(\mathbf{t}^V)] = |B^V(\sigma)| \text{ and } [k_\sigma^V : \bar{\mathbb{Q}}_C^V] \leq h_{H_\sigma^V}^V(\mathbf{C}). \quad (5.9)$$

In particular $K_\sigma^V/\bar{\mathbb{Q}}_C^V$ is regular if $B^V(\sigma)$ is a H_s^V -rigid braid orbit.

Proof. By what precedes it remains to prove the inequality in (5.9). By the class equation $[k_\sigma^V : \bar{\mathbb{Q}}_C^V]$ equals the number of braid orbits $B^V(\sigma)$ in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$

permuted by $\tilde{\Delta}_{\mathbf{C}}^V$. Now let $\delta \in \tilde{\Delta}_{\mathbf{C}}^V$, $B = B^V(\sigma)$ be a braid orbit in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ and $B^\delta = B^V(\sigma^\delta)$ the image of B under δ . Then the stabilizer of $[\sigma^\delta]$ in H_s^V satisfies $H_{\sigma^\delta}^V = (H_\sigma^V)^{\delta^{-1}}$ by Proposition 3.5. As $H_s^V \triangleleft \tilde{\Delta}_{\mathbf{C}}^V$, it is the image of H_σ^V under an automorphism of H_s^V . Thus using the definition (5.8) of $h_U^V(\mathbf{C})$ for $U = H_\sigma^V$ we obtain

$$[k_\sigma^V : \mathbb{Q}_{\mathbf{C}}^V] = |\{B^V(\sigma^\delta) \mid \delta \in \tilde{\Delta}_{\mathbf{C}}^V\}| \leq h_U^V(\mathbf{C}). \quad \square$$

In contrast to the situation in Theorem I.6.8 the extension $K_\sigma^V/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^V)$ of degree

$$[K_\sigma^V : \mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^V)] \leq l_U^V(\mathbf{C}) \quad \text{for } U = H_\sigma^V$$

is here decomposed into a purely geometric part of degree $|B^V(\sigma)|$ and an extension of constants $k_\sigma^V/\mathbb{Q}_{\mathbf{C}}^V$, whose degree is bounded by the (generally much smaller) number of braid orbits $h_U^V(\mathbf{C})$. A disadvantage now comes from the fact that in general K_σ^V is not a rational function field any more. In the next section we give explicit criteria for rationality of K_σ^V in the case $V = 1$.

5.2 Braid Orbit Genera

As above let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ a class vector of G with $s \geq 3$ components, $\sigma \in \Sigma(\mathbf{C})$ and $B(\sigma) = [\sigma]^{H_s}$ the orbit of $[\sigma]$ under the pure braid group H_s . Also let

$$B_s(\sigma) := [\sigma]^{\Gamma_{s-1}} \quad \text{and} \quad B_j(\sigma) := B_{j+1}(\sigma)^{\Gamma_{j-1}} \quad \text{for } 1 \leq j \leq s-1 \quad (5.10)$$

be the orbit of $B_{j+1}(\sigma)$ under $\Gamma_{j-1} := \Gamma_{j-1}^{(s)} / \Gamma_j^{(s)}$ (with $\Gamma_j^{(s)}$ from Corollary 2.9), where the elements of the orbit $B_j(\sigma)$ are orbits of type B_{j+1} . Denote the number of cycles of $\beta_{ij} \Gamma_j^{(s)}$ on $B_j(\sigma)$ with c_{ij} . Then

$$g_j(\sigma) := 1 - |B_j(\sigma)| + \frac{1}{2} \sum_{i=1}^{j-1} (|B_j(\sigma)| - c_{ij}) \quad (5.11)$$

is called the j -th braid orbit genus of σ .

In analogy to the previous section we call a braid orbit $B_j(\sigma)$ rigid if there are no further braid orbits $B_j(\tau)$ in $B_{j+1}(\sigma)^{H_j}$ such that the stabilizers of the elements of $B_j(\sigma)$ and $B_j(\tau)$ differ in H_j only by an automorphism of H_j .

Proposition 5.4. *If $B_j(\sigma)$ is a rigid Γ_{j-1} -orbit, then*

$$|B_i(\sigma)| = 1 \quad \text{and} \quad g_i(\sigma) = 0 \quad \text{for } i = 1, \dots, j-1. \quad (5.12)$$

Proof. If $B_j(\sigma)$ is a rigid Γ_{j-1} -orbit in $B_{j+1}(\sigma)^{H_j}$, then it stays invariant under all factor groups $\Gamma_{i-1} = \Gamma_{i-1}^{(s)} / \Gamma_i^{(s)}$ for $i < j$. Consequently we have $|B_i(\sigma)| = 1$ and $g_i(\sigma) = 0$ for $i < j$. \square

Remark. Since $\Gamma_2 = H_3 \cong Z_2$ acts trivially on all Γ_3 -orbits inside a H_4 -orbit, as $H_4 \cong \Gamma_3 \rtimes H_3$, (5.12) certainly holds for all $i \leq 3$.

The case $s = 4$ also possesses another particularity:

Proposition 5.5. *In the case $s = 4$ we have $g_4(\sigma) = g_4(\sigma^\beta)$ for all $\beta \in \tilde{H}_4$.*

Proof. It is easily verified that for $s = 4$ the pairs β_{14} and β_{23} , β_{24} and $\beta_{14}^{-1}\beta_{13}\beta_{14}$, and β_{34} and β_{12} all have the same action on $\Sigma_4(G)$ since they only differ by the central involution $\iota_4 = (\beta_1\beta_2)^3$. Thus the permutation types of $\{\beta_{14}, \beta_{24}, \beta_{34}\}$ coincide with those of $\{\beta_{1\omega}4\omega, \beta_{2\omega}4\omega, \beta_{3\omega}4\omega\}$ for all $\omega \in S_4$ and hence also with those of $\{\beta_{14}^\beta, \beta_{24}^\beta, \beta_{34}^\beta\}$ for all $\beta \in \tilde{H}_4$. \square

The corresponding assertion for $s \geq 5$ is false in general. The next theorem contains the fundamental characterization of the braid orbit genera by intermediate fields of K_σ/k_σ .

Theorem 5.6. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ a class vector of G with $s \geq 3$ and $\sigma \in \Sigma(\mathbf{C})$. Also let K_j be the algebraic closure of $\mathbb{Q}(t_1, \dots, t_j)$ inside K_σ . Then for $1 \leq j \leq s$ the field extensions $K_j/K_{j-1}(t_j)$ satisfy*

$$[K_j : K_{j-1}(t_j)] = |B_j(\sigma)| \quad \text{and} \quad g(K_j/K_{j-1}) = g_j(\sigma). \quad (5.13)$$

Proof. The proof uses descending induction on j . First, clearly we have $K_\sigma = K_s(t)$ with $t = t_{s+1}$ and $K_{s-1} = K_s \cap \bar{M}_{s-1}$. Thus application of Theorem 2.8 yields

$$[K_s : K_{s-1}(t_s)] = [\bar{K}_s : \bar{M}_{s-1}(t_s)] = (\Gamma_{s-1} : (\Gamma_{s-1} \cap H_\sigma)) = |B_s(\sigma)|$$

with $\bar{K}_s := \bar{M}_{s-1}K_s$. Similarly for $1 < j < s$ with $\bar{K}_j := \bar{M}_{j-1}K_j$ and

$$\Psi_j := \text{Gal}(\bar{M}_s/\bar{K}_j(t_{j+1}, \dots, t_s)) = \Gamma_{j-1}^{(s)} \cap H_\sigma \Gamma_j^{(s)}$$

we obtain the sequence of equalities

$$[K_j : K_{j-1}(t_j)] = [\bar{K}_j : \bar{M}_{j-1}(t_j)] = (\Gamma_{j-1}^{(s)} / \Gamma_j^{(s)} : \Psi_j / \Gamma_j^{(s)}) = |B_j(\sigma)|.$$

Here we have $K_0 = k_\sigma$ by Theorem 5.3. This proves the first part of the assertion.

Let $f(X)$ be the minimal polynomial of a primitive element of $\bar{K}_j/\bar{M}_{j-1}(t_j)$. The Galois group of $f(X)$ is equivalent as permutation group on the zeroes of $f(X)$ to the permutation representation of $\Gamma_j^{(s)}$ on the cosets of Ψ_j in $\Gamma_{j-1}^{(s)}$, respectively of $\Gamma_{j-1}^{(s)} / \Gamma_j^{(s)}$ on the cosets of $\Psi_j / \Gamma_j^{(s)}$, and hence to the permutation representation of Γ_{j-1} on $B_j(\sigma)$. By Theorem 2.10, and since $\bar{K}_j \leq \bar{M}_j$ only the valuation ideals \mathfrak{D}_{ij} generated by the $(t_i - t_j)$ for $1 \leq i < j$ ramify in $\bar{K}_j/\bar{M}_{j-1}(t_j)$. Here by Theorem 2.4 the inertia group of a suitable extension of \mathfrak{D}_{ij} onto \bar{M}_j is generated by the element $\beta_{ij} \Gamma_j^{(s)} \in \text{Gal}(\bar{M}_j/\bar{M}_{j-1}(t_j))$. According to Theorem I.9.1 the ramification type of \mathfrak{D}_{ij} in $\bar{K}_j/\bar{M}_{j-1}(t_j)$ and hence the degree of the different of

$\bar{K}_j/\bar{M}_{j-1}(t_j)$ may be read off from the cycle decomposition of $\beta_{ij}\Gamma_j^{(s)}$ on $B_j(\sigma)$; it equals

$$\sum_{i=1}^{j-1} \sum_{k=1}^{c_{ij}} (e_{ijk} - 1) = \sum_{i=1}^{j-1} (|B_j(\sigma)| - c_{ij}),$$

where c_{ij} denotes the number of cycles of $\beta_{ij}\Gamma_j^{(s)}$ on $B_j(\sigma)$ and e_{ijk} for $1 \leq k \leq c_{ij}$ their lengths. The genus formula then yields

$$g(\bar{K}_j/\bar{M}_{j-1}) = 1 - [\bar{K}_j : \bar{M}_{j-1}(t_j)] + \frac{1}{2} \sum_{i=1}^{j-1} (|B_j(\sigma)| - c_{ij}) = g_j(\sigma).$$

Since the genus of K_j/K_{j-1} does not change by the extension of constants to \bar{M}_{j-1} , the second part of the assertion follows. \square

In the further text the field K_s in Theorem 5.6 will play a special role and then be denoted by \mathcal{H}_σ , so that $K_\sigma = \mathcal{H}_\sigma(t)$.

5.3 A Rationality Criterion for the Pure Braid Group

With the help of Theorem 5.6 it is now easy to formulate sufficient criteria for the rationality of K_σ/k_σ . One is given by the following oddness condition, whose validity implies the existence of a divisor of odd degree in K_j/K_{j-1} :

(O_j) In the action of $\beta_{ij}\Gamma_j^{(s)}$ on $B_j(\sigma)$ there occurs for some $i < j$ a cycle length e_{ijk} an odd number of times.

With this we get:

Theorem 5.7 (Braid Orbit Theorem). *Let G be a finite group with trivial center, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$, $\sigma \in \Sigma(\mathbf{C})$ and $B(\sigma)$ the H_s -orbit of $[\sigma]$. For $j = 4, \dots, s$ assume further that $g_j(\sigma) = 0$ and that the oddness condition (O_j) is satisfied. Then $K_\sigma = k_\sigma(u_1, \dots, u_s, t)$ is a rational function field over k_σ and there exists a geometric Galois extension $N_\sigma/k_\sigma(\mathbf{u}, t)$ with*

$$\text{Gal}(N_\sigma/k_\sigma(\mathbf{u}, t)) \cong G \quad \text{and} \quad \bar{M}_s N_\sigma = \bar{N}_\sigma. \quad (5.14)$$

Proof. By the Remark following Proposition 5.4 we have $K_3 = k_\sigma(t_1, t_2, t_3)$. For j with $4 \leq j \leq s$ let now K_{j-1}/k_σ be a rational function field. Then by (5.13) the genus $g(K_j/K_{j-1}) = g_j(\sigma)$ equals zero. Since only prime divisors of equal degree are conjugate in \bar{K}_j/K_j , the oddness condition (O_j) together with Theorem I.9.1 imply that the valuation \mathfrak{D}_{ij} ideal generated by $(t_i - t_j)$ possesses an extension onto K_j with odd residue class degree. Thus K_j/K_{j-1} and hence by induction K_j/k_σ is a rational function field. The first part of the assertion then follows from the fact that $K_\sigma = \mathcal{H}_\sigma(t)$ with $\mathcal{H}_\sigma = K_s$ according to the notation introduced at the end of the last section. The second part is obtained using Theorem 3.9(b) for $V = 1$. \square

Under the additional assumption that $B(\sigma)$ is a rigid braid orbit, the Regularity Theorem 5.3 implies:

Corollary 5.8 (Rigid Braid Orbit Theorem). *If in Theorem 5.7 the braid orbit $B(\sigma)$ is additionally supposed rigid, then there even exists a rational function field $\mathbb{Q}_C(\mathbf{u}, t)/\mathbb{Q}_C$ and a geometric Galois extension $N_\sigma/\mathbb{Q}_C(\mathbf{u}, t)$ with*

$$\text{Gal}(N_\sigma/\mathbb{Q}_C(\mathbf{u}, t)) \cong G \quad \text{and} \quad \bar{M}_s N_\sigma = \bar{N}_\sigma. \quad (5.15)$$

In particular we have $\mathbb{Q}_C = \mathbb{Q}$ if C is a rational class vector.

This result is now employed to construct G -realizations over \mathbb{Q} for the simple group $L_2(25)$. This is the smallest among the groups $L_2(q)$ with $q \neq 16$ for which such a realization could not be found with the rigidity theorems in the first chapter.

Example 5.1 (Przywara (1991)). Let $G = P\Sigma L_2(25)$ be the group obtained from the simple group $L_2(25)$ by extension with the field automorphism. Then the class vector $\mathbf{C} = (2A, 2C, 2D, 12A)$ of G in Atlas notation is rational with $l(\mathbf{C}) = 12$ and $h(\mathbf{C}) = 1$, i.e., $B = \Sigma(\mathbf{C})/\text{Inn}(G)$ forms a rigid braid orbit. The permutation types of β_{i4} on B may be calculated as $(3^2, 2^2, 1^2)$ for β_{14} and $(5, 3, 2^2)$ for β_{24} and β_{34} . Thus we have $g_4(\sigma) = 0$ for $[\sigma] \in B$. Since clearly the oddness condition (O_4) is also satisfied, by the Rigid Braid Orbit Theorem $K_\sigma = \mathbb{Q}(u_1, \dots, u_4, t)$ is a rational function field over \mathbb{Q} and there exists a geometric Galois extension $N/\mathbb{Q}(\mathbf{u}, t)$ with the group $P\Sigma L_2(25)$.

The fixed field K'_σ of the subgroup $G' \cong L_2(25)$ of G is of degree 2 over $\mathbb{Q}(\mathbf{u}, t)$ and is regular over $\mathbb{Q}(\mathbf{u})$. Since $2A \subset G'$ and $12A \subset G'$ only the numerator divisors \mathfrak{P}_i of $(t - t_i)$ for $i = 2, 3$ are ramified in $K'_\sigma/\mathbb{Q}(\mathbf{u}, t)$. By the genus formula $K'_\sigma/\mathbb{Q}(\mathbf{u})$ has genus zero and is even a rational function field, since for example the prime divisor of \mathfrak{P}_2 in $K'_\sigma/\mathbb{Q}(\mathbf{u}, t)$ is of degree 1. Thus we have $K'_\sigma = \mathbb{Q}(\mathbf{u}, z)$, say, and $\text{Gal}(N/\mathbb{Q}(\mathbf{u}, z))$ yields a G -realization of $L_2(25)$ over \mathbb{Q} . \square

Example 5.1 has been generalized by Shiina (2003b) to groups $L_2(p^2)$ with $p \not\equiv \pm 1 \pmod{24}$ and by Dettweiler (2003) for $S_{2n}(p^2)$ with the same p . A more far reaching result by Thompson and Völklein (1998) is presented here in Theorem 10.9 as an application of the Katz algorithm.

5.4 Rational Translation of Braid Orbits

Next we want to investigate the behavior of braid orbits under translation. Because of the number of generators of the acting braid group a braid orbit can only be expected to be the full image of another braid orbit, if the translation maps a class vector of length s into one of length at most s . For $s \geq 4$ this is only possible under rather restrictive conditions. Let $\bar{N}/\bar{M}_s(t)$ be a Galois extension with group G contained in $\bar{M}_{s+1}(t)$ parametrized by $[\sigma]$ and with class vector \mathbf{C} , i.e., $\bar{N} = \bar{N}_\sigma$ with $\sigma \in \Sigma(\mathbf{C})/\text{Inn}(G)$, and $\bar{L}/\bar{M}_s(t)$ the rational field extension chosen to achieve

the translation. Then the number of ramified points of $\bar{N}\bar{L}/\bar{L}$, multiplied by their residue class degrees, satisfy

$$ns - 2(n-1) - i \leq s$$

by the Hurwitz relative genus formula, where i denotes the number of prime divisors of \bar{L} ramified in $\bar{L}/\bar{M}_s(t)$ but unramified in $\bar{N}\bar{L}/\bar{L}$. Since $i \leq 2(n-1)$ this forces $s = 4$. But then we have $i = 2(n-1)$ and all ramification orders in $\bar{L}/\bar{M}_s(t)$ are equal to 2. If we further assume that the class vector \mathbf{C} does not only consist of involution classes (which rules out only fields \bar{N} of genus $g(\bar{N}/\bar{M}_s) = 1$), then we either have $(n, i) = (2, 2)$ and $\bar{L}/\bar{M}_s(t)$ is a Z_2 -translation of type $(1A, 1A, 2A, 2A)$, or $(n, i) = (4, 6)$ and $\bar{L}/\bar{M}_s(t)$ is an E_4 -translation of type $(1A, 2A, 2A, 2A)$. If without loss of generality we restrict ourselves to primitive field extensions, then a single possibility for the translation field remains. This proves part (a) of the following theorem:

Theorem 5.9. (a) *For a finite Galois extension $\bar{N}/\bar{M}_s(t)$ inside $\bar{M}_{s+1}/\bar{M}_s(t)$ of genus $g > 1$ with at least $s \geq 4$ ramification points there exists only one possible primitive translation into a Galois extension with at most s ramification points, namely a Z_2 -translation φ_{Z_2} with the class vector $(1A, 1A, 2A, 2A)$.*

(b) *The translation φ_{Z_2} from (a) maps a generating 4-system σ belonging to the class vector $\mathbf{C} = (C_1, C_2, C_3, C_4)$ with two involution classes C_3 and C_4 to*

$$\tilde{\sigma} := \varphi_{Z_2}(\sigma) = (\sigma_1, \sigma_1^{\sigma_3\sigma_2^{-1}}, \sigma_2, \sigma_2^{\sigma_3}) \in \tilde{\Sigma}(\tilde{\mathbf{C}}) \quad (5.16)$$

with $\tilde{\mathbf{C}} = (C_1, C_1, C_2, C_2)$. If G possesses no subgroup of index 2 then $\tilde{\sigma}$ is a generating system of G .

(c) *If moreover G has trivial center, then the translation map*

$$\varphi_{Z_2} : \Sigma(\mathbf{C})/\text{Inn}(G) \rightarrow \Sigma(\tilde{\mathbf{C}})/\text{Inn}(G)$$

is injective and maps $H_4^{Z_2}$ -orbits onto full $H_4^{Z_2}$ -orbits for

$$H_4^{Z_2} := \{\beta \in \tilde{H}_4 \mid q(\beta) \in Z_2 = \langle(34)\rangle\} = H_4 \cup H_4\beta_3.$$

Proof. By the preceding considerations, only (b) and (c) remain to be proved.

As $i = 2$ the original class vector \mathbf{C} contains two classes of involutions, which by the choice of the translation class vector $(1A, 1A, 2A, 2A)$ are the classes C_3 and C_4 . The translation formula can now be obtained as in the proof of Theorem I.6.3: The Galois group $\text{Gal}(\bar{M}_{s+1}/\bar{L})$, which in accordance with Theorem I.6.3 will be denoted by $\Psi_{Z_2} \trianglelefteq \Gamma_4$, is generated by the generators of inertia groups $\gamma_1, \gamma_2, \gamma_3^2, \gamma_4^2$, together with two elements conjugate to γ_i , $i = 1, 2$, by non-trivial coset representatives of Ψ_{Z_2} in Γ_4 . For example, with the choice $\tilde{\gamma}_1 = \gamma_1^{\gamma_3^{-1}\gamma_2^{-1}}, \tilde{\gamma}_2 = \gamma_2^{\gamma_3^{-1}}$, the generating system $(\gamma_1, \tilde{\gamma}_1, \gamma_2, \tilde{\gamma}_2, \gamma_3^2, \gamma_4^2)$ satisfies the product relation, and we have

$$\Psi_{Z_2} = \langle \gamma_1, \gamma_1^{\gamma_3^{-1}\gamma_2^{-1}}, \gamma_2, \gamma_2^{\gamma_3^{-1}}, \gamma_3^2, \gamma_4^2 \mid \gamma_1 \cdots \gamma_4^2 = 1 \rangle, \quad (5.17)$$

since Ψ_{Z_2} is a free profinite group of rank 5. Application of the canonical epimorphism

$$\psi : \Gamma_4 \rightarrow G, \quad \gamma_i \mapsto \sigma_i \in C_i,$$

yields the translation formula (5.16) due to $\sigma_3^2 = \sigma_4^2 = 1$. By construction $\tilde{\sigma}$ generates a subgroup of G isomorphic to $\text{Gal}(\bar{N}/\bar{L})$. Since this can have index at most 2 in G , the additional assumption forces $G = \langle \tilde{\sigma} \rangle$.

If the center of G is trivial (or has odd order), then the translation map φ_{Z_2} is injective by Theorem I.7.4. It remains to verify the compatibility with the $H_4^{Z_2}$ -orbits. For this we compute the φ_{Z_2} -image of the $H_4^{Z_2}$ -orbit $B^{Z_2}(\sigma)$ of σ . Since the action of the central element $\iota_4 = (\beta_1 \beta_2)^3 \in H_4$ on $B^{Z_2}(\sigma)$ is trivial, it suffices to determine the image of the generators of

$$\Gamma_3 \cup \Gamma_3 \beta_3 = \langle \beta_{14}, \beta_{24}, \beta_3 \rangle.$$

This equals

$$\begin{aligned} \varphi_{Z_2}(\sigma^{\beta_{14}}) &= \varphi_{Z_2}(\sigma)^{\beta_2^{-1} \beta_3^{-1} \beta_2 \beta_3 \beta_2}, \\ \varphi_{Z_2}(\sigma^{\beta_{24}}) &= \varphi_{Z_2}(\sigma)^{\beta_2^{-2} \beta_3 \beta_2^2}, \\ \varphi_{Z_2}(\sigma^{\beta_3}) &= \varphi_{Z_2}(\sigma)^{\beta_2^{-1} \beta_{34} \beta_2}. \end{aligned} \quad (5.18)$$

Hence the subgroup U of \tilde{H}_4 generated by $\beta_2^{\beta_3 \beta_2}, \beta_3^{\beta_2^2}, \beta_{34}^{\beta_2}$ and the central element ι_4 acts on the image $\varphi_{Z_2}(B^{Z_2}(\sigma))$. Now $U^{\beta_2^{-1}}$ obviously contains the elements β_{34} and $(\beta_2^{\beta_3})^2 = (\beta_2^2)^{\beta_3} = \beta_{24}$, and thus by the sphere relation (1.13) also β_{14} , so we conclude $H_4 \leq U^{\beta_2^{-1}}$ and thus $U^{\beta_2^{-1}} = \langle H_4, \beta_2^{\beta_3}, \beta_3^{\beta_2} \rangle$. The relation

$$\beta_3^2 \beta_2^{\beta_3} (\beta_3^{\beta_2})^{-1} \beta_2^{-2} = 1$$

finally implies $U^{\beta_2^{-1}} = \langle H_4, \beta_3^{\beta_2} \rangle$, whence the result

$$U = \langle H_4^{\beta_2}, \beta_3^{\beta_2^2} \rangle = \langle H_4, \beta_3 \rangle = H_4^{Z_2}. \quad \square$$

Example 5.2. For the group A_5 the sets $\Sigma(\mathbf{C}_i)/\text{Inn}(G)$ for $\mathbf{C}_1 = (3A, 2A, 2A, 2A)$, $\mathbf{C}_2 = (3A, 3A, 2A, 2A)$ and $\mathbf{C}_3 = (3A, 3A, 3A, 3A)$ each form a single H_4 -orbit of length 18. The above theorem now shows that the orbits B_2 and B_3 can be obtained by a rational translation from B_1 . But this translation does not preserve the braid orbit genera: We have $g_4(\sigma_1) = 1$, $g_4(\sigma_2) = 2$, $g_4(\sigma_3) = 1$ for $\sigma_i \in B_i$. \square

Example 5.3. For $G = S_5$ the set $B := \Sigma(\mathbf{C})/\text{Inn}(G)$ for $\mathbf{C} = (6A, 6A, 2A, 2A)$ forms a single H_4 -orbit of length 24. Although the translation map φ_{Z_2} to $\Sigma(\tilde{\mathbf{C}})/\text{Inn}(G)$ with $\tilde{\mathbf{C}} = (6A, 6A, 6A, 6A)$ is injective, since A_5 contains no elements of order 6, $\varphi_{Z_2}(B)$ splits into two H_4 -orbits \tilde{B}_1, \tilde{B}_2 , of lengths 12, whose union is a single $H_4^{Z_2}$ -orbit. This example shows that the translation map in Theorem 5.9(c) does not in general preserve H_4 -orbits. On the other hand, this can be used for a

reduction of braid orbit genera. In this case we have $g(\sigma) = 2$ and $g(\tilde{\sigma}) = 0$ for $\sigma \in B$, $\tilde{\sigma} \in \tilde{B}_1 \cup \tilde{B}_2$. \square

In view of Theorem 5.9 it is natural to ask under which conditions a braid orbit $B = B(\sigma)$ is mapped at least into a single braid orbit under a rational translation. As the Example 5.3 shows, this will in general require additional assumptions which guarantee that the field \mathcal{K}_σ and the field \mathcal{L} generated over $\bar{\mathbb{Q}}(\mathbf{t})$ by the ramification points of $\bar{L}/\bar{M}_s(t)$ are linearly disjoint over $\bar{\mathbb{Q}}(\mathbf{t})$. With a specialization argument it can be shown that this hypothesis is already sufficient.

5.5 Groups of Automorphisms as Galois Groups

At the end of this paragraph we prove a higher-dimensional analogue of the Extension Theorem I.8.7. Let V be a symmetry group of the class vector $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$. According to (5.2) and (5.3)

$$B^V(\sigma) := [\sigma]^{H_s^V} \quad \text{with} \quad H_s^V := \{\beta \in \tilde{H}_s \mid \mathbf{C}^\beta \in \mathbf{C}^V\}$$

denotes the V -symmetric braid orbit of $[\sigma]$. For an intermediate group A between $\text{Inn}(G)$ and $\text{Aut}(G)$ set, in analogy to the notation in Chapter I.8,

$$\Delta_{\sigma^A}^V := \{\delta \in \tilde{\Delta}_{\mathbf{C}}^V \mid \sigma^{\delta A} = \sigma^A\} \quad \text{and} \quad H_{\sigma^A}^V := \tilde{H}_s \cap \Delta_{\sigma^A}^V \quad (5.19)$$

with $\tilde{\Delta}_{\mathbf{C}}^V$ from (3.20) and

$$K_{\sigma^A}^V := \bar{M}_s(t)^{\Delta_{\sigma^A}^V} \quad \text{and} \quad \bar{K}_{\sigma^A}^V := \bar{M}_s(t)^{H_{\sigma^A}^V} = \bar{\mathbb{Q}} K_{\sigma^A}^V. \quad (5.20)$$

Then we first have:

Theorem 5.10. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$, V a symmetry group of \mathbf{C} and $B^V(\sigma)$ the V -symmetrized braid orbit of $\sigma \in \Sigma(\mathbf{C}^V)$. Furthermore let A be an intermediate group between $\text{Inn}(G)$ and $\text{Aut}(G)$ acting on $B^V(\sigma)$. Then there exists a geometric Galois extension $N_{\sigma^A}^V/K_{\sigma^A}^V$ with*

$$\text{Gal}(N_{\sigma^A}^V/K_{\sigma^A}^V) \cong A \quad \text{and} \quad \text{Gal}(N_{\sigma^A}^V/K_{\sigma^A}^V) \cong \text{Inn}(G). \quad (5.21)$$

If here $B^V(\sigma)$ is rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$, then $K_{\sigma^A}^V/\mathbb{Q}_{\mathbf{C}}^V$ is regular.

Proof. Let $\bar{N}_\sigma/\bar{M}_s(t)$ be the Galois extension with $\text{Gal}(\bar{N}_\sigma/\bar{M}_s(t)) \cong G$ belonging to $[\sigma]$ by the Hurwitz classification (Theorem 3.4). The fixed field of the center $\mathcal{Z}(G)$ herein is denoted by \bar{N}_σ^A . By definition \bar{N}_σ is Galois over $K_{\sigma^A}^V$ in (5.20), and every automorphism of $\bar{N}_\sigma/K_{\sigma^A}^V$ acts on the normal subgroup $\text{Gal}(\bar{N}_\sigma/\bar{M}_s(t))$ as an element of A . The fixed field N_σ^A of the centralizer of $\text{Gal}(\bar{N}_\sigma/\bar{M}_s(t))$ in

$\text{Gal}(\bar{N}_\sigma/K_{\sigma^A}^V)$ thus has the following properties: it satisfies $\bar{M}_s N_\sigma^A = \bar{N}_\sigma^A$ and $\text{Gal}(N_\sigma^A/K_{\sigma^A}^V)$ is isomorphic to a subgroup of A .

By the assumptions, A and hence also $\bar{A} := A/\text{Inn}(G)$ acts on $B^V(\sigma)$ and decomposes $B^V(\sigma)$ according to Corollary I.8.4 (see I, (8.12)) into orbits of length $|\bar{A}|$, which implies

$$[K_\sigma^V : K_{\sigma^A}^V] = [\Delta_{\sigma^A}^V : \Delta_\sigma^V] = |\bar{A}|$$

with Δ_σ^V from (3.22). From

$$\text{Gal}(N_\sigma^A/K_\sigma^V) \cong \text{Gal}(\bar{N}_\sigma^A/\bar{M}_s(t)) \cong \text{Inn}(G)$$

we thus immediately obtain (5.21). Furthermore from the action of \bar{A} on $B^V(\sigma)$ follows $(H_{\sigma^A}^V : H_\sigma^V) = |\bar{A}|$, which first proves $[K_\sigma^V : K_{\sigma^A}^V] = [\bar{K}_\sigma^V : \bar{K}_{\sigma^A}^V]$ and thus

$$[N_\sigma^A : K_{\sigma^A}^V] = [\bar{\mathbb{Q}} N_\sigma^A : \bar{K}_{\sigma^A}^V].$$

The latter implies that $N_\sigma^A/K_{\sigma^A}^V$ contains no extension of constants and hence is a geometric Galois extension. \square

Remark. In the case $\mathcal{Z}(G) = 1$ the field N_σ^A coincides with N_σ in Theorem 3.9.

The question of rationality of $K_{\sigma^A}^V/\mathbb{Q}_C^V$ can at least in the case $V = 1$ be decided with the methods of Paragraph 4, by investigating the coarser class of generating systems σ^A instead of the braid orbit $B(\sigma)$ of $[\sigma]$. This is worked out in Matzat (1991a), §5.2. Another special case has been proved by Völklein.

Theorem 5.11 (Völklein (1992b)). *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$, $V = \text{Sym}(\mathbf{C})$, $W = \{\omega \in V \mid \mathbf{C}^\omega = \mathbf{C}\}$ and $A := \{\alpha \in \text{Aut}(G) \mid \mathbf{C}^\alpha = \mathbf{C}\}$. If then for a $\sigma \in \Sigma(\mathbf{C})$ the braid orbit $B^W(\sigma)$ is rigid in $\Sigma(\mathbf{C})/\text{Inn}(G)$ and A acts transitively on it, then there exists a geometric Galois extension $N_\sigma^A/\mathbb{Q}_C^V(v_1, \dots, v_s, t)$ over the purely transcendental field $\mathbb{Q}_C^V(\mathbf{v}, t)$ with*

$$\text{Gal}(N_\sigma^A/\mathbb{Q}_C^V(\mathbf{v}, t)) \cong A. \quad (5.22)$$

If here \mathbf{C} is V -symmetric, then we have $\mathbb{Q}_C^V = \mathbb{Q}$.

Proof. By assumption the braid orbit $B^W(\sigma)$ is rigid in $\Sigma(\mathbf{C})/\text{Inn}(G)$ and thus $B^V(\sigma)$ is rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$. From Theorem 5.10 the existence of a geometric Galois extension $N_\sigma^A/K_{\sigma^A}^V$ with

$$\text{Gal}(N_\sigma^A/K_{\sigma^A}^V) \cong A \quad \text{and} \quad k_{\sigma^A}^V = \mathbb{Q}_C^V$$

now follows. It remains to show the rationality of $K_{\sigma^A}^V/\mathbb{Q}_C^V$. Since A acts transitively on $B^W(\sigma)$, at least we have

$$\mathbb{Q}_C^V(\mathbf{t}^V) \leq K_{\sigma^A}^V \leq K_{\sigma^A}^W = \mathbb{Q}_C^W(\mathbf{t}^W)$$

(compare Theorem 3.9 for $A = \text{Inn}(G)$). Here, since $\mathbf{C}^W = \mathbf{C}$, the vector $\mathbf{t}^W = (\tilde{t}_1, \dots, \tilde{t}_s, t)$ consists of t and the elementary symmetric functions \tilde{t}_j of those t_i with equal conjugacy class C_i . By the main theorem on symmetric polynomials at least the field $K_{\sigma^A}^W/\mathbb{Q}_{\mathbf{C}}^W$ is a purely transcendental function field. By definition of W for each $\delta \in \text{Gal}(\bar{\mathbb{Q}}(\mathbf{t}^W)/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^W))$ there exists exactly one $\bar{\omega} \in V/W$ with $\mathbf{C}^{c(\delta)} = \mathbf{C}^{\bar{\omega}}$, which then permutes the systems of equal conjugacy classes in \mathbf{C} . As in the proof of Theorem 3.11 this implies that the field extension $K_{\sigma^A}^V/\mathbb{Q}_{\mathbf{C}}^V$ is regular and we have $\bar{\mathbb{Q}}K_{\sigma^A}^V = \bar{\mathbb{Q}}(\mathbf{t}^W)$. Since by construction V/W permutes the class vectors belonging to \mathbf{C}^V the group $\text{Gal}(\bar{\mathbb{Q}}(\mathbf{t}^W)/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^V))$ permutes the elementary symmetric polynomials $\tilde{t}_1, \dots, \tilde{t}_s$ and leaves t invariant. Since the same holds for the subgroup $\text{Gal}(\bar{\mathbb{Q}}(\mathbf{t}^W)/K_{\sigma^A}^V)$, we obtain with Speiser's Lemma (Proposition 3.10) as in the proof of Theorem 3.11 transcendentals v_1, \dots, v_s independent over $\mathbb{Q}_{\mathbf{C}}^V(t)$ with $K_{\sigma^A}^V = \mathbb{Q}_{\mathbf{C}}^V(v_1, \dots, v_s, t)$ and moreover

$$\text{Gal}(\mathbb{Q}_{\mathbf{C}}^V(\mathbf{v}, t)/\mathbb{Q}_{\mathbf{C}}^V(\mathbf{t}^V)) \cong V/W. \quad (5.23)$$

□

Unfortunately the condition that A acts transitively on $B^W(\sigma)$ is rather restrictive. Nevertheless Völklein (1992b, 1993) was able to find interesting examples by the investigation of centerless groups with very many outer automorphisms. Here we will use Theorems 5.10 and 5.11 in Section IV.4.3, to construct higher dimensional GA-realizations fulfilling some additional rationality condition.

6 Unramified Rational Places

This paragraph provides a close connection with Chapter I by showing that the existence of unramified rational places of the fixed field of a class of generating systems of G in $k(t)$ and the existence of geometric Galois extensions over $k(t)$ are interconnected via specialization. Using a theorem of Conway and Parker on the existence of rigid braid orbits this implies in particular the solution of the inverse problem of Galois theory over $k(t)$ for PAC-fields k of characteristic zero.

6.1 Specialization of the Fundamental Group

In the subsequent sections we will several times use the following specialization theorem for the algebraic fundamental group (see Grothendieck (1971), Exp. X, Cor. 3.9, and compare with Theorem I.10.6 for the mixed characteristic case).

Theorem 6.1 (Grothendieck (1971)). *Let \bar{K} be an algebraically closed field of characteristic 0 and $\wp : \mathbb{P}^1(\bar{K}) \rightarrow \mathbb{P}^1(k)$ a place of \bar{K} onto a subfield \bar{k} . Then for any finite \wp -stable subset \mathcal{S} of $\mathbb{P}^1(\bar{K})$ with $\bar{\mathcal{S}} := \wp(\mathcal{S})$ we have*

$$\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{K}) \setminus \mathcal{S}) \cong \pi_1^{\text{alg}}(\mathbb{P}^1(\bar{k}) \setminus \bar{\mathcal{S}}). \quad (6.1)$$

The isomorphism is uniquely determined by \wp up to an inner automorphism of π_1^{alg} .

Sketch of proof. Since $\bar{k} \leq \bar{K}$ we may consider $\bar{\mathcal{S}}$ as a subset of $\mathbb{P}^1(\bar{K})$. Since \mathcal{S} and $\bar{\mathcal{S}}$ have equal cardinality (compare Theorem I.2.2 for subfields of \mathbb{C}) we see

$$\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{K}) \setminus \mathcal{S}) \cong \pi_1^{\text{alg}}(\mathbb{P}^1(\bar{k}) \setminus \bar{\mathcal{S}}).$$

This implies the assertion with the proof of Theorem I.2.2 if there we replace \mathbb{C} by \bar{K} . \square

In what follows let $\wp_{\mathbf{a}}$ denote the place defined by

$$\begin{aligned} \wp_{\mathbf{a}} : \mathbb{P}^1(\bar{\mathbb{Q}}(t_1, \dots, t_s, t)) &\rightarrow \mathbb{P}^1(\bar{\mathbb{Q}}(t)), \\ (t_1, \dots, t_s) &\mapsto \mathbf{a} = (a_1, \dots, a_s) \in \mathbb{P}^1(\bar{\mathbb{Q}})^s, \end{aligned} \quad (6.2)$$

$\wp_{\mathbf{a}}$ the corresponding valuation ring and $\mathfrak{p}_{\mathbf{a}}$ its valuation ideal. The latter is unramified in $\bar{M}_s(t)/\bar{\mathbb{Q}}(t)$ when $\mathbf{a} \in \mathbb{P}^1(\bar{\mathbb{Q}})_s^*$. Furthermore, let $\hat{\mathfrak{p}}_{\mathbf{a}}$ denote an extension of $\mathfrak{p}_{\mathbf{a}}$ to \bar{M}_{s+1} and $\bar{\mathfrak{p}}_{\mathbf{a}}$ its restriction to $M_s(t)$. Then the specialization theorem for the fundamental group leads to:

Proposition 6.2. *For $\mathbf{a} \in \mathbb{P}^1(\bar{\mathbb{Q}})_s^*$, $s \geq 3$, we have $\bar{M}_s(t)\bar{\mathfrak{p}}_{\mathbf{a}} = \bar{\mathbb{Q}}(t)$, and $\bar{M}_{s+1} := \bar{M}_{s+1}\hat{\mathfrak{p}}_{\mathbf{a}}$ is the maximal field extension of $\bar{\mathbb{Q}}(t)$ unramified outside the set \mathbb{S} of numerator divisors of $(t - a_i)$ for $i = 1, \dots, s$. In particular we have*

$$\text{Gal}(\bar{M}_{s+1}/\bar{\mathbb{Q}}(t)) \cong \Gamma_s = \langle \gamma_1, \dots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle. \quad (6.3)$$

Proof. Since $\bar{M}_s \bar{\mathfrak{p}}_{\mathbf{a}} / \bar{\mathbb{Q}}$ is algebraic, we have $\bar{M}_s \bar{\mathfrak{p}}_{\mathbf{a}} = \bar{\mathbb{Q}}$ and $\bar{M}_s(t) \bar{\mathfrak{p}}_{\mathbf{a}} = \bar{\mathbb{Q}}(t)$. Now let \mathbf{T} be the set of numerator divisors of $(t - t_i)$ for $i = 1, \dots, s$ in $\bar{M}_s(t) / \bar{M}_s$. As in Theorem 2.10 let further \hat{M}_s denote the algebraic closure of \bar{M}_s in an algebraically closed hull \hat{M}_{s+1} of \bar{M}_{s+1} and $\hat{\mathbf{T}}$ the set of extensions of \mathbf{T} to $\hat{M}_s(t)$. By Theorem 2.10 the Galois extension $\hat{M}_s \hat{M}_{s+1} / \hat{M}_s(t)$ is maximal (inside \hat{M}_{s+1}) unramified outside $\hat{\mathbf{T}}$ and we have canonically

$$\mathrm{Gal}(\bar{M}_{s+1} / \bar{M}_s(t)) \cong \mathrm{Gal}(\hat{M}_s \bar{M}_{s+1} / \hat{M}_s(t)) = \pi_1^{\mathrm{alg}}(\mathbb{P}^1(\hat{M}_s) \setminus \mathcal{T})$$

with $\mathcal{T} = \{t_1, \dots, t_s\}$. By Theorem 6.1 the extension of $\hat{\mathfrak{p}}_{\mathbf{a}}$ to $\hat{M}_s \bar{M}_{s+1}$ induces an isomorphism of fundamental groups. With $\mathcal{S} = \{a_1, \dots, a_s\}$ we thus have

$$\pi_1^{\mathrm{alg}}(\mathbb{P}^1(\hat{M}_s) \setminus \mathcal{T}) \cong \pi_1^{\mathrm{alg}}(\mathbb{P}^1(\bar{\mathbb{Q}}) \setminus \mathcal{S}) = \mathrm{Gal}(\bar{M}_{\mathbf{S}} / \bar{\mathbb{Q}}(t)).$$

Composition of the two isomorphisms yields (6.3), using Theorem I.2.2. \square

As a consequence we obtain in particular (compare also Corollary I.10.7):

Corollary 6.3. *Let G be a finite group. Then the Hurwitz classifications \mathbf{N}_s and $\mathbf{N}_{\mathbf{S}}$ of $\Sigma_s(G) / \mathrm{Aut}(G)$ (and also $\Sigma_s(G) / \mathrm{Inn}(G)$) are compatible on $\mathbf{N}_s(G)$ resp. $\mathbf{N}_{\mathbf{S}}(G)$ with the specialization homomorphism of the fundamental group, i.e., with the restrictions $\tilde{\mathfrak{p}}_{\mathbf{a}}$ of $\hat{\mathfrak{p}}_{\mathbf{a}}$ to \bar{N}_{σ} we have*

$$\bar{N}_{\sigma}^{\cdot} := \bar{N}_{\sigma} \tilde{\mathfrak{p}}_{\mathbf{a}} = \bar{M}_{\mathbf{S}}^{\ker(\sigma)}. \quad (6.4)$$

6.2 The Specialization Theorem

Now let K_{σ}^V be the fixed field of σ introduced in Theorem 3.9 and kK_{σ}^V for $k_{\sigma}^V \leq k \leq \bar{\mathbb{Q}}$ be an extension of constants of K_{σ}^V . Also let \wp be a place of $\mathbb{P}^1(kK_{\sigma}^V)$ into $\mathbb{P}^1(k(t))$, whose extensions $\bar{\wp}$ to $\mathbb{P}^1(\bar{M}_s(t))$ are unramified over $\bar{\mathbb{Q}}(t)$, i.e., for which there exists $\mathbf{a} \in \mathbb{P}^1(\bar{\mathbb{Q}})^{\circ}$ with $\bar{\wp} = \bar{\wp}_{\mathbf{a}}$. Such a place is abbreviated as an *unramified rational place of $kK_{\sigma}^V / k(t)$* . Let $\Gamma_k = \mathrm{Gal}(\bar{\mathbb{Q}} / k)$ and $\pi_{\mathbf{S}}(\Gamma_k)$ denote the image of the permutation representation of Γ_k on the set \mathbf{S} of numerator divisors of $(t - a_i)$ in $\bar{\mathbb{Q}}(t) / \bar{\mathbb{Q}}$ (compare I, (4.26)).

Theorem 6.4. *Let G be a finite group with trivial center, $\mathbf{C} \in \mathrm{Cl}(G)^s$ with $s \geq 3$, V a symmetry group of \mathbf{C} and $\sigma \in \Sigma(\mathbf{C})$. Then we have:*

(a) *If $kK_{\sigma}^V / k(t)$ for $k_{\sigma}^V \leq k \leq \bar{\mathbb{Q}}$ possesses an unramified rational place, then there exists a geometric Galois extension $N / k(t)$ satisfying*

$$\mathrm{Gal}(N / k(t)) \cong G, \quad \bar{\mathbb{Q}}N = \bar{N}_{\sigma}^{\cdot} \in \mathbf{N}_{\mathbf{S}}(G) \quad \text{and} \quad \pi_{\mathbf{S}}(\Gamma_k) \leq V. \quad (6.5)$$

(b) *If there exists a geometric Galois extension $N / k(t)$ with group G , $\bar{\mathbb{Q}}N = \bar{N}_{\sigma}^{\cdot}$ and $\pi_{\mathbf{S}}(\Gamma_k) \leq V$, then we have $k \geq k_{\sigma}^V$, and $kK_{\sigma}^V / k(t)$ possesses an unramified rational place.*

Proof. By Theorem 3.9(b) there exists a geometric Galois extension N_σ/K_σ^V with

$$\mathrm{Gal}(N_\sigma/K_\sigma^V) \cong G \quad \text{and} \quad \bar{M}_s N_\sigma = \bar{N}_\sigma.$$

Hence we also have $\mathrm{Gal}(kN_\sigma/kK_\sigma^V) \cong G$. Now let \wp be an unramified rational place of $kK_\sigma^V/k(t)$, \mathfrak{p} the corresponding valuation ideal, $\hat{\mathfrak{p}} = \hat{\mathfrak{p}}_a$ an extension of \mathfrak{p} to \bar{M}_{s+1} with corresponding restrictions $\tilde{\mathfrak{p}}$ to kN_σ and $\bar{\mathfrak{p}}$ to kK_σ^V respectively, and $N := kN_\sigma \tilde{\mathfrak{p}}$ the residue class field of kN_σ modulo $\tilde{\mathfrak{p}}$. Since the extension of constants with $\bar{\mathbb{Q}}$ commutes with the residue class map and $\bar{\mathfrak{p}}$ has residue degree 1 in $\bar{M}_s(t)/\bar{\mathbb{Q}}(\mathbf{t}^V)$, we have

$$\bar{\mathbb{Q}}N = \bar{\mathbb{Q}}N_\sigma \tilde{\mathfrak{p}} = \bar{N}_\sigma \tilde{\mathfrak{p}} = \bar{N}_\sigma^\cdot.$$

The sequence of inequalities

$$|G| = [kN_\sigma : kK_\sigma^V] \geq [N : k(t)] \geq [\bar{\mathbb{Q}}N : \bar{\mathbb{Q}}(t)] = |G|$$

now shows that $N/k(t)$ is geometric and Galois of degree $|G|$, which implies that $\mathrm{Gal}(N/k(t)) \cong G$. Finally from $k(\mathbf{t}^V)\mathfrak{p} = k(t)$ we obtain $\mathbf{a}^V \in k$ and hence $\pi_{\mathbf{s}}(\Gamma_k) \leq V$.

Now let $N/k(t)$ be a geometric Galois extension with $\mathrm{Gal}(N/k(t)) \cong G$ and $\bar{\mathbb{Q}}N = \bar{N}_\sigma^\cdot$. To this corresponds via the Hurwitz classification the ordered set $\mathbb{S} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ of unramified prime divisors of $\bar{N}_\sigma^\cdot/\bar{\mathbb{Q}}(t)$, where \mathfrak{P}_i is the numerator divisor of $(t-a_i)$. For \mathbb{S} we have by assumption $\pi_{\mathbf{s}}(\Gamma_k) \leq V$. Here V is a symmetry group of $\mathbf{C} = ([\sigma_1], \dots, [\sigma_s])$ since the inertia groups of $\mathfrak{P}_i \in \mathbb{S}$ conjugate over $k(t)$ coincide and Γ_k acts on $\Sigma_s(G)/\mathrm{Inn}(G)$ via the cyclotomic character.

By Corollary 6.3 the field \bar{N}_σ^\cdot is the image of $\bar{N}_\sigma \in \mathbf{N}_s(G)$ under the restriction of a place $\hat{\wp}$ of $\mathbb{P}^1(\bar{M}_{s+1})$ in $\mathbb{P}^1(\bar{\mathbb{Q}}(t))$ with $\hat{\wp}(t_i) = a_i$ for $i = 1, \dots, s$. (Different such places differ by an element of \hat{H}_s .) Now let $\delta \in \mathrm{Gal}(\bar{N}_\sigma^\cdot/N)$ and $\tilde{\delta}$ an extension of δ to $\bar{N}_\sigma^\cdot/k(t)$. Since then the residue class fields of \bar{N}_σ^\cdot and $\bar{N}_\sigma^{\tilde{\delta}}$ by the respective restrictions of the valuation ideal $\hat{\mathfrak{p}}$ of $\hat{\wp}$ both yield $\bar{N}_\sigma^\cdot = (\bar{N}_\sigma^\cdot)^\delta$, we obtain $\bar{N}_\sigma^{\tilde{\delta}} = \bar{N}_\sigma^\cdot$ from Corollary 6.3. Since δ centralizes the group $\mathrm{Gal}(\bar{N}_\sigma^\cdot/\bar{\mathbb{Q}}(t))$, $\tilde{\delta}$ also centralizes the group $\mathrm{Gal}(\bar{N}_\sigma^\cdot/\bar{M}_s(t))$. This implies $[\sigma]^{\tilde{\delta}} = [\sigma]$ which finally proves $\tilde{\delta} := \tilde{\delta}|_{\bar{M}_s(t)} \in \Delta_\sigma^V$ and hence $k \geq k_\sigma^V$.

Now let N_σ be the field introduced in (3.24) with $\mathrm{Gal}(N_\sigma/K_\sigma^V) \cong G$. Then $\tilde{\delta}$, belonging to the centralizer of $\mathrm{Gal}(\bar{N}_\sigma^\cdot/\bar{M}_s(t))$, lies in $\mathrm{Gal}(\bar{N}_\sigma^\cdot/kN_\sigma)$ and thus leaves kN_σ pointwise fixed. Hence also $N^\cdot := kN_\sigma \tilde{\mathfrak{p}}$ and $K^\cdot := kK_\sigma^V \tilde{\mathfrak{p}}$ are left pointwise fixed by $\tilde{\delta}$. This forces $K^\cdot = k(t)$ and $N^\cdot = N$, since $N^\cdot/k(t)$ is Galois with $\bar{\mathbb{Q}}N^\cdot = \bar{N}_\sigma^\cdot$ and N is uniquely determined as the fixed field of the centralizer of $\mathrm{Gal}(\bar{N}_\sigma^\cdot/\bar{\mathbb{Q}}(t))$ in $\mathrm{Gal}(\bar{N}_\sigma^\cdot/k(t))$. In particular the restriction \wp of $\hat{\wp}$ to $\mathbb{P}^1(kK_\sigma^V)$ is an unramified rational place of $kK_\sigma^V/k(t)$. \square

Composition of Theorems 5.3 and 6.4 yields:

Theorem 6.5 (Specialization Theorem). *Let G be a finite group with trivial center, $\mathbf{C} \in \mathrm{Cl}(G)^s$ a class vector with $s \geq 3$ and V a symmetry group of \mathbf{C} . Furthermore,*

assume that the braid orbit $B^V(\sigma)$ of $\sigma \in \Sigma(\mathbf{C})$ is rigid under H_s^V . Then there exists a geometric Galois extension $N/\mathbb{Q}_\mathbf{C}^V(t)$ with

$$\text{Gal}(N/\mathbb{Q}_\mathbf{C}^V(t)) \cong G \quad \text{and} \quad \bar{\mathbb{Q}}N = \bar{N}_\sigma^\circ \quad (6.6)$$

if and only if $K_\sigma^V/\mathbb{Q}_\mathbf{C}^V(t)$ possesses an unramified rational place.

Here we have $\mathbb{Q}_\mathbf{C}^V = \mathbb{Q}$ if \mathbf{C} is V -symmetric.

The main problem with the application of Theorem 6.5 is in general the difficult proof of existence of unramified rational places. This handicap vanishes by definition if the field of constants k is assumed to be pseudo algebraically closed (see Section 6.4 for the definition). Then it only remains to ensure the existence of rigid braid orbits, which is essentially possible by a group theoretic result of Conway and Parker.

6.3 The Theorem of Conway and Parker

For the proof of the theorem of Conway and Parker a number of preparatory remarks have to be made. For a finite group G let $W(G)$ denote the semigroup generated by the words in G , where the word consisting of $\sigma \in G$ is denoted by w_σ for better distinction. The natural mapping

$$e : W(G) \rightarrow G, \quad w_{\sigma_1} \cdots w_{\sigma_s} \mapsto \sigma_1 \cdots \sigma_s, \quad (6.7)$$

is called the evaluation function. Furthermore, for $w = w_{\sigma_1} \cdots w_{\sigma_s} \in W(G)$ let

$$\bar{w} := \tilde{B}(w) = \tilde{B}(w_{\sigma_1} \cdots w_{\sigma_s}) \quad (6.8)$$

denote the orbit of w under the full Artin braid group \tilde{B}_s via the action on the indices (1.5) and

$$H(G) := \{\bar{w} \mid w \in W(G)\} \quad (6.9)$$

the set of such orbits.

Proposition 6.6. (a) Equipped with the product $\bar{w}_1 \cdot \bar{w}_2 := \overline{w_1 w_2}$ the set $H(G)$ becomes a semigroup, with

$$\bar{w}_\sigma \bar{w}_\tau = \bar{w}_\tau \bar{w}_{\sigma^\tau}. \quad (6.10)$$

(b) The evaluation function e is a class function on $H(G)$. Every $\bar{w} \in H(G)$ with $e(\bar{w}) = 1$ lies in the center of $H(G)$.

Proof. Obviously the product $\bar{w}_1 \bar{w}_2$ is well defined and using the braid action of β_1 we obtain

$$\bar{w}_\sigma \bar{w}_\tau = \overline{w_\sigma w_\tau} = \overline{w_\tau w_{\sigma^\tau}} = \bar{w}_\tau \bar{w}_{\sigma^\tau}.$$

Since by (1.5) the action of β_i on G^s leaves invariant the product of the components, e is constant on the classes \bar{w} . Now let $\bar{w} \in H(G)$ with $e(\bar{w}) = 1$, say $\bar{w} = \bar{w}_{\sigma_1 \cdots \sigma_s}$.

Then iterating (6.10) we find for $\tau \in G$

$$\bar{w}_\tau \bar{w}_{\sigma_1 \dots \sigma_s} = \bar{w}_\tau \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} = \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} \bar{w}_\tau = \bar{w}_{\sigma_1 \dots \sigma_s} \bar{w}_\tau$$

since $\sigma_1 \cdots \sigma_s = 1$. Thus \bar{w} commutes with all generators \bar{w}_τ of $W(G)$ and therefore lies in the center of $H(G)$. \square

By Proposition 6.6(b) the braid orbit

$$\tilde{u} := \prod_{\sigma \in G \setminus \{1\}} \bar{w}_\sigma^{o(\sigma)} \in H(G) \quad (6.11)$$

lies in the center of $H(G)$. We define a congruence relation on $H(G)$ by $\bar{w}_1 \equiv \bar{w}_2$ if there exist $n_i \in \mathbb{N}$ with $\bar{u}^{n_1} \bar{w}_1 = \bar{u}^{n_2} \bar{w}_2$. Then the factor group

$$\tilde{G} := H(G)/ \equiv \quad (6.12)$$

with multiplication defined on the representatives satisfies:

Proposition 6.7. (a) \tilde{G} is a central group extension of G . The canonical epimorphism $\varphi : \tilde{G} \rightarrow G$ is induced by the evaluation function e .

(b) The congruence classes $\tilde{\sigma}$ of \bar{w}_σ generate \tilde{G} , and we have $\varphi(\tilde{\sigma}) = \sigma$ and

$$\tilde{\sigma} \tilde{\tau} = \tilde{\tau} \tilde{\sigma}^{\tilde{\tau}}. \quad (6.13)$$

Proof. Let $\sigma \in G \setminus \{1\}$. Since $e(\bar{w}_\sigma^{o(\sigma)}) = 1$ the element $\bar{w}_\sigma^{o(\sigma)}$ lies in $\mathcal{Z}(H(G))$ and may hence be taken as the first factor of \tilde{u} . Thus there exists $\bar{w} \in H(G)$ with $\bar{u} = \bar{w}_\sigma \bar{w}$. As above iteration of (6.10) yields $\bar{w}_\sigma \bar{w} = \bar{w} \bar{w}_\sigma$ since $e(\bar{u}) = 1$. Consequently $\tilde{\sigma}$ is invertible in \tilde{G} . Now \tilde{G} is generated by the elements $\tilde{\sigma}$ for $\sigma \in G \setminus \{1\}$ and thus forms a group. Further by Proposition 6.6(b) it is a central extension of G , for which the canonical epimorphism φ is induced by the evaluation function. This proves (a), and (b) follows by Proposition 6.6(a). \square

For G a finite group let $F := F(G) = \langle \gamma_\sigma \mid \sigma \in G \rangle$ be the free group over G and

$$\psi : F \rightarrow G, \quad \gamma_\sigma \mapsto \sigma,$$

the corresponding epimorphism with kernel $R := \ker(\psi)$. The *Schur multiplier* of G is defined as the quotient

$$M(G) := ([F, F] \cap R)/[F, R]$$

(see Huppert (1967), Kap. V, Satz 23.5). If the Schur multiplier $M(G)$ is generated by commutators, then from (6.13) we obtain an interesting lifting property of the evaluation function. Here for $\sigma = (\sigma_1, \dots, \sigma_s) \in G^s$, resp. $\bar{w}_\sigma = \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} \in H(G)$ we use the notation

$$s(\sigma) := (m_C(\sigma))_{C \in \text{Cl}(G)} \quad \text{with} \quad m_C(\sigma) = |\{\sigma_j \mid \sigma_j \in C\}| \quad (6.14)$$

for the vector of conjugacy class multiplicities (the *shape function*).

Proposition 6.8. *Let G be a finite group whose Schur multiplier $M(G)$ is generated by commutators, and \tilde{G} a central extension of G . Further let $\{\tilde{\sigma} \mid \sigma \in G\}$ be a system of representatives of G in \tilde{G} satisfying (6.13). Then for all $\sigma, \tau \in G^s$ with $s(\sigma) = s(\tau)$ and $\sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_s$ we have $\tilde{\sigma}_1 \cdots \tilde{\sigma}_s = \tilde{\tau}_1 \cdots \tilde{\tau}_s$.*

Proof. Let F, R, ψ be defined for G as above, and $\tilde{\psi}$ the epimorphism

$$\tilde{\psi} : F \rightarrow \tilde{G}, \quad \gamma_\sigma \mapsto \tilde{\sigma} \quad \text{with} \quad \kappa \circ \tilde{\psi} = \psi,$$

where κ denotes the canonical epimorphism from \tilde{G} to G . Then since $\tilde{\psi}(R) \leq \ker(\kappa)$ the group $\tilde{\psi}(R)$ is a subgroup of $\mathcal{L}(\tilde{G})$, which shows that $\tilde{\psi}([F, R]) = 1$. By assumption the Schur multiplier $M(G)$ of G is generated by commutators, hence modulo $[F, R]$ by elements $[\gamma, \delta] \in [F, F] \cap R$. Since the commutator of $\sigma := \kappa(\tilde{\psi}(\gamma))$ and $\tau := \kappa(\tilde{\psi}(\delta))$ in G is trivial, and hence $\sigma^\tau = \sigma$, it follows from (6.13) that $\tilde{\sigma}\tilde{\tau} = \tilde{\tau}\tilde{\sigma}$, whence $[\tilde{\sigma}, \tilde{\tau}] = 1$. Consequently we have $\tilde{\psi}([F, F] \cap R) = 1$, and $\tilde{\psi}$ induces an epimorphism

$$\bar{\psi} : \bar{F} := F/([F, F] \cap R) \rightarrow \tilde{G} \quad \text{with} \quad \bar{\psi}(\bar{\gamma}_\sigma) = \tilde{\sigma}.$$

For $\bar{R} := R/([F, F] \cap R)$ we thus have on the one hand $\bar{R} = \ker(\kappa \circ \bar{\psi})$ and hence $\bar{\psi}(\bar{R}) = \ker(\kappa)$, and on the other $[\bar{F}, \bar{F}] \cap \bar{R} = 1$, which forces $[\tilde{G}, \tilde{G}] \cap \bar{\psi}(\bar{R}) = 1$. Hence $\kappa([\tilde{G}, \tilde{G}])$ is isomorphic to a subgroup of G , and \tilde{G} may be embedded into the direct product of G with $A := \tilde{G}/[\tilde{G}, \tilde{G}]$, where the embedding is given by

$$\iota : \tilde{G} \rightarrow G \times A, \quad \tilde{\sigma} \mapsto (\sigma, \alpha_\sigma) \quad \text{with} \quad \alpha_\sigma := \tilde{\sigma}[\tilde{G}, \tilde{G}]$$

for the system of representatives $\{\tilde{\sigma} \mid \sigma \in G\}$. According to (6.13) any $\sigma, \tau \in G$ satisfy

$$\alpha_{\sigma^\tau} = \tilde{\sigma}^\tau[\tilde{G}, \tilde{G}] = \tilde{\sigma}^\tau[\tilde{G}, \tilde{G}] = \tilde{\sigma}[\tilde{G}, \tilde{G}] = \alpha_\sigma,$$

and α_σ only depends on the conjugacy class of σ . The assertion now follows from the equality

$$\prod_{i=1}^s \tilde{\sigma}_i = \prod_{i=1}^s (\sigma_i, \alpha_{\sigma_i}) = \left(\prod_{i=1}^s \sigma_i, \prod_{i=1}^s \alpha_{\sigma_i} \right) = \left(\prod_{i=1}^s \tau_i, \prod_{i=1}^s \alpha_{\tau_i} \right) = \prod_{i=1}^s \tilde{\tau}_i. \quad \square$$

In the following lemma we collect some final prerequisites for the proof of the theorem of Conway and Parker.

Lemma 6.9. *Let G be a finite group.*

(a) *If $\tau_1, \tau_2 \in G$ are conjugate elements of G of order $n = o(\tau_i)$, and if G is generated by $\sigma_1, \dots, \sigma_s$, then we have*

$$\bar{w}_{\tau_1}^n \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} = \bar{w}_{\tau_2}^n \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s}.$$

(b) *If $\bar{w}, \bar{v} \in H(G)$ satisfy $s(\bar{w}) \geq s(\bar{v}\bar{u})$ then there exists $\bar{x} \in H(G)$ with $\bar{w} = \bar{v}\bar{x}$.*

(c) There exists $m \in \mathbb{N}$ such that for all $i \geq m$ left multiplication

$$\bar{u} : H(G)_i \rightarrow H(G)_{i+1}, \quad \bar{w} \mapsto \bar{u}\bar{w},$$

is bijective on $H(G)_i := \{\bar{w} \in H(G) \mid s(\bar{w}) = s(\bar{u}^i)\}$.

Proof. By Proposition 6.6(b) we have $\bar{w}_{\tau_1}^n \in \mathcal{Z}(H(G))$. Hence for $\tau := \tau_1$ we have

$$\begin{aligned} \bar{w}_{\tau}^n \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} &= \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_{j-1}} \bar{w}_{\tau}^n \bar{w}_{\sigma_j} \cdots \bar{w}_{\sigma_s} \\ &= \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_j} \bar{w}_{\tau^{\sigma}}^n \bar{w}_{\sigma_{j+1}} \cdots \bar{w}_{\sigma_s} = \bar{w}_{\tau^{\sigma}}^n \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s} \end{aligned}$$

which proves (a) by induction since $G = \langle \sigma_1, \dots, \sigma_s \rangle$.

For the proof of (b) first let $\bar{v} = \bar{w}_{\sigma}$ with $\sigma \in G$, $n := o(\sigma)$ and $C := [\sigma]$. Then if $\bar{w} = \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s}$ and $s(\bar{w}) \geq s(\bar{w}_{\sigma} \bar{u})$, there exist more than $n|C|$ indices j with $\sigma_j \in C$, and thus at least one $\tau \in C$ occurs more than n times among the σ_j . For this τ we have that $\bar{w} = \bar{w}_{\tau}^n \bar{w}_{\tau_1} \cdots \bar{w}_{\tau_r}$ with $\tau_i \in G$ and $\tau_1 = \tau$ by (6.10). Since $[\sigma_1], \dots, [\sigma_s]$ covers the non-trivial conjugacy classes of G , the same holds for $[\tau_1], \dots, [\tau_r]$, proving $G = \langle \tau_1, \dots, \tau_r \rangle$ (see Fried and Jarden (1986), Lemma 12.4). So by (a) we deduce

$$\bar{w} = \bar{w}_{\tau}^n \bar{w}_{\tau_1} \cdots \bar{w}_{\tau_r} = \bar{w}_{\sigma}^n \bar{w}_{\tau_1} \cdots \bar{w}_{\tau_r} = \bar{w}_{\sigma} \bar{x}$$

for a suitable $\bar{x} \in H(G)$. This proves (b) by induction on the length of \bar{v} .

From (b) it follows that for the choice of $\bar{v} = \bar{u}$ left multiplication by \bar{u} from $H(G)_i$ to $H(G)_{i+1}$ is surjective for all $i \geq 1$. Since all the $H(G)_i$ are finite sets, there exists $m \in \mathbb{N}$ such that this map is even bijective for all $i \geq m$. This completes the proof. \square

After these preparations the proof of the theorem of Conway and Parker is easily completed (see also Fried and Völklein (1991), Appendix).

Theorem 6.10 (Conway and Parker). *Let G be a finite group whose multiplier $M(G)$ is generated by commutators. Furthermore let $\mathbf{C} \in \text{Cl}(G)^s$ be a class vector of G containing each nontrivial class of G sufficiently often. Then all $\sigma \in \Sigma(\mathbf{C}^{S_s})$ lie in a single orbit under the full Artin braid group \tilde{B}_s .*

Proof. Let $\sigma, \tau \in G^s$ with $s(\sigma) = s(\tau)$ and $\sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_s$ and $\bar{w}_1 := \bar{w}_{\sigma_1} \cdots \bar{w}_{\sigma_s}$, $\bar{w}_2 := \bar{w}_{\tau_1} \cdots \bar{w}_{\tau_s}$. By Propositions 6.7 and 6.8 this implies that $\tilde{\sigma}_1 \cdots \tilde{\sigma}_s = \tilde{\tau}_1 \cdots \tilde{\tau}_s$. Hence there exist $n_i \in \mathbb{N}$ with $\bar{u}^{n_1} \bar{w}_1 = \bar{u}^{n_2} \bar{w}_2$, where since $s(\bar{w}_1) = s(\bar{w}_2)$ we even have $n_1 = n_2 =: n$. By Lemma 6.9(b) there exist $\bar{v} \in H(G)$ and $\bar{x}_i \in H(G)_m$ with $\bar{w}_1 = \bar{v} \bar{x}_1$ and $\bar{w}_2 = \bar{v} \bar{x}_2$. Since \tilde{G} forms a group, there also exist $l \in \mathbb{N}_0$ and $\bar{y} \in H(G)$ with $\bar{y} \bar{v} = \bar{u}^l$.

Thus from $\bar{u}^n \bar{w}_1 = \bar{u}^n \bar{w}_2$ it follows that $\bar{u}^n \bar{v} \bar{x}_1 = \bar{u}^n \bar{v} \bar{x}_2$ and after multiplication by \bar{y} from the left also $\bar{u}^{n+l} \bar{x}_1 = \bar{u}^{n+l} \bar{x}_2$. Now $\bar{x}_i \in H(G)_m$, so by Lemma 6.9(c) this forces $\bar{x}_1 = \bar{x}_2$. Hence we have

$$\bar{w}_1 = \bar{v} \bar{x}_1 = \bar{v} \bar{x}_2 = \bar{w}_2,$$

i.e., σ and τ lie in the same \tilde{H}_s -orbit. \square

Remark. In the proof of Theorem 6.10 the assumption $e(\sigma) = 1$ was not used.

Corollary 6.11. *Under the hypothesis of Theorem 6.10, $\Sigma(\mathbf{C}^{S_s})/\text{Inn}(G)$ is a single orbit under the full Hurwitz braid group \tilde{H}_s . In particular \mathbf{C} is then an H_s^V -rigid class vector with respect to the full symmetry group V of \mathbf{C} .*

Proof. This result follows immediately from Theorem 6.10 since the Artin braid $\beta_1 \cdots \beta_s \beta_s \cdots \beta_1$ acts trivially on $\Sigma_s(G)/\text{Inn}(G)$. \square

We are now in a position to give the solution by Fried and Völklein (1991) of the inverse problem of Galois theory over $k(t)$ for pseudo algebraically closed fields k .

6.4 The Inverse Galois Problem over PAC-Fields

A field k is called *pseudo algebraically closed* or *PAC* for short if every absolutely irreducible algebraic variety \mathcal{X} defined over k possesses a k -rational point, and hence the corresponding function field $k(\mathcal{X})/k$ possesses a rational place. The set $\mathcal{X}(k)$ of k -rational points of \mathcal{X} then lies dense in the Zariski topology of \mathcal{X} (see Fried and Jarden (1986), Prop. 10.1), and the field $k(\mathcal{X})$ possesses rational places outside of any proper subvariety of \mathcal{X} . Perhaps the most interesting non-trivial example of a PAC-field known at present is the field $\mathbb{Q}^{\text{tr}}(\sqrt{-1})$ generated over \mathbb{Q} by all totally real algebraic numbers and $\sqrt{-1}$ (following from Pop (1996), Thm. 5).

Now let \mathcal{K}_{σ}^V denote the algebraic closure of $\mathbb{Q}(t_1, \dots, t_s)^V$ in K_{σ}^V ; then we have $K_{\sigma}^V = \mathcal{K}_{\sigma}^V(t)$. By the above, the regular field extensions $k\mathcal{K}_{\sigma}^V/kk_{\sigma}^V$ resp. $kK_{\sigma}^V/kk_{\sigma}^V(t)$ obtained by extension of constants by a PAC-field k then possess unramified rational places (in the sense of Section 6.2). Furthermore, we have $kk_{\sigma}^V = k$ if the class vector \mathbf{C} of σ is V -symmetric and H_s^V -rigid. Thus all assumptions of Theorem 6.4(a) are satisfied for $kK_{\sigma}^V/k(t)$ if only the center of G is trivial. It remains to show how this restriction on the center and the additional hypothesis on the multiplier in the theorem of Conway and Parker can be overcome.

Proposition 6.12. *Let G be a finite group. Then we have:*

- (a) *The Schur multiplier $M(H)$ of any representation group H of G is generated by commutators.*
- (b) *G is a factor group of a finite group H with $\mathcal{Z}(H) = 1$, whose Schur multiplier $M(H)$ is generated by commutators.*

Proof. Let $M_G \cong M(G)$ denote the kernel of the surjection $H \rightarrow G$. Then clearly $M_G \leq H' \cap \mathcal{Z}(H)$. For a representation group R of H let $M_R \cong M(H)$ denote the kernel of $R \rightarrow H$ satisfying $M_R \leq R' \cap \mathcal{Z}(R)$. Let $\bar{R} := R/[R, R]$. Then $\bar{M}_R := M_R/[R, R]$ contains no nontrivial commutators in \bar{R} and $\bar{M}_R \leq \bar{R}' \cap \mathcal{Z}(\bar{R})$. The surjection $R \rightarrow H$ induces a map $\varphi : \bar{R} \rightarrow H$ with kernel \bar{M}_R . From $M_G \leq H'$ we get $\bar{U} := \varphi^{-1}(M_G) \leq \bar{R}' \bar{M}_R = \bar{R}'$. Clearly $\bar{R}/\bar{U} \cong G$. Furthermore, $[\bar{R}, \bar{U}] \leq \bar{M}_R$. Since \bar{M}_R contains no nontrivial commutators we even have $[\bar{R}, \bar{U}] = 1$. Therefore

\bar{R} is a central extension of G with kernel $\bar{U} \leq \bar{R}'$. It follows that $|\bar{U}| \leq |M(G)|$, hence $\bar{M}_R = 1$ and $M_R = [R, R]$, proving (a).

By (a), replacing G by a representation group if necessary, we may assume that the Schur multiplier of G is generated by commutators. Write $m = |G|$ and choose S to be a nonabelian simple group with trivial multiplier ($S = L_2(8)$ will do, see Huppert (1967), Satz 25.7). Then clearly the regular wreath product $H = S \wr G$ has trivial center. Any central extension of S splits since $M(S) = 1$. By induction, the same holds for every central extension of S^m . Thus every representation group of $H = S^m \rtimes G$ contains a normal subgroup isomorphic to S^m such that the quotient is a representation group of G . Therefore $M(H) \cong M(G)$ is generated by commutators. \square

With this supplement to Theorem 6.10 the Specialization Theorem 6.5 leads to:

Theorem 6.13 (Fried and Völklein (1991)). *Let k be a PAC-field of characteristic 0. Then for every finite group G there exists a geometric Galois extension $N/k(t)$ with group $\text{Gal}(N/k(t)) \cong G$.*

Proof. Let G be a finite group. By Proposition 6.12(b) G is the factor group of a finite group H with trivial center and whose multiplier is generated by commutators. If we now take a class vector $\mathbf{C} \in \text{Cl}(H)^s$ containing each class sufficiently often and the same number of times, then \mathbf{C} is V -symmetric with respect to the full symmetry group V and by Corollary 6.11 also H_s^V -rigid. Hence for $\sigma \in \Sigma(\mathbf{C})$ due to $k_\sigma^V = \mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$ we certainly have $kk_\sigma^V = k$. Since k is pseudo algebraically closed and thus $kK_\sigma^V/k(t)$ possesses unramified rational places, by Theorem 6.4(a) there exists a geometric Galois extension $N/k(t)$ with $\text{Gal}(N/k(t)) \cong G$. If now U is a normal subgroup of H with $H/U \cong G$, then the result follows by passage from N to the fixed field N^U . \square

With the Hilbert irreducibility theorem this implies the following:

Corollary 6.14. *Over a Hilbertian PAC-field of characteristic 0 every finite group occurs as Galois group.*

The structure of the absolute Galois group Γ_k of such a Hilbertian PAC-field k will be completely determined in IV.3.3. Using rigid analytic patching methods the results of Theorem 6.13 and Corollary 6.14 can be generalized to arbitrary characteristic, see Theorem VI.4.8 and Corollary VI.4.9.

7 Braids and Geometric Automorphisms

To facilitate the search for rational places, we here specialize the fixed fields of classes of generating systems to function fields in two variables. This then opens the possibility of replacing braid orbit genera by the usually smaller symmetrized braid orbit genera obtained by using geometric automorphisms. In the case $s = 4$ we moreover give explicit formulae for these. In analogy to the Twisted Rigidity Theorem I.6.10 this finally leads to a Twisted Braid Orbit Theorem, which will subsequently be employed for the realization of the Mathieu group M_{24} as geometric Galois group over $\bar{\mathbb{Q}}(t)$.

7.1 Specialization to Two Variables

In this paragraph in analogy to (6.2) we let

$$\wp'_a : \mathbb{P}^1(\bar{\mathbb{Q}}(t)) \rightarrow \mathbb{P}^1(\bar{\mathbb{Q}}(u, t)), \quad \begin{cases} (t_1, \dots, t_{s-1}) \mapsto (a_1, \dots, a_{s-1}) \in \mathbb{P}^1(\bar{\mathbb{Q}})_{s-1}, \\ (t_s, t_{s+1}) \mapsto (u, t), \end{cases} \quad (7.1)$$

be an unramified place of $\bar{\mathbb{Q}}(t)$ according to Section 5.2 into the field of rational functions in u and t over $\bar{\mathbb{Q}}$, $\bar{\wp}'_a$ an extension of \wp'_a to $\mathbb{P}^1(\bar{M}_s(t))$, $\hat{\wp}'_a$ a further extension to $\mathbb{P}^1(\bar{M}_{s+1})$ and \mathfrak{p}'_a resp. $\bar{\mathfrak{p}}'_a$, $\hat{\mathfrak{p}}'_a$ the corresponding valuation ideals with residue class fields $\bar{M}'_s(t) := \bar{M}_s(t)\bar{\mathfrak{p}}'_a$ resp. $\bar{M}'_{s+1} := \bar{M}_{s+1}\hat{\mathfrak{p}}'_a$. Then in analogy to Proposition 6.2 we have the result:

Proposition 7.1. *For $s \geq 4$ the residue class fields \bar{M}'_i satisfy:*

(a) $\bar{M}'_s/\bar{\mathbb{Q}}(u)$ is a maximal Galois extension unramified outside the set $\mathbf{T} = \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_{s-1}\}$ of numerator divisors \mathfrak{Q}_i of $(u - a_i)$ with

$$\text{Gal}(\bar{M}'_s/\bar{\mathbb{Q}}(u)) \cong \text{Gal}(\bar{M}_s/\bar{M}_{s-1}(t_s)) \cong \Gamma_{s-1}. \quad (7.2)$$

(b) $\bar{M}'_{s+1}/\bar{M}'_s(t)$ is a maximal Galois extension unramified outside the set $\mathbf{S}' = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ of numerator divisors \mathfrak{P}_i of $(t - a_i)$ for $i = 1, \dots, s-1$ and \mathfrak{P}_s of $(t - u)$ with

$$\text{Gal}(\bar{M}'_{s+1}/\bar{M}'_s(t)) \cong \text{Gal}(\bar{M}_{s+1}/\bar{M}_s(t)) \cong \Gamma_s. \quad (7.3)$$

(c) $\bar{M}'_{s+1}/\bar{\mathbb{Q}}(u, t)$ is Galois with

$$H'_{s+1} := \text{Gal}(\bar{M}'_{s+1}/\bar{\mathbb{Q}}(u, t)) \cong \text{Gal}(\bar{M}_{s+1}/\bar{M}_{s-1}(u, t)) \cong \Gamma_s \rtimes \Gamma_{s-1}. \quad (7.4)$$

Proof. Since $\bar{M}'_{s-1}/\bar{\mathbb{Q}}(a_1, \dots, a_{s-1})$ is algebraic, we have $\bar{M}'_{s-1} = \bar{\mathbb{Q}}$. From this, (a) and (b) follow as in the proof of Proposition 6.2 from Theorem 2.10 using Theorem 6.1. With these results (c) is obvious. In fact, according to Corollary 2.9 we have

$$H'_{s+1} \cong \Gamma_{s-1}^{(s+1)} \cong \Gamma_s \rtimes \Gamma_{s-1}. \quad \square$$

By Proposition 7.1 we thus obtain a Hurwitz classification compatible with \mathbf{N}_s from (3.6) and $\mathbf{N}_{\mathbf{s}}$ from I, (4.4), for the set $\bar{\mathbf{N}}'_s(G)$ of intermediate fields of $\bar{M}'_{s+1}/\bar{M}'_s(t)$ with Galois group isomorphic to G . In fact, with the place given by

$$\wp_{a_s} : \mathbb{P}^1(\bar{\mathbb{Q}}(u, t)) \rightarrow \mathbb{P}^1(\bar{\mathbb{Q}}(t)), \quad u \mapsto a_s \quad \text{with} \quad a_s \in \bar{\mathbb{Q}} \setminus \{a_1, \dots, a_{s-1}\}, \quad (7.5)$$

and its extension $\hat{\wp}_{a_s}$ onto $\mathbb{P}^1(\bar{M}'_{s+1})$ and the set \mathbf{S} of numerator divisors of $(t - a_i)$ for $i = 1, \dots, s$ we obtain:

Corollary 7.2. *The specialization at the restriction to $\mathbb{P}^1(\bar{M}'_{s+1})$ of the place $\hat{\wp}'_{\mathbf{a}}$ from (7.1) induces a bijection*

$$\mathbf{N}'_s : \Sigma_s(G)/\text{Aut}(G) \rightarrow \bar{\mathbf{N}}'_s(G), \quad \sigma^{\text{Aut}(G)} \mapsto \bar{N}'_{\sigma} := \bar{N}_{\sigma} \tilde{\mathfrak{p}}'_{\mathbf{a}}, \quad (7.6)$$

with $\tilde{\mathfrak{p}}'_{\mathbf{a}} := \hat{\mathfrak{p}}'_{\mathbf{a}} \cap \bar{N}_{\sigma}$ and

$$\hat{\wp}'_{\mathbf{a}} \circ \mathbf{N}_s = \mathbf{N}'_s \quad \text{and} \quad \hat{\wp}_{a_s} \circ \mathbf{N}'_s = \mathbf{N}_{\mathbf{s}}. \quad (7.7)$$

Proof. For suitable extensions of $\wp_{\mathbf{a}}$ from (6.2), $\wp'_{\mathbf{a}}$ and \wp_{a_s} we have $\hat{\wp}_{\mathbf{a}} = \hat{\wp}_{a_s} \circ \hat{\wp}'_{\mathbf{a}}$. Thus the assertions result from Corollary 6.3. \square

Remark. The Hurwitz classification (7.6) may also be refined to a mapping from $\Sigma_s(G)/\text{Inn}(G)$ onto $\bar{\mathbf{N}}'_s(G)$ without destroying the identity (7.7).

Supplementing (7.4) we will in future use the notations

$$H'_s := \text{Gal}(\bar{M}'_s(t)/\bar{\mathbb{Q}}(u, t)) \quad \text{and} \quad \Delta'_s := \text{Gal}(\bar{M}'_s(t)/\mathbb{Q}(u, t)). \quad (7.8)$$

7.2 Action of Geometric Automorphisms

Now let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ a class vector of G and V a symmetry group of \mathbf{C} . Furthermore, for the set \mathbf{S}' in Proposition 7.1(b) let

$$\Delta_{\mathbf{S}'}^V := \{\delta \in \text{Aut}(\bar{M}'_s(t)/\mathbb{Q}) \mid \pi_{\mathbf{S}'}(\delta) \in V\}, \quad H_{\mathbf{S}'}^V := \text{Aut}(\bar{M}'_s(t)/\bar{\mathbb{Q}}) \cap \Delta_{\mathbf{S}'}^V, \quad (7.9)$$

where $\pi_{\mathbf{S}'}(\delta)$ is the permutation representation of δ on \mathbf{S}' . (This notation in particular implies the assumptions that δ permutes the set \mathbf{S}' and fixes \mathfrak{P}_s .) In analogy to Section I.6.3, we now call \mathbf{S}' a *V-configuration*, if

$$\pi_{\mathbf{S}'}(\Delta'_s) \leq V \quad \text{and} \quad H_{\mathbf{S}'}^V / H'_s \cong V. \quad (7.10)$$

Thus the elements δ of Δ'_s resp. of $\Delta_{\mathbf{S}'}^V$ can be extended to automorphisms $\bar{\delta}$ of \bar{M}'_{s+1} and hence naturally act according to (7.6) and (3.10) on $\Sigma_s(G)/\text{Inn}(G)$. Correspondingly in this paragraph for $\sigma \in \Sigma(\mathbf{C})$ we will write

$$\Delta_{\sigma}^V := \{\delta \in \Delta_{\mathbf{S}'}^V \mid [\sigma]^{\delta} = [\sigma]\} \quad \text{and} \quad H_{\sigma}^V := H_{\mathbf{S}'}^V \cap \Delta_{\sigma}^V. \quad (7.11)$$

In accordance with the previous use of the rigidity notion we now call the $H_{\mathbf{s}'}^V$ -orbit $B = B_{\mathbf{s}'}^V(\sigma)$ rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ if in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ there exists no further $H_{\mathbf{s}'}^V$ -orbit whose stabilizer differs from that of B only by automorphisms of $H_{\mathbf{s}'}^V$. Then let

$$K_{\sigma}^V := \bar{M}'_s(t)^{\Delta_{\sigma}^V} \quad \text{and} \quad \mathcal{K}_{\sigma}^V := (\bar{M}'_s)^{\Delta_{\sigma}^V}. \quad (7.12)$$

Theorem 7.3. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$, $s \geq 4$, with symmetry group V and \mathbf{s}' a V -configuration. Then for $\sigma \in \Sigma(\mathbf{C})$ we have:*

- (a) $K_{\sigma}^V / \mathcal{K}_{\sigma}^V$ is a rational function field, say $K_{\sigma}^V = \mathcal{K}_{\sigma}^V(\tilde{t})$.
- (b) If the $H_{\mathbf{s}'}^V(\sigma)$ -orbit $B_{\mathbf{s}'}^V(\sigma)$ of $[\sigma]$ is rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$, then the field extension $\mathcal{K}_{\sigma}^V / \mathbb{Q}_{\mathbf{C}}^V$ is regular.

Proof. By assumption $\delta \in \Delta_{\sigma}^V$ permutes the set \mathbf{s}' of prime divisors of $\bar{M}'_s(t)/\bar{M}'_s$ in Proposition 7.1(b) and hence in particular maps the field of constants \bar{M}'_s onto itself. Thus $\mathcal{K}_{\sigma}^V = K_{\sigma}^V \cap \bar{M}'_s$ is the fixed field of the $\delta \in \Delta_{\sigma}^V$ restricted to \bar{M}'_s . Now $\bar{M}'_s K_{\sigma}^V$, being a subfield of $\bar{M}'_s(t)$, by Lüroth's theorem has genus zero over \bar{M}'_s . The same then also applies to $K_{\sigma}^V / \mathcal{K}_{\sigma}^V$, since in characteristic zero the genus does not change under extension of constants. Now \mathfrak{P}_s is the only prime divisor in \mathbf{s}' not corresponding to an algebraic place, so it has to remain invariant under Δ_{σ}^V . Thus \mathfrak{P}_s does not split in $\bar{M}'_s(t)/K_{\sigma}^V$ and therefore possesses residue degree 1 in $K_{\sigma}^V / \mathcal{K}_{\sigma}^V$. Consequently $K_{\sigma}^V / \mathcal{K}_{\sigma}^V$ is even a rational function field, which proves (a).

If the $H_{\mathbf{s}'}^V$ -orbit $B_{\mathbf{s}'}^V(\sigma)$ is rigid in $\Sigma(\mathbf{C})/\text{Inn}(G)$, then it remains invariant under the full group

$$\Delta_{\mathbf{s}'}^V(\mathbb{Q}_{\mathbf{C}}^V) := \{\delta \in \text{Aut}(\bar{M}'_s(t)/\mathbb{Q}_{\mathbf{C}}^V) \mid \pi_{\mathbf{s}'}(\delta) \in V\} = \langle H_{\mathbf{s}'}^V, \text{Gal}(\bar{M}'_s(t)/\mathbb{Q}_{\mathbf{C}}^V(u, t)) \rangle$$

which then also proves (b). \square

The following proposition now shows a connection to the geometric automorphisms investigated in Chapter I.6.

Proposition 7.4. *Under the assumptions of Theorem 7.3 for $\bar{\mathcal{K}}_{\sigma}^V := \bar{\Phi} \mathcal{K}_{\sigma}^V$ we have:*

- (a) *The field extension $\bar{\mathcal{K}}_{\sigma} / \bar{\mathcal{K}}_{\sigma}^V$ is Galois with*

$$\bar{W} := \text{Gal}(\bar{\mathcal{K}}_{\sigma} / \bar{\mathcal{K}}_{\sigma}^V) \cong \text{Gal}(\bar{K}_{\sigma} / \bar{K}_{\sigma}^V) \cong W \leq V. \quad (7.13)$$

Here $W = V$ if $B_{\mathbf{s}'}^V(\sigma)$ consists of a single H_s' -orbit.

(b) *The restrictions $\tilde{\eta}$ of all elements $\bar{\eta} \in \bar{W}$ to $\bar{\Phi}(u)$ form a group of geometric automorphisms \tilde{W} isomorphic to W , which are determined by their action on the numerator divisors \mathfrak{Q}_i of $(u - a_i)$ for $i = 1, \dots, s-1$. Here the \mathfrak{Q}_i are permuted by $\tilde{\eta}$ in the same way as the numerator divisors \mathfrak{P}_i of $(t - a_i)$ by the $\eta \in H_{\sigma}^V$ with $\eta|_{\bar{\mathcal{K}}_{\sigma}} = \bar{\eta}$.*

(c) *Each $\tilde{\eta} \in \tilde{W}$ possesses a unique extension onto $\bar{\Phi}(u, t)$ leaving invariant the numerator divisor of $(t - u)$. The extensions $\bar{\eta}$ of $\tilde{\eta}$ onto $\bar{K}_{\sigma} = \bar{\mathcal{K}}_{\sigma}(t)$ with this property thus only differ by an automorphism of $\bar{K}_{\sigma} / \bar{\Phi}(u, t)$.*

Proof. As the kernel of the permutation representation $\pi_{\mathbf{s}'} : H_{\sigma}^V \rightarrow V$, H_{σ} is normal in H_{σ}^V with factor group $W \leq V$. Thus we first see

$$\text{Gal}(\bar{K}_{\sigma}/\bar{K}_{\sigma}^V) \cong H_{\sigma}^V/H_{\sigma} \cong W \leq V.$$

Now let $\eta \in H_{\mathbf{s}'}^V$ with $\eta|_{\bar{M}'_s} = 1$. As $\mathfrak{P}_s^{\eta} = \mathfrak{P}_s$ there exists a $v \in \bar{M}'_s$ with

$$t^{\eta} - u = (t - u)^{\eta} = v(t - u),$$

which implies $v = 1$ and hence $t^{\eta} = t$ resp. $\eta = 1$. Consequently the restriction of $H_{\mathbf{s}'}^V$ onto \bar{M}'_s is faithful and we have

$$\text{Gal}(\bar{\mathcal{K}}_{\sigma}/\bar{\mathcal{K}}_{\sigma}^V) \cong \text{Gal}(\bar{K}_{\sigma}/\bar{K}_{\sigma}^V),$$

which proves (7.13). If $B_{\mathbf{s}'}^V(\sigma)$ consists of a single H'_s -orbit, then by (7.10) we further have

$$(H_{\sigma}^V : H_{\sigma}) = (H_{\mathbf{s}'}^V : H'_s) \frac{(H'_s : H_{\sigma})}{(H_{\mathbf{s}'}^V : H_{\sigma}^V)} = |V|$$

and so $W = V$. This completes the proof of (a).

Now let \mathfrak{P}_i denote the numerator divisors of $(t - a_i)$ resp. $(t - u)$ in $\bar{K}_{\sigma}/\bar{\mathcal{K}}_{\sigma}$. Then for each $\bar{\eta} \in \bar{W}$ there exists $\omega \in W$ satisfying $\mathfrak{P}_i^{\bar{\eta}} = \mathfrak{P}_{i\omega}$. For $1 \leq i < j \leq s-1$ we obtain from this the equations

$$t^{\bar{\eta}} - u^{\bar{\eta}} = v(t - u), \quad t^{\bar{\eta}} - a_i = v_i(t - a_{i\omega}), \quad t^{\bar{\eta}} - a_j = v_j(t - a_{j\omega}),$$

with $v, v_i, v_j \in \bar{\mathcal{K}}_{\sigma}$. From this results

$$v = v_i = v_j = \frac{a_i - a_j}{a_{i\omega} - a_{j\omega}} \in \bar{\mathbb{Q}},$$

hence the restrictions of $\bar{\eta}$ onto $\bar{\mathbb{Q}}(t)$ and also onto $\bar{\mathbb{Q}}(u)$ are automorphisms. In particular the restrictions $\tilde{\eta}$ of $\bar{\eta}$ in \bar{W} onto $\bar{\mathbb{Q}}(u)$ form a group of geometric automorphisms in the sense of Chapter I.6. As

$$(u - a_i)^{\tilde{\eta}} = u^{\bar{\eta}} - a_i = t^{\bar{\eta}} - v(t - u) - a_i = v(u - a_{i\omega}),$$

they permute the numerator divisors \mathfrak{Q}_i of $(u - a_i)$ also via $\mathfrak{Q}_i^{\tilde{\eta}} = \mathfrak{Q}_{i\omega}$, and since $s \geq 4$ they are even uniquely determined by this by Proposition I.6.1. This proves (b).

Part (c) of the assertion follows from the fact that an extension of $\tilde{\eta}$ onto $\bar{\mathbb{Q}}(u, t)$ is already determined by the image of t . \square

7.3 Symmetrized Braid Orbit Genera

By Theorem 7.3 the function field $K_\sigma^V/\mathbb{Q}_C^V$ is rational only if the function field in one variable $\mathcal{K}_\sigma^V/\mathbb{Q}_C^V$ is rational. If k_σ^V denotes the precise field of constants of \mathcal{K}_σ^V , then the genus of $\mathcal{K}_\sigma^V/k_\sigma^V$ resp. of $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}$ is called the s -th V -symmetrized braid orbit genus of σ :

$$g_s^V(\sigma) := g(\mathcal{K}_\sigma^V/k_\sigma^V) = g(\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}). \quad (7.14)$$

This only depends on the $H_{s'}^V$ -orbit $B_{s'}^V(\sigma)$, since the fields $\bar{\mathcal{K}}_\sigma^V$ are conjugate over $(\bar{M}_s')^{H_{s'}^V} = \bar{\mathbb{Q}}(u)^{\tilde{W}}$.

The symmetrized braid orbit genus $g_s^V(\sigma)$ is in general considerably smaller than the usual braid orbit genus $g_s(\sigma)$ in (5.11). Namely, we have:

Proposition 7.5. *Under the assumptions of Theorem 7.3 and with the group W of Proposition 7.4(a) we have:*

$$(a) \quad g_s^1(\sigma) = g(\bar{\mathcal{K}}_\sigma/\bar{\mathbb{Q}}) = g_s(\sigma) \text{ with } g_s(\sigma) \text{ as in (5.11),} \quad (7.15)$$

$$(b) \quad g_s(\sigma) - 1 = |W|(g_s^V(\sigma) - 1) + \frac{1}{2} \deg(\mathfrak{D}(\bar{\mathcal{K}}_\sigma/\bar{\mathcal{K}}_\sigma^V)). \quad (7.16)$$

Proof. The place $\bar{\wp}'_a$ is inert and genus preserving in $\bar{M}_s/\bar{M}_{s-1}(t_s)$ by Proposition 7.1(a). Using the fields K_j from Theorem 5.6 we get from $\bar{M}_{s-1}K_s$ and \bar{M}_{s-1} the residue class fields $\bar{\mathcal{K}}_\sigma$ and $\bar{\mathbb{Q}}$ respectively and thus

$$g_s(\sigma) = g(K_s/K_{s-1}) = g(\bar{M}_{s-1}K_s/\bar{M}_{s-1}) = g(\bar{\mathcal{K}}_\sigma/\bar{\mathbb{Q}}) = g(\mathcal{K}_\sigma/k_\sigma) = g_s^1(\sigma).$$

By Proposition 7.4(a) the field extension $\bar{\mathcal{K}}_\sigma/\bar{\mathcal{K}}_\sigma^V$ is Galois with group \tilde{W} isomorphic to W . The equation in (b) now follows from the Hurwitz genus formula. \square

Remark. Since the groups $V \geq W$ in Proposition 7.4(a) satisfy

$$g_s^V(\sigma) = g_s^W(\sigma), \quad (7.17)$$

we may if necessary assume $V = W$ for the computation of $g_s^V(\sigma)$.

In the following, we illustrate on the example of $s = 4$ how the V -symmetrized braid orbit genera introduced above may be calculated explicitly. Here we can restrict ourselves to $V = Z_2$ and $V = Z_3$, since by Theorem I.6.5 these are the only groups of geometric automorphisms $V \leq S_4$ with fixed points. The next proposition is only for the purpose of preparation. As already announced in Section 2.1, we here denote the discrete full Hurwitz braid group by \tilde{H}_s^\vee , and consequently

$$\check{H}_s^V := \{\beta \in \tilde{H}_s^\vee \mid q(\beta) \in V\}.$$

Proposition 7.6. *For $V = Z_2$, respectively $V = Z_3$, two elements of finite order in $\check{H}_4^V/\mathcal{Z}(\check{H}_4)$ are conjugate if and only if their canonical images in V coincide.*

Proof. By Proposition 1.9 we have

$$\tilde{H}_4^\vee / \mathcal{L}(\tilde{H}_4^\vee) \cong Z_2^2 \rtimes \mathrm{PSL}_2(\mathbb{Z}) \cong E_4 \rtimes (Z_2 * Z_3)$$

with the free product $Z_2 * Z_3$ (see Lyndon and Schupp (1977), p.25) and

$$E_4 = \langle \beta_1 \beta_3^{-1}, (\beta_1 \beta_2 \beta_3)^2 \rangle / ((\beta_1 \beta_2 \beta_3)^4).$$

Since for $V = Z_2$ and $V = Z_3$ the subgroups $\check{H}_4^V / \mathcal{L}(\check{H}_4)$ possess elements of order 2 respectively 3, namely $\tau := \beta_1 \beta_4 \mathcal{L}(\check{H}_4)$ respectively $\rho := \beta_1 \beta_2 \mathcal{L}(\check{H}_4)$, the isomorphism $\check{H}_4 / \mathcal{L}(\check{H}_4) \cong G_3$ proved in Theorem 1.6 implies

$$\check{H}_4^V / \mathcal{L}(\check{H}_4) \cong G_3 \rtimes V. \quad (7.18)$$

Since here G_3 is a free group (of rank 2), the elements of finite order $\tilde{\beta} := \beta \mathcal{L}(\check{H}_4) \in \check{H}_4^V / \mathcal{L}(\check{H}_4)$ certainly satisfy $o(\tilde{\beta}) = o(q(\tilde{\beta}))$ with $q(\tilde{\beta}) := q(\beta)$.

Now first let $V = Z_3$ and $\tilde{\beta}, \tilde{\beta}' \in \check{H}_4^V / \mathcal{L}(\check{H}_4)$ be elements of order 3 with $q(\tilde{\beta}) = q(\tilde{\beta}')$. Then their images $\bar{\beta}, \bar{\beta}'$ in $\mathrm{PSL}_2(\mathbb{Z})$ are conjugate, so that there exists an $\bar{\eta} \in \mathrm{PSL}_2(\mathbb{Z})$ with $\bar{\beta}^{\bar{\eta}} = \bar{\beta}'$. As $q(E_4) = \langle (12)(34), (13)(24) \rangle$, there exists a preimage $\tilde{\eta} \in \check{H}_4^\vee / \mathcal{L}(\check{H}_4^\vee)$ with

$$q(\tilde{\eta}) \in \mathcal{N}_{S_4}(\langle q(\tilde{\beta}) \rangle) \cong S_4 / q(E_4).$$

Consequently there exists $\tilde{\eta}' \in E_4$ with $\tilde{\beta}^{\tilde{\eta}'} = \tilde{\eta}' \tilde{\beta}'$. This then satisfies $q(\tilde{\eta}') = 1$ and so $\tilde{\eta}' = 1$. Thus $\tilde{\beta}$ and $\tilde{\beta}'$ are conjugate in $\check{H}_4 / \mathcal{L}(\check{H}_4)$ and hence in particular in $\check{H}_4^V / \mathcal{L}(\check{H}_4)$.

The assertion can be verified in a similar manner for elements of order 2 (for this, see also Gillette and Van Buskirk (1968), Thm. 4.17). \square

For $V \leq S_4$ and a V -configuration $\$'$, the preceding proposition and the isomorphisms

$$H_{\$'}^V \cong (\check{H}_4^V / \mathcal{L}(\check{H}_4)) \hat{\cong} \Gamma_3 \rtimes V \quad (7.19)$$

following from (7.18) and Proposition 2.6(b) immediately imply:

Corollary 7.7. *For $s = 4$ two closed elements (generators of closed subgroups) of finite order in $H_{\$'}^V$ are conjugate if and only if their canonical images in V coincide.*

In the following, let $\$'$ be a V -configuration for $V = Z_2$ respectively $V = Z_3$ and

$$\bar{\mathbb{Q}}(\tilde{u}) := (\bar{M}_s')^{H_{\$'}^V} \leq \bar{\mathbb{Q}}(u) \quad (7.20)$$

be the fixed field of $H_{\$'}^V$, $\tilde{\mathbb{T}} := \{\tilde{\mathfrak{Q}}_1, \dots, \tilde{\mathfrak{Q}}_{\tilde{s}}\}$ the set of prime divisors of $\bar{\mathbb{Q}}(\tilde{u})$ ramified in $\bar{M}_s'/\bar{\mathbb{Q}}(\tilde{u})$, and $\tilde{\beta}_1, \dots, \tilde{\beta}_{\tilde{s}}$ generators of the corresponding inertia groups. Being elements of $H_{\$'}^V$ these act on $B := B_{\$'}^V(\sigma)$ (compare Theorem 7.3). The corresponding permutation representation of $\tilde{\beta}_i$ will be denoted by $\pi_B(\tilde{\beta}_i)$.

Theorem 7.8. Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^4$, V a symmetry group of \mathbf{C} , $\mathbf{S}' \subseteq \mathbb{P}(\bar{M}'_4(t)/\bar{M}'_4)$ a V -configuration and $B := B_{\mathbf{S}'}^V(\sigma) \subseteq \Sigma(\mathbf{C}^V)$ a $H_{\mathbf{S}'}^V$ -orbit. Then we have

$$g_s^V(\sigma) = 1 - |B| + \frac{1}{2} \sum_{i=1}^3 (|B| - c_i), \quad (7.21)$$

where the c_i count the number of cycles in $\pi_B(\tilde{\beta}_i)$. Furthermore we have:

- (a) $\pi_B(\tilde{\beta}_1) = \pi_B(\beta_{14})$, $\pi_B(\tilde{\beta}_2) = \pi_B(\beta_1)$, $\pi_B(\tilde{\beta}_3) = \pi_B(\beta_1\beta_{14})$ for $V = \langle(12)\rangle$,
- (b) $\pi_B(\tilde{\beta}_1) = \pi_B(\beta_{14})$, $\pi_B(\tilde{\beta}_2) = \pi_B(\tilde{\beta}_3) = \pi_B(\beta_1\beta_2)$ for $V = \langle(123)\rangle$.

Proof. Obviously exactly three prime divisors $\tilde{\Omega}_i$ ramify in $\bar{M}'_4/\bar{\mathbb{Q}}(\tilde{u})$. The permutation representation of $H_{\mathbf{S}'}^V$ on B is equivalent to the coset representation of $H_{\mathbf{S}'}^V$ on $H_\sigma^V = \text{Gal}(\bar{M}'_4/\bar{\mathcal{K}}_\sigma^V)$, thus the cycle lengths e_{ij} of $\tilde{\beta}_i$ with say $j = 1, \dots, r_i$ coincide by Theorem I.9.1 with the ramification indices of the prime divisors of $\tilde{\Omega}_i$ in $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u})$. As we obtain the degree of the different of $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u})$ by addition of the ramification indices e_{ij} diminished by 1, this gives

$$\deg(\mathfrak{D}(\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u}))) = \sum_{i=1}^3 \sum_{j=1}^{r_i} (e_{ij} - 1) = \sum_{i=1}^3 (|B| - c_i).$$

Thus (7.21) follows from the Hurwitz genus formula for $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u})$. There remains the task of determining the permutation representations $\pi_B(\tilde{\beta}_i)$ for the groups Z_2 and Z_3 .

Therefore first let $V = \langle(12)\rangle$, \tilde{V} the group of geometric automorphisms induced by V on $\bar{\mathbb{Q}}(u)$ by Proposition 7.4 and $\bar{\mathbb{Q}}(\tilde{u}) := \bar{\mathbb{Q}}(u)^{\tilde{V}}$. Then obviously $\tilde{\Omega}_1$ and $\tilde{\Omega}_2$ are conjugate in $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(\tilde{u})$, while $\tilde{\Omega}_3$ is ramified. So in $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u})$ at most the prime divisors of

$$\tilde{\Omega}_1 = \Omega_1\Omega_2, \quad \tilde{\Omega}_2 = \Omega_3^2, \quad \tilde{\Omega}_3 = \Omega_4^2$$

are ramified, with a certain prime divisor Ω_4 of $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}$. Hence the generators of inertia groups over Ω_1 in $\text{Gal}(\bar{M}'_4/\bar{\mathbb{Q}}(\tilde{u}))$ also generate inertia groups over $\tilde{\Omega}_1$. If β'_{14} denotes the image of β_{14} in H'_4 , then by Theorem 2.4 and Proposition 7.1 the element $\tilde{\beta}_1 := \beta'_{14}$ is a generator of the inertia group of an extension of $\tilde{\Omega}_1$ in $\bar{M}'_4/\bar{\mathbb{Q}}(u)$. Since the permutation representation of β'_{14} on B coincides with that of β_{14} , we certainly have $\pi_B(\tilde{\beta}_1) = \pi_B(\beta_{14})$.

Next we determine the permutation action on B of a generating element $\tilde{\beta}_3$ of the inertia group of an extension of $\tilde{\Omega}_3$ onto \bar{M}'_4 . Since Ω_4 is unramified in $\bar{M}'_4/\bar{\mathbb{Q}}(u)$, the element $\tilde{\beta}_3$ has order 2. From Theorem I.6.5 we conclude that the geometric automorphism η_2 corresponding to (12) acts on $\Sigma_4(G)/\text{Inn}(G)$ as $\beta_1\beta_{14}$ and hence as $\beta'_1\beta'_{14} \in H_{\mathbf{S}'}^V$. By Corollary 7.7 the element $\tilde{\beta}_3$ is conjugate to $\beta'_1\beta'_{14}$ in $H_{\mathbf{S}'}^V$, which proves that $\pi_B(\tilde{\beta}_3) = \pi_B(\beta_1\beta_{14})$.

For $V = \langle(12)\rangle$ it only remains to determine the permutation representation on B of a generator $\tilde{\beta}_2$ of the inertia group of an extension $\tilde{\Omega}_2$ onto \bar{M}'_4 . Obviously $\tilde{\beta}_2$ lies in the centralizer C of β'_{34} in $H_{\mathbf{S}'}^V = H'_4 \cup \beta'_1 H'_4$. Since the intersection

of C with H'_4 has index at most 2 in C , β'_1 lies in C and $(\beta'_1)^2 = \beta'_{12}$ as part of a free generating system of H'_4 generates its own centralizer in H'_4 , we conclude that $C \cap H'_4 = \langle \beta'_{12} \rangle$. By the proof of Proposition 5.5 the braids β_{12} and β_{34} differ only by the central involution $(\beta_1 \beta_2)^3$ with $(\beta'_1 \beta'_2)^3 = 1$. From this it follows that $\beta'_{12} = \beta'_{34}$ and hence $C = \langle \beta'_1 \rangle$. Now $\tilde{\Omega}_2 = \Omega_3^2$, so β'_{34} generates a subgroup of index 2 in $\langle \tilde{\beta}_2 \rangle$, and we may choose $\tilde{\beta}_2 = \beta'_1$, which shows $\pi_B(\tilde{\beta}_2) = \pi_B(\beta_1)$.

Now let $V = \langle (123) \rangle$ and $\bar{\mathbb{Q}}(\tilde{u}) := \bar{\mathbb{Q}}(u)^{\bar{V}}$. Then Ω_1, Ω_2 and Ω_3 are conjugate in $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(\tilde{u})$, and two prime divisors of $\bar{\mathbb{Q}}(\tilde{u})$ fully ramify in $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}(\tilde{u})$, say $\tilde{\Omega}_2$ and $\tilde{\Omega}_3$. With certain prime divisors Ω_4 and Ω_5 of $\bar{\mathbb{Q}}(u)/\bar{\mathbb{Q}}$ we thus have

$$\tilde{\Omega}_1 = \Omega_1 \Omega_2 \Omega_3, \quad \tilde{\Omega}_2 = \Omega_4^3, \quad \tilde{\Omega}_3 = \Omega_5^2.$$

As in the case of the group $\langle (12) \rangle$ it is now immediately seen that $\tilde{\beta}_1 = \beta'_{14}$ generates the inertia group of an extension of $\tilde{\Omega}_1$ onto \bar{M}'_4 , which then implies that $\pi_B(\tilde{\beta}_1) = \pi_B(\beta_{14})$. For $i = 2$ and $i = 3$ the inertia group generators $\tilde{\beta}_i$ have order 3. Since the geometric automorphism η_3 for $\langle (123) \rangle$ in Theorem I.6.5 acts on $\Sigma_4(G)/\text{Inn}(G)$ as $\beta_1 \beta_2$ and hence as $\beta'_1 \beta'_2 \in H_{\mathbf{s}'}^V$, either $\tilde{\beta}_i$ or $\tilde{\beta}_i^{-1}$ is conjugate to $\beta'_1 \beta'_2$ in $H_{\mathbf{s}'}^V$. Consequently $\tilde{\beta}_2$ and $\tilde{\beta}_3$ may be chosen such that they satisfy $\pi_B(\tilde{\beta}_1) = \pi_B(\tilde{\beta}_2) = \pi_B(\beta_1 \beta_2)$. \square

In a completely similar fashion the symmetrized braid orbit genera may also be computed in the case $s > 4$ (see Przywara (1991), §3).

7.4 A Twisted Braid Orbit Theorem

By definition $\mathcal{K}_{\sigma}^V/\bar{\mathbb{Q}}$ is a rational function field if and only if $g_s^V(\sigma) = 0$. For the proof that $\mathcal{K}_{\sigma}^V/k_{\sigma}^V$ is a rational function field, besides the assumption that $g_s^V(\sigma) = 0$ we need the existence of a prime divisor of odd degree. This again can be guaranteed by an oddness condition:

(O'): Under the action of $\tilde{\beta}_1, \dots, \tilde{\beta}_{\tilde{s}}$ on $B_{\mathbf{s}'}^V$ one of the cycle lengths, summed over all $\tilde{\beta}_i$ of the same permutation type, occurs an odd number of times.

Proposition 7.9. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 4$ and V a symmetry group of \mathbf{C} . Furthermore for $\sigma \in \Sigma(\mathbf{C})$ assume that with respect to a V -configuration \mathbf{s}' we have $g_s^V(\sigma) = 0$ and the oddness condition (O') is satisfied. Then $\mathcal{K}_{\sigma}^V/k_{\sigma}^V$ is a rational function field, say $\mathcal{K}_{\sigma}^V = k_{\sigma}^V(\tilde{v})$.*

Proof. The permutation representation of $H_{\mathbf{s}'}^V$ on $B := B_{\mathbf{s}'}^V(\sigma)$ is equivalent to the coset representation of $H_{\mathbf{s}'}^V$ on $H_{\sigma}^V = \text{Gal}(\bar{M}'_s/\bar{\mathcal{K}}_{\sigma}^V)$. By Theorem I.9.1 the cycle lengths e_{ij} of $\tilde{\beta}_i$ coincide with the ramification indices of the prime divisors of $\tilde{\Omega}_i$ in $\bar{\mathcal{K}}_{\sigma}^V/\bar{\mathbb{Q}}(\tilde{u})$. Now among these prime divisors at most those can be conjugate in $\bar{\mathcal{K}}_{\sigma}^V/\bar{\mathbb{Q}}(\tilde{u})$ for which the corresponding $\tilde{\Omega}_i$ are conjugate in $\bar{\mathbb{Q}}(\tilde{u})/\mathcal{K}_B^V$, where

\mathcal{K}_B^V denotes the fixed field of the orbit B in $\Delta_{\mathbf{s}'}^V$, and moreover the ramification indices e_{ij} agree. Therefore condition (O') implies that \mathcal{K}_{σ}^V possesses a divisor of odd degree. Together with $g(\mathcal{K}_{\sigma}^V/k_{\sigma}^V) = g_s^V(\sigma) = 0$ this yields the rationality of $\mathcal{K}_{\sigma}^V/k_{\sigma}^V$. \square

Combining the previous result with Theorem 7.3 we hence obtain the following main result of this paragraph:

Theorem 7.10 (Twisted Braid Orbit Theorem). *Let G be a finite group with trivial center, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 4$, V a symmetry group of \mathbf{C} and $\mathbf{s}' \subseteq \mathbb{P}(\bar{M}'_s(t)/\bar{M}'_s)$ a V -configuration. Furthermore assume that the $H_{\mathbf{s}'}^V$ -orbit $B_{\mathbf{s}'}^V(\sigma)$ of $\sigma \in \Sigma(\mathbf{C})$ is rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$, that $g_s^V(\sigma) = 0$ and the oddness condition (O') is satisfied. Then $K_{\sigma}^V = \mathbb{Q}_{\mathbf{C}}^V(\tilde{v}, \tilde{t})$ is a rational function field over $\mathbb{Q}_{\mathbf{C}}^V$ and there exists a geometric Galois extension $N_{\sigma}/\mathbb{Q}_{\mathbf{C}}^V(\tilde{v}, \tilde{t})$ with*

$$\text{Gal}(N_{\sigma}/\mathbb{Q}_{\mathbf{C}}^V(\tilde{v}, \tilde{t})) \cong G \quad \text{and} \quad \bar{M}'_s N_{\sigma} = \bar{N}'_{\sigma}. \quad (7.22)$$

Here $\mathbb{Q}_{\mathbf{C}}^V = \mathbb{Q}$ if \mathbf{C} is V -symmetric.

Proof. The rationality of $K_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V$ already follows from Theorem 7.3 and Proposition 7.9. The field N_{σ} is then obtained as in Theorem 3.7(b) as the fixed field of the centralizer of $\text{Gal}(\bar{N}'_{\sigma}/\bar{M}'_s(t)) \cong G$ in $\text{Gal}(\bar{N}'_{\sigma}/K_{\sigma}^V)$. \square

If we only want to secure the existence of such a Galois extension over $\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$, instead of proving the rationality of $\mathcal{K}_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V$ it suffices to find an unramified rational place \wp of $K_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$. Here such a place \wp is called unramified if any extension $\bar{\wp}$ of \wp to $\mathbb{P}^1(\bar{M}'_s(t))$ is of type $\bar{\wp}_{as}$ with \wp_{as} from (7.5).

Corollary 7.11. *Let G , \mathbf{C} , V , \mathbf{s}' and $B_{\mathbf{s}'}^V(\sigma)$ be as in Theorem 7.10. If $K_{\sigma}^V/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ possesses an unramified rational place, then there exists a geometric Galois extension $N_{\sigma}/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})$ with*

$$\text{Gal}(N_{\sigma}/\mathbb{Q}_{\mathbf{C}}^V(\tilde{t})) \cong G \quad \text{and} \quad \bar{\mathbb{Q}}(t) N_{\sigma} = \bar{N}'_{\sigma}. \quad (7.23)$$

Proof. For this proof we let \tilde{N}_{σ} be the fixed field of the centralizer of $\text{Gal}(\bar{N}'_{\sigma}/\bar{M}'_s(t))$ in $\text{Gal}(\bar{N}'_{\sigma}/K_{\sigma}^V)$. For $V = 1$ we then have $\bar{\mathbb{Q}}\tilde{N}_{\sigma} = \bar{N}'_{\sigma}$, and hence by (7.7)

$$\bar{\mathbb{Q}}N_{\sigma} = \bar{N}'_{\sigma}\tilde{\mathfrak{p}} = \bar{N}'_{\sigma} \in \mathbf{N}_{\mathbf{s}}(G),$$

where $\tilde{\mathfrak{p}}$ denotes the valuation ideal of the unique extension $\tilde{\wp}$ of \wp to \bar{N}'_{σ} . In particular, $N_{\sigma}/\mathbb{Q}_{\mathbf{C}}$ is regular with group $\text{Gal}(N_{\sigma}/\mathbb{Q}_{\mathbf{C}}(\tilde{t})) \cong G$.

Since $\tilde{t} \in \bar{\mathbb{Q}}(t)$ we correspondingly have

$$\bar{\mathbb{Q}}(t)N_{\sigma} = \bar{N}'_{\sigma}\tilde{\mathfrak{p}} = \bar{N}'_{\sigma}$$

for arbitrary V , from which as above the assertion follows in the case $V \neq 1$. \square

In the next section by way of example the biggest Mathieu group M_{24} is realized as a geometric Galois group over $\mathbb{Q}(t)$ using the Twisted Braid Orbit Theorem.

7.5 Geometric Galois Extensions over $\mathbb{Q}(t)$ with M_{24}

Let G be the Mathieu group M_{24} in its natural permutation representation of degree 24, and conform to Atlas notation $2A$ the class of involutions of type $(2^8, 1^8)$ and $12B$ the class of elements of order 12 of permutation type (12^2) . Then the class vector $\mathbf{C} = (2A, 2A, 2A, 12B)$ is rational, and one finds $l(\mathbf{C}) = 144$ and $h(\mathbf{C}) = 1$. In particular \mathbf{C} is a H_4 -rigid class vector of G with the single braid orbit $B := \Sigma(\mathbf{C})/\text{Inn}(G)$. The types of the permutations $\pi_B(\beta_{i4})$ are $(5^3, 3^{39}, 2^6)$ for $i = 1, 2, 3$. Consequently the fourth braid orbit genus for $[\sigma] \in B$ equals

$$g_4(\sigma) = 1 - 144 + \frac{3}{2}(3 \cdot 4 + 39 \cdot 2 + 6) = 1.$$

Thus the untwisted braid orbit theorem (Theorem 5.7) is not applicable. Nevertheless we have:

Theorem 7.12. *There exists a geometric Galois extension $N_\sigma/\mathbb{Q}(\tilde{v}, \tilde{t})$ with*

$$\text{Gal}(N_\sigma/\mathbb{Q}(\tilde{v}, \tilde{t})) \cong M_{24} \quad \text{and} \quad \bar{\mathbb{Q}}N_\sigma = \bar{N}'_\sigma, \quad (7.24)$$

where $\sigma \in \Sigma(2A, 2A, 2A, 12B)$. In particular, M_{24} possesses a G -realization over \mathbb{Q} .

Proof. For $V = \langle (12) \rangle$, Theorem 7.8 yields the permutation types $(5^3, 3^{39}, 2^6)$, $(6^{19}, 5^3, 4^3, 3)$ and (2^{72}) for $\pi_B(\tilde{\beta}_i)$, from which

$$g_4^V(\sigma) = 1 - 144 + \frac{1}{2}(96 + 118 + 72) = 0$$

follows. Since $\tilde{\beta}_1$ satisfies the oddness condition (O'), Theorem 7.10 shows the existence of a geometric Galois extension $N_\sigma/\mathbb{Q}(\tilde{v}, \tilde{t})$ with (7.24). \square

Another proof of Theorem 7.12 is given by Dettweiler (2004), Thm. 3.10, using a criterion for rational curves in Hurwitz spaces generalizing the Twisted Braid Orbit Theorem.

An equation for the M_{24} -extension in Theorem 7.12 has been computed by Granboulan (1996) using dessins d'enfants. By his computations he found that the fixed field of M_{23} is the function field of a conic without rational points over \mathbb{Q} . Therefore this field extension cannot be specialized to M_{23} -extensions over \mathbb{Q} as it was possible in the case of M_{11} in Theorem I.6.12. So by Theorem II.9.9 the Mathieu group M_{23} remains the only sporadic simple group not yet realized as Galois group over \mathbb{Q} .

Remark. Further G -realizations of simple groups have been discovered by Shiina (2003a), Thm. 0.2. Using the (Twisted) Braid Orbit Theorem he proved geometric Galois extensions over $\mathbb{Q}(t)$ for the simple groups

$$L_3(9), L_5(2), U_4(3), U_5(2), U_6(5), S_4(4), S_6(3), {}^3D_4(2), {}^2F_4(2)', G_2(4).$$

His results supplement Theorem II.10.2.

8 Ramified Rational Places

In this paragraph we study the specialization into ramified places. Here the existence of a rational ramified place in the ramification locus of the field of constants of the Galois extension implies the Galois realization of the decomposition group at this place inside the Galois extension. The latter may easily be described using the Hurwitz classification. Since the decomposition group at inert places is isomorphic to the original group, these again lead to existence theorems for Galois extensions like for example the Rigid Braid Cycle Theorem contained in Section 8.3. In contrast, rational places in the ramification locus of the Galois extension lead at most to realizations of proper factor groups of subgroups of the original group. But they can sometimes be used to deduce the existence of prime divisors of odd degree and therefore to verify oddness conditions. This is described in Section 8.4.

8.1 Decomposition Groups of Ramified Places

Let \wp_{ij} for $1 \leq i < j \leq s+1$ denote the place

$$\wp_{ij} : \mathbb{P}^1(\bar{\mathbb{Q}}(\mathbf{t})) \rightarrow \mathbb{P}^1(\bar{\mathbb{Q}}(\mathbf{t}_j^\vee)) := \mathbb{P}^1(\bar{\mathbb{Q}}(t_1, \dots, t_{j-1}, t_{j+1}, \dots, t_{s+1})), \quad t_j \mapsto t_i, \quad (8.1)$$

with the valuation ideal \mathfrak{D}_{ij} . This by Theorem 2.4 possesses an extension $\hat{\mathfrak{D}}_{ij}$ onto \bar{M}_{s+1} with inertia group

$$I(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) = \langle \beta_{ij} \rangle. \quad (8.2)$$

Here we moreover need to know the decomposition group of $\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}$:

Theorem 8.1. *The decomposition group $D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})$ in $\bar{M}_{s+1}/\bar{\mathbb{Q}}(\mathbf{t})$ with $s \geq 3$ is generated as profinite group by*

$$\begin{aligned} \beta_{ij}, \quad \beta_{kl} \quad &\text{for } k < l < i < j \quad \text{or} \quad k < i < j < l \\ &\text{or} \quad i < k < l < j \quad \text{or} \quad i < j < k < l, \\ \beta_{kl}^{\beta_{il}} \quad &\text{for } k < i < l < j \quad \text{and} \quad \beta_{kl}^{\beta_{jl}} \quad \text{for } i < k < j < l. \end{aligned} \quad (8.3)$$

In particular it coincides with the centralizer and the normalizer of $\langle \beta_{ij} \rangle$ in $H_{s+1} = \text{Gal}(\bar{M}_{s+1}/\bar{\mathbb{Q}}(\mathbf{t}))$:

$$D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) = \mathcal{C}_{H_{s+1}}(\beta_{ij}) = \mathcal{N}_{H_{s+1}}(\langle \beta_{ij} \rangle). \quad (8.4)$$

Proof. As in the proof of Theorem 2.4 let \mathcal{D}_{ij} denote the hyperplane in \mathcal{X}^{s+1} defined by $x_i = x_j$ and \mathcal{D}'_{ij} the complement of the intersections $\mathcal{D}_{ij} \cap \mathcal{D}_{kl}$ for $\{k, l\} \neq \{i, j\}$ in \mathcal{D}_{ij} . Then the residue class field extension $\bar{M}_{s+1}\hat{\mathfrak{D}}_{ij}/\bar{\mathbb{Q}}(t_1, \dots, t_{s+1})$ \mathfrak{D}_{ij} is a maximal algebraic field extension unramified over \mathcal{D}'_{ij} . In particular the

Galois group of this field extension is isomorphic to the algebraic fundamental group of \mathcal{D}_{ij} :

$$\mathrm{Gal}(\bar{M}_{s+1}\hat{\mathfrak{D}}_{ij}/\bar{\mathbb{Q}}(\mathbf{t})\mathfrak{D}_{ij}) \cong \pi_1^{\mathrm{alg}}(\mathcal{D}_{ij}).$$

Hence we also have

$$D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})/I(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) \cong \pi_1^{\mathrm{alg}}(\mathcal{D}_{ij}). \quad (8.5)$$

Here the preimage $D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})$ of $\pi_1^{\mathrm{alg}}(\mathcal{D}_{ij})$ is generated as a profinite group by those elements of the embedded group $\pi_1^{\mathrm{top}}(\mathcal{X}_{s+1}; \mathcal{P}_0)$ of homotopy classes of paths with respect to the base point $\mathcal{P}_0 = (1, \dots, s+1)$, which can simultaneously and continuously be deformed to homotopy classes in \mathcal{D}_{ij} with respect to the base point $\mathcal{P}_{ij} = (1, \dots, j-1, i, j+1, \dots, s+1)$ such that β_{ij} becomes homotopy equivalent to zero. Hence profinite generators of $D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})$ are given by the elements listed in (8.3) (see Figure 8.1).

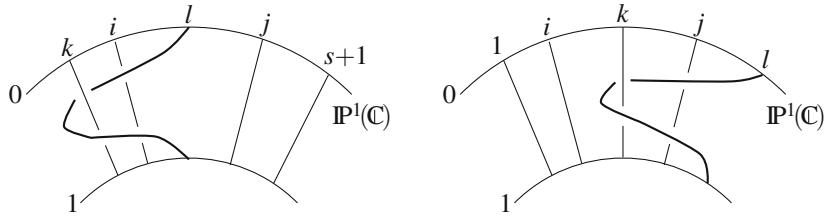


Fig. 8.1 $\beta_{il}^{-1} \beta_{kl} \beta_{il}$

$\beta_{jl}^{-1} \beta_{kl} \beta_{jl}$

Since all these generators commute with β_{ij} and even generate the full centralizer of β_{ij} in H_{s+1} , we first have

$$D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) = \mathcal{C}_{H_{s+1}}(\beta_{ij}).$$

Immediately from the relations between the generators β_{ij} of H_{s+1} or also from Theorem 3.3 together with Theorem I.2.10 we conclude that β_{ij} cannot be conjugate to any of its non-trivial powers in H_{s+1} . Hence the centralizer of β_{ij} coincides with the normalizer in H_{s+1} of the subgroup generated by this element, which completes the proof of the theorem. \square

For the study of residue class fields of intermediate fields of $\bar{M}_{s+1}/\bar{M}_s(t)$ only the intersection of $D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})$ with $\Gamma_s = \mathrm{Gal}(\bar{M}_{s+1}/\bar{M}_s(t))$ is relevant. For this the above leads to the following:

Corollary 8.2. *The intersection Γ_{ij} of $D(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij})$ with Γ_s is given by*

$$\Gamma_{ij} = \langle \gamma_1, \dots, \gamma_{i-1}, \gamma_i \gamma_j, \gamma_{i+1}^{\gamma_j}, \dots, \gamma_{j-1}^{\gamma_j}, \gamma_{j+1}, \dots, \gamma_s \rangle \quad (8.6)$$

for $1 \leq i < j \leq s$, respectively by

$$\Gamma_{ij} = \langle \gamma_i \rangle \text{ for } 1 \leq i < j = s+1. \quad (8.7)$$

8.2 Description via the Hurwitz Classification

Now let $\tilde{\mathfrak{D}}_{ij}$ denote the restriction of $\hat{\mathfrak{D}}_{ij}$ to an intermediate field \bar{N}_σ of $\bar{M}_{s+1}/\bar{M}_s(t)$ given by the Hurwitz classification (Theorem 3.4).

Theorem 8.3. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$ and $\sigma \in \Sigma(\mathbf{C})$. Then the decomposition group of the restriction $\tilde{\mathfrak{D}}_{ij}$ of $\hat{\mathfrak{D}}_{ij}$ onto $\bar{N}_\sigma/\bar{M}_s(t)$ is isomorphic to the subgroup*

$$G_{ij} := \langle \sigma_1, \dots, \sigma_{i-1}, \tilde{\sigma}_i, \sigma_{i+1}, \dots, \sigma_{j-1}, \sigma_{j+1}, \dots, \sigma_s \rangle \quad \text{for } 1 \leq i < j \leq s \quad (8.8)$$

of G with $\tilde{\sigma}_i := (\sigma_i \cdots \sigma_j)(\sigma_{i+1} \cdots \sigma_{j-1})^{-1}$, respectively to

$$G_{ij} := \langle \sigma_i \rangle \quad \text{for } 1 \leq i < j = s+1. \quad (8.9)$$

Proof. The decomposition group $D(\tilde{\mathfrak{D}}_{ij}/\bar{\mathfrak{D}}_{ij})$ is obtained by Corollary 8.2 as

$$D(\tilde{\mathfrak{D}}_{ij}/\bar{\mathfrak{D}}_{ij}) = \Gamma_{ij}/(\Gamma_{ij} \cap \ker(\sigma)).$$

To describe the isomorphism type in the parametrizing group G we observe that by (3.10) and Proposition 3.5, H_{s+1} acts inversely on Γ_s and on $\Sigma_s(G)$. So it centralizes the image σ_{ij}^* of $\beta_{ij}^* := (\beta_i^2)^{\beta_{i+1} \cdots \beta_{j-1}}$ instead of $\beta_{ij} = (\beta_i^2)^{\beta_{i+1}^{-1} \cdots \beta_{j-1}^{-1}}$.

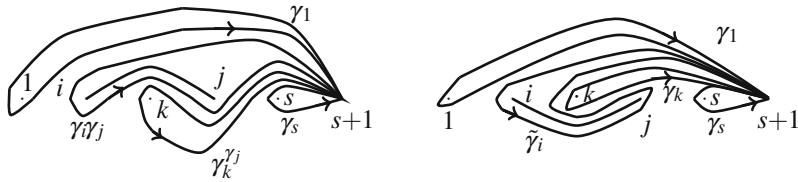


Fig. 8.2 $\mathcal{N}_{\Gamma_s}(\langle \beta_{ij} \rangle)$

$\mathcal{N}_{\Gamma_s}(\langle \beta_{ij}^* \rangle)$

According to Figure 8.2 we thus get $G_{ij} = \langle \sigma_{ij} \rangle$ with the generating system

$$\sigma_{ij} = (\sigma_1, \dots, \sigma_{i-1}, \sigma_i \cdots \sigma_j (\sigma_{i+1} \cdots \sigma_{j-1})^{-1}, \sigma_{i+1}, \dots, \sigma_{j-1}, \sigma_{j+1}, \dots, \sigma_s).$$

The proof for $j = s+1$ is immediate. \square

Since the intersection of $I(\hat{\mathfrak{D}}_{ij}/\mathfrak{D}_{ij}) = \langle \beta_{ij} \rangle$ with Γ_s is trivial for $j \leq s$, Theorem 8.3 immediately implies:

Corollary 8.4. *For $1 \leq i < j \leq s$ the Galois group of the residue class field extension $\bar{N}_\sigma \tilde{\mathfrak{D}}_{ij}/\bar{M}_s(t) \bar{\mathfrak{D}}_{ij}$ is isomorphic to G_{ij} :*

$$\text{Gal}(\bar{N}_\sigma \tilde{\mathfrak{D}}_{ij}/\bar{M}_s(t) \bar{\mathfrak{D}}_{ij}) \cong G_{ij}. \quad (8.10)$$

Denoting the generating system of G_{ij} in (8.8) by σ_{ij} we have more precisely

$$\bar{N}_\sigma \tilde{\mathfrak{D}}_{ij} = \bar{N}_{\sigma_{ij}} \in \bar{\mathbf{N}}_{s-1}(G_{ij}). \quad (8.11)$$

Here the containment relation $\bar{N}_{\sigma_{ij}} \in \bar{\mathbf{N}}_{s-1}(G_{ij})$ makes sense only for $s \geq 4$, since $\bar{\mathbf{N}}_2$ is not defined. The residue class map described in (8.11) is moreover compatible with the Galois action of the decomposition group, i.e., we have:

Proposition 8.5. *The action of $\gamma \in \mathcal{C}_{H_{s+1}}(\beta_{ij})$ on $\bar{\mathbf{N}}_s(G)$ commutes with the residue class map. Thus the image $\bar{\gamma} \in \text{Gal}(\bar{M}_{s+1}\bar{\mathfrak{D}}_{ij}/\bar{\mathbb{Q}}(t)\bar{\mathfrak{D}}_{ij})$ of γ satisfies*

$$\bar{N}_\sigma^\gamma \tilde{\mathfrak{D}}_{ij} = \bar{N}_{\sigma_{ij}}^{\bar{\gamma}}. \quad (8.12)$$

On the level of classes of generating systems (8.11) furnishes a canonical map ψ_{ij} from the orbit of $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ under $\Psi_{ij} := \mathcal{C}_{H_{s+1}}(\beta_{ij})\Gamma_s/\Gamma_s$ to $\Sigma_{s-1}(G_{ij})/A$, where A denotes the group of automorphisms of G_{ij} induced by $\mathcal{N}_G(G_{ij})$:

$$\psi_{ij} : [\sigma]^{\Psi_{ij}} \rightarrow \Sigma_{s-1}(G_{ij})/A, \quad [\sigma] \mapsto \sigma_{ij}^A. \quad (8.13)$$

In the special case $\mathcal{N}_G(G_{ij}) = G_{ij}$ we have $A = \text{Inn}(G_{ij})$. Then ψ_{ij} becomes a map constant on the β_{ij} -cycles in $[\sigma]^{\Psi_{ij}}$, whose image is a full H_{s-1} -orbit in $\Sigma_{s-1}(G_{ij})/\text{Inn}(G_{ij})$.

8.3 Braid Cycle Orbits

Reduction of the Galois extension N_σ/K_σ given in Theorem 3.7 by the restriction of a valuation ideal $\tilde{\mathfrak{D}}_{ij}$ with $j \leq s$ onto N_σ yields a Galois extension $N_{\sigma_{ij}}/K_{\sigma_{ij}}$, which after extension of constants to $\bar{M}_{ijs} := \bar{M}_s(t)\bar{\mathfrak{D}}_{ij}$ becomes the Galois extension (8.10) and thus under suitable assumptions possesses a Galois group isomorphic to G_{ij} .

The rationality of $K_{\sigma_{ij}}$ can be checked following the procedure of Section 5.2. In analogy to the notations used there for $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ let $B_{ij}(\sigma)$ denote the orbit of the braid cycle $[\sigma]_{ij} := [\sigma]^{(\beta_{ij})}$ under Ψ_{ij} , i.e.,

$$B_{ij}(\sigma) := [\sigma]_{ij}^{\Psi_{ij}} \quad \text{with} \quad \Psi_{ij} := \mathcal{C}_{H_{s+1}}(\beta_{ij})\Gamma_s/\Gamma_s. \quad (8.14)$$

This orbit of braid cycles can now be structured via the groups $\Gamma_k^{(s)}$ defined in Corollary 2.9 like the braid orbit $B(\sigma)$ in Section 4.2. For this let

$$B_{ijs}(\sigma) := [\sigma]_{ij}^{\Psi_{ij,s-1}} \quad \text{with} \quad \Psi_{ij,s-1} := \Psi_{ij} \cap \Gamma_{s-1} \quad (8.15)$$

and inductively for $s > k \geq 1$

$$B_{ijk}(\sigma) := B_{ij,k+1}(\sigma)^{\Psi_{ij,k-1}} \quad \text{with} \quad \Psi_{ij,k-1} := (\Psi_{ij} \Gamma_k^{(s)} \cap \Gamma_{k-1}^{(s)})/\Gamma_k^{(s)}. \quad (8.16)$$

Here each $B_{ijk}(\sigma)$ is considered as a set of Ψ_{ijk} -orbits. With this we can define the *reduced braid orbit genera*

$$g_{ijk}(\sigma) := 1 - |B_{ijk}(\sigma)| + \frac{1}{2} \sum_{j \neq l=1}^k (|B_{ijk}(\sigma)| - c_{ijkl}), \quad (8.17)$$

where c_{ijkl} counts the number of $\beta_{lk}\Gamma_k^{(s)}$ -orbits on $B_{ijk}(\sigma)$. In analogy to Theorem 5.6 these satisfy:

Theorem 8.6. *Let G be a finite group, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$ and $\sigma \in \Sigma(\mathbf{C})$. Further let K_k denote the algebraic closure of $\mathbb{Q}(t_1, \dots, t_k)$ in K_σ and K_{ijk} for $1 \leq i < j \leq s$ the residue class field of K_k by the restriction of $\bar{\mathfrak{D}}_{ij}$. Then these satisfy $K_{ij,j-1} = K_{ijj}$ and*

$$[K_{ijk} : K_{ij,k-1}(t_k)] = |B_{ijk}(\sigma)| \quad \text{and} \quad g(K_{ijk}/K_{ij,k-1}) = g_{ijk}(\sigma) \quad (8.18)$$

for the k with $1 \leq k \leq s$ different from j .

In particular we have $K_{\sigma_{ij}} = k_\sigma(\mathbf{t}_j^\vee)$ if the braid cycle $[\sigma]_{ij}$ remains Ψ_{ij} -invariant.

Proof. The proof runs completely along the same lines as that of Theorem 5.6. One only has to notice that by Theorem 8.1 the Galois group of the residue class field extension $\bar{M}_s(t)\bar{\mathfrak{D}}_{ij}/\bar{\mathbb{Q}}(\mathbf{t})\bar{\mathfrak{D}}_{ij}$ is isomorphic to $\Psi_{ij}/\langle \beta_{ij} \rangle$. Finally, the additional remark follows from $K_{\sigma_{ij}} = K_{ijj}(t)$. \square

To obtain information on $\text{Gal}(N_{\sigma_{ij}}/K_{\sigma_{ij}})$ we now first determine the decomposition group by the restriction of $\bar{\mathfrak{D}}_{ij}$ in the Galois extension $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ obtained from N_σ/K_σ by extension of constants with $\bar{\mathbb{Q}}$.

Proposition 8.7. *The decomposition group of the restriction of $\tilde{\mathfrak{D}}_{ij}$ to $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ is isomorphic to a subgroup \tilde{G}_{ij} of G with*

$$\tilde{G}_{ij} \cong (\mathcal{C}_{H_{s+1}}(\beta_{ij}) \cap \ker(\sigma) \cdot \Gamma_\sigma) / (\mathcal{C}_{H_{s+1}}(\beta_{ij}) \cap \ker(\sigma) \cdot \mathcal{C}_{\Gamma_\sigma}(G)) \quad (8.19)$$

with $\Gamma_\sigma = \text{Gal}(\bar{N}_\sigma/\bar{K}_\sigma)$. In particular we have

$$G_{ij} \leq \tilde{G}_{ij} \leq \mathcal{N}_G(G_{ij}) \quad \text{for } 1 \leq i < j \leq s, \quad (8.20)$$

$$G_{ij} \leq \tilde{G}_{ij} \leq \mathcal{C}_G(\sigma_i) \quad \text{for } 1 \leq i < j = s+1. \quad (8.21)$$

Proof. The relevant decomposition groups are obtained as factor groups of the intersections of $\mathcal{C}_{H_{s+1}}(\beta_{ij})$ with $\text{Gal}(\bar{M}_{s+1}/\bar{K}_\sigma) = \ker(\sigma) \cdot \Gamma_\sigma$ and with $\text{Gal}(\bar{M}_{s+1}/\bar{N}_\sigma^\circ) = \ker(\sigma) \cdot \mathcal{C}_{\Gamma_\sigma}(G)$. This immediately yields (8.19) and (8.21). For (8.20) we use in addition that the Galois extension $\bar{N}_\sigma/\bar{M}_s(t)$ is obtained from $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ by extension of constants with \bar{M}_s , and hence \tilde{G}_{ij} contains a normal subgroup isomorphic to G_{ij} . \square

Since $\tilde{\mathfrak{D}}_{ij}$ for $j \leq s$ is unramified in $\bar{N}_\sigma / \bar{M}_s(t)$ and hence also in $\bar{N}_\sigma^\circ / \bar{K}_\sigma$, Proposition 8.7 immediately gives:

Corollary 8.8. *Let $\bar{N}_{\sigma_{ij}}^\circ / \bar{K}_{\sigma_{ij}}$ be the residue field extension obtained from $\bar{N}_\sigma^\circ / \bar{K}_\sigma$ upon reduction by the restriction of $\tilde{\mathfrak{D}}_{ij}$ with $j \leq s$. Then with \tilde{G}_{ij} from (8.19) we have*

$$\text{Gal}(\bar{N}_\sigma^\circ / \bar{K}_\sigma) \cong \tilde{G}_{ij} \quad \text{and} \quad \bar{M}_{ijs} \bar{N}_{\sigma_{ij}}^\circ = \bar{N}_{\sigma_{ij}}. \quad (8.22)$$

Here in the case $\mathcal{N}_G(G_{ij}) = G_{ij}$ we have $\tilde{G}_{ij} = G_{ij}$.

Our goal now is, starting from the Galois extension in (8.22), to arrive at a geometric Galois extension over a rational function field over \mathbb{Q}_C with Galois group isomorphic to G_{ij} or at least \tilde{G}_{ij} . In general this is only possible under additional rigidity and rationality assumptions. The latter will again be formulated as oddness conditions:

(O_{ijk}): In the action of $\beta_{lk} \Gamma_k^{(s)}$ on $B_{ijk}(\sigma)$ for some $l < k$ there occurs a cycle length an odd number of times.

With this we obtain:

Theorem 8.9 (Braid Cycle Theorem). *Let G be a finite group with trivial center and $C \in \text{Cl}(G)^s$, $s \geq 3$, a class vector of G . Further let $\sigma \in \Sigma(C)$ and a pair (i, j) with $1 \leq i < j \leq s$ be chosen such that $B(\sigma)$ is a rigid H_s -orbit and $B_{ij}(\sigma)$ is a rigid Ψ_{ij} -orbit of β_{ij} -cycles in $B(\sigma)$. Assume $g_{ijk}(\sigma) = 0$ and the oddness condition (O_{ijk}) for all $k = 4, \dots, s$. If moreover G_{ij} is self-normalizing in G , then there exists a geometric Galois extension $N_{\sigma_{ij}} / \mathbb{Q}_C(\tilde{\mathbf{u}}, t)$ with $\tilde{\mathbf{u}} = (\tilde{u}_1, \dots, \tilde{u}_{s-1})$ and*

$$\text{Gal}(N_{\sigma_{ij}} / \mathbb{Q}_C(\tilde{\mathbf{u}}, t)) \cong G_{ij} \quad \text{and} \quad \bar{M}_{ijs} N_{\sigma_{ij}} = \bar{N}_{\sigma_{ij}}. \quad (8.23)$$

Proof. The Rigid Braid Orbit Theorem 5.8 yields the existence of a Galois extension N_σ / K_σ with $K_\sigma = \mathbb{Q}_C(u_1, \dots, u_s, t)$ and $\text{Gal}(N_\sigma / K_\sigma) \cong G$. Let $N_{\sigma_{ij}} := N_\sigma \tilde{\mathfrak{D}}_{ij}$ and $K_{\sigma_{ij}} := K_\sigma \tilde{\mathfrak{D}}_{ij}$ with the restrictions of $\tilde{\mathfrak{D}}_{ij}$ to N_σ and K_σ respectively. Then we have $\bar{\Phi} N_{\sigma_{ij}} = \bar{N}_{\sigma_{ij}}^\circ$ and $\bar{\Phi} K_{\sigma_{ij}} = \bar{K}_{\sigma_{ij}}$, so $\text{Gal}(N_{\sigma_{ij}} / K_{\sigma_{ij}})$ by Corollary 8.8 contains a normal subgroup isomorphic to $\tilde{G}_{ij} = G_{ij}$. Since G_{ij} was assumed to be self-normalizing in G , the extension $N_{\sigma_{ij}} / K_{\sigma_{ij}}$ is geometric and Galois with group $\text{Gal}(N_{\sigma_{ij}} / K_{\sigma_{ij}}) \cong G_{ij}$.

The rigidity of $B_{ij}(\sigma)$ inside $B(\sigma)$ implies that

$$[K_{\sigma_{ij}} : \mathbb{Q}_C(t_j^\vee)] = [\bar{K}_{\sigma_{ij}} : \bar{\Phi}(t_j^\vee)],$$

whence the regularity of $K_{\sigma_{ij}} / \mathbb{Q}_C$. Further from the vanishing of the reduced braid genera $g_{ijk}(\sigma)$ we first obtain that by (8.18) the algebraic closures K_{ijk} of $\mathbb{Q}_C(t_1, \dots, t_k)$ in $K_{\sigma_{ij}}$ have genus $g(K_{ijk} / K_{ij,k-1}) = 0$ for $j \neq k$ and $K_{ijj} = K_{ij,j-1}$. By the oddness condition (O_{ijk}) the extensions $K_{ijk} / K_{ij,k-1}(t_k)$ for $j \neq k$ possess prime divisors of odd degree and thus are rational over $K_{ij,k-1}$ and therefore over \mathbb{Q}_C . Consequently in $\mathcal{K}_{\sigma_{ij}} := K_{ijs}$ there exist $s - 1$ independent tran-

scendentals $\tilde{u}_1, \dots, \tilde{u}_{s-1}$ with $\mathcal{K}_{\sigma_{ij}} = \mathbb{Q}_C(\tilde{\mathbf{u}})$ and therefore $K_{\sigma_{ij}} = \mathbb{Q}_C(\tilde{\mathbf{u}}, t)$. This completes the proof of the first part of (8.23).

The second part follows by construction immediately from Corollary 8.8. \square

Remark. If instead of $\mathcal{N}_G(G_{ij}) = G_{ij}$ we only have $\mathcal{N}_G(\tilde{G}_{ij}) = \tilde{G}_{ij}$ with \tilde{G}_{ij} from (8.19), then the Braid Cycle Theorem still holds for \tilde{G}_{ij} at the place of G_{ij} .

We now call $[\sigma]_{ij} \subseteq B(\sigma)$ a *rigid braid cycle* if no further braid cycle $[\tau]_{ij} \subseteq B(\sigma)$ possesses a stabilizer in Ψ_{ij} which differs from the one of $[\sigma]_{ij}$ only by an automorphism of Ψ_{ij} . Then as a special case of Theorem 8.9 we obtain the easily applicable

Corollary 8.10 (Rigid Braid Cycle Theorem). *Let G, \mathbf{C}, σ and $B(\sigma)$ be as in Theorem 8.9. If $[\sigma]_{ij}$ is a rigid braid cycle with $\mathcal{N}_G(G_{ij}) = G_{ij}$, then there exists a geometric Galois extension $N_{\sigma_{ij}}/\mathbb{Q}_C(\mathbf{t}_j^\vee)$ with*

$$\text{Gal}(N_{\sigma_{ij}}/\mathbb{Q}_C(\mathbf{t}_j^\vee)) \cong G_{ij} \quad \text{and} \quad \bar{M}_{ijs} N_{\sigma_{ij}} = \bar{N}_{\sigma_{ij}}. \quad (8.24)$$

Proof. Since a rigid braid cycle in particular remains invariant under Ψ_{ij} , we have $\bar{K}_{\sigma_{ij}} = \bar{\mathbb{Q}}(\mathbf{t}_j^\vee)$ by Theorem 8.6 and hence in the proof of Theorem 8.9 also $K_{\sigma_{ij}} = \mathbb{Q}_C(\mathbf{t}_j^\vee)$. \square

Remark. A braid cycle $[\sigma]_{ij}$ is certainly rigid if inside $B(\sigma)$ it is characterized by its length, the inserted conjugacy class $\tilde{C}_i = [\tilde{\sigma}_i]$ of G and the reduced group G_{ij} . (Such cycles were called *stable* in Matzat (1991a).)

Finally the use of the Braid Cycle Theorem is demonstrated in an example computed by F. Häfner:

Example 8.1. Let $G = M_{24}$ and \mathbf{C} be the rational class vector $(2A, 2A, 4A, 5A)$ in Atlas-notation. Then $\Sigma(\mathbf{C})/\text{Inn}(G)$ is a rigid H_4 -orbit of length 2000. On this, β_{23} possesses precisely twelve 12-cycles. Among these only one possesses $\text{Aut}(M_{22})$ as the reduced group G_{23} , with the class vector $\mathbf{C}_{23} = (2A, 12A, 5A)$. This is hence a rigid braid cycle and since $\text{Aut}(M_{22})$ as a maximal subgroup of M_{24} is self-normalizing, by the Rigid Braid Cycle Theorem it leads to a geometric Galois extension $N_{\sigma_{23}}/\mathbb{Q}(\mathbf{t}_3^\vee)$ with the group $\text{Aut}(M_{22})$. Passing to the rational fixed field of M_{22} we thus obtain a geometric Galois extension with the simple group M_{22} for the class vector $(6A, 5A, 5A)$ over \mathbb{Q} (see Theorem II.9.9 for another G -realization of M_{22}).

Two of the 12-cycles lead to Galois extensions with the maximal subgroup $G_{23} \cong 2^6 \cdot 3 \cdot S_6$ of M_{24} with $\mathbf{C}_{23} = (2A, 12B, 5A)$. Since here the two classes of generating systems of G_{23} coincide — we even have $l(\mathbf{C}_{23}) = 1$ — and moreover $\mathcal{Z}(G_{23}) = 1$, by the Rigid Braid Orbit Theorem 5.8 there now exists a geometric Galois extension over $\mathbb{Q}(\mathbf{t}_3^\vee)$ with the group $2^6 \cdot 3 \cdot S_6$. From this one can further deduce geometric Galois extensions defined over \mathbb{Q} with the exceptional covering groups $3 \cdot S_6$ and $3 \cdot A_6$ of the groups S_6 and A_6 . The remaining nine 12-cycles produce the same class vector $\mathbf{C}_{23} = (2A, 12B, 5A)$ but the reduced group G_{23} coincides with the full group $G = M_{24}$. Therefore in the last case $\tilde{\mathcal{D}}_{23}$ remains inert in $\bar{N}_\sigma/\bar{M}_4(t)$ and also in $\bar{N}_\sigma^\circ/\bar{K}_\sigma$. \square

Remark. The reduction by the places \wp_{ij} can in an obvious way be iterated and if necessary be combined with the use of geometric automorphisms.

8.4 Prime Divisors of Odd Degree

The explicit knowledge of the decomposition groups $\tilde{G}_{i,s+1}$ from (8.19) seems to be of less importance for the realization of groups as Galois groups, since the Galois groups of the corresponding residue class field extensions are proper factor groups of subgroups of $\mathcal{N}_G(\langle \sigma_i \rangle)$. More precisely we have by Proposition 8.7:

Proposition 8.11. *Reduction of the Galois extension $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ by the corresponding restrictions of $\tilde{\mathfrak{D}}_{i,s+1}$ yields a Galois extension $\bar{N}_{\sigma_{i,s+1}}^\circ/\bar{K}_{\sigma_{i,s+1}}$ with*

$$\text{Gal}(\bar{N}_{\sigma_{i,s+1}}^\circ/\bar{K}_{\sigma_{i,s+1}}) \cong \tilde{G}_{i,s+1}/\langle \sigma_i \rangle. \quad (8.25)$$

But these decomposition groups can sometimes be used to deduce the existence of prime divisors of odd degree or even of degree 1 in root fields \bar{L}_σ of $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ respectively L_σ of N_σ/K_σ . This comes from the following result, which is an immediate consequence of Theorem I.9.1.

Proposition 8.12. *Let \bar{L}_σ be an intermediate field of $\bar{N}_\sigma^\circ/\bar{K}_\sigma$ and π_U the permutation representation of $\text{Gal}(\bar{N}_\sigma^\circ/\bar{K}_\sigma) \cong G$ on the cosets of $U = \text{Gal}(\bar{N}_\sigma^\circ/\bar{L}_\sigma)$. Then $\tilde{G}_{i,s+1}/\langle \sigma_i \rangle$ acts on the cycles of $\pi_U(\sigma_i)$ as on the prime divisors of $\tilde{\mathfrak{D}}_{i,s+1}|_{\bar{K}_\sigma}$ in \bar{L}_σ . The corresponding permutation representation of $\tilde{G}_{i,s+1}/\langle \sigma_i \rangle$ is faithful at least in the case of the regular representation $U = 1$.*

Remark. With the help of Proposition 8.12 it is actually rather easy to obtain a lower estimate for $\tilde{G}_{i,s+1}$ by determining the image of the permutation representation of $\mathcal{C}_{\Gamma_\sigma}(G)$ on the cycles of $\pi_U(\sigma_i)$. (Since $\Gamma_\sigma = G \cdot H_\sigma$, this action coincides with the one given in Section 3.3 of Dèbes and Fried (1990).)

Thus Proposition 8.12 entails the main Theorem 3.14 in Dèbes and Fried (1990) in the following form:

Theorem 8.13 (Dèbes and Fried (1990)). *Let G be a finite group with trivial center, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$ and $\sigma \in \Sigma(\mathbf{C})$. Using the assumptions and notation of Propositions 8.7 and 8.12 and with the intermediate field L_σ of N_σ/K_σ with $\bar{\mathbb{Q}}L_\sigma = \bar{L}_\sigma$ we have:*

(a) *If in the action of $\tilde{G}_{i,s+1}/\langle \sigma_i \rangle$ (resp. $\mathcal{C}_G(\sigma_i)/\langle \sigma_i \rangle$) on the cycles of $\pi_U(\sigma_i)$ there occurs a cycle orbit of odd length, then $\tilde{\mathfrak{D}}_{i,s+1}|_{\bar{K}_\sigma}$ possesses a prime divisor (resp. divisor) of odd degree in \bar{L}_σ .*

(b) *If in the action of $\tilde{G}_{i,s+1}/\langle \sigma_i \rangle$ (resp. $\mathcal{C}_G(\sigma_i)/\langle \sigma_i \rangle$) on the cycles of $\pi_U(\sigma_i)$ an odd cycle orbit length occurs an odd number of times, then $\tilde{\mathfrak{D}}_{i,s+1}|_{K_\sigma}$ possesses a prime divisor of odd degree in L_σ .*

Proof. Part (a) follows immediately from Theorem I.9.1 with Proposition 8.12. Part (b) is obtained from the fact that at most prime divisors of the same degree of $\bar{\mathfrak{D}}_{i,s+1}|_{\bar{K}_\sigma}$ in \bar{L}_σ can be conjugate in \bar{L}_σ/L_σ . \square

Using the field $\mathcal{K}_\sigma = K_s$ defined in Section 4.2 we thus deduce:

Corollary 8.14. *If in Theorem 8.13 we have $g(L_\sigma/\mathcal{K}_\sigma) = 0$, then under the assumptions to (a) the field $\bar{\mathbb{Q}}L_\sigma/\bar{\mathbb{Q}}\mathcal{K}_\sigma$ and under the assumptions to (b) even the field $L_\sigma/\mathcal{K}_\sigma$ is a rational function field.*

This result cannot apply to the fixed field of M_{23} in the M_{24} -extension of Theorem 7.12, as shown by the result of Granboulan (1996) cited above. This is verified by direct computations in the following example.

Example 8.2. Let $N_\sigma/\mathbb{Q}(\tilde{v}, \tilde{t})$ be the M_{24} -extension belonging to the class vector $(2A, 2A, 2A, 12B)$ and $V = \langle(12)\rangle$ constructed in Theorem 7.12. Then in $K_\sigma^V = \mathbb{Q}(\tilde{v}, \tilde{t})$ the prime divisors $\mathfrak{P}_3 := \bar{\mathfrak{D}}_{35}|_{K_\sigma^V}$ and $\mathfrak{P}_4 := \bar{\mathfrak{D}}_{45}|_{K_\sigma^V}$ both possess the residue degree 1 (and $\bar{\mathfrak{D}}_{15}|_{K_\sigma^V} = \bar{\mathfrak{D}}_{25}|_{K_\sigma^V}$ the residue degree 2). Using Proposition 8.12 we obtain with $G = M_{24}$

$$\tilde{G}_{35} \cong \mathcal{C}_G(\sigma_3) \cong 2^{1+6} \cdot L_3(2).$$

Further \tilde{G}_{35} acts transitively both on the eight fixed points and on the eight transpositions of σ_3 as the group $2^3 \cdot L_3(2)$. Thus \mathfrak{P}_3 splits in the fixed field L_σ of M_{23} in two prime divisors of degree 8. For \mathfrak{P}_4 we obtain

$$\tilde{G}_{45} \cong \mathcal{C}_G(\sigma_4) \cong \langle \sigma_4 \rangle,$$

so that the two 12-cycles remain fixed under σ_4 . But here the two prime divisors of \mathfrak{P}_4 are conjugate in \bar{L}_σ/L_σ under complex conjugation. This follows from the fact that the intersection of $\mathcal{N}_G(\langle \sigma_4 \rangle)$ (containing the decomposition group of \mathfrak{P}_4 in N_σ/K_σ^V) with M_{23} contains no involution τ with $\sigma_4^\tau = \sigma_4^{-1}$ (compare Corollary I.10.5). Hence \mathfrak{P}_4 possesses a prime divisor of degree 2 in L_σ with decomposition group of type $\tilde{G}_{45}:2$. \square

9 The Katz Algorithm

It is the aim of this paragraph to introduce the convolution functor and to describe the Katz algorithm based upon it. With this for example all rigid generating systems of irreducible linear groups can be related to generating systems of GL_1 , or can be derived from such. Typical examples for this procedure will be presented in the subsequent paragraph.

9.1 The Convolution Functor

We present the convolution functor introduced by Katz (1996) in the algebraic version of Dettweiler and Reiter (2000) as slightly varied in Dettweiler (2003). The latter is better adapted to the notation used here and moreover sometimes leads to easier formulas than in the original form.

In the following let k be a field, $V \cong k^n$ a k -vector space and $\sigma = (\sigma_1, \dots, \sigma_s)$ an s -tuple in $\mathrm{GL}(V) \cong \mathrm{GL}_n(k)$. We will use the notation

$$\sigma_\infty := \sigma_1 \cdots \sigma_s \quad \text{and} \quad \sigma_0 := \sigma_\infty^{-1}.$$

Further let $G := \langle \sigma_1, \dots, \sigma_s \rangle$ be the subgroup of $\mathrm{GL}(V)$ generated by σ . (In the applications of Katz's algorithm we will have $\sigma_0 = \mathrm{Id}$, so that $\sigma = (\sigma_1, \dots, \sigma_s)$ is an element of $\Sigma_s(G)$.)

Furthermore let $F_s := \langle \gamma_1, \dots, \gamma_s \rangle$ be the free group on s generators and $\mathrm{Rep}(k[F_s])$ the category of finite dimensional $k[F_s]$ -modules. Its objects

$$(\sigma, V) = (\sigma_1, \dots, \sigma_s, V)$$

consist of a finite dimensional k -vector space V together with images $\sigma_1, \dots, \sigma_s \in \mathrm{GL}(V)$ of $\gamma_1, \dots, \gamma_s$. The morphisms

$$\phi : (\sigma, V) \longrightarrow (\tilde{\sigma}, \tilde{V}) \quad \text{with} \quad \phi \circ \sigma_i = \tilde{\sigma}_i \circ \phi$$

are linear maps from V to \tilde{V} with the compatibility conditions $\phi \circ \sigma_i = \tilde{\sigma}_i \circ \phi$ for $i = 1, \dots, s$. An element $(\sigma, V) \in \mathrm{Rep}(k[F_s])$ is called *irreducible* respectively *absolutely irreducible* if V is irreducible, respectively absolutely irreducible as $k[F_s]$ -module.

For $(\sigma, V) \in \text{Rep}(k[F_s])$ with $V \cong k^n$ and $c \in k^\times$ the matrices

$$P_c(\sigma_i) := \begin{pmatrix} \iota_n & & & & \\ & \ddots & & & \\ & & \iota_n & & \\ c(\sigma_1 - \iota_n) & \dots & c(\sigma_{i-1} - \iota_n) & c\sigma_i & \sigma_{i+1} - \iota_n \dots \sigma_s - \iota_n \\ & & & \iota_n & \\ & & & & \ddots \\ & & & & \iota_n \end{pmatrix} \quad (9.1)$$

in $\text{GL}_s(V) \cong \text{GL}_{sn}(k)$ with $\iota_n \in \text{GL}(V)$ the identity matrix, are the *Pochhammer transforms* (in honor of Pochhammer (1870), who for the first time gave such a relation between hyperelliptic differential equations, compare also Haraoka (1994)). The Pochhammer transforms define a functor

$$P_c : \text{Rep}(k[F_s]) \longrightarrow \text{Rep}(k[F_s]), \quad (\sigma, V) \mapsto (P_c(\sigma), V^s), \quad (9.2)$$

with $P_c(\sigma) := (P_c(\sigma_1), \dots, P_c(\sigma_s))$, which here will be called the *Pochhammer transformation* (called convolution in Dettweiler (2003)). The product

$$P_c(\sigma_\infty) := P_c(\sigma_1) \cdots P_c(\sigma_s)$$

satisfies the easily verifiable formula

$$P_c(\sigma_\infty) - c\iota_{sn} = c \text{ diag}(\sigma_2 \cdots \sigma_s, \dots, \sigma_s, \iota_n) \cdot \begin{pmatrix} \sigma_1 - \iota_n & \dots & \sigma_s - \iota_n \\ \vdots & & \vdots \\ \sigma_1 - \iota_n & \dots & \sigma_s - \iota_n \end{pmatrix} \quad (9.3)$$

which will turn out to be quite useful. Moreover we observe the following:

Proposition 9.1. *Let $(\sigma, V) \in \text{Rep}(k[F_s])$, $c \in k^\times$ and $(P_c(\sigma), V)$ a Pochhammer transform. Then both*

$$\begin{aligned} X &:= X_V := (\ker(\sigma_1 - \iota_n), \dots, \ker(\sigma_s - \iota_n))^t \leq V^s \quad \text{and} \\ Y &:= Y_V := \bigcap_{i=1}^s \ker(P_c(\sigma_i) - \iota_{sn}) \leq V^s \end{aligned}$$

are $H := \langle P_c(\sigma_1), \dots, P_c(\sigma_s) \rangle$ -invariant subspaces of V^s .

Thus the functor P_c induces a residue class functor \bar{P}_c onto a lower dimensional vector space $W := V^s / (X + Y)$, which will here be called *convolution* (middle convolution in Dettweiler (2003)):

$$\bar{P}_c(\sigma, V) := (\bar{P}_c(\sigma), W) \quad \text{with} \quad W := V^s / (X_V + Y_V). \quad (9.4)$$

Remark. A morphism $\phi : (\sigma, V) \rightarrow (\tilde{\sigma}, \tilde{V})$ in $\text{Rep}(k[F_s])$ induces canonical morphisms

$$P_c(\phi) : (P_c(\sigma), V^s) \rightarrow (P_c(\tilde{\sigma}), \tilde{V}^s), \quad (v_1, \dots, v_s)^t \mapsto (\phi(v_1), \dots, \phi(v_s))^t,$$

$$\bar{P}_c(\phi) : (\bar{P}_c(\sigma), W) \rightarrow (\bar{P}_c(\tilde{\sigma}), \tilde{W}) \quad \text{with } W = V^s / (X + Y), \quad \tilde{W} = \tilde{V}^s / (\tilde{X} + \tilde{Y}),$$

on $\text{Rep}(k[F_s])$. In this way the Pochhammer transformation P_c and the convolution \bar{P}_c become endofunctors on $\text{Rep}(k[F_s])$.

The dimension of the image $W := V^s / (X + Y)$ of \bar{P}_c is given by a simple formula:

Proposition 9.2. *Let $(\sigma, V) \in \text{Rep}(k[F_s])$ with $\dim_k(V) = n$ and $\sigma_i \neq \iota_n$ for $i = 1, \dots, s$, and $1 \neq c \in k^\times$. Then the dimension of the image $W := V^s / (X + Y)$ of the convolution \bar{P}_c is given by*

$$\dim_k(W) = \sum_{i=1}^s \text{rk}(\sigma_i - \iota_n) - (n - \text{rk}(c\sigma_\infty - \iota_n)).$$

Proof. We first show that $Y = Y_V$ is given by

$$Y = \{(\sigma_2 \cdots \sigma_s(v), \sigma_3 \cdots \sigma_s(v), \dots, \sigma_s(v), v)^t \mid v \in \ker(c\sigma_\infty - \iota_n)\}. \quad (9.5)$$

To see this let us write Z for the right hand side of this equation. From

$$(P_c(\sigma_i) - \iota_n)(\sigma_2 \cdots \sigma_s(v), \dots, \sigma_s(v), v)^t = (0, \dots, -v + c\sigma_\infty(v), \dots, 0)^t$$

with non-trivial i th row it already follows that $Y \geq Z$. Now let $\mathbf{y} = (y_1, \dots, y_s)^t \in Y$. Then by definition $(P_c(\sigma_i) - \iota_n)\mathbf{y} = 0$ for all $i = 1, \dots, s$ and hence also

$$\begin{aligned} z_i &:= c(\sigma_1 - \iota_n)y_1 + \dots + c(\sigma_{i-1} - \iota_n)y_{i-1} + (c\sigma_i - \iota_n)y_i \\ &\quad + (\sigma_{i+1} - \iota_n)y_{i+1} + \dots + (\sigma_s - \iota_n)y_s = 0. \end{aligned}$$

Thus the differences

$$z_{i+1} - z_i = (1 - c)y_i + (c - 1)\sigma_{i+1}(y_{i+1})$$

also vanish, and so $y_i = \sigma_{i+1}(y_{i+1})$ as $c \neq 1$. Plugging this into z_s we obtain

$$0 = z_s = c(\sigma_1 \cdots \sigma_s - \sigma_2 \cdots \sigma_s)y_s + \dots + (c\sigma_s - \iota_n)y_s = (c\sigma_\infty - \iota_n)y_s$$

and so $y_s \in \ker(c\sigma_\infty - \iota_n)$. This shows that $Y \leq Z$ and hence our claim $Y = Z$.

Next we show that $X \cap Y = 0$. For this let

$$\mathbf{v} = (\sigma_2 \cdots \sigma_s(v), \dots, v)^t \in X \cap Y.$$

Then $(\sigma_i - \iota_n)(\sigma_{i+1} \cdots \sigma_s)(v) = 0$ for all i and hence

$$\sigma_i \cdots \sigma_s(v) = \sigma_{i+1} \cdots \sigma_s(v) = \dots = v \quad \text{for } i = 1, \dots, s.$$

Thus we have

$$v \in \bigcap_{i=1}^s \ker(\sigma_i - \iota_n) \cap \ker(c\sigma_\infty - \iota_n).$$

Due to $v = \sigma_1 \cdots \sigma_s(v)$ and $c \neq 0$ this leads to $v = 0$ and hence to $X \cap Y = 0$.

Our assertion about the dimension follows immediately from these two formulas:

$$\begin{aligned} \dim_k(W) &= s n - \sum_{i=1}^s \dim_k(\ker(\sigma_i - \iota_n)) - \dim_k(Y) \\ &= \sum_{i=1}^s \operatorname{rk}(\sigma_i - \iota_n) - (n - \operatorname{rk}(c\sigma_\infty - \iota_n)). \end{aligned}$$

□

Remark. In the case $c = 1$ one obtains directly from the definition that

$$Y = \{(v_1, \dots, v_s)^t \mid \sum_{i=1}^s (\sigma_i - \iota_n) v_i = 0\}.$$

The next result shows that the convolution behaves well with respect to invariant subspaces and their direct sums.

Proposition 9.3. *Let $(\sigma, V) \in \operatorname{Rep}(k[F_s])$ and $G := \langle \sigma_1, \dots, \sigma_s \rangle$. Further let \bar{P}_c be a convolution with $c \in k^\times$ and $H := \langle \bar{P}_c(\sigma_1), \dots, \bar{P}_c(\sigma_s) \rangle$.*

(a) *If $U \leq V$ is a G -invariant subspace, then U^s is an H -invariant subspace of V^s .*

(b) *If $V = U_1 \oplus U_2$ is a direct sum of two G -submodules then also*

$$\bar{P}_c(\sigma, V) = \bar{P}_c(\sigma, U_1) \oplus \bar{P}_c(\sigma, U_2).$$

Proof. We first show (a). By definition of \bar{P}_c we see that $U^s \leq V^s$ is H -invariant. It remains to show the formula $U^s \cap (X_V + Y_V) = X_U + Y_U$. In the case $c = 1$ this follows immediately from Proposition 9.1. For $c \neq 1$ we certainly have $X_U + Y_U \leq U^s \cap (X_V + Y_V)$. If now $v = (v_1, \dots, v_s)^t$ is an element of $U^s \cap (X_V + Y_V)$ then by Proposition 9.1 and the proof of Proposition 9.2 we get

$$v_i = w_i + \sigma_{i+1} \cdots \sigma_s(u) \quad \text{with} \quad w_i \in \ker(\sigma_i - \iota_n), u \in \ker(c\sigma_\infty - \iota_n).$$

From this it follows that

$$\sum_{i=1}^s (\sigma_i - \iota_n) v_i = \sum_{i=1}^s (\sigma_i \cdots \sigma_s - \sigma_{i+1} \cdots \sigma_s)(u) = (\sigma_\infty - \iota_n)(u) = \left(\frac{1}{c} - 1\right)u \in U$$

and hence $u \in U$ due to $c \neq 1$. Thus also all of the components w_i lie in U , which implies that $\mathbf{v} \in X_U + Y_U$.

Assertion (b) follows immediately from assertion (a). \square

9.2 Multiplicativity of Convolution

In order to simplify our assumptions we introduce a hypothesis which will always be satisfied in our application cases of irreducible linear groups. We say that $(\sigma, V) \in \text{Rep}(k[F_s])$ satisfies hypothesis (H) if for all $a \in k^\times$ the following two statements hold:

$$(H1) : \quad \ker(a\sigma_i - \iota_n) \cap \bigcap_{j \neq i} \ker(\sigma_j - \iota_n) = 0 \quad \text{for } i = 1, \dots, s,$$

$$(H2) : \quad U_i(a) := \text{im}(a\sigma_i - \iota_n) + \sum_{j \neq i} \text{im}(\sigma_j - \iota_n) = V \quad \text{for } i = 1, \dots, s.$$

Let us point out the following:

Remark. (a) The k -vector spaces $U_i(a)$ are $\langle \sigma \rangle$ -invariant, as is

$$U_\infty := \sum_{j=1}^s \text{im}(\sigma_j - \iota_n). \quad (9.6)$$

(b) Under hypothesis (H) we have $U_\infty = V$.

The next statement is equally obvious.

Proposition 9.4. *For $(\sigma, V) \in \text{Rep}(k[F_s])$ the hypothesis (H) holds in any of the two cases:*

- (1) (σ, V) is irreducible and $\dim_k(V) > 1$.
- (2) We have $\dim_k(V) = 1$ and $(\sigma_1, \dots, \sigma_s)$ has at least two components with $\sigma_i \neq \iota_1$.

We now show that hypothesis (H) is preserved by convolution.

Proposition 9.5. *If hypothesis (H) is satisfied for $(\sigma, V) \in \text{Rep}(k[F_s])$, then it also holds for $\bar{P}_c(\sigma, V)$ for all $c \in k^\times$.*

Proof. We start with the special case $a = 1$. Here for part (H1) we have to check the validity of

$$\bigcap_{i=1}^s \ker(\tau_i - \iota_{ns}) + X = Y + X, \quad \text{for } X := X_V, Y := Y_V$$

where $\tau = P_c(\sigma)$. Let us denote the left hand side by U . Then certainly $U \geq Y + X$. On the other hand $\mathbf{v} = (v_1, \dots, v_s)^t \in U$ satisfies

$$(\tau_j - \iota_{ns})\mathbf{v} \in (0, \dots, \ker(\sigma_j - \iota_n), \dots, 0)^t.$$

This implies that $(\sigma_i - \iota_n)v_j \in \ker(\sigma_j - \iota_n)$ for $i \neq j$ as well as $(c\sigma_j - \iota_n)v_i \in \ker(\sigma_j - \iota_n)$. So

$$(\sigma_j - \iota_n)v_j \in \ker(c\sigma_j - \iota_n) \cap \bigcap_{i \neq j} \ker(\sigma_i - \iota_n) = 0,$$

which implies $\mathbf{v} \in \bigcap_{i=1}^s \ker(\tau_i - \iota_{ns}) + X = Y + X$ and hence $U \leq Y + X$.

For part (H2) in the case $a = 1$ we need to verify

$$\sum_{i=1}^s \text{im}(\tau_i - \iota_{ns}) = V^s.$$

Again denoting the left hand side by U , we trivially have $U \leq V^s$. By (H2) for (σ, V) for any $\mathbf{v} \in V^s$ there exist elements $w_{ij} \in V$ with

$$v_i = \sum_{j < i} c(\sigma_j - \iota_n)w_{ij} + (c\sigma_i - \iota_n)w_{ii} + \sum_{j > i} (\sigma_j - \iota_n)w_{ij} \quad \text{for } i = 1, \dots, s.$$

So the vector $\mathbf{v}_i := (0, \dots, v_i, \dots, 0)^t$ has the form

$$\mathbf{v}_i = (\tau_i - \iota_{ns})\mathbf{w}_i \quad \text{with } \mathbf{w}_i = (w_{i1}, \dots, w_{is})^t.$$

Consequently,

$$\mathbf{v} = \sum_{i=1}^s \mathbf{v}_i = \sum_{i=1}^s (\tau_i - \iota_{ns})\mathbf{w}_i \in U.$$

In the case $a \neq 1$ for fixed i we let U denote the intersection of

$$\bigcap_{j \neq i} \ker(\sigma_j - \iota_n) + X \quad \text{with } \ker(a\sigma_i - \iota_n) + X + Y.$$

Then for (H1) we need to show that $U = X + Y$. Clearly $U \geq X + Y$. Now let $\mathbf{v} = (v_1, \dots, v_s)^t \in U$, so that we have

$$(\tau_j - \iota_{ns})\mathbf{v} \in X \quad \text{for } j \neq i \quad \text{and} \quad (a\tau_i - \iota_{ns})\mathbf{v} \in X + Y.$$

The latter leads to a linear system of equations

$$\begin{aligned} A\mathbf{v} &= \mathbf{w} & \text{with } \mathbf{w} = (w_1, \dots, \overset{i}{0}, \dots, w_s)^t \in X_1, \\ B\mathbf{v} &= \mathbf{u} & \text{with } \mathbf{u} \in X + Y, \end{aligned}$$

with the matrices

$$A = \begin{pmatrix} c\sigma_1 - \iota_n & \dots & \sigma_s - \iota_n \\ \vdots & \ddots & \vdots \\ c\sigma_1 - \iota_n & \dots & c\sigma_s - \iota_n \end{pmatrix}, \quad B = \begin{pmatrix} (a-1)\iota_n & & 0 \\ & \ddots & \\ ac(\sigma_1 - \iota_n) & \dots & ac\sigma_i - \iota_n & \dots & a(\sigma_s - \iota_n) \\ & & & \ddots & \\ 0 & & & & (a-1)\iota_n \end{pmatrix}.$$

The second system of equations implies

$$u_j = (a-1)v_j \quad \text{for } j \neq i \quad \text{and} \quad u_i = (a-1)v_i + az_i \quad \text{with}$$

$$z_i = c(\sigma_1 - \iota_n)v_1 + \dots + (c\sigma_i - \iota_n)v_i + \dots + (\sigma_s - \iota_n)v_s.$$

From this one obtains $\mathbf{u} = (a-1)\mathbf{v} + a\mathbf{z}_i$ with $\mathbf{z}_i := (0, \dots, z_i, \dots, 0)^t$, which then yields $(a-1)\mathbf{v} + a\mathbf{z}_i \in X + Y$. For \mathbf{z}_i we obtain analogously

$$\begin{aligned} A\mathbf{z}_i &= ((\sigma_i - \iota_n)z_i, \dots, 0, \dots, c(\sigma_i - \iota_n)z_i)^t \in X, \\ B\mathbf{z}_i &= (0, \dots, (ac\sigma_i - \iota_n)z_i, \dots, 0) \in X + Y. \end{aligned}$$

According to (H1) for (σ, V) the image of \mathbf{z}_i in $\bar{U} := U/(X + Y)$ is zero, which implies $\mathbf{z}_i \in X + Y$ and so finally also $\mathbf{v} \in X + Y$ as $a \neq 1$.

To check (H2) in the case $a \neq 1$ we have to verify that

$$\operatorname{im}(a\tau_i - \iota_{ns}) + \sum_{j \neq i} \operatorname{im}(\tau_j - \iota_{ns}) = V^s \quad \text{for } i = 1, \dots, s.$$

Denoting again the left hand side by U we certainly have $U \leq V^s$. For $\mathbf{v} \in V^s$ the assumption (H2) for (σ, V) yields the existence of vectors $w_{ij} \in V$ with

$$v_i = \sum_{j < i} ac(\sigma_j - \iota_n)w_{ij} + (ac\sigma_i - \iota_n)w_{ii} + \sum_{j > i} a(\sigma_j - \iota_n)w_{ij}.$$

For $\mathbf{v}_j := (0, \dots, v_j, \dots, 0)^t$ and $\mathbf{w}_j = (w_{j1}, \dots, w_{js})^t$ it then follows that $\mathbf{v}_i = (a\tau_i - \iota_{ns})\mathbf{w}_i$ as well as $\mathbf{v}_j = a(\tau_j - \iota_{ns})\mathbf{w}_j$ for $j \neq i$. So we have

$$\mathbf{v} = \sum_{i=j}^s \mathbf{v}_j = \sum_{j \neq i} a(\tau_j - \iota_{ns})\mathbf{w}_j + (a\tau_i - \iota_{ns})\mathbf{w}_i \in U. \quad \square$$

Theorem 9.6. Assume that $(\sigma, V) \in \operatorname{Rep}(k[F_s])$ satisfies hypothesis (H) and let $c_1, c_2 \in K^\times$ with $c_1c_2 = c$. Then we have an isomorphism

$$\bar{P}_c(\sigma, V) \cong \bar{P}_{c_2}(\bar{P}_{c_1}(\sigma, V))$$

as $k[F_s]$ -modules and hence in particular

$$\bar{P}_1(\sigma, V) \cong (\sigma, V).$$

Proof. In a first step we verify the highlighted special case $\bar{P}_1(\sigma, V) \cong (\sigma, V)$. From the representation of Y for $c = 1$ in the Remark after Proposition 9.2 it follows that $X \leq Y$ and so $X + Y = Y$. As $U_\infty = V$ by the Remark (b) before Proposition 9.4 the linear map

$$\phi : V^s \longrightarrow V, \quad (v_1, \dots, v_s)^t \mapsto \sum_{i=1}^s (\sigma_i - \iota_n) v_i$$

is surjective with kernel Y . So $\bar{P}_1 = \phi \circ P_1$ induces an isomorphism of k -vector spaces. The isomorphy in $k[F_s]$ then follows upon verification of $\phi \circ P_1(\sigma_i) = \sigma_i \circ \phi$.

In a second step for $\tau = P_{c_1}(\sigma)$ we show the formula

$$\bar{P}_{c_2}(\bar{P}_{c_1}(\sigma, V)) \cong \bar{P}_{c_2}(\tau, V^s)/\bar{P}_{c_2}(\tau, X_V + Y_V(c_1)), \quad (9.7)$$

where the added c_i is meant to indicate the action with P_{c_i} . According to the first step we may here assume that $c_1 \neq 1 \neq c_2$. Let us abbreviate $(\bar{\tau}, W) := \bar{P}_{c_1}(\sigma, V)$ and

$$X_1 := X_V, \quad Y_1 := Y_V(c_1), \quad X_2 := X_V^s, \quad Y_2 := Y_V^s(c_2).$$

Clearly assertion (9.7) would follow from

$$X_W = (X_2 + X_1^s + Y_1^s)/(X_1^s + Y_1^s) \quad \text{and} \quad Y_W = (Y_2 + X_1^s + Y_1^s)/(X_1^s + Y_1^s).$$

To prove the formula for X_W we denote the right hand side by U . Then certainly $U \leq X_W$. By definition we now have

$$X_W = (\ker(\bar{\tau}_1 - \iota_m), \dots, \ker(\bar{\tau}_s - \iota_m))^t \quad \text{with} \\ \ker(\bar{\tau}_i - \iota_m) = \{w_i + X_1 + Y_1 \in W \mid (\tau_i - \iota_{sn})w_i \in X_1 + Y_1\}$$

with $m = \dim_k(W)$. Using (9.5) we obtain

$$(\tau_i - \iota_{sn})w_i = (x_{i1} + \sigma_2 \cdots \sigma_s(y_i), x_{i2} + \sigma_3 \cdots \sigma_s(y_i), \dots, x_{is} + y_i)$$

with $x_{ij} \in \ker(\sigma_j - \iota_n)$ and $y_i \in \ker(c_1 \sigma_\infty - \iota_n)$. According to (H1) the right hand side has the form $(0, \dots, *, \dots, 0)$. So we have $y_i \in \ker(\sigma_j - \iota_n)$ for $j \neq i$ and $y_i \in \ker(c_1 \sigma_i - \iota_n)$. This shows that

$$(\tau_i - \iota_{sn})(w_i) \in (0, \dots, \ker(\sigma_i - \iota_n), \dots, 0)^t,$$

which finally implies that $w_i \in \ker(\tau_i - \iota_{sn}) + X_1$ and hence $X_W \leq U$.

Now let U denote the right hand side in the stipulated formula for Y_W . Then we have $U \leq Y_W$. An element $(\bar{z}_1, \dots, \bar{z}_s)$ from

$$Y_W = \bigcap_{i=1}^s \ker(\bar{\rho}_i - \iota_{sm}) \quad \text{with} \quad (\bar{\rho}_1, \dots, \bar{\rho}_s) = \bar{P}_{c_2}(\tau)$$

is a solution of the homogeneous system of linear equations

$$c_2(\bar{\tau}_1 - \iota_m)\bar{z}_1 + \dots + (c_2\bar{\tau}_i - \iota_m)\bar{z}_i + \dots + (\bar{\tau}_s - \iota_m)\bar{z}_s = 0 \quad (1 \leq i \leq s).$$

Here the components \bar{z}_j have the form $\bar{z}_j = z_j + X_1 + Y_1$ with $z_j \in V^s$. This implies for $\rho = P_{c_2}(\tau)$ that

$$(\rho_i - \iota_{s^2 n})(z_1, \dots, z_s)^t \in X_1^s + Y_1^s \quad \text{for } i = 1, \dots, s,$$

from which we conclude $(z_1, \dots, z_s)^t \in Y_2 + X_1 + Y_1$ and thus finally $(\bar{z}_1, \dots, \bar{z}_s) \in U$.

In the third and last step of the proof we show the claimed general multiplication formula for the convolution. For this it suffices to show that the linear map

$$\bar{\phi} : \bar{P}_{c_2}(\bar{P}_{c_1}(\sigma, V)) \longrightarrow \bar{P}_c(\sigma, V)$$

induced by

$$\phi : P_{c_2}(P_{c_1}(\sigma, V)) \longrightarrow P_c(\sigma, V), \quad (v_1, \dots, v_s)^t \mapsto \sum_{i=1}^s (\tau_i - \iota_{ns}) v_i,$$

is an isomorphism in $\text{Rep}(k[F_s])$. By the first step we may assume that $c_1 \neq 1 \neq c_2$. The surjectivity of ϕ follows directly from (H2), case $a = 1$, in the proof of Proposition 9.5. We now use the notation X_1, Y_1, X_2, Y_2 from the second step and in addition

$$X := X_V \quad \text{and} \quad Y := Y_V(c).$$

Then from the second step we first obtain the isomorphisms

$$\begin{aligned} \bar{P}_{c_2}(\bar{P}_{c_1}(\sigma, V)) &\cong \bar{P}_{c_2}(\tau, V^s) / \bar{P}_{c_2}(\tau, X_1 + Y_1) \\ &\cong (\rho, (V^s)^s) / (\rho, (X_1 + Y_1)^s + X_2 + Y_2) \end{aligned}$$

for the underlying vector spaces. Here by definition we have $X_2 = \ker(\phi)$ and $Y_1^s \leq X_2$. So the canonical homomorphism is certainly well-defined and surjective. Furthermore,

$$\phi(X_1^s) = \sum_{i=1}^s (\tau_i - \iota_{ns}) X_1 = (\dots, (c_1 \sigma_i - \iota_n) \ker(\sigma_i - \iota_n), \dots)^t \cong X_1 = X.$$

Using (9.5) this gives

$$\begin{aligned}\phi(Y_2) &= \phi(\{(\tau_2 \cdots \tau_s(v), \dots, \tau_s(v), v)^t \mid v \in \ker(c_2 \tau_\infty - \iota_{ns})\}) \\ &= \{\tau_\infty(v) - v \mid v \in \ker(c_2 \tau_\infty - \iota_{ns})\} = \ker(c_2 \tau_\infty - \iota_{ns}).\end{aligned}$$

Here $\mathbf{v} = (v_1, \dots, v_s)^t \in \ker(c_2 \tau_\infty - \iota_{ns})$ if and only if $(c P_{c_1}(\sigma_\infty) - c_1 \iota_{ns})\mathbf{v} = 0$, respectively if $c(P_{c_1}(\sigma_\infty) - c_1 \iota_{ns})\mathbf{v} = c_1(1-c)\mathbf{v}$. By (9.3) this is equivalent to

$$c \operatorname{diag}(\sigma_2 \cdots \sigma_s, \dots, \sigma_s, \iota_n) \begin{pmatrix} \sigma_1 - \iota_n & \dots & \sigma_s - \iota_n \\ \vdots & & \vdots \\ \sigma_1 - \iota_n & \dots & \sigma_s - \iota_n \end{pmatrix} \mathbf{v} = (1-c)\mathbf{v}.$$

The last line of this linear system of equations reads

$$z_s = c(\sigma_1 - \iota_n)v_1 + \dots + (c\sigma_s - \iota_n)v_s = 0$$

with the z_s from the proof of Proposition 9.2. The lines before that yield $v_i = \sigma_{i+1}(v_{i+1})$ for $i = 1, \dots, s-1$, which as in the proof of Proposition 9.2 gives that $z_i = 0$ for $i = 1, \dots, s-1$, as well as

$$z_s = (c\sigma_\infty - \iota_n)v_s = 0 \quad \text{respectively} \quad v_s \in \ker(c\omega_\infty - \iota_n),$$

where $\omega := \bar{P}_c(\sigma)$. With this we have

$$\phi(Y_2) = Y_V(c) = Y.$$

Taken together we obtain

$$\phi(X_2 + Y_2 + X_1^s) = \phi(Y_2 + X_1^s) = \phi(Y_2) + \phi(X_1^s) = Y + X.$$

Comparing dimensions then shows that

$$\dim_k(X_2 + Y_2 + X_1^s) = \dim_k(X_2) + \dim_k(X + Y)$$

with $\dim_k(X_2) = \dim_k(\ker(\phi)) = (s-1)sn$. Thus,

$$\dim_k((V^s)^s / (X_2 + Y_2 + X_1^s)) = \dim(V^s / (X + Y)),$$

which shows that $\bar{\phi}$ is an isomorphism.

It remains to check the compatibility of $\bar{\phi}$ with the group operations, that is, the validity of

$$\phi \circ (\rho_i - \iota_{ns}) = (\omega_i - \iota_{ns}) \circ \phi \quad \text{for } i = 1, \dots, s.$$

This follows with $\mathbf{v}_j := (0, \dots, v_j, \dots, 0)^t$ from

$$\phi(\rho_i - \iota_{ns})\mathbf{v}_j = \begin{cases} c_2(\tau_i - \iota_{ns})(\tau_j - \iota_{ns})v_j & j < i \\ (\tau_i - \iota_{ns})(c_2\tau_j - \iota_{ns})v_j & \text{for } j = i \\ (\tau_i - \iota_{ns})(\tau_j - \iota_{ns})v_j & j > i \end{cases} = (0, \dots, w_i, \dots, 0)^t =: \mathbf{w}_i$$

in combination with

$$(\omega_i - \iota_{ns})\phi(\mathbf{v}_j) = (\omega_i - \iota_{ns})(\tau_j - \iota_{ns})(\mathbf{v}_j) = \mathbf{w}_i. \quad \square$$

Corollary 9.7. Assume that $(\sigma, V) \in \text{Rep}(k[F_s])$ satisfies the hypothesis (H). Then $\bar{P}_c(\sigma, V)$ is irreducible if and only if (σ, V) is.

Proof. This follows immediately from Proposition 9.3(a) together with the invertibility of \bar{P}_c shown in Theorem 9.6. \square

9.3 Linear Rigidity

The concept of linear rigidity is closely related with the rigidity of a tuple of group elements and has proved highly useful in connection with the Katz algorithm. We call an s -tuple $(\sigma_1, \dots, \sigma_s) \in \text{GL}_n(k)^s$ *linearly rigid* (physically rigid in Katz (1996)), if $\sigma_1 \cdots \sigma_s = \iota_n$ and the conjugacy classes \tilde{C}_i of σ_i in $\text{GL}_n(k)$ satisfy the following rigidity condition: If $(\tau_1, \dots, \tau_s) \in \text{GL}_n(k)^s$ is a further s -tuple with $\tau_i \in \tilde{C}_i$, then there exists $\rho \in \text{GL}_n(k)$ with $\tau_i = \sigma_i^\rho$ for all i . So the group G generated by $\sigma_1, \dots, \sigma_s$ does not enter the picture.

If now C_i is the conjugacy class of σ_i in $G := \langle \sigma_1, \dots, \sigma_s \rangle \leq \text{GL}_n(k)$ then $\mathbf{C} = (C_1, \dots, C_s)$ is called *GL-stable* (or *stable* for short), if it satisfies the following *stability condition*:

(S) Every $\alpha \in \mathcal{N}_{\text{GL}_n(k)}(G)$ with $C_i^\alpha = C_i$ for $i = 1, \dots, s$ lies in $\mathcal{C}_{\text{GL}_n(k)}(G) \cdot G$.

The connection between linear rigidity and rigidity is explained by the next result (see Theorem I.5.10 and the subsequent Remark):

Proposition 9.8. Let $\sigma \in \text{GL}_n(k)^s$ with $\sigma_1 \cdots \sigma_s = \iota_n$, $G := \langle \sigma_1, \dots, \sigma_s \rangle$ and $C_i := [\sigma_i]$ in G . Then we have:

(a) If σ is linearly rigid and $\mathbf{C} = (C_1, \dots, C_s)$ is GL-stable then σ , respectively $\Sigma_s(\sigma)$ is rigid.

(b) If $\mathcal{N}_{\text{GL}_n(k)}(G) = \mathcal{C}_{\text{GL}_n(k)}(G) \cdot G$ then every linearly rigid $\sigma \in \Sigma_s(G)$ is rigid.

Conversely it is not true that the rigidity of $\sigma \in \Sigma_s(G)$ implies linear rigidity. This results from the fact that for linearly rigid tuples the generating system class number $l(\mathbf{C})$ agrees in G with the normalized structure constant $n(\mathbf{C})$, which is not usually satisfied for rigid tuples (see for example the oddments in Section II.9.5).

A crucial role for the criterion for linear rigidity used in Katz's algorithm is played by the so-called Lemma of Scott (1977):

Proposition 9.9 (Lemma of Scott). *Let k be any field, $V = k^n$ and $(\sigma_1, \dots, \sigma_s) \in \mathrm{GL}(V)^s$ with $\sigma_1 \cdots \sigma_s = \mathrm{Id}_V$. Further let $c(\sigma_i)$ be the codimension of the fixed point space $F(\sigma_i)$ in V , $c(\sigma)$ the codimension of $F(\sigma) := \bigcap_{i=1}^s F(\sigma_i)$, and $c(\sigma^*)$ and $c(\sigma^*)$ the corresponding codimensions for the dual action. Then we have*

$$\sum_{i=1}^s c(\sigma_i) \geq c(\sigma) + c(\sigma^*).$$

Proof. We define

$$U := \{\mathbf{v} = (v_1, \dots, v_s)^t \in V^s \mid v_i \in (1 - \sigma_i)V\}$$

and linear maps

$$\begin{aligned} \phi : V &\longrightarrow U, & v &\mapsto ((1 - \sigma_1)v, \dots, (1 - \sigma_s)v)^t, \\ \psi : U &\longrightarrow V, & \mathbf{v} &\mapsto v_1 + \sigma_1(v_2) + \dots + \sigma_1 \cdots \sigma_{s-1}(v_s). \end{aligned}$$

Then the identity

$$\iota_n - \sigma_1 \cdots \sigma_s = (1 - \sigma_1) + \sigma_1(1 - \sigma_2) + \dots + \sigma_1 \cdots \sigma_{s-1}(1 - \sigma_s)$$

in $k[\mathrm{GL}(V)]$ immediately yields $\psi((1 - \sigma_1)v, \dots, (1 - \sigma_s)v) = 0$ and thus $\mathrm{im}(\phi) \leq \ker(\psi)$. Now let $G := \langle \sigma_1, \dots, \sigma_s \rangle$. Then

$$\psi(U) = (1 - \sigma_1)V + \sigma_1(1 - \sigma_2)V + \dots + \sigma_1 \cdots \sigma_{s-1}(1 - \sigma_s)V = \sum_{i=1}^s (1 - \sigma_i)V$$

is the smallest G -submodule W of V such that the action of G is trivial on V/W . Thus we have

$$\dim_k(\psi(U)) = c(\sigma^*) = \dim_k(U/\ker(\psi)).$$

Now $\ker(\phi)$ is the subspace of fixed points of G , so by definition it has dimension $\dim_k(\phi(U)) = c(\sigma)$. So we get the two expressions

$$\dim_k(U) = \sum_{i=1}^s c(\sigma_i) \quad \text{with} \quad c(\sigma_i) = \dim_k((1 - \sigma_i)V)$$

and

$$\begin{aligned} \dim_k(U) &= \dim_k(U/\ker(\psi)) + \dim_k(\ker(\psi)/\mathrm{im}(\phi)) + \dim_k(\mathrm{im}(\phi)) \\ &\geq c(\sigma^*) + c(\sigma), \end{aligned}$$

which together prove the claim. \square

Corollary 9.10. *If $\sigma = (\sigma_1, \dots, \sigma_s) \in \mathrm{GL}_n(k)^s$ with $\sigma_1 \cdots \sigma_s = \iota_n$ is irreducible, then*

$$\sum_{i=1}^s \mathrm{rk}(\sigma_i - \iota_n) \geq 2n.$$

Proof. In the case of irreducibility of $\langle \sigma_1, \dots, \sigma_s \rangle$ we have $c(\sigma) = n = c(\sigma^*)$, and the claim follows from Proposition 9.9. \square

Remark. In the case of permutation representations, Scott's formula just says that the genus (as computed by the Hurwitz relative genus formula) of a cover of the Riemann sphere ramified at s points with inertia generators σ_i is non-negative.

The next theorem contains the previously announced criterion for linear rigidity in the form presented by Strammbach and Völklein (1999):

Theorem 9.11. *Let $\sigma \in \mathrm{GL}_n(k)^s$ be absolutely irreducible with $\sigma_1 \cdots \sigma_s = \iota_n$. Then we have*

(a) $\mathrm{rid}(\sigma) := \sum_{i=1}^s \mathrm{codim}_k(\mathcal{C}_{k^{n \times n}}(\sigma_i)) - 2(n^2 - 1) \geq 0$.

(b) *If $k = \bar{k}$ is algebraically closed then moreover $\mathrm{rid}(\sigma) = 0$ if and only if σ is linearly rigid.*

Proof. For part (a) let $\tau_1, \dots, \tau_s \in \mathrm{GL}_n(k)^s$ with $\tau_1 \cdots \tau_s = \iota_n$ with τ_i conjugate in $\mathrm{GL}_n(k)$ to σ_i , that is, there exist $\rho_i \in \mathrm{GL}_n(k)$ such that $\tau_i = \rho_i \sigma_i \rho_i^{-1}$ for $i = 1, \dots, s$. Further let $W = k^{n \times n}$ be the vector space of $n \times n$ -matrices over k and define linear maps

$$\phi_i : W \longrightarrow W, \quad \rho \mapsto \sigma_i \rho \tau_i^{-1},$$

of W into itself. We first show that

$$c(\phi_i) = n^2 - \dim_k(F(\phi_i)) = n^2 - \dim_k(\mathcal{C}_W(\sigma_i)). \quad (9.8)$$

For $\omega_i \in F(\phi_i)$ we have $\omega_i = \sigma_i \omega_i \tau_i^{-1}$. As $\rho_i \sigma_i \rho_i^{-1} = \tau_i = \omega_i^{-1} \sigma_i \omega_i$ this is equivalent to $\omega_i \rho_i \in \mathcal{C}_W(\sigma_i)$, respectively $\omega_i \in \mathcal{C}_W(\sigma_i) \rho_i^{-1}$. From this (9.8) follows due to $\dim_k(\mathcal{C}_W(\sigma_i) \rho_i^{-1}) = \dim(\mathcal{C}_W(\sigma_i))$.

Next we show that $\mathrm{rid}(\sigma) \geq 0$. For this we use the dual vector space W^* via

$$W \times W^* \longrightarrow k, \quad (\rho, \delta) \mapsto \mathrm{tr}(\rho \delta),$$

and the map

$$\phi_i^* : W^* \longrightarrow W^*, \quad \delta \mapsto \tau_i \delta \sigma_i^{-1},$$

dual to ϕ_i . Specializing ϕ_i to conjugation with σ_i , that is, choosing $\tau_i = \sigma_i$, we obtain

$$\dim_k(F(\phi)) = \dim_k(\mathcal{C}_W(\langle \sigma_1, \dots, \sigma_s \rangle)) = 1$$

because of the absolute irreducibility of (σ, V) , and similarly $\dim_k(F(\phi^*)) = 1$. So from the Lemma of Scott and (9.8) we get

$$2(n^2 - 1) = c(\phi) + c(\phi^*) \leq \sum_{i=1}^s c(\phi_i) = \sum_{i=1}^s \text{codim}_k(\mathcal{C}_W(\sigma_i))$$

as claimed.

For part (b) we first assume that $\text{rid}(\sigma) = 0$, but not yet that $k = \bar{k}$. Then by (a) we have

$$\sum_{i=1}^s \text{codim}_k(\mathcal{C}_W(\sigma_i)) = \sum_{i=1}^s c(\phi_i) = 2(n^2 - 1),$$

so by the Lemma of Scott $c(\phi) + c(\phi^*) \leq 2(n^2 - 1)$. Thus either $F(\phi) \neq 0$ or $F(\phi^*) \neq 0$. Assume that $F(\phi) \neq 0$ and $0 \neq \rho \in F(\phi)$. Then ρ is invertible due to the irreducibility of (σ, V) . As $F(\phi) = \bigcap_{i=1}^s F(\phi_i)$ we see that $\phi_i(\rho) = \rho$ for all $i = 1, \dots, s$. But this is equivalent to $\sigma_i \rho \tau_i^{-1} = \rho$, that is, $\rho^{-1} \sigma_i \rho = \tau_i$ for all i . So σ is linearly rigid.

For the converse we assume that $k = \bar{k}$; so let $\sigma \in \text{GL}_n(\bar{k})^s$ be linearly rigid. Further let $C_i := [\sigma_i]$ be the conjugacy class of σ_i in the algebraic group $G = \text{GL}_n(\bar{k})$. We define a morphism

$$\pi : C_1 \times \cdots \times C_s \longrightarrow G' := G/\mathcal{L}(G), \quad (\sigma_1, \dots, \sigma_s) \mapsto \sigma_1 \cdots \sigma_s \pmod{\mathcal{L}(G)}.$$

As σ is linearly rigid, the fibre $\mathcal{O} := \pi^{-1}(\iota_n)$ forms a single G -orbit under simultaneous conjugation. Consequently we have

$$\dim_k(\mathcal{O}) \leq \dim_k(G') = \dim_k(G) - \dim_k(\mathcal{L}(G)) = n^2 - 1$$

(by Springer (1998), Ch. 2.1). On the other hand by Springer (1998), Ch. 5.1, Ch. 1.8 and Ch. 2.1 we have

$$\begin{aligned} \dim_k(\mathcal{O}) &\geq \dim_k(C_1 \times \cdots \times C_s) - \dim_k(G') = \sum_{i=1}^s \dim_k(C_i) - \dim_k(G') \\ &= \sum_{i=1}^s \text{codim}_k(\mathcal{C}_W(\sigma_i)) - \dim_k(G'). \end{aligned}$$

This ensues

$$\sum_{i=1}^s \text{codim}_k(\mathcal{C}_W(\sigma_i)) \leq \dim_k(G') + \dim_k(\mathcal{O}) \leq 2(n^2 - 1).$$

This implies that $\text{rid}(\sigma) \leq 0$ and hence by (a) the desired equality $\text{rid}(\sigma) = 0$. \square

The invariant $\text{rid}(\sigma)$ in Theorem 9.11 is called the *rigidity defect*; Katz (1996) uses the notion *rigidity index* for $2 - \text{rid}(\sigma)$.

9.4 The Existence Algorithm of Katz

For the convolution operator the Jordan normal forms of the components of the image $\bar{P}_c(\sigma)$ can easily be calculated from those of $\sigma_1, \dots, \sigma_s$, based upon the following observation:

Proposition 9.12. *Assume that $(\sigma, V) \in \text{Rep}(k[F_s])$ satisfies hypothesis (H). Then for $\bar{\tau} := \bar{P}_c(\sigma)$ we have:*

- (a) $\text{rk}(\sigma_i - \iota_n) = \text{rk}(\bar{\tau}_i - \iota_m)$ for $1 \leq i \leq s$,
- (b) $\text{rk}(c\sigma_\infty - \iota_n) = \text{rk}(\bar{\tau}_\infty - c\iota_m)$.

Proof. For the proof of (a) we show that

$$\phi_i : \text{im}(\bar{\tau}_i - \iota_m) \rightarrow \text{im}(\sigma_i - \iota_m), \quad \mathbf{w}_i = (0, \dots, w_i, \dots, 0)^t + X + Y \mapsto (\sigma_i - \iota_n)w_i, \quad (9.9)$$

is an isomorphism with $\phi_i \circ \bar{\tau}_i = c\sigma_i \circ \phi_i$. For this let $\tau := P_c(\sigma)$. Then $Y \leq \ker(\tau_i - \iota_{sn})$ by Proposition 9.1. Thus ϕ_i is well-defined and injective. By (H) we have $U_i(c) = V$, so ϕ_i is moreover surjective and hence an isomorphism of vector spaces. The compatibility with the group operations is now obtained as

$$\phi_i(\tau_i(\tau_i - \iota_{sn}))(\mathbf{w}_i + X + Y) = (\sigma_i - \iota_n)c\sigma_i w_i = c\sigma_i \phi_i(\tau_i - \iota_{sn})(\mathbf{w}_i + X + Y).$$

For the proof of (b) we show that the map

$$\begin{aligned} \phi_\infty : \text{im}(\bar{\tau}_\infty - c\iota_m) &\rightarrow \text{im}(c\sigma_\infty - \iota_n), \\ \mathbf{w} = (w_1, \dots, w_s)^t + X + Y &\mapsto (c\sigma_\infty - \iota_n)w_i, \end{aligned} \quad (9.10)$$

is an isomorphism with $\phi_\infty \circ (\bar{\tau}_\infty - \iota_m) = (c\sigma_\infty - \iota_n) \circ \phi_\infty$. According to (9.5) we have

$$Y = \{(\sigma_2 \cdots \sigma_s(v), \dots, \sigma_s(v), v)^t \mid v \in \ker(c\sigma_\infty - \iota_n)\},$$

which immediately gives $\phi_\infty(Y) = 0$. Further by (9.3) we also have

$$(\tau_\infty - c\iota_{sn})X = (\tau_\infty - c\iota_{sn})(\ker(\sigma_1 - \iota_n), \dots, \ker(\sigma_s - \iota_n))^t = 0.$$

Thus, ϕ_∞ is well-defined and both injective as well as surjective, hence an isomorphism. The compatibility with the group action follows since

$$\begin{aligned} \phi_\infty(\tau_\infty - c\iota_{sn})^2(\mathbf{w} + X + Y) &= (c\sigma_\infty - \iota_n)^2 w_s \\ &= (\sigma_\infty - \iota_n)\phi_\infty(\tau_\infty - c\iota_{sn})(\mathbf{w} + X + Y). \end{aligned}$$

□

The above rank formulas lead to an explicit description of the Jordan normal forms of the images under convolution. They also form a crucial prerequisite in the explicit examples computed in the subsequent paragraphs.

Corollary 9.13. Let $k = \bar{k}$ be algebraically closed, $(\sigma, V) \in \text{Rep}(k[F_s])$ absolutely irreducible with $s > 1$, $c \in k^\times$ and $\tau = \bar{P}_c(\sigma)$.

(a) Let $\text{diag}(J_{i,1}, \dots, J_{i,k_i})$ be the Jordan normal form of σ_i with Jordan blocks $J_{i,j}$ of lengths n_{ij} and eigenvalues a_{ij} . Then the Jordan normal form $\text{diag}(\tilde{J}_{i,1}, \dots, \tilde{J}_{i,\tilde{k}_i})$ of τ_i is obtained as follows: Every Jordan block $J_{i,j}$ of σ_i leads to a Jordan block $\tilde{J}_{i,j}$ of τ_i of length m_{ij} with eigenvalues $\tilde{a}_{ij} = ca_{ij}$, where

$$m_{ij} = \begin{cases} n_{ij} & \text{if } a_{ij} \neq 1, \frac{1}{c}, \\ n_{ij} - 1 & \text{if } a_{ij} = 1, \\ n_{ij} + 1 & \text{if } a_{ij} = \frac{1}{c}. \end{cases}$$

The other Jordan blocks of τ_i have length 1 and eigenvalue 1.

(b) Let $\text{diag}(J_{\infty,1}, \dots, J_{\infty,k_\infty})$ be the Jordan normal form of $\sigma_\infty = \sigma_1 \cdots \sigma_s$ with Jordan blocks $J_{\infty,j}$ of lengths $n_{\infty j}$ and with eigenvalues $a_{\infty j}$. Then the Jordan normal form $\text{diag}(\tilde{J}_{\infty,1}, \dots, \tilde{J}_{\infty,\tilde{k}_\infty})$ of τ_∞ is obtained as follows: every Jordan block $J_{\infty,j}$ leads to a Jordan block $\tilde{J}_{\infty,j}$ of length $m_{\infty j}$ and eigenvalue $\tilde{a}_{\infty j} = ca_{\infty j}$, where

$$m_{\infty j} = \begin{cases} n_{\infty j} & \text{if } a_{\infty j} \neq 1, \frac{1}{c}, \\ n_{\infty j} + 1 & \text{if } a_{\infty j} = 1, \\ n_{\infty j} - 1 & \text{if } a_{\infty j} = \frac{1}{c}. \end{cases}$$

All other Jordan blocks of τ_∞ have length 1 and eigenvalue c .

Proof. The assertion of Corollary 9.13 follows almost immediately from Proposition 9.12. For (a) one needs to observe that the lengths of Jordan blocks of σ_i with eigenvalue $a_{ij} \neq 1, \frac{1}{c}$ is preserved, while those for eigenvalues $a_{ij} = 1$ get shorter by one due to the factorization by the eigenspace of σ_i for the eigenvalue 1 (as part of X). Using $\bar{P}_{1/c} \circ \bar{P}_c = \text{Id}$ this implies that the lengths of Jordan blocks of σ_i for the eigenvalue $a_{ij} = \frac{1}{c}$ are increased by 1.

In (b) again the lengths of Jordan blocks of σ_∞ for eigenvalues $a_{\infty j} \neq 1, \frac{1}{c}$ are preserved. But here because of the factorization by the eigenspace of σ_∞ for $\frac{1}{c}$ according to (9.5) the lengths of Jordan blocks for the eigenvalue $\frac{1}{c}$ are decreased by 1, and hence correspondingly increase by 1 for the eigenvalue 1. \square

From Corollary 9.13 it is now possible relatively easily to derive the invariance theorem of Katz (1996), Ch. 6.0, for the rigidity defect.

Theorem 9.14 (Katz). Let $(\sigma, V) \in \text{Rep}(k[F_s])$ satisfy (H). Then for all $c \in \bar{k}^\times$ the rigidity defect is invariant under \bar{P}_c , that is, $\text{rid}(\bar{P}_c(\sigma)) = \text{rid}(\sigma)$.

Proof. For $i \in S := \{1, \dots, s, \infty\}$ let $a_{ij} \in \bar{k}$ denote the eigenvalues of $\sigma_i \in \text{GL}_n(\bar{k})$. Further let $e_i^{(\ell)}(a_{ij})$ be the number of Jordan blocks of length at least ℓ . Then $\mathcal{C}_W(\sigma_i)$ with $W = k^{n \times n}$ has dimension

$$\dim_k(\mathcal{C}_W(\sigma_i)) = \sum_{\ell \geq 1} \sum_j e_i^{(\ell)}(a_{ij})^2, \quad (9.11)$$

as is easily read off from the Jordan normal form. Correspondingly we denote by $\tilde{e}_i^{(\ell)}(\tilde{a}_{ij})$ the number of Jordan blocks of length at least ℓ of τ_i with eigenvalue \tilde{a}_{ij} for $i \in S$. According to Corollary 9.13 these satisfy

$$\tilde{e}_i^{(\ell)}(ca_{ij}) = \begin{cases} e_i^{(\ell)}(a_{ij}) & \text{for } a_{ij} \neq 1, \frac{1}{c} \text{ and } \ell \geq 1, \\ e_i^{(\ell+1)}(a_{ij}) & \text{for } a_{ij} = 1 \text{ and } \ell \geq 1, \\ e_i^{(\ell-1)}(a_{ij}) & \text{for } a_{ij} = \frac{1}{c} \text{ and } \ell \geq 2, \end{cases}$$

for $i = 1, \dots, s$, respectively

$$\tilde{e}_\infty^{(\ell)}(ca_{\infty j}) = \begin{cases} e_\infty^{(\ell)}(a_{\infty j}) & \text{for } a_{\infty j} \neq 1, \frac{1}{c} \text{ and } \ell \geq 1, \\ e_\infty^{(\ell-1)}(a_{\infty j}) & \text{for } a_{\infty j} = 1 \text{ and } \ell \geq 2, \\ e_\infty^{(\ell+1)}(a_{\infty j}) & \text{for } a_{\infty j} = \frac{1}{c} \text{ and } \ell \geq 1. \end{cases}$$

From this we obtain

$$\sum_{\ell} e_i^{(\ell)}(a_{ij})^2 - e_i^{(1)}(1)^2 = \sum_{\ell} \tilde{e}_i^{(\ell)}(ca_{ij})^2 - \tilde{e}_i^{(1)}(1)^2 =: p_i,$$

$$\sum_{\ell} e_\infty^{(\ell)}(a_{\infty j})^2 - e_\infty^{(1)}\left(\frac{1}{c}\right)^2 = \sum_{\ell} \tilde{e}_\infty^{(\ell)}(ca_{\infty j})^2 - \tilde{e}_\infty^{(1)}(c)^2 =: p_\infty,$$

with the eigenspace dimensions $e_i^{(1)}(1)$, $\tilde{e}_i^{(1)}(1)$, $e_\infty^{(1)}\left(\frac{1}{c}\right)$, $\tilde{e}_\infty^{(1)}(c)$. So p_i , p_∞ and also $p := \sum_{i \in S} p_i$ are invariant under the convolution \bar{P}_c . From Proposition 9.12 we obtain moreover that

$$n - e_i^{(1)}(1) = m - \tilde{e}_i^{(1)}(1) =: r_i \quad \text{for } i = 1, \dots, s,$$

$$n - e_\infty^{(1)}\left(\frac{1}{c}\right) = m - \tilde{e}_\infty^{(1)}(c) =: r_\infty$$

and from this the invariance of $r := \sum_{i \in S} r_i$ and $q := \sum_{i \in S} r_i^2$. This translates to the rigidity defect as

$$\begin{aligned} \text{rid}(\sigma) - 2 &= (s-1)n^2 - \sum_{i \in S} \sum_{j, \ell} e_i^{(\ell)}(a_{ij})^2 \\ &= (s-1)n^2 - p - e_\infty^{(1)}\left(\frac{1}{c}\right)^2 - \sum_{i=1}^s e_i^{(1)}(1)^2 \\ &= (s-1)n^2 - p - (n - r_\infty)^2 - \sum_{i=1}^s (n - r_i)^2 \\ &= -2n^2 - p + 2nr - q = 2n(r-n) - p - q. \end{aligned}$$

This expression is clearly \bar{P}_c -invariant, since on the one hand $n(r-n) = (m-r)m$ by Proposition 9.2, and on the other hand the convolution $\bar{P}_{1/c}$ inverse to \bar{P}_c interchanges the roles of $\frac{1}{c}$ and c (at σ_∞ respectively τ_∞). \square

For the Katz algorithm we now need one further operation on $\text{Rep}(k[F_s])$, the *multiplication with $\mathbf{c} = (c_1, \dots, c_s) \in (k^\times)^s$* . This is defined by

$$M_{\mathbf{c}} : \text{Rep}(k[F_s]) \rightarrow \text{Rep}(k[F_s]), \quad (\sigma, V) \mapsto (M_{\mathbf{c}}(\sigma), V), \quad (9.12)$$

with $M_{\mathbf{c}}(\sigma) := (c_1\sigma_1, \dots, c_s\sigma_s)$.

Remark. Obviously $M_{\mathbf{c}}$ preserves irreducibility and absolute irreducibility of (σ, V) .

The next result contains the core of the algorithm presented by Katz (1996), Ch. 6.4, for the existence of linearly rigid s -tuples.

Theorem 9.15 (Katz). *Let $k = \bar{k}$ be an algebraically closed field. Then every irreducible linearly rigid s -tuple $(\sigma_1, \dots, \sigma_s) \in \text{GL}_n(\bar{k})^s$ with $\sigma_1 \cdots \sigma_s = \iota_n$ is connected to an s -tuple in $\text{GL}_1(\bar{k}) = \bar{k}^\times$ via iterative application of multiplication and convolution.*

Proof. Let $V = k^n$ and $W = k^{n \times n}$ with $n \geq 2$. By assumption we have $\sigma_\infty = \iota_n$. Further we use the notation

$$n_i := \min\{\text{rk}(c_i\sigma_i - \iota_n) \mid c_i \in k^\times\}.$$

If $\sigma = (\sigma_1, \dots, \sigma_s)$ is linearly rigid then by Theorem 9.11 and (9.11) we have

$$\begin{aligned} sn^2 - 2(n^2 - 1) &= \sum_{i=1}^s \dim_k(\mathcal{C}_W(\sigma_i)) \\ &\leq \sum_{i=1}^s ((n - n_i)^2 + n_i(n - n_i)) = \sum_{i=1}^s n(n - n_i) = sn^2 - n \sum_{i=1}^s n_i, \end{aligned}$$

from which it follows that

$$n \sum_{i=1}^s n_i \leq 2(n^2 - 1) \quad \text{and} \quad \sum_{i=1}^s n_i < 2n.$$

As (σ, V) is irreducible, so is $(M_{\mathbf{c}}(\sigma), V)$, so by Corollary 9.10 the product $c_1 \cdots c_s$ must be different from 1. Hence by Proposition 9.2 the dimension m of the image of the operator $\bar{P}_{1/c} \circ M_{\mathbf{c}}$, for $\mathbf{c} = (c_1, \dots, c_s)$ and $c := c_1 \cdots c_s$, satisfies

$$\begin{aligned} m &= \sum_{i=1}^s \text{rk}(c_i\sigma_i - \iota_n) + \text{rk}\left(\frac{1}{c}c_1\sigma_1 \cdots c_s\sigma_s - \iota_n\right) - n \\ &= \sum_{i=1}^s n_i - n < n. \end{aligned}$$

Since moreover

$$\text{rk}(c\bar{\tau}_\infty - \iota_m) = \text{rk}(\sigma_\infty - \iota_n) = 0$$

we also get $c\bar{\tau}_\infty = \iota_m$ for the next step in the induction. By decreasing dimension this stops after finitely many steps with $n = 1$. \square

Remark. Corollary 9.13, Theorem 9.14 and Theorem 9.15 also hold for not necessarily algebraically closed fields k , as long as these contain all eigenvalues of $\sigma_1, \dots, \sigma_s$ in \bar{k} .

9.5 Braid Compatibility

In the next result we show that convolution commutes with the action of the Artin braid group on the generators γ_i of F_s in Theorem 1.2 and hence also with the action on its images $(\sigma, V) \in \text{Rep}(k[F_s])$ up to isomorphism.

Theorem 9.16. *Let $(\sigma, V) \in \text{Rep}(k[F_s])$ and $\beta \in \tilde{B}_s$ an element of the full Artin braid group. Then for $c \in k^\times$ we have:*

- (a) $P_c(\sigma^\beta, V) \cong (P_c(\sigma)^\beta, V^s)$,
- (b) $\bar{P}_c(\sigma^\beta, V) \cong (\bar{P}_c(\sigma)^\beta, W)$.

Proof. The proof relies on a generalized Burau representation $D : \tilde{B}_s \rightarrow \text{GL}_{ns}(k)$ of the braid group \tilde{B}_s , which is given by

$$D(\beta_i) = \text{diag}(\iota_n, \dots, \iota_n, D_i, \iota_n, \dots, \iota_n) \quad \text{with } D_i = \begin{pmatrix} 0 & \sigma_i \\ 1 & 1 - \sigma_{i+1} \end{pmatrix}$$

on the generators β_i . Indeed, direct calculation shows that

$$P_c(\sigma)^{\beta_i} = D(\beta_i)^{-1} P_c(\sigma^{\beta_i}) D(\beta_i),$$

and thus (a) holds. Part (b) follows from this by observing that $D(\beta_i)X = X$ and $D(\beta_i)Y = Y$. \square

In the case $\gamma_1 \cdots \gamma_s = 1$ by Theorem 1.7 we have moreover an action of the full Hurwitz braid group \tilde{H}_s on the generators of the factor group $G_s = F_s / \langle \gamma_1 \cdots \gamma_s \rangle$ modulo simultaneous conjugation. Obviously this satisfies:

Proposition 9.17. *The Pochhammer transformation P_c and the convolution \bar{P}_c both commute with simultaneous conjugation in $\text{GL}_n(k)$ and in $\text{GL}_{sn}(k)$ respectively $\text{GL}_m(k)$.*

With the proof of Theorem 9.16 one thus sees that in the case $\sigma_\infty = \iota_n$ both P_c and \bar{P}_c commute with the action of the full Hurwitz braid group \tilde{H}_s . From this we conclude:

Corollary 9.18. *Let $\sigma = (\sigma_1, \dots, \sigma_s) \in \text{GL}_n(k)^s$ with $\sigma_1 \cdots \sigma_s = \iota_n$ and $\beta \in \tilde{H}_s$ an element of the full Hurwitz braid group. Then in $\text{GL}_{sn}(k)$ respectively $\text{GL}_m(k)$ we have, modulo simultaneous conjugation:*

$$[P_c(\sigma^\beta)] = [P_c(\sigma)^\beta] \quad \text{respectively} \quad [\bar{P}_c(\sigma^\beta)] = [\bar{P}_c(\sigma)^\beta].$$

Thus convolution \bar{P}_c sends braid orbits of s -tuple classes $[\sigma]$ in $\mathrm{GL}_n(k)$ to such in $\mathrm{GL}_m(k)$. If $G \leq \mathrm{GL}_n(k)$ is a subgroup, then under suitable additional stability hypotheses this will also send braid orbits of classes of generating systems in $\Sigma_s(G)/\mathrm{Inn}(G)$ (see Proposition 5.1) to corresponding braid orbits of subgroups of $\mathrm{GL}_m(k)$. We will see stringent applications for this in Sections 10.3 and 10.4.

To close this section we formulate two further properties of the convolution \bar{P}_c in the form of exercises, since they will not be needed here.

Exercise 9.19. Let $(\sigma, V) \in \mathrm{Rep}(k[F_s])$ with $\sigma \in \mathrm{GL}_n(k)^s$, and $c \in k^\times$.

(a) The dual representation (σ^*, V^*) of (σ, V) satisfies

$$\bar{P}_c(\sigma^*, V^*) \cong \bar{P}_c(\sigma, V)^*.$$

(b) The representation (σ^{-1}, V) with the inverse group action satisfies

$$\bar{P}_c(\sigma^{-1}, V) \cong (\bar{P}_{1/c}(\sigma^{-1}), V).$$

(See Dettweiler and Reiter (2000), Thms. 5.4 and 5.5.)

10 Applications of the Katz Algorithm

In this paragraph we present several applications of Katz's algorithm. In particular we will find very general G-realizations over \mathbb{Q} for many classical groups over \mathbb{F}_q even for higher prime powers q . The results presented here originate mainly in the papers of Dettweiler and Reiter (1999, 2000), and partly also go back to Völklein (1993, 1998) and Thompson and Völklein (1998) but who did not use the Katz algorithm.

10.1 Jordan–Pochhammer Tuples

The simplest non-trivial linearly rigid s -tuples in $\mathrm{GL}_n(k)$ are the classical Jordan–Pochhammer tuples. They are obtained for $n \geq 3$ by a single application of the convolution to an n -tuple $\mathbf{a} = (a_1, \dots, a_n)$ in $\mathrm{GL}_1(k) \cong k^\times$. As here we are interested in finite groups we will use the base field $k = \mathbb{F}_q$ for a prime power q . We choose $1 \neq a_i \in k^\times$ for $i = 1, \dots, n$ and set $a_\infty := \prod_{i=1}^n a_i$, so that $a_1 \cdots a_n a_\infty^{-1} = 1$. Let $c \in k^\times$. Then

$$\sigma = (\sigma_1, \dots, \sigma_n) := P_c(a_1, \dots, a_n) \in \mathrm{GL}_n(k)^n \quad (10.1)$$

together with $\sigma_\infty = \sigma_1 \cdots \sigma_n$ and $\sigma_0 = \sigma_\infty^{-1}$ is called a (*normalized*) *Jordan–Pochhammer tuple*, or *JP-tuple* for short. For $c \notin \{1, a_0\}$ we call σ an *irreducible Jordan–Pochhammer tuple*. (In Völklein (1998) this is also called a *Thompson tuple*.)

Remark. (a) The elements $\sigma_1, \dots, \sigma_n$ are pseudo-reflections with characteristic polynomial $f_i(X) = (X - 1)^{n-1}(X - ca_i)$ for $i = 1, \dots, n$. The product σ_∞ is a c -fold pseudo-reflection with characteristic polynomial $f_\infty(X) = (X - c)^{n-1}(X - ca_\infty)$.

(b) For $1 \leq i \leq n$, in the case $ca_i \neq 1, -1$ the element σ_i is a non-involutory homology, in the case $ca_i = 1$ it is a transvection, and in the case $ca_i = -1$ a reflection.

Up to the form of $f_\infty(X)$ these claims follow immediately from the definition in (10.1), for $f_\infty(X)$ one can use in addition Corollary 9.13(b).

Proposition 10.1. *Let $(\sigma_1, \dots, \sigma_n) = P_c(a_1, \dots, a_n) \in \mathrm{GL}_n(k)^n$, $n \geq 2$, be an irreducible Jordan–Pochhammer tuple and $G := \langle \sigma_1, \dots, \sigma_n \rangle$ the subgroup generated by it. Then:*

- (a) *G is irreducible and $\sigma = (\sigma_0, \dots, \sigma_n)$ is linearly rigid.*
- (b) *In the case $n > 3$ the group G is moreover primitive.*

Proof. Clearly $(a_0, \dots, a_n) \in \mathrm{GL}_1(k)^{n+1}$ with $a_0 = a_\infty^{-1}$ is linearly rigid, and the subgroup $\langle a_1, \dots, a_n \rangle \leq \mathrm{GL}_1(k)$ is absolutely irreducible. By Proposition 9.2 we have $P_c = \tilde{P}_c$ as $c \notin \{1, a_0\}$. Since $n \geq 2$ hypothesis (H) holds by Proposition 9.4(b). Thus $\sigma = (\sigma_0, \dots, \sigma_n)$ is linearly rigid by Theorem 9.14 and (σ, V) is irreducible by Corollary 9.7 where $V = k^n$.

For the proof of (b) we assume that $V = \bigoplus_{i=1}^m V_i$ is a direct sum of subspaces V_i of dimension l that are transitively permuted by G . In the case $l > 1$ we then have $V_1 \cap \ker(\sigma_i - \iota_n) \neq 0$ for all i , from which we get $\sigma_i(V_1) \leq V_1$ and by the irreducibility of G then $m = 1$. In case $l = 1$ we have $m = n$ and the action of G on the set of V_i 's induces a permutation representation $\pi_n : G \rightarrow S_n$. If the image $\pi_n(\sigma_i)$ is non-trivial for some generator σ_i , then after renumbering we may assume that $\sigma_i(V_1) = V_2$, say. But as $V_1 \oplus \ker(\sigma_i - \iota_n) = V = V_2 \oplus \ker(\sigma_i - \iota_n)$ there exist subspaces $W_i \leq \ker(\sigma_i - \iota_n)$ with $V_1 \oplus V_2 = V_1 \oplus W_1 = V_2 \oplus W_2$. Then

$$\sigma_i(V_1 \oplus V_2) \leq \sigma_i(V_1) + \sigma_i(W_1) = V_2 + W_1 \leq V_1 \oplus V_2$$

shows the σ_i -invariance of $V_1 \oplus V_2$. Thus $\sigma_i(V_1) = V_2$, $\sigma_i(V_2) = V_1$ and $\sigma_i(V_j) = V_j$ for $j \geq 3$. In particular $\pi_n(\sigma_i) = (1\ 2)$ is a transposition. The same holds for σ_∞ using $\ker(c\sigma_\infty - \iota_n)$. So $\pi_n(G) \leq S_n$ is a transitive group generated by $n+1$ transpositions with product the identity. In the case $n > 3$ this contradicts the Hurwitz relative genus formula (see Section I.5.2). So G is primitive. \square

The next result of Völklein (1998) classifies the finite groups generated by irreducible JP-tuples for $n > 8$.

Theorem 10.2. *Let $(\sigma_1, \dots, \sigma_n) = P_c(a_1, \dots, a_n)$ be an irreducible JP-tuple over $\mathbb{F}_q = \mathbb{F}_p(a_1, \dots, a_n, c)$ and $G = \langle \sigma_1, \dots, \sigma_n \rangle \leq \mathrm{GL}_n(q)$. Then for $n > 8$ we have:*

(a) *G leaves invariant a non-trivial bilinear form on (σ, \mathbb{F}_q^n) if and only if $q = p$ is an odd prime, $n = 2m$ is even and $a_1 = \dots = a_n = c = -1$. In this case $G \cong \mathrm{Sp}_{2m}(p)$.*

(b) *G leaves invariant a non-trivial Hermitian form on (σ, \mathbb{F}_q^n) if and only if $q = \tilde{q}^2$ is a square and the norms satisfy $\mathcal{N}_{\mathbb{F}_q/\mathbb{F}_{\tilde{q}}}(a_i) = \mathcal{N}_{\mathbb{F}_q/\mathbb{F}_{\tilde{q}}}(c) = 1$ for $1 \leq i \leq n$. In this case $\mathrm{SU}_n(\tilde{q}) \leq G \leq \mathrm{GU}_n(\tilde{q})$.*

(c) *If we are neither in case (a) nor (b) then $\mathrm{SL}_n(q) \leq G \leq \mathrm{GL}_n(q)$.*

Proof. We start with two general remarks: an automorphism $\alpha : a \mapsto \bar{a}$ of $k = \mathbb{F}_q$ of order 1 or 2 can be extended to an automorphism of $\mathrm{GL}_n(k)$ via

$$\alpha^* : \sigma \mapsto \sigma^* := (\bar{\sigma}^{-1})^t. \quad (10.2)$$

It transforms a JP-tuple $\sigma = (\sigma_1, \dots, \sigma_n) := P_c(a_1, \dots, a_n)$ to another JP-tuple $\alpha^*(\sigma) = (\sigma_1^*, \dots, \sigma_n^*) = P_{\bar{c}-1}(\bar{a}_1^{-1}, \dots, \bar{a}_n^{-1})$ with $\sigma_\infty^* = (\sigma_\infty)^*$. Note that any non-trivial G -invariant bilinear form on (σ, V) , with $V = \mathbb{F}_q^n$, is non-degenerate due to the irreducibility of (σ, V) .

Now assume that (σ, V) carries a non-degenerate bilinear form. Then from the form of $\sigma_1, \dots, \sigma_n$ we obtain on the one hand that $ca_i = \pm 1$, and from the form of σ_∞ also $c = \pm 1$. Since $c \neq 1$ this shows that $c = -1$ and $a_i = -1$. So $\sigma_1, \dots, \sigma_n$ are transvections in $\mathrm{GL}_n(p)$ with $p \neq 2$. As $\det(\sigma_i) = 1$ we also have $\det(\sigma_\infty) = 1$ and hence $n = 2m$ is even. By the Theorem II.2.2 of Kantor this forces that $G = \mathrm{Sp}_{2m}(p)$, showing (a).

Now assume that (σ, V) carries a non-degenerate Hermitian form. Then $q = \tilde{q}^2$ is a square and G is a subgroup of $\mathrm{GU}_n(\tilde{q})$. By Huppert (1967), II, §10.5, the latter

is equivalent to $\sigma_i^* = \sigma_i$ for $i = 1, \dots, n$ (up to simultaneous conjugation in $\mathrm{GL}_n(q)$). As above this implies that $\bar{c}\bar{a}_i = (ca_i)^{-1}$ as well as $\bar{c} = c^{-1}$ and so $\bar{a}_i = a_i^{-1}$. This leads to the necessary and sufficient condition $\mathcal{N}_{\mathbb{F}_q/\mathbb{F}_{\tilde{q}}}(a_i) = 1$ for $i = 1, \dots, n$ and $\mathcal{N}_{\mathbb{F}_q/\mathbb{F}_{\tilde{q}}}(c) = 1$, which shows the first part of (b).

For the last step we assume that (σ, V) has no non-trivial invariant bilinear form, but possibly an invariant Hermitian form. If $\sigma_1, \dots, \sigma_n$ are reflections, which can only happen when $p \neq 2$, then $ca_i = -1$ for $i = 1, \dots, n$. Then the Theorem II.2.4 of Wagner shows that for $n > 8$ we either have $\mathrm{SU}_n(\tilde{q}) \leq G \leq \mathrm{GU}_n(\tilde{q})$ or $\mathrm{SL}_n(q) \leq G \leq \mathrm{GL}_n(q)$. Indeed, the remaining case (d) in the cited result can not occur here, as S_{n+1} and S_{n+2} cannot be generated by $n+1$ transpositions with product 1 (compare Proposition II.2.8).

If not all of the σ_i are reflections then there is either a transvection or a non-involutory homology among the σ_i . Now let N denote the normal subgroup of G generated by the conjugates in G of this element. Then (N, V) is irreducible, as G is primitive, hence also primitive according to the proof of Proposition 10.1(b). So assertions (b) and (c) hold for N in place of G . In the case of a non-involutory homology this follows from the Theorem II.2.3 of Wagner, and in the case of a transvection from the Theorem II.2.2 of Kantor, where in characteristic 2 the groups S_{n+1} and S_{n+2} can be excluded as above. As $N \trianglelefteq G$ we finally deduce (b) and (c) also for G (using the characterization of unitary groups as the fixed points under α^*). \square

Since there are no irreducible JP-tuples over $k = \mathbb{F}_2$, the theorems of Kantor and Wagner allow us to give the following more precise result:

Remark. (a) If G is not generated by reflections then Theorem 10.2 holds when $n \geq 4$.

(b) If G is generated by non-involutory homologies, then the assertion of Theorem 10.2 even holds for $n \geq 3$.

We reformulate the special case (a) in Theorem 10.2 as an existence result (compare also Prop. III.10.5 in the first edition Malle and Matzat (1999)):

Corollary 10.3. *For odd primes $p \in \mathbb{P}$ and $m \geq 2$ the groups $S_{2m}(p)$ possess G -realizations over $\mathbb{Q}(\sqrt{p^*})$, with $p^* = (-1)^{\frac{p-1}{2}} p$, with respect to suitable rigid generating systems.*

Proof. By the proof of Theorem 10.2(a) the elements $\sigma_1, \dots, \sigma_n$ are transvections generating $\mathrm{Sp}_{2m}(p)$. Moreover $\sigma = (\sigma_0, \dots, \sigma_n)$ is linearly rigid, where $-\sigma_0$ is also a transvection according to the part (b) of the Remark preceding Proposition 10.1.

It is well known that $\mathrm{Sp}_{2m}(p)$ contains two classes of transvections with character field $\mathbb{Q}(\sqrt{p^*})$. Both of them are GL-stable and are interchanged by $\mathrm{CSp}_{2m}(p)$. Consequently σ is rigid by Proposition 9.8 and thus with the Basic Rigidity Theorem I.4.8 leads to a G -realization of $S_{2m}(p) = \mathrm{Sp}_{2m}(p)/\mathcal{Z}(\mathrm{Sp}_{2m}(p))$ over $\mathbb{Q}(\sqrt{p^*})$. \square

This result will be extended considerably to certain prime powers in Theorem 10.9.

Remark. The Classification Theorem 10.2 for irreducible JP-tuples with its applications also holds with $m = n - 1$ in place of n for the reducible case $1 \neq c = a_0$, since then $W = \mathbb{F}_q^n / Y$ with $Y = \bigcap_{i=1}^n \ker(\sigma_i - \iota_n)$ is irreducible in dimension $n - 1$.

10.2 Linear and Unitary Groups

In this section we start from modified Jordan–Pochhammer tuples to construct G-realizations over \mathbb{Q} for linear and unitary groups. These results were first obtained by Völklein (1993) and Dettweiler and Reiter (1999) but with different proofs.

Theorem 10.4. *Let $p \in \mathbb{P}$ be an odd prime, $q = p^e \neq 3$ and $n > \varphi(q - 1)$. Then $\mathrm{GL}_n(q)$ and $\mathrm{PGL}_n(q)$ possess G-realizations over \mathbb{Q} .*

Proof. We start with the case that $n = 2m$ is even. Then from $n = 2m > \varphi(q - 1) = 2l$ with $l \geq 1$ we first get $m \geq 2$ and thus $n \geq 4$. Now let $a \in \mathbb{F}_q$ be a generator of \mathbb{F}_q^\times and $a_1 = a, \dots, a_{2l}$ the primitive powers of a . We let $\mathbf{a} = (a_1, \dots, a_{2l}, -1, \dots, -1) \in \mathbb{F}_q^{2m+1}$. Then $a_1 \cdots a_{2l} = 1$ and $a_\infty = -1$. With Proposition 9.2 the convolution \tilde{P}_{-1} yields

$$\tilde{P}_{-1}(a_1, \dots, a_{2m+1}) = (\sigma_1, \dots, \sigma_{2m+1}) \in \mathrm{GL}_{2m}(q)^{2m+1}$$

with $\sigma_\infty = -\iota_{2m}$. According to Corollary 9.13 the $\sigma_1, \dots, \sigma_{2l}$ are homologies with non-trivial eigenvalues $-a_1, \dots, -a_{2l}$ respectively, and $\sigma_{2l+1}, \dots, \sigma_{2m+1}$ are transvections. Furthermore, the group $G = \langle \sigma_1, \dots, \sigma_{2m+1} \rangle$ is irreducible by Corollary 9.7 and Theorem 9.14, and $\sigma = (\sigma_0, \dots, \sigma_{2m+1})$ with $\sigma_0 = \sigma_\infty^{-1} = -\iota_{2m}$ is linearly rigid. From Theorem 10.2(c) with the subsequent Remarks concerning homologies and the case $c = a_0$ we thus obtain that $G = \mathrm{GL}_n(q)$ since $\det(\sigma_1) = a$ generates \mathbb{F}_q^\times . The trivially satisfied stability condition in Proposition 9.8(b) implies the rigidity of σ . The conjugacy classes C_i of σ_i for $i = 1, \dots, 2l$ are permuted by the cyclotomic character according to Corollary I.2.7, while those for $i = 2l + 1, \dots, 2m + 1$ are rational. Let $V \leq S_{2l}$ denote the corresponding permutation group, then $\Sigma_V(C_0, \dots, C_{2m+1})$ is V -symmetric. Consequently by Theorem 3.11 the field of definition K_σ^V of \bar{N}_σ from Theorem 3.4 (Hurwitz classification) is regular over \mathbb{Q} and rational. Thus we have $K_\sigma^V = \mathbb{Q}(\mathbf{v}, t)$ in the notation of Theorem 3.11. So first $\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/\mathcal{L}(\mathrm{GL}_n(q))$ has a G-realization over \mathbb{Q} . Now by Theorem II.1.4 the center $\mathcal{Z}(\mathrm{GL}_n(q))$ has a complement in $\mathcal{N}_{\mathrm{GL}_n(q)}(\langle \sigma_{2m+1} \rangle)$. This yields the normalizer condition (N) for the Galois extension $\bar{N}_\sigma \mathbb{Q}(\mathbf{v})/\overline{\mathbb{Q}(\mathbf{v})}(t)$ of algebraic function fields in one variable over $\mathbb{Q}(\mathbf{v})$ with the Galois group $\mathrm{GL}_n(q)$ and the field of definition $K_\sigma^V = \mathbb{Q}(\mathbf{v}, t)$. Thus by Theorem I.3.9 also $\mathrm{GL}_n(q)$ has a G-realization over \mathbb{Q} .

Now we consider the case when $n = 4m + 1$. Here we extend the $2m + 1$ -tuple $(\sigma_1, \dots, \sigma_{2m+1}) \in \mathrm{GL}_{2m}(q)^{2m+1}$ introduced in the first part to $(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3})$ via $\tilde{\sigma}_{2m+2} = \tilde{\sigma}_{2m+3} := -\iota_{2m}$. Then we again have $\tilde{\sigma}_0 = \tilde{\sigma}_\infty = -\iota_{2m}$, and

$(\tilde{\sigma}_0, \dots, \tilde{\sigma}_{2m+3})$ is linearly rigid. From Proposition 9.2 we get with the convolution \bar{P}_{-1}

$$\bar{P}_{-1}(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3}) = (\tau_1, \dots, \tau_{2m+3}) \in \mathrm{GL}_{4m+1}(q)^{2m+3}$$

with $\tau_\infty = -\iota_{4m+1} = \tau_0$. Here according to Corollary 9.13 the elements τ_1, \dots, τ_{2l} are non-involutory homologies with non-trivial eigenvalues a_1, \dots, a_{2l} respectively, the elements $\tau_{2l+1}, \dots, \tau_{2m+1}$ are reflections, and the Jordan normal forms of τ_{2m+2} and τ_{2m+3} consist of $2m$ Jordan blocks of length 2 and one of length 1, all with eigenvalue 1. By Theorem 9.14 $\tau = (\tau_0, \dots, \tau_{2m+3})$ is linearly rigid and $H := \langle \tau \rangle$ is irreducible by Corollary 9.7, hence also primitive by the proof of Proposition 10.1(b). Now let $N \trianglelefteq H$ be the normal subgroup generated by the non-involutory homologies. Then N is itself primitive and does not leave invariant any non-trivial Hermitian form. So $N = \mathrm{GL}_n(q)$, with $n = 4m + 1$, by the Theorem II.2.3 of Wagner, using that $\det(\tau_1) = a$ generates \mathbb{F}_q^\times . Thus we also have $H = \mathrm{GL}_n(q)$. Since both the stabilizer condition (S) (by Proposition 9.8) and the normalizer condition (N) for τ_{2m+1} (by Theorem II.1.4) are satisfied, a symmetrization as above yields G-realizations of $\mathrm{PGL}_n(q)$ and $\mathrm{GL}_n(q)$ over \mathbb{Q} for $n = 4m + 1$.

It remains to consider the case $n = 4m + 3$ with $n \geq 7$. Here we start with $(a_1, \dots, a_{2l}, -1, \dots, -1) \in \mathbb{F}_q^{2m+3}$, where a_1, \dots, a_{2l} are chosen as in the first case, whence $a_\infty = -1$. The convolution \bar{P}_{-1} now leads to

$$\bar{P}_{-1}(a_1, \dots, a_{2m+1}) = (\sigma_1, \dots, \sigma_{2m+3}) \in \mathrm{GL}_{2m+2}(q)^{2m+3}$$

with $\sigma_\infty = -\iota_{2m+3} = \sigma_0$. Again, $\sigma_1, \dots, \sigma_{2l}$ are non-involutory homologies, while $\sigma_{2l+1}, \dots, \sigma_{2m+3}$ are now transvections. Here we set $\tilde{\sigma}_{2m+2} = -\sigma_{2m+2}$, $\tilde{\sigma}_{2m+3} = -\sigma_{2m+3}$ and replace $(\sigma_1, \dots, \sigma_{2m+3})$ by $(\sigma_1, \dots, \sigma_{2m+1}, \tilde{\sigma}_{2m+2}, \tilde{\sigma}_{2m+3})$. Then again $\tilde{\sigma}_\infty = -\iota_{2m+2}$. Now according to Proposition 9.2 application of \bar{P}_{-1} yields

$$\bar{P}_{-1}(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3}) = (\tau_1, \dots, \tau_{2m+3}) \in \mathrm{GL}_{4m+3}(q)^{2m+3}$$

with $\tau_\infty = -\iota_{4m+3}$. Here, as above, τ_1, \dots, τ_{2l} are non-involutory homologies and $\tau_{2l+1}, \dots, \tau_{2m+1}$ are reflections. With the arguments from the previous two cases one obtains again that the group $H = \langle \tau_1, \dots, \tau_{2m+3} \rangle$ is the whole group $\mathrm{GL}_{4m+3}(q)$ and that $\tau = (\tau_0, \dots, \tau_{2m+3})$ is linearly rigid as well as rigid. From this, the existence proof for G-realizations of $\mathrm{PGL}_{4m+3}(q)$ and $\mathrm{GL}_{4m+3}(q)$ can be completed as above using symmetrization. \square

Remark. For odd n Theorem 10.4 continues to hold for $q = 3$ with $l = 0$; for even n and $l = 0$ the above construction leads to the group $\mathrm{SL}_n(3)$ instead of $\mathrm{GL}_n(3)$.

Theorem 10.5. *Let $p \in \mathbb{P}$ be odd, $q = p^e$ and $n > \varphi(q+1)$. Then $\mathrm{GU}_n(q)$ and $\mathrm{PGU}_n(q)$ possess G-realizations over \mathbb{Q} .*

Proof. As in the proof of Theorem 10.4 we start with the case that $n = 2m$ is even, with $n > \varphi(q+1) = 2l$, where $l \geq 1$ and thus $n \geq 4$. Now let $a \in \mathbb{F}_{q^2}^\times$ be a generator of the cyclic subgroup of order $q+1$, and $a_1 = a, \dots, a_{2l}$ its primitive powers. Then $\mathcal{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a_i) = \mathcal{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(-1) = 1$ for all i . Application of \bar{P}_{-1} to

$(a_1, \dots, a_{2l}, -1, \dots, -1) \in \mathbb{F}_{q^2}^{2m+1}$ with $a_\infty = -1$ then yields

$$\bar{P}_{-1}(a_1, \dots, a_{2m+1}) = (\sigma_1, \dots, \sigma_{2m+1}) \in \mathrm{GL}_{2m}(q^2)^{2m+1}$$

with homologies $\sigma_1, \dots, \sigma_{2l}$, transvections $\sigma_{2l+1}, \dots, \sigma_{2m+1}$, and $\sigma_\infty = -\iota_{2m}$. By the Theorem of Katz the tuple $\sigma = (\sigma_0, \dots, \sigma_{2m+1})$ is linearly rigid and generates an irreducible subgroup G of $\mathrm{GL}_{2m}(q^2)$. By Theorem 10.2(b) in the case $c = a_0$ we thus have $G = \mathrm{GU}_{2m}(q)$. The stability condition $\mathcal{N}_{\mathrm{GL}_n(q^2)}(G) = \mathcal{Z}(\mathrm{GL}_n(q^2)) \cdot G$ in Proposition 9.8(b) is satisfied according to the proof of Theorem II.3.2. Thus $\sigma = (\sigma_0, \dots, \sigma_{2m+1})$ is rigid in G . The cyclotomic character permutes the conjugacy classes $C_i = [\sigma_i]$ for $i = 1, \dots, 2l$, and fixes $C_0, C_{2l+1}, \dots, C_{2m+1}$. So $\Sigma_V(C_0, \dots, C_{2m+1})$ becomes V -symmetric for the corresponding permutation group $V \leq S_{2l}$, whence the field of definition K_σ^V of \bar{N}_σ is regular over \mathbb{Q} and rational, say $K_\sigma^V = \mathbb{Q}(\mathbf{v}, t)$. Consequently $\mathrm{PGU}_{2m}(q) = G/\mathcal{Z}(G)$ possesses a G -realization over \mathbb{Q} . According to the proof of Theorem II.3.2 we have $\mathcal{N}_G(\langle \sigma_{2m+1} \rangle) = \mathcal{Z}(G)\langle \sigma_{2m+1} \rangle$ and hence the normalizer condition (N) for $\bar{N}_\sigma \mathbb{Q}(\mathbf{v})/\mathbb{Q}(\mathbf{v})(t)$. So $\mathrm{GU}_{2m}(q)$ also has a G -realization over \mathbb{Q} (compare the proof of Theorem 10.4).

Now let $n = 4m + 1$ and thus $n \geq 5$. In analogy to what we did in the proof of Theorem 10.4 we extend $(\sigma_1, \dots, \sigma_{2m+1})$ from the first case to $(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3})$ with $\tilde{\sigma}_{2m+2} = \tilde{\sigma}_{2m+3} = -\iota_{2m}$ and thus $\tilde{\sigma}_\infty = -\iota_{2m}$ (and $\tilde{\sigma}_i = \sigma_i$ else). Application of \bar{P}_{-1} yields

$$\bar{P}_{-1}(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3}) = (\tau_1, \dots, \tau_{2m+3}) \in \mathrm{GL}_{4m+1}(q^2)^{2m+3}$$

with homologies τ_1, \dots, τ_{2l} with non-trivial eigenvalues a_1, \dots, a_{2l} respectively, reflections $\tau_{2l+1}, \dots, \tau_{2m+1}$, and unipotent elements τ_{2m+2}, τ_{2m+3} with Jordan normal form containing one block of size 1 and all others of size two, as in the corresponding case of Theorem 10.4. Here $\tau_\infty = -\iota_{4m+1} = \tau_0$. Then $\tau = (\tau_0, \dots, \tau_{2m+3})$ is linearly rigid and $H := \langle \tau \rangle$ is an irreducible subgroup of $\mathrm{GL}_{4m+1}(q^2)$. As $\tau_i^* = \tau_i$ for all i by the choice of the a_i and of c , H leaves invariant a Hermitian form, and since a generates \mathbb{F}_{q^2} over \mathbb{F}_p , we have $H = \mathrm{GU}_{4m+1}(q)$. As above τ is rigid in H since it moreover satisfies the stability condition. So we can complete the proof as in the first case to obtain G -realizations over \mathbb{Q} for $\mathrm{PGU}_{4m+1}(q)$ and $\mathrm{GU}_{4m+1}(q)$.

In the last case $n = 4m + 3$ we have $n \geq 7$. Here we start with the tuple $(a_1, \dots, a_{2l}, -1, \dots, -1) \in \mathbb{F}_{q^2}^{2m+3}$ with a_i as in the first case and $a_\infty = -1$. From this we obtain

$$\bar{P}_{-1}(a_1, \dots, a_{2m+3}) = (\sigma_1, \dots, \sigma_{2m+3}) \in \mathrm{GL}_{2m+2}(q^2)^{2m+3}$$

with $\sigma_\infty = -\iota_{2m+2}$. As in the corresponding part of the proof of Theorem 10.4 we modify the σ_i to $(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3})$ with $\tilde{\sigma}_{2m+2} = -\sigma_{2m+2}$, $\tilde{\sigma}_{2m+3} = -\sigma_{2m+3}$ and $\tilde{\sigma}_i = \sigma_i$ else. A second application of \bar{P}_{-1} then yields

$$\bar{P}_{-1}(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{2m+3}) = (\tau_1, \dots, \tau_{2m+3}) \in \mathrm{GL}_{4m+3}(q^2)^{2m+3}$$

with $\tau_\infty = -\iota_{4m+3} = \tau_0$. As above we may conclude that $\boldsymbol{\tau} = (\tau_0, \dots, \tau_{2m+3})$ is linearly rigid and generates $H = \mathrm{GU}_{4m+3}(q^2)$. The stability condition already verified above then yields the rigidity of $\boldsymbol{\tau}$ in H . From here on the remaining assertions for $n = 4m + 3$ can be deduced as in the previous two cases. \square

10.3 Symplectic Groups

In this section we present examples of G-realizations over \mathbb{Q} from braid rigid generating systems which are not rigid. Here the braid compatibility of the convolution plays a crucial role. The results presented here essentially go back to Thompson and Völklein (1998) and Dettweiler and Reiter (2000). We start with some technical preparations.

Proposition 10.6. *Let $Q \in k^{n \times n}$ be a matrix and $\sigma_h \in \mathrm{GL}_n(k)$ be such that $\sigma_h^t Q \sigma_h = Q$ for $h = 1, \dots, s$. Then for all $c \in k^\times$ we have*

$$P_{c-1}(\sigma_h)^t \mathbf{Q} P_c(\sigma_h) = \mathbf{Q} \quad \text{for } \mathbf{Q} = (Q_{ij})_{i,j=1}^s \in k^{sn \times sn}$$

with

$$Q_{ij} = \begin{cases} c^{-1/2} Q(\sigma_i^{-1} - \iota_n)(\sigma_j - \iota_n) & i < j \\ c^{-1/2} Q(\sigma_i^{-1} - c\iota_n)(\sigma_j - \iota_n) & \text{for } i = j \\ c^{1/2} Q(\sigma_i^{-1} - \iota_n)(\sigma_j - \iota_n) & i > j. \end{cases}$$

Proof. The stated formulas are easily verified by solving the associated linear system of equations. \square

Corollary 10.7. *If in Proposition 10.6 we additionally have that $Q^t = \mp Q$ and $c = -1$, then*

$$\mathbf{Q}^t = \pm \mathbf{Q} \quad \text{for } \mathbf{Q} = (Q_{ij}).$$

So if $\langle \sigma_1, \dots, \sigma_s \rangle$ is an orthogonal (respectively symplectic) group, then $P_{-1}(\sigma)$ and $\bar{P}_{-1}(\sigma)$ generate subgroups of a symplectic (respectively orthogonal) group.

Proof. In the special case $c = -1$ with $Q^t = \mp Q$ Proposition 10.6 first yields $Q_{ij}^t = \pm Q_{ij}$ and from this

$$\mathbf{Q}^t = (Q_{ij})^t = \pm(Q_{ij}) = \pm\mathbf{Q}. \quad \square$$

Proposition 10.8. *Let $G = D_{2m} < \mathrm{GL}_2(\mathbb{C})$ be a dihedral group of order $4m$ in its natural reflection representation, $\mathbf{C} = (C_1, \dots, C_s)$ a class vector of G with classes C_1, C_2 of reflections, C_3, \dots, C_{l+3} of non-involutory bihomologies and C_{l+4}, \dots, C_s the class of the central involution $-\iota_2$, satisfying $\Sigma(\mathbf{C}) \neq \emptyset$. Then we have:*

(a) $|\Sigma(\mathbf{C})/\mathrm{Inn}(G)| = 2^l$.

(b) *The pure Hurwitz braid group H_s acts sharply transitively on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ with $\mathrm{im}(H_s) \cong Z_2^l$. This is generated by the images $\bar{\beta}_{24}, \dots, \bar{\beta}_{2,l+3}$ of $\beta_{ij} \in H_s$.*

(c) The fixed field \bar{L}_s in $\bar{M}_s/\bar{\mathbb{Q}}(t_1, \dots, t_s)$ of the kernel of the above action is generated by

$$u_j \quad \text{for } j = 4, \dots, l+3 \quad \text{with} \quad u_j^2 = \frac{t_j - t_1}{t_j - t_2} : \frac{t_3 - t_1}{t_3 - t_2}.$$

In particular $\bar{L}_s/\bar{\mathbb{Q}}$ is a rational function field.

Proof. The group $G = D_{2m}$ is the semidirect product $G = T \rtimes Z_2$ of a diagonal torus T of order $2m$ containing elements of the form $\text{diag}(a, a^{-1})$ by a cyclic group Z_2 generated by a reflection ρ , say $\rho = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. If now there exists some $(\sigma_1, \dots, \sigma_s) \in \Sigma(\mathbf{C})$ then due to $\sigma_1 \cdots \sigma_s = \iota_2$ all of $\sigma_1 \sigma_2, \sigma_3, \dots, \sigma_s$ lie in T and $\sigma_1 \sigma_2$ is a square in G if $\sigma_3 \cdots \sigma_s$ is a square in T . So the latter is a necessary and sufficient condition for $\Sigma(\mathbf{C}) \neq \emptyset$.

The conjugacy classes of a non-involutory bihomology $\sigma = \text{diag}(a, a^{-1})$ consists of σ and its inverse. So for the computation of $|\Sigma(\mathbf{C})/\text{Inn}(G)|$ we may arrange by conjugation that $\sigma_1 = \rho$ and $\sigma_3 \in C_3$. Then $\sigma_2 = \sigma_1^{-1} \sigma_3 \cdots \sigma_s$ is a reflection, and we have exactly two choices for $\sigma_i \in C_i$ for each $4 \leq i \leq l+3$. This yields 2^l possibilities, giving $|\Sigma(\mathbf{C})/\text{Inn}(G)| = 2^l$ as claimed.

The action of H_s on $\Sigma(\mathbf{C})/\text{Inn}(G)$ is obtained from Proposition 5.1. Let's first observe that $\beta_{12} = \beta_1^2$ acts on all σ_i by conjugation from the left with $\sigma_1 \sigma_2 \in T$, i.e., β_{12} acts trivially on $\Sigma(\mathbf{C})/\text{Inn}(G)$, so that $\bar{\beta}_{12} = \text{id}$. Since T is abelian, the braids β_{ij} for $3 \leq i < j \leq s$ fix all classes of generating systems $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$, whence $\bar{\beta}_{ij} = \text{id}$ for these i, j as well. The braids β_{ij} for $i = 1, 2$ and $3 \leq j \leq s$ all act on σ_j by conjugation with σ_i . So the action is transitive and we have $\bar{\beta}_{1j} = \bar{\beta}_{2j}$ as well as $\bar{\beta}_{2j}^2 = \text{id}$ for $j \leq l+3$ and $\bar{\beta}_{ij} = \text{id}$ else. Finally, the sphere relation $\bar{\beta}_{12} \bar{\beta}_{23} \bar{\beta}_{24} \cdots \bar{\beta}_{2,l+3} = \text{id}$ from Section 1.2 yields the product relation $\bar{\beta}_{23} \bar{\beta}_{24} \cdots \bar{\beta}_{2,l+3} = \text{id}$. So the image H_s acts by

$$\bar{H}_s = \langle \bar{\beta}_{23}, \dots, \bar{\beta}_{2,l+3} \mid \bar{\beta}_{2j}^2 = \text{id}, \bar{\beta}_{23} \cdots \bar{\beta}_{2,l+3} = \text{id} \rangle^{\text{ab}} \cong (\mathbb{Z}/2\mathbb{Z})^l,$$

since all generators $\bar{\beta}_{2j}$ commute.

For the proof of (c) we may assume that $s = l+3$. Then $\bar{H}_s = 1$ for $s = 3$ and $\bar{L} = \bar{\mathbb{Q}}(t_1, t_2, t_3)$. For $s = 4$ the sphere relation gives that

$$\bar{H}_4 = \langle \bar{\beta}_{14}, \bar{\beta}_{24} \mid \bar{\beta}_{14}^2 = \text{id}, \bar{\beta}_{14} \bar{\beta}_{24} = \text{id} \rangle^{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z},$$

that is, $\bar{L}_4/\bar{L}_3(t_4)$ has degree 2 and ramifies in $c \frac{t_4 - t_1}{t_4 - t_2}$ with $c \in \bar{L}_3$. From the sphere relations we further deduce that $\bar{\beta}_{13} = \bar{\beta}_{23} = \bar{\beta}_{24} \neq \text{id}$ with $\bar{\beta}_{13} \bar{\beta}_{23} = \text{id}$. So by symmetry $\bar{L}_4/\bar{\mathbb{Q}}(t_1, \dots, t_4)$ also ramifies in $\frac{t_3 - t_1}{t_3 - t_2}$. This shows that

$$\bar{L}_4 = \bar{L}_3(t_4, u_4) \quad \text{with} \quad u_4^2 = \frac{t_4 - t_1}{t_4 - t_2} : \frac{t_3 - t_1}{t_3 - t_2}$$

after a normalization according to the sphere relation $\bar{\beta}_{23}\bar{\beta}_{24} = \text{id}$. Since we have $t_4 \in \bar{\mathbb{Q}}(t_1, t_2, t_3, u_4)$ the extension $\bar{L}_4/\bar{\mathbb{Q}}$ is moreover rational. The claim for $s > 4$ now follows by induction over s and permutation of the variables. \square

After these preparations we now come to the main result of this section:

Theorem 10.9. *Let $p \in \mathbb{P}$ be odd, $q = p^e$ and $2m > q$. Then:*

- (a) *If e is even then the symplectic group $S_{2m}(q)$ has a G -realization over $\bar{\mathbb{Q}}$.*
- (b) *If e is odd then $S_{2m}(q)$ has a G -realization over $\mathbb{Q}(\sqrt{p^*})$.*

Proof. We start with the case that $q \equiv 1 \pmod{4}$, which implies in particular that $q \geq 5$. Then the dihedral group D_{q-1} of order $2(q-1)$ is isomorphic to the general orthogonal group $\text{GO}_2^+(q)$. Further, $\varphi(q-1) = 2l$ is even with $l \geq 1$. Let $a \in \mathbb{F}_q^\times$ be a generator and $a_1 = a, \dots, a_{2l}$ its primitive powers, with $a_{l+i} = a_i^{-1}$ for $1 \leq i \leq l$. Since $2m > q$ and $\varphi(q-1) \leq q-2$ we have $m \geq l+2$. Now choose $(\sigma_1, \dots, \sigma_{m+2}) \in D_{q-1}^{m+2}$ with reflections σ_1, σ_2 , a bihomology σ_3 of order 4, representatives $\sigma_4, \dots, \sigma_{l+3}$ of the different classes of bihomologies $\text{diag}(a_i, a_i^{-1})$, and $\sigma_{l+4} = \dots = \sigma_{m+2} = -\iota_2$. Then after a suitable choice of the parity of the reflections according to Proposition 10.8 we may attain $\sigma_\infty = -\iota_2$, and the corresponding class $[\sigma] = [\sigma_1, \dots, \sigma_{m+2}, \sigma_\infty]$ of generating systems of D_{q-1} lies in the unique H_s -braid orbit of length 2^l for $s = m+3$.

With the convolution \bar{P}_{-1} according to Proposition 9.2 we obtain

$$\bar{P}_{-1}(\sigma_1, \dots, \sigma_{m+2}) = (\tau_1, \dots, \tau_{m+2}) \in \text{GL}_{2m}(q)^{m+2}.$$

Here by Corollary 9.13 the elements τ_1, τ_2 are transvections, τ_3 is a bihomology of order 4, $\tau_4, \dots, \tau_{l+3}$ are bihomologies of order $q-1$, $\tau_{l+4}, \dots, \tau_{m+2}$ are bitransvections and $\tau_\infty = -\iota_{2m}$. By Corollaries 9.7 and 10.7 the group H generated by the τ_i is an irreducible subgroup of $\text{Sp}_{2m}(q)$. Now let $N \trianglelefteq H$ be the normal subgroup generated by the transvections in H . Then H itself is also irreducible and by the Theorem II.2.2(a) of Kantor isomorphic to $\text{Sp}_{2m}(\tilde{q})$ for some $\tilde{q}|q$. But then $H = \text{Sp}_{2m}(q)$, since for example the traces $a_i + a_i^{-1}$ generate \mathbb{F}_q^\times .

Now denote by $C_i := [\tau_i]$ for $i = 1, \dots, m+2$ the conjugacy class of τ_i in H , and $C_s = [\tau_\infty^{-1}] = [-\iota_{2m}]$. Then $\mathbf{C} = (C_1, \dots, C_s)$ is GL-stable, since $\text{CSp}_{2m}(q)$ interchanges the two classes of transvections and leaves invariant all of the other conjugacy classes. By Corollary 9.18 the convolution \bar{P}_{-1} then transfers the H_s -braid orbit of $[\sigma]$ to a corresponding H_s -braid orbit in $\Sigma(\mathbf{C})/\text{Inn}(H)$, and due to the invertibility of \bar{P}_{-1} we moreover have $|\Sigma(\mathbf{C})/\text{Inn}(H)| = 2^l$. Now choose $\boldsymbol{\tau} \in \Sigma(\mathbf{C})$. Then by Proposition 10.8

$$K_{\boldsymbol{\tau}} = \mathbb{Q}_{\mathbf{C}}(t_1, t_2, t_3, u_4, \dots, u_{l+3}, t_{l+4}, \dots, t_{m+2}, t) =: \mathbb{Q}_{\mathbf{C}}(\mathbf{t}^\vee, \mathbf{u})$$

with $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}_{C_1}(w_{q-1} + w_{q-1}^{-1})$, where w_{q-1} denotes a primitive $(q-1)$ st root of unity and $\mathbb{Q}_{C_1} = \mathbb{Q}$, respectively $\mathbb{Q}_{C_1} = \mathbb{Q}(\sqrt{p^*})$, according to whether C_1 is rational (if e is even) or non-rational (when e is odd) (see e.g. Thompson and Völklein (1998), 1.4 and 1.5). The cyclotomic character permutes the conjugacy classes

C_4, \dots, C_{l+3} . Let the corresponding permutation group $V \leq S_l$ act on t_4, \dots, t_{l+3} as well as on u_4, \dots, u_{l+3} in the same way and let U be the $\mathbb{Q}_C(\mathbf{t}^\vee)$ -vector space

$$U = \mathbb{Q}_C(\mathbf{t}^\vee) \langle u_4, \dots, u_{l+3} \rangle$$

with the lifted action of the cyclotomic character on the u_i . Then by Proposition 3.10 (Lemma of Speiser) U has a $\mathbb{Q}_{C_1}(\mathbf{t}^\vee)$ -form $\tilde{U} = \bigoplus_{i=4}^{l+3} \mathbb{Q}_{C_1}(\mathbf{t}^\vee) v_i$, and the V -symmetrized fixed field $K_\tau^V := \mathbb{Q}_{C_1}(\mathbf{t}^\vee, \mathbf{v})$ of \tilde{N}_τ is regular and rational over \mathbb{Q}_{C_1} . So by the Rigid Braid Orbit Theorem (Corollary 5.8), $S_{2m}(q) = \mathrm{Sp}_{2m}(q)/\mathcal{L}(\mathrm{Sp}_{2m}(q))$ has a G-realization over \mathbb{Q}_{C_1} , with $\mathbb{Q}_{C_1} = \mathbb{Q}$ or $\mathbb{Q}_{C_1} = \mathbb{Q}(\sqrt{p^*})$ according to the parity of e .

In the second case $q \equiv 3 \pmod{4}$ with $q \geq 3$ we proceed accordingly, now starting from the dihedral group $D_{q+1} = \mathrm{GO}_2^-(q) \leq \mathrm{GL}_2(q)$ and a generating element a of a cyclic subgroup of order $q+1$ in $\mathbb{F}_{q^2}^\times$ and using $l = \frac{1}{2}\varphi(q+1)$ and $m \geq l+1$. Observe that in this case again the subgroup $H \leq \mathrm{GL}_{2m}(q)$ generated by τ is isomorphic to $\mathrm{Sp}_{2m}(q)$. \square

Remark. Observe that the second symmetrization ω used in Dettweiler and Reiter (2000) in order to get rid of the irrationality $\sqrt{p^*}$ which interchanges t_1 and t_2 is not independent of the V -symmetrization used here, as $\omega(u_j) = u_j^{-1}$, so that the Lemma of Speiser cannot be applied.

10.4 Orthogonal Groups

Using the transformation rules for the convolution \bar{P}_{-1} in Corollary 10.7 it is possible in suitable circumstances to construct G-realizations of orthogonal groups starting from G-realizations of symplectic groups. Examples for this, resulting from Theorem 10.9, are collected in the present section. These have their origin in Dettweiler and Reiter (2000). We start with the case of odd-dimensional orthogonal groups.

Theorem 10.10. *Let $n = 2m + 1$ and $q = p^e$ be odd with $m > q$. Then $\mathrm{SO}_n(q)$ possesses a G-realization over \mathbb{Q} .*

Proof. As in the proof of Theorem 10.9 we first treat the case when $q \equiv 1 \pmod{4}$. For this we start with the variation

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+2}) := (\tau_1, -\tau_2, \tau_3, \dots, \tau_{m+1}, -\tau_{m+2}) \in \mathrm{Sp}_{2m}(q)^{m+2}$$

of the $(m+2)$ -tuple $(\tau_1, \dots, \tau_{m+2})$ constructed there, with $\tilde{\tau}_\infty = \tau_\infty = -\iota_{2m}$. Then the convolution \bar{P}_{-1} by Proposition 9.2 gives

$$\bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{2m+2}) =: (\rho_1, \dots, \rho_{m+2}) \in \mathrm{GL}_{4m-1}(q)^{m+2}.$$

By Corollary 9.13 here ρ_1 is a reflection, ρ_3 a rational bihomology of order 4, $\rho_4, \dots, \rho_{l+3}$ are bihomologies of order $q-1$, $\rho_{l+4}, \dots, \rho_{m+1}$ are bireflections, ρ_2

and ρ_{m+2} are unipotent with Jordan normal form as in Corollary 9.13(a), and $\rho_\infty = -\iota_{4m-1}$. The group H generated by the ρ_i is an irreducible subgroup of $\mathrm{GO}_{4m-1}(q)$ by Corollaries 9.7 and 10.7. According to the proof of Proposition 10.1(b) then H as well as its normal subgroup generated by its reflections are both primitive. But then by the Theorem II.2.4 of Wagner et al. we have

$$\mathrm{GO}_{4m-1}(q) \geq H \geq N \geq \mathcal{Q}_{4m-1}(\tilde{q}) \quad \text{with } \tilde{q}|q.$$

Since the traces of $\rho_4, \dots, \rho_{l+3}$ generate \mathbb{F}_q over \mathbb{F}_p and $\det(\rho_1) = -1$, $\mathrm{spin}(\rho_4) \notin (\mathbb{F}_q^\times)^2$, we hence have $H = \mathrm{GO}_{4m-1}(q)$. Now let $C_i := [\rho_i]$ for $i = 1, \dots, m+2$ denote the conjugacy class of ρ_i in H , and $C_s := [\rho_\infty^{-1}] = [-\iota_{4m-1}]$ for $s = m+3$. Then by Table 1.1 in Chapter II the class vector $\mathbf{C} = (C_1, \dots, C_s)$ is GL -stable. According to Corollary 9.18 the H_s -action on the braid orbit of $[\tau_1, \dots, \tau_s]$ is transported by \bar{P}_{-1} isomorphically onto $\Sigma(\mathbf{C})/\mathrm{Inn}(H)$. For $\rho \in \Sigma(\mathbf{C})$ we obtain the field of definition

$$K_\rho = \mathbb{Q}_\mathbf{C}(\mathbf{t}^\vee, \mathbf{u}) \quad \text{with} \quad \mathbb{Q}_\mathbf{C} = \mathbb{Q}(w_{q-1} + w_{q-1}^{-1})$$

of $\bar{N}_\rho/\bar{\mathbb{Q}}(\mathbf{t})$, in the notation of the proof of Theorem 10.9, since each of the classes $C_1, C_2, C_3, C_{l+4}, \dots, C_s$ is rational. V -symmetrization exactly as in the symplectic case then leads to the rational field of definition $K_\rho^V = \mathbb{Q}(\mathbf{t}^\vee, \mathbf{v})$ from the proof of Theorem 10.9. This shows the existence of a G -realization \tilde{N}/K_ρ^V of $\mathrm{SO}_{4m-1}(q) = \mathrm{GO}_{4m-1}(q)/\mathcal{Z}(\mathrm{GO}_{4m-1}(q))$ over \mathbb{Q} .

For dimension $4m+1$ we use a second variation of $(\tau_1, \dots, \tau_{m+2})$, namely

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) := (\tau_1, -\tau_2, \dots, \tau_{m+2}, -\iota_{2m}) \quad \text{with} \quad \tilde{\tau}_\infty = -\iota_{2m}$$

and analogously put

$$(\rho_1, \dots, \rho_{m+3}) := \bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) \in \mathrm{GL}_{4m+1}(q)^{m+3}.$$

Then $H := \langle \rho \rangle$ becomes the group $\mathrm{GO}_{4m+1}(q)$. As above V -symmetrization then yields a G -realization over \mathbb{Q} of $\mathrm{SO}_{4m+1}(q)$ when $2m > q$.

In the case $q \equiv -1 \pmod{4}$ we proceed completely analogously with the starting tuple $(\tau_1, \dots, \tau_{m+2}) \in \mathrm{Sp}_{2m}(q)^{m+2}$ from the corresponding part of the proof of Theorem 9.10. The variants of τ and of ρ as above and V -symmetrization then yield the assertion of the theorem in this case as well. \square

Corollary 10.11. *If in Theorem 10.10 we moreover have $q \equiv \pm 3 \pmod{8}$ then also the simple groups $O_n(q)$ possess G -realizations over \mathbb{Q} .*

Proof. We start again with the case $q \equiv 1 \pmod{4}$, for which we vary the generators of $D_{2m} = \mathrm{GO}_2^+(q)$ in the proof of Theorem 10.9 by letting

$$\sigma' := (\sigma_1, \sigma_2, \sigma_3, \sigma'_4, \dots, \sigma'_{l+3}, -\iota_2, \dots, -\iota_2) \in \mathrm{GO}_2^+(q)^s$$

with pairwise non-conjugate bihomologies σ'_j of order $(q-1)/2$. (Then $\sigma_3 \sigma'_j$ has order $q-1$ for $j = 4, \dots, l+3$.) As in the proofs of Theorems 10.9 and 10.10 from

this we obtain successively

$$\tau' := \bar{P}_{-1}(\sigma'), \quad \tilde{\tau}', \quad \rho' := \bar{P}_{-1}(\tilde{\tau}') \text{ and } \tilde{\rho}' := (-\rho'_1, \rho'_2, \dots, \rho'_{m+2}).$$

As in those cases the group $\tilde{H}' := \langle \tilde{\rho}' \rangle$ is isomorphic to $\mathrm{SO}_{4m-1}(q)$. But now we have $\mathrm{spin}(\tilde{\rho}'_i) \in (\mathbb{F}_q^\times)^2$ for $i = 4, \dots, m+2$, while $\mathrm{spin}(\tilde{\rho}'_3) \notin (\mathbb{F}_q^\times)^2$ as $q \equiv 5 \pmod{8}$. Because of $\tilde{\rho}'_\infty = \iota_{4m-1}$ there hence exists a unique further $i \in \{2, 3\}$ with $\mathrm{spin}(\tilde{\rho}'_i) \notin (\mathbb{F}_q^\times)^2$, say $\tilde{\rho}'_2$. We denote the V -symmetrized G-realization over \mathbb{Q} belonging to $\tilde{\rho}'$ by \tilde{N}'/\tilde{K}' , with $\tilde{K}' = K_{\tilde{\rho}'}^V = \mathbb{Q}(\mathbf{t}^\vee, \mathbf{v})$ as above. The fixed field \tilde{L}' of $\mathrm{O}_{4m-1}(q)$ herein has degree 2 over \tilde{K}' and is only ramified in the numerator divisors of $t - t_2$ and $t - t_3$. Thus \tilde{L}' is rational over \tilde{K}' and over \mathbb{Q} , and \tilde{N}'/\tilde{K}' yields a G-realization of $\mathrm{O}_{4m-1}(q)$ over \mathbb{Q} . Starting instead with the second variant of τ in the proof of Theorem 10.10, applied to τ' we then also obtain a G-realization of $\mathrm{O}_{4m+1}(q)$ over \mathbb{Q} (when $2m > q$).

The case $q \equiv -1 \pmod{4}$ and so $q \equiv 3 \pmod{8}$ is proved analogously, now starting from the group $\mathrm{GO}_2^-(q)$ in place of $\mathrm{GO}_2^+(q)$, and with $l = \frac{1}{2}\varphi(q+1)$ instead of $\frac{1}{2}\varphi(q+1)$. \square

For orthogonal groups in even dimension we show:

Theorem 10.12. *Let $n = 2m$ be even, $q = p^e$ odd and $m > q$.*

- (a) *If $q \equiv 1 \pmod{4}$ then $\mathrm{PGO}_n^+(q)$ and $\mathrm{PSO}_n^+(q)$ possess G-realizations over \mathbb{Q} .*
- (b) *If $q \equiv -1 \pmod{4}$ then $\mathrm{PGO}_n^-(q)$ and $\mathrm{PSO}_n^-(q)$ possess G-realizations over \mathbb{Q} .*

Proof. In (a), with $q \equiv 1 \pmod{4}$, we use as starting point the variation

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) := (\tau_1, \dots, \tau_{m+1}, -\tau_{m+2}, -\iota_{2m}) \in \mathrm{Sp}_{2m}(q)^{m+3}$$

of the tuple $(\tau_1, \dots, \tau_{m+2})$ from the proof of Theorem 10.9. Application of the convolution \bar{P}_{-1} yields

$$\bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) =: (\rho_1, \dots, \rho_{m+3}) \in \mathrm{GL}_{4m}(q)^{m+3}.$$

Here, according to Corollary 9.13 the elements ρ_1, ρ_2 are reflections, $\rho_3, \dots, \rho_{l+3}$ are bihomologies of order 4, $q-1$ respectively, $\rho_{l+4}, \dots, \rho_{m+1}$ are bireflections, ρ_{m+2}, ρ_{m+3} are unipotent and $\rho_\infty = -\iota_{4m}$. By Corollaries 9.7 and 10.7 the group $H = \langle \rho \rangle$ generated by the ρ_i is an irreducible subgroup of $\mathrm{GO}_{4m}^+(q)$. As H is moreover primitive by the proof of Proposition 10.1(b), we have $H \geq \Omega_{4m}^+(\tilde{q})$ for some $\tilde{q}|q$ by the Theorem II.2.4 of Wagner. As above, the traces of $\rho_4, \dots, \rho_{l+3}$ generate \mathbb{F}_q and we have $\det(\rho_1) = -1$ and $\mathrm{spin}(\rho_4) \notin (\mathbb{F}_q^\times)^2$. Thus, $H = \mathrm{GO}_{4m}^+(q)$.

Now let $C_i := [\rho_i]$ in H for $i = 1, \dots, m+3$ and $C_s := [\rho_\infty^{-1}]$ for $s = m+4$. Then the components $C_1, C_2, C_3, C_{l+4}, \dots, C_s$ of $\mathbf{C} = (C_1, \dots, C_s)$ are rational, and we have $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(w_{q-1} + w_{q-1}^{-1})$ for a primitive $(q-1)$ st root of unity w_{q-1} . Since the two classes of reflections in $\mathrm{GO}_{4m}^+(q)$ are conjugate in the conformal group $\mathrm{CO}_{4m}^+(q)$, the stabilizer $F_1 := \{\alpha \in \mathrm{CO}_{4m}^+(q) \mid C_1^\alpha = C_1\}$ has index 2 in $\mathrm{CO}_{4m}^+(q)$.

But then $F_1 = \mathcal{C}_{\mathrm{GL}_{4m}(q)}(H) \cdot H$ and the class vector \mathbf{C} of H is GL -stable. Consequently the H_s -action on the braid orbit of $[\tau_1, \dots, \tau_{m+3}]$ is transported isomorphically to $\Sigma(\mathbf{C})/\mathrm{Inn}(H)$. As above V -symmetrization then leads to a G -realization \tilde{N}/\tilde{K} over \mathbb{Q} of $\mathrm{PGO}_{4m}^+(q)$. The fixed field \tilde{L} of $\mathrm{PSO}_{4m}^+(q)$ herein has degree 2 over \tilde{K} and is only ramified at the two reflection classes C_1, C_2 , so in the numerator divisors of $t - t_1$ and $t - t_2$. Thus \tilde{L}/\tilde{K} and then also \tilde{L}/\mathbb{Q} are rational, and $\mathrm{PSO}_{4m}^+(q)$ also has a G -realization over \mathbb{Q} .

In dimension $4m + 2$ we use the variation

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+4}) := (\tau_1, \dots, \tau_{m+2}, -\iota_{2m}, -\iota_{2m}) \in \mathrm{Sp}_{2m}(q)^{m+4}$$

of $(\tau_1, \dots, \tau_{m+2})$. This yields

$$\bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+4}) =: (\rho_1, \dots, \rho_{m+4}) \in \mathrm{GL}_{4m+2}(q)^{m+4}.$$

Then $H := \langle \rho \rangle$ is a primitive subgroup of $\mathrm{GO}_{4m+2}(q)$, whence $H = \mathrm{GO}_{4m+2}(q)$ according to the theorem of Wagner. Copying the proof in the previously treated case then furnishes G -realizations over \mathbb{Q} for $\mathrm{PGO}_{4m+2}(q)$ and $\mathrm{PSO}_{4m+2}^+(q)$.

For the proof of (b) we start with the variation

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) := (\tau_1, \dots, \tau_{m+1}, -\tau_{m+2}, -\iota_{2m}) \in \mathrm{Sp}_{2m}(q)^{m+3}$$

of the $(m+2)$ -tuple $(\tau_1, \dots, \tau_{m+2})$ used in the corresponding case of Theorem 10.9. An application of \bar{P}_{-1} leads to

$$\bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+3}) =: (\rho_1, \dots, \rho_{m+3}) \in \mathrm{GL}_{4m}(q^2)^{m+3}.$$

The group $H := \langle \rho \rangle$ generated by the ρ_i is an irreducible and primitive subgroup of $\mathrm{GO}_{4m}^+(q^2)$. Stability under the Frobenius automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ yields that $H \leq \mathrm{GO}_{4m}^-(q)$, which by the theorem of Wagner again shows equality $H = \mathrm{GO}_{4m}^-(q)$. As above the class vector $\mathbf{C} = (C_1, \dots, C_s)$ formed of the $C_i = [\rho_i]$ is GL -stable with $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}(w_{q-1} + w_{q-1}^{-1})$. Thus V -symmetrization leads to a G -realization of $\mathrm{PGO}_{4m}^-(q)$ and then of $\mathrm{PSO}_{4m}^-(q)$ over \mathbb{Q} . Application of the convolution \bar{P}_{-1} to the second variation

$$(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+4}) := (\tau_1, \dots, \tau_{m+2}, -\iota_{2m}, -\iota_{2m}) \in \mathrm{Sp}_{2m}(q)^{m+4}$$

of $(\tau_1, \dots, \tau_{m+2})$ gives

$$\bar{P}_{-1}(\tilde{\tau}_1, \dots, \tilde{\tau}_{m+4}) =: (\rho_1, \dots, \rho_{m+4}) \in \mathrm{GL}_{4m+2}(q^2)^{m+4},$$

which then leads to the corresponding result for the case $n = 4m + 2$ with $m > q$. \square

Remark. Using $\sigma_3 = \mathrm{diag}(y, y^{-1}) \in D_{2m} \leq \mathrm{GL}_2(q)$ with a primitive third (respectively sixth) root of unity y (in place of $\sigma_3 = \mathrm{diag}(x, x^{-1})$ with a primitive fourth root of unity x) yields the corresponding assertions of Theorem 10.12 in the case that $q \equiv \pm 1 \pmod{6}$ instead of $q \equiv \pm 1 \pmod{4}$.

10.5 Results for Groups in Characteristic Two

In the case of groups over fields of even order we only work out the example case of linear and unitary groups from Dettweiler and Reiter (2000).

Theorem 10.13. *Let $q = 2^e$ and $n = 4m > 2q$.*

- (a) *If e is even then $\mathrm{PGL}_n(q)$ has a G-realization over \mathbb{Q} .*
- (b) *If e is odd then $\mathrm{PGU}_n(q)$ has a G-realization over \mathbb{Q} .*

Proof. In case (a) we have $q \equiv 1 \pmod{3}$, so \mathbb{F}_q^\times contains a primitive third root of unity y . Further let $a \in \mathbb{F}_q$ be a generator of \mathbb{F}_q^\times and $a_1 = a, a_2, \dots, a_{2l}$ the primitive powers of a , where again we set $l = \frac{1}{2}\varphi(q-1)$. Starting from the tuple

$$\mathbf{a} = (a_1, \dots, a_{2l}, y, y^{-1}, \dots, y, y^{-1}) \in (\mathbb{F}_q^\times)^{2m}$$

with product 1 we form

$$\bar{P}_y(a_1, \dots, a_{2m}, y^{-1}) =: (\sigma_1, \dots, \sigma_{2m+1}) \in \mathrm{GL}_{2m}(q)^{2m+1}$$

with $\sigma_\infty = y\iota_{2m}$, and then

$$\bar{P}_{y^{-1}}(\sigma_1, \dots, \sigma_{2m}, y\sigma_{2m+1}, y^{-1}\iota_{2m}) =: (\tau_1, \dots, \tau_{2m+2}) \in \mathrm{GL}_{4m}(q)^{2m+2}.$$

Then τ_1, \dots, τ_{2m} are homologies with eigenvalues $a_1, \dots, a_{2l}, y^{\pm 1}$ respectively, τ_{2m+1} is unipotent, τ_{2m+2} is conjugate to $\mathrm{diag}(y, y^{-1}, \dots, y, y^{-1})$, and $\tau_\infty = y^{-1}\iota_{4m}$. The associated tuple $\tilde{\tau} = (\tau_1, \dots, \tau_{2m+1}, y\tau_{2m+2})$ thus has product $\tilde{\tau}_\infty = \iota_{4m}$ and is linearly rigid. It generates a group H which by Corollary 9.7 and the proof of Proposition 10.1(b) is a primitive subgroup of $\mathrm{GL}_{4m}(q)$. Due to the presence of homologies H is not contained in $\mathrm{GU}_{4m}(q)$, so by Theorem II.2.3 we have $\mathrm{SL}_{4m}(\tilde{q}) \leq H$ for some $\tilde{q}|q$. As $\det(\tilde{\tau}_1) = a$ generates \mathbb{F}_q^\times we thus have $H = \mathrm{GL}_{4m}(q)$, and $\tilde{\tau}$ is a rigid generating system of H by Proposition 9.8(b). The cyclotomic character permutes the conjugacy classes C_1, \dots, C_{2m} of the $\tilde{\tau}_i$, generating a subgroup V of $S_{2l} \times Z_2^{m-l}$ of order $2l = \varphi(q-1)$. By the multi-variate variant of the Strong Rigidity Theorem 3.11 the V -symmetrized field of definition $K_{\tilde{\tau}}^V$ of $\bar{N}_{\tilde{\tau}}/\bar{\mathbb{Q}}(\mathbf{t})$ is a rational function field over \mathbb{Q} and so leads to a G-realization of $\mathrm{PGL}_{4m}(q)$ over \mathbb{Q} .

In part (b) we have that $q \equiv -1 \pmod{3}$. Here, we use a generator a of a cyclic subgroup of order $q+1$ of $\mathbb{F}_{q^2}^\times$ and a primitive third root of unity $y \in \mathbb{F}_{q^2}$ and then proceed as above. \square

Remark. For $n = 4m+2$ by Völklein (1993) there also exist G-realizations of $\mathrm{PGL}_n(q)$ and $\mathrm{PGU}_n(q)$ over \mathbb{Q} for $n > \varphi(q-1)$ or $n > \varphi(q+1)$ respectively. For these no simplified approach via the Katz algorithm seems to be known (see also Section III.9.4 of the first edition Malle and Matzat (1999)).

Corollary 10.14. *Under the assumptions of Theorem 10.13 we also have:*

- (a) *If e is even and $\gcd(n, q - 1) = 1$ then $L_n(q)$ has a G-realization over \mathbb{Q} .*
- (b) *If e is odd and $\gcd(n, q + 1) = 1$ then $U_n(q)$ has a G-realization over \mathbb{Q} .*

Proof. Under the stated conditions $L_n(q)$ agrees with $\mathrm{PGL}_n(q)$, respectively $U_n(q)$ agrees with $\mathrm{PGU}_n(q)$, so that the claim is immediate from Theorem 10.13. \square

Further G-realizations of groups in characteristic 2 can be obtained starting from suitable tuples in $\mathrm{GL}_2(q)$ and $\mathrm{GO}_2^\pm(q)$, see Dettweiler and Reiter (2000). In order to obtain G-realizations over \mathbb{Q} one needs to take into account the Remark at the end of Section 10.3.

IV Embedding Problems

The question of whether a given Galois extension can be embedded into a larger one is called an embedding problem. These occur in a natural way if, starting from the chief factors, one tries to realize composite groups as Galois groups over a given field. In the number theoretical context this question already has a long history which beginning with the work of Scholz (1929) and Reichardt (1937) finally led to the realization of all solvable groups as Galois groups over \mathbb{Q} by Šafarevič (1954a,c,d, 1989). In this chapter we mainly study embedding problems for geometric field extensions, for which interest arose only much later, starting with Saltman (1982).

The first part contains the elementary theory. After several simple reduction theorems in Paragraph 1 we present in Paragraphs 2 and 3 the two presently known basic constructions for proper solutions of embedding problems. These are the solution of split embedding problems with abelian kernel and the solution of centerless embedding problems with GAR-kernel. These are presented here in the form suitable to regular solutions as introduced by Matzat (1995) as parametric solutions. By Fried and Völklein (1992) the second of these constructions also leads to the proof reproduced in Section 3.3 that the absolute Galois group of a Hilbertian PAC field is free. Paragraph 4 contains methods for the verification, and an overview of the presently known GAR-realizations of simple groups. In Paragraph 5 we study embedding problems with abelian kernel and give the criterion from Matzat (1991b) for the solvability of geometric Frattini embedding problems. This is applied to the A_n -polynomials constructed by Mestre (1990) to realize all central extensions of A_n as Galois groups over $\mathbb{Q}(t)$.

In the second part we employ cohomological methods. The principal result in Paragraph 6 is the criterion of Serre (1984) for the solvability of central embedding problems with kernel Z_2 , which relies on the computation of the cohomological embedding obstruction from invariants of the quadratic trace form. As examples we treat the central extensions of the symmetric groups S_n following Sonn (1991). Paragraph 7 contains local-global principles for more general Brauer embedding problems found by Sonn (1990, 1994a,b) with applications to the realization of

central extensions of almost simple groups over $\mathbb{Q}^{\text{ab}}(t)$. In Paragraph 8 we study the question when the solvability of all accompanying Brauer embedding problems, this is the concordance (compatibility) condition introduced by Delone and Faddeev (1944), implies the solvability of the originally given embedding problem. The remaining second embedding obstruction is here called Hasse obstruction. For this, a cohomological description is derived in Paragraph 9. Finally in Paragraph 10 we prove the Theorem of Scholz (1937) and Reichardt (1937) on the realizability of nilpotent groups as Galois groups over arbitrary global fields. Here we use a variant of proof given by Rzedowski-Calderon (1989) and Madan, Rzedowski-Calderon and Villa-Salvador (1996).

1 Geometric Embedding Problems

This first paragraph of the chapter serves as introduction and for the comparison of different types of embedding problems over Hilbertian fields. Also, the two first elementary reduction theorems for embedding problems are proved.

1.1 Hilbertian Fields

For the convenience of the reader and to fix notation we briefly recall the most important definitions and results on Hilbertian fields. All proofs can be found in the monograph of Fried and Jarden (1986), Ch. 11 and Ch. 12, for example.

First let K be an arbitrary field and $f_i(\mathbf{t}, X) \in K(\mathbf{t})[X]$, $\mathbf{t} = (t_1, \dots, t_r)$, for $i = 1, \dots, m$ irreducible separable polynomials over the rational function field $K(\mathbf{t})$. Then the set of all $\mathbf{a} \in K^r$ for which $f_i(\mathbf{a}, X) \in K[X]$ is defined and irreducible is called a *Hilbertian set of K in K^r* :

$$\mathcal{H}_K(f_1, \dots, f_m) := \{\mathbf{a} \in K^r \mid f_i(\mathbf{a}, X) \in K[X] \text{ def. and irred.}\}. \quad (1.1)$$

(This corresponds to the notion of separable Hilbert set in loc. cit.) K is called a *Hilbertian field*, if every Hilbertian set of K is nonempty.

The Hilbertian fields occurring in the sequel are all obtained from the following three theorems. The first was already proved by Hilbert (1892) in the case of number fields, in the case of function fields over infinite fields of constants by Franz (1931) and for congruence function fields by Inaba (1944) (see also Fried and Jarden (1986), Cor. 12.8 and Thm. 12.9):

Theorem 1.1. *Fields with product formula are Hilbertian.*

From this, one obtains the so-called classical Hilbertian fields by the following theorem:

Theorem 1.2. *If K is a Hilbertian field, then so is any finitely generated separable extension field L of K . Moreover, every Hilbert set of L also contains elements from K .*

This theorem follows from Cor. 11.7 and Remark 11.8(b) in loc. cit. The next result is equivalent to a theorem of Weissauer (1982), which originally was proved with model theoretic methods. A classical proof goes back to Fried and can be found in Fried and Jarden (1986), Prop. 12.14, respectively also in Matzat (1987), Ch. IV.A.

Theorem 1.3. *Let K be Hilbertian, N/K an (infinite) Galois extension, and L a proper finite separable extension of K with $L \cap N = K$. Then the composite $M = LN$ in a separable algebraic closure \bar{K} of K is Hilbertian. Moreover, any Hilbert set of M contains elements of L .*

Note that a Hilbert set of M does not necessarily contain elements from K . From this result the theorem of Weissauer can easily be reobtained in its original formulation (compare Fried and Jarden (1986), Cor. 12.15, or Matzat (1987), Ch. IV.A, Folgerung 1):

Corollary 1.4 (Weissauer (1982)). *If K is a Hilbertian field, L/K an (infinite) separable algebraic field extension, and N the Galois hull of L/K , then every finite separable extension field M of L not contained in N is Hilbertian.*

From this theorem respectively its corollary, it follows for example that \mathbb{Q}^{ab} is Hilbertian. In fact, \mathbb{Q}^{ab} has degree 2 over its maximal totally real subfield, and this is Galois over \mathbb{Q} . Since also the maximal totally real intermediate field \mathbb{Q}^{tr} of $\bar{\mathbb{Q}}/\mathbb{Q}$ is Galois over \mathbb{Q} , all proper finite extension fields of \mathbb{Q}^{tr} like $\mathbb{Q}^{tr}(\sqrt{-1})$ are Hilbertian, although \mathbb{Q}^{tr} itself is not.

1.2 Solutions of Embedding Problems

Let K continue to be an arbitrary field and $\Gamma_K := \text{Gal}(\bar{K}/K)$ the Galois group of a separable algebraic closure \bar{K} of K . A Galois extension N/K with group G is then determined by the restriction $\varphi : \Gamma_K \rightarrow G = \text{Gal}(N/K)$ with $\ker(\varphi) = \text{Gal}(\bar{K}/N)$. Now given a group extension $\tilde{G} = H \cdot G$ of a group H as normal subgroup with G and corresponding canonical epimorphism $\kappa : \tilde{G} \rightarrow G$, we are led to the question of whether there exists a homomorphism $\tilde{\varphi} : \Gamma_K \rightarrow \tilde{G}$, which extends φ via κ such that the following diagram commutes:

$$\begin{array}{ccccccc}
 & & & \Gamma_K & & & \\
 & & \swarrow \tilde{\varphi} & & \downarrow \varphi & & \\
 1 & \longrightarrow & H & \xrightarrow{\iota} & \tilde{G} & \xrightarrow{\kappa} & G \longrightarrow 1 \\
 & & & & & & (1.2)
 \end{array}$$

This is called the *embedding problem* $\mathcal{E}(\varphi, \kappa)$ given by φ and κ . The homomorphism $\tilde{\varphi}$ is called a *solution of the embedding problem* $\mathcal{E}(\varphi, \kappa)$ and the corresponding field $\tilde{N} := \bar{K}^{\ker(\tilde{\varphi})}$ a *solution field* of $\mathcal{E}(\varphi, \kappa)$. Note that $\tilde{\varphi}$ determines \tilde{N} but not vice versa. If here $\tilde{\varphi}$ is an epimorphism, then $\tilde{\varphi}$ respectively \tilde{N} is called a *proper solution (field) of the embedding problem*. In the latter case we have $\text{Gal}(\tilde{N}/K) \cong \tilde{G}$.

For a better description of embedding problems we employ the group theoretic terminology: H is called the *kernel* of the embedding problem $\mathcal{E}(\varphi, \kappa)$. The embedding problem is called *finite* if \tilde{G} is a finite group. It is called *split* respectively *non-split* if the corresponding group extension $\tilde{G} = H \cdot G$ splits respectively does not split. Further $\mathcal{E}(\varphi, \kappa)$ is called a *central* respectively *Frattini embedding problem*, if the kernel H lies in the center of \tilde{G} resp. in the Frattini subgroup of \tilde{G} .

If more particularly K/k is a function field with field of constants k , an embedding problem $\mathcal{E}(\varphi, \kappa)$ with epimorphisms $\varphi : \Gamma_K \rightarrow G$ and $\kappa : \tilde{G} \rightarrow G$ is called a *geometric embedding problem* if $N := \tilde{K}^{\ker(\varphi)}$ is geometric over K or equivalently regular over k . Correspondingly, a (proper) solution $\tilde{\varphi}$ of such an embedding problem is called a *geometric (proper) solution* if also $\tilde{N} := \tilde{K}^{\ker(\tilde{\varphi})}$ is geometric over K . Since only geometric embedding problems can possess geometric solutions, this hypothesis will sometimes be assumed implicitly.

In the following the deformable solutions of embedding problems will be of particular interest. This notion can be made more precise as follows: From a Galois extension N/K with group G and a system of $r \geq 1$ variables $\mathbf{t} = (t_1, \dots, t_r)$ over K one obtains a Galois extension $N^* := N(\mathbf{t})$ over $K^* := K(\mathbf{t})$ with the group $G^* \cong G$. Thus every embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with $\varphi : \Gamma_K \rightarrow G$ and $\kappa : \tilde{G} \rightarrow G$ can be lifted to a uniquely defined embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ over K^* with the extensions $\varphi^* : \Gamma_{K^*} \rightarrow G^*$ of φ and the composition $\kappa^* : \tilde{G} \rightarrow G^*$ of κ with the above isomorphism. A solution $\tilde{\varphi}^*$ of $\mathcal{E}(\varphi^*, \kappa^*)$ is now called a *regular solution of the embedding problem $\mathcal{E}(\varphi, \kappa)$ (in r variables)*, if the field N is algebraically closed in $\tilde{N}^* := (\tilde{K}^*)^{\ker(\tilde{\varphi}^*)}$, i.e., \tilde{N}^*/N is a regular field extension (by Nagata (1977), Thm. 3.5.2). The existence of a regular solution implies the existence of solutions:

Theorem 1.5. (a) *If a finite embedding problem $\mathcal{E}(\varphi, \kappa)$ over a Hilbertian field K possesses a regular (proper) solution, then it also possesses a (proper) solution.*

(b) *If a finite geometric embedding problem over an algebraic function field K/k possesses a regular (proper) solution, then it also possesses a geometric (proper) solution.*

Proof. Let K be a Hilbertian field, $K^* = K(\mathbf{t})$ and $\tilde{\varphi}$ a regular solution of $\mathcal{E}(\varphi, \kappa)$ with solution field $\tilde{N}^* = K^*[X]/(f(\mathbf{t}, X))$ whose existence is assumed in (a). Then by definition there exists a specialization $\mathbf{t} \mapsto \mathbf{a} \in K^r$ such that $\tilde{N}_{\mathbf{a}} := K[X]/(f(\mathbf{a}, X))$ is Galois over K with $\text{Gal}(\tilde{N}_{\mathbf{a}}/K) \cong \text{Gal}(\tilde{N}^*/K^*)$. Now let $\wp_{\mathbf{a}}$ be the place of K^*/K defined by $\mathbf{t} \mapsto \mathbf{a}$ with prime ideal $\mathfrak{p}_{\mathbf{a}}$ (compare Section III.6.1), $\hat{\wp}_{\mathbf{a}}$ an extension of $\wp_{\mathbf{a}}$ to the separable algebraic closure \tilde{K}^* of K^* with prime ideal $\hat{\mathfrak{p}}_{\mathbf{a}}$ and $K_{\mathbf{a}}^*$ the decomposition field of $\hat{\mathfrak{p}}_{\mathbf{a}}/\mathfrak{p}_{\mathbf{a}}$ (see Nagata (1977), Ch. VI, §3). Then we have

$$\Gamma_{K_{\mathbf{a}}^*} := \text{Gal}(\tilde{K}^*/K_{\mathbf{a}}^*) \cong \text{Gal}(\tilde{k} K^*/K^*) \cong \Gamma_K.$$

Furthermore, as $K_{\mathbf{a}}^* \cap \tilde{N}^* = K^*$ the homomorphisms $\varphi^*, \tilde{\varphi}^*$ by restriction to $\Gamma_{K_{\mathbf{a}}^*}$ define epimorphisms

$$\begin{aligned} \varphi_{\mathbf{a}}^* : \Gamma_{K_{\mathbf{a}}^*} &\rightarrow \text{Gal}(K_{\mathbf{a}}^* N^* / K_{\mathbf{a}}^*) \cong \text{Gal}(N^* / K^*) = G^*, \\ \tilde{\varphi}_{\mathbf{a}}^* : \Gamma_{K_{\mathbf{a}}^*} &\rightarrow \text{Gal}(K_{\mathbf{a}}^* \tilde{N}^* / K_{\mathbf{a}}^*) \cong \text{Gal}(\tilde{N}^* / K^*) \leq \tilde{G}^*, \end{aligned}$$

with $\kappa^* \circ \tilde{\varphi}_{\mathbf{a}}^* = \varphi_{\mathbf{a}}^*$. Moreover, by construction the first of these also satisfies $\rho_{\mathbf{a}} \circ \varphi_{\mathbf{a}}^* = \varphi_{\mathbf{a}}^* \circ \rho_{\mathbf{a}}$ with the isomorphism $\rho_{\mathbf{a}} : \Gamma_{K_{\mathbf{a}}^*} \rightarrow \Gamma_K$ (respectively for the corresponding factor groups) given by the residue class map. Thus $\tilde{\varphi}_{\mathbf{a}} := \rho_{\mathbf{a}} \circ \tilde{\varphi}_{\mathbf{a}}^* \circ \rho_{\mathbf{a}}^{-1}$ is an epimorphism of Γ_K onto $\text{Gal}(\tilde{N}_{\mathbf{a}}/K)$ with $\kappa \circ \tilde{\varphi}_{\mathbf{a}} = \varphi$. This proves (a).

By Theorems 1.1 and 1.2 the algebraic function field K/k in (b) is always Hilbertian, so the existence of a regular solution by (a) implies at least the existence of

solutions. It remains to show that among these are even geometric ones. By assumption k respectively N is algebraically closed in N resp. \tilde{N}^* , and in particular \tilde{N}^*/k is regular. If \bar{k} is the algebraic closure of k in a separable algebraic closure of \tilde{N}^* , the polynomial $f(\mathbf{t}, X) \in K^*[X]$ remains irreducible in $\bar{k}K^*[X]$. We now apply Theorem 1.3 to an intermediate field K' of K/k different from K over which K is finite separable. Using the notation $N' := \bar{k}K'$, $L' := K$ and $M' := \bar{k}K$ in analogy to Theorem 1.3 we obtain that every Hilbertian set of the Hilbertian field $\bar{k}K$ contains elements from K . Thus there exists an $\mathbf{a} \in K^r$ for which $f(\mathbf{a}, X)$ remains irreducible even in $\bar{k}K[X]$. The splitting field $\tilde{N}_{\mathbf{a}}$ of $f(\mathbf{a}, X)$ with $\text{Gal}(\tilde{N}_{\mathbf{a}}/K) \cong \text{Gal}(\tilde{N}^*/K^*)$ is then geometric over K , and in the same way as in part (a) it yields a geometric solution $\tilde{\varphi}_{\mathbf{a}}$ of the given embedding problem $\mathcal{E}(\varphi, \kappa)$. If here $\text{Gal}(\tilde{N}^*/K^*) \cong \tilde{G}$, then also $\text{Gal}(\tilde{N}_{\mathbf{a}}/K) \cong \tilde{G}$, thus regular proper solutions of the embedding problem always furnish geometric proper solutions. \square

Remark. If in Theorem 1.5(a) resp. (b) the given solution field \tilde{N}^* is different from N^* , then there even exist infinitely many different (geometric) solutions of the given embedding problem.

In the next section the different behavior of the notions introduced so far are illustrated on an elementary reduction theorem.

1.3 Direct Decomposition of the Kernel

If the kernel H of a finite embedding problem $\mathcal{E}(\varphi, \kappa)$ is a direct product of normal subgroups of $\tilde{G} = H \cdot G$, say $H = \prod_{i=1}^r H_i$, then in a natural way one obtains embedding problems $\mathcal{E}(\varphi, \kappa_i)$ for the factor groups $\tilde{G}_i := \tilde{G}/H_i^\vee$ with $H_i^\vee := H_1 \cdots H_{i-1} H_{i+1} \cdots H_r$, with kernels $H/H_i^\vee \cong H_i$. The following result, which in the case of Galois algebras goes back to Kochendörffer (1953), answers the question on the connection between the solvability respectively the proper solvability of $\mathcal{E}(\varphi, \kappa)$ and of $\mathcal{E}(\varphi, \kappa_i)$.

Theorem 1.6. *Assume that the kernel of the finite embedding problem $\mathcal{E}(\varphi, \kappa)$ over K (resp. K/k) decomposes into a direct product $H = \prod_{i=1}^r H_i$ of normal subgroups H_i of $\tilde{G} = H \cdot G$. Then for the corresponding embedding problems $\mathcal{E}(\varphi, \kappa_i)$ with the fixed field N of $\ker(\varphi)$ we have:*

- (a) *$\mathcal{E}(\varphi, \kappa)$ possesses a (proper) solution if and only if $\mathcal{E}(\varphi, \kappa_i)$ for $i = 1, \dots, r$ possess (proper) solutions (linearly disjoint over N).*
- (b) *If $\mathcal{E}(\varphi, \kappa)$ possesses a geometric (proper) solution then $\mathcal{E}(\varphi, \kappa_i)$ for $i = 1, \dots, r$ possess geometric (proper) solutions (linearly disjoint over $\bar{k}N$). If $\mathcal{E}(\varphi, \kappa_i)$ for $i = 1, \dots, r$ possess geometric (proper) solutions linearly disjoint over $\bar{k}N$ then $\mathcal{E}(\varphi, \kappa)$ possesses a geometric (proper) solution.*
- (c) *$\mathcal{E}(\varphi, \kappa)$ possesses a regular (proper) solution if and only if $\mathcal{E}(\varphi, \kappa_i)$ for $i = 1, \dots, r$ possess regular (proper) solutions.*

Proof. First it is clear that a solution $\tilde{\varphi} : \Gamma_K \rightarrow \tilde{G}$ leads to solutions $\tilde{\varphi}_i : \Gamma_K \rightarrow \tilde{G}_i$ of $\mathcal{E}(\varphi, \kappa_i)$ by composition with the canonical epimorphisms $\pi_i : \tilde{G} \rightarrow \tilde{G}_i$. In this way obviously a geometric resp. regular solution of $\mathcal{E}(\varphi, \kappa)$ yields geometric resp. regular solutions of $\mathcal{E}(\varphi, \kappa_i)$. If moreover $\tilde{\varphi}$ is proper with solution field \tilde{N} , then the fixed fields \tilde{N}_i of H_i^\vee are proper solution fields of $\mathcal{E}(\varphi, \kappa_i)$, which since $H = \prod_{i=1}^r H_i$ are linearly disjoint over N , and even after extension of constants with k over kN in the geometric case. It remains to show that the reverse implications in (a), (b) and (c) hold.

So assume that the embedding problems $\mathcal{E}(\varphi, \kappa_i)$ in (a) have solutions $\tilde{\varphi}_i : \Gamma_K \rightarrow \tilde{G}_i$ with solution fields \tilde{N}_i . Then $\tilde{\varphi}_i$ can be decomposed into an epimorphism $\tilde{\psi}_i : \Gamma_K \rightarrow \tilde{E}_i := \text{Gal}(\tilde{N}_i/K)$, followed by a monomorphism $\tilde{\varepsilon}_i : \tilde{E}_i \rightarrow \tilde{G}_i$, so that $\kappa_i \circ \tilde{\varepsilon}_i \circ \tilde{\psi}_i = \varphi$. By assumption \tilde{G} is the subdirect product (pull-back) of the \tilde{G}_i over G :

$$\tilde{G} = \tilde{G}_1 \times_G \cdots \times_G \tilde{G}_r = \{(\sigma_1, \dots, \sigma_r) \mid \kappa_i(\sigma_i) = \kappa_j(\sigma_j) \text{ for } i, j = 1, \dots, r\}$$

with $\kappa : \tilde{G} \rightarrow G$, $(\sigma_1, \dots, \sigma_r) \mapsto \kappa_1(\sigma_1)$. The composite \tilde{N} of the fields \tilde{N}_i (in \tilde{K}) is Galois over K and contains the field N . With the canonical mapping $\tilde{\pi}_i$ from $\tilde{E} := \text{Gal}(\tilde{N}/K)$ to $\tilde{E}_i = \text{Gal}(\tilde{N}_i/K)$ we get $\kappa_i \circ \tilde{\varepsilon}_i \circ \tilde{\pi}_i = \tilde{\kappa}$ where $\tilde{\kappa}$ denotes the canonical epimorphism from \tilde{E} onto $G = \text{Gal}(N/K)$. Thus

$$\tilde{\varepsilon} : \tilde{E} \rightarrow \tilde{G}, \quad \sigma \mapsto ((\tilde{\varepsilon}_i \circ \tilde{\pi}_i)(\sigma))_{i=1, \dots, r},$$

defines an injective homomorphism with $\kappa \circ \tilde{\varepsilon} = \tilde{\kappa}$. By composition with the restriction $\tilde{\psi} : \Gamma_K \rightarrow \tilde{E}$ we obtain a homomorphism $\tilde{\varphi} := \tilde{\varepsilon} \circ \tilde{\psi} : \Gamma_K \rightarrow \tilde{G}$ with

$$\kappa \circ \tilde{\varphi} = \kappa \circ \tilde{\varepsilon} \circ \tilde{\psi} = \tilde{\kappa} \circ \tilde{\psi} = \varphi$$

and hence a solution of $\mathcal{E}(\varphi, \kappa)$. If moreover the φ_i are proper solutions and the fields \tilde{N}_i are linearly disjoint over N , $\tilde{\varphi}$ is surjective due to

$$[\tilde{N} : N] = \prod_{i=1}^r [\tilde{N}_i : N] = \prod_{i=1}^r |H_i| = |H|,$$

and hence gives a proper solution. This shows (a), compare Fig. 1.1.

If the $\mathcal{E}(\varphi, \kappa_i)$ possess geometric solutions, which even after extension of constants to the algebraic closure remain linearly disjoint, k is algebraically closed in the solution field \tilde{N} , and the construction above yields a geometric solution of $\mathcal{E}(\varphi, \kappa)$. With the same argument as above it also follows that this solution is proper if and only if the solutions of the $\mathcal{E}(\varphi, \kappa_i)$ are.

In (c) we assume the existence of regular solutions $\tilde{\varphi}_i^*$ of $\mathcal{E}(\varphi, \kappa_i)$. Let $\tilde{N}_i^*/K(t_i)$ be the solution fields, where without loss of generality the parameter systems $t_i = (t_{i1}, \dots, t_{ir_i})$ form an algebraically independent system of variables. By assumption N is algebraically closed in each of the \tilde{N}_i^* , hence also in the composite \tilde{N}^* of these fields in an algebraic closure of $K^* := K(t_1, \dots, t_r)$. As above the canonical homomorphism $\tilde{\psi}^* : \Gamma_{K^*} \rightarrow \tilde{E}^* := \text{Gal}(\tilde{N}^*/K^*)$ can be extended to a homomorphism $\tilde{\varphi}^* : \Gamma_{K^*} \rightarrow \tilde{G}$ with $\kappa^* \circ \tilde{\varphi}^* = \varphi^*$, which is a regular solution of the embedding

$$\begin{array}{ccccccc}
& & & \Gamma_K & & & \\
& & & \tilde{\psi} \swarrow & \downarrow \tilde{\psi}_i & & \\
& & & \tilde{E} & \xrightarrow{\tilde{\pi}_i} & \tilde{E}_i & \\
& & \tilde{\varepsilon} \downarrow & \swarrow \tilde{\kappa} & & \downarrow \varphi & \\
1 & \longrightarrow & H & \longrightarrow & \tilde{G} & \xrightarrow{\kappa} & G \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \parallel \\
1 & \longrightarrow & H_i & \longrightarrow & \tilde{G}_i & \xrightarrow{\kappa_i} & G \longrightarrow 1
\end{array}$$

Fig. 1.1 Subdirect product

problem $\mathcal{E}(\varphi, \kappa)$. If all the solutions $\tilde{\varphi}_i^*$ are proper, $\tilde{\varphi}^*$ is also proper by (a), since the fields $K^* \tilde{N}_i^*$ are linearly disjoint over $K^* N$. \square

This theorem shows that in contrast to the case for ordinary solutions of embedding problems in the regular case the proper solvability of $\mathcal{E}(\varphi, \kappa)$ is equivalent to the proper solvability of the embedding problems $\mathcal{E}(\varphi, \kappa_i)$. Sometimes the additional hypothesis in Theorem 1.6(a) for the general case can already be assured by group theoretic conditions, like the following easy observation.

Remark. If the normal subgroups H_i in Theorem 1.6 possess pairwise coprime orders, the solution fields of the $\mathcal{E}(\varphi, \kappa_i)$ are necessarily linearly disjoint over N .

A trivial application of Theorem 1.6(c) now yields:

Corollary 1.7. *If the groups H_i for $i = 1, \dots, r$ possess G -realizations over a field K , then so does their direct product $H = \prod_{i=1}^r H_i$.*

Proof. This follows immediately from Theorem 1.6(c), since G -realizations are regular proper solutions of embedding problems with trivial cokernel. \square

1.4 From Improper to Proper Solutions

In several important cases the solvability of embedding problems implies the proper solvability. The first is the following special result on Frattini embedding problems (see Dentzer (1995b)).

Proposition 1.8. *Every solution of a finite (geometric) Frattini embedding problem is a proper (geometric) solution.*

Proof. First let $\mathcal{E}(\varphi, \kappa)$ be an ordinary Frattini embedding problem with kernel H over K , $\tilde{\varphi}$ a solution of $\mathcal{E}(\varphi, \kappa)$ with solution field \tilde{N} and $\text{Gal}(\tilde{N}/K) = E$, $\tilde{\psi} : \Gamma_K \rightarrow E$ the canonical epimorphism and $\varepsilon : E \rightarrow \tilde{G} = H \cdot G$ the homomorphism with $\varepsilon \circ \tilde{\psi} = \tilde{\varphi}$. Since $(\kappa \circ \varepsilon)(E) = G$ we conclude that $\tilde{G} = \langle H, \varepsilon(E) \rangle$, which implies $\tilde{G} = \varepsilon(E)$ since $H \leq \Phi(\tilde{G})$. Hence ε and so also $\tilde{\varphi}$ are epimorphisms.

Now let $\mathcal{E}(\varphi, \kappa)$ be a geometric Frattini embedding problem over the algebraic function field K/k with the proper solution $\tilde{\varphi}$ and the corresponding field \tilde{N} , so that $\tilde{N}^H = N$ and $\tilde{N}^{\tilde{G}} = K$. With the algebraic closure \tilde{k} of k in \tilde{N} the composites $\tilde{k}K$ and $\tilde{k}N$ (in \tilde{N}) are Galois over K . In particular the subgroup $U := \text{Gal}(\tilde{N}/\tilde{k}N)$ of H is normal in \tilde{G} , and with $\tilde{H} := H/U$ we have

$$\tilde{G}/U \cong \text{Gal}(\tilde{k}N/K) = \text{Gal}(\tilde{k}N/N) \times \text{Gal}(\tilde{k}N/\tilde{k}K) \cong \tilde{H} \times G.$$

Since by assumption $H \leq \Phi(\tilde{G})$ we also have $\tilde{H} \leq \Phi(\tilde{G}/U)$. Thus $\tilde{H} = 1$ and $\tilde{k} = k$, \tilde{N}/k is regular and hence \tilde{N}/K geometric. \square

A general but conditional result is already due to Ikeda (1960) and Nobusawa (1961).

Theorem 1.9 (Ikeda (1960)). *Assume that every finite split (geometric) embedding problem over a field K (resp. K/k) with kernel H is (geometrically) properly solvable. Then any finite (geometric) embedding problem $\mathcal{E}(\varphi, \kappa)$ with kernel H over K having a (geometric) solution also possesses a (geometric) proper solution.*

Proof. Let $N := \bar{K}^{\ker(\varphi)}$ and $\tilde{G} = H \cdot G$ the inverse image of κ . By assumption there exists a homomorphism $\tilde{\varphi}$ from $\Gamma_K = \text{Gal}(\bar{K}/K)$ to \tilde{G} with $\kappa \circ \tilde{\varphi} = \varphi$. The kernel of $\tilde{\varphi}$ is then a subgroup Γ_1 of Γ_K whose fixed field N_1 contains the field N and is Galois over K with group $G_1 = \text{Gal}(N_1/K)$. In particular there exist canonical epimorphisms $\varphi_1 : \Gamma_K \rightarrow G_1$, $\varepsilon : G_1 \rightarrow G$ with $\varepsilon \circ \varphi_1 = \varphi$ and a monomorphism $\tilde{\varepsilon} : G_1 \rightarrow \tilde{G}$ with $\tilde{\varepsilon} \circ \varphi_1 = \tilde{\varphi}$. In the subdirect product

$$\tilde{G}_1 := \tilde{G} \times_G G_1 = \{(\tilde{\sigma}, \hat{\sigma}) \mid \tilde{\sigma} \in \tilde{G}, \hat{\sigma} \in G_1, \kappa(\tilde{\sigma}) = \varepsilon(\hat{\sigma})\}$$

the kernel of the projection p_2 from \tilde{G}_1 onto the second factor is isomorphic to $\ker(\kappa) = H$, and $C_1 := \{(\tilde{\varepsilon}(\hat{\sigma}), \hat{\sigma}) \mid \hat{\sigma} \in G_1\}$ forms a complement to $\ker(p_2)$ in \tilde{G}_1 isomorphic to G_1 . Hence \tilde{G}_1 is the semidirect product of H with $C_1 \cong G_1$.

Now by assumption the embedding problem $\mathcal{E}(\varphi_1, p_2)$ has a proper solution, i.e., there exists an epimorphism $\tilde{\varphi}_1 : \Gamma_K \rightarrow \tilde{G}_1$ with $p_2 \circ \tilde{\varphi}_1 = \varphi_1$. This can be composed with the projection $p_1 : \tilde{G}_1 \rightarrow \tilde{G}$ to an epimorphism $\tilde{\varphi}' := p_1 \circ \tilde{\varphi}_1 : \Gamma_K \rightarrow \tilde{G}$ satisfying

$$\kappa \circ \tilde{\varphi}' = \kappa \circ p_1 \circ \tilde{\varphi}_1 = \varepsilon \circ p_2 \circ \tilde{\varphi}_1 = \varepsilon \circ \varphi_1 = \varphi.$$

Consequently $\tilde{\varphi}'$ is a proper solution of $\mathcal{E}(\varphi, \kappa)$.

If $\mathcal{E}(\varphi, \kappa)$ is a geometric embedding problem over the function field K/k with geometric solution $\tilde{\varphi}$, then $\mathcal{E}(\varphi_1, p_2)$ also becomes a split geometric embedding problem over K/k . By assumption this possesses a proper geometric solution $\tilde{\varphi}_1$,

$$\begin{array}{ccccccc}
 & & & & \Gamma_K & & \\
 & & & & \downarrow & & \\
 & & & & \tilde{\varphi}_1 & \nearrow & \varphi_1 \\
 & & & & p_2 & \nearrow & \downarrow \\
 1 & \longrightarrow & H & \longrightarrow & \tilde{G}_1 & \xrightarrow{p_2} & G_1 \longrightarrow 1 \\
 & & & & p_1 \downarrow & \nearrow \tilde{\varepsilon} & \downarrow \varepsilon \quad \downarrow \varphi \\
 & & & & \tilde{G} & \xrightarrow{\kappa} & G \longrightarrow 1 \\
 & & & & \iota & &
 \end{array}$$

Fig. 1.2 Proper solution

i.e., the corresponding solution field $\tilde{N}_1 := \bar{K}^{\ker(\tilde{\varphi}_1)}$ is regular over k . Being a subfield of \tilde{N}_1 , $\tilde{N} := \bar{K}^{\ker(\tilde{\varphi}')}$ is also regular over k and hence a geometric extension field of K with $\text{Gal}(\tilde{N}/K) \cong \tilde{G}$. \square

Corollary 1.10. *If the embedding problem $\mathcal{E}(\varphi, \kappa)$ in Theorem 1.9 possesses a regular solution over K in r variables and if over $K(t_1, \dots, t_r)$ every split embedding problem with kernel H is regularly properly solvable, then $\mathcal{E}(\varphi, \kappa)$ also has a regular proper solution.*

Proof. By assumption N is algebraically closed in the fixed field N_1^* of $\ker(\tilde{\varphi}^*)$ with respect to the lifted embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ over $K^* := K(\mathbf{t})$, $\mathbf{t} = (t_1, \dots, t_r)$, extending $\mathcal{E}(\varphi, \kappa)$. If $\tilde{\varphi}_1^*$ is a regular proper solution of the embedding problem over K^* corresponding to $\mathcal{E}(\varphi_1^*, p_2^*)$, then again N_1^* is algebraically closed in the corresponding solution field \tilde{N}_1^* . Hence N is even algebraically closed in the fixed field $\tilde{N}^* \leq \tilde{N}_1^*$ of the kernel of $\tilde{\varphi}' := p_1 \circ \tilde{\varphi}_1^*$, and $\tilde{\varphi}'$ yields a regular proper solution of $\mathcal{E}(\varphi, \kappa)$. \square

In the last section of this paragraph we give some fields over which every finite embedding problem is solvable.

1.5 Fields with Projective Galois Group

A profinite group Γ is called *projective profinite group*, if in the diagram (1.2) with Γ_K replaced by Γ every (pro-) finite embedding problem has a solution, equivalently if the cohomological dimension of Γ is at most 1. The fields of importance here with projective absolute Galois group are collected in the following theorem.

Theorem 1.11. *The following fields have projective absolute Galois group:*

- (a) *the fields of transcendence degree 1 over an algebraically closed field,*
- (b) *the finite fields and their algebraic extension fields,*

- (c) *the p -adic number fields with algebraically closed residue class field,*
- (d) *the algebraic number fields containing all roots of unity,*
- (e) *all PAC-fields (see Section III.6.4 for the definition).*

Theorem 1.11(a) is the Theorem of Tsen (see for example Shatz (1972), Ch. IV, Thm. 24), part (b) is a theorem of Chevalley (loc. cit., Thm. 25), part (c) is a theorem of Lang (loc. cit., Thm. 27), part (d) is a theorem of Serre (1964), Ch. II, Prop. 9 (see also Ribes (1970), Ch. V, Thm. 8.8), and part (e) is a theorem of Ax (see Fried and Jarden (1986), Thm. 10.17). As an immediate consequence we obtain:

Corollary 1.12. *Over the fields listed in Theorem 1.11, every finite embedding problem is solvable.*

A corresponding characterization theorem for fields over which all finite embedding problems are properly solvable is obtained from the following:

Theorem 1.13 (Freiheitssatz of Iwasawa (1953)). *A profinite group Γ of countably infinite rank is free profinite precisely when every finite embedding problem for Γ has a proper solution.*

A proof for this result can be found for example in Ribes (1970), Ch. I, Thm. 9.3, or in Fried and Jarden (1986), Cor. 24.2.

2 Split Embedding Problems with Abelian Kernel

In this paragraph we solve split embedding problems with abelian kernel over a Hilbertian field K using a wreath product construction. Over fields with projective Galois group this leads to the proper solvability of finite embedding problems with solvable kernel. Next we characterize those finite groups which can hereby be constructed inductively as geometric Galois groups over every Hilbertian field.

2.1 Wreath Products

We prove that every Galois extension N/GK over a Hilbertian field K can be embedded into a Galois extension with a wreath product $H \wr G$ as Galois group, if only H possesses a G -realization over K . Since $K(t)$ is Hilbertian we can assume without loss of generality that the involved G -realization is a G -realization of one variable. In the next proposition, \mathbf{t}^G denotes a generating system of $K(\mathbf{t})^G/K$ according to III.(3.21).

Proposition 2.1. *Let K be a field, H a finite group with G -realization of one variable over K , and G a permutation group of degree r . Then there exists a geometric Galois extension M over the unirational field $K(\mathbf{t}^G)$ with*

$$\text{Gal}(M/K(\mathbf{t}^G)) \cong H \wr G \quad \text{and} \quad \text{Gal}(M/K(\mathbf{t})) \cong H^r. \quad (2.1)$$

Proof. Let $N/HK(t)$ be a geometric Galois extension, $x \in N$ a primitive element of $N/K(t)$ and $f(t, X)$ the minimal polynomial of x over $K(t)$. If t_1, \dots, t_r denote algebraically independent transcendentals over K , $K(\mathbf{t}) := K(t_1, \dots, t_r)$ and x_i a zero of $f(t_i, X)$ for $i = 1, \dots, r$ in an algebraic closure of $K(\mathbf{t})$, then $M := K(\mathbf{t}, \mathbf{x})$ with $\mathbf{x} = (x_1, \dots, x_r)$ is a geometric Galois extension of $K(\mathbf{t})$ with

$$\text{Gal}(M/K(\mathbf{t})) = \prod_{i=1}^r H_i \cong H^r,$$

where $H_i = \text{Gal}(M/K(\mathbf{t}, \mathbf{x}_i^\vee)) \cong H$ and $\mathbf{x}_i^\vee = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_r)$. Any $\sigma \in G$ permutes the transcendentals t_i via $t_i^\sigma := t_{(i)\sigma}$ and thus induces an automorphism of $K(\mathbf{t})/K$. The set of these automorphisms forms a subgroup of $\text{Aut}(K(\mathbf{t})/K)$ with the unirational fixed field $K(\mathbf{t}^G)$. Since every extension $\tilde{\sigma}$ of $\sigma \in \text{Gal}(K(\mathbf{t})/K(\mathbf{t}^G))$ to M permutes the zeroes of the polynomials $f(t_i, X)$, we have $\tilde{\sigma} \in \text{Aut}(M/K(\mathbf{t}^G))$ and $M/K(\mathbf{t}^G)$ is Galois. Obviously $\prod_{i=1}^r H_i$ is normal in $\tilde{G} := \text{Gal}(M/K(\mathbf{t}^G))$. The group of those $\tilde{\sigma} \in \tilde{G}$ permuting x_1, \dots, x_r forms a complement isomorphic to G of $\prod_{i=1}^r H_i$ in \tilde{G} which permutes the factors H_i by conjugation inside \tilde{G} according to $H_i^{\tilde{\sigma}} = H_{(i)\sigma}$. Consequently we have $\tilde{G} \cong H \wr G$. \square

Since $K(\mathbf{t}^G)$ is not in general a rational function field, Proposition 2.1 and the Hilbert irreducibility theorem alone do not suffice to obtain Galois extensions over K with wreath products as Galois groups.

Theorem 2.2. *Let K be a field, H a finite group with G -realization in one variable over K , G a transitive subgroup of S_r , $\tilde{G} \cong H \wr G$ and $\kappa : \tilde{G} \rightarrow G$ the canonical epimorphism. Then every embedding problem $\mathcal{E}(\varphi, \kappa)$ with epimorphism $\varphi : \Gamma_K \rightarrow G$ possesses a regular proper solution.*

Proof. Let N be the fixed field of $\ker(\varphi)$ with $\text{Gal}(N/K) = G$ and t_1, \dots, t_r algebraically independent transcendentals over K . Further let $K(\mathbf{t}^G)$ and M be the same fields as those in the proof of Proposition 2.1 with $\text{Gal}(M/K(\mathbf{t}^G)) \cong H \wr G$. Then the composite $\tilde{M} := NM$ is also Galois over $K(\mathbf{t}^G)$ with the group

$$D := \text{Gal}(\tilde{M}/K(\mathbf{t}^G)) \cong \text{Gal}(\tilde{M}/N(\mathbf{t}^G)) \times \text{Gal}(\tilde{M}/M) \cong (H \wr G) \times G.$$

Denoting by σ_N respectively $\sigma_{K(\mathbf{t})}$ the representation of $\sigma \in G$ as element of $\text{Gal}(N/K)$ resp. of $\text{Gal}(K(\mathbf{t})/K(\mathbf{t}^G))$, we see that

$$\tilde{G} := \{\delta \in D \mid \delta|_N = \sigma_N, \delta|_{K(\mathbf{t})} = \sigma_{K(\mathbf{t})} \text{ for some } \sigma \in G\}$$

is a subgroup of D isomorphic to $H \wr G$, since any $\bar{\delta} \in \text{Gal}(M/K(\mathbf{t}^G))$ extends to a unique $\delta \in \tilde{G}$. By definition of \tilde{G} the fixed field $\tilde{M}^{\tilde{G}}$ is regular over K with $N\tilde{M}^{\tilde{G}} = N(\mathbf{t})$. Since moreover the N -vector space $U := \bigoplus_{i=1}^r Nt_i$ is \tilde{G} -invariant, $\tilde{M}^{\tilde{G}}$ is a purely transcendental function field over K by Speiser's Lemma (Proposition III.3.10), say $\tilde{M}^{\tilde{G}} = K(\mathbf{v})$.

Now set $K^* := K(\mathbf{v})$, $N^* := N(\mathbf{v}) = N(\mathbf{t})$ and $\mathcal{E}(\varphi^*, \kappa^*)$ the embedding problem lifted from $\mathcal{E}(\varphi, \kappa)$ to N^*/K^* . Then the canonical epimorphism $\tilde{\varphi}^* : \Gamma_{K^*} \rightarrow \text{Gal}(\tilde{M}/K^*) \cong \tilde{G}$ satisfies $\kappa^* \circ \tilde{\varphi}^* = \varphi^*$. Thereby $\tilde{\varphi}^*$ is a proper solution of $\mathcal{E}(\varphi^*, \kappa^*)$ and hence a regular proper solution of the original embedding problem $\mathcal{E}(\varphi, \kappa)$. \square

Special cases of this theorem can already be found in Kuyk (1970), Prop. 1, and Saltman (1982), Thm. 3.12(d).

2.2 Split Extensions with Abelian Kernel

From the embedding theorem for wreath products we can immediately deduce an embedding theorem for semidirect products with abelian kernel, using the following group theoretical result (see for example Suzuki (1982), Ch. 2, Thm. 10.10):

Proposition 2.3. *Let $\tilde{G} = H \rtimes G$ be a semidirect product of a finite abelian group H with a finite group G of order r . Then \tilde{G} is isomorphic to the factor group of the regular wreath product $H \wr G$ by a normal subgroup U contained in the base group H^r :*

$$\tilde{G} \cong (H \wr G)/U \quad \text{with} \quad U \leq H^r. \tag{2.2}$$

This fact together with Theorem 2.2 and the existence of G-realizations for finite abelian groups allows to deduce the following embedding theorem, which in the case of number fields already goes back to Scholz (1929), in the case of Hilbertian fields to Uchida (1980) and in the geometric case to Saltman (1982):

Theorem 2.4. *Over any field every finite split embedding problem with abelian kernel has a regular proper solution.*

In particular every finite split (geometric) embedding problem with abelian kernel over a Hilbertian field K (function field K/k) has a (geometric) proper solution.

Proof. Let N/GK be a Galois extension with epimorphism $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = H \rtimes G$ a semidirect product of H with G and the projection $\kappa : \tilde{G} \rightarrow G$, so that we have to solve the embedding problem $\mathcal{E}(\varphi, \kappa)$. For this, let $W := H \wr G$ be the regular wreath product with the canonical epimorphism $\lambda : W \rightarrow G$. Since by Theorem I.5.1 respectively Theorem III.4.5 and Corollary III.4.8 with Corollary 1.7 every finite abelian group has a G-realization over \mathbb{Q} as well as over \mathbb{F}_p , by extension of constants it has a G-realization over K . So all assumptions for $\mathcal{E}(\varphi, \lambda)$ in Theorem 2.2 are satisfied. Thus $\mathcal{E}(\varphi, \lambda)$ possesses a regular proper solution ψ^* with $\lambda^* \circ \psi^* = \varphi^*$, where $\mathcal{E}(\varphi^*, \lambda^*)$ denotes the corresponding lifted embedding problem.

Now let K^* be the fixed field of $\text{im}(\varphi^*)$ and M^* the solution field corresponding to ψ^* . Then

$$\text{Gal}(M^*/K^*) \cong W = H \wr G.$$

By Proposition 2.3 the wreath product W has a normal subgroup $U \leq H^r$ with $W/U \cong \tilde{G}$. The fixed field $\tilde{N}^* := (M^*)^U$ then contains $N^* = NK^*$ and is Galois over K^* with group

$$\text{Gal}(\tilde{N}^*/K^*) \cong \tilde{G} = H \rtimes G.$$

We denote by $\tilde{\kappa}^*$ the restriction map from $\text{Gal}(M^*/K^*)$ onto $\text{Gal}(\tilde{N}^*/K^*)$. Then with $\tilde{\varphi}^* := \tilde{\kappa}^* \circ \psi^*$ we have

$$\kappa^* \circ \tilde{\varphi}^* = \lambda^* \circ \psi^* = \varphi^*,$$

and $\tilde{\varphi}^*$ is a proper solution of the embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$. Hence $\tilde{\varphi}^*$ is a regular proper solution of the original embedding problem $\mathcal{E}(\varphi, \kappa)$.

The application to ordinary and geometric solutions of embedding problems over Hilbertian fields follows immediately from Theorem 1.5. \square

Using the reduction theorem of Ikeda (Theorem 1.9 and Corollary 1.10) in addition to the above result we obtain:

Corollary 2.5. *If a finite embedding problem with abelian kernel over a Hilbertian field K possesses an ordinary (geometric/regular) solution, then it also possesses a corresponding proper solution.*

Since over fields with projective Galois group (improper) solutions of finite embedding problems always exist, induction over a chief series yields from Corollary 2.5:

Theorem 2.6 (Iwasawa (1953)). *Let K be a Hilbertian field with projective absolute Galois group. Then every finite embedding problem over K with solvable kernel has a proper solution.*

Proof. Let N/K be a finite Galois extension with epimorphism $\varphi : \Gamma_K \rightarrow G = \text{Gal}(N/K)$ and $\tilde{G} = H \cdot G$ a group extension with finite solvable kernel and canonical epimorphism $\kappa : \tilde{G} \rightarrow G$. Further let H_1 be maximal with respect to inclusion among the normal subgroups of \tilde{G} properly contained in H and $\tilde{G}_1 := \tilde{G}/H_1$. Then H/H_1 is a chief factor of \tilde{G} and hence a finite abelian group. Since Γ_K is projective by assumption, it follows from Corollary 2.5 that the embedding problem $\mathcal{E}(\varphi, \kappa_1)$ with canonical epimorphism $\kappa_1 : \tilde{G}_1 \rightarrow G$ has a proper solution $\tilde{\varphi}_1$. Replacing G by \tilde{G}_1 and H by H_1 we may inductively continue until $\tilde{G}_s = \tilde{G}$. Then $\kappa = \kappa_1 \circ \dots \circ \kappa_s$, and $\tilde{\varphi} := \tilde{\varphi}_s$ is a proper solution of $\mathcal{E}(\varphi, \kappa)$. \square

In the next section we shall give a group theoretic characterization of those groups which can be realized as Galois groups by successive solution of split embedding problems with abelian kernel and passage to Galois intermediate fields.

2.3 Semiabelian Groups

A group G is called a *semiabelian group* if it is generated by a finite set of abelian subgroups A_i

$$G = \langle A_1, \dots, A_n \rangle \quad \text{with} \quad A_i \leq \mathcal{N}_G(A_j) \text{ for } i \leq j. \quad (2.3)$$

The following theorem contains the characterizations of semiabelian groups which are of interest to us (see Stoll (1995) for a further characterization):

Theorem 2.7 (Dentzer (1995b)). *For a finite group $G \neq 1$ the following are equivalent:*

- (a) G is semiabelian.
- (b) G possesses an abelian normal subgroup A and a semiabelian proper subgroup U with $G = AU$.
- (c) G can be constructed in infinitely many steps, starting from the trivial group, of semidirect products with a finite abelian kernel and taking factor groups.

Proof. If $G = \langle A_1, \dots, A_n \rangle$, where without loss of generality we may assume $A_n \not\leq \langle A_1, \dots, A_{n-1} \rangle$, is a semiabelian group, then $A := A_n$ is an abelian normal subgroup and $U := \langle A_1, \dots, A_{n-1} \rangle$ by (2.3) is a semiabelian proper subgroup of G .

If (b) holds, the action of U on A defines a homomorphism $\varphi : U \rightarrow \text{Aut}(A)$ and thus a semidirect product $A \rtimes U$ with finite abelian kernel. Now via the epimorphism

$$\psi : A \rtimes U \rightarrow G, \quad (\sigma, \tau) \mapsto \sigma\tau,$$

G is isomorphic to a factor group of $A \rtimes U$. Thus (c) follows by descending induction on the order of U .

Now let G be constructed according to (c) in a finite number of steps taking factor groups of semidirect products with abelian kernel, say as the last member of a finite sequence of quotients $G_i := (A_i \rtimes G_{i-1}) / N_i$ with A_i abelian and $G_0 = 1$. Let $G = (A_n \rtimes G_{n-1}) / N_n$ with minimal n . Then G cannot be a factor group of G_{n-1} , since otherwise G could also be obtained as factor of $A_{n-1} \rtimes G_{n-2}$ in contradiction to the minimality of n . Hence $\bar{A}_n := A_n N_n / N_n$ is an abelian normal subgroup and $\bar{G}_{n-1} := G_{n-1} N_n / N_n$ a proper subgroup of G with $G = \bar{G}_{n-1} \bar{A}_n = \langle \bar{G}_{n-1}, \bar{A}_n \rangle$. Since herein by construction \bar{G}_{n-1} can be obtained in at most $n - 1$ steps as factor group of a semidirect product with abelian kernel, (2.3) follows with \bar{A}_n in place of A_n by descending induction on n . \square

From this characterization we immediately obtain from Theorem 2.4:

Corollary 2.8. *Finite semiabelian groups possess G -realizations over any field and therefore are Galois groups over every Hilbertian field.*

In view of this result it is natural to ask which groups lie in the class of semiabelian groups. A partial answer is given by:

Proposition 2.9 (Thompson (1986)). (a) *Finite groups G of nilpotency class 2, i.e., with $G' \leq \mathcal{Z}(G)$, are semiabelian.*

(b) *Finite solvable groups G with only abelian Sylow subgroups are semiabelian.*

Proof. Since the properties of G in (a) and (b) also hold for every subgroup, the proof can in both cases be done by induction over the group order.

For (a), let U denote a maximal and hence semiabelian subgroup of G . Then the group A generated by a $\sigma \in G \setminus U$ and $\mathcal{Z}(G)$ is an abelian subgroup of G with $AU = G$. As $G/\mathcal{Z}(G)$ is abelian by assumption, A is even normal. Thus G is semiabelian by Theorem 2.7(b).

For (b), let F be the Fitting subgroup of G , i.e., the maximal nilpotent normal subgroup. Being nilpotent, F is the direct product of its Sylow subgroups and hence by assumption abelian. Since for $G \neq 1$ the Frattini subgroup $\Phi(G)$ is a proper subgroup of F (Huppert (1967), Ch. III, Satz 4.2(c)), G possesses a maximal and by induction semiabelian subgroup U with $FU = G$. This proves part (b). \square

In the particular case of p -groups this leads to:

Corollary 2.10 (Dentzer (1995b)). *Let p be a prime.*

(a) *All groups of order p^n with $n \leq 4$ are semiabelian.*

(b) *The groups of order 2^5 are semiabelian.*

Proof. Groups of order p or p^2 are abelian, those of order p^3 of nilpotency class at most 2. If $|G| = p^4$, then G has a maximal abelian normal subgroup A of order $|A| = p^a$ and $8 \leq a(a+1)$ and thus $a \geq 3$ (Huppert (1967), Ch. III, Satz 7.3(b)). If G is non-abelian, it possesses a maximal subgroup $U \neq A$ with $AU = G$ which proves (a).

Part (b) of the corollary follows by explicit verification of the condition in Theorem 2.7(b) for all 51 isomorphism types of groups of order 32. \square

Unfortunately among the groups of order p^5 for $p \neq 2$ and among those of order 2^6 there exist some which are not semiabelian (see Dentzer ([1995b](#)), Prop. 2.10 and App. A).

3 Embedding Problems with Centerless Kernel

We study embedding problems over Hilbertian fields K in which the kernel H has trivial center. If here H possesses a GA-realization over K with an additional rationality condition, then every embedding problem over K with this kernel and even with kernel H^r is solvable. The latter can be used via induction over a chief series for the realization of groups as Galois groups whose composition factors possess a GAR-realization over K as defined below. Finally the methods presented here allow us to prove that the absolute Galois groups of Hilbertian PAC-fields are free.

3.1 The Notion of GAR-Realization

The notion of a GA-realization was already introduced in Section I.5.2: $\text{Gal}(N/K)$ is called a GA-realization of H over k , if N/K is a geometric Galois extension with group H over a rational function field K/k , which is part of a geometric (with respect to k) Galois extension with group $A := \text{Aut}(H)$ (under identification of H with $\text{Inn}(H)$, which is only possible in case $\mathcal{L}(H) = 1$). Here N^A/k does not necessarily have to be rational. Such a GA-realization is called a *GAR-realization of H over k* if in addition the following rationality condition is satisfied:

(R): Every finite extension field R/N^A with $\bar{k}R = \bar{k}K$ is a rational function field over the algebraic closure of k in R .

(Here \bar{k} denotes the algebraic closure of k in an algebraic closure of K .) Sufficient criteria for the validity of (R) will be discussed in the next paragraph.

The advantage of this notion of GAR-realization lies in the following easy group theoretic fact (see for example Suzuki (1982), Ch. 2, Thm. 7.11):

Proposition 3.1. *Let $\tilde{G} = H \cdot G$ be a group extension of a centerless finite group H with a finite group G . Then \tilde{G} is isomorphic to a subgroup U of $\text{Aut}(H) \times G$ with*

$$U \cap \text{Aut}(H) = \text{Inn}(H) \quad \text{and} \quad p_2(U) = G \tag{3.1}$$

(where p_2 denotes the projection onto the second factor.)

This proposition leads to the following embedding theorem:

Theorem 3.2. *Let K be a field and H a finite group with GAR-realization over K . Then every finite embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with kernel H possesses a regular proper solution.*

In particular, such ordinary (geometric) embedding problems over a Hilbertian field always possess (geometric) proper solutions.

Proof. Let N/GK be a finite Galois extension with epimorphism $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = G \cdot H$ a group extension with canonical epimorphism $\kappa : \tilde{G} \rightarrow G$. According to

the automorphism condition (A) there exists a geometric Galois extension $M/K(\mathbf{t})$ with $\text{Aut}(M/K) \geq A \cong \text{Aut}(H)$, where moreover $K(\mathbf{t})$ is the fixed field of the subgroup $\text{Inn}(H) \cong H$ of A . Denote the composite of N with M respectively with M^A in an algebraic closure of M by \tilde{M} resp. \tilde{M}^A . Then \tilde{M}/M^A is Galois with

$$\text{Gal}(\tilde{M}/M^A) = \text{Gal}(\tilde{M}/\tilde{M}^A) \times \text{Gal}(\tilde{M}/M) \cong \text{Aut}(H) \times G. \quad (3.2)$$

By Proposition 3.1 the group \tilde{G} is isomorphic to a subgroup U of $\text{Aut}(H) \times G$ with property (3.1). Consequently the fixed field $R := \tilde{M}^U$ is a geometric extension field of M^A with $NR = N(\mathbf{t})$. The rationality condition (R) now implies that R/K is a rational function field. Since N is algebraically closed inside \tilde{M} , the canonical epimorphism $\tilde{\varphi}^* : \Gamma_R \rightarrow \text{Gal}(\tilde{M}/R)$ yields a regular proper solution of $\mathcal{E}(\varphi, \kappa)$.

The application to ordinary and geometric embedding problems as usual follows immediately from Theorem 1.5. \square

Furthermore, by induction over a normal series Theorem 3.2 yields:

Corollary 3.3. *Let K be a Hilbertian field and G a finite group which has a normal series*

$$G \triangleright G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$$

with the following properties:

- (1) G/G_0 is isomorphic to the Galois group of a Galois extension N_0/K .
- (2) G_{i-1}/G_i has a GAR-realization over K for $i = 1, \dots, n$.

Then there exists a Galois extension N/K with $\text{Gal}(N/K) \cong G$.

If here K/k is an algebraic function field and N_0/K a geometric Galois extension, then there exists a geometric Galois extension N/K with $\text{Gal}(N/K) \cong G$.

Proof. Let G/G_{i-1} be isomorphic to the Galois group of a (geometric) Galois extension N_{i-1}/K and $H := G_{i-1}/G_i$. Then by Theorem 3.2 there exists a (geometric) Galois extension N_i/K with $\text{Gal}(N_i/K) \cong G/G_i$. Thus Corollary 3.3 is obtained from Theorem 3.2 by induction on i . \square

Remark. In the proofs of Theorem 3.2 and Corollary 3.3 the rationality condition (R) was only used to guarantee that every geometric extension field R/N^A with $\bar{k}R = \bar{k}K$ is a rational function field over k (compare to the definition in Matzat (1985b) resp. Matzat (1987), Ch. IV, §4).

3.2 Embedding Problems with Characteristically Simple Kernel

To obtain an assertion in the form of Corollary 3.3, in which the assumption on the factors of a normal series are replaced by the corresponding, but much more easily verifiable assumptions on the composition factors, we first have to solve embedding problems with characteristically simple non-abelian kernel. The first step is given by:

Proposition 3.4. *Let K be a field and H a finite non-abelian simple group with GA-realization over K . Then the r -fold direct product H^r possesses a GA-realization over K .*

Proof. In the proof let $A := \text{Aut}(H)$ and $\bar{A} := \text{Out}(H)$. By assumption H has a GA-realization over K , i.e., there exists a tower of geometric Galois extensions $N \geq K(\mathbf{t}) \geq K(\mathbf{t})^{\bar{A}}$, $\mathbf{t} = (t_1, \dots, t_s)$ a system of independent transcendentals, with $\text{Gal}(N/K(\mathbf{t})) \cong H$ and $\text{Gal}(N/K(\mathbf{t})^{\bar{A}}) \cong A$. Further let $f(\mathbf{t}, X) \in K(\mathbf{t})[X]$ resp. $g(\mathbf{u}, X) \in K(\mathbf{u})[X]$ be minimal polynomials of primitive elements of $N/K(\mathbf{t})$ resp. $N/K(\mathbf{u})$, where $\mathbf{u} = (u_1, \dots, u_q)$ with $u_j = h_j(\mathbf{t}) \in K(\mathbf{t})$ is a generating system of the unirational function field $K(\mathbf{t})^{\bar{A}}/K$. If now $\underline{\mathbf{t}} := (\mathbf{t}_1, \dots, \mathbf{t}_r)$ with $\mathbf{t}_i = (t_{i1}, \dots, t_{is})$ is a system of rs over K independent transcendentals, then the zeroes of $f(\mathbf{t}_i, X) \in K(\mathbf{t}_i)[X]$ generate fields $N_i/K(\mathbf{t}_i)$ in an algebraic closure of $K(\mathbf{t}_1, \dots, \mathbf{t}_r)$, with $H_i := \text{Gal}(N_i/K(\mathbf{t}_i)) \cong H$ and

$$\text{Gal}(M/K(\underline{\mathbf{t}})) \cong \prod_{i=1}^r H_i \cong H^r \quad (3.3)$$

for the composite $M := N_1 \cdots N_r$. For the fixed field $N_i^{A_i}$ of N_i under the action induced by A we write $K(\mathbf{u}_i) := K(\mathbf{t}_i)^{\bar{A}_i}$ with $u_{ij} = h_j(\mathbf{t}_i) \in K(\mathbf{t}_i)$. Then with $\underline{\mathbf{u}} := (\mathbf{u}_1, \dots, \mathbf{u}_r)$ we further have

$$\text{Gal}(M/K(\underline{\mathbf{u}})) \cong \prod_{i=1}^r A_i \cong A^r. \quad (3.4)$$

Since H is non-abelian simple the automorphism group of H^r is the wreath product of A with the symmetric group S_r :

$$\text{Aut}(H^r) \cong A \wr S_r \cong A^r \rtimes S_r. \quad (3.5)$$

An action of $\sigma \in S_r$ on $K(\underline{\mathbf{u}})$ is obtained in a natural way by restriction to $K(\underline{\mathbf{u}})$ of the automorphisms of $K(\underline{\mathbf{t}})$ given by the action $t_{ij}^\sigma := t_{(i)\sigma,j}$. Since the restriction $\bar{\sigma}$ satisfies

$$u_{ij}^{\bar{\sigma}} = h_j(\mathbf{t}_i^\sigma) = h_j(\mathbf{t}_{(i)\sigma}) = u_{(i)\sigma,j} \quad (3.6)$$

and hence permutes the fields $K(\mathbf{u}_i)$ according to $K(\mathbf{u}_i)^{\bar{\sigma}} = K(\mathbf{u}_{(i)\sigma})$, this yields a faithful representation of S_r into $\text{Aut}(K(\underline{\mathbf{u}})/K)$, whose fixed field will be denoted by F .

By (3.6) all extensions $\tilde{\sigma}$ of $\bar{\sigma} \in \text{Gal}(K(\underline{\mathbf{u}})/F)$ onto M only interchange the zeroes of $g(\mathbf{u}_i, X) \in K(\mathbf{u}_i)[X]$ for $i = 1, \dots, r$, so M/F is Galois. By fixing extensions of $\tilde{\sigma}$ which permute a given system of representatives of the zeroes of $g(\mathbf{u}_i, X)$ we thus obtain a complement to A^r in $\text{Gal}(M/F)$, and easily verify

$$\text{Gal}(M/F) \cong A^r \rtimes S_r \cong A \wr S_r \cong \text{Aut}(H^r). \quad (3.7)$$

Since here the purely transcendental function field $K(\underline{\mathbf{t}})$ occurs as the fixed field of $\text{Inn}(H^r) \cong H^r$, $\text{Gal}(M/K(\underline{\mathbf{t}}))$ yields a GA-realization of H^r . \square

After these preparations we come to the embedding theorem for characteristically simple kernel:

Theorem 3.5. *Let K be a field and $\prod_{i=1}^r H_i \cong H^r$ a characteristically simple finite group whose simple factor H is non-abelian and has a GAR-realization over K . Then every finite embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with kernel H^r has a regular proper solution.*

In particular, such ordinary (geometric) embedding problems over a Hilbertian field always possess proper (geometric) solutions.

Proof. Let N/GK be a finite Galois extension with epimorphism $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = H^r \cdot G$ a group extension with canonical epimorphism $\kappa : \tilde{G} \rightarrow G$. By Theorem 1.6(c) we can in addition assume without loss of generality that H^r is a minimal normal subgroup of \tilde{G} and hence G acts transitively on the set $\{H_1, \dots, H_r\}$ of direct factors of H^r .

The notations M , $K(\underline{\mathbf{t}})$, $K(\underline{\mathbf{u}})$ and F , as well as N_i , H_i and A_i , are used as in the proof of Proposition 3.4. Further let $\tilde{M} := NM$ be the composite of N and M in an algebraic closure of M . Then \tilde{M}/F is Galois with

$$\text{Gal}(\tilde{M}/F) = \text{Gal}(\tilde{M}/NF) \times \text{Gal}(\tilde{M}/M) \cong \text{Aut}(H^r) \times G. \quad (3.8)$$

By Proposition 3.1 there exists a subgroup U of $\text{Gal}(\tilde{M}/F)$ isomorphic to \tilde{G} , whose fixed field $R := \tilde{M}^U$ is a geometric extension field of F/K with $NR = N(\underline{\mathbf{t}})$. It remains to establish that R/K is a rational function field.

In what follows we identify U with \tilde{G} and U/H^r with G . Moreover the normalizer of H_i in \tilde{G} is denoted by C_i . First we prove that the fixed field \tilde{M}^D of $D := \cap_{i=1}^r C_i$ is a rational function field over N^D , where N^D denotes the fixed field of the group D restricted to N . From the assumptions it follows that the Galois group of the field extension $K_1 N_1 / K_1(\mathbf{t}_1)$ obtained from $N_1/K(\mathbf{t}_1)$ by extension of constants with $K_1 := N^{C_1}$ is a GAR-realization of H_1 over K_1 , where $K_1(\underline{\mathbf{u}}_1)$ is the unirational fixed field of $A_1 \cong \text{Aut}(H_1)$. \tilde{G} permutes the generating systems $\underline{\mathbf{u}}_1, \dots, \underline{\mathbf{u}}_r$ of $K(\underline{\mathbf{u}}_i)/K$ according to (3.6). This implies that u_{11}, \dots, u_{1q} are elements of \tilde{M}^{C_1} , and the subfield $N(\mathbf{t}_1)$ of $N(\underline{\mathbf{t}})$ remains invariant under C_1 . The fixed field $N(\mathbf{t}_1)^{C_1}$ is thus a geometric extension field of $K_1(\underline{\mathbf{u}}_1)$, whose composite with N yields the field $N(\mathbf{t}_1)$. From the rationality condition (R) for H_1 now follows that $N(\mathbf{t}_1)^{C_1}$ is a rational function field over K_1 , say $N(\mathbf{t}_1)^{C_1} = K_1(\mathbf{v}_1)$ with a transcendence basis $\mathbf{v}_1 = (v_{11}, \dots, v_{1s})$. As the permutation representation of \tilde{G} on $\{H_1, \dots, H_r\}$ is transitive, there exist elements $\sigma_i \in G$ for $i = 1, \dots, r$ with $(1)\sigma_i = i$. Then the transcendence basis $\{\mathbf{v}_i := \mathbf{v}_1^{\sigma_i} \mid i = 1, \dots, r\}$ is C_i -invariant, and as $D = \cap_{i=1}^r C_i$ we see that $v_{ij} \in \tilde{M}^D$ for $1 \leq i \leq r$, $1 \leq j \leq s$. Moreover $N(\mathbf{v}_i) = N(\mathbf{t}_i)$, so $\underline{\mathbf{v}} := (\mathbf{v}_1, \dots, \mathbf{v}_r)$ forms a system of r,s independent transcendentals over N^D . In addition to the inclusion $N^D(\underline{\mathbf{v}}) \leq \tilde{M}^D \leq N(\underline{\mathbf{t}})$ we have the degree estimates

$$[N(\underline{\mathbf{t}}) : \tilde{M}^D] \geq [N : N^D] = [N(\underline{\mathbf{v}}) : N^D(\underline{\mathbf{v}})],$$

which due to $N(\underline{\mathbf{t}}) = N(\underline{\mathbf{v}})$ implies $\tilde{M}^D = N^D(\underline{\mathbf{v}})$. By construction every $\sigma \in G = \text{Gal}(N(\underline{\mathbf{v}})/R)$ permutes the transcendence basis v_{ij} according to $v_{ij}^\sigma = v_{(i)\sigma,j}$. In particular the N -vector space $\bigoplus_{i=1}^r \bigoplus_{j=1}^s N v_{ij}$ is G -invariant. Since moreover by the above R/K is geometric with $NR = N(\underline{\mathbf{v}}) = N(\underline{\mathbf{t}})$, it follows from Speiser's Lemma (Proposition III.3.10) that R/K is a rational function field. Now N is algebraically closed in \tilde{M} , so $\tilde{\varphi}^* : \Gamma_R \rightarrow \text{Gal}(\tilde{M}/R)$ gives a regular proper solution of $\mathcal{E}(\varphi, \kappa)$.

The assertion about ordinary and geometric embedding problems again follows by application of Theorem 1.5. \square

Theorem 3.5 is suited for induction proofs along a chief series. A first result is given in:

Theorem 3.6 (Embedding Theorem for Centerless Kernel). *Let K be a Hilbertian field and H a finite group whose composition factors have GAR-realizations over K . Then every finite embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with kernel H possesses a proper solution.*

If here the embedding problem is geometric, it even has a geometric proper solution.

Proof. Let N/GK be a finite (geometric) Galois extension with restriction $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = H \cdot G$ a group extension with the canonical epimorphism $\kappa : \tilde{G} \rightarrow G$. Furthermore let H_1 be maximal with respect to inclusion among the normal subgroups of \tilde{G} properly contained in H and $\tilde{G}_1 := \tilde{G}/H_1$. Then H/H_1 is a chief factor of \tilde{G} and hence a characteristically simple group. By assumption the simple factors of H/H_1 are non-abelian and possess a GAR-realization over K . It now follows from Theorem 3.5 that the embedding problem $\mathcal{E}(\varphi, \kappa_1)$ with the canonical epimorphism $\kappa_1 : \tilde{G}_1 \rightarrow G$ has a (geometric) proper solution $\tilde{\varphi}_1$. Replacing G by \tilde{G}_1 and H by H_1 we may inductively continue until $\tilde{G}_s = \tilde{G}$. Then $\kappa = \kappa_1 \circ \dots \circ \kappa_s$, and $\tilde{\varphi} := \tilde{\varphi}_s$ is a (geometric) proper solution of $\mathcal{E}(\varphi, \kappa)$. \square

In the special case $G = 1$ Theorem 3.6 yields:

Corollary 3.7. *Let K be a Hilbertian field and H a finite group whose composition factors have GAR-realizations over K . Then H possesses a G -realization over K .*

In the next paragraph we hence study the question of which simple groups can be shown to have GAR-realizations over \mathbb{Q} or at least over \mathbb{Q}^{ab} . But first we apply the methods developed so far to determine the Galois groups of Hilbertian PAC-fields. Clearly, for these fields the verification of the rationality condition (R) is not necessary.

3.3 Galois Groups of Hilbertian PAC-Fields

To be able to apply the Theorem of Conway and Parker (Thm. III.6.10) also to the solution of embedding problems, these have to be reduced to the case where the

Schur multiplier of the kernel is generated by commutators. The decisive induction step is achieved in the next proposition.

Proposition 3.8. *Let K be a field. Then every finite split embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with non-abelian characteristically simple kernel H can be reduced to a split embedding problem $\mathcal{E}(\varphi, \tilde{\kappa})$, whose kernel \tilde{H} has trivial center as well as trivial Schur multiplier.*

Proof. In the proof we follow the outline of the proof of Proposition III.6.12. As usual let $G := \text{im}(\varphi)$ and \tilde{G} be the inverse image of κ , so that $\tilde{G} = H \rtimes G$ by assumption. Obviously the action of G on H defined by the semidirect product can be lifted in a unique way to an action on the universal central extension R of H . In this way we obtain a semidirect product $E := R \rtimes G$ with canonical epimorphism $\psi : E \rightarrow \tilde{G}$. As in the proof of Proposition III.6.12 let S be a finite non-abelian simple group with trivial Schur multiplier (say $S = \text{SL}_2(8)$), and $\tilde{E} := S \wr E = S^e \rtimes E$ with $e := |E|$ the regular wreath product with canonical epimorphism $\tilde{\psi} : \tilde{E} \rightarrow E$. Then E acts on S^e by permutation of the factors in the regular permutation representation and we have

$$\tilde{E} = S^e \rtimes E = S^e \rtimes (R \rtimes G) = (S^e \rtimes R) \rtimes G = \tilde{H} \rtimes G$$

with $\tilde{H} := S^e \rtimes R$ and $\mathcal{Z}(\tilde{H}) = 1$. Since both S and R are perfect groups with trivial Schur multiplier, the Schur multiplier $M(\tilde{H})$ is also trivial, as can easily be seen.

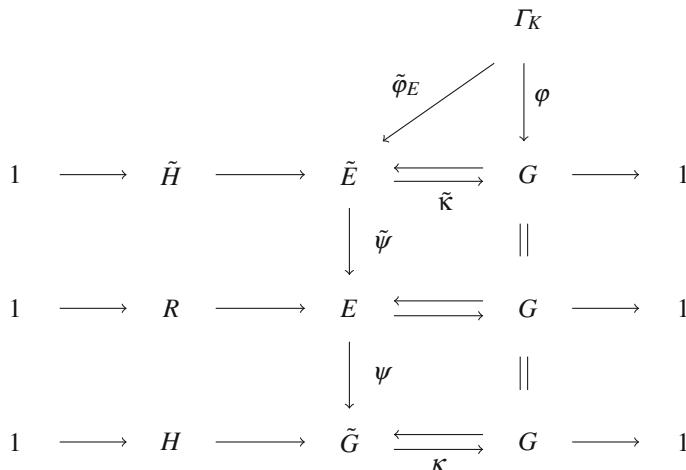


Fig. 3.1 Trivializing the Schur multiplier

The embedding problem $\mathcal{E}(\varphi, \tilde{\kappa})$ with $\tilde{\kappa} := \kappa \circ \psi \circ \tilde{\psi}$ is hence split with kernel \tilde{H} , where moreover $\mathcal{Z}(\tilde{H}) = M(\tilde{H}) = 1$. But this proves the assertion, since every (proper) solution $\tilde{\varphi}_E$ of $\mathcal{E}(\varphi, \tilde{\kappa})$ yields a (proper) solution $\tilde{\varphi} := \psi \circ \tilde{\psi} \circ \tilde{\varphi}_E$

of $\mathcal{E}(\varphi, \kappa)$. Furthermore geometric respectively regular solutions of $\mathcal{E}(\varphi, \tilde{\kappa})$ lead to geometric resp. regular solutions of $\mathcal{E}(\varphi, \kappa)$. \square

With Proposition 3.8 we are able to prove a pendant to Theorem 3.5 for PAC-fields.

Proposition 3.9. *Let K be a PAC-field of characteristic 0. Then every finite split embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with characteristically simple non-abelian kernel has a regular proper solution.*

Proof. By Proposition 3.8 we can replace $\mathcal{E}(\varphi, \kappa)$ by a finite split embedding problem $\mathcal{E}(\varphi, \tilde{\kappa})$, whose kernel \tilde{H} has trivial center and trivial Schur multiplier. For this let $G = \text{im}(\varphi)$, $N := \bar{K}^{\ker(\varphi)}$ and \tilde{G} the inverse image of $\tilde{\kappa}$.

By the Theorem of Conway and Parker (more precisely, Cor. III.6.11) there exists, for $s \in \mathbb{N}$ large enough, a class vector $\mathbf{C} \in \text{Cl}(\tilde{H})^s$ in which every conjugacy class of \tilde{H} occurs the same number of times and for which $\Sigma(\mathbf{C}^{S_s})/\text{Inn}(\tilde{H})$ forms a single orbit under the full Hurwitz braid group \tilde{H}_s . Let $V \leq S_s$ denote the symmetry group of \mathbf{C} extended by the permutations on the components of \mathbf{C} induced by $A := \text{Aut}(\tilde{H})$. Then $B := \Sigma(\mathbf{C}^V)/\text{Inn}(\tilde{H})$ is a single orbit under H_s^V and A acts on B . By Theorem III.5.10 there exists a geometric Galois extension $N_\sigma^A/K_{\sigma^A}^V$ with

$$\text{Gal}(N_\sigma^A/K_{\sigma^A}^V) \cong A \quad \text{and} \quad \text{Gal}(N_\sigma^A/K_\sigma^V) \cong \tilde{H}.$$

Here $K_{\sigma^A}^V$ and K_σ^V are regular over \mathbb{Q} due to $(\mathbf{C}^*)^V = \mathbf{C}^V$, and we have $N_\sigma^A = N_\sigma$ since $\mathcal{L}(\tilde{H}) = 1$. Consequently $NN_\sigma/KK_{\sigma^A}^V$ is a Galois extension with group

$$\text{Gal}(NN_\sigma/KK_{\sigma^A}^V) \cong A \times G.$$

According to Proposition 3.1 this Galois group contains a subgroup U isomorphic to \tilde{G} , whose fixed field R is regular over K with $NR = NK_\sigma^V$. As intermediate field of $NK_\sigma^V/KK_{\sigma^A}^V$, R is also an intermediate field of $\bar{M}_s(t)/\mathbb{Q}(\mathbf{t}^V)$. Since in this Galois extension $t = t_{s+1}$ remains invariant (as $V \leq S_s$), $R = \mathcal{R}(t)$ with $\mathcal{R} := \bar{M}_s \cap R$, so that

$$\text{Gal}(NN_\sigma/\mathcal{R}(t)) \cong \tilde{G} \quad \text{and} \quad \text{Gal}(NN_\sigma/N\mathcal{R}(t)) \cong \tilde{H}.$$

Now \mathcal{R} is regular over the PAC-field K , so \mathcal{R}/K possesses a rational place \wp for which we can moreover assume that its extension to $N\mathcal{R}/N(t)$ is unramified in the sense of Section III.6.2. Denote by $\tilde{\wp}$ an extension of \wp on NN_σ and by $\tilde{\mathfrak{p}}$ the corresponding valuation ideal. Then by passage to the residue class fields $NN_\sigma\tilde{\mathfrak{p}}/R\mathfrak{p}$ with $\mathfrak{p} := \tilde{\mathfrak{p}} \cap R$ we obtain by Theorem III.6.4 a Galois extension $\tilde{N}/K(t)$ with

$$\text{Gal}(\tilde{N}/K(t)) \cong \tilde{G} \quad \text{and} \quad \tilde{N} \geq N(t).$$

Since here N is algebraically closed inside \tilde{N} , the canonical epimorphism $\tilde{\varphi}^* : \Gamma_{K(t)} \rightarrow \text{Gal}(\tilde{N}/K(t))$ yields a regular proper solution of $E(\varphi, \tilde{\kappa})$. \square

After these preparations we are in a position to prove the main result of this section.

Theorem 3.10 (Fried and Völklein (1992)). *The absolute Galois group of a countable Hilbertian PAC-field of characteristic 0 is free profinite of countable infinite rank.*

Proof. The absolute Galois group Γ_K of a countable Hilbertian PAC-field K has at most countable rank, since K and hence also \bar{K} contain only countably many elements. (Here rank is defined as the cardinality of a minimal set of topological generators, compare Fried and Jarden (1986), Ch. 15.1.) Since split embedding problems with elementary abelian kernel Z_p^n over a Hilbertian field are always properly solvable by Theorem 2.2, the rank of Γ_K cannot be finite. By the Freiheitssatz of Iwasawa (Theorem 1.13) it hence suffices to show that every finite embedding problem over K has a proper solution.

Obviously we may assume that the kernel H of the embedding problem is characteristically simple, since the general case can be reduced to this by induction over a chief series. Since K is a PAC-field, the theorem of Ax (Theorem 1.11(e)) implies that Γ_K is projective profinite and therefore every finite embedding problem over K with kernel H has at least an improper solution. From this the existence of a proper solution can be concluded with the Theorem of Ikeda (Theorem 1.9), if every finite split embedding problem over K with kernel H has a proper solution. The latter now follows from the Theorem of Iwasawa (Theorem 2.6) in the case of abelian kernel, and from Proposition 3.9 and using Theorem 1.5(a) for non-abelian kernel.

□

Remark. In Theorem VI.4.10 we will prove the generalization by Pop (1996) of Theorem 3.10 to positive characteristic using rigid analytic methods.

Since the PAC field $\mathbb{Q}^{\text{tr}}(\sqrt{-1})$ already introduced in Section III.6.4 is Hilbertian by the Theorem of Weissauer (Corollary 1.4) from the Theorem of Fried and Völklein we may conclude:

Corollary 3.11. *The absolute Galois group of $\mathbb{Q}^{\text{tr}}(\sqrt{-1})$ is free profinite of countable infinite rank.*

Corollary 3.11 states a result of the type of the following conjecture due to Šafarevič:

Conjecture of Šafarevič: The absolute Galois group of \mathbb{Q}^{ab} is free profinite of countable infinite rank.

Unfortunately \mathbb{Q}^{ab} is not a PAC field by a result of Frey (see Fried and Jarden (1986), Cor. 10.15). The proof of the conjecture would follow with the results of this section, if every finite non-abelian simple group possessed a GAR-realization over \mathbb{Q}^{ab} . A list of the results obtained so far on this question is contained in the next paragraph.

4 Verification of the GAR-Property

We present sufficient criteria under which a GA-realization of a group is even a GAR-realization. These are then applied to check the rationality condition for the GA-realizations in one and more variables over \mathbb{Q} or over \mathbb{Q}^{ab} constructed so far.

4.1 GAR-Realizations in One Variable

In the first section we give criteria under which a GA-realization in one variable of G over k , i.e., the Galois group $\text{Gal}(N/k(t))$ of a geometric field extension $N/k(t)$ as constructed in Chapters I and II, is in fact a GAR-realization over k . The simplest sufficient condition is furnished by an oddness condition for prime divisors in the ramification locus. In the following let as usually \bar{k} denote the algebraic closure of k in a separable algebraic closure of $K := k(t)$ and $\bar{K} := \bar{k}K$, $\bar{N} := \bar{k}N$, and so on.

Proposition 4.1. *Let $K = k(t)$ be a rational function field in one variable over a perfect field of constants k and $\text{Gal}(N/K)$ a GA-realization of a finite group G over k with fixed field $F = N^{\text{Aut}(G)}$. If F/k contains a prime divisor \mathfrak{Q} of degree 1 whose inertia group in \bar{K}/\bar{F} has odd index in $\text{Gal}(\bar{K}/\bar{F}) \cong \text{Out}(G)$, then $\text{Gal}(N/K)$ is a GAR-realization of G over k .*

Proof. Let R be a field as in condition (R) in Section 3.1. Since \bar{k}/k is separable, we have $g(R/\tilde{k}) = g(\bar{K}/\bar{k}) = 0$, where \tilde{k} denotes the algebraic closure of k in R . By assumption the prime divisor $\mathfrak{Q} \in \text{IP}(F/k)$ splits into an odd number of prime divisors in $\text{IP}(\bar{K}/\bar{k})$, which hence form an orbit of odd length under $\text{Gal}(\bar{K}/F)$. Since $\text{Gal}(\bar{K}/R) \leq \text{Gal}(\bar{K}/F)$, $\text{IP}(\bar{K}/\bar{k})$ contains an orbit of odd length under $\text{Gal}(\bar{K}/R)$, which yields a prime divisor of odd degree in R/\tilde{k} . Thus R/\tilde{k} is a rational function field. \square

For some of the possible groups of outer automorphisms determined in Theorem I.6.2, the assumption formulated in Proposition 4.1 is always satisfied.

Corollary 4.2. *Let $\text{Gal}(N/K)$ be as in Proposition 4.1. Further assume that all prime divisors $\mathfrak{Q} \in \text{IP}(F/k)$ ramified in \bar{K}/F have residue degree 1. If either $\text{Out}(G) = Z_n$ for some $n \in \mathbb{N}$ or $\text{Out}(G) = D_n$ for odd $n \in \mathbb{N}$, then $\text{Gal}(N/K)$ is a GAR-realization of G over k .*

Proof. In the first case the index of the inertia group of the prime divisors ramified of degree n in \bar{K}/\bar{F} equals 1, in the second case it equals n for those ramified of order 2. Hence the corollary is an immediate consequence of Proposition 4.1. \square

With these observations our results on GA-realizations in Theorem II.10.3 imply the following:

Theorem 4.3. *The following simple groups possess GAR-realizations in one variable over \mathbb{Q} (here p always denotes a prime number):*

- (a) *The non-abelian simple alternating groups A_n with $n \neq 6$.*
- (b) *The linear groups $L_2(p)$ for $\left(\frac{a}{p}\right) = -1$, where $a \in \{2, 3, 5, 7\}$.*
- (c) *The linear groups $L_{2n+1}(p)$ for $\gcd(2n+1, p-1) = 1$, $p > 3$ and $p \not\equiv -1 \pmod{12}$.*
- (d) *The unitary groups $U_{2n+1}(p)$ for $\gcd(2n+1, p+1) = 1$, $p > 2$ and $p \not\equiv 1 \pmod{12}$.*
- (e) *The symplectic groups $S_{2n}(p)$ for odd primes $p \not\equiv \pm 1 \pmod{24}$, $p \nmid n$, or for $p = 2$.*
- (f) *The orthogonal groups $O_{2n+1}(p)$ for $n \geq 1$ and odd primes $p \not\equiv \pm 1 \pmod{24}$.*
- (g) *The orthogonal groups $O_{2n}^+(2)$ for $n \geq 5$.*
- (h) *The orthogonal groups $O_{2n}^-(2)$ for $n \geq 3$.*
- (i) *The groups $G_2(p)$.*
- (j) *The groups $F_4(p)$ for $p \geq 5$.*
- (k) *The groups $E_6(p)$ for $p \equiv 5, 17, 23, 35, 44, 47 \pmod{57}$.*
- (l) *The groups ${}^2E_6(p)$ for $p \equiv 3, 10, 13, 22, 34, 40, 52 \pmod{57}$, $p > 3$.*
- (m) *The groups $E_8(p)$ for $p \geq 7$.*
- (n) *The sporadic simple groups with the possible exception of M_{23} .*

Proof. GA-realizations in one variable over \mathbb{Q} for the simple groups listed in the theorem were constructed in Corollary I.5.4 for A_n , in Theorem I.8.9 for $L_2(p)$, and in Theorem III.7.12 for M_{24} . For the remaining groups this assertion is contained in Theorem II.10.3. Since in all cases $\text{Out}(G)$ is either trivial or cyclic of order 2, the assertion follows immediately from Corollary 4.2. \square

4.2 Fields of Constants with Trivial Brauer Group

If the Brauer group $\text{Br}(k)$ of the field of constants, or more precisely its 2-torsion group $\text{Br}_2(k)$ is trivial, the rationality condition (R) is automatically satisfied for every GA-realization in one variable over k . This is a consequence of the following fact, which is a particular case of the Application in Serre (1979), Ch. X, §7 (see also Serre (1964), Ch. III, §2, Ex. 2).

Proposition 4.4. *Let $K = k(t)$ be a rational function field in one variable over a perfect field of constants k of characteristic different from 2 and with $\text{Br}_2(k) = 0$. Then every conic over k has a k -rational point.*

As a consequence of this we obtain:

Corollary 4.5. *Under the assumptions of Proposition 4.4 every GA-realization of a finite group G in one variable over k is a GAR-realization.*

Proof. Since the field R/\tilde{k} in the proof of Proposition 4.1 has genus 0, it is either rational or the function field of a conic without rational points (see for example Artin (1967), Ch. XVI, Thms. 6 and 8). Proposition 4.4 rules out the second possibility, so that in fact R/\tilde{k} is rational. \square

Remark. Corollary 4.5 can in particular be applied to fields k of characteristic different from 2 with projective Galois group like $k = \mathbb{Q}^{\text{ab}}$, since for such fields we always have $\text{Br}_2(k) = 0$ by Serre (1964), Ch. II, §2, Prop. 5 (see also Ribes (1970), Ch. V, Cor. 3.7).

With Corollary 4.5 from Theorem II.10.2 we get immediately:

Theorem 4.6. *The following simple groups possess GAR-realizations in one variable over \mathbb{Q}^{ab} :*

- (a) *The non-abelian simple alternating groups A_n .*
- (b) *The groups of Lie type $G(p)$ for $2 < p \in \mathbb{P}$ with the possible exception ${}^3D_4(p)$.*
- (c) *The groups $S_{2n}(2)$, $O_{2n}^+(2)$, $O_{2n}^-(2)$.*
- (d) *The sporadic simple groups.*

Obviously not all non-abelian finite simple groups G can possess GAR-realizations in one variable over $k = \mathbb{Q}$ respectively $k = \mathbb{Q}^{\text{ab}}$, since in general $\text{Out}(G)$ does not embed into $\text{Aut}(k(t)/k) \cong \text{PGL}_2(k)$. This necessitates the investigation of GAR-realizations in several variables.

4.3 GAR-Realizations in Several Variables

The following proposition contains a sufficient condition for GA-realizations in several variables constructed from Theorem III.5.10 to satisfy the rationality condition (R) and hence to be a GAR-realization.

Proposition 4.7. *Let G be a group with $\mathcal{Z}(G) = 1$, $A := \text{Aut}(G)$ and $N_\sigma/K_{\sigma A}^V$ the Galois extension constructed in Theorem III.5.10 with*

$$\text{Gal}(N_\sigma/K_{\sigma A}^V) \cong \text{Aut}(G) \quad \text{and} \quad \text{Gal}(N_\sigma/K_\sigma^V) \cong G,$$

and k the algebraic closure of \mathbb{Q} in K_σ^V . Further assume that $K_\sigma^V/k(t)$ is rational and has a transcendence basis u_1, \dots, u_s such that the k -vector space $U := \bigoplus_{i=1}^s ku_i$ remains invariant under $\text{Gal}(K_\sigma^V/K_{\sigma A}^V)$. Then $\text{Gal}(N_\sigma/K_{\sigma A}^V)$ is a GAR-realization of G over k .

Proof. Let $K := K_\sigma^V$, $F := K_{\sigma^A}^V$ and \bar{K} the composite of K with an algebraic closure \bar{k} of k in an algebraic closure of K . Further let R/F be a finite field extension with $\bar{k}R = \bar{K} = k(\mathbf{u})$ and $\tilde{k} := \bar{k} \cap R$. Then with $\text{Gal}(\bar{K}/F)$ the group $\Delta := \text{Gal}(\bar{K}/R)$ also leaves the \tilde{k} -vector space $\bar{U} := \bigoplus_{i=1}^s \tilde{k}u_i$ invariant. By Speiser's Lemma (Proposition III.3.10) the fixed point set of Δ in \bar{U} hence forms an r -dimensional \tilde{k} -vector space in R , whose bases are algebraically independent generating systems of R/\tilde{k} . \square

Remark. The assumption of linearity of $\text{Gal}(K_\sigma^V/K_{\sigma^A}^V)$ on U in the above proposition coincides with the transcendence condition (T) in Völklein (1994) respectively (L) in Völklein (1996); this can also already be found in Matzat (1992), Anm. 2.

The above proposition together with Theorem III.5.10 yields the existence theorem for GAR-realizations in several variables.

Theorem 4.8. *Let G be a finite group with $\mathcal{L}(G) = 1$, $\mathbf{C} \in \text{Cl}(G)^s$ with $s \geq 3$, V a symmetry group of \mathbf{C} and $B^V(\sigma)$ the V -symmetrized braid orbit of $[\sigma] \in \Sigma(\mathbf{C}^V)/\text{Inn}(G)$. If $B^V(\sigma)$ is rigid in $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ and $\text{Aut}(G)$ acts on $B^V(\sigma)$, then there exists a geometric Galois extension N_σ/K_σ^V , regular over $\mathbb{Q}_\mathbf{C}^V$, with*

$$\text{Gal}(N_\sigma/K_{\sigma^A}^V) \cong \text{Aut}(G) \quad \text{and} \quad \text{Gal}(N_\sigma/K_\sigma^V) \cong G. \quad (4.1)$$

If here $K_\sigma^V/\mathbb{Q}_\mathbf{C}^V$ is a rational function field and $\text{Gal}(K_\sigma^V/K_{\sigma^A}^V)$ acts linearly on the k -vector space generated by a transcendence basis of $K_\sigma^V/\mathbb{Q}_\mathbf{C}^V$, then $\text{Gal}(N_\sigma/K_\sigma^V)$ is a GAR-realization of G over $\mathbb{Q}_\mathbf{C}^V$.

Remark. In the case $V = 1$ the rationality of $K_\sigma^V/\mathbb{Q}_\mathbf{C}^V$ can be checked using the Braid Orbit Theorem III.5.7.

As an example for the application of this theorem we obtain GAR-realizations over \mathbb{Q} from the G-realizations in Corollary III.10.14 of the simple groups $L_n(q)$ and $U_n(q)$.

Corollary 4.9 (Völklein (1994)). *Assume $q = 2^e$ and $n = 4m > 2q$.*

(a) *For e even and $\gcd(n, q - 1) = 1$ the groups $L_n(q)$ possess GAR-realizations over \mathbb{Q} .*

(b) *For e odd and $\gcd(n, q + 1) = 1$ the groups $U_n(q)$ possess GAR-realizations over \mathbb{Q} .*

Proof. To verify (b) we show that the Galois extensions $N_{\tilde{\tau}}/K_{\tilde{\tau}}^V$ in Theorem III.10.13 are GAR-realizations of $\text{PGU}_n(q)$ over \mathbb{Q} . Here by Theorem III.3.11 the field $K_{\tilde{\tau}}^V$ is a rational function field over \mathbb{Q} of the form $K_{\tilde{\tau}}^V = \mathbb{Q}(v_1, \dots, v_{2m}, t)$ where

$$\bar{\mathbb{Q}}v_1 \oplus \dots \oplus \bar{\mathbb{Q}}v_{2m} = \bar{\mathbb{Q}}t_1 \oplus \dots \oplus \bar{\mathbb{Q}}t_{2m} =: \bar{U}.$$

Since the class vector $\mathbf{C} = (C_1, \dots, C_{2m})$ is V -symmetric with respect to the symmetry group V from Theorem III.10.13, and $\Sigma(\mathbf{C}^V)/\text{Inn}(G)$ forms a single H_s^V -

orbit B for $V = \text{Sym}(\mathbf{C})$, the outer automorphism group

$$\text{Out}(\text{U}_n(q)) \cong \text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2) \cong Z_{2e}$$

acts on B . Further by construction the vector space \bar{U} is mapped to itself by $\text{Gal}(\mathbb{Q}(\mathbf{v}, t)/K_{\tilde{\tau}}^V) \cong \text{Out}(\text{U}_n(q))$. Thus all hypotheses of Theorem 4.8 are satisfied and the assertion follows.

For part (a) we can argue in a similar manner, where here due to the non-trivial graph automorphism an additional consideration is required. This can be found in Völklein (1994), Cor. 2. \square

Frequently it is useful to employ the specializations to two variables discussed in Chapter III.7, since for these the GAR-property reduces to the symmetry property that $\text{Aut}(G)$ acts on $B_{\mathbf{s}'}^V(\sigma)$.

4.4 Specialization to GAR-Realizations in Two Variables

The basis for the existence proof of GAR-realization in two variables is given by:

Theorem 4.10. *Let $N_\sigma/\mathbb{Q}_C^V(\tilde{v}, \tilde{t})$ be the Galois extension from the Twisted Braid Orbit Theorem III.7.10 with*

$$\text{Gal}(N_\sigma/\mathbb{Q}_C^V(\tilde{v}, \tilde{t})) \cong G. \quad (4.2)$$

If $\text{Aut}(G)$ acts on the V -symmetrized braid orbit $B_{\mathbf{s}'}^V(\sigma)$, then (4.2) is a GAR-realization of G over \mathbb{Q}_C^V .

Proof. The fact that (4.2) is a GA-realization over \mathbb{Q}_C^V follows directly from the proof of Theorem III.5.10 and hence need not be repeated. It remains to verify the rationality condition (R). For this let $K_{\sigma_A}^V = \mathbb{Q}_C^V(\tilde{v}, \tilde{t})^{\text{Out}(G)}$, R be an intermediate field of $\bar{\mathbb{Q}}(\tilde{v}, \tilde{t})/K_{\sigma_A}^V$ with $\bar{\mathbb{Q}}R = \bar{\mathbb{Q}}(\tilde{v}, \tilde{t}) = \bar{K}_\sigma^V$ and \tilde{k} the algebraic closure of \mathbb{Q} in R . Then for $\mathcal{R} := R \cap \bar{M}'_s$ we have $\bar{\mathbb{Q}}\mathcal{R} = \bar{\mathcal{K}}_\sigma^V$ (in the notation of Section III.7.2), and hence $g(\mathcal{R}/\tilde{k}) = 0$. The group $\text{Gal}(\bar{\mathcal{K}}_\sigma^V/\mathcal{R})$ permutes the ramified prime divisors $\mathfrak{Q}_{ij}/\tilde{\mathfrak{Q}}_i$ of $\bar{\mathcal{K}}_\sigma^V/\bar{\mathbb{Q}}(\tilde{u})$, and the ramification indices e_{ij} correspond to the cycle lengths of $\pi(\tilde{\beta}_i)$. Thus the oddness condition (O') entails the rationality of \mathcal{R}/\tilde{k} . By assumption we also have

$$g(R/\mathcal{R}) = g(K_\sigma^V/\mathcal{K}_\sigma^V) = g_s^V(\sigma) = 0.$$

According to the proof of Theorem III.7.3 the numerator divisor \mathfrak{P}_s of $(t-u)$ is the only non-algebraic prime divisor in \mathbf{s}' which therefore does not split in $\bar{M}'_s(t)/K_{\sigma_A}^V$ and thus possesses the residue degree 1 even in R/\mathcal{R} . Consequently, R/\mathcal{R} and hence also R/\tilde{k} are rational function fields. \square

If the field of constants has trivial Brauer group, then according to Proposition 4.4 and Corollary 4.5 the rationality condition is void for all function fields in one variable. As $\text{Br}(\mathbb{Q}^{\text{ab}}) = 0$ we thus obtain from Theorem 4.10, by dropping the oddness condition (O'):

Corollary 4.11. *Under the assumptions in the Twisted Braid Orbit Theorem III.7.10 but without the oddness condition (O'), if $\text{Aut}(G)$ acts on the V -symmetrized braid orbit $B_{S'}^V(\sigma)$, then G possesses a GAR-realization in two variables over \mathbb{Q}^{ab} .*

Finally we demonstrate the applicability of Theorem 4.10 on the example of the groups $L_3(3)$ and $L_3(4)$. Note that since $\text{Out}(L_3(4)) = Z_2 \times S_3$, the group $L_3(4)$ cannot possess a GAR-realization in one variable over \mathbb{Q} .

Example 4.1. Let $G = L_3(3)$, $\mathbf{C} = (3A, 3A, 3B, 2A)$ in Atlas notation and $V = \langle (12) \rangle$. Being a rational class vector, \mathbf{C} is also V -symmetric. Since the conjugacy classes $3A$, $3B$ and $2A$ of G are invariant under all outer automorphisms, $\text{Out}(G) \cong Z_2$ acts on $\Sigma(\mathbf{C}^V)/\text{Inn}(G) = \Sigma(\mathbf{C})/\text{Inn}(G)$. According to Przywara (1991), Satz 3(h), $\Sigma(\mathbf{C})/\text{Inn}(G)$ forms a single H_4^V -orbit B of length 12, on which the $\tilde{\beta}_i$ have the permutation types $\pi_B(\tilde{\beta}_1) = (4^2, 2^2)$, $\pi_B(\tilde{\beta}_2) = (2^6)$ and $\pi_B(\tilde{\beta}_3) = (6, 4, 1^2)$. Thus for $[\sigma] \in B$ we have $g_4^V(\sigma) = 0$ as well as the oddness condition (O'). Hence by Theorem 4.10 the group $L_3(3)$ has a GAR-realization in two variables over \mathbb{Q} . \square

Example 4.2. Let $G = L_3(4)$, $\tilde{G} = \text{PGL}_3(4) = G \cdot S_3$, $\tilde{\mathbf{C}} = (2A, 2C, 6E, 3B)$ a class vector of \tilde{G} and $V = 1$. Then $\tilde{\mathbf{C}}$ is rational and hence V -symmetric, and $\text{Out}(\tilde{G}) \cong Z_2$ acts on $\Sigma(\tilde{\mathbf{C}}^V)/\text{Inn}(G) = \Sigma(\mathbf{C})/\text{Inn}(G)$. By Przywara (1991), Satz 1(h), H_4^V has a single orbit B on $\Sigma(\mathbf{C})/\text{Inn}(G)$ of length 54, on which the $\tilde{\beta}_i$ have the permutation types $(5^4, 3^8, 2^5)$, $(4^{10}, 2^7)$ and $(3^{12}, 2^8, 1^2)$. For $[\sigma] \in B$ we thus have $g_4^V(\sigma) = 0$ and (O'). Consequently \tilde{G} has a GAR-realization $\text{Gal}(N/\mathbb{Q}(\tilde{v}, \tilde{t}))$ in two variables over \mathbb{Q} .

To obtain a GAR-realization even for the subgroup $G = L_3(4)$ of \tilde{G} , a further consideration is necessary. Let F be the fixed field in N of $\text{Aut}(\tilde{G}) = \tilde{G} \cdot Z_2$, K , $L = \mathbb{Q}(\tilde{v}, \tilde{t})$ the intermediate fields corresponding to G and \tilde{G} respectively, and \bar{N} , \bar{F} , \bar{K} and \bar{L} the fields obtained from the former by extension of constants with $\bar{\mathbb{Q}}$. In particular the field extension \bar{N}/F is then Galois. Here \bar{K}/\bar{L} is a Galois extension of algebraic function fields in one variable over the field of constants $\bar{\mathbb{Q}}(\tilde{v})$ with group S_3 . In this the prime divisors corresponding to the three classes $2C$, $6E$ and $3B$ are ramified of orders 2, 2 and 3. Consequently \bar{K} is a rational function field over $\bar{\mathbb{Q}}(\tilde{v})$. Furthermore \bar{N}/\bar{K} is Galois with group G and corresponding class vector $\mathbf{C} = (6 \cdot 2A, 3 \cdot 3A)$ of length 9.

Now let R be an intermediate field of \bar{K}/F of finite degree over F satisfying $\bar{\mathbb{Q}}R = \bar{K}$ and with field of constants \tilde{k} . Then by the proof of Theorem 4.10, the field $\tilde{R} := R \cap \bar{L}$ is a rational function field in one variable over the field of constants $\tilde{\mathcal{R}} := \tilde{R} \cap \bar{M}'_4$, which in turn by the property (R) of $\text{Gal}(N/L)$ is a rational function field in one variable over \tilde{k} , say $\tilde{\mathcal{R}} = \tilde{k}(\tilde{u})$ with $\bar{\mathbb{Q}}(\tilde{u}) = \bar{\mathbb{Q}}(\tilde{v})$. As $\bar{M}'_4 \cap R = \tilde{\mathcal{R}}$, $\tilde{\mathcal{R}}$ is also algebraically closed in R . So extension of constants with $\bar{\mathbb{Q}}$ of $R/\tilde{\mathcal{R}}$ yields

$\bar{K}/\bar{\mathbb{Q}}(\tilde{v})$, proving $g(R/\tilde{\mathcal{R}}) = 0$. Since \bar{N}/R is Galois, the automorphisms of \bar{K}/R can only permute the three prime divisors of \bar{N}/\bar{K} ramified of order 3. Thus $R/\tilde{\mathcal{R}}$ possesses at least one prime divisor of odd degree and hence is a rational function field.

This proves that R/\tilde{k} and also K/\mathbb{Q} are rational function fields, and so $\text{Gal}(N/K)$ is a GAR-realization in two variables of $L_3(4)$ over \mathbb{Q} . \square

Some further examples can be found in Matzat (1992) and in Przywara (1991).

5 Frattini Embedding Problems

Via a reduction theorem of Nobusawa (1961) every finite embedding problem may be decomposed into a Frattini embedding problem followed by a split embedding problem. Since until now only split embedding problems have been treated, we here collect some results on Frattini embedding problems. The embedding theorem presented in Section 5.2 contains the theorems of Feit (1989) and Völklein (1992a) as special cases. This is applied to realize the covering groups of several simple groups S as geometric Galois groups over $\mathbb{Q}(t)$, so for example $S = A_n$ with kernel Z_2 using the A_n -polynomials constructed by Mestre (1990), and some sporadic simple groups S with Schur multiplier Z_3 .

5.1 A Decomposition Theorem

We recall from Section 1.1 that an embedding problem $\mathcal{E}(\varphi, \kappa)$ with $G = \text{im}(\kappa)$ is called a Frattini embedding problem if the kernel H is contained in the Frattini group $\Phi(\tilde{G})$ of $\tilde{G} = H \cdot G$. The relevance of Frattini embedding problems is illuminated by the following result:

Theorem 5.1 ((Nobusawa (1961)). *Every finite (geometric) embedding problem over a field K can be decomposed into a (geometric) Frattini embedding problem, followed by a split (geometric) embedding problem, both over K .*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over K and

$$1 \rightarrow H \rightarrow \tilde{G} \rightarrow G \rightarrow 1 \quad (5.1)$$

$\iota \qquad \qquad \kappa$

be the corresponding group extension. Also let U denote a minimal subgroup of \tilde{G} with $\langle H, U \rangle = \tilde{G}$. Then this satisfies $H \cap U \leq \Phi(U)$ and $U/(H \cap U) \cong G$, hence

$$1 \rightarrow H \cap U \rightarrow U \rightarrow G \rightarrow 1 \quad (5.2)$$

$\iota_1 \qquad \qquad \kappa_1$

is a Frattini extension. The action of U on H inside of \tilde{G} defines a split group extension

$$1 \rightarrow H \rightarrow E \xrightarrow{\quad \leftarrow \quad} U \rightarrow 1 \quad (5.3)$$

$\iota_2 \qquad \qquad \kappa_2$

so that $E = H \rtimes U$ is a semidirect product of H with U with respect to the given action. Obviously

$$\chi : E = H \rtimes U \rightarrow \tilde{G}, \quad (\eta, \gamma) \mapsto \eta\gamma,$$

is an epimorphism of E on \tilde{G} with kernel isomorphic to $H \cap U$. If the embedding problems $\mathcal{E}(\varphi, \kappa_1)$ and $\mathcal{E}(\varphi_1, \kappa_2)$ belonging to (5.2) and (5.3) are solvable over K ,

i.e., if there exist homomorphisms $\varphi_1 : \Gamma_K \rightarrow U$ and $\varphi_2 : \Gamma_K \rightarrow E$ with $\kappa_1 \circ \varphi_1 = \varphi$ and $\kappa_2 \circ \varphi_2 = \varphi_1$, then $\tilde{\varphi} := \chi \circ \varphi_2 : \Gamma_K \rightarrow \tilde{G}$ is a homomorphism with

$$\kappa \circ \tilde{\varphi} = \kappa \circ \chi \circ \varphi_2 = \kappa_1 \circ \kappa_2 \circ \varphi_2 = \kappa_1 \circ \varphi_1 = \varphi$$

and hence a solution of $\mathcal{E}(\varphi, \kappa)$. If $\mathcal{E}(\varphi_1, \kappa_2)$ is properly solvable, i.e., φ_1 (by Proposition 1.8) and φ_2 are epimorphisms, then $\tilde{\varphi}$ is an epimorphism as well, and therefore a proper solution of $\mathcal{E}(\varphi, \kappa)$.

If $\mathcal{E}(\varphi, \kappa)$ is assumed to be a geometric embedding problem and hence the geometric embedding problems $\mathcal{E}(\varphi, \kappa_1)$ and $\mathcal{E}(\varphi_1, \kappa_2)$ possess geometric (proper) solutions, then $\tilde{\varphi}$ is itself a geometric (proper) solution of $\mathcal{E}(\varphi, \kappa)$. \square

Corollary 5.2. *If in Theorem 5.1 the Frattini embedding problem $\mathcal{E}(\varphi, \kappa_1)$ has a regular solution φ_1^* and moreover the lifted split embedding problem $\mathcal{E}(\varphi_1^*, \kappa_2^*)$ has a regular (proper) solution φ_2^* , then $\mathcal{E}(\varphi, \kappa)$ has a regular (proper) solution φ^* .*

Proof. This follows immediately from the proof of Theorem 5.1, since under the above assumptions the field $N := \bar{K}^{\ker(\varphi)}$ is algebraically closed in the solution field $N_1^* := (\bar{K}_1^*)^{\ker(\varphi_1^*)}$ and N_1^* is algebraically closed in $N_2^* := (\bar{K}_2^*)^{\ker(\varphi_2^*)}$, where $K_1^* := K(\mathbf{t}_1)$ and $K_2^* := K(\mathbf{t}_1, \mathbf{t}_2)$. \square

5.2 The Frattini Embedding Theorem

From now on let K/k denote a rational function field over a subfield k of $\bar{\mathbb{Q}}$ and N/K a finite geometric Galois extension with group G . By using the Hilbert irreducibility theorem we may then assume that K/k has transcendence degree 1, say $K = k(t)$. Then $\bar{N} := \bar{\mathbb{Q}}N$ is a geometric Galois extension of $\bar{\mathbb{Q}}(t)$ with group G and hence may be classified by the Hurwitz classification for function fields in one variable (Theorem I.4.1): $\bar{N} = \bar{N}_\sigma$ with $\sigma \in \Sigma_s(G)$.

Now let $\tilde{G} = H \cdot G$ be a finite group extension with structure homomorphisms ι, κ as in (5.1). Then the class of generating systems $[\sigma] \in \Sigma_s(G)/\text{Inn}(G)$ is called *uniquely liftable* to a class of generating systems $[\tilde{\sigma}] \in \Sigma_s(\tilde{G})/\text{Inn}(\tilde{G})$ if there exists a class vector $\tilde{\mathbf{C}} = (\tilde{C}_1, \dots, \tilde{C}_s)$ of \tilde{G} with $\kappa(\tilde{\mathbf{C}}) = \mathbf{C} := ([\sigma_1], \dots, [\sigma_s])$, such that $[\sigma]$ has precisely one preimage $[\tilde{\sigma}] \in \Sigma_s(\tilde{G})/\text{Inn}(\tilde{G})$ under κ . (By this definition for example the class of generating systems $[\sigma, \sigma, 1]$ respectively $[\sigma, 1, \sigma]$ of $Z_2 = \langle \sigma \rangle$ is uniquely liftable to a class of generating systems $[\tilde{\sigma}] \in (2A, (n-1)A, nA)$ of S_n , see Proposition I.5.2).

For Frattini extensions the unique liftability can be read off from the decomposition of conjugacy classes.

Proposition 5.3. *Let $\tilde{G} = H \cdot G$ be a Frattini extension, $\mathbf{C} = (C_1, \dots, C_s)$ a class vector of G such that for each $i = 1, \dots, s-1$ there exist conjugacy classes \tilde{C}_i of \tilde{G} with $\kappa(\tilde{C}_i) = C_i$ and*

$$\prod_{i=1}^{s-1} \frac{|\tilde{C}_i|}{|C_i|} = \frac{|\text{Inn}(\tilde{G})|}{|\text{Inn}(G)|}. \quad (5.4)$$

Then for each class of generating systems $[\sigma] \in \Sigma(\mathbf{C})/\text{Inn}(G)$ of G there exists precisely one $\tilde{C}_s \in \text{Cl}(\tilde{G})$ with $\kappa(\tilde{C}_s) = C_s$ such that $\Sigma(\tilde{\mathbf{C}})/\text{Inn}(\tilde{G})$ contains one and hence precisely one preimage $[\tilde{\sigma}]$ of $[\sigma]$ under κ .

Proof. Let $\sigma = (\sigma_1, \dots, \sigma_s)$ be an element of $[\sigma]$. Then any preimage $\tilde{\sigma} \in \tilde{G}^s$ of σ under κ is a generating system of \tilde{G} . The number of such generating systems whose first $s-1$ components fall into the respective classes \tilde{C}_i is equal to $|\text{Inn}(\tilde{G})|/|\text{Inn}(G)|$ by (5.4). Since the last component $\tilde{\sigma}_s$ of $\tilde{\sigma}$ is uniquely determined by $\tilde{\sigma}_1 \cdots \tilde{\sigma}_s = 1$, all these generating systems are contained in a single orbit under $\text{Inn}(\tilde{G})$. Hence $[\sigma]$ is uniquely liftable to $[\tilde{\sigma}] \in \Sigma(\tilde{\mathbf{C}})/\text{Inn}(\tilde{G})$, and in particular the conjugacy class $\tilde{C}_s := [\tilde{\sigma}_s]$ is independent of the choice of σ inside $[\sigma]$ and of $\tilde{\sigma}_i$ inside \tilde{C}_i for $i = 1, \dots, s-1$. \square

The next proposition facilitates the determination of $|\tilde{C}_i|/|C_i|$ in special cases:

Proposition 5.4. Assume the hypotheses of Proposition 5.3. Then with $f_i := |\tilde{C}_i|/|C_i|$ we have:

- (a) If $H \leq \mathcal{C}_{\tilde{G}}(\tilde{\sigma}_i)$ and $\gcd(|H|, o(\tilde{\sigma}_i)) = 1$, then $f_i = 1$.
- (b) If H has trivial intersection with $\mathcal{C}_{\tilde{G}}(\tilde{\sigma}_i)$, then $f_i = |H|$.

In the following we call \mathbf{C} a *k-rational class vector* respectively a *k-symmetric class vector* if all $\delta \in \Delta := \text{Gal}(\bar{K}/K)$ satisfy $\mathbf{C}^{c(\delta)} = \mathbf{C}$ resp. $\mathbf{C}^\delta = \mathbf{C}$ with the notations from Section I.4.2. (With this definition the \mathbb{Q} -rational class vectors are the rational class vectors in the sense of Section I.4.2.) We can now state the embedding theorem announced in the introduction which mainly applies to Frattini embedding problems.

Theorem 5.5 (Frattini Embedding Theorem). *Let $K = k(t)$ be a rational function field in one variable over a (not necessarily finite) number field k , N/GK a geometric Galois extension with $\bar{\mathbb{Q}}N = \bar{N}_\sigma \in \bar{\mathbf{N}}_\mathbf{s}(G)$ and $\varphi : \Gamma_K \rightarrow G$ the corresponding epimorphism. Further let $\tilde{G} = H \cdot G$ be a finite group extension with epimorphism $\kappa : \tilde{G} \rightarrow G$ satisfying the two properties:*

- (1) *The class $[\sigma]$ of generating systems of G is uniquely liftable to a class $[\tilde{\sigma}]$ of generating systems of \tilde{G} in a k -symmetric class vector $\tilde{\mathbf{C}}$.*
- (2) *There exist a prime divisor $\mathfrak{P} \in \text{IP}(K/k)$ of degree 1 and an extension \mathfrak{P}' of \mathfrak{P} onto $N' := N^{\mathcal{Z}(G)}$ such that $\mathcal{Z}(\tilde{G})$ has a complement in the preimage in \tilde{G} of the decomposition group $D(\mathfrak{P}'/\mathfrak{P})$.*

Then the embedding problem $\mathcal{E}(\varphi', \kappa')$, where φ', κ' denote the composition of φ, κ with the canonical epimorphism from G to $G' := G/\mathcal{Z}(G)$, has a geometric proper solution. In particular there exists a geometric Galois extension \tilde{N}/K with $\tilde{N} \geq N'$ and

$$\text{Gal}(\tilde{N}/K) \cong \tilde{G} \quad \text{and} \quad \bar{\mathbb{Q}}\tilde{N} = \bar{N}_{\tilde{\sigma}}. \quad (5.5)$$

Proof. Let $\bar{G} := \text{Gal}(\bar{N}_\sigma/\bar{\mathbb{Q}}(t)) \cong G$, $\Gamma := \text{Gal}(\bar{N}_\sigma/K)$, $\Delta := \text{Gal}(\bar{\mathbb{Q}}(t)/K)$. First from $\Gamma = \bar{G} \times \text{Gal}(\bar{N}_\sigma/N)$ it follows that $[\sigma]$ is a fixed point under the action of Δ on $\Sigma(G)/\text{Inn}(G)$ given in I.(4.9). By assumption (1) the same holds for the class of

generating systems $[\tilde{\sigma}] \in \Sigma(\tilde{G})/\text{Inn}(\tilde{G})$. Hence $K \geq K_{\tilde{\sigma}}$, and by Proposition I.4.6 the field $\bar{N}_{\tilde{\sigma}} \in \bar{N}_{\tilde{\sigma}}(\tilde{G})$ is Galois over K . Now we identify \tilde{G} with $\text{Gal}(\bar{N}_{\tilde{\sigma}}/\bar{\mathbb{Q}}(t))$ and write $\tilde{H} := \text{Gal}(\bar{N}_{\tilde{\sigma}}/\bar{N}_{\sigma})$ and $\tilde{\Gamma} := \text{Gal}(\bar{N}_{\tilde{\sigma}}/K)$. Since then by Proposition I.4.6 every element of $\tilde{\Gamma}$ acts as an inner automorphism on \tilde{G} , the centralizer $\mathcal{C}_{\tilde{\Gamma}}(\tilde{G})$ is a supplement to \tilde{G} in $\tilde{\Gamma}$.

In the case $\mathcal{Z}(\tilde{G}) = 1$ the group $\mathcal{C}_{\tilde{\Gamma}}(\tilde{G})$ is even a complement to \tilde{G} in $\tilde{\Gamma}$ which we denote by $\tilde{\Delta}$. Its fixed field \tilde{N} is a geometric Galois extension of K with corresponding restriction

$$\tilde{\varphi} : \Gamma_K \rightarrow \text{Gal}(\tilde{N}/K) \cong \tilde{G}. \quad (5.6)$$

Now \tilde{N} contains the fixed field N° of $\tilde{\Delta} \times H$, and $\text{Gal}(\bar{N}_{\sigma}/N^\circ)$ centralizes the group \tilde{G} , so N' , being the fixed field of $\mathcal{C}_{\Gamma}(\tilde{G})$, is a subfield of N° and thus also of N . Hence in particular there exists an epimorphism $\lambda : \tilde{G} \rightarrow G'$ with $\lambda \circ \tilde{\varphi} = \varphi'$. Under extension of constants with $\bar{\mathbb{Q}}$, the tower of fields $\tilde{N}/N'/K$ goes over into $\bar{N}_{\tilde{\sigma}}/\bar{N}'/\bar{\mathbb{Q}}(t)$. Since $\kappa([\tilde{\sigma}]) = [\sigma]$ by construction, and for a suitable choice of representatives even $\kappa(\tilde{\sigma}) = \sigma$ and hence $\kappa \circ \psi_{\tilde{\sigma}} = \psi_{\sigma}$, the restriction $\tilde{\varphi} : \Gamma_K \rightarrow \text{Gal}(\bar{N}_{\sigma}/\bar{\mathbb{Q}}(t))$, $\varphi' : \Gamma_K \rightarrow \text{Gal}(\bar{N}'/\bar{\mathbb{Q}}(t))$ satisfy $\kappa' \circ \tilde{\varphi} = \varphi'$ and moreover $\lambda \circ \tilde{\varphi} = \varphi'$. Hence we have $\lambda = \kappa'$ and $\tilde{\varphi}$ is a geometric proper solution of $\mathcal{E}(\varphi', \kappa')$.

In the case $\mathcal{Z}(\tilde{G}) \neq 1$ we denote the fixed field of $\mathcal{C}_{\tilde{\Gamma}}(\tilde{G})$ by L . As $L \geq N'$ this contains the fixed field K' of $D(\mathfrak{P}'/\mathfrak{P})$. Then $\tilde{L} := \bar{\mathbb{Q}}L$ and $\tilde{K}' := \bar{\mathbb{Q}}K'$ satisfy $\text{Gal}(\bar{N}_{\tilde{\sigma}}/\tilde{L}) \cong \mathcal{Z}(\tilde{G})$ and $\text{Gal}(\bar{N}_{\tilde{\sigma}}/\tilde{K}') \cong \tilde{G}'$, where $\tilde{G}' = \kappa^{-1}(D(\mathfrak{P}'/\mathfrak{P}))$ is the preimage of $D(\mathfrak{P}'/\mathfrak{P})$ in \tilde{G} . By the Remark in Section I.3.2, \tilde{G} possesses a complement $\tilde{\Delta}$ in $\tilde{\Gamma}$ inside the group $\text{Gal}(\bar{N}_{\tilde{\sigma}}/K')$, with fixed field $M := \bar{N}_{\tilde{\sigma}}^{\tilde{\Delta}}$ say. The Galois closure \tilde{M} of M/K is then the fixed field of $\tilde{\Delta} \cap \mathcal{C}_{\tilde{\Gamma}}(\tilde{G})$ and thus contains L .

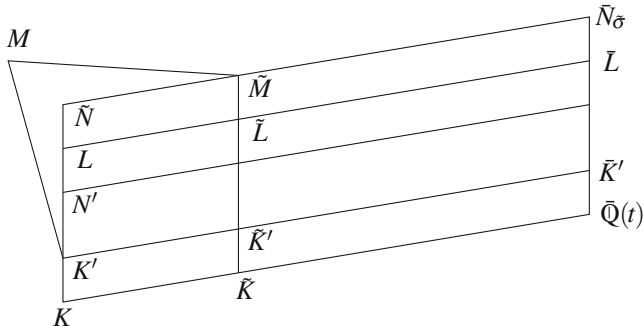


Fig. 5.1 Field tower for the Frattini Embedding Theorem

Denote the composites of K, K', L with the algebraic closure \tilde{k} of k in \tilde{M} by \tilde{K}, \tilde{K}' resp. \tilde{L} , so the corresponding Galois groups are $\text{Gal}(\tilde{M}/\tilde{K}) \cong \tilde{G}$, $\text{Gal}(\tilde{M}/\tilde{K}') \cong \tilde{G}'$ and $\text{Gal}(\tilde{M}/\tilde{L}) \cong \mathcal{Z}(\tilde{G})$. Moreover $\text{Gal}(\tilde{M}/K)$ is isomorphic to a subgroup of the holomorph $\text{Hol}(\tilde{G})$. Here the elements of the complement $\text{Gal}(\tilde{M}/M)$ act on $\text{Gal}(\tilde{M}/\tilde{K})$ since $\text{Gal}(\bar{N}_{\tilde{\sigma}}/K') = \langle \tilde{G}', \mathcal{C}_{\tilde{\Gamma}}(\tilde{G}) \rangle$ as elements of $\text{Gal}(\tilde{M}/\tilde{K}')$ by conjugation. Now the centralizer $\text{Gal}(\tilde{M}/L)$ of $\text{Gal}(\tilde{M}/\tilde{K})$ in $\text{Gal}(\tilde{M}/K)$ is isomor-

phic to a subgroup of $\text{Gal}(\tilde{M}/\tilde{K}')$ containing $\text{Gal}(\tilde{M}/\tilde{L}) \cong \mathcal{Z}(\tilde{G})$ (compare with the proof of Theorem I.3.9). By assumption (2), the group $\text{Gal}(\tilde{M}/\tilde{L})$ possesses a complement in this subgroup and hence also in $\text{Gal}(\tilde{M}/L)$. If we now denote the fixed field of this complement by \tilde{N} , then since $\bar{\Phi}\tilde{N} = \tilde{N}_{\tilde{\sigma}}$ and $\text{Gal}(\tilde{N}_{\tilde{\sigma}}/\tilde{N}) \leq \mathcal{C}_{\tilde{F}}(\tilde{G})$ we have

$$\text{Gal}(\tilde{N}_{\tilde{\sigma}}/K) = \text{Gal}(\tilde{N}_{\tilde{\sigma}}/\bar{\Phi}(t)) \times \text{Gal}(\tilde{N}_{\tilde{\sigma}}/\tilde{N}).$$

Thus \tilde{N}/K is a geometric Galois extension with $\text{Gal}(\tilde{N}/K) \cong \tilde{G}$ and $\tilde{N} \geq N'$. From this we conclude as in the case $\mathcal{Z}(\tilde{G}) = 1$ that the corresponding restriction $\tilde{\varphi}$ as in (5.6) yields a geometric proper solution of $\mathcal{E}(\varphi', \kappa')$. \square

The example given above of an extension of Z_2 to an S_n shows that in general one cannot expect \tilde{N} to contain the field N , since otherwise the S_n -extension constructed in Theorem I.5.3 would contain every geometric Z_2 -extension of $\mathbb{Q}(t)$ ramified in two given points.

Remark. In the case $\mathcal{Z}(\tilde{G}) = 1$ the condition (2) of Theorem 5.5 is always satisfied. According to Theorem I.3.9 it can hence be weakened to the normalizer condition (N).

If condition (2) of Theorem 5.5 is not satisfied, we obtain at least the following:

Corollary 5.6. *If only condition (1) of Theorem 5.5 is satisfied, then the embedding problem given by $\tilde{\varphi} : \Gamma_K \rightarrow \text{Gal}(N'/K) \cong G/\mathcal{Z}(G)$ and the residue class map $\tilde{\kappa} : \tilde{G}/\mathcal{Z}(\tilde{G}) \rightarrow G/\mathcal{Z}(G)$ induced by κ possesses a geometric proper solution.*

Proof. The field L in the second part of the proof furnishes a solution field. \square

5.3 Centerless Frattini Extensions

In the special case of Frattini extensions with trivial center we obtain from Theorem 5.5 the following version of Lemma 2.7 in Feit (1989):

Proposition 5.7. *Assume a Frattini extension $\tilde{G} = H \cdot G$ with $\mathcal{Z}(\tilde{G}) = \mathcal{Z}(G) = 1$ satisfies the following: The conjugacy classes $C_i = [\sigma_i]$ of G possess k -rational classes \tilde{C}_i as preimages in \tilde{G} for $i = 1, \dots, s$ with $f_i = 1$ for $i = 1, \dots, s-2$ and $f_{s-1} = |H|$ and with $\text{Sym}(\tilde{C}) = \text{Sym}(C)$. Then the conditions (1) and (2) of the Frattini Embedding Theorem are satisfied.*

Proof. From the k -rationality of the classes \tilde{C}_i and $\text{Sym}(\tilde{C}) = \text{Sym}(C)$ it follows that the class vector $\tilde{\mathbf{C}}$ is k -symmetric. Thus the assertion follows immediately from Proposition 5.3 and the above Remark. \square

As an application we prove a result of Feit where the idea of the proof is to obtain central Frattini extensions as subgroups of centerless Frattini extensions.

Theorem 5.8 (Feit (1989)). (a) *The central group extensions of types $3 \cdot A_6$ and $3 \cdot A_7$ possess G-realizations over \mathbb{Q} .*

(b) *The covering groups $3 \cdot S$ with $S \in \{\text{M}_{22}, \text{McL}, \text{Suz}, \text{ON}, \text{Fi}_{22}, \text{Fi}'_{24}\}$ possess G-realizations over \mathbb{Q} .*

Proof. For the proof of (a) we can restrict ourselves to non-split group extensions. Starting points are the rational rigid class vectors of the symmetric groups S_6 and S_7 from Proposition I.5.2, hence $(2B, 5A, 6B)$ for S_6 and $(2B, 6C, 7A)$ for S_7 in Atlas notation. In the case $n = 6$, both classes $2B$ and $6B$ possess a single preimage class in $3 \cdot S_6$ of the same order, say $2\tilde{B}$ and $6\tilde{B}$, and $5A$ splits into three preimage classes, with one, $5\tilde{A}$, containing elements of order 5 and two with elements of order 15. Hence $\tilde{\mathbf{C}} := (2\tilde{B}, 5\tilde{A}, 6\tilde{B})$ is a rational class vector of $3 \cdot S_6$, and we have $f_2 = 1$ and $f_1 = f_3 = 3$. By Proposition 5.7, all assumptions of Theorem 5.5 are hence satisfied and there exists a geometric Galois extension over $\mathbb{Q}(t)$ with the group $3 \cdot S_6$ for the class vector $\tilde{\mathbf{C}}$. As $5\tilde{A} \subset 3 \cdot A_6$, only two prime divisors of $\mathbb{Q}(t)/\mathbb{Q}$ of degree 1 are ramified in the fixed field K of $3 \cdot A_6$. Thus K/\mathbb{Q} is a rational function field and $3 \cdot A_6$ possesses a G-realization over \mathbb{Q} . The same proof applies to the case $n = 7$ with $f_3 = 1$ and $f_1 = f_2 = 3$ and leads to a G-realization of $3 \cdot A_7$ over \mathbb{Q} .

The results collected in (b) are obtained by the same method using the following rationally rigid class vectors of $\text{Aut}(S)$ from Propositions II.9.1, II.9.2, II.9.4, II.9.7, and the corresponding class indices f_i :

$$\begin{aligned} \text{Aut}(\text{M}_{22}) &: (2B, 4C, 11A), f_3 = 1, f_1 = f_2 = 3, \\ \text{Aut}(\text{McL}) &: (3A, 4B, 10B), f_2 = 1, f_1 = f_3 = 3, \\ \text{Aut}(\text{Suz}) &: (2C, 8D, 13A), f_3 = 1, f_1 = f_2 = 3, \\ \text{Aut}(\text{ON}) &: (2B, 4A, 22A), f_2 = 1, f_1 = f_3 = 3, \\ \text{Aut}(\text{Fi}_{22}) &: (2D, 5A, 42A), f_2 = 1, f_1 = f_3 = 3, \\ \text{Aut}(\text{Fi}'_{24}) &: (2C, 8D, 29A), f_3 = 1, f_1 = f_2 = 3. \end{aligned}$$

This completes the proof of Theorem 5.8. \square

For another realization of the group $3 \cdot A_6$ see also Example III.8.1.

Remark. With the exception of J_3 , Theorem 5.8(b) contains all sporadic groups whose Schur multiplier has order divisible by 3. The rational class vector $\mathbf{C} = (2B, 3B, 8B)$ of $\text{Aut}(J_3)$ in Proposition II.9.8(a), which at present yields the only known G-realization for J_3 over \mathbb{Q} , has class indices $f_1 = f_2 = f_3 = 3$ in $3 \cdot \text{Aut}(J_3)$, so that the classes of generating systems contained in $\Sigma(\mathbf{C})$ do not lift uniquely to $3 \cdot \text{Aut}(J_3)$!

Finally we demonstrate with an example that with the centerless version of the Frattini Embedding Theorem also centers different from Z_3 can be treated.

Example 5.1. Let $S := \text{L}_3(4)$ and $G := \text{PGL}_3(4)$. The Schur multiplier of S has order 48 and possesses precisely one elementary abelian factor group E_4 of order 4.

This defines a central non-split group extension

$$1 \rightarrow E_4 \rightarrow \tilde{S} \rightarrow L_3(4) \rightarrow 1.$$

By a theorem of Thompson (1973) there exists an automorphism of the full covering group of $L_3(4)$ cyclically permuting the three non-trivial elements of E_4 . Obviously this is already induced by $\mathrm{PGL}_3(4)$, hence the above exact sequence may be lifted to a centerless Frattini extension:

$$1 \rightarrow E_4 \rightarrow \tilde{G} \rightarrow \mathrm{PGL}_3(4) \rightarrow 1.$$

According to Example 4.2 the group $\mathrm{PGL}_3(4)$ possesses a G-realization in two and hence also in one variable over \mathbb{Q} with the class vector $(2A, 2C, 6E, 3B)$, say $N/\mathbb{Q}(t)$. As $2A, 3B \subset \mathrm{PGL}_3(4)$ the fixed field of $G = \mathrm{PGL}_3(4)$ in this field extension is rational, say $N^G = \mathbb{Q}(t)$, and the $\mathrm{PGL}_3(4)$ -extension $N/\mathbb{Q}(t)$ has the class vector $(2A, 2A, 3A, 3B, 3B)$. The preimage classes $2\tilde{A}$ and $3\tilde{A}$ in \tilde{G} of $2A$ and $3A$ are uniquely determined by the conditions $f_1 = f_2 = f_3 = 1$, and by Proposition 5.4(b) we have $f_4 = f_5 = 4$. Hence the preimage vector $\tilde{\mathbf{C}}$ of \mathbf{C} is rational with $\mathrm{Sym}(\tilde{\mathbf{C}}) = \mathrm{Sym}(\mathbf{C})$ and by the Frattini Embedding Theorem together with Proposition 5.7 there exists a Galois extension $\tilde{N}/\mathbb{Q}(t)$ containing $N/\mathbb{Q}(t)$ with $\mathrm{Gal}(\tilde{N}/\mathbb{Q}(t)) \cong \tilde{G}$. Here the fixed field of \tilde{S} , which coincides with the fixed field of $L_3(4)$ in $N/\mathbb{Q}(t)$, is rational, say $\tilde{N}^{\tilde{S}} = \mathbb{Q}(u)$. Hence there exists a geometric Galois extension $\tilde{N}/\mathbb{Q}(u)$ with $\mathrm{Gal}(\tilde{N}/\mathbb{Q}(u)) \cong \tilde{S}$ and $\mathcal{Z}(\tilde{S}) = E_4$. \square

In the next section we treat central Frattini embedding problems without the detour via a centerless Frattini embedding problem.

5.4 Central Frattini Extensions and $2 \cdot A_n$

For central Frattini extensions the assumptions of Theorem 5.5 can for example be verified by use of the following version of a theorem of Völklein (1992a):

Proposition 5.9. *Assume a central Frattini extension $\tilde{G} = H \cdot G$ with $G = \mathrm{Gal}(N/K)$ and $\mathcal{Z}(G) = 1$ satisfies:*

(1') *We have $\gcd(o(\sigma_i), |H|) = 1$ for $i = 1, \dots, s$.*

(2') *The field N/k possesses a prime divisor of degree 1.*

Then the conditions (1) and (2) of Theorem 5.5 are satisfied.

Proof. By Proposition 5.4(a) it follows from (1') that $f_i = 1$ for $i = 1, \dots, s$. Now let \tilde{C}_i for $i = 1, \dots, s-1$ denote the preimage classes of C_i in \tilde{G} whose elements have the same order as those of C_i . Then $[\sigma]$ may by Proposition 5.3 be uniquely lifted to a class of generating systems $[\tilde{\sigma}]$ of \tilde{G} with $\tilde{\sigma}_i \in \tilde{C}_i$ for $i = 1, \dots, s-1$, which uniquely determines a conjugacy class $\tilde{C}_s = [\tilde{\sigma}_s]$. If now $\tilde{\mathbf{C}} = (\tilde{C}_1, \dots, \tilde{C}_s)$ were not k -symmetric, then there would exist a $\delta \in \mathrm{Gal}(\bar{\mathbb{Q}}(t)/k(t))$ with $\tilde{C}_s^{c(\delta)} \neq \tilde{C}_s$ and hence $[\tilde{\sigma}]^\delta \neq [\tilde{\sigma}]$, in contradiction to the unique liftability of $[\sigma] = [\sigma]^\delta$. Thus (1) is satisfied.

Now let \mathfrak{P}' be the prime divisor of degree 1 in N/k whose existence is assumed in (2'). Then the decomposition group $D(\mathfrak{P}'/\mathfrak{P})$ in $\text{Gal}(N/K)$ equals the inertia group and thus has order coprime to H . The group $H = \mathcal{Z}(\tilde{G})$ hence has a complement in the preimage of $D(\mathfrak{P}'/\mathfrak{P})$ in \tilde{G} , which proves (2). \square

Using the above version of the Frattini embedding theorem we now construct G -realizations over \mathbb{Q} for the groups $2 \cdot A_n$. Since the A_n -extensions exhibited in Theorem I.5.3 do in general not embed into extensions with the covering groups (see Vila (1985)), we first present families of A_n -polynomials found by Mestre (1990).

Lemma 5.10. *For the general polynomial of odd degree $n \geq 3$ over \mathbb{Q}*

$$g(X) = X^n - s_1 X^{n-1} + \dots \pm s_n \in \mathbb{Q}(s_1, \dots, s_n)[X]$$

there exists a coprime polynomial $h \in \mathbb{Q}(\mathbf{s})[X]$ and a separable polynomial $q \in \mathbb{Q}(\mathbf{s})[X]$, both of degree $n-1$, with

$$gh' - g'h = -q^2, \quad (5.7)$$

where ' denotes formal differentiation with respect to X .

Proof. Let $K := \mathbb{Q}(\mathbf{s})$ and $\tilde{K} := \mathbb{Q}(\mathbf{t})$ where t_1, \dots, t_n are the zeroes of $g(X)$ in an algebraic closure \tilde{K} of K . Then \tilde{K}/K is Galois with group S_n , which acts on t_1, \dots, t_n in its natural permutation representation: $t_i^\sigma = t_{(i)\sigma}$. The equation (5.7) in $K[X]$ is obviously equivalent to the identity

$$(h/g)' = -(q/g)^2 \quad (5.8)$$

in the quotient field $K(X)$. As the degree of the numerator is smaller than the degree of the denominator, both sides possess partial fraction expansions in $\tilde{K}(X)$ of the form

$$\frac{h}{g} = \sum_{i=1}^n \frac{u_i}{X-t_i}, \quad \frac{q}{g} = \sum_{i=1}^n \frac{v_i}{X-t_i}.$$

Thus the solvability of (5.8) is equivalent to the solvability of the following system of algebraic equations

$$u_i = v_i^2 \quad \text{and} \quad v_i \left(\sum_{i \neq j=1}^n \frac{v_j}{t_i - t_j} \right) = 0 \text{ for } i = 1, \dots, n. \quad (5.9)$$

If here v_i and hence also u_i vanished, then t_i would be a zero of h in contradiction to the assumed coprimeness of g and h . Thus (5.9) reduces to the linear system for the v_j

$$\sum_{i \neq j=1}^n \frac{v_j}{t_i - t_j} = 0 \quad \text{for } i = 1, \dots, n. \quad (5.10)$$

Since the coefficient matrix is skew symmetric of odd dimension n , it possesses an eigenvalue 0. Specializing g for example to $\tilde{g}(X) := X^n - X$ we deduce that the

rank of this matrix is actually equal to $n - 1$. Consequently there exists an eigenvector $\mathbf{v} \in \tilde{K}^n$ to the eigenvalue 0 uniquely determined up to scalar multiples. Since the rows and columns of the coefficient matrix of the system of linear equations (5.10) are permuted by $\sigma \in S_n = \text{Aut}(\tilde{K}/K)$ like the variables t_i , there exist $x(\sigma) \in K$ with

$$v_i^\sigma = x(\sigma)v_{(i)\sigma} \quad \text{and} \quad x(\sigma\tau) = x(\sigma)^\tau x(\tau) \quad \text{for } \sigma, \tau \in S_n.$$

By Hilbert's Theorem 90 there then also exists an eigenvector $\mathbf{v} \in \tilde{K}^n$ satisfying $v_i^\sigma = v_{(i)\sigma}$ for all $\sigma \in S_n$. This yields solution polynomials $h, q \in K[X]$ for (5.8) and thus (5.7) with $\deg(h) \leq n - 1$.

To prove the remaining condition we again specialize g to \bar{g} . As is easily verified, the polynomials

$$\bar{h} := n^2 X^{n-1} - (n-2)^2, \quad \bar{q} := nX^{n-1} + n - 2 \in \mathbb{Q}[X], \quad (5.11)$$

then constitute solutions of equation (5.7) with g replaced by \bar{g} . In particular the solutions satisfy in this case that \bar{h} is prime to \bar{g} of degree $n - 1$ and \bar{q} is separable. Hence this is also true for the generic solutions h, q of the original non-specialized problem. \square

Proposition 5.11. *The polynomials g, h in Lemma 5.10 satisfy:*

$$(a) \quad f(t, X) := g(X) - t h(X) \in \mathbb{Q}(\mathbf{s}, t)[X] \quad (5.12)$$

has the Galois group S_n over $\mathbb{Q}(\mathbf{s}, t)$ and group A_n over $\mathbb{Q}(\mathbf{t}, t)$ respectively, where $\mathbb{Q}(\mathbf{t})$ is the splitting field of $g(X)$ over $\mathbb{Q}(\mathbf{s})$.

$$(b) \quad \tilde{f}(u, X) := \frac{g(u)h(X) - g(X)h(u)}{X - u} \in \mathbb{Q}(\mathbf{s}, u)[X] \quad (5.13)$$

has the Galois group S_{n-1} over $\mathbb{Q}(\mathbf{s}, u)$ respectively A_{n-1} over $\mathbb{Q}(\mathbf{t}, u)$.

Proof. By the coprimeness of g and h in $K[X]$ asserted in Lemma 5.10 the polynomial $f(t, X) \in K(t)[X]$ is certainly irreducible. Moreover its discriminant $D(f)$ is a polynomial in t , whose degree is bounded by $2(n-1)$ according to the expansion theorem for determinants applied to the resultant $R(f, f')$. If b_i is one of the $n-1$ distinct zeroes b_1, \dots, b_{n-1} of $q \in K[X]$ in \tilde{K} , then $h(b_i) \neq 0$ due to the coprimeness of g and h . Setting $c_i := g(b_i)/h(b_i)$, the polynomials $f_i(X) := f(c_i, X)$ satisfy $f_i(b_i) = 0$. Thus from

$$h(b_i)f'_i(b_i) = h(b_i)g'(b_i) - g(b_i)h'(b_i) = q^2(b_i),$$

it follows moreover that $f'_i(b_i) = f''_i(b_i) = 0$, i.e., that b_i is even a threefold zero of $f_i(X)$. By the Dedekind discriminant theorem at least $(t - c_i)^2$ is a divisor of $D(f)$. Computation of the discriminant of the specialized polynomial $\bar{f} = \bar{g} - t \bar{h}$ with $\bar{g} = X^n - X$ and \bar{h} from (5.11)

$$D(\bar{f}) = D(\bar{g})(n^n(n-2)^{n-2}t^{n-1} + 1)^2 \quad (5.14)$$

shows that the c_i are all distinct. Thus the above estimate for the degree of the discriminant as a polynomial in t forces

$$D(f(t, X)) = c_0 \prod_{i=1}^{n-1} (t - c_i)^2 \quad \text{with} \quad c_0 =_2 D(g) \text{ in } \mathbb{Q}(\mathbf{s})^\times, \quad (5.15)$$

since $D(f(0, X)) = D(g)$. The above shows that $f(t, X)$ decomposes modulo $(t - c_i)$ in the form

$$f_i(X) = f(c_i, X) = (X - b_i)^3 g_i(X)$$

with a separable polynomial $g_i(X) \in K[X]$ of degree $n - 3$ and prime to $X - b_i$. Since $t - c_i$ cannot be an inessential discriminant divisor the decomposition of $f(t, X)$ over the residue class field K of $K(t)$ modulo $(t - c_i)$ corresponds to the decomposition of the numerator divisor \mathfrak{P}_i of $(t - c_i)$ in a root field $L/K(t)$ of $f(t, X)$ (see Narkiewicz (1990), IV, §3, Thm. 4.12). Hence \mathfrak{P}_i splits in $L/K(t)$ as $\mathfrak{P}_i = \mathfrak{Q}_i^3 \mathfrak{R}_i$ with $\deg(\mathfrak{Q}_i) = 1$ and a divisor \mathfrak{R}_i prime to \mathfrak{Q}_i . If $N/K(t)$ is the Galois closure of $L/K(t)$, then for each extension $\tilde{\mathfrak{P}}_i$ of \mathfrak{P}_i onto N the inertia group $I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$ is a cyclic group of order 3, which by Theorem I.9.1 in the natural permutation representation of S_n is generated by a 3-cycle. Thus by the Hurwitz classification the Galois group $\text{Gal}(f(t, X))$ contains a transitive normal subgroup generated by 3-cycles. Consideration of the possible blocks of imprimitivity shows that such a group is necessarily also primitive, so it follows from a theorem of Jordan (see Huppert (1967), Kap. II, Satz 4.5) that $A_n \leq \text{Gal}(f(t, X))$. Therefore (a) follows by the discriminant formula (5.15) since $\text{Gal}(g) \cong S_n$ over $\mathbb{Q}(\mathbf{s})$ and $\text{Gal}(g) = 1$ over $\mathbb{Q}(\mathbf{t})$.

With exactly the same proof as for Corollary I.9.11 it follows from this that $\text{Gal}(\tilde{f}(u, X))$ is the one point stabilizer of S_n and A_n respectively, which implies (b).

□

Theorem 5.12 (Mestre (1990)). *For $n \geq 4$ the covering groups $2 \cdot A_n$ of A_n possess G -realizations over \mathbb{Q} .*

Proof. For odd n we obtain from the polynomial $f(t, X) \in \mathbb{Q}(\mathbf{t}, t)[X]$ in (5.12) by specialization of the t_i to $a_i \in \mathbb{Q}$ with the Hilbert irreducibility theorem polynomials

$$f_{\mathbf{a}}(t, X) \in \mathbb{Q}(t)[X] \quad \text{with} \quad \text{Gal}(f_{\mathbf{a}}) \cong A_n \quad (5.16)$$

and $\mathbf{a} \in \mathbb{Q}^n$ with pairwise distinct components a_i . The splitting field $N_{\mathbf{a}}/\mathbb{Q}(t)$ of such a polynomial is then geometric over $\mathbb{Q}(t)$ and belongs in the Hurwitz classification to the class vector \mathbf{C} consisting of $n - 1$ copies of the class of 3-cycles. Now $\gcd(2, 3) = 1$, so condition (1') in Proposition 5.9 is satisfied. As

$$f_{\mathbf{a}}(0, X) = \prod_{i=1}^n (X - a_i),$$

the numerator divisor \mathfrak{P}_0 of t splits completely in the root field $L_{\mathbf{a}}/\mathbb{Q}(t)$. Thus the image of the decomposition group $D(\tilde{\mathfrak{P}}_0/\mathfrak{P}_0)$ of any extension $\tilde{\mathfrak{P}}_0$ of \mathfrak{P}_0 to $N_{\mathbf{a}}$ in the natural permutation representation of A_n is trivial. So we even have $D(\tilde{\mathfrak{P}}_0/\mathfrak{P}_0) = 1$, and \mathfrak{P}_0 splits also in $N_{\mathbf{a}}/\mathbb{Q}(t)$ into prime divisors of degree 1. In particular, the condition (2') in Proposition 5.9 is satisfied and by the Frattini Embedding Theorem $N_{\mathbf{a}}/\mathbb{Q}(t)$ may be embedded into a Galois extension $\tilde{N}_{\mathbf{a}}/\mathbb{Q}(t)$ with

$$\text{Gal}(\tilde{N}_{\mathbf{a}}/\mathbb{Q}(t)) \cong 2 \cdot A_n.$$

The fixed field L of A_{n-1} inside $N_{\mathbf{a}}/\mathbb{Q}(t)$ has genus $g(L/\mathbb{Q}) = 0$ by the Hurwitz genus formula and is rational since $\deg(\mathfrak{Q}_i) = 1$ for the divisors \mathfrak{Q}_i of \mathfrak{P}_i defined in the proof of Proposition 5.11. So we have $L = \mathbb{Q}(u)$ and

$$\text{Gal}(\tilde{N}_{\mathbf{a}}/\mathbb{Q}(u)) \cong 2 \cdot A_{n-1},$$

i.e., also the suitably specialized A_{n-1} -extensions in (5.13) can be embedded into geometric Galois extensions over $\mathbb{Q}(u)$ with group $2 \cdot A_{n-1}$. \square

Explicit generators for the Galois extensions with group $2 \cdot A_n$ are calculated in the papers of Schneps (1992) and Swallow (1994), based on work of Crespo (1989).

Remark 1. For $n \neq 6, 7$ the group $2 \cdot A_n$ in Theorem 5.12 is the full covering group of A_n . In the two exceptional cases $n = 6$ and $n = 7$ the Schur multiplier of A_n is cyclic of order 6 (compare Theorem 5.8(a)).

Remark 2. By application of the Hurwitz classification for arbitrary algebraically closed intermediate fields of \mathbb{C}/\mathbb{Q} (see for example Matzat (1987), Kap. II, §1.1) in Theorem 5.5, the specialization of \mathbf{t} to $\mathbf{a} \in \mathbb{Q}^n$ with pairwise distinct components can be avoided and one thus obtains G-realizations of $2 \cdot A_n$ in $n + 1$ variables over \mathbb{Q} .

In the last section of this paragraph we will see that for the A_n -extensions of Mestre every central embedding problem can be solved.

5.5 Central Extensions of A_n

The starting point is given by the following easy group theoretic fact.

Proposition 5.13. *Let G be a perfect group with universal central extension group R and $\tilde{G} = H \cdot G$ a central group extension with canonical epimorphisms $\lambda : R \rightarrow G$ and $\kappa : \tilde{G} \rightarrow G$. Then there exists a unique homomorphism $\psi : R \rightarrow \tilde{G}$ with $\kappa \circ \psi = \lambda$.*

Proof. The central Frattini extension U from (5.2) contained in $\tilde{G} = H \cdot G$ is a factor group of R . By composition of the canonical map from R onto U with the embedding of U into \tilde{G} we obtain the stated homomorphism $\psi : R \rightarrow \tilde{G}$, which is uniquely determined by the equation $\kappa \circ \psi = \lambda$. \square

This yields a reduction theorem for the corresponding embedding problems.

Theorem 5.14. *Let N/K be a finite Galois extension with perfect Galois group G and canonical epimorphism $\varphi : \Gamma_K \rightarrow G$. Further let $\lambda : R \rightarrow G$, $\kappa : \tilde{G} \rightarrow G$ be as in Proposition 5.13. Then we have:*

- (a) *If $\tilde{\varphi}$ is an ordinary (geometric/regular) solution of $\mathcal{E}(\varphi, \lambda)$, then $\psi \circ \tilde{\varphi}$ is an ordinary (geometric/regular) solution of $\mathcal{E}(\varphi, \kappa)$.*
- (b) *If K is a Hilbertian field, then the existence of an ordinary (geometric/regular) solution of $\mathcal{E}(\varphi, \lambda)$ implies the existence of an ordinary (geometric/regular) proper solution of $\mathcal{E}(\varphi, \kappa)$.*

Proof. Part (a) of the assertion is an immediate consequence of Proposition 5.13. Part (b) follows from (a) using Corollary 2.5. \square

A Galois extension N/K for which the embedding problem for each central extension \tilde{G} of $G = \text{Gal}(N/K)$ is solvable is called a *universally central embeddable Galois extension*. Examples for these are given in the following:

Corollary 5.15. *Let K be a Hilbertian field of characteristic zero. Then we have:*

- (a) *The geometric Galois extensions $N/A_n\mathbb{Q}(t)$ in Theorem 5.12 for $n \geq 5$ and $n \neq 6, 7$ are universally central embeddable.*
- (b) *The geometric Galois extensions $N/S\mathbb{Q}(t)$ with $S \in \{\text{McL, Suz, ON, Fi}_{22}, \text{Fi}'_{24}\}$ in Theorem 5.8 are universally central embeddable.*

Proof. The proof follows from Theorem 5.14 and the cited Theorems, since in (a) the groups $2 \cdot A_n$ for $n = 5$ and $n \geq 8$ and in (b) the groups $3 \cdot S$ are the full covering groups of A_n respectively S (compare the remarks in Sections 5.4 and 5.3). \square

Remark. The result of Corollary 5.15(a) remains true for $n = 6$ and $n = 7$ if one uses the G -realizations over \mathbb{Q} for $6 \cdot A_6$ and $6 \cdot A_7$ constructed by Mestre (1998) (compare also the end of Section 6.4).

In the next paragraph we treat central embedding problems which cannot be solved by unique liftability of classes of generating systems.

6 The Quadratic Trace Form

In this paragraph we study central embedding problems with kernel Z_2 on a cohomological basis. The main ingredient here is a criterion going back to Serre (1984), with which the cohomological embedding obstruction can be expressed in terms of the Hasse-Witt-invariant of the quadratic trace form of the corresponding field extension. Thus it is possible to realize all central extensions of the symmetric groups S_n for $n \geq 4$ as geometric Galois groups over $\mathbb{Q}(t)$.

6.1 The Cohomological Embedding Obstruction

As before let N/GK be a finite Galois extension with epimorphism $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = H \cdot G$ a finite group extension with epimorphism $\kappa : \tilde{G} \rightarrow G$. If here the kernel H is abelian, then the equivalence class of the group extension $H \cdot G$ with given action of G on H is described by a cohomology class $h \in H^2(G, H)$ (see for example Huppert (1967), Kap. I, Satz 17.2, or Suzuki (1982), Ch. 2, §7). Via the inflation

$$\varphi^* : H^2(G, H) \rightarrow H^2(\Gamma_K, H), \quad h \mapsto \varphi^*(h) =: h(\varphi, \kappa), \quad (6.1)$$

h is mapped to an element $h(\varphi, \kappa) \in H^2(\Gamma_K, H)$. With this the solvability of $\mathcal{E}(\varphi, \kappa)$ may be decided.

Theorem 6.1. *Let N/GK be a finite Galois extension with canonical epimorphism $\varphi : \Gamma_K \rightarrow G$ and $\tilde{G} = H \cdot G$ a finite group extension with abelian kernel defined by the cocycle $b = (b_{\sigma, \tau}) \in Z^2(G, H)$ in the cohomology class $h \in H^2(G, H)$, and $\kappa : \tilde{G} \rightarrow G$ the canonical epimorphism.*

- (a) *The embedding problem $\mathcal{E}(\varphi, \kappa)$ is solvable if and only if $h(\varphi, \kappa) = 0$ in $H^2(\Gamma_K, H)$.*
- (b) *Every cochain $c = (c_\gamma) \in C^1(\Gamma_K, H)$ with $\delta(c) = \varphi^*(b)$ defines a solution $\tilde{\varphi}_c$ of $\mathcal{E}(\varphi, \kappa)$ with kernel $\Gamma_c := \{\gamma \in \Gamma_N \mid c_\gamma = 1\}$ and vice versa.*

Proof. We employ the following commutative diagram with the fiber product (sub-direct product) $\tilde{\Gamma} := \tilde{G} \times_G \Gamma_K$ and the projections $p_1 : \tilde{\Gamma} \rightarrow \tilde{G}$ and $p_2 : \tilde{\Gamma} \rightarrow \Gamma_K$:

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \longrightarrow & \tilde{G} \times_G \Gamma_K & \xleftarrow[\substack{p_2 \\ \downarrow p_1}]{} & \Gamma_K \longrightarrow 1 \\ & & & & \downarrow & & \downarrow \varphi \\ 1 & \longrightarrow & H & \xrightarrow{\iota} & \tilde{G} & \xrightarrow{\kappa} & G \longrightarrow 1 \end{array} \quad (6.2)$$

Since the group extension in the top row of (6.2) belongs to the cohomology class $h(\varphi, \kappa)$, it splits precisely if $h(\varphi, \kappa) = 0$. But then there exists a homomorphism $\varepsilon : \Gamma_K \rightarrow \tilde{\Gamma}$ with $p_2 \circ \varepsilon = \text{Id}_{\Gamma_K}$, and $\tilde{\varphi} := p_1 \circ \varepsilon$ is a homomorphism from Γ_K to \tilde{G} with $\kappa \circ \tilde{\varphi} = \varphi$ and hence yields a solution of $\mathcal{E}(\varphi, \kappa)$. Conversely, if the embedding problem $\mathcal{E}(\varphi, \kappa)$ possesses a solution $\tilde{\varphi}$, then the homomorphism $\varepsilon : \Gamma_K \rightarrow \tilde{\Gamma}$,

$\gamma \mapsto (\tilde{\varphi}(\gamma), \gamma)$ splits the group extension in the top row of (6.2). But this implies $h(\varphi, \kappa) = 0$.

For the explicit description of solutions we go back to the defining factor set $\varphi^*(b)$. Since this splits, there exists a $c = (c_\gamma) \in C^1(\Gamma_K, H)$ with $\partial(c) = \varphi^*(b)$, i.e., with

$$c_{\gamma_1}^{\varphi(\gamma_2)} c_{\gamma_2} = c_{\gamma_1 \gamma_2} b_{\varphi(\gamma_1), \varphi(\gamma_2)}. \quad (6.3)$$

From this we may define a homomorphism

$$\tilde{\varphi}_c : \Gamma_K \rightarrow \tilde{G} = \{(\eta, \sigma) \mid \eta \in H, \sigma \in G\}, \quad \gamma \mapsto (c_\gamma, \varphi(\gamma)), \quad (6.4)$$

from Γ_K to $\tilde{G} = H \cdot G$ with the usual composition

$$(\eta_1, \sigma_1)(\eta_2, \sigma_2) = (b_{\sigma_1, \sigma_2}^{-1} \eta_1^{\sigma_2} \eta_2, \sigma_1 \sigma_2),$$

with $\kappa \circ \tilde{\varphi}_c = \varphi$. Since conversely every homomorphism $\tilde{\varphi} : \Gamma_K \rightarrow \tilde{G}$ with $\kappa \circ \tilde{\varphi} = \varphi$ via (6.4) yields a 1-cochain $c = (c_\gamma)$ satisfying (6.3), and thus leads to $\partial(c) = \varphi^*(b)$, the above procedure in fact produces all solutions of $\mathcal{E}(\varphi, \kappa)$. \square

Remark. If in Theorem 6.1 we replace Γ_K by the Galois group E of a Galois extension M/K containing N , and φ by the restriction $\psi : E \rightarrow G$, then $\mathcal{E}(\varphi, \kappa)$ possesses a solution inside M/K if and only if $\psi^*(h) = 0$ in $H^2(E, H)$.

Corollary 6.2. *If in Theorem 6.1 in addition the field K is Hilbertian, then $h(\varphi, \kappa) = 0$ is even equivalent to the proper solvability of $\mathcal{E}(\varphi, \kappa)$.*

Proof. This statement follows from the above Theorem by the Theorem of Ikeda (resp. Corollary 2.5). \square

The following proposition contains an illustrating example for Theorem 6.1 which will be needed later on. For this denote by (a, b) the class of the quaternion algebra

$$\mathbb{A}_{a,b} = K[i, j] \quad \text{with} \quad i^2 = a, j^2 = b, ij = -ji$$

in the Brauer group $\mathrm{Br}_2(K)$, which is isomorphic to $H^2(\Gamma_K, \mathbb{Z}_2)$ (see for example Serre (1979), Ch. XIV, §2).

Proposition 6.3. *Let K be a field of characteristic different from 2, $N := K(\sqrt{x})$ a quadratic extension of K with group $G = \mathbb{Z}_2$ and epimorphism $\varphi : \Gamma_K \rightarrow \mathbb{Z}_2$. Further let κ be the canonical epimorphism of \mathbb{Z}_4 onto \mathbb{Z}_2 . Then the following are equivalent:*

- (1) *The embedding problem $\mathcal{E}(\varphi, \kappa)$ has a (proper) solution.*
- (2) *The element x lies in the norm group of N/K .*
- (3) *In $H^2(\Gamma_K, \mathbb{Z}_2) \cong \mathrm{Br}_2(K)$ we have $(-1, x) = 0$.*

Proof. Since $Z_4 = Z_2 \cdot Z_2$ is a Frattini extension, every solution $\tilde{\varphi}$ of $\mathcal{E}(\varphi, \kappa)$ is already proper by Proposition 1.8. The solution field \tilde{N} then has the form $\tilde{N} = N(\sqrt{y})$ with $y = a + b\sqrt{x}$ and $a, b \in K$. A generating element σ of $\mathrm{Gal}(\tilde{N}/K) \cong \mathbb{Z}_4$

then acts via

$$\sigma : \sqrt{y} \mapsto \sqrt{y'} \mapsto -\sqrt{y} \mapsto -\sqrt{y'}, \quad \sqrt{x} \mapsto -\sqrt{x},$$

where $y' := a - b\sqrt{x}$. Consequently $c := \sqrt{yy'x^{-1}}$ is σ -invariant and thus an element of K^\times with $c^2x = yy' = a^2 - b^2x$. In particular we get that

$$x = \frac{a^2 - b^2x}{c^2} = \mathcal{N}_{N/K}\left(\frac{x}{c}\right) \quad (6.5)$$

is a norm of N/K . Conversely a solution of (6.5) leads to a solution $\tilde{\varphi} : \Gamma_K \rightarrow \text{Gal}(\tilde{N}/K)$ of $\mathcal{E}(\varphi, \kappa)$ with $\tilde{N} := N(\sqrt{y})$ for $y := a + b\sqrt{x}$. This proves the equivalence of (1) and (2).

In the case $b^2 + c^2 \neq 0$ it follows from (6.5) that x may be written as the sum of two squares:

$$x = \left(\frac{ab}{b^2 + c^2}\right)^2 + \left(\frac{ac}{b^2 + c^2}\right)^2 =: u^2 + v^2. \quad (6.6)$$

A corresponding representation also exists in the case $b^2 + c^2 = 0$ since then -1 is a square in K . Thus we have

$$(-1, x) = (-1, u^2 + v^2) = (-1, w^2 + 1) = (-w^2, w^2 + 1) = 0$$

for $w := \frac{u}{v}$. Conversely from $(-1, x) = 0$ there follows the existence of nontrivial $a, b, c \in K$ with $a^2 - b^2x - c^2x = 0$ (see for example Jacobson (1980), Ch. 9.15), and therefore (6.5). This shows the equivalence of (2) and (3). \square

In the next section we introduce the second ingredient of Serre's formulae.

6.2 The Trace Form

Let K be a field with characteristic different from 2 and L/K a separable field extension of degree n . Then

$$q_{L/K} : L \rightarrow K, \quad x \mapsto \text{trace}_{L/K}(x^2), \quad (6.7)$$

is a non-degenerate quadratic form on L with corresponding bilinear form

$$b_{L/K} : L \times L \rightarrow K, \quad (x, y) \mapsto \frac{1}{2}(q_{L/K}(x+y) - q_{L/K}(x) - q_{L/K}(y)). \quad (6.8)$$

Denote by $\{z_1, \dots, z_n\}$ a basis of L/K and write $x \in L$ as $x = \sum_{i=1}^n x_i z_i$ with $x_i \in K$. Then

$$q_{L/K}(x) = \sum_{i,j=1}^n b_{ij} x_i x_j \quad \text{with} \quad b_{ij} = b_{L/K}(z_i, z_j) = \text{trace}_{L/K}(z_i z_j), \quad (6.9)$$

and this defines a non-degenerate quadratic form over K :

$$q_{L/K}(\mathbf{X}) = \sum_{i,j=1}^n b_{ij} X_i X_j \in K[X_1, \dots, X_n]. \quad (6.10)$$

If further

$$\hat{q}_{L/K}(\mathbf{X}) := \sum_{i=1}^n a_i X_i^2 \quad (6.11)$$

is a diagonal form equivalent to $q_{L/K}(\mathbf{X})$, then the element

$$w_2(q_{L/K}) := \sum_{1 \leq i < j \leq n} (a_i, a_j) \in \text{Br}_2(K), \quad (6.12)$$

which is independent of the choice of the diagonal form $\hat{q}_{L/K}$, is called the *Hasse-Witt-invariant* of $q_{L/K}(\mathbf{X})$ (see for example Jacobson (1980), Prop. 9.9 or also Serre (1992), Ch. 9). By the above, $w_2(q_{L/K})$ only depends on the field extension L/K . Furthermore the element of the square class group $K^\times/(K^\times)^2$

$$\prod_{i=1}^n a_i (K^\times)^2 = d_{L/K}(K^\times)^2 \quad (6.13)$$

is the discriminant of the quadratic form $q_{L/K}(\mathbf{X})$. It contains the discriminant $d_{L/K}$ of the field extension L/K .

The next theorem furnishes an important tool for the computation of the Hasse-Witt-invariants of quadratic forms over rational function fields $K = k(t)$:

Theorem 6.4 (Harder). *Let k be a field of characteristic different from 2 and (M, b) a regular bilinear space over the polynomial ring $k[X]$ consisting of a finitely generated projective $k[X]$ -module M and a non-degenerate bilinear form $b : M \times M \rightarrow k[X]$. Then (M, b) is extended from k , i.e., there exists a vector space V over k such that*

$$(M, b) = k[X] \otimes_k (V, b). \quad (6.14)$$

The proof for this result can be found in Scharlau (1985), Ch. 6, Thm. 3.3. Now call a non-degenerate quadratic form over a ring R a *strictly non-degenerate quadratic form* if its discriminant is a unit in R . Then we obtain the following variant of the Theorem of Harder (see also Serre (1992), Thm. 9.1.3):

Corollary 6.5. *A strictly non-degenerate quadratic form over $k[X]$ is extended from k , i.e., it is equivalent over $k[X]$ to a quadratic form with coefficients in k .*

From this we can easily deduce:

Theorem 6.6 (Serre (1992)). *Let k be a field of characteristic different from 2, $K := k(t)$ and L/K a finite separable field extension with Galois closure N/K . Further assume that for all prime divisors $\tilde{\mathfrak{P}}$ of N/K not dividing the numerator divisor of the order of the inertia group $I(\tilde{\mathfrak{P}}/\mathfrak{P})$ in N/K is odd. Then $q_{L/K}(\mathbf{X})$ is equivalent over K to a quadratic form with coefficients in k .*

Proof. Let $R := k[t]$, S the algebraic closure of R in L and \mathfrak{D}_t the t -different of L/K . By the assumption on the orders of the inertia groups in N/K the inverse of the different \mathfrak{D}_t^{-1} is the square of a fractional ideal, $\mathfrak{D}_t^{-1} = \mathfrak{A}^2$ say. The R -module \mathfrak{A} is free of rank $n := [L : K]$ and by construction self-adjoint under the quadratic form $q_{L/K}(\mathbf{X})$. Consequently $d_{L/K}$ is a unit in R and thus an element of k . This proves the assertion using Corollary 6.5. \square

6.3 A Criterion of Serre

For the understanding of Serre's criterion one needs some prerequisites from the cohomology theory of the symmetric groups S_n : It is well known that

$$H^1(S_n, \mathbb{Z}_2) = \langle s_n \rangle \cong \mathbb{Z}_2 \quad \text{for } n \geq 2, \quad (6.15)$$

$$H^2(S_n, \mathbb{Z}_2) = \langle \tilde{s}_n^+, \tilde{s}_n^- \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{for } n \geq 4, \quad (6.16)$$

(see for example Huppert (1967), Kap. V, Satz 25.8), where

$$s_n : S_n \rightarrow \{\pm 1\}$$

is the signature and \tilde{s}_n^\pm are the cohomology classes of the following two non-split central extensions \tilde{S}_n^\pm of S_n :

$$\begin{aligned} \tilde{S}_n^+ &= \langle \sigma, \tau_1, \dots, \tau_{n-1} \mid \sigma^2 = 1, \tau_i^2 = 1, \\ &\quad (\tau_i \tau_{i+1})^3 = 1, \sigma \tau_i = \tau_i \sigma, \tau_i \tau_j = \sigma \tau_j \tau_i \text{ for } j \geq i+2 \rangle, \end{aligned} \quad (6.17)$$

$$\begin{aligned} \tilde{S}_n^- &= \langle \sigma, \tau_1, \dots, \tau_{n-1} \mid \sigma^2 = 1, \tau_i^2 = \sigma, \\ &\quad (\tau_i \tau_{i+1})^3 = \sigma, \tau_i \tau_j = \sigma \tau_j \tau_i \text{ for } j \geq i+2 \rangle. \end{aligned} \quad (6.18)$$

Further in $H^2(S_n, \mathbb{Z}_2)$ with the cup product the following holds:

$$\tilde{s}_n^+ + \tilde{s}_n^- = s_n \cdot s_n =: \tilde{s}_n^\times \quad (6.19)$$

where \tilde{s}_n^\times is the cohomology class of the central extension $\tilde{S}_n^\times = S_n \times_{\mathbb{Z}_2} \mathbb{Z}_4$.

Now as in the previous section let K be a field of characteristic different from 2 and $L = K(x)$ a separable field extension of degree n with minimal polynomial $f \in K[X]$. Then any numbering $x = x_1, \dots, x_n$ of the roots of f defines an embedding of $\text{Gal}(f)$ into S_n and thus with the natural homomorphism $\Gamma_K \rightarrow \text{Gal}(f)$ a homomorphism $\varphi : \Gamma_K \rightarrow S_n$. This induces further homomorphisms

$$\varphi_1^* : H^1(S_n, \mathbb{Z}_2) \rightarrow H^1(\Gamma_K, \mathbb{Z}_2) \cong K^\times / (K^\times)^2, \quad (6.20)$$

$$\varphi_2^* : H^2(S_n, \mathbb{Z}_2) \rightarrow H^2(\Gamma_K, \mathbb{Z}_2) \cong \text{Br}_2(K). \quad (6.21)$$

The images of φ_1^* and φ_2^* can be computed explicitly by formulae discovered by Serre (1984).

Proposition 6.7 (Serre's formulae). *With the notations introduced above we have*

$$(a) \quad \varphi_1^*(s_n) = d_{L/K} \cdot (K^\times)^2, \quad (6.22)$$

$$(b) \quad \varphi_2^*(\tilde{s}_n^+) + (2, d_{L/K}) = w_2(q_{L/K}) = \varphi_2^*(\tilde{s}_n^-) + (-2, d_{L/K}). \quad (6.23)$$

Part (a) of Proposition 6.7 follows directly by combining the map φ of Γ_K to S_n with the sign s_n . The proof of part (b) uses non-abelian cohomology and will not be given here. The reader can find it in the original paper of Serre (1984) or also in Fröhlich (1985). In Serre's article, only the first part of equation (6.23) is shown, but the second follows easily with (6.19) and part (a) since

$$\begin{aligned} \varphi_2^*(\tilde{s}_n^+) + (2, d_{L/K}) &= \varphi_2^*(\tilde{s}_n^-) + \varphi_2^*(s_n \cdot s_n) + (2, d_{L/K}) \\ &= \varphi_2^*(\tilde{s}_n^-) + (d_{L/K}, d_{L/K}) + (2, d_{L/K}) \\ &= \varphi_2^*(\tilde{s}_n^-) + (-1, d_{L/K}) + (2, d_{L/K}) = \varphi_2^*(\tilde{s}_n^-) + (-2, d_{L/K}). \end{aligned}$$

An elementary proof of Proposition 6.7(b) using orthogonal representations instead of non-abelian cohomology has been discovered by Ledet (2000) (see also Ledet (2005), Thm. 6.2.2).

Now let N/K be the Galois hull of L/K with Galois group $G := \text{Gal}(N/K) \cong \text{Gal}(f)$ and

$$1 \longrightarrow Z_2 \xrightarrow{\iota^\pm} \tilde{G}^\pm \xrightarrow{\kappa^\pm} G \longrightarrow 1 \quad (6.24)$$

the central group extension induced by

$$1 \longrightarrow Z_2 \longrightarrow \tilde{S}_n^\pm \longrightarrow S_n \longrightarrow 1.$$

Then by Theorem 6.1 the corresponding embedding problems $\mathcal{E}(\varphi, \kappa^\pm)$ are solvable precisely when $\varphi_2^*(\tilde{s}_n^\pm) = 0$. With these interpretations Serre's formulae (6.23) read as follows:

Theorem 6.8 (Serre (1984)). *Let K be a field of characteristic different from 2, $L := K(x)$ a separable extension of degree $n \geq 4$ and $G = \text{Gal}(f) \leq S_n$ the Galois group of the minimal polynomial f of x over K . Further let N be the Galois closure of L/K and $\varphi : \Gamma_K \rightarrow G$ the canonical epimorphism. Then the following assertions are equivalent for the central Galois extension $\tilde{G}^\pm = Z_2 \cdot G$:*

(1) *The embedding problem $\mathcal{E}(\varphi, \kappa^\pm)$ has a solution.*

(2) *In $\text{Br}_2(K)$ we have $w_2(q_{L/K}) = (\pm 2, d_{L/K})$.*

If these are satisfied and either K is Hilbertian or $\mathcal{E}(\varphi, \kappa)$ does not split, then $\mathcal{E}(\varphi, \kappa^\pm)$ even possesses a proper solution.

Remark. If the Galois group $G = \text{Gal}(f)$ in Theorem 6.8 is already a subgroup of A_n , then $d_{L/K} \in (K^\times)^2$ and hence $(\pm 2, d_{L/K}) = 0$.

With Theorem 6.8 one obtains the original proof of Theorem 5.12 of Mestre (1990). For this one essentially has to show that the Hasse-Witt-invariant of the quadratic trace form $q_{L_a/\mathbb{Q}(t)}$ of the root field $L_a/\mathbb{Q}(t)$ of $f_a(t, X)$ is trivial. By Theorem 6.6 it suffices to check this at $t = 0$. The latter is obvious since $f_a(0, X) = \prod_{i=1}^n (X - a_i)$ with $a_i \in \mathbb{Q}$. To deduce finally that the so obtained solution of the embedding problem in $\tilde{A}_n = 2 \cdot A_n$ is proper geometric, one can, for example, use Proposition 1.8.

In the next section we present the application of Serre's criterion to central extensions of S_n .

6.4 Central Extensions of S_n

The following reduction step for central embedding problems was outlined to us by H. Völklein.

Theorem 6.9. *For a Galois extension N/GK the following are equivalent:*

- (1) *Every central (geometric) embedding problem has a (geometric) solution.*
- (2) *Every (geometric) embedding problem of $\text{Gal}(N/K)$ into subdirect products $(M \cdot G) \times_{G/G'} P$, where P is a central Frattini extension of G/G' and $M \cdot G$ is a representation group of G , has a (geometric) solution.*

Proof. We reduce (2) to (1). For $G := \text{Gal}(N/K)$ let

$$1 \longrightarrow H \xrightarrow{\iota} \tilde{G} \xrightarrow{\kappa} G \longrightarrow 1$$

be a central group extension and $\mathcal{E}(\varphi, \kappa)$ the corresponding embedding problem with the canonical epimorphism $\varphi : \Gamma_K \rightarrow G$. By the Theorem 5.1 of Nobusawa this can be decomposed into a central Frattini embedding problem followed by a split embedding problem with abelian kernel. Since the latter is always solvable by Theorem 2.4, we may assume without loss that H is contained in the Frattini subgroup of \tilde{G} so that

$$H \leq \Phi(\tilde{G}) \cap \mathcal{Z}(\tilde{G}).$$

Let $G = F/R$ be a presentation of G as factor group of the free group F on n generators modulo the relations R . Since $H \leq \Phi(\tilde{G})$, the extension \tilde{G} also has a presentation on n generators, say $\tilde{G} = F/\tilde{R}$, such that H is the preimage of R under the canonical epimorphism from F/\tilde{R} to F/R . As moreover H is central in \tilde{G} , we see that $\tilde{R} \geq [R, F]$, and \tilde{G} is a factor group of $F/[R, F]$. By Huppert (1967), Kap. V, Satz 23.5, $\bar{F} = F/[R, F]$ fits into an exact sequence

$$1 \longrightarrow A \times M \longrightarrow F/[R, F] \longrightarrow G \longrightarrow 1,$$

where $M = (F' \cap R)/[R, F]$ is the Schur multiplier of G and A is free abelian of rank n . Finite factor groups of \bar{F} which project onto G correspond to normal subgroups U of $A \times M$. Without loss we may restrict to the case where $U = A^{(m)} \leq$

$A \times M$ is the free subgroup of m -th powers of the first factor, for some $m \in \mathbb{N}$, since arbitrary finite epimorphic images of \tilde{F} are clearly factors of such with kernel U as above. Then A/U is a central normal subgroup of $\tilde{G} = \tilde{F}/U$, with $\tilde{G}/(A/U) \cong M \cdot G$ a representation group of G . Also, the commutator group \tilde{G}' of \tilde{G} is normal in \tilde{G} and disjoint from A/U since $M = (F' \cap R)/[R, F] \cong G' \cap H$. Now, we have

$$\tilde{G}/\tilde{G}' \cong F/\tilde{R}/F'/(F' \cap \tilde{R}) \cong F/\tilde{R}/F'\tilde{R}/\tilde{R} \cong F/F'\tilde{R} \text{ and } G/G' \cong F/F'R.$$

This shows that \tilde{G}/\tilde{G}' is an extension

$$1 \longrightarrow F'R/F'\tilde{R} \longrightarrow \tilde{G}/\tilde{G}' \longrightarrow G/G' \longrightarrow 1$$

with kernel

$$F'R/F'\tilde{R} \cong R/(R \cap F'\tilde{R}) \cong R/\tilde{R}/(R \cap F'\tilde{R})/\tilde{R} \cong H/M \cong Z_m^n,$$

so that

$$1 \longrightarrow Z_m^n \longrightarrow \tilde{G}/\tilde{G}' \longrightarrow G/G' \longrightarrow 1. \quad (6.25)$$

This is a Frattini extension since $A/U \leq H \leq \Phi(\tilde{G})$, so $Z_m^n \leq \Phi(\tilde{G}/\tilde{G}')$. Thus \tilde{G} may be obtained as a subdirect product

$$\tilde{G} = (M \cdot G) \times_{G/G'} \tilde{G}/\tilde{G}'.$$

□

Remark. If K is a Hilbertian field, then the existence of a solution to a central embedding problem always implies the existence of a proper solution (compare the proof of Theorem 5.14(b)).

If G is a group with cyclic commutator factor group of order $p \in \mathbb{P}$ the criterion takes an especially simple form:

Corollary 6.10. *For a Galois extension N/GK with $|G/G'| = p \in \mathbb{P}$ the following are equivalent:*

- (1) *Every central (geometric) embedding problem has a (geometric) solution.*
- (2) *Every (geometric) embedding problem of $\text{Gal}(N/K)$ into a group of type $\tilde{G} \times_{Z_p} Z_{p^m}$ for $m \geq 1$ has a (geometric) solution, where \tilde{G} is an arbitrary representation group of G .*

We can now prove the main result of this section.

Theorem 6.11 (Sonn (1991)). *For $n \geq 4$ every central group extension of S_n possesses a G -realization over \mathbb{Q} .*

Proof. According to Corollary 6.10 it suffices to show that for suitable G -realizations of S_n over \mathbb{Q} the embedding problems into $\tilde{S}_n^\pm \times_{Z_2} Z_{2^m}$ possess geometric solutions, which are then automatically proper. For this let $n \geq 5$ be an odd natural number and $m \in \mathbb{N}$ fixed, where without loss we may take $m \geq 2$ since \tilde{S}_n^\pm are epimorphic images of $\tilde{S}_n^\pm \times_{Z_2} Z_4$.

By Theorem I.5.1 the cyclic group Z_{2^m} has a G-realization over \mathbb{Q} , say

$$\text{Gal}(M/\mathbb{Q}(v)) \cong Z_{2^m}.$$

Let the quadratic intermediate field herein be generated by the square root of $x \in \mathbb{Q}(v)$. Let w be transcendental over $\mathbb{Q}(v)$ and set $K := \mathbb{Q}(v, w)$. Then \sqrt{x} also generates the quadratic intermediate field of the Galois extension KM/K with $\text{Gal}(KM/K) \cong Z_{2^m}$. The zeroes t_1, t_2 of the polynomial

$$g_2(X) := (X - w - \sqrt{x})(X - w + \sqrt{x}) = X^2 - 2wX + w^2 - x \in K[X]$$

are algebraically independent over \mathbb{Q} since $2w$ and $w^2 - x$ are algebraically independent. Completing these to a system of independent transcendental elements t_1, \dots, t_n over \mathbb{Q} , we see that

$$g(X) := g_2(X) \prod_{i=3}^n (X - t_i) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n \quad (6.26)$$

is a polynomial with coefficients algebraically independent over \mathbb{Q} . From these according to Lemma 5.10 we form the polynomial

$$f(t, X) := g(X) - th(X) \in K(\mathbf{t}, t)[X] \quad \text{with } \mathbf{t} = (t_3, \dots, t_n), \quad (6.27)$$

which by Proposition 5.11(a) has Galois group S_n since $D(g) = D(g_2) =_2 x$. Since \mathbb{Q} is Hilbertian, \mathbf{t} may be specialized to $\mathbf{a} = (a_3, \dots, a_n) \in \mathbb{Q}^{n-2}$ with pairwise distinct a_i such that the residue class polynomial $f_{\mathbf{a}}(t, X)$ also has group S_n over $K(t)$. Now the splitting field $N_{\mathbf{a}}$ of $f_{\mathbf{a}}$ over $K(t)$ contains the field $K(t, \sqrt{x})$, so we get as Galois group of the composite $MN_{\mathbf{a}}$ over $K(t)$

$$\text{Gal}(MN_{\mathbf{a}}/K(t)) \cong S_n \times_{Z_2} Z_{2^m}. \quad (6.28)$$

Let $L_{\mathbf{a}}$ be a root field of $f_{\mathbf{a}}$ over $K(t)$. For the determination of the quadratic trace form $q_{L_{\mathbf{a}}/K(t)}(\mathbf{X})$ of $L_{\mathbf{a}}/K(t)$ we may specialize the variable t to 0 by Theorem 6.6, since the inertia groups of $N_{\mathbf{a}}/K(t, \sqrt{x})$ all have order 3 by the proof of Proposition 5.11. Thus we obtain with (6.27) and (6.26) from $\text{trace}(1^2) = 2$ and $\text{trace}(\sqrt{x^2}) = 2x$

$$q_{L_{\mathbf{a}}/K(t)} \sim 2X_1^2 + 2xX_2^2 + X_3^2 + \dots + X_n^2$$

and hence the Hasse-Witt-invariant

$$w_2(q_{L_{\mathbf{a}}/K(t)}) = (2, 2x) = (2, x). \quad (6.29)$$

With Serre's formulae (Proposition 6.7(b)) and using $d_{L_{\mathbf{a}}/K(t)} =_2 x$ the embedding obstructions thus equal

$$\varphi^*(\tilde{s}_n^+) = w_2(q_{L_{\mathbf{a}}/K(t)}) + (2, d_{L_{\mathbf{a}}/K(t)}) = (2, x) + (2, x) = 0,$$

$$\varphi^*(\tilde{s}_n^-) = w_2(q_{L_{\mathbf{a}}/K(t)}) + (-2, d_{L_{\mathbf{a}}/K(t)}) = (2, x) + (-2, x) = (-1, x) = 0$$

by Proposition 6.3, since by construction $K(t, \sqrt{x})/K(t)$ can be embedded into a Z_4 -extension. Consequently for $G = S_n$ both embedding problems $\mathcal{E}(\varphi, \kappa^\pm)$ in Theorem 6.8 possess a proper solution. Their solution fields $\tilde{N}_{\underline{\mathbf{a}}}^\pm$ satisfy

$$\mathrm{Gal}(\tilde{N}_{\underline{\mathbf{a}}}/K(t)) \cong \tilde{S}_n^\pm. \quad (6.30)$$

Now $\tilde{N}_{\underline{\mathbf{a}}}^\pm/K(t)$ is not geometric with respect to K , since \sqrt{x} is algebraic over K . But as $\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}$ is regular, extension of constants with $\bar{\mathbb{Q}}$ furnishes a Galois extension $\bar{\mathbb{Q}}\tilde{N}_{\underline{\mathbf{a}}}^\pm/\bar{\mathbb{Q}}K(t)$ with isomorphic Galois group. If $\tilde{f}_{\underline{\mathbf{a}}}^\pm(v, w, t, X) \in K(t)[X]$ is a generating normal polynomial of this Galois extension, then by Theorem 1.3 the Hilbert set $\mathcal{H}_{\mathbb{Q}K(t)}(\tilde{f}_{\underline{\mathbf{a}}}^\pm(v, w, t, X))$ contains elements in \mathbb{Q}^3 . In particular w, t may be specialized to elements $a_1, a_2 \in \mathbb{Q}$ such that $\tilde{f}_{\underline{\mathbf{a}}}^\pm(v, x) := \tilde{f}_{\underline{\mathbf{a}}}^\pm(v, a_1, a_2, X)$ generates a geometric Galois extension $\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(v)$ with

$$\mathrm{Gal}(\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(v)) \cong \tilde{S}_n^\pm. \quad (6.31)$$

Since its quadratic subextension is $\mathbb{Q}(v, \sqrt{x})$, we further see that

$$\tilde{G}^\pm := \mathrm{Gal}(M\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(v)) \cong \tilde{S}_n^\pm \times_{Z_2} Z_{2^m}. \quad (6.32)$$

It remains to show that $M\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(v)$ is geometric. This follows from the fact that

$$\tilde{U} := \mathrm{Gal}(M\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(v, \sqrt{x})) \cong \tilde{A}_n \times_{Z_2} Z_{2^m}$$

is the only maximal normal subgroup of \tilde{G}^\pm . This completes the proof for odd n .

As in the proof of Theorem 5.12 of Mestre one notes that the root field $L_{\underline{\mathbf{a}}}$ of $f_{\underline{\mathbf{a}}}$ (obtained from $f_{\underline{\mathbf{a}}}$ by specializing w, t to a_1, a_2 as above) is a rational function field over \mathbb{Q} , say $L_{\underline{\mathbf{a}}} = \mathbb{Q}(u)$. Thus $\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(u)$ is a geometric Galois extension with

$$\mathrm{Gal}(\tilde{N}_{\underline{\mathbf{a}}}^\pm/\mathbb{Q}(u)) \cong \tilde{S}_{n-1} \times_{Z_2} Z_{2^m}.$$

This yields the desired result also in the case of even n . □

The above proof even shows the following about the splitting field $N_{\underline{\mathbf{a}}}/\mathbb{Q}(v)$ of $f_{\underline{\mathbf{a}}}(v, t)$:

Corollary 6.12. *For $n \geq 4$ the Galois extensions $N_{\underline{\mathbf{a}}}/s_n\mathbb{Q}(v)$ for n odd respectively $N_{\underline{\mathbf{a}}}/s_n\mathbb{Q}(u)$ for n even are universally central embeddable.*

Remark. By Theorems 5.12 and 6.11 the three groups $\tilde{A}_4 \cong \mathrm{SL}_2(3)$, $\tilde{S}_4^+ \cong \mathrm{GL}_2(3)$ and \tilde{S}_4^- possess G-realizations over \mathbb{Q} . According to Dentzer (1995b) these are the only non-semiabelian groups G of order $|G| < 64$.

Apart from the above examples the criterion of Serre was also applied to prove the existence of G-realizations over \mathbb{Q} for the groups $6 \cdot A_6$, $6 \cdot A_7$, $\mathrm{SL}_2(7)$ and $2 \cdot M_{12}$ by Mestre (1994, 1998) and for $2 \cdot S_6(2)$ by Häfner (1992). In particular the G-realizations of the simple groups A_6, A_7 , etc. are universally central embeddable. Further applications are collected in Bayer-Fluckiger (1994), §5.

7 Brauer Embedding Problems

Brauer embedding problems are the natural generalization of the central embedding problems with kernel Z_2 considered in the previous paragraph. Here we first prove that the solvability of Brauer embedding problems implies the existence of proper regular solutions. Then we show that the ordinary solvability satisfies a local-global principle in the horizontal case (localization with respect to prime divisors of the field of constants) as well as in the vertical case (localization with respect to prime divisors over the field of constants). The latter finally allows to obtain G-realizations for a number of central extensions of simple groups over \mathbb{Q}^{ab} .

7.1 Regular Solutions of Brauer Embedding Problems

A *Brauer embedding problem over K* is an embedding problem $\mathcal{E}(\varphi, \kappa)$ with finite abelian kernel, whose kernel H is isomorphic to a subgroup of the group of units U_N of $N = \bar{K}^{\ker(\varphi)}$ as G -operator group (with $G = \text{im}(\varphi)$). Thus H is generated by a root of unity ζ_n of order n lying in N , and the embedding obstruction $h(\varphi, \kappa)$ for $h \in H^2(G, H)$ lies in $H^2(\Gamma_K, \langle \zeta_n \rangle)$. The name is explained by the following result:

Proposition 7.1. *Let K be a field of characteristic prime to n . Then we have*

$$H^2(\Gamma_K, \langle \zeta_n \rangle) \cong \text{Br}_n(K), \quad (7.1)$$

where $\text{Br}_n(K)$ denotes the n -torsion of the Brauer group $\text{Br}(K)$ of K .

Proof. From the short exact sequence

$$1 \longrightarrow \langle \zeta_n \rangle \longrightarrow \bar{K}^\times \xrightarrow{n} \bar{K}^\times \longrightarrow 1$$

follows, using Hilbert's Theorem 90, the exactness of

$$0 = H^1(\Gamma_K, \bar{K}^\times) \longrightarrow H^2(\Gamma_K, \langle \zeta_n \rangle) \longrightarrow H^2(\Gamma_K, \bar{K}^\times) \xrightarrow{n} H^2(\Gamma_K, \bar{K}^\times)$$

and hence the assertion due to

$$\text{Br}(K) \cong H^2(\Gamma_K, \bar{K}^\times) \quad (7.2)$$

(see for example Serre (1979), Ch. XIV, §2). \square

By Proposition 7.1 the solvability of Brauer embedding problems may be decided inside $\text{Br}_n(K)$ and hence inside the Brauer group $\text{Br}(K)$. From one solution of such a Brauer embedding problem, further ones can be obtained in an easy way, as is shown in the next theorem:

Theorem 7.2. Let $\tilde{N} := N(\sqrt[n]{x})$ be a solution field of the Brauer embedding problem $\mathcal{E}(\varphi, \kappa)$ with kernel $H \cong \mathbb{Z}_n$ over K . Then all solution fields of $\mathcal{E}(\varphi, \kappa)$ are of the form

$$\tilde{N}_a := N(\sqrt[n]{ax}) \quad \text{with } a \in K^\times. \quad (7.3)$$

Proof. According to Theorem 6.1(b) there exists $c \in C^1(\Gamma_K, H)$ such that $\tilde{\varphi}_c : \Gamma_K \rightarrow \tilde{G} = H \cdot G$ in (6.4) is a solution of $\mathcal{E}(\varphi, \kappa)$ with solution field $\tilde{N} := N(\sqrt[n]{x})$. By assumption H is isomorphic as G -module to $\langle \zeta_n \rangle \leq N^\times$. For a fixed zero y of $X^n - x \in N[X]$ we get apart from c a further homomorphism

$$d : \Gamma_N \rightarrow \langle \zeta_n \rangle, \quad \gamma \mapsto y^{\gamma-1},$$

with the same kernel $\Gamma_c = \text{Gal}(\bar{K}/\tilde{N})$. Since c and d differ only by an automorphism of $\langle \zeta_n \rangle$ and as $\zeta_n \in N$, the cochain c defining \tilde{N} can be chosen so that we even have $d(\gamma) = c_\gamma$ and hence $c_\gamma = y^{\gamma-1}$ for all $\gamma \in \Gamma_N$.

If now $N(\tilde{y})$ with $\tilde{y}^n = \tilde{x} \in N$ is any solution field of $\mathcal{E}(\varphi, \kappa)$, a suitable defining cochain \tilde{c} satisfies correspondingly $\tilde{c}_\gamma = \tilde{y}^{\gamma-1}$ and $\delta(\tilde{c}c^{-1}) = 1$. In particular we have $\tilde{c}c^{-1} \in Z^1(\Gamma_K, \langle \zeta_n \rangle) \subseteq Z^1(\Gamma_K, \bar{K}^\times)$, which since $H^1(\Gamma_K, \bar{K}^\times) = 1$ implies $\tilde{c}c^{-1} \in B^1(\Gamma_K, \bar{K}^\times)$. Hence there exists an $\tilde{a} \in \bar{K}^\times$ with $\tilde{c}_\gamma c_\gamma^{-1} = \tilde{a}^{\gamma-1}$ for all $\gamma \in \Gamma_K$. Since $(\tilde{a}^n)^{\gamma-1} = 1$ this shows that $\tilde{a}^n =: a \in K$. As

$$\tilde{y}^{\gamma-1} = \tilde{c}_\gamma = \tilde{a}^{\gamma-1} c_\gamma = (\tilde{a}y)^{\gamma-1},$$

it follows that $N(\tilde{y}) = N(\tilde{a}y) = N(\sqrt[n]{ax})$.

Conversely, any field $N(\sqrt[n]{ax})$ with $a \in K$ clearly gives a solution field for $\mathcal{E}(\varphi, \kappa)$, with the cochain $(\sqrt[n]{a^{\gamma-1}} c_\gamma) \in C^1(\Gamma_K, \langle \zeta_n \rangle)$, for example. \square

The preceding theorem has the following easy consequence:

Corollary 7.3. If a Brauer embedding problem over a field K is solvable, then it also possesses a proper regular solution.

Proof. Let $\tilde{N} = N(\sqrt[n]{x})$ be a solution field of the given Brauer embedding problem $\mathcal{E}(\varphi, \kappa)$ over K with $N = \bar{K}^{\ker(\varphi)}$. Then $\tilde{N}(t) = N(t, \sqrt[n]{x})$ is a solution field of the Brauer embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ lifted to the rational function field $K(t)$ (compare Section 1.2). By Theorem 7.2 the field $\tilde{N}^* := N(t, \sqrt[n]{tx})$ also gives a solution field of $\mathcal{E}(\varphi^*, \kappa^*)$. As N is algebraically closed in \tilde{N}^* and moreover $[\tilde{N}^* : N(t)] = n$, this belongs to a proper regular solution of $\mathcal{E}(\varphi, \kappa)$. \square

It thus remains to study the question of solvability of Brauer embedding problems. Here local-global principles prove to be effective.

7.2 The Horizontal Local-Global Principle

The basis for the subsequent proofs is given by the following structure theorem for the Brauer group of rational function fields, which goes back in characteristic zero to Faddeev (1951), and for non-zero characteristic to Auslander and Brumer (1968):

Theorem 7.4. Let $K = k(t)$ be a rational function field in one variable, and p a prime different from the characteristic of k . Then the sequence of p -primary components of Brauer groups

$$0 \rightarrow \mathrm{Br}_{p^\infty}(k) \rightarrow \mathrm{Br}_{p^\infty}(K) \rightarrow \bigoplus_{\mathfrak{P} \in \mathrm{P}_0(K/k)} \mathrm{Br}_{p^\infty}(K_{\mathfrak{P}})/\mathrm{Br}_{p^\infty}(K_{\mathfrak{P}}) \rightarrow 0 \quad (7.4)$$

is exact and splits, where $\mathrm{P}_0(K/k)$ is the set of primes of K/k different from \mathfrak{P}_∞ , $K_{\mathfrak{P}}$ denotes the completion and $K_{\mathfrak{P}}$ the residue class field of K at \mathfrak{P} .

A simple proof of this result can be found in Scharlau (1969), Kor. 2.2, for example. With the following exact sequence going back to Witt (see Serre (1979), Ch. XII, Thm. 2)

$$0 \longrightarrow \mathrm{Br}(K_{\mathfrak{P}}) \longrightarrow \mathrm{Br}(K_{\mathfrak{P}}) \longrightarrow \Gamma_{K_{\mathfrak{P}}}^* \longrightarrow 0, \quad (7.5)$$

where $\Gamma_{K_{\mathfrak{P}}}^*$ denotes the group of continuous homomorphisms from the absolute Galois group $\Gamma_{K_{\mathfrak{P}}}$ to \mathbb{Q}/\mathbb{Z} , we obtain from (7.4) the Theorem of Auslander, Brumer and Faddeev in the following form:

Corollary 7.5. Under the assumptions of Theorem 7.4 we have

$$\mathrm{Br}_{p^\infty}(K) \cong \mathrm{Br}_{p^\infty}(k) \oplus \bigoplus_{\mathfrak{P} \in \mathrm{P}_0(K/k)} (\Gamma_{K_{\mathfrak{P}}}^*)_{p^\infty}. \quad (7.6)$$

By construction, this result is compatible with extension of constants, i.e., for a field extension l/k linearly disjoint from K/k and $L := l(t)$ the following diagram becomes commutative

$$\begin{array}{ccc} \mathrm{Br}_{p^\infty}(K) & \longrightarrow & \mathrm{Br}_{p^\infty}(k) \oplus \bigoplus_{\mathfrak{P} \in \mathrm{P}_0(K/k)} (\Gamma_{K_{\mathfrak{P}}}^*)_{p^\infty} \\ \downarrow & & \downarrow \\ \mathrm{Br}_{p^\infty}(L) & \longrightarrow & \mathrm{Br}_{p^\infty}(l) \oplus \bigoplus_{\mathfrak{Q} \in \mathrm{P}_0(L/l)} (\Gamma_{L_{\mathfrak{Q}}}^*)_{p^\infty}, \end{array} \quad (7.7)$$

where the horizontal arrows denote the isomorphisms in Corollary 7.5 and the vertical arrows are the restriction maps, such that on the right hand side $\Gamma_{K_{\mathfrak{P}}}^*$ is mapped component-wise onto $\bigoplus_{\mathfrak{Q}|\mathfrak{P}} \Gamma_{L_{\mathfrak{Q}}}^*$.

With this statement the following result can be derived without difficulty:

Proposition 7.6. Let $K = k(t)$ be a rational function field in one variable over a global field and p a prime different from the characteristic of k . Then the product of the restriction maps

$$\rho : \mathrm{Br}_{p^\infty}(K) \longrightarrow \prod_{\mathfrak{p} \in \mathrm{P}(k)} \mathrm{Br}_{p^\infty}(K_{\mathfrak{p}}) \quad (7.8)$$

is injective, where \mathfrak{p} runs over all prime divisors (places) of k including the infinite ones, and $K_{\mathfrak{p}} := k_{\mathfrak{p}}(t)$ denotes the rational function field over the completion of k with respect to \mathfrak{p} .

Proof. For the proof we employ (7.7) with $l = k_{\mathfrak{p}}$ and $L = K_{\mathfrak{p}}$. By Corollary 7.5 it thus remains to show that the map

$$\rho : \text{Br}_{p^\infty}(k) \oplus \bigoplus_{\mathfrak{P} \in \text{IP}_0(K/k)} (\Gamma_{K_{\mathfrak{P}}}^*)_{p^\infty} \longrightarrow \prod_{\mathfrak{p} \in \text{IP}(k)} \left(\text{Br}_{p^\infty}(k_{\mathfrak{p}}) \oplus \bigoplus_{\mathfrak{Q} \in \text{IP}_0(K_{\mathfrak{p}}/k_{\mathfrak{p}})} (\Gamma_{K_{\mathfrak{p}} \mathfrak{Q}}^*)_{p^\infty} \right) \quad (7.9)$$

is injective. The injectivity on $\text{Br}_{p^\infty}(k)$ is assured by a classical theorem of Brauer, Hasse and Noether (see for example Weil (1974), Ch. XI, Thm. 2). It thus suffices to show the injectivity of

$$\rho_{\mathfrak{P}} : (\Gamma_{K_{\mathfrak{P}}}^*)_{p^\infty} \rightarrow \prod_{\mathfrak{p} \in \text{IP}(k)} \bigoplus_{\mathfrak{Q} \mid \mathfrak{P}} (\Gamma_{K_{\mathfrak{p}} \mathfrak{Q}}^*)_{p^\infty}.$$

Therefore let $f \in \ker(\rho_{\mathfrak{P}})$ and $N/K\mathfrak{P}$ the cyclic extension defined by the fixed field of $\ker(f)$. Then we have $NK_{\mathfrak{p}}\mathfrak{Q} = K_{\mathfrak{p}}\mathfrak{Q}$ for all $\mathfrak{p} \in \text{IP}(k)$ and $\mathfrak{Q} \in \text{IP}(K_{\mathfrak{p}}/k_{\mathfrak{p}})$ with $\mathfrak{Q} \mid \mathfrak{P}$, i.e., every prime divisor of $K\mathfrak{P}$ splits completely in $N/K\mathfrak{P}$. This implies $N = K\mathfrak{P}$ and hence $f = 0$, as desired. \square

Remark. The assertion of Proposition 7.6 continues to hold for rational function fields in several variables over global fields (see Sonn (1990), Thm. 2).

Now let k be a global field and $\mathcal{E}(\varphi, \kappa)$ a finite embedding problem over $K := k(t)$ with $\varphi : \Gamma_K \rightarrow G = \text{Gal}(N/K)$ and $\kappa : \tilde{G} \rightarrow G$. Then to each $\mathfrak{p} \in \text{IP}(k)$ is associated in a natural way a restriction map

$$\varphi_{\mathfrak{p}} : \Gamma_{K_{\mathfrak{p}}} \rightarrow G_{\mathfrak{p}} = \text{Gal}(NK_{\mathfrak{p}}/K_{\mathfrak{p}}), \quad (7.10)$$

and after identification of $G_{\mathfrak{p}}$ with the decomposition group of some $\tilde{\mathfrak{p}}/\mathfrak{p}$ in G also an epimorphism

$$\kappa_{\mathfrak{p}} : \tilde{G}_{\mathfrak{p}} := \kappa^{-1}(G_{\mathfrak{p}}) \rightarrow G_{\mathfrak{p}}. \quad (7.11)$$

These two epimorphisms define an embedding problem $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ over $K_{\mathfrak{p}}$ with the same kernel as $\mathcal{E}(\varphi, \kappa)$. In the case of Brauer embedding problems Proposition 7.6 furnishes the following local-global-principle.

Theorem 7.7 (Sonn (1990)). *Let $K = k(t)$ be a rational function field over a global field and $\mathcal{E}(\varphi, \kappa)$ a Brauer embedding problem over K , whose kernel has order prime to the characteristic of k . Then $\mathcal{E}(\varphi, \kappa)$ is solvable over K if and only if for all $\mathfrak{p} \in \text{IP}(k)$ the local Brauer embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are solvable over $K_{\mathfrak{p}} = k_{\mathfrak{p}}(t)$.*

Proof. By Theorem 1.6 we may assume that the order n of the kernel is a prime power. Let $h(\varphi, \kappa) \in H^2(\Gamma_K, \langle \zeta_n \rangle) \cong \text{Br}_n(K)$ be the cohomological obstruction to the embedding problem $\mathcal{E}(\varphi, \kappa)$. Then the images $h(\varphi, \kappa)_{\mathfrak{p}} \in \text{Br}_n(K_{\mathfrak{p}})$ of $h(\varphi, \kappa)$ under the map ρ in (7.8) constitute the cohomological obstructions of the local Brauer embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$. If all these are solvable, then $h(\varphi, \kappa)_{\mathfrak{p}} = 0$

for all $\mathfrak{p} \in \text{IP}(k)$ by Theorem 6.1. The solvability of $\mathcal{E}(\varphi, \kappa)$ then follows from the injectivity of ρ . \square

With the proof of Theorem 7.7 we immediately obtain the following variant of the Theorem of Brauer, Hasse and Noether used in the proof:

Corollary 7.8. *Over global fields the local-global principle for Brauer embedding problems is valid.*

With Theorem 7.7 Brauer embedding problems over rational function fields with global field of constants can be reduced to Brauer embedding problems over rational function fields with complete field of constants. Such field extensions will be the subject of the following chapter.

7.3 The Vertical Local-Global Principle

The basis of the vertical local-global principle for Brauer embedding problems is given by the following corollary to Theorem 7.4:

Proposition 7.9. *Let $K = k(t)$ be a rational function field in one variable and p a prime different from the characteristic of k . Then the product of the restriction maps*

$$\rho : \text{Br}_{p^\infty}(K) \rightarrow \prod_{\mathfrak{P} \in \text{IP}_0(K/k)} \text{Br}_{p^\infty}(K_{\mathfrak{P}}) \quad (7.12)$$

is injective, where \mathfrak{P} runs over all prime divisors of K/k different from \mathfrak{P}_∞ and $K_{\mathfrak{P}}$ denotes the completion of K with respect to \mathfrak{P} .

Remark. Proposition 7.9 also holds in the case that p equals the characteristic of K (see for example Kucera (1994), Lemma 8).

As in the previous section this implies a local-global-principle for Brauer embedding problems:

Theorem 7.10 (Sonn (1994a)). *Let $K = k(t)$ be a rational function field in one variable and $\mathcal{E}(\varphi, \kappa)$ a Brauer embedding problem over K , whose kernel has order prime to the characteristic of k . Then $\mathcal{E}(\varphi, \kappa)$ is solvable over K if and only if for all $\mathfrak{P} \in \text{IP}_0(K/k)$ the local Brauer embedding problems $\mathcal{E}(\varphi_{\mathfrak{P}}, \kappa_{\mathfrak{P}})$ are solvable over $K_{\mathfrak{P}}$.*

The vertical local-global-principle becomes particularly easy to use if the field of constants has a projective absolute Galois group, since then the local embedding problems have to be solved only for the finitely many ramified \mathfrak{P} .

Theorem 7.11 (Sonn (1994b)). *Let $K = k(t)$ be a rational function field in one variable over a field k with projective Galois group and N/K a finite Galois extension ramified at the prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ of K/k and possibly at the infinite*

prime \mathfrak{P}_∞ . Also let $\mathcal{E}(\varphi, \kappa)$ with $\varphi : \Gamma_K \rightarrow \text{Gal}(N/K)$ be a Brauer embedding problem whose kernel H has order prime to the characteristic of k . Then $\mathcal{E}(\varphi, \kappa)$ is solvable if and only if the finitely many local embedding problems $\mathcal{E}(\varphi_{\mathfrak{P}_i}, \kappa_{\mathfrak{P}_i})$ for $i = 1, \dots, r$ are solvable.

Proof. Note that for prime divisors $\tilde{\mathfrak{P}}/\mathfrak{P}$ not ramified in N/K , the local field extensions $N_{\tilde{\mathfrak{P}}}/K_{\mathfrak{P}}$ are extensions of constants of power series fields, since $K_{\mathfrak{P}} = K\mathfrak{P}((t))$ and $N_{\tilde{\mathfrak{P}}} = N\tilde{\mathfrak{P}}((t))$. Thus solutions of $\mathcal{E}(\varphi_{\mathfrak{P}}, \kappa_{\mathfrak{P}})$ can be obtained by lifting solutions of a finite embedding problem with kernel H over the field $K\mathfrak{P}$ with projective absolute Galois group, which is always solvable by Corollary 1.12. \square

From the above we may derive a particularly simple sufficient criterion for the solvability of local embedding problems in the ramified case.

Corollary 7.12. *Assume that K contains the $\exp(\tilde{G})$ -th roots of unity, where $\tilde{G} = H \cdot G$. For the solvability of $\mathcal{E}(\varphi, \kappa)$ it suffices that for each $\mathfrak{P}_i \in \mathbb{P}(K/k)$ ramified in N/K different from \mathfrak{P}_∞ the inertia group $I_i = I(\tilde{\mathfrak{P}}_i/\mathfrak{P}_i)$ satisfies either*

$$\gcd(|I_i|, |H|) = 1 \quad \text{or} \quad \mathcal{C}_G(I_i) = I_i. \quad (7.13)$$

Proof. The Galois extension $N_{\tilde{\mathfrak{P}}_i}/K_{\mathfrak{P}_i}$ is composed of the extension of constants $N\tilde{\mathfrak{P}}_i((t))/K\mathfrak{P}_i((t))$ followed by a cyclic extension $N_{\tilde{\mathfrak{P}}_i}/N\tilde{\mathfrak{P}}_i((t))$ of degree $e_i = |I_i|$ regular over $N\tilde{\mathfrak{P}}_i$. Thus the first of these two extensions is Galois and the second a Kummer extension with the group $I_i \leq \mathcal{L}(G_i)$ for $G_i = \text{Gal}(N_{\tilde{\mathfrak{P}}_i}/K_{\mathfrak{P}_i})$.

In the case $\gcd(|I_i|, |H|) = 1$ the preimage of I_i in $\tilde{G}_i = H \cdot G_i$ splits into a direct product $H \times \tilde{I}_i$ with $\tilde{I}_i \cong I_i$ and $\kappa_{\mathfrak{P}_i}(\tilde{I}_i) = I_i$. By the assumption on the projectivity of Γ_K the embedding problem belonging to the group extension

$$1 \longrightarrow H \longrightarrow \tilde{G}_i / \tilde{I}_i \longrightarrow G_i / I_i \longrightarrow 1$$

is solvable (by extension of constants), with solution $\tilde{\varphi}_i : \Gamma_K \rightarrow \tilde{G}_i / \tilde{I}_i$, say. According to the universal mapping property of the fiber product there also exists a homomorphism

$$\tilde{\varphi}_{\mathfrak{P}_i} : \Gamma_K \rightarrow \tilde{G}_i = G_i \times_{G_i / I_i} \tilde{G}_i / \tilde{I}_i$$

with $\kappa_{\mathfrak{P}_i} \circ \tilde{\varphi}_{\mathfrak{P}_i} = \varphi_{\mathfrak{P}_i}$ and thus a solution to $\mathcal{E}(\varphi_{\mathfrak{P}_i}, \kappa_{\mathfrak{P}_i})$.

In the second case $I_i \cong \mathcal{C}_G(I_i) \cong \mathcal{N}_G(I_i)$ we have $I_i = G_i$ since $G_i \trianglelefteq \mathcal{N}_G(I_i)$. Hence $N_{\tilde{\mathfrak{P}}_i}/K_{\mathfrak{P}_i}$ is a Kummer extension generated by the e_i -th root of some $u \in K_{\mathfrak{P}}^\times$. Denoting by \tilde{e}_i the exponent of $\tilde{G}_i = H \cdot G_i$, the field $K_{\mathfrak{P}_i}(v)$ with $v^{\tilde{e}_i} = u$ yields a solution field and thus a (not necessarily proper) solution of $\mathcal{E}(\varphi_{\mathfrak{P}_i}, \kappa_{\mathfrak{P}_i})$. \square

Remark. Using the reduction theorem of Kochendörffer in Section 8.1 the conditions for the solvability of $\mathcal{E}(\varphi_{\mathfrak{P}_i}, \kappa_{\mathfrak{P}_i})$ on the inertia groups I_i can be weakened to

$$\gcd((G_i : I_i), (H : C_i)) = 1, \quad (7.14)$$

where $G_i = \mathcal{C}_G(I_i)$ and C_i is a complement of the Frattini extension inside the group extension $H \cdot I_i = \kappa^{-1}(I_i)$ (as described in Theorem 5.1).

In the next section we collect some examples for the application of the vertical local-global-principle.

7.4 Covering Groups of Simple Groups over $\mathbb{Q}^{\text{ab}}(t)$

With the help of the vertical local-global-principle a number of covering groups of classical groups which do not belong to the matrix groups investigated in Chapter II can be realized as geometric Galois groups over $\mathbb{Q}^{\text{ab}}(t)$.

Theorem 7.13 (Sonn (1994b), Malle and Sonn (1996)). *The universal central extensions of the following almost simple groups have G-realizations over $\mathbb{Q}^{\text{ab}}(t)$:*

- (a) $\text{PGL}_n(q)$ for $n \geq 3$ or $q \geq 4$,
- (b) $\text{PGU}_n(q)$ for $n \geq 3$, $(n, q) \neq (3, 2)$,
- (c) $\text{PCSp}_{2n}(q)$ for $n \geq 2$,
- (d) $\text{SO}_{2n+1}(q)$ for $n \geq 3$, q odd,
- (e) $\text{E}_7(q)$ and $\text{E}_7(q)_{ad}$ for $q = p^\nu$ with $p \geq 3$.

Proof. First note that if G is such that $S \leq G \leq \text{Aut}(S)$ for a non-abelian simple group S , then the Schur multiplier of G is a subgroup of that of S (see Sonn (1994b), Lemma 6). In case (d), the Schur multiplier of $\text{O}_{2n+1}(q)$ is cyclic of order 2 except for $\text{O}_7(3)$, where it has order 6. In the general case, the criterion in Corollary 7.12 applies to the Galois realizations of $\text{SO}_{2n+1}(q)$ in Theorem II.3.7 with the class vector containing one class of involutions, a class of elements of odd order, and a class of self-centralizing semisimple elements, since the orders of the elements in the first two classes are coprime. This also gives the result for the exceptional case $\text{O}_7(3)$.

Similarly in cases (b), (c) we can start with the G-realization of $\text{GU}_n(q)$ respectively $\text{CSp}_{2n}(q)$ in Theorems II.3.2 and II.3.4, since again these have the properties required in Corollary 7.12. Some care has to be taken due to several exceptional multipliers, see Sonn (1994b) and Malle and Sonn (1996).

The Schur multiplier of $\text{E}_7(q)$, q odd, has order 2. So for (e), the assertion may be deduced from Theorem II.5.17, where we obtained a Galois realization of $\text{E}_7(q)_{ad}$ with respect to a class vector containing a class C_p of elements of order p and a class C_T^δ containing elements generating their proper centralizer.

The proof for case (a) is similar, starting from the G-realizations of the groups $\text{PGL}_n(q)$ given by Walter (1984) (see also the Remark after Theorem II.3.2; the G-realizations of Belyi presented in Section II.1.3 are not suited for an application of Corollary 7.12.) See Sonn (1994b) for details. \square

For the sporadic groups, we have an almost complete result (see Malle and Sonn (1996)):

Theorem 7.14. *The full covering groups of all groups G with $S \leq G \leq \text{Aut}(S)$, where S is sporadic simple with the possible exception of M_{22} , possess G -realizations over $\mathbb{Q}^{\text{ab}}(t)$.*

Proof. By the Remark after Theorem 5.8, the threefold covering groups of G as in the Theorem, for $S \neq J_3$, are already realized as Galois groups over $\mathbb{Q}(t)$. We treat the remaining groups S with non-trivial Schur multiplier.

In Propositions. II.9.1–II.9.7 we proved G -realizations for the automorphism groups of sporadic groups S with class vector \mathbf{C} listed in Table 7.1. In all cases, elements from the first two classes have coprime orders, while those in the third class generate their full centralizer. Choosing one ramification point at infinity, it follows that Corollary 7.12 applies regardless of the order of the p -primary part of the Schur multiplier we are looking at.

Table 7.1 Class vectors for some sporadic groups

$\text{Aut}(S)$	\mathbf{C}
$M_{12}:2$	$(2C, 3A, 12A)$
$J_2:2$	$(3A, 8C, 14A)$
$HS:2$	$(2C, 5C, 30A)$
Co_1	$(3A, 5C, 13A)$
$F_{i22}:2$	$(2D, 5A, 42A)$
B	$(2C, 3A, 55A)$
Ru	$(2A, 5A, 13A)$

This only leaves the groups Suz and J_3 to consider. Hunt (1986) gave a G -realization for $\text{Aut}(Suz)$ with the rationally rigid class vector $(2C, 3B, 28A)$. The Schur multiplier here has order 6, and elements from class $28A$ are self-centralizing. For J_3 it is easy to verify that $(2B, 3A, 34A)$ provides a semirational rigid class vector of $\text{Aut}(J_3)$. As J_3 has Schur multiplier of order 3 we can apply the criterion. \square

Further applications of Brauer embedding problems in particular for groups of small order are collected in the monograph of Ledet (2005).

8 Concordant Embedding Problems

Every embedding problem is accompanied by embedding problems belonging to sections of the group extension. At least a necessary condition for the solvability of an embedding problem is then the solvability of all accompanying Brauer embedding problems. This condition was introduced by Delone and Faddeev (1944) and is nowadays called concordance condition. In order to avoid special cases in positive characteristic in the characterization, we first solve embedding problems whose kernel has order a power of the characteristic of the ground field. For this we employ among others the reduction theorem of Kochendörffer, which will be proved more generally for regular solutions. After that we show that the standard reduction theorems including the theorem of Kochendörffer continue to hold for the concordance condition. Finally as the main result of this paragraph we show, using a duality theorem of Tate, that abelian embedding problems over global fields are concordant if and only if all induced local embedding problems are solvable.

8.1 The Reduction Theorem of Kochendörffer

As a preparation for the proof of the theorem of Kochendörffer for regular embedding problems we need to introduce a generalization of the wreath product construction. Let G be group with subgroup U and let

$$1 \longrightarrow H \longrightarrow \tilde{U} \xrightarrow{\pi} U \longrightarrow 1$$

be an exact sequence of groups. We choose and fix a system of right coset representatives of U in G and denote by $\bar{\sigma}$ the coset representative of $\sigma \in G$. Let $H \wr_U G$ be the set of pairs

$$H \wr_U G := \{(\sigma, \psi) \mid \sigma \in G, \psi : G/U \rightarrow \tilde{U} \text{ such that } \pi(\psi(\tau)) = \overline{\tau\sigma^{-1}}\sigma\bar{\tau}^{-1}\}.$$

We define a multiplication on $H \wr_U G$ by

$$(\sigma_1, \psi_1)(\sigma_2, \psi_2) := (\sigma_1\sigma_2, \psi_1^{\sigma_2}\psi_2)$$

where $\psi^\sigma(\tau) := \psi(\tau\sigma^{-1})$ for all $\tau \in G$. This multiplication endows $H \wr_U G$ with the structure of a group, an extension of $H^{(G:U)}$ by G (see Ishkhanov, Lure and Faddeev (1997), Ch. 3, §7, for example). This extension is called here the *wreath extension (transference* in the Russian literature) of H with G over the group extension $\tilde{U} = H \cdot U$ of H with the subgroup U of G . It is the natural generalization of the twisted wreath product $H \wr_U G$ (defined for split extensions $H \rtimes U$ in Suzuki (1982), Ch. 2, §10) to the non-split case.

We can now state an embedding theorem generalizing Theorem 2.2.

Theorem 8.1. Let K be a field and N/GK a finite Galois extension. Further let $U \leq G$ be a subgroup with fixed field $L := N^U$, $\tilde{U} := H \cdot U$ a finite group extension with kernel H and $H \wr_U G$ the wreath extension over \tilde{U} . Assume that the embedding problem $\mathcal{E}(\psi, \lambda)$ with the restriction $\psi : \Gamma_L \rightarrow U$ and the canonical epimorphism $\lambda : \tilde{U} \rightarrow U$ has a (proper) regular solution. Then the embedding problem $\mathcal{E}(\varphi, \kappa)$ defined by the restriction $\varphi : \Gamma_K \rightarrow G$ and the canonical epimorphism $\kappa : H \wr_U G \rightarrow G$ possesses a (proper) regular solution.

Proof. Let \tilde{N}_1 denote the solution field of a (proper) regular solution of $\mathcal{E}(\psi, \lambda)$, where without loss we may assume that this solution is 1-regular and the Galois group

$$\tilde{U}_1^* := \text{Gal}(\tilde{N}_1/L(t_1)) \cong \tilde{U}_1 \leq \tilde{U} = H \cdot U$$

is isomorphic to a subgroup $\tilde{U}_1 = H_1 \cdot U$ of \tilde{U} . Then in particular \tilde{N}_1/N is regular with

$$H_1^* := \text{Gal}(\tilde{N}_1/N(t_1)) \cong H_1 \leq H$$

(where $H_1 = H$ in the case of a proper solution). Further let x be a primitive element of L/K and $x_i := x^{\sigma_i} \in N$ with a system $\{\sigma_i \mid i = 1, \dots, r\}$ of coset representatives of U in G (and $\sigma_1 = 1$). Let y be a primitive element of $\tilde{N}_1/L(t_1)$ with minimal polynomial $f(Y, t_1) \in L(t_1)[Y]$. For a given system $\mathbf{t} = (t_1, \dots, t_r)$ of independent variables over K denote by \tilde{N}_i the splitting field of $f^{\sigma_i}(Y, t_i) \in K(x_i, t_i)[Y]$ inside an algebraic closure of $K(\mathbf{t})$. Then the composite $\tilde{N}^* := \tilde{N}_1 \cdots \tilde{N}_r$ is regular over N .

Via its action on the cosets of U , the group G also acts on $\{t_1, \dots, t_r\}$ via $t_i = t_1^{\sigma_i}$ and in this way extends to a group $G^* \cong G$ of automorphisms of $N(\mathbf{t})/K(\mathbf{t}^G)$. By Speiser's Lemma (Proposition III.3.10) the fixed field of this action $K^* := N(\mathbf{t})^{G^*}$ is rational over K and can be generated explicitly in the following form:

$$K^* = K(v_1, \dots, v_r) \quad \text{with } v_j := \sum_{i=1}^r x_i^{j-1} t_i. \quad (8.1)$$

By Cramer's rule we have the inverse formula

$$t_i = \frac{V_i(\mathbf{x}, \mathbf{v})}{V(\mathbf{x})}, \quad (8.2)$$

where $V(\mathbf{x})$ denotes the Vandermonde determinant and $V_i(\mathbf{x}, \mathbf{v})$ the determinant obtained from $V(\mathbf{x})$ by replacing the i -th row by (v_1, \dots, v_r) .

Equation (8.2) shows that $t_i \in K^*(x_i)$. Consequently the zeroes of the polynomials $f^{\sigma_i}(Y, t_i)$ also generate the field extensions $\tilde{N}_i(\mathbf{v})/K^*(x_i)$. Since G^* permutes these polynomials, the composite \tilde{N}^* of the $\tilde{N}_i(\mathbf{v}) = \tilde{N}_i(\mathbf{t})$ for $i = 1, \dots, r$ is Galois over the fixed field K^* of G^* , and by construction the Galois group equals

$$\text{Gal}(\tilde{N}^*/K^*) \cong H_1 \wr_U G \leq H \wr_U G, \quad (8.3)$$

with $H_1 = H$ in the proper case. In particular the restriction map $\tilde{\varphi}^* : \Gamma_{K^*} \rightarrow \text{Gal}(\tilde{N}^*/K^*)$ gives a (proper) regular solution of $\mathcal{E}(\varphi, \kappa)$ in r variables. \square

Remark. The assertion $t_i \in K^*(x_i)$ is easier to verify if instead of v_j we use the generators $v_j^* := V_j^*(\mathbf{x}, \mathbf{t})/V(\mathbf{x})$ from Matzat (1987) where $V_j^*(\mathbf{x}, \mathbf{t})$ denotes the determinant obtained from $V(\mathbf{x})$ by replacing the j -th column by the transposed of (t_1, \dots, t_r) . Then the inverse formula takes the form $t_i = \sum_{j=1}^r x_i^{j-1} v_j^*$.

With the help of this theorem we arrive at the following generalization of the classical reduction theorem of Kochendörffer.

Theorem 8.2 (Kochendörffer (1953)). *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem with abelian kernel H over K and U a subgroup of $G = \varphi(\Gamma_K)$ of index $(G : U)$ prime to $|H|$. Further let L denote the fixed field of U , ψ the restriction of φ to $\Gamma_L \leq \Gamma_K$ and λ the restriction of κ to $\tilde{U} = H \cdot U \leq H \cdot G = \tilde{G}$. Then $\mathcal{E}(\varphi, \kappa)$ possesses a (regular) solution if and only if $\mathcal{E}(\psi, \lambda)$ possesses a (regular) solution.*

Proof. Evidently every solution field \tilde{N} of the embedding problem $\mathcal{E}(\varphi, \kappa)$ is also a solution field of $\mathcal{E}(\psi, \lambda)$, so that the (regular) solvability of $\mathcal{E}(\varphi, \kappa)$ implies the (regular) solvability of $\mathcal{E}(\psi, \lambda)$. It thus remains to prove the reverse assertion.

Let $h \in H^2(G, H)$ be the cohomology class describing the group extension $\tilde{G} = H \cdot G$. Then $\tilde{U} = H \cdot U$ is a group extension belonging to the restriction $\rho_U^G(h) \in H^2(U, H)$. We consider the following commutative diagram

$$\begin{array}{ccc} H^2(G, H) & \xrightarrow{\varphi^*} & H^2(\Gamma_K, H) \\ \downarrow \rho_U^G & & \downarrow \rho_L^K \\ H^2(U, H) & \xrightarrow{\psi^*} & H^2(\Gamma_L, H) \end{array}$$

with inflations φ^* and ψ^* . As $|H|$ and $(G : U)$ are coprime, the multiplication by $(G : U)$ on $H^2(\Gamma_K, H)$ is injective. Since the composition of restriction and corestriction acts as multiplication by $(G : U)$ on $H^2(\Gamma_K, H)$, the restriction ρ_L^K is injective (see for example Serre (1964), Ch. I, Cor. to Prop. 9, or Shatz (1972), Ch. II, Prop. 10). In particular from the solvability of $\mathcal{E}(\psi, \lambda)$, i.e., from $\psi^*(\rho_U^G(h)) = 0$, we immediately obtain $\varphi^*(h) = 0$ and thus by Theorem 6.1(a) the solvability of $\mathcal{E}(\varphi, \kappa)$. According to the Remark following Theorem 6.1 a solution field can already be found inside the Galois closure of \tilde{M}/K , where \tilde{M} denotes the solution field of $\mathcal{E}(\psi, \lambda)$.

In the case of regular solvability an additional argument is necessary. By the proof of Theorem 8.1 the field $\tilde{N}_1(\mathbf{v})$ is a solution of the embedding problem $\mathcal{E}(\psi^*, \lambda^*)$ lifted from $\mathcal{E}(\psi, \lambda)$ to $L(\mathbf{v})$. By the first part of the proof the corresponding embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ then also possesses a solution $\tilde{\varphi}^*$ with solution field contained in the Galois closure of $\tilde{N}_1(\mathbf{v})/K^*$, hence inside \tilde{N}^* . Since by construction N is algebraically closed in \tilde{N}^* , any such solution is automatically a regular solution of $\mathcal{E}(\varphi, \kappa)$. \square

Remark. By Corollary 2.5 the above theorem of Kochendörffer also holds for proper (regular) solutions of embedding problems, but in general not for geometric solutions (proper or not).

As a simple application of the reduction theorem of Kochendörffer we obtain the very useful

Theorem 8.3. *Let K be a field of characteristic p and H a finite p -group. Then we have:*

(a) *Every finite embedding problem over K with kernel H is solvable.*

(b) *If K is a Hilbertian field then every finite embedding problem over K with kernel H has a proper solution.*

Proof. Let first H be abelian. By the reduction theorem of Kochendörffer we may assume by passage to a Sylow p -subgroup that $G = \text{Gal}(N/K)$ is a finite p -group. Then part (a) of the theorem follows from the fact that the maximal pro- p factor group of Γ_K is a free pro- p group (see Shatz (1972), Ch. III, Prop. 30, or also Serre (1964), Ch. I, Prop. 16(iii) together with loc. cit., Ch. II, Prop. 3). In the case of a Hilbertian field K the maximal pro- p factor group of Γ_K is not finitely generated. Consequently every finite embedding problem over K with abelian p -kernel even possesses a proper solution, which proves (b).

The assertion for a general p -group H now follows by induction along a $\tilde{G} = H \cdot G$ -normal series of H with abelian factors. \square

Remark. In the case of embedding problems with abelian kernel H Theorem 8.3 will allow to assume, using Theorem 1.6, that the characteristic of K does not divide $|H|$.

This observation will prove to be very useful in the study of the concordance condition.

8.2 The Concordance Condition

First we give a precise definition of the notion of an accompanying embedding problem. For this let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over a field K with epimorphisms $\varphi : \Gamma_K \rightarrow G = \text{Gal}(N/K)$ and $\kappa : \tilde{G} = H \cdot G \rightarrow G$. For a subgroup $B \leq G$ let $L := N^B$ be the fixed field and $U := \kappa^{-1}(B)$. Further let V be a normal subgroup of U contained in H , $A := H/V$ and \tilde{B} the group extension $A \cdot B = U/V$. Then the embedding problem $\mathcal{E}(\psi, \lambda)$ defined by the canonical epimorphisms $\psi : \Gamma_L \rightarrow B$, $\lambda : \tilde{B} \rightarrow B$ is called an *accompanying embedding problem* of $\mathcal{E}(\varphi, \kappa)$. If moreover $\mathcal{E}(\psi, \lambda)$ is a Brauer embedding problem, it is called an *accompanying Brauer embedding problem*. Clearly, if $\mathcal{E}(\varphi, \kappa)$ is solvable, then all accompanying embedding problems are solvable, see Fig. 8.1.

For an embedding problem $\mathcal{E}(\varphi, \kappa)$ to possess sufficiently many accompanying Brauer embedding problems, the fixed field N of $\ker(\varphi)$ has to contain enough roots of unity. So let n be the part of $\exp(H)$ prime to the characteristic of K , $N_n := N(\zeta_n)$ with a primitive n -th root of unity ζ_n , $G_n := \text{Gal}(N_n/K)$ with restriction $\varphi_n : \Gamma_K \rightarrow G_n$, and $\tilde{G}_n := \tilde{G} \times_G G_n$ the subdirect product of \tilde{G} with G_n over G with projection

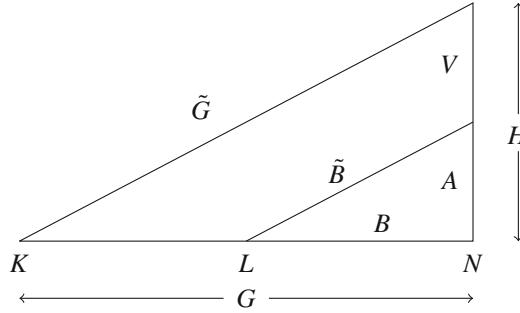


Fig. 8.1 Accompanying Brauer embedding problem

κ_n onto G_n . Then Theorem 1.6(a) implies that the embedding problem $\mathcal{E}(\varphi_n, \kappa_n)$ is solvable if and only if $\mathcal{E}(\varphi, \kappa)$ is solvable, and moreover that $\mathcal{E}(\varphi_n, \kappa_n)$ is properly solvable if and only if $\mathcal{E}(\varphi, \kappa)$ is properly solvable with solution field \tilde{N} linearly disjoint from N_n over N .

In the following $\mathcal{E}(\varphi, \kappa)$ is called a *concordant embedding problem*, if all accompanying Brauer embedding problems of $\mathcal{E}(\varphi_n, \kappa_n)$ are solvable. The concordance condition is hence a necessary prerequisite for the solvability of $\mathcal{E}(\varphi, \kappa)$. In the investigation of concordant embedding problems by definition we may assume without loss of generality that N contains a primitive n -th root of unity.

Now let H be an abelian group and $\hat{H}_{(p)} := \text{Hom}(H, \bar{K}^\times)$ the part of the character group \hat{H} of H prime to the characteristic p of K , with $\exp(\hat{H}_{(p)}) = n$. By taking the action of Γ_K on H given by the restriction map $\varphi : \Gamma_K \rightarrow G$ and the action of G on H given by the group extension \tilde{G} , $\hat{H}_{(p)}$ can be made into a Γ_K -module via

$$\chi^\gamma(\tau) := (\chi(\tau^{\gamma^{-1}}))^\gamma \quad \text{for } \chi \in \hat{H}_{(p)}, \gamma \in \Gamma_K, \tau \in H. \quad (8.4)$$

Let Γ_χ be the stabilizer of $\chi \in \hat{H}_{(p)}$ in Γ_K and K_χ its fixed field, so that χ becomes a Γ_χ -homomorphism. Obviously K_χ is contained in N . In addition to the inflation $\varphi^* : H^2(G, H) \rightarrow H^2(\Gamma_K, H)$ from (6.1) we obtain a homomorphism

$$\rho_\chi^* : H^2(\Gamma_K, H) \xrightarrow{\rho_\chi} H^2(\Gamma_\chi, H) \xrightarrow{\chi^*} \text{Br}(K_\chi) \quad (8.5)$$

by composition of the restriction ρ_χ with the homomorphism $\chi^* : H^2(\Gamma_\chi, H) \rightarrow H^2(\Gamma_\chi, \bar{K}^\times)$ induced by χ .

Theorem 8.4. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over K with abelian kernel H and with cohomological obstruction $h(\varphi, \kappa) \in H^2(\Gamma_K, H)$. Then we have:*

(a) $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if

$$\rho_\chi^*(h(\varphi, \kappa)) = 0 \quad \text{for all } \chi \in \hat{H}_{(p)}. \quad (8.6)$$

(b) $\mathcal{E}(\varphi, \kappa)$ is solvable if in addition the following map is injective:

$$\rho_H^* := \prod_{\chi \in \hat{H}_{(p)}} \rho_\chi^* : H^2(\Gamma_K, H) \rightarrow \prod_{\chi \in \hat{H}_{(p)}} \text{Br}(K_\chi). \quad (8.7)$$

Proof. By the above we may assume that the fixed field N of $\ker(\varphi)$ contains a primitive n -th root of unity for $n = \exp(\hat{H}_{(p)})$. Via restriction every $\chi \in \hat{H}_{(p)}$ defines epimorphisms

$$\varphi_\chi : \Gamma_\chi \rightarrow G_\chi := \text{Gal}(N/K_\chi), \quad \kappa_\chi : \tilde{G}_\chi := H \cdot G_\chi \rightarrow G_\chi, \quad (8.8)$$

and thus an embedding problem $\mathcal{E}(\varphi_\chi, \kappa_\chi)$ accompanying $\mathcal{E}(\varphi, \kappa)$. This is even a Brauer embedding problem, since χ is a Γ_χ -homomorphism and moreover $\chi(H) \leq N^\times$. From the concordance condition follows the solvability of $\mathcal{E}(\varphi_\chi, \kappa_\chi)$ and therefore the vanishing of the embedding obstruction which by (8.5) equals $\rho_\chi^*(h(\varphi, \kappa)) \in \text{Br}(K_\chi)$.

Now assume (8.6) and let $\mathcal{E}(\psi, \lambda)$ be an accompanying Brauer embedding problem of $\mathcal{E}(\varphi, \kappa)$. By definition, if we denote by L the fixed field of $\ker(\psi)$, there exists a Γ_L -homomorphism $\chi : H \rightarrow N^\times$ with $\chi(H) = \ker(\lambda)$ by identifying the kernel of $\mathcal{E}(\psi, \lambda)$ with a group of roots of unity in N . Thus L contains the field K_χ and $\mathcal{E}(\psi, \lambda)$ is an accompanying embedding problem of $\mathcal{E}(\varphi_\chi, \kappa_\chi)$, which is hence solvable. This proves (a).

Part (b) of the theorem follows immediately from (a) together with Theorem 6.1(a). \square

Remark. From Theorem 8.4(a) it follows that the concordance condition does not change if we adjoin further roots of unity to N .

Fortunately the basic reduction theorems for embedding problems continue to hold for concordant embedding problems. So in addition to Theorem 1.6 we obtain:

Corollary 8.5. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem with abelian kernel H . Assume that moreover $H = \prod_{i=1}^r H_i$ decomposes into a direct product of normal subgroups H_i of $\tilde{G} = H \cdot G$. Then $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if the accompanying embedding problems $\mathcal{E}(\varphi, \kappa_i)$ in Theorem 1.6 for $i = 1, \dots, r$ are concordant.*

Proof. The assertion follows immediately from Theorem 8.4(a) with Remark due to the equality $\hat{H}_{(p)} = \prod_{i=1}^r \hat{H}_{i,(p)}$. \square

Further we obtain the following supplement to the Theorem 8.2 of Kochendörffer.

Corollary 8.6. *Assume the hypotheses of Theorem 8.2. Then the embedding problem $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if $\mathcal{E}(\psi, \lambda)$ is concordant.*

Proof. With the notations introduced in the proof of Theorem 8.2, ρ_χ^* from (8.5) and the analogously defined map $\sigma_\chi^* : H^2(\Gamma_L, H) \rightarrow \text{Br}(L_\chi)$ in the Brauer group of

$L_\chi = LK_\chi$ we obtain the following commutative diagram with vertical restriction maps:

$$\begin{array}{ccccc} H^2(G, H) & \xrightarrow{\varphi^*} & H^2(\Gamma_K, H) & \xrightarrow{\rho_\chi^K} & \mathrm{Br}(K_\chi) \\ \downarrow \rho_U^G & & \downarrow \rho_L^K & & \downarrow \beta_L^K \\ H^2(U, H) & \xrightarrow{\psi^*} & H^2(\Gamma_L, H) & \xrightarrow{\sigma_\chi^K} & \mathrm{Br}(L_\chi) \end{array}$$

By Theorem 8.4(a) the embedding problem $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if the cohomology class $h \in H^2(G, H)$ defining $\tilde{G} = H \cdot G$ satisfies

$$(\rho_\chi^* \circ \varphi^*)(h) = \rho_\chi^*(h(\varphi, \kappa)) = 0 \quad \text{for all } \chi \in \hat{H}_{(p)}.$$

Since the cohomology class $\rho_U^G(h)$ defines $\tilde{U} = H \cdot U$, this immediately implies the concordance condition for $\mathcal{E}(\psi, \lambda)$:

$$(\sigma_\chi^K \circ \psi^*)(\rho_U^G(h)) = 0 \quad \text{for all } \chi \in \hat{H}_{(p)}. \quad (8.9)$$

Conversely the concordance condition (8.9) for $\mathcal{E}(\psi, \lambda)$ first yields

$$(\beta_L^K \circ \rho_\chi^* \circ \varphi^*)(h) = 0 \quad \text{for all } \chi \in \hat{H}_{(p)}.$$

But since $\gcd([L_\chi : K_\chi], |H|) = 1$, the restriction β_L^K is injective on the $\exp(\hat{H}_{(p)})$ -torsion of the Brauer group $\mathrm{Br}(K_\chi) \cong H^2(\Gamma_\chi, \bar{K}^\times)$ (see for example Serre (1964), Cor. to Prop. 9, or Shatz (1972), Ch.II, Prop. 10). So the previous equation allows to recover the concordance condition for $\mathcal{E}(\varphi, \kappa)$. \square

With the first of these two reduction theorems for the concordance condition we get the following easy solvability criterion:

Theorem 8.7. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over K with abelian kernel H . Assume that Γ_K acts trivially on $\hat{H}_{(p)}$. Then the concordance condition implies the solvability of $\mathcal{E}(\varphi, \kappa)$.*

Proof. Let p be the characteristic of K . Then the concordance condition is vacuously satisfied for the Sylow p -subgroup H_p of H , and the corresponding embedding problem is solvable by Theorem 8.3(a). Thus by Theorem 1.6(a) we may assume that p does not divide $|H|$ and hence we have $\hat{H}_{(p)} = \hat{H}$. By the structure theorem for finite abelian groups, \hat{H} is a direct product $\hat{H} = \prod_{i=1}^r \langle \chi_i \rangle$ of cyclic groups. Since Γ_K is supposed to act trivially on $\langle \chi_i \rangle$, we have $\Gamma_{\chi_i} = \Gamma_K$ and hence $\varphi_{\chi_i} = \varphi$ for $i = 1, \dots, r$. Let

$$H_i := \bigcap_{i \neq j=1}^r \ker(\chi_j) \cong \langle \chi_i \rangle$$

for the kernels of the accompanying Brauer embedding problems $\mathcal{E}(\varphi, \kappa_{\chi_i})$ in the proof of Theorem 8.4. Since $H \cong \hat{H}$ these lead to a direct decomposition of the

kernel H of $\mathcal{E}(\varphi, \kappa)$:

$$H = \prod_{i=1}^r H_i \quad \text{with} \quad H_1 \cdots H_{i-1} H_i H_{i+1} \cdots H_r = \ker(\chi_i).$$

Thus the embedding problems $\mathcal{E}(\varphi, \kappa_{\chi_i})$ coincide with the accompanying embedding problems $\mathcal{E}(\varphi, \kappa_i)$ in Corollary 8.5. The concordance condition for $\mathcal{E}(\varphi, \kappa)$ then implies the solvability of $\mathcal{E}(\varphi, \kappa_i)$ for $i = 1, \dots, r$ and with Corollary 8.5 also the solvability of $\mathcal{E}(\varphi, \kappa)$. \square

In the following two sections we study the concordance condition in the case of local and global ground fields.

8.3 Concordance over Local Fields

The main tool for the investigation of concordant embedding problems over local fields, i.e., over fields complete with respect to a discrete valuation and with finite residue field, is a duality theorem of Tate, which we cite without proof (see also Serre (1964), Ch. II, Thm. 2 with Rem. 2, or Ishkhanov, Lure and Faddeev (1997), Thm. A.3.1).

Theorem 8.8 (Duality Theorem of Tate (1962)). *Let K be a local field and H a finite Γ_K -module of order prime to the characteristic of K . Then the groups $H^i(\Gamma_K, H)$ and $H^{2-i}(\Gamma_K, \hat{H})$ are in duality by virtue of the cup product*

$$\cdot : H^i(\Gamma_K, H) \times H^{2-i}(\Gamma_K, \hat{H}) \rightarrow H^2(\Gamma_K, \bar{K}^\times) \cong \text{Br}(K) \quad (8.10)$$

for $i = 0, 1, 2$.

This allows to give a very easy proof (found by Hoechsmann (1968)) of the following important result:

Theorem 8.9 (Demuškin and Šafarevič (1959)). *Concordant finite embedding problems with abelian kernel over a local field are always solvable.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be a concordant embedding problem with kernel H over a local field K . By Theorems 8.3 and 1.6 we may assume without loss of generality that the characteristic of K is prime to $|H|$ and thus we have $\hat{H}_{(p)} = \hat{H}$. Moreover, the fixed field N of $\ker(\varphi)$ can be assumed to contain a primitive $\exp(H)$ -th root of unity. By Theorem 8.4(b) we have to show the injectivity of the map ρ_H^* . Let $X := H^0(\Gamma_K, \hat{H})$ be the group of characters of H invariant under the Γ_K -action defined in (8.4). Then for each $g \in H^2(\Gamma_K, H)$ and $\chi \in X$ we have using the cup-product

$$g \cdot \chi = \rho_\chi^*(g) \in H^2(\Gamma_K, \bar{K}^\times) \cong \text{Br}(K) \quad (8.11)$$

(see for example Shatz (1972), Ch. II, Remark 1 following Thm. 9). By the Duality Theorem of Tate for $g \neq 0$ there exist $\chi \in X$ with $\rho_\chi^*(g) \neq 0$. Thus

$$\prod_{\chi \in X} \rho_\chi^* : H^2(\Gamma_K, H) \longrightarrow \prod_{\chi \in X} \text{Br}(K) \quad (8.12)$$

is injective, and a fortiori the same is true for ρ_H^* . \square

Proposition 8.10. *The conclusion of Theorem 8.9 also holds for the fields \mathbb{IR} and \mathbb{C} .*

Proof. It suffices to show the injectivity of (8.12) for $K = \mathbb{IR}$ and $K = \mathbb{C}$. For $K = \mathbb{C}$ this is trivial due to $H^2(\Gamma_K, H) = 0$.

So let $K = \mathbb{IR}$. Then the only non-trivial element of Γ_K is the involution ρ mapping every root of unity to its inverse. The $\chi \in H^0(\Gamma_K, \hat{H})$ are hence characterized by $\chi(\tau^\rho) = \chi(\tau)^{-1}$ for all $\tau \in H$. Now let

$$T := \{\tau \cdot \tau^\rho \mid \tau \in H\} \leq H.$$

In the case $T = 1$ we always have $\tau^\rho = \tau^{-1}$, so every $\chi \in \hat{H}$ is Γ_K -invariant and the assertion follows from Theorem 8.7. Otherwise, the factor group $H_1 := H/T$ has smaller order than H , and we can prove (8.12) by induction on $|H|$. In the long cohomology sequence

$$\dots \longrightarrow H^2(\Gamma_K, T) \longrightarrow H^2(\Gamma_K, H) \xrightarrow{\omega_2^*} H^2(\Gamma_K, H_1) \longrightarrow \dots$$

induced by $1 \rightarrow T \rightarrow H \xrightarrow{\omega} H_1 \rightarrow 1$, with $\Gamma_K \cong Z_2$, we have that $H^2(\Gamma_K, T)$ maps to 0 by the definition of T (see Huppert (1967), Kap. I, Satz 16.10) and hence ω_2^* is injective. Thus for $g \in H^2(\Gamma_K, H)$ with $g \neq 0$ there exists by induction a $\chi_1 \in H^0(\Gamma_K, \hat{H}_1)$ with $\rho_{\chi_1}^*(\omega_2^*(g)) \neq 0$. Denoting by χ the character obtained by inflation of χ_1 to H , we obtain $\chi \in H^0(\Gamma_K, \hat{H})$ with $\rho_\chi^*(g) = \rho_{\chi_1}^*(\omega_2^*(g)) \neq 0$. \square

Remark. If in Theorems 8.3 and 8.9, respectively in Proposition 8.10 the ground field K is not Hilbertian, then the investigated solvable embedding problems will in general not have a proper solution!

8.4 Concordance over Global Fields

With the help of Theorem 8.9 of Demuškin and Šafarevič one obtains a characterization of the concordance condition for embedding problems over global fields K by local solvability, where global fields are the finite algebraic number fields over \mathbb{Q} , and algebraic function fields in one variable over finite fields. This relies on a local-global principle for the concordance condition. In the sequel as in Section 7.2 we denote by $\text{IP}(K)$ the set of all prime divisors of K (including the infinite ones, if they exist).

Proposition 8.11. A finite embedding problem $\mathcal{E}(\varphi, \kappa)$ with abelian kernel over a global field is concordant if and only if for all $\mathfrak{p} \in \text{IP}(K)$ the local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are concordant.

Proof. The local embedding problems were defined in Section 7.2. For the proof as above we may assume without loss of generality that $|H|$ is prime to the characteristic of K and that the fixed field N of $\ker(\varphi)$ contains the $\exp(H)$ -th roots of unity. We consider the following commutative square

$$\begin{array}{ccc} H^2(\Gamma_K, H) & \xrightarrow{\rho_H^*} & \prod_{\chi \in \hat{H}} \text{Br}(K_{\chi}) \\ \downarrow \alpha & & \downarrow \beta \\ \prod_{\mathfrak{p} \in \text{IP}(K)} H^2(\Gamma_{K_{\mathfrak{p}}}, H) & \xrightarrow{\sigma_H^*} & \prod_{\mathfrak{p} \in \text{IP}(K)} \prod_{\chi \in \hat{H}} \text{Br}(K_{\mathfrak{p}, \chi}) \end{array}$$

with ρ_H^* from (8.7), the product $\sigma_H^* = \prod_{\mathfrak{p} \in \text{IP}(K)} \sigma_{\mathfrak{p}, H}^*$ of the analogously defined local maps and the products of restriction maps

$$\alpha = \prod_{\mathfrak{p} \in \text{IP}(K)} \alpha_{\mathfrak{p}}, \quad \beta = \prod_{\chi \in \hat{H}} \prod_{\mathfrak{p} \in \text{IP}(K)} \beta_{\chi, \mathfrak{p}}.$$

Let first $\mathcal{E}(\varphi, \kappa)$ be a concordant embedding problem with embedding obstruction $h(\varphi, \kappa) \in H^2(\Gamma_K, H)$. Then by Theorem 8.4(a) we have $\rho_H^*(h(\varphi, \kappa)) = 0$. This implies $\sigma_H^*(h(\varphi, \kappa)_{\mathfrak{p}}) = 0$ for $\mathfrak{p} \in \text{IP}(K)$ and the embedding obstruction $h(\varphi, \kappa)_{\mathfrak{p}} = \alpha_{\mathfrak{p}}(h(\varphi, \kappa))$ of the local embedding problem $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$. So $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ is concordant.

Conversely, if all local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are concordant, the embedding obstruction $h(\varphi, \kappa)$ of $\mathcal{E}(\varphi, \kappa)$ satisfies

$$(\beta \circ \rho_H^*)(h(\varphi, \kappa)) = (\sigma_H^* \circ \alpha)(h(\varphi, \kappa)) = 0.$$

For the concordance of $\mathcal{E}(\varphi, \kappa)$ it remains to show that β is injective on the image of ρ_H^* . For this we compare β with the map $\tilde{\beta} = \prod_{\chi \in \hat{H}} \tilde{\beta}_{\chi}$, with components

$$\tilde{\beta}_{\chi} = \prod_{\tilde{\mathfrak{p}} \in \text{IP}(K_{\chi})} \tilde{\beta}_{\chi, \tilde{\mathfrak{p}}} : \text{Br}(K_{\chi}) \longrightarrow \prod_{\tilde{\mathfrak{p}} \in \text{IP}(K_{\chi})} \text{Br}(K_{\chi, \tilde{\mathfrak{p}}})$$

the injective maps obtained from the Theorem of Brauer, Hasse and Noether (see for example Weil (1974), Ch. XI, Thm. 2). By construction for $b = (b_{\chi})_{\chi \in \hat{H}} \in \rho_H^*(H^2(\Gamma_K, H))$ and $\tilde{\mathfrak{p}} \mid \mathfrak{p}$ the images $\tilde{\beta}_{\chi, \tilde{\mathfrak{p}}}(b_{\chi})$ are embedding obstructions of Brauer embedding problems conjugate over $K_{\mathfrak{p}}$ to the localization $\mathcal{E}(\varphi_{\chi, \mathfrak{p}}, \kappa_{\chi, \mathfrak{p}})$ at \mathfrak{p} of $\mathcal{E}(\varphi_{\chi}, \kappa_{\chi})$. Thus in particular $\tilde{\beta}_{\chi, \tilde{\mathfrak{p}}}(b_{\chi})$ vanishes for $\tilde{\mathfrak{p}} \mid \mathfrak{p}$ if and only if $\beta_{\chi, \mathfrak{p}}(b_{\chi}) = 0$. This proves injectivity of β on the image of ρ_H^* and hence the assertion. \square

Remark. Obviously Proposition 8.11 remains valid more generally if the Brauer group satisfies a local-global principle, as for example in the case of rational function fields over global fields (compare Sections 7.2 and 7.3).

Using the results on local fields the previous proposition immediately gives:

Theorem 8.12. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem with abelian kernel H over a global field K . Then we have:*

- (a) $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if for all $\mathfrak{p} \in \mathbb{P}(K)$ the local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are solvable.
- (b) $\mathcal{E}(\varphi, \kappa)$ is solvable, if in addition the following product of restriction maps is injective:

$$\alpha : H^2(\Gamma_K, H) \longrightarrow \prod_{\mathfrak{p} \in \mathbb{P}(K)} H^2(\Gamma_{K_{\mathfrak{p}}}, H). \quad (8.13)$$

Proof. Part (a) follows with the Theorem 8.9 of Demuškin and Šafarevič and Proposition 8.10 immediately from the local-global principle for the concordance condition in Proposition 8.11.

Under the assumption (a) in the proof of Proposition 8.11 we have $\rho_H^*(h(\varphi, \kappa)) = 0$ for the embedding obstruction $h(\varphi, \kappa) \in H^2(\Gamma_K, H)$ of $\mathcal{E}(\varphi, \kappa)$ and hence also $(\sigma_H^* \circ \alpha)(h(\varphi, \kappa)) = (\beta \circ \rho_H^*)(h(\varphi, \kappa)) = 0$. Since σ_H^* is injective by Theorem 8.9 and Proposition 8.10 respectively, and α is so by assumption, we conclude that $h(\varphi, \kappa) = 0$ and hence the solvability of $\mathcal{E}(\varphi, \kappa)$. This proves part (b). \square

9 The Hasse Embedding Obstruction

In this paragraph we study the embedding obstruction of concordant embedding problems. This will be called the Hasse embedding obstruction, since it was discovered by Hasse (1948) and constitutes an obstruction to the validity of the local-global-principle for embedding problems. We then present cohomological descriptions of the Hasse obstruction for arbitrary and for global fields, whose coincidence is proved using a comparison theorem of Tate for the cohomology of global fields.

9.1 Kummer Extensions

As in the previous paragraph let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over a field K with abelian kernel H . Moreover we will always assume that the characteristic of K does not divide the order $|H|$ and that the fixed field N of $\ker(\varphi)$ contains a primitive $\exp(H)$ -th root of unity. This is possible by Sections 8.1 and 8.2 without loss of generality. Then by (8.4) the character group \hat{H} of H becomes a Γ_K -module and hence also a \tilde{G} -module via

$$\chi^\sigma(\tau) = (\chi(\tau^{\sigma^{-1}}))^\sigma \quad \text{for all } \chi \in \hat{H}, \sigma \in \tilde{G}, \tau \in H. \quad (9.1)$$

Every solution field \tilde{N} of $\mathcal{E}(\varphi, \kappa)$ is a Kummer extension of N and as such is described by an exact sequence

$$1 \longrightarrow N^\times \xrightarrow{\varepsilon} \tilde{X} \xrightarrow{\eta} \hat{H} \longrightarrow 1 \quad (9.2)$$

of H -modules, where \tilde{X} denotes the elements of \tilde{N}^\times whose $\exp(H)$ -th power lies in N , ε is the inclusion and η the homomorphism

$$\eta : \tilde{X} \rightarrow \hat{H}, \quad x \mapsto \eta(x) \text{ with } \eta(x)(\tau) = \frac{x^\tau}{x} \quad (\tau \in H).$$

Therefore the action of H on \tilde{X} is given by

$$x^\tau = x \cdot \varepsilon(\eta(x)(\tau)) \quad \text{for all } x \in \tilde{X}, \tau \in H \quad (9.3)$$

(see for example Jacobson (1980), Thm. 8.23). Since \tilde{N} is Galois over K , this is even an exact sequence of \tilde{G} -modules. This yields the following criterion for the solvability of $\mathcal{E}(\varphi, \kappa)$:

Theorem 9.1. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem over K with abelian kernel H , whose order is prime to the characteristic of K . Then $\mathcal{E}(\varphi, \kappa)$ possesses a solution if and only if there exist a \tilde{G} -module \tilde{X} and \tilde{G} -homomorphisms ε and η satisfying (9.2) and (9.3).*

Proof. It remains to deduce the solvability of $\mathcal{E}(\varphi, \kappa)$ from the existence of \tilde{X} satisfying (9.2) and (9.3) (which are necessary by what precedes). With a system of representatives $\{x_\chi \mid \chi \in \hat{H}\}$ of \hat{H} in \tilde{X} we construct from \tilde{X} an N -algebra

$$\tilde{A} := \bigoplus_{\chi \in \hat{H}} Nx_\chi$$

with the product of representatives

$$x_\chi x_{\tilde{\chi}} = c_{\chi, \tilde{\chi}} x_{\chi \tilde{\chi}} \quad \text{with } c = (c_{\chi, \tilde{\chi}}) \in Z^2(\hat{H}, N^\times)$$

defined in \tilde{X} . Obviously \tilde{A} is Galois over N with group H and also Galois over K with group \tilde{G} . Therefore it splits into a direct sum of K -isomorphic extension fields \tilde{N}_i of N Galois over K with

$$\text{Gal}(\tilde{N}_i/K) \cong \{\sigma \in \tilde{G} \mid \tilde{N}_i^\sigma = \tilde{N}_i\}$$

(see for example Wolf (1956), §9, Satz 1, with comments in §11). The embedding \tilde{N} of one of these into a given separable algebraic closure \tilde{K} of K yields a solution field generated by elements from \tilde{X} . Therefore the restriction of Γ_K to $\text{Gal}(\tilde{N}/N)$ defines a solution $\tilde{\varphi}$ of $\mathcal{E}(\varphi, \kappa)$. This is proper precisely when \tilde{A} is already a field. \square

We now want to check to what extent the \tilde{G} -module \tilde{X} is determined as H -module by N^\times, \hat{H} and the action (9.3) of H on \tilde{X} . The H -action on \tilde{X} , which is trivial on $\hat{H} = \tilde{X}/N^\times$ by (9.1) and also on $N^\times \leq \tilde{X}$, can be extended to a $\mathbb{Z}[H]$ -action on these modules in a natural way. Then (9.2) becomes an exact sequence of $\mathbb{Z}[H]$ -modules, where for better distinction \tilde{X} as $\mathbb{Z}[H]$ -module is denoted by X . By trivial extension of the H -action from \hat{H} to $\mathbb{Z}[\hat{H}]$ and extension to a $\mathbb{Z}[H]$ -action, the free \mathbb{Z} -module $\mathbb{Z}[\hat{H}]$ becomes a $\mathbb{Z}[H]$ -module. The fiber product X_H of X with $\mathbb{Z}[\hat{H}]$ over \hat{H} in the category of $\mathbb{Z}[H]$ -modules with respect to the homomorphisms

$$\eta : X \rightarrow \hat{H} \quad \text{and} \quad \xi : \mathbb{Z}[\hat{H}] \rightarrow \hat{H}, \quad \sum_{\chi \in \hat{H}} m_\chi \chi \mapsto \prod_{\chi \in \hat{H}} \chi^{m_\chi}, \quad (9.4)$$

thus decomposes as \mathbb{Z} -module into the direct sum of N^\times and $\mathbb{Z}[\hat{H}]$:

$$X_H = X \times_{\hat{H}} \mathbb{Z}[\hat{H}] = N^\times \oplus \zeta(\mathbb{Z}[\hat{H}]) \quad (9.5)$$

with the \mathbb{Z} -section $\zeta : \mathbb{Z}[\hat{H}] \rightarrow X_H$. According to (9.3) we have the well-defined $\mathbb{Z}[H]$ -action

$$x^\tau = x \cdot (\xi \circ \eta_H(x))(\tau) \quad \text{for } x \in X_H, \tau \in H,$$

on X_H . Using the direct decomposition $x = (u, \zeta(\sum_{\chi \in \hat{H}} m_\chi \chi))$ and substituting $\mathbb{Z}[\hat{H}]$ for $\zeta(\mathbb{Z}[\hat{H}])$ in (9.5) we obtain the formula

$$(u, \sum_{\chi \in \hat{H}} m_\chi \chi)^\tau = (u \prod_{\chi \in \hat{H}} \chi(\tau)^{m_\chi}, \sum_{\chi \in \hat{H}} m_\chi \chi). \quad (9.6)$$

Thus X_H is determined up to equivalence as the direct sum of the \mathbb{Z} -modules N^\times and $\mathbb{Z}[\hat{H}]$ with the $\mathbb{Z}[H]$ -action (9.6) not depending on X , and therefore can be constructed even without the knowledge of X . This proves:

Corollary 9.2. *Denote by X the \tilde{G} -module \tilde{X} in Theorem 9.1 considered as $\mathbb{Z}[H]$ -module and $\mathbb{Z}[\hat{H}]$ the trivial $\mathbb{Z}[H]$ -module over \hat{H} . Then as a \mathbb{Z} -module the fiber product in the category of $\mathbb{Z}[H]$ -modules $X_H := X \times_{\hat{H}} \mathbb{Z}[\hat{H}]$ decomposes into a direct sum $N^\times \oplus \mathbb{Z}[\hat{H}]$ with the $\mathbb{Z}[H]$ -action given in (9.6). In particular, there exists a $\mathbb{Z}[H]$ -epimorphism from X_H onto X .*

The assertion of Corollary 9.2 can also be visualized by the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} e_H : 1 & \longrightarrow & N^\times & \xrightarrow{\varepsilon_H} & X_H & \xrightarrow{\eta_H} & \mathbb{Z}[\hat{H}] \longrightarrow 1 \\ \uparrow \xi_1^* & & \parallel & & \downarrow \xi_X & & \downarrow \xi \\ e : 1 & \longrightarrow & N^\times & \xrightarrow{\varepsilon} & X & \xrightarrow{\eta} & \hat{H} \longrightarrow 1 \end{array} \quad (9.7)$$

Since here the two exact sequences are determined up to equivalence, they define elements $e_H = e_H(\varphi, \kappa) \in \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)$ and $e = e(\varphi, \kappa) \in \text{Ext}_H^1(\hat{H}, N^\times)$ (with the convention $\text{Ext}_H^n(\cdot, \cdot) := \text{Ext}_{\mathbb{Z}[H]}^n(\cdot, \cdot)$ for groups H) which depend formally on φ and κ via $N := \bar{K}^{\ker(\varphi)}$ and $H := \ker(\kappa)$. These satisfy $\xi_1^*(e) = e_H$ with the map ξ_1^* induced on $\text{Ext}_H^1(\hat{H}, N^\times)$ by ξ .

Remark. For each $\sigma \in G$ acting on $\mathbb{Z}[\hat{H}]$ by (9.1) and on N^\times via the Galois action we obtain an exact sequence equivalent to the first line of (9.7) because of

$$(u \prod_{\chi \in \hat{H}} \chi(\tau)^{m_\chi}, \sum_{\chi \in \hat{H}} m_\chi \chi)^\sigma = (u^\sigma \prod_{\chi \in \hat{H}} \chi^\sigma(\tau^\sigma)^{m_\chi}, \sum_{\chi \in \hat{H}} m_\chi \chi^\sigma).$$

Therefore, the element $e_H \in \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)$ even lies in $\text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)^G$.

9.2 Definition of the Hasse Obstruction

Starting from the \tilde{G} -module \tilde{X} in Theorem 9.1 we may form the fiber product of \tilde{X} and $\mathbb{Z}[\hat{H}]$ over \hat{H} as $\mathbb{Z}[\tilde{G}]$ -module. This fits into the following commutative

diagram with exact rows

$$\begin{array}{ccccccc} \tilde{e}_H : 1 & \longrightarrow & N^\times & \xrightarrow{\tilde{\varepsilon}_H} & \tilde{X}_H & \xrightarrow{\tilde{\eta}_H} & \mathbb{Z}[\hat{H}] \longrightarrow 1 \\ \uparrow \tilde{\xi}_1^* & & \parallel & & \downarrow \tilde{\xi}_X & & \downarrow \tilde{\xi} \\ \tilde{e} : 1 & \longrightarrow & N^\times & \xrightarrow{\varepsilon} & \tilde{X} & \xrightarrow{\eta} & \hat{H} \longrightarrow 1 \end{array} \quad (9.8)$$

with $\tilde{e}_H = \tilde{e}_H(\varphi, \kappa) \in \text{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times)$ and $\tilde{e} = \tilde{e}(\varphi, \kappa) \in \text{Ext}_{\tilde{G}}^1(\hat{H}, N^\times)$. As a first condition for the solvability of the embedding problem $\mathcal{E}(\varphi, \kappa)$ we have to answer the question whether the H -action on X_H may be extended to a \tilde{G} -action on \tilde{X}_H compatible with the given G -action.

The following lemma contains an argument needed to prove the subsequent two-step solvability criterion and will itself be used again later on. Here a G -module M is called *cohomologically trivial in dimension i* , if $H^i(U, M) = 0$ for all subgroups U of G .

Lemma 9.3. *Let M be a G -module cohomologically trivial in dimension i . Then we have*

$$H^i(G, \text{Hom}(\mathbb{Z}[\hat{H}], M)) = 0. \quad (9.9)$$

Proof. Let R be a system of representatives of the finitely many G -orbits on \hat{H} and G_χ the stabilizer of $\chi \in R$. Then $\mathbb{Z}[\hat{H}]$ possesses the following direct decomposition as G -module

$$\mathbb{Z}[\hat{H}] = \prod_{\chi \in R} \mathbb{Z}[G/G_\chi].$$

From this the Lemma of Shapiro (see for example Serre (1964), Ch. I, Prop. 10, or Shatz (1972), Ch. II, Thm. 8) yields

$$\begin{aligned} H^i(G, \text{Hom}(\mathbb{Z}[\hat{H}], M)) &\cong \prod_{\chi \in R} H^i(G, \text{Hom}(\mathbb{Z}[G/G_\chi], M)) \\ &\cong \prod_{\chi \in R} H^i(G_\chi, \text{Hom}(\mathbb{Z}, M)) \cong \prod_{\chi \in R} H^i(G_\chi, M) = 0. \end{aligned} \quad \square$$

Theorem 9.4 (Yakovlev (1964)). *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem with abelian kernel H of order prime to the characteristic of K and N be the fixed field of $\ker(\varphi)$. Further denote by $e_H = e_H(\varphi, \kappa) \in \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)^G$ the uniquely determined equivalence class of extensions of $\mathbb{Z}[H]$ -modules in (9.7) according to Corollary 9.2 with Remark. Then we have:*

(a) $\mathcal{E}(\varphi, \kappa)$ is concordant if and only if there exists an element $\tilde{e}_H = \tilde{e}_H(\varphi, \kappa) \in \text{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times)$ with restriction $t_1^*(\tilde{e}_H) = e_H$. This is then uniquely determined as the preimage of $e_H(\varphi, \kappa)$.

(b) $\mathcal{E}(\varphi, \kappa)$ has a solution, if in addition there exists an element $\tilde{e} = \tilde{e}(\varphi, \kappa) \in \text{Ext}_{\tilde{G}}^1(\hat{H}, N^\times)$ with $\tilde{\xi}_1^*(\tilde{e}) = \tilde{e}_H$.

Proof. By Theorem 9.1 and the above we only have to prove part (a). The group extension

$$1 \longrightarrow H \xrightarrow{\iota} \tilde{G} \xrightarrow{\kappa} G \longrightarrow 1$$

with $G = \varphi(\Gamma_K)$ and $H = \ker(\kappa)$ corresponding to the cohomology class $h \in H^2(G, H)$ gives rise to the Hochschild–Serre sequence (see for example Serre (1964), Ch. I, §2.6, or Shatz (1972), Ch. II, §4, (25))

$$0 \longrightarrow H^1(G, M^H) \xrightarrow{\kappa_1^*} H^1(\tilde{G}, M) \xrightarrow{\iota_1^*} H^1(H, M)^G \xrightarrow{\vartheta_2} H^2(G, M^H)$$

with the inflation κ_1^* and the restriction ι_1^* and the transgression ϑ_2 for the \tilde{G} -module

$$M := N[H]^\times \cong \text{Map}(\hat{H}, N^\times) \cong \text{Hom}(\mathbb{Z}[\hat{H}], N^\times), \quad (9.10)$$

where the canonical isomorphisms in (9.10) are used for the identification. Using that H acts trivially on \hat{H} and N^\times , and with the canonical isomorphism

$$H^i(F, N[H]^\times) = H^i(F, \text{Hom}(\mathbb{Z}[\hat{H}], N^\times)) \cong \text{Ext}_F^i(\mathbb{Z}[\hat{H}], N^\times) \quad (9.11)$$

for $F \in \{G, \tilde{G}, H\}$ (see for example Benson (1991), Prop. 3.1.8(iii)), as well as the vanishing of $\text{Ext}_G^1(\mathbb{Z}[\hat{H}], N^\times)$ by Hilbert's Satz 90 and Lemma 9.3 we obtain the two isomorphic exact sequences

$$\begin{array}{ccccccc} 0 & \xrightarrow{\kappa_1^*} & H^1(\tilde{G}, N[H]^\times) & \xrightarrow{\iota_1^*} & H^1(H, N[H]^\times)^G & \xrightarrow{\vartheta_2} & H^2(G, N[H]^\times) \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & \text{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times) & \longrightarrow & \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)^G & \longrightarrow & \text{Ext}_G^2(\mathbb{Z}[\hat{H}], N^\times). \end{array} \quad (9.12)$$

Here the element $e_H \in \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times)^G$ is given as an element of the group $H^1(H, N[H]^\times)^G \cong \text{Hom}(H, \text{Hom}(\mathbb{Z}[\hat{H}], N^\times))^G$ by the homomorphism

$$\delta_H : H \rightarrow \text{Hom}(\mathbb{Z}[\hat{H}], N^\times), \quad \tau \mapsto \left(\sum_{\chi \in \hat{H}} m_\chi \chi \mapsto \prod_{\chi \in \hat{H}} \chi(\tau)^{m_\chi} \right).$$

Thus an element $\tilde{e}_H \in \text{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times) \cong H^1(\tilde{G}, N[H]^\times)$ with $\iota_1^*(\tilde{e}_H) = e_H$ exists precisely if the homomorphism δ_H can be extended to a crossed homomorphism $\tilde{\delta}_H$ from \tilde{G} to $\text{Hom}(\mathbb{Z}[\hat{H}], N^\times)$ (for this see for example Hilton and Stammbach (1971), Ch. VI.5). Furthermore, \tilde{e}_H is then uniquely determined by e_H because of the injectivity of ι_1^* .

To determine the extendability of δ_H we let $\{\tilde{\sigma} \mid \sigma \in G\}$ be a system of representatives of G in \tilde{G} with $\tilde{1}_G = 1_{\tilde{G}}$ and with cocycle $b = (b_{\sigma, \tau}) \in h$ (compare Theorem 6.1). Then for each

$$\mathbf{c}_\sigma := (c_\sigma(\chi))_{\chi \in \hat{H}} \in \text{Map}(\hat{H}, N^\times) \cong N[H]^\times$$

we obtain by multiplicative extension of δ_H from

$$\tilde{\delta}_H : \tilde{G} \rightarrow \text{Hom}(\mathbb{Z}[\hat{H}], N^\times), \quad \tilde{\sigma} \mapsto \left(\sum_{\chi \in \hat{H}} m_\chi \chi \mapsto \prod_{\chi \in \hat{H}} c_\sigma(\chi)^{m_\chi} \right)$$

a well-defined map from \tilde{G} to $N[H]^\times$. It can easily be checked that this is a crossed homomorphism with respect to the given action of G on \hat{H} and N if and only if

$$\mathbf{c}_\sigma^\tau \mathbf{c}_\tau = \mathbf{c}_{\sigma\tau} \mathbf{b}_{\sigma,\tau} \quad \text{with } \mathbf{b}_{\sigma,\tau} := (\chi(b_{\sigma,\tau}))_{\chi \in \hat{H}} \in \text{Map}(\hat{H}, N^\times) \cong N[H]^\times,$$

for all $\sigma, \tau \in G$, i.e., if the factor system b splits over $N[H]^\times$. Therefore, if we denote by v_2^* the cohomological map

$$v_2^* : H^2(G, H) \longrightarrow H^2(G, N[H]^\times) \tag{9.13}$$

induced by the embedding $v : H \rightarrow N[H]^\times$, then $\tilde{\vartheta}_H$ becomes a crossed homomorphism if and only if $v_2^*(h) = 0$.

Finally we prove that $v_2^*(h) = 0$ if and only if $\mathcal{E}(\varphi, \kappa)$ is concordant. For this we use the final part of the Hochschild–Serre sequence for the group extension $\Gamma_K = \Gamma_N \cdot G$

$$H^1(\Gamma_N, N[H]^\times)^G \xrightarrow{\tilde{\vartheta}_2} H^2(G, N[H]^\times) \xrightarrow{\tilde{\varphi}^*} H^2(\Gamma_K, N[H]^\times). \tag{9.14}$$

Now let R denote a system of representatives of the orbits in \hat{H} under the action of G respectively Γ_K and $[\chi]^G$ the G -orbit of $\chi \in R$ in \hat{H} . Then we have

$$H^2(G, N[H]^\times) \cong \prod_{\chi \in R} H^2(G, \text{Map}([\chi]^G, N^\times)) \cong \prod_{\chi \in R} H^2(G_\chi, N^\times)$$

by the Lemma of Shapiro since $\text{Map}([\chi]^G, N^\times)$ is the G -module induced from the G_χ -module N^\times . With the corresponding decomposition of the Γ_K -module $N[H]^\times$ from (9.14) we arrive at the following diagram

$$\begin{array}{ccccc} H^2(G, H) & \xrightarrow{\varphi^*} & H^2(\Gamma_K, H) & \xrightarrow{\rho_H^*} & \prod_{\chi \in \hat{H}} \text{Br}(K_\chi) \\ \downarrow v_2^* & & \downarrow & & \uparrow \\ H^2(G, N[H]^\times) & \xrightarrow{\tilde{\varphi}^*} & H^2(\Gamma_K, N[H]^\times) & & \\ \downarrow \cong & & \downarrow \cong & & \\ \prod_{\chi \in R} H^2(G_\chi, N^\times) & \longrightarrow & \prod_{\chi \in R} H^2(\Gamma_\chi, N^\times) & \longrightarrow & \prod_{\chi \in R} \text{Br}(K_\chi) \end{array} \tag{9.15}$$

Here the homomorphisms in the lower row are injective on the $\exp(H)$ -torsion part, since their composite by Proposition 7.1 gives the embedding of the $\exp(H)$ -torsion of the relative Brauer groups $H^2(G_\chi, N^\times) \cong \text{Br}(K_\chi, N)$ into the absolute Brauer groups $\text{Br}(K_\chi)$ (see Jacobson (1980), Ch. IV.7). Since the preceding considerations

are independent of the choice of the system of representatives $R \subseteq \hat{H}$ the characterization of the concordance condition $\rho_H^* \circ \varphi^*(h) = 0$ from Theorem 8.4(a) by $v_2^*(h) = 0$ follows immediately from the diagram (9.15). \square

Remark. By the explicit description of the transgression ϑ_2 (see for example Suzuki (1982), Ch. 2, §7) it follows from

$$\frac{\tilde{\delta}_H(\tilde{\sigma}\tilde{\tau})}{\tilde{\delta}_H(\tilde{\sigma})^\tau\tilde{\delta}_H(\tilde{\tau})} \cdot \frac{\mathbf{c}_\sigma^\tau \mathbf{c}_\tau}{\mathbf{c}_{\sigma\tau}} = \mathbf{b}_{\sigma,\tau} \quad \text{for } \tilde{\sigma}, \tilde{\tau} \in \tilde{G} \text{ with } \kappa(\tilde{\sigma}) = \sigma, \kappa(\tilde{\tau}) = \tau \in G,$$

that $\vartheta_2(e_H) = v_2^*(h)$. Therefore,

$$p(\varphi, \kappa) := \vartheta_2(e_H) = v_2^*(h) \in H^2(G, N[H]^\times) \cong \mathrm{Ext}_G^2(\mathbb{Z}[\hat{H}], N^\times) \quad (9.16)$$

constitutes the *concordance obstruction* (or *first embedding obstruction*) of $\mathcal{E}(\varphi, \kappa)$.

By Theorem 9.4(b) the *Hasse embedding obstruction* (or *second embedding obstruction*) for the solvability of a concordant embedding problem is the obstruction for the existence of an $\tilde{e} = \tilde{e}(\varphi, \kappa) \in \mathrm{Ext}_{\tilde{G}}^1(\hat{H}, N^\times)$ with $\tilde{\xi}_1^*(\tilde{e}) = \tilde{e}_H$. This is obtained in a natural way as the image of \tilde{e}_H under the map

$$\tilde{v}_1^* : \mathrm{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times) \longrightarrow \mathrm{Ext}_{\tilde{G}}^1(Y(\hat{H}), N^\times) \quad (9.17)$$

in the long sequence of Ext-groups induced by the embedding \tilde{v} in the exact sequence of $\mathbb{Z}[G]$ -modules

$$1 \longrightarrow Y(\hat{H}) \xrightarrow{\tilde{v}} \mathbb{Z}[\hat{H}] \xrightarrow{\tilde{\xi}} \hat{H} \longrightarrow 1 \quad (9.18)$$

with $Y(\hat{H}) := \ker(\tilde{\xi})$ for $\tilde{\xi}$ in (9.8). Thus (9.17) with (9.11) leads to the following consequence of Theorem 9.4 (see also Ishkhanov, Lure and Faddeev (1997), Thm. 3.11):

Corollary 9.5. *The Hasse embedding obstruction $q(\varphi, \kappa)$ for the solvability of a concordant finite embedding problem $\mathcal{E}(\varphi, \kappa)$ with abelian kernel is the image of $\tilde{e}_H(\varphi, \kappa) \in \mathrm{Ext}_{\tilde{G}}^1(\mathbb{Z}[\hat{H}], N^\times)$ under the map \tilde{v}_1^* in (9.17):*

$$q(\varphi, \kappa) := \tilde{v}_1^*(\tilde{e}_H(\varphi, \kappa)) \in \mathrm{Ext}_{\tilde{G}}^1(Y(\hat{H}), N^\times) \cong H^1(\tilde{G}, \mathrm{Hom}(Y(\hat{H}), N^\times)). \quad (9.19)$$

In the next sections under additional assumptions we give more convenient expressions for the Hasse embedding obstruction.

9.3 Translation of the Hasse Obstruction

First we want to simplify the Hasse obstruction by reducing G to a suitable factor group of a subgroup of index prime to $|H|$. The first step is achieved as follows:

Proposition 9.6. *Let $\mathcal{E}(\varphi, \kappa)$ be a concordant finite embedding problem for which the assumptions of Theorem 9.4 are satisfied. Let U be a normal subgroup of $G = \varphi(\Gamma_K)$ acting trivially on the character group \hat{H} , with factor group $F := G/U$ and fixed field $L := N^U$. Then the Hasse obstruction $q(\varphi, \kappa) \in \text{Ext}_{\hat{G}}^1(Y(\hat{H}), N^\times)$ has a representation as the preimage in $\text{Ext}_F^1(Y(\hat{H}), L^\times)$ under an injective homomorphism.*

Proof. We first consider the following commutative diagram, whose lower row is the first part of the Hochschild–Serre sequence (9.12) restricted to $Y(\hat{H})$, and with $\iota_1^*, v_1^*, \tilde{v}_1^*$ in their previous meaning:

$$\begin{array}{ccc} \text{Ext}_{\hat{G}}^1(\mathbb{Z}[\hat{H}], N^\times) & \xrightarrow{\iota_1^*} & \text{Ext}_H^1(\mathbb{Z}[\hat{H}], N^\times) \\ \downarrow \tilde{v}_1^* & & \downarrow v_1^* \\ 0 \rightarrow \text{Ext}_G^1(Y(\hat{H}), N^\times) & \xrightarrow{\tilde{\kappa}_1^*} & \text{Ext}_{\hat{G}}^1(Y(\hat{H}), N^\times) \xrightarrow{\tilde{\iota}_1^*} \text{Ext}_H^1(Y(\hat{H}), N^\times). \end{array} \quad (9.20)$$

The maps here satisfy $(v_1^* \circ \iota_1^*)(\tilde{e}_H) = v_1^*(e_H) = 0$, since e_H has preimages under ξ_1^* in $\text{Ext}_H^1(\hat{H}, N^\times)$ by Corollary 9.2. Consequently the Hasse obstruction $q(\varphi, \kappa)$ possesses precisely one preimage

$$q_G = q_G(\varphi, \kappa) \in \text{Ext}_G^1(Y(\hat{H}), N^\times) \quad \text{with } \tilde{\kappa}_1^*(q_G) = q(\varphi, \kappa). \quad (9.21)$$

For the second step we exploit the exact sequence

$$1 \longrightarrow U \xrightarrow{\omega} G \xrightarrow{\pi} F \longrightarrow 1. \quad (9.22)$$

The first part of the Hochschild–Serre sequence for this group extension yields an exact sequence

$$0 \longrightarrow \text{Ext}_F^1(Y(\hat{H}), L^\times) \xrightarrow{\pi_1^*} \text{Ext}_G^1(Y(\hat{H}), N^\times) \xrightarrow{\omega_1^*} \text{Ext}_U^1(Y(\hat{H}), N^\times)^F. \quad (9.23)$$

Since U acts trivially on $\mathbb{Z}[\hat{H}]$ and hence on $Y(\hat{H})$, and $Y(\hat{H})$ is finitely generated as subgroup of $\mathbb{Z}[\hat{H}]$ and torsion free, $Y(\hat{H})$ splits as U -module into a direct sum of finitely many copies of \mathbb{Z} , say $Y(\hat{H}) \cong \bigoplus_{i=1}^r \mathbb{Z}$. Using Hilbert's Satz 90 this yields

$$\text{Ext}_U^1(Y(\hat{H}), N^\times) = \prod_{i=1}^r \text{Ext}_U^1(\mathbb{Z}, N^\times) = \prod_{i=1}^r H^1(U, N^\times) = 0.$$

Thus the map π_1^* in (9.23) is even bijective, and there exists a unique element

$$q_F = q_F(\varphi, \kappa) \in \text{Ext}_F^1(Y(\hat{H}), L^\times) \quad \text{with } \pi_1^*(q_F) = q_G(\varphi, \kappa). \quad (9.24)$$

□

In the special case $G = U$ we may recover Theorem 8.7 from Proposition 9.6. With the reduction principle of Kochendörffer for concordant and solvable embedding problems we obtain the final form of Theorem 9.4:

Theorem 9.7 (Yakovlev (1964)). *Let $\mathcal{E}(\varphi, \kappa)$ be a finite embedding problem with abelian kernel H of order prime to the characteristic of K , N the fixed field of $\ker(\varphi)$ and $G = \text{Gal}(N/K)$. Further let V be a subgroup of G with $\gcd((G : V), |H|) = 1$ containing a normal subgroup U of G with trivial action on \hat{H} . Then the Hasse obstruction $q(\varphi, \kappa)$ may be represented by an element of $\text{Ext}_F^1(Y(\hat{H}), L^\times)$ with $F := V/U$ and $L := N^U$.*

Remark. From now on we will distinguish between the different representations of the Hasse obstruction, namely $q(\varphi, \kappa)$ in $\text{Ext}_{\tilde{G}}^1(Y(\hat{H}), N^\times)$ from Equation (9.19), in $\text{Ext}_G^1(Y(\hat{H}), N^\times)$ from (9.21) respectively in $\text{Ext}_F^1(Y(\hat{H}), L^\times)$ from (9.24), only by indicating the relevant group.

In the next section we further study the Hasse embedding obstruction in the case of a global ground field K .

9.4 The Hasse Obstruction for Global Fields

In this section let N/GK be a finite Galois extension of global fields. For such an extension we have the following two fundamental short exact sequences of G -modules

$$1 \longrightarrow N^\times \xrightarrow{\alpha} J(N) \xrightarrow{\beta} C(N) \longrightarrow 1 \quad (9.25)$$

with the idele group $J(N)$ and the idele class group $C(N)$, and

$$1 \longrightarrow \mathbb{D}^\circ(N) \xrightarrow{\tilde{\alpha}} \mathbb{D}(N) \xrightarrow{\tilde{\beta}} \mathbb{Z} \longrightarrow 1 \quad (9.26)$$

with the free abelian group $\mathbb{D}(N)$ (written multiplicatively) over $\mathbb{P}(N)$ and the obvious extended G -action from $\mathbb{P}(N)$ to $\mathbb{D}(N)$, and the degree map

$$\tilde{\beta} : \mathbb{D}(N) \longrightarrow \mathbb{Z}, \quad \prod_{\mathfrak{p} \in \mathbb{P}(N)} \mathfrak{p}^{m_\mathfrak{p}} \mapsto \sum_{\mathfrak{p} \in \mathbb{P}(N)} m_\mathfrak{p} \cdot \deg(\mathfrak{p}),$$

into the trivial G -module \mathbb{Z} .

Now we tensor with a torsion free G -module M and extend the G -action on the G -module A onto $M \otimes A$ via

$$(x \otimes a)^\sigma := x^\sigma \otimes a^\sigma \quad \text{for } x \in M, a \in A, \sigma \in G.$$

By this process, (9.25) and (9.26) again yield short exact sequences of G -modules and then long cohomology sequences for the modified cohomology groups of Tate. These satisfy:

Theorem 9.8 (Comparison Theorem of Tate (1966)). *Let N/GK be a finite Galois extension of global fields and M a torsion free G -module. Then the long exact sequences of Tate cohomology groups originating from (9.25) and (9.26) are connected for all $i \in \mathbb{Z}$ by the commutative diagram*

$$\begin{array}{ccccccc} \xrightarrow{\partial_i} & H^i(G, M \otimes \mathbb{D}^0(N)) & \xrightarrow{\tilde{\alpha}_i^*} & H^i(G, M \otimes \mathbb{D}(N)) & \xrightarrow{\tilde{\beta}_i^*} & H^i(G, M \otimes \mathbb{Z}) & \xrightarrow{\partial_{i+1}} \\ & \downarrow \gamma_i^N & & \downarrow \gamma_i^J & & \downarrow \gamma_i^C & \\ \xrightarrow{\partial_j} & H^j(G, M \otimes N^\times) & \xrightarrow{\alpha_j^*} & H^j(G, M \otimes J(N)) & \xrightarrow{\beta_j^*} & H^j(G, M \otimes C(N)) & \xrightarrow{\partial_{j+1}} \end{array}$$

with isomorphisms γ_i^N , γ_i^J and γ_i^C , where $j := i + 2$.

For the proof we refer the reader to the original paper Tate (1966).

Now let M be a G -module, finitely generated and free as \mathbb{Z} -module. Then $\text{Hom}(M, \mathbb{Z})$ is torsion free and satisfies the assumptions of Theorem 9.8. The validity of

$$\text{Hom}(M, \mathbb{Z}) \otimes A \cong \text{Hom}(M, \mathbb{Z}) \otimes \text{Hom}(\mathbb{Z}, A) \cong \text{Hom}(M, A) \quad (9.27)$$

for all G -modules A then implies, together with Theorem 9.8, the exactness of

$$\dots \longrightarrow H^i(G, \text{Hom}(M, \mathbb{D}(N))) \longrightarrow H^i(G, \text{Hom}(M, \mathbb{Z})) \longrightarrow \\ \longrightarrow H^{i+3}(G, \text{Hom}(M, N^\times)) \longrightarrow H^{i+1}(G, \text{Hom}(M, \mathbb{D}(N))) \longrightarrow \dots \quad (9.28)$$

for all $i \in \mathbb{Z}$. The decomposition

$$\mathbb{D}(N) = \prod_{\mathfrak{p} \in \mathbb{P}(K)} \mathbb{D}_{\mathfrak{p}} \quad \text{with } \mathbb{D}_{\mathfrak{p}} := \prod_{\tilde{\mathfrak{p}} \in \mathbb{P}(N), \tilde{\mathfrak{p}} \mid \mathfrak{p}} \tilde{\mathfrak{p}}^{\mathbb{Z}}$$

of $\mathbb{D}(N)$ as G -module first implies

$$\text{Hom}(M, \mathbb{D}(N)) \cong \bigoplus_{\mathfrak{p} \in \mathbb{P}(K)} \text{Hom}(M, \mathbb{D}_{\mathfrak{p}}).$$

Denoting by $G_{\mathfrak{p}}$ the decomposition group of an extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p} \in \mathbb{P}(K)$ in $\mathbb{P}(N)$ we obtain that $\mathbb{D}_{\mathfrak{p}}$ respectively $\text{Hom}(M, \mathbb{D}_{\mathfrak{p}})$ are the G -modules induced from the $G_{\mathfrak{p}}$ -modules $\tilde{\mathfrak{p}}^{\mathbb{Z}}$ respectively $\text{Hom}(M, \mathbb{Z})$. The Lemma of Shapiro then gives

$$H^i(G, \text{Hom}(M, \mathbb{D}(N))) \cong \bigoplus_{\mathfrak{p} \in \mathbb{P}(K)} H^i(G_{\mathfrak{p}}, \text{Hom}(M, \mathbb{Z})). \quad (9.29)$$

Equations (9.28) and (9.29) now yield the following exact sequence as a consequence of the Comparison Theorem of Tate:

Corollary 9.9. *Let N/GK be as in Theorem 9.8 and M a G -module which is finitely generated and free as \mathbb{Z} -module. Then the following sequence of Tate cohomology*

groups is exact for all $i \in \mathbb{Z}$:

$$\begin{aligned} & \longrightarrow \bigoplus_{\mathfrak{p} \in \mathbb{P}(K)} H^i(G_{\mathfrak{p}}, \text{Hom}(M, \mathbb{Z})) \xrightarrow{\tilde{\beta}_i^*} H^i(G, \text{Hom}(M, \mathbb{Z})) \xrightarrow{\partial_i + 3 \circ \gamma_i^C} \\ & H^{i+3}(G, \text{Hom}(M, N^{\times})) \xrightarrow{(\gamma_{i+1}^J)^{-1} \circ \alpha_{i+3}} \bigoplus_{\mathfrak{p} \in \mathbb{P}(K)} H^{i+1}(G_{\mathfrak{p}}, \text{Hom}(M, \mathbb{Z})) \end{aligned} \quad (9.30)$$

A further step for the main result of this section will be given by the following short exact sequence.

Proposition 9.10. *Let A be a finite abelian group and $A^* := \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ its dual group. Then the following sequence is exact:*

$$0 \longrightarrow \text{Hom}(\mathbb{Z}[A], \mathbb{Z}) \longrightarrow \text{Hom}(Y(A), \mathbb{Z}) \longrightarrow A^* \longrightarrow 0. \quad (9.31)$$

Proof. From the exact injective resolution

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

of \mathbb{Z} we obtain the following piece of the long exact sequence of Hom- and Ext-groups

$$0 = \text{Hom}(A, \mathbb{Q}) \longrightarrow \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \longrightarrow \text{Ext}^1(A, \mathbb{Z}) \longrightarrow \text{Ext}^1(A, \mathbb{Q}) = 0$$

with $\text{Ext}^1 = \text{Ext}_{\mathbb{Z}}^1$ and thus

$$\text{Ext}^1(A, \mathbb{Z}) \cong \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) = A^*. \quad (9.32)$$

Further the exact sequence (9.18) with A in place of \hat{H} yields:

$$\begin{aligned} 0 \longrightarrow \text{Hom}(A, \mathbb{Z}) \longrightarrow \text{Hom}(\mathbb{Z}[A], \mathbb{Z}) \longrightarrow \text{Hom}(Y(A), \mathbb{Z}) \longrightarrow \\ \text{Ext}^1(A, \mathbb{Z}) \longrightarrow \text{Ext}^1(\mathbb{Z}[A], \mathbb{Z}). \end{aligned}$$

Here we have $\text{Hom}(A, \mathbb{Z}) = 0$ due to the finiteness of A and $\text{Ext}^1(\mathbb{Z}[A], \mathbb{Z}) = 0$ because $\mathbb{Z}[A]$ is free as \mathbb{Z} -module. Thus the above, together with (9.32), yields (9.31). \square

The commutative diagram in Figure 9.1 of Tate cohomology groups is patched together from the following ingredients. The upper two rows come from the exact sequence (9.30) of Tate for F, L in place of G, N and the F -modules $\mathbb{Z}[\hat{H}]$ and $Y(\hat{H})$. The first two columns are the long cohomology sequences arising from the short exact sequence (9.31), and we have used the abbreviations

$$\begin{aligned} V &:= \text{Hom}(\mathbb{Z}[\hat{H}], \mathbb{Z}), \quad W := \text{Hom}(Y(\hat{H}), \mathbb{Z}), \\ P &:= H^1(F, \text{Hom}(\mathbb{Z}[\hat{H}], L^{\times})), \quad Q := H^1(F, \text{Hom}(Y(\hat{H}), L^{\times})). \end{aligned}$$

The third row is completed with the cokernel T of the homomorphism θ defined by the vanishing of the cohomology groups in the last row which will be proved

together with Theorem 9.11. The sums are all taken over $\mathfrak{p} \in \mathbb{P}(K)$.

$$\begin{array}{ccccccc}
\bigoplus H^{-2}(F_{\mathfrak{p}}, V) & \longrightarrow & H^{-2}(F, V) & \longrightarrow & P^{\dagger} & \longrightarrow & \bigoplus H^{-1}(F_{\mathfrak{p}}, V) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\bigoplus H^{-2}(F_{\mathfrak{p}}, W) & \longrightarrow & H^{-2}(F, W) & \longrightarrow & Q & \longrightarrow & \bigoplus H^{-1}(F_{\mathfrak{p}}, W)^{\dagger} \\
\downarrow & & \downarrow & & \downarrow \psi & & \\
\bigoplus H^{-2}(F_{\mathfrak{p}}, \hat{H}^*) & \xrightarrow{\theta} & H^{-2}(F, \hat{H}^*) & \longrightarrow & T & \longrightarrow & 0 \\
\downarrow & & \downarrow & & & & \\
\bigoplus H^{-1}(F_{\mathfrak{p}}, V)^{\dagger} & \longrightarrow & H^{-1}(F, V)^{\dagger} & & & &
\end{array}$$

Fig. 9.1 Hasse obstruction for global fields

From this we can deduce the following result (see Ishkhanov, Lure and Faddeev (1997), Thm. 3.14.2, for the version dualized via loc. cit. Thm. A.6).

Theorem 9.11 (Yakovlev (1967)). *Assume the hypotheses of Theorem 9.7 and moreover let K be a global field. Then there exists an isomorphism*

$$\psi : Q = \text{Ext}_F^1(Y(\hat{H}), L^{\times}) \longrightarrow T = H^{-2}(F, \hat{H}^*)/\theta\left(\bigoplus_{\mathfrak{p} \in \mathbb{P}(K)} H^{-2}(F_{\mathfrak{p}}, \hat{H}^*)\right). \quad (9.33)$$

In particular the Hasse embedding obstruction from Theorem 9.7 possesses a representation $q(\varphi, \kappa) \in T$.

Proof. We first prove that the four cohomology groups marked by \dagger in Figure 9.1 vanish. Obviously

$$P = H^1(F, \text{Hom}(\mathbb{Z}[\hat{H}], L^{\times})) = 0 \quad (9.34)$$

by Lemma 9.3 since L^{\times} is cohomologically trivial in dimension 1. Since the trivial F -module \mathbb{Z} is cohomologically trivial in dimension -1 , the same lemma gives

$$H^{-1}(F, V) = H^{-1}(F, \text{Hom}(\mathbb{Z}[\hat{H}], \mathbb{Z})) = 0, \quad (9.35)$$

$$H^{-1}(F_{\mathfrak{p}}, V) = H^{-1}(F_{\mathfrak{p}}, \text{Hom}(\mathbb{Z}[\hat{H}], \mathbb{Z})) = 0. \quad (9.36)$$

It remains to show the vanishing of $H^{-1}(F_{\mathfrak{p}}, W)$. Since by Lemma 9.12 below

$$H^{-1}(F_{\mathfrak{p}}, W) = H^{-1}(F_{\mathfrak{p}}, \text{Hom}(Y(\hat{H}), \mathbb{Z})) \cong H^1(F_{\mathfrak{p}}, Y(\hat{H}))^* \quad (9.37)$$

it suffices to prove the vanishing of $H^1(F_{\mathfrak{p}}, Y(\hat{H}))$. For this we employ the following long cohomology sequence derived from (9.18):

$$\begin{aligned}
0 \longrightarrow & H^0(F_{\mathfrak{p}}, Y(\hat{H})) \longrightarrow H^0(F_{\mathfrak{p}}, \mathbb{Z}[\hat{H}]) \xrightarrow{\tilde{\xi}_0^*} H^0(F_{\mathfrak{p}}, \hat{H}) \xrightarrow{\partial_1} \\
& H^1(F_{\mathfrak{p}}, Y(\hat{H})) \xrightarrow{\tilde{v}_1^*} H^1(F_{\mathfrak{p}}, \mathbb{Z}[\hat{H}]).
\end{aligned}$$

Let R_p be a system of representatives of the F_p -orbits in \hat{H} and F_χ the stabilizer in F_p of $\chi \in R_p$. Then analogously to the proof of Lemma 9.3 we have

$$\begin{aligned} H^1(F_p, \mathbb{Z}[\hat{H}]) &\cong \prod_{\chi \in R_p} H^1(F_p, \mathbb{Z}[F_p/F_\chi]) \\ &\cong \prod_{\chi \in R_p} H^1(F_\chi, \mathbb{Z}) \cong \prod_{\chi \in R_p} \text{Hom}(F_\chi, \mathbb{Z}) = 0. \end{aligned}$$

since F_χ is finite. Further, $\tilde{\xi}_0^*$ is surjective since every F_p -invariant element of \hat{H} is the image of an F_p invariant element of $\mathbb{Z}[\hat{H}]$, and hence \tilde{v}_1^* is injective. This implies $H^1(F_p, Y(\hat{H})) = 0$, which together with (9.37) finally gives

$$H^{-1}(F_p, W) = H^{-1}(F_p, \text{Hom}(Y(\hat{H}), \mathbb{Z})) = 0. \quad (9.38)$$

Substituting (9.34), (9.35), (9.36) and (9.38) in Figure 9.1 we obtain from the lower three rows the existence of a monomorphism $\psi : Q \rightarrow T$ making the diagram commutative. By a simple diagram chasing in the upper three rows it follows that ψ is also surjective. This completes the proof of Theorem 9.11. \square

Lemma 9.12. *Let G be a finite group and M a G -module, which as \mathbb{Z} -module is finitely generated and free. Then we have*

$$H^{-i}(G, \text{Hom}(M, \mathbb{Z})) \cong H^i(G, M)^* \quad \text{for } i \in \mathbb{Z}. \quad (9.39)$$

Proof. We consider \mathbb{Z}, \mathbb{Q} and \mathbb{Q}/\mathbb{Z} as trivial G -modules. Since M is a projective \mathbb{Z} -module,

$$0 \longrightarrow \text{Hom}(M, \mathbb{Z}) \longrightarrow \text{Hom}(M, \mathbb{Q}) \longrightarrow \text{Hom}(M, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0 \quad (9.40)$$

becomes an exact sequence of \mathbb{Z} - as well as $\mathbb{Z}[G]$ -modules. Now the multiplication by $|G|$ on $\text{Hom}(M, \mathbb{Q})$ is an isomorphism. Consequently, $\text{Hom}(M, \mathbb{Q})$ is relative (weakly) projective (see Cartan and Eilenberg (1956), Ch. XII, Ex. 1). This implies (by loc. cit., Ch. XII, Prop. 2.2) that

$$H^i(G, \text{Hom}(M, \mathbb{Q})) = 0 \quad \text{for } i \in \mathbb{Z}. \quad (9.41)$$

Thus in the long cohomology sequence derived from (9.40) we get

$$0 \longrightarrow H^{-i-1}(G, \text{Hom}(M, \mathbb{Q}/\mathbb{Z})) \xrightarrow{\partial_{-i}} H^{-i}(G, \text{Hom}(M, \mathbb{Z})) \longrightarrow 0,$$

so the connecting homomorphisms ∂_{-i} become isomorphisms. Together with the isomorphisms

$$\gamma_{-i-1, i} : H^{-i-1}(G, \text{Hom}(M, \mathbb{Q}/\mathbb{Z})) \longrightarrow H^i(G, M)^* \quad (9.42)$$

coming from the duality theorem (loc. cit., Ch. XII, Thm. 6.4, (4')), resp. Ishkhanov, Lure and Faddeev (1997), Thm. A.6) this yields the required isomorphisms $\gamma_{-i-1,i} \circ \partial_{-i}^{-1}$ for (9.39). \square

The representation of the Hasse obstruction in Theorem 9.11 is particularly suited for the shrinking process which was used by Šafarevič (1954d, 1958) for the realization of solvable groups as Galois groups and for the solution of split embedding problems with nilpotent kernel over number fields (compare the dualized version in Ishkhanov, Lure and Faddeev (1997), Prop. 5.5.4). A complete proof of the theorem of Šafarevič has been executed in some detail for example in the monograph Neukirch, Schmidt and Wingberg (2000), Ch. X. Here instead of giving a short report on this proof we prefer to explain the easier special case of nilpotent groups but with complete proofs. This again constitutes a bridge between embedding problems and the results on G-realizations over fields in positive characteristic presented in the next chapter.

10 Nilpotent Galois Groups over Global Fields

To close this chapter we use the method of Scholz (1937) and Reichardt (1937) to construct Galois extensions with nilpotent Galois group over global fields K , where we assume moreover that the group order is coprime to the order of the group of roots of unity contained in the prime field of K . In the case of global fields of positive characteristic this technical condition could be removed by a method of proof presented by Madan, Rzedowski-Calderon and Villa-Salvador (1996). This then yields in particular G-realizations for all nilpotent groups over finite fields.

10.1 Scholz Extensions

In what follows K will usually denote a global field of characteristic p . Otherwise we will speak of general fields.

Nilpotent groups are direct products of groups of prime power order. By Theorem 1.6(a) it hence suffices to realize finite ℓ -groups G as Galois groups, for $\ell \in \text{IP}$. These possess an upper central series with cyclic factors, say

$$G = G_n, \quad G_{n-1} = G_n/Z_\ell, \quad G_{n-2} = G_{n-1}/Z_\ell, \dots, G_1 = Z_\ell,$$

where the cyclic normal subgroup Z_ℓ is contained in the center of G_i for each i . Thus ℓ -extensions over K may be built by solving central embedding problems with cyclic ℓ -kernel. Such embedding problems are always solvable for $\ell = p$ and even properly solvable over global fields by Theorem 8.3(b), so we may assume from now on that $\ell \neq p$.

The following result shows that the Hasse obstruction for such embedding problems is always trivial:

Proposition 10.1. *Let K be an arbitrary field and $\mathcal{E}(\varphi, \kappa)$ a finite central embedding problem over K with elementary abelian kernel H . If $\mathcal{E}(\varphi, \kappa)$ is concordant then it is also solvable.*

Proof. Let $\ell \in \text{IP}$ be the exponent of H . By our above remark we may assume that ℓ is different from the characteristic of K . Let ζ_ℓ denote an ℓ -th root of unity. Since $\gcd([K(\zeta_\ell) : K], \ell) = 1$ the restriction

$$\rho_{K(\zeta_\ell)}^K : H^2(\Gamma_K, H) \longrightarrow H^2(\Gamma_{K(\zeta_\ell)}, H) \tag{10.1}$$

is injective (compare the proof of Theorem 8.2). Thus we may assume that K contains ζ_ℓ . Now $\mathcal{E}(\varphi, \kappa)$ is a central embedding problem over $K = K(\zeta_\ell)$, so Γ_K acts trivially on H via $\varphi(\Gamma_K)$, and hence because of $\zeta_\ell \in K$ also trivially on \hat{H} by (8.4). Thus by Theorem 8.7 the solvability of $\mathcal{E}(\varphi, \kappa)$ follows from its concordance. \square

Remark. In the case of a global field K with $\zeta_\ell \in K$ and a cyclic kernel H Proposition 10.1 also follows immediately from the Theorem of Brauer, Hasse and Noether

(see for example Weil (1974), Ch. XI, Thm. 2, resp. the proof of Prop. 7.6), which yields the injectivity of the product of the restriction maps

$$\rho : H^2(\Gamma_K, H) \longrightarrow \prod_{\mathfrak{p} \in \mathbb{P}(K)} H^2(\Gamma_{K_{\mathfrak{p}}}, H)$$

(see Corollary 7.8 resp. Theorem 8.12(b)).

With Theorem 8.12(a) the preceding Proposition gives:

Corollary 10.2. *For a finite central embedding problem $\mathcal{E}(\varphi, \kappa)$ with elementary abelian kernel over a global field K we have: $\mathcal{E}(\varphi, \kappa)$ is solvable if and only if for all $\mathfrak{p} \in \mathbb{P}(K)$ the local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are solvable.*

Remark. If in Proposition 10.1 and Corollary 10.2 the embedding problem even has a cyclic kernel, then the lifted embedding problem over $K(\zeta_{\ell})$ becomes a Brauer embedding problem. Because of the product formula for Hasse-invariants (see for example Weil (1974), Ch. XIII, Thm. 2) it then suffices to prove local solvability for all but one $\mathfrak{p} \in \mathbb{P}(K(\zeta_{\ell}))$.

We now formulate a sufficient condition for the local and hence global solvability of central embedding problems with cyclic kernel. For this, let $\text{Ram}(N/K)$ denote the set of prime divisors of K ramified in N/K . Here for simplicity in the case of number fields we add those infinite primes of K which yield a non-trivial extension of the completion $K_{\mathfrak{p}}$.

Proposition 10.3. *Let $\mathcal{E}(\varphi, \kappa)$ be a finite central embedding problem with cyclic kernel $H \cong \mathbb{Z}_{\ell}$ for $\ell \in \mathbb{P}$ over a global field K and N the fixed field of $\ker(\varphi)$ with $\text{Gal}(N/K) = G$. Furthermore, let*

$$\mathbb{S}_0 := \{\mathfrak{p} \in \mathbb{P}(K) \mid \mathfrak{p} \mid \ell \text{ or } \mathfrak{p} \mid \infty\} \quad (10.2)$$

in the case that K has characteristic 0, and $\mathbb{S}_0 := \emptyset$ otherwise. Assume that all $\mathfrak{p} \in \text{Ram}(N/K)$ and $\tilde{\mathfrak{p}} \in \mathbb{P}(N)$ with $\tilde{\mathfrak{p}} \mid \mathfrak{p}$ satisfy the following three conditions:

$$(0) \mathfrak{p} \notin \mathbb{S}_0, \quad (1) \mathcal{N}(\mathfrak{p}) \equiv 1 \pmod{\ell^e}, \quad (2) D(\tilde{\mathfrak{p}}/\mathfrak{p}) = I(\tilde{\mathfrak{p}}/\mathfrak{p}),$$

where $\ell^e = \exp_{\ell}(|H.G|)$ and \mathcal{N} denotes the absolute norm. Then $\mathcal{E}(\varphi, \kappa)$ is solvable. In the case $\zeta_{\ell} \in K$ one exception for $\mathfrak{p} \in \text{Ram}(N/K)$ is admissible.

Proof. For $\mathfrak{p} \in \mathbb{P}(K)$ we consider the local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ induced by $\mathcal{E}(\varphi, \kappa)$:

$$\begin{array}{ccccccc} & & & I_{K_{\mathfrak{p}}} & & & \\ & & & \downarrow \varphi_{\mathfrak{p}} & & & \\ & & \tilde{\varphi}_{\mathfrak{p}} & \swarrow & & & \\ 1 & \longrightarrow & Z_{\ell} & \longrightarrow & \tilde{G}_{\mathfrak{p}} & \xrightarrow{\kappa_{\mathfrak{p}}} & G_{\mathfrak{p}} \longrightarrow 1 \end{array}$$

with $G_{\tilde{\mathfrak{p}}} = \text{Gal}(N_{\tilde{\mathfrak{p}}}/K_{\mathfrak{p}}) \cong D(\tilde{\mathfrak{p}}/\mathfrak{p})$ (compare (7.10) and (7.11)). If $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ is split, it is trivially solvable. This case occurs in characteristic 0 for example for all prime divisors \mathfrak{p} of ∞ , since then $G_{\mathfrak{p}} = 1$ by the convention introduced before Proposition 10.3. By Zassenhaus' Splitting Theorem (Huppert (1967), Ch. I, Thm. 18.1) the same holds for all prime divisors of $|G|$ with $\mathfrak{p} \nmid \ell$ since there $\gcd(\ell, |G_{\mathfrak{p}}|) = 1$ by (2). Hence we may now assume that $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ is a Frattini embedding problem and moreover that \mathfrak{p} is only tamely ramified in N/K since the prime divisors of ℓ are unramified in N/K by (0).

In the unramified case $G_{\mathfrak{p}}$ is the Galois group of a residue field extension of global fields, hence cyclic. As $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ is a Frattini embedding problem, this implies that $\tilde{G}_{\mathfrak{p}}$ is again cyclic. Since the maximal unramified Galois extension of $K_{\mathfrak{p}}$ has procyclic Galois group, $\varphi_{\mathfrak{p}}$ can be lifted to an unramified solution $\tilde{\varphi}_{\mathfrak{p}}$ of $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$.

In the tamely ramified case again $G_{\mathfrak{p}} \cong D(\tilde{\mathfrak{p}}/\mathfrak{p}) \cong I(\tilde{\mathfrak{p}}/\mathfrak{p})$ is cyclic of order ℓ^f for some $f \leq e-1$, say. Hence the condition $\zeta_{\ell^e} \in K_{\mathfrak{p}}$ ensures that $N_{\tilde{\mathfrak{p}}}/K_{\mathfrak{p}}$ is a Kummer extension, generated by an ℓ^f -th root of a prime element of $K_{\mathfrak{p}}$. As $\zeta_{\ell^{f+1}} \in K_{\mathfrak{p}}$ the ℓ^{f+1} -th roots of this prime element generate a cyclic Galois extension of $K_{\mathfrak{p}}$ with group $\tilde{G}_{\mathfrak{p}} = Z_{\ell^{f+1}}$ in the non-split case, and there exists an epimorphism $\tilde{\varphi}_{\mathfrak{p}} : \Gamma_{K_{\mathfrak{p}}} \rightarrow \tilde{G}_{\mathfrak{p}}$ with $\kappa_{\mathfrak{p}} \circ \tilde{\varphi}_{\mathfrak{p}} = \varphi_{\mathfrak{p}}$.

Thus all local embedding problems $\mathcal{E}(\varphi_{\mathfrak{p}}, \kappa_{\mathfrak{p}})$ are solvable and hence by Proposition 10.1 also the global embedding problem $\mathcal{E}(\varphi, \kappa)$. In the case $\zeta_{\ell} \in K$ we may admit one exception by the Remark following Corollary 10.2. \square

In generalization of conditions (0)–(2) in Proposition 10.3 we call a finite Galois extension N/K an *n-Scholz extension relative to $\mathbb{S}_1 \subset \mathbb{P}(K)$* if all $\mathfrak{p} \in \text{Ram}(N/K) \setminus \mathbb{S}_1$ and $\tilde{\mathfrak{p}} \in \mathbb{P}(N)$ with $\tilde{\mathfrak{p}}|\mathfrak{p}$ satisfy

$$(0) \mathfrak{p} \notin \mathbb{S}_0, \quad (1) \zeta_n \in K_{\mathfrak{p}}, \quad (2) D(\tilde{\mathfrak{p}}/\mathfrak{p}) = I(\tilde{\mathfrak{p}}/\mathfrak{p}). \quad (10.3)$$

(In the general definition of relative Scholz extensions it is usually assumed that moreover $\mathbb{S}_0 \subseteq \mathbb{S}_1$, so that condition (0) becomes superfluous.)

Furthermore, we call an embedding problem $\mathcal{E}(\varphi, \kappa)$ over K an *n-Scholz embedding problem (relative to \mathbb{S}_1)* if the fixed field N of $\ker(\varphi)$ is an *n-Scholz extension of K (relative to \mathbb{S}_1)*, and a solution $\tilde{\varphi}$ of $\mathcal{E}(\varphi, \kappa)$ is called an *n-Scholz solution (relative to \mathbb{S}_1)* if the solution field \tilde{N} of $\tilde{\varphi}$ is a *n-Scholz extension of K (relative to \mathbb{S}_1)*.

Corollary 10.4. *Let K be a global field and $\mathbb{S}_1 \subset \mathbb{P}(K)$ either empty or consisting of a prime divisor which is nonsplit in $K(\zeta_{\ell})/K$. Then every finite central ℓ^m -Scholz embedding problem relative to \mathbb{S}_1 with kernel Z_{ℓ} and $\exp_{\ell}(|G|) < \ell^m$ possesses a proper solution over K .*

Proof. If $\mathcal{E}(\varphi, \kappa)$ is split, then it possesses a proper solution by Theorem 2.4. In the non-split case it at least has a solution by Proposition 10.3 and using the injectivity of the restriction $\rho_{K(\zeta_{\ell})}^K$ in (10.1). But by Proposition 1.8 this is a proper solution, since in this case we have a Frattini embedding problem. \square

For an inductive proof it remains to determine when Scholz embedding problems even possess (proper) Scholz solutions.

10.2 Scholz Embedding Problems

A Galois extension N/K over a global field K with ℓ -Galois group G can be obtained for example by tensoring a Galois extension N_0/K_0 with $\text{Gal}(N_0/K_0) \cong G$ over the prime field $K_0 = \mathbb{Q}$ respectively $K_0 = \mathbb{F}_p(t)$, $p \neq \ell$, with K over K_0 , at least in the case that K/K_0 and N_0/K_0 are linearly disjoint. The latter can be guaranteed by requiring that $\text{Ram}(K/K_0) \cap \text{Ram}(N_0/K_0) = \emptyset$. Thus we will now construct Galois extensions with ℓ -Galois groups over K_0 whose socle is ramified outside a given finite set of prime divisors of K_0 . Here the *socle of an ℓ -Galois extension N/K* with group G is the maximal elementary abelian intermediate field, i.e., the fixed field of $\Phi(G) = G^\ell G'$.

Lemma 10.5. *Let $K = \mathbb{Q}$ respectively $K = \mathbb{F}_p(t)$, $\ell \neq p$ a prime with $\zeta_\ell \notin K$, $\mathbb{S}_1 := \{(\ell)\}$ in the case $K = \mathbb{Q}$, resp. $\mathbb{S}_1 = \emptyset$ otherwise, and $\mathbb{S} \subset \text{IP}(K)$ a finite subset containing \mathbb{S}_0 . Then we have:*

- (a) *Every split central (geometric) ℓ^m -Scholz embedding problem $\mathcal{E}(\varphi, \kappa)$ over K relative to \mathbb{S}_1 with kernel Z_ℓ and $\exp_\ell(\varphi(\Gamma_K)) < \ell^m$ possesses a proper (geometric) ℓ^m -Scholz solution relative to \mathbb{S}_1 .*
- (b) *If $\varphi(\Gamma_K)$ is an ℓ -group and the socle of N/K of the fixed field N of $\ker(\varphi)$ is ramified outside of \mathbb{S} only, then $\mathcal{E}(\varphi, \kappa)$ possesses also such a solution. Moreover, its solution field \tilde{N} satisfies*

$$\text{Ram}(\tilde{N}/K) \subseteq \text{Ram}(N/K) \cup \{\mathfrak{q}\} \quad \text{for some } \mathfrak{q} \in \text{IP}(K) \setminus \mathbb{S}. \quad (10.4)$$

Proof. For $\mathfrak{r} \in \text{Ram}(N/K)$ let r denote the associated prime number in the case of \mathbb{Q} respectively the associated monic prime polynomial $r \in \mathbb{F}_p[t]$ with numerator divisor \mathfrak{r} in the case of $\mathbb{F}_p(t)$ (with $r = 1/t$ in the case $\mathfrak{r} = \mathfrak{p}_\infty$). Further let N^* denote the field generated over N by a primitive ℓ^m -th root of unity ζ_{ℓ^m} and the roots $\sqrt[\ell^m]{r}$ for $\mathfrak{r} \in \text{Ram}(N/K)$. By the Dirichlet Density Theorem (see for example Narkiewicz (1990), Cor. 7 to Prop. 7.9) there exists a prime ideal $\mathfrak{q} \in \text{IP}(K) \setminus \mathbb{S}$ with associated prime element q which splits completely in N^*/K . In particular it satisfies $\mathcal{N}(\mathfrak{q}) \equiv 1 \pmod{\ell^m}$.

In the case $K = \mathbb{Q}$ let $K_+^{(q)}$ denote the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_q)$ of degree $(q-1)/2$. Correspondingly in the case of $K = \mathbb{F}_p(t)$ let $K_+^{(q)}$ denote the maximal subfield of the cyclotomic extension $K^{(q)}/K$ in which the denominator divisor \mathfrak{p}_∞ of (t) splits completely. This field coincides with the ray class field modulo \mathfrak{q} and has degree $(p^d - 1)/(p - 1)$ over K , with $d = \deg(\mathfrak{q})$ (see for example Goss (1996), Ch. 7.5). Then in both cases $K_+^{(q)}/K$ is unramified outside \mathfrak{q} .

Since $\ell \neq 2$ in the case $K = \mathbb{Q}$ respectively $\ell \nmid (p-1)$ in the case $K = \mathbb{F}_p(t)$ the extension $K_+^{(q)}/K$ contains a cyclic subfield L of degree ℓ . The divisor \mathfrak{q} is completely split in $K(\sqrt[\ell]{r})/K$ for $\mathfrak{r} \in \text{Ram}(N/K)$, so there exists an $x \in K$ with $x^\ell \equiv r \pmod{\mathfrak{q}}$. By the decomposition law \mathfrak{r} is also completely split in L/K .

The composite $\tilde{N} := LN$ thus has the Galois group $\text{Gal}(\tilde{N}/K) = G \times Z_\ell$ with $\text{Ram}(\tilde{N}/K) = \text{Ram}(N/K) \cup \{\mathfrak{q}\}$. Since we have $\mathfrak{q} \notin \$$ and by the decomposition properties of \mathfrak{q} and $\mathfrak{r} \in \text{Ram}(N/K)$ in N/K respectively L/K the extension \tilde{N}/K is ℓ^m -Scholz relative to $\$_1$. Obviously φ may now be extended via the canonical epimorphism $\lambda : \Gamma_K \rightarrow \text{Gal}(L/K) \cong \ker(\kappa)$ to an ℓ^m -Scholz solution (relative to $\$_1$)

$$\tilde{\varphi} = \varphi \times \lambda : \Gamma_K \longrightarrow G \times Z_\ell = \tilde{G} \quad \text{with } \kappa \circ \tilde{\varphi} = \varphi.$$

In the case of positive characteristic L/K is a geometric field extension. Thus \tilde{N}/K is also a geometric field extension. This proves (a).

If N/K is an ℓ -extension with socle S , then the socle \tilde{S} of the solution field \tilde{N} of $\tilde{\varphi}$ satisfies

$$\text{Ram}(\tilde{S}/K) \subseteq \text{Ram}(S/K) \cup \{\mathfrak{q}\}.$$

In particular the socle of \tilde{N}/K is unramified in $\$$, which proves (b). \square

Remark. If in Lemma 10.5 the denominator divisor \mathfrak{p}_∞ of (t) splits completely in N/K , then it also splits completely in \tilde{N}/K .

Lemma 10.6. *Let K and $\$_1$ be as in Lemma 10.5. Then every (geometric) non-split central ℓ^m -Scholz embedding problem $\mathcal{E}(\varphi, \kappa)$ over K relative to $\$_1$ with kernel Z_ℓ and $\exp_\ell(\varphi(\Gamma_K)) < \ell^m$ possesses a proper (geometric) solution where the solution field \tilde{N} satisfies*

$$\text{Ram}(\tilde{N}/K) \subseteq \text{Ram}(N/K) \cup \$_1. \quad (10.5)$$

Proof. The existence of a proper solution $\tilde{\varphi}$ with solution field \tilde{N} already follows from Corollary 10.4. This will now be modified so that also (10.5) holds.

For this let $\mathfrak{q} \in \text{Ram}(\tilde{N}/K) \setminus \text{Ram}(N/K)$ with $\mathfrak{q} \notin \$_1$, i.e., $\mathfrak{q} \neq (\ell)$, and $\mathfrak{Q} \in \mathbb{P}(N)$ a prime divisor of \mathfrak{q} . Then there exists a $\tilde{\mathfrak{Q}} \in \mathbb{P}(\tilde{N})$ with $\tilde{\mathfrak{Q}}^\ell = \mathfrak{Q}$. Since the inertia group $I(\tilde{\mathfrak{Q}}/\mathfrak{q})$ is a subgroup of the multiplicative group of the residue field we have $\mathcal{N}(\tilde{\mathfrak{Q}}) = \mathcal{N}(\mathfrak{Q}) \equiv 1 \pmod{\ell}$. On the other hand we have $\mathcal{N}(\mathfrak{Q}) = \mathcal{N}(\mathfrak{q})^{l^k}$ with $k \in \mathbb{N}$, which implies $\mathcal{N}(\mathfrak{q}) \equiv 1 \pmod{\ell}$. Thus as in the proof of Lemma 10.5 the field $K_+^{(q)}$ possesses a subfield L of degree ℓ linearly disjoint to N/K which is unramified outside \mathfrak{q} . The composite $L\tilde{N}/K$ thus has Galois group $\text{Gal}(L\tilde{N}/K) \cong \tilde{G} \times Z_\ell$, and the inertia group I of the extensions $\tilde{\mathfrak{Q}} \in \mathbb{P}(L\tilde{N})$ of \mathfrak{q} lies in a central subgroup of type $Z_\ell \times Z_\ell$. Since \mathfrak{q} is tamely ramified, I is cyclic. The fixed field \tilde{N}' of I then has the Galois group

$$\text{Gal}(\tilde{N}'/K) \cong (\tilde{G} \times Z_\ell)/I \cong \tilde{G},$$

and we have $\text{Ram}(\tilde{N}'/K) = \text{Ram}(\tilde{N}/K) \setminus \{\mathfrak{q}\}$.

Now as in Lemma 10.5 the given solution $\tilde{\varphi}$ of $\mathcal{E}(\varphi, \kappa)$ can be extended via the canonical epimorphism $\lambda : \Gamma_K \rightarrow \text{Gal}(L/K)$ first to

$$\tilde{\varphi}' = \tilde{\varphi} \times \lambda : \Gamma_K \rightarrow \tilde{G} \times Z_\ell = \text{Gal}(L\tilde{N}/K).$$

Then by composing with the canonical map $\pi_{L\tilde{N}/\tilde{N}'} : \text{Gal}(L\tilde{N}/K) \rightarrow \text{Gal}(\tilde{N}'/K)$ we obtain an epimorphism $\tilde{\varphi}'$ onto $\text{Gal}(\tilde{N}'/K) \cong \tilde{G}$ with $\tilde{\varphi}' \circ \kappa = \varphi$. Therefore, $\tilde{\varphi}'$ defines a proper solution of $\mathcal{E}(\varphi, \kappa)$ with solution field \tilde{N}' . Since in the case of positive characteristic $\mathcal{E}(\varphi, \kappa)$ is a geometric Frattini embedding problem, by Proposition 1.8 also $\tilde{\varphi}'$ is a geometric solution. The assertion hence follows by induction. \square

Remark. By using a theorem of Tate on the solvability of global embedding problems with local prescription (see for example Serre (1992), Prop. 2.1.7) the exceptional position of ℓ in Lemma 10.6 can be removed.

Lemma 10.7. *Let K, \mathbb{S}_1 and \mathbb{S} be as in Lemma 10.5. Then every (geometric) non-split central ℓ^m -Scholz embedding problem $\mathcal{E}(\varphi, \kappa)$ over K relative to \mathbb{S}_1 with kernel Z_ℓ and $|\varphi(\Gamma_K)| = \ell^n < \ell^m$ possesses a proper (geometric) ℓ^m -Scholz solution relative to \mathbb{S}_1 , where the solution field \tilde{N} satisfies*

$$\text{Ram}(\tilde{N}/K) \subseteq \text{Ram}(N/K) \cup \mathbb{S}_1 \cup \{\mathfrak{q}\} \quad \text{for some } \mathfrak{q} \in \text{IP}(K) \setminus \mathbb{S}. \quad (10.6)$$

Proof. By Lemma 10.6 the embedding problem $\mathcal{E}(\varphi, \kappa)$ has a proper solution $\tilde{\varphi}$ whose solution field \tilde{N} satisfies (10.5). We are going to modify this solution to obtain a Scholz solution, such that at most one additional ramified place appears.

For $\mathfrak{r} \in \mathbf{T} := \text{Ram}(\tilde{N}/K) \setminus \mathbb{S}_1$ with associated prime element r fix prime divisors $\mathfrak{R} \in \text{IP}(N)$ and $\tilde{\mathfrak{R}} \in \text{IP}(\tilde{N})$. Since $I(\mathfrak{R}/\mathfrak{r}) = D(\mathfrak{R}/\mathfrak{r})$ and $\ker(\kappa) \cong Z_\ell$ the decomposition group $D(\tilde{\mathfrak{R}}/\mathfrak{r})$ is contained in the preimage \tilde{I} of type $Z_\ell \cdot I(\mathfrak{R}/\mathfrak{r})$ in \tilde{G} . If \tilde{I} is cyclic, then $\tilde{I} = I(\tilde{\mathfrak{R}}/\mathfrak{r}) = D(\tilde{\mathfrak{R}}/\mathfrak{r})$. In the non-cyclic case the above shows that either also $D(\tilde{\mathfrak{R}}/\mathfrak{r}) = I(\tilde{\mathfrak{R}}/\mathfrak{r})$ or $D(\tilde{\mathfrak{R}}/\mathfrak{r}) = I(\tilde{\mathfrak{R}}/\mathfrak{r}) \times Z_\ell$. Now let

$$\begin{aligned} \mathbf{T}_0 &:= \{\mathfrak{r} \in \mathbf{T} \mid D(\tilde{\mathfrak{R}}/\mathfrak{r}) = I(\tilde{\mathfrak{R}}/\mathfrak{r})\}, \\ \mathbf{T}_1 &:= \mathbf{T} \setminus \mathbf{T}_0 = \{\mathfrak{r}_1, \dots, \mathfrak{r}_k\}, \end{aligned}$$

and r_i the prime elements associated to \mathfrak{r}_i . For $\mathfrak{r}_i \in \mathbf{T}_1$ let $\sigma_i := \left(\frac{\tilde{N}/N}{\mathfrak{R}_i} \right) \in \ker(\varphi) \cong Z_\ell$ be the Artin symbol of \mathfrak{R}_i (see for example Narkiewicz (1990), Ch. 7, §3). The σ_i are independent of the choice of the extension $\mathfrak{R}_i/\mathfrak{r}_i$ because $\ker(\varphi) \leq \mathscr{Z}(\tilde{G})$. Since $\tilde{\mathfrak{R}}_1/\mathfrak{R}_1$ is inert, $\langle \sigma_1 \rangle = \text{Gal}(\tilde{N}/N)$, so there exists $e_i \in \mathbb{N}$ with $\sigma_i = \sigma_1^{e_i}$.

The field $K(\zeta_{\ell^m})$ is the composite of $K(\zeta_\ell)/K$ with a cyclic field K'/K of degree ℓ^{m-1} . Thus $\tilde{N}K'/K$ is an ℓ -extension and $N' := K(\zeta_\ell \cup \{\sqrt[\ell]{r} \mid \mathfrak{r} \in \mathbf{T}\})$ is a Kummer extension with group Z_ℓ^s over $K(\zeta_\ell)$ for some $s \in \mathbb{N}$. As $\zeta_\ell \notin K$ the group $\text{Gal}(N'/K) \cong Z_\ell^s \rtimes Z_f$ with $1 \neq f | (\ell - 1)$ has no quotient of order ℓ . In particular, $\tilde{N}K'$ and N' are linearly disjoint over K .

By the Dirichlet Density Theorem there exists a $\mathfrak{q} \in \text{IP}(K) \setminus \mathbb{S}$ with associated prime element q which splits completely in $\tilde{N}(\zeta_{\ell^m} \cup \{\sqrt[\ell]{r} \mid \mathfrak{r} \in \mathbf{T}_0\})/K$ and in

$K(\zeta_\ell, \sqrt[\ell]{r_i/r_1^{e_i}})/K$ for $i = 2, \dots, k$ and which is inert in $K(\zeta_\ell, \sqrt[\ell]{r_1})/K(\zeta_\ell)$. As $\mathcal{N}(\mathfrak{q}) \equiv 1 \pmod{\ell}$ the field $K_+^{(q)}$ as in the proof of Lemma 10.5 possesses a cyclic subfield L of degree ℓ over K which is unramified outside of \mathfrak{q} and hence is linearly disjoint with \tilde{N}/K . Since the prime divisor \mathfrak{q} splits completely in $K(\sqrt[\ell]{r})/K$ for $\mathfrak{r} \in \mathbf{T}_0$ there exists an $x \in K$ with $x^\ell \equiv r \pmod{\mathfrak{q}}$. By the decomposition law \mathfrak{r} splits completely in L/K , so the Artin symbol evaluates to $(\frac{L/K}{\mathfrak{r}}) = 1$. Correspondingly \mathfrak{r}_1 is inert in L/K with Artin symbol $\rho_1 := (\frac{L/K}{\mathfrak{r}_1}) \neq 1$. Since \mathfrak{q} splits completely in $K(\zeta_\ell, \sqrt[\ell]{r_i/r_1^{e_i}})/K$ there exist $x_i \in K$ with

$$r_1^{e_i} x_i^\ell \equiv r_i \pmod{\mathfrak{q}} \quad \text{for } i = 2, \dots, k,$$

which implies $\rho_i := (\frac{L/K}{\mathfrak{r}_i}) = \rho_1^{e_i}$.

Now let $D \cong Z_\ell$ be the decomposition group in $\text{Gal}(L\tilde{N}/N) \cong Z_\ell \times Z_\ell$ of an extension of \mathfrak{R}_1 and $\tilde{N}' := (L\tilde{N})^D$. Then the extensions of prime divisors $\mathfrak{r} \in \mathbf{T}_0$ split completely in $L\tilde{N}/N$ and hence a fortiori in \tilde{N}'/N , in particular \mathfrak{r} satisfies the Scholz condition (1). By construction of \tilde{N}' the same holds for \mathfrak{r}_1 . For the remaining $\mathfrak{r}_i \in \mathbf{T}_1$ the projections of $(\frac{L\tilde{N}/N}{\mathfrak{R}_i})$ onto $\text{Gal}(LN/N) \cong \text{Gal}(L/K)$ respectively $\text{Gal}(\tilde{N}/N)$ are given by the pairs $(\rho_i, \sigma_i) = (\rho_1^{e_i}, \sigma_1^{e_i})$. But the automorphism of $L\tilde{N}/N$ belonging to (ρ_1, σ_1) is trivial on \tilde{N}' , so the extensions of the \mathfrak{r}_i for $i = 2, \dots, k$ split in \tilde{N}'/N and thus satisfy the Scholz condition (1). Finally it remains to state that the remaining ramification divisor \mathfrak{q} satisfies the Scholz conditions (0), (1) and (2) since $\mathfrak{q} \notin \mathbb{S}$, $\mathcal{N}(\mathfrak{q}) \equiv 1 \pmod{\ell^m}$ and \mathfrak{q} is unramified in \tilde{N}/K .

As in the proof of Lemma 10.6 there now exists an epimorphism $\tilde{\varphi}' : \Gamma_K \rightarrow \text{Gal}(\tilde{N}'/K)$ which on N coincides with $\tilde{\varphi}$ and hence with φ . This gives a proper ℓ^m -Scholz solution of $\mathcal{E}(\varphi, \kappa)$ with respect to \mathbb{S}_1 , unramified outside of $\text{Ram}(\tilde{N}/K) \cup \{\mathfrak{q}\}$. If $\mathcal{E}(\varphi, \kappa)$ is geometric, then this solution is geometric as well, being the solution to a Frattini embedding problem (by Proposition 1.8). \square

Remark. If in Lemma 10.6 the denominator divisor \mathfrak{p}_∞ of (t) splits completely in N/K , then by construction of L this also holds in \tilde{N}/K .

In conclusion we obtain (see also Serre (1992), Thm. 2.1.3):

Theorem 10.8. *Let $K = \mathbb{Q}$ respectively $K = \mathbb{F}_p(t)$ with $p \neq \ell$ and $\zeta_\ell \notin K$, $\mathbb{S}_1 = \{(\ell)\}$ for $K = \mathbb{Q}$ resp. $\mathbb{S}_1 = \emptyset$ otherwise, and \mathbb{S} a finite subset of $\mathbb{P}(K)$ containing \mathbb{S}_0 . Then we have:*

(a) *Every central (geometric) ℓ^m -Scholz embedding problem $\mathcal{E}(\varphi, \kappa)$ relative to \mathbb{S}_1 over K with $|\varphi(\Gamma_K)| = \ell^n < \ell^m$ with kernel Z_ℓ possesses a proper (geometric) ℓ^m -Scholz solution relative to \mathbb{S}_1 , with a solution field \tilde{N} satisfying*

$$\text{Ram}(\tilde{N}/K) \subseteq \text{Ram}(N/K) \cup \mathbb{S}_1 \cup \{\mathfrak{q}\} \quad \text{for some } \mathfrak{q} \in \mathbb{P}(K) \setminus \mathbb{S}.$$

(b) *If the socle of N/K is ramified outside of \mathbb{S} , then $\mathcal{E}(\varphi, \kappa)$ also possesses a solution with this additional property.*

Proof. Assertion (a) follows from Lemma 10.5(a) and Lemma 10.7. In the case of a split embedding problem the second part is a consequence of Lemma 10.5(b), and in the non-split case it follows from the fact that in a Frattini embedding problem the socle remains the same. Indeed, otherwise \tilde{N}'/K would contain a Z_ℓ -extension \tilde{L}/K with $\tilde{L} \not\leq N$, in contradiction to the fact that $\text{Gal}(\tilde{N}'/N)$ is contained in the Frattini subgroup $\Phi(\tilde{G})$ of \tilde{G} . \square

10.3 The Theorem of Scholz and Reichardt

With the preparations in the previous sections it is now easy to prove the general version of the Theorem of Scholz-Reichardt for global fields (compare Scholz (1937), Reichardt (1937) for number fields and Rzedowski-Calderon (1989), Geyer and Jarden (1998) for function fields).

Theorem 10.9. *Let K be a global field of characteristic $p \geq 0$. Then every finite nilpotent group G with $2 \nmid |G|$ in the case $p = 0$ resp. $\gcd(|G|, p - 1) = 1$ in the case $p > 0$ occurs as Galois group over K .*

Proof. A nilpotent group is the direct product of its ℓ -Sylow subgroups, so by Theorem 1.6(a) it suffices to realize finite ℓ -groups for $\ell \mid |G|$ as Galois groups over K . Moreover, by Theorem 8.3(b) we may assume that $\ell \neq p$.

Now let $K_0 = \mathbb{Q}$ respectively $K_0 = \text{IF}_p(t)$ for some $t \in K$ and $\$$ be the set of prime divisors of K_0 ramified in K/K_0 . By our assumptions on ℓ we have $\zeta_\ell \notin K_0$. By induction it then follows from Theorem 10.8 that for every finite ℓ -group G_ℓ there exists a Galois extension N_ℓ/K_0 with Galois group G_ℓ whose socle $S(N_\ell)$ is unramified outside $\$$, and which is geometric in the function field case. Now, $S(K \cap N_\ell) \leq K \cap S(N_\ell)$ so the socle $S(K \cap N_\ell)$ is unramified over K_0 . This implies that $S(K \cap N_\ell) = K_0$, and hence also $K \cap N_\ell = K_0$ since N_ℓ/K is an ℓ -extension. So K and N_ℓ are linearly disjoint over K_0 , and the composite $N_\ell K/K$ has Galois group isomorphic to G_ℓ (and is geometric in the function field case). \square

In the case of global fields of characteristic 0 Šafarevič (1954a, 1989) was able to remove the assumption $2 \nmid |G|$ in Theorem 10.9 in a complicated induction process by stepwise shrinking the embedding obstructions. With a generalization of the method of proof he then succeeded to solve split embedding problems with nilpotent kernel and thus realize all finite solvable groups as Galois groups over finite number fields (see Šafarevič (1954b,c,d, 1958)). Revised proofs can also be found in the monographs Ishkhanov, Lure and Faddeev (1997) and Neukirch, Schmidt and Wingberg (2000).

In contrast to this it is possible in the case of global fields of positive characteristic p to remove the assumption $\gcd(|G|, p - 1) = 1$ by an elementary method of Madan, Rzedowski-Calderon and Villa-Salvador (1996) which proceeds by variation of the base field.

10.4 Nilpotent Galois Groups over Global Function Fields

In this section let k be a finite field with p^r elements, $K := k(t)$ and $\ell \in \mathbb{P}$ with $\text{ord}_\ell(p^r - 1) = e \geq 1$. Furthermore, let G be an ℓ -group of order ℓ^n with Frattini subgroup $\Phi(G) = G'G^\ell$ of order ℓ^m and Frattini factor group $G/\Phi(G) \cong Z_\ell^s$ with $s = n - m$. The ground field K will now first be replaced by $F := k(u)$ with $u = t^{\ell^m}$. After extension of constants with $\tilde{k} := k(\zeta_{\ell^m})$ the extension of $\tilde{K} := \tilde{k}K$ over $\tilde{F} := \tilde{k}F$ is cyclic of order ℓ^m and \tilde{K}/F is Galois with group

$$\text{Gal}(\tilde{K}/F) \cong Z_{\ell^m} \rtimes Z_{\ell^f} \quad \text{with } f < m.$$

As in the previous section we denote by $F^{(q)}$ the cyclotomic extension for a prime polynomial $q \in k[u]$ with numerator divisor $\mathfrak{q} \in \mathbb{P}(F/k)$. With these notations we have:

Lemma 10.10. *Let \mathbb{S} be a finite subset of $\mathbb{P}(F/k)$. Then there exist infinitely many families $\mathbf{T} := \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\}$ of pairwise distinct prime divisors $\mathfrak{q}_i \in \mathbb{P}(F/k) \setminus \mathbb{S}$ with*

- (1) $\deg(\mathfrak{q}_i) = d_i$ with $d_1 < d_2 \dots < d_s$,
- (2) $\ell^{n+e} | (p^{rd_i} - 1)$ respectively $\zeta_{\ell^{n+e}} \in F_{\mathfrak{q}_i}$ for $1 \leq i \leq s$,
- (3) \mathfrak{q}_i is inert in K/F for $1 \leq i \leq s$,
- (4) \mathfrak{q}_i splits completely in F_{i-1}^*/F for $1 < i \leq s$, where F_{i-1}^* is the composite of the $F^{(q_j)}(\sqrt[p]{\mathfrak{q}_j})$ for $1 \leq j \leq i-1$.

Proof. We first note that \tilde{K} and $\tilde{F}_{i-1}^* := F_{i-1}^*(\zeta_{\ell^{n+e}})$ are Galois over F and linearly disjoint over \tilde{F} . Thus by the Dirichlet Density Theorem there exist infinitely many $\mathfrak{q}_i \in \mathbb{P}(F/k)$ which split completely in \tilde{F}_{i-1}^*/F and stay inert in \tilde{K}/\tilde{F} . For these we obtain (2) and (4). Now let $\mathfrak{q} \in \mathbb{P}(F/k)$ be a prime divisor whose extensions $\tilde{\mathfrak{q}} \in \mathbb{P}(\tilde{K}/\tilde{k})$ are inert in \tilde{K}/\tilde{F} . Then the decomposition group in $\text{Gal}(\tilde{K}/F)$ satisfies $D(\tilde{\mathfrak{q}}/\mathfrak{q}) = \text{Gal}(\tilde{K}/\tilde{F})$ because $f < m$, so (3) follows. It is now easy to obtain from these infinitely many $\mathfrak{q}_i \in \mathbb{P}(F/k)$ infinitely many families $\mathbf{T} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\}$ with pairwise distinct $\mathfrak{q}_i \in \mathbb{P}(F/k) \setminus \mathbb{S}$. \square

After these preparations we come to the main point of the proof:

Proposition 10.11. *Let k be a finite field of characteristic p with $\zeta_\ell \in k$, $K := k(t)$ and G a finite ℓ -group of rank s . Then for each \mathbf{T} as in Lemma 10.10 there exists a geometric Galois extension N/K with*

$$\text{Gal}(N/K) \cong G \quad \text{and} \quad \text{Ram}(N/K) = \{\tilde{\mathfrak{q}}_1, \dots, \tilde{\mathfrak{q}}_s\}, \quad (10.7)$$

where $\tilde{\mathfrak{q}}_i \in \mathbb{P}(K/k)$ are the uniquely determined extensions of $\mathfrak{q}_i \in \mathbf{T}$.

Proof. For the proof we have to perform the three steps in Lemmata 10.5–10.7 in suitably modified form. First we construct an ℓ^{n+e} -Scholz-extension F_0/F with group $\text{Gal}(F_0/F) \cong G/\Phi(G)$. For $\mathfrak{q}_i \in \mathbf{T}$ with associated prime element q_i let $F_+^{(q_i)}/F$ denote the corresponding ray class field modulo \mathfrak{q}_i . Since $[F_+^{(q_i)} : F] =$

$(p^{rd_i} - 1)/(p^r - 1)$ the extension $F_+^{(q_i)}/F$ possesses a cyclic intermediate field L_i/F of degree ℓ . The composite F_0 of the fields L_1, \dots, L_s is then a geometric Galois extension over F with

$$\mathrm{Gal}(F_0/F) \cong Z_\ell^s \cong G/\Phi(G).$$

By the choice of \mathbf{T} each \mathfrak{q}_i splits completely in L_j/F for $j < i$ and ramifies in L_i/F . For $j > i$ the divisor \mathfrak{q}_j splits completely in $L_i(\sqrt[\ell]{\mathfrak{q}_i})/F$, hence by the proof of Lemma 10.5 it follows that \mathfrak{q}_i splits completely in L_j/F . Thus F_0/F is a geometric ℓ^{n+e} -Scholz extension.

The group G possesses a lower central series

$$G \triangleright G_0 = \Phi(G) \triangleright G_1 \triangleright \dots \triangleright G_m = 1$$

with $G_{i-1}/G_i \cong Z_\ell$ for $1 \leq i \leq m$. By Proposition 10.3 the central Frattini embedding problem

$$1 \longrightarrow Z_\ell = G_0/G_1 \longrightarrow G/G_1 \longrightarrow G/G_0 = \mathrm{Gal}(F/F_0) \longrightarrow 1$$

with kernel Z_ℓ has a proper geometric solution with solution field \tilde{F}_0 , say. As in the proof of Lemma 10.6 any divisor $\mathfrak{q} \in \mathrm{Ram}(\tilde{F}_0/F) \setminus \mathbf{T}$ different from \mathfrak{p}_∞ satisfies $\mathcal{N}(\mathfrak{q}) \equiv 1 \pmod{\ell}$. Hence the full cyclotomic extension $F^{(\mathfrak{q})}/F$ (the ray class field modulo $\mathfrak{q}\mathfrak{p}_\infty$) possesses a cyclic intermediate field L of degree ℓ unramified outside \mathfrak{q} and \mathfrak{p}_∞ . But L/F and \tilde{F}_0/F are linearly disjoint, so $\mathrm{Gal}(L\tilde{F}_0/F) \cong G_0 \times Z_\ell$. Now let F_1 be the inertia field of an extension $\mathfrak{Q} \in \mathrm{IP}(L\tilde{F}_0/F)$ of \mathfrak{q} . Then as in the proof of Lemma 10.6 we obtain $\mathrm{Gal}(F_1/F) \cong G/G_1$ and $\mathrm{Ram}(F_1/F) \setminus \{\mathfrak{p}_\infty\} \subseteq \mathrm{Ram}(\tilde{F}_0/F) \setminus \{\mathfrak{q}\}$. After finitely many induction steps we thus arrive at a Galois extension F_1/F with

$$\mathrm{Gal}(F_1/F) \cong G/G_1 \quad \text{and} \quad \mathrm{Ram}(F_1/F) \subseteq \mathbf{T} \cup \{\mathfrak{p}_\infty\}.$$

Now there might still exist $\mathfrak{q}_i \in \mathbf{T}$ inert in F_1/F_0 , or \mathfrak{p}_∞ might ramify. These problems can be solved in the function field case by a translation technique. For this let $v := \sqrt[\ell]{u} = t^{\ell^{m-1}}$. Then $F(v)$ and F_1 are linearly disjoint over F and hence we have

$$\mathrm{Gal}(F_1(v)/F) \cong G/G_1 \times Z_\ell.$$

By construction $\mathfrak{q}_i \in \mathbf{T}$ is inert in $F(v)/F$ and satisfies the Scholz conditions (10.3) in F_0/F . Thus the extensions $\mathfrak{Q}_i \in \mathrm{IP}(F_0/k)$ of \mathfrak{q}_i are inert in $F_0(v)/F_0$. Since in the case of global fields the decomposition groups modulo inertia groups are cyclic, the \mathfrak{Q}_i have residue degree 1 in $F_1(v)/F_0(v)$. Hence the uniquely determined extensions $\tilde{\mathfrak{q}}_i \in \mathrm{IP}(F(v)/k)$ of \mathfrak{q}_i satisfy the Scholz conditions (10.3) for $F_1(v)/F(v)$.

Finally, \mathfrak{p}_∞ is ramified in $F(v)/F$ but unramified in F_0/F . Thus the extensions of \mathfrak{p}_∞ are ramified in $F_0(v)/F_0$ and unramified in $F_0(v)/F(v)$. Since the inertia groups are cyclic, these extensions are also unramified in $F_1(v)/F_0(v)$. Thus the unique extension $\tilde{\mathfrak{p}}_\infty \in \mathrm{IP}(F(v)/k)$ of \mathfrak{p}_∞ is unramified in $F_1(v)/F(v)$. This proves that $F_1(v)/F(v)$ is an ℓ^{n+e} -Scholz extension with group G/G_1 .

After m such induction steps we finally obtain a geometric Galois extension F_m/K with Galois group $G/G_m \cong G$. \square

From Theorem 10.9 and Proposition 10.11 we now obtain:

Theorem 10.12 (Madan et al. (1996)). *Over a global field K/k of positive characteristic every finite nilpotent group occurs as Galois group of a geometric Galois extension.*

Proof. We decompose the nilpotent group G into the direct product of its ℓ -Sylow subgroups G_ℓ . By Theorem 10.9 for each $\ell \nmid |k^\times|$ there exists a geometric Galois extension N_ℓ/K with $\text{Gal}(N_\ell/K) \cong G_\ell$. For ℓ dividing $|k^\times|$ we choose a rational subfield $k(t)$ of K and construct by Proposition 10.11 a Galois extension $N'_\ell/k(t)$ with $\text{Gal}(N'_\ell/k(t)) \cong G_\ell$ and unramified in $\mathfrak{S} := \text{Ram}(K/k(t))$. Since then N'_ℓ and K are linearly disjoint over $k(t)$, the composite $N_\ell := N'_\ell K$ is a geometric Galois extension of K with group $\text{Gal}(N_\ell/K) \cong G_\ell$. \square

Remark. In Madan, Rzedowski-Calderon and Villa-Salvador (1996) the following extension of Theorem 10.12 is shown: If s is the maximal rank of the ℓ -Sylow subgroups G_ℓ of the nilpotent group G then there exists a geometric Galois extension N/K with $\text{Gal}(N/K) \cong G$ and $|\text{Ram}(N/K)| \leq s$. This is obtained by a generalization of Proposition 10.11 to the case $\zeta_\ell \notin k$ together with the construction of an element $t \in K$ and a geometric Galois extension $N/k(t)$ with $\text{Gal}(N/k(t)) \cong G$, for which all $\mathfrak{q} \in \text{Ram}(N/k(t))$ are inert in $K/k(t)$.

As an immediate consequence of Theorem 10.12 we obtain:

Corollary 10.13. *Over a finite field every finite nilpotent group possesses a G -realization.*

The theorem of Šafarevič implies the corresponding result for all finite solvable groups.

V Additive Polynomials

In this chapter we construct polynomials with prescribed Galois group in positive characteristic. The new underlying phenomenon here is the fact that all finite Galois extensions can be generated by finite vector spaces of roots of suitable polynomials. Polynomials having such a vector space of zeroes over \mathbb{F}_q are called q -additive. Their Galois groups possess in a natural way a matrix representation into a general linear group over \mathbb{F}_q . The Galois theory of q -additive polynomials can thus be called *modular Galois theory*.

Finite linear groups also occur as Galois groups in the theory of difference modules with respect to the Frobenius operator, which will here be called Frobenius modules for short. This connection provides a non-trivial upper bound for the Galois group of a finite Galois extension. Good lower bounds can then be obtained in analogy to the Dedekind Criterion. If the two bounds agree — and this will usually happen in our applications — the cumbersome algorithmic computation of the Galois group can be avoided. This will be explained in Paragraphs 1 and 2.

In Paragraphs 3 and 4 we will start from a Steinberg cross section matrix to construct Frobenius modules and additive polynomials with Galois group over $\mathbb{F}_q(\mathbf{t})$ a given finite group of Lie type $G(\mathbb{F}_q)$, in particular for all infinite series of classical groups (sometimes only over fields of odd characteristic). In the final Paragraph 5 we then demonstrate how to use field restriction to obtain Galois extensions with the same Galois group over smaller fields of constants and in particular over $\mathbb{F}_p(t)$.

The contents of this chapter was developed, on the basis of Matzat (2003) and Malle (2003) in the diploma theses of Garcia Lopez, Albert, Maier and Stichel and first published in Garcia Lopez (2010), Albert and Maier (2011) and Stichel (2014).

A non-constructive proof for the existence of G -realizations over \mathbb{F}_q of the \mathbb{F}_q -points of semisimple simply connected linear algebraic groups defined over \mathbb{F}_q had earlier been found by Nori (1994), see also Gille (2000). Some more special polynomials for various series of nearly simple classical groups had been constructed

before by Abhyankar and collaborators. These are mainly collected in a series of papers on “nice polynomials for nice groups” (see among others Abhyankar ([1994](#), [1996a,b](#)), Abhyankar and Loomis ([1998](#), [1999](#)), and Abhyankar and Inglis ([2001](#))). We give hints on these at the end of the corresponding sections.

1 Frobenius Modules

This first paragraph contains a short introduction to the theory of (ordinary) Frobenius modules and their connection to Galois extensions in positive characteristic as well as to additive polynomials. The presentation follows the first parts of Matzat (2003). As Frobenius modules are special types of difference modules, farther reaching information can for example be found in the monograph of van der Put and Singer (1997).

1.1 Ordinary Frobenius Modules

Throughout this chapter K will denote a field of positive characteristic $\text{char}(K) = p \in \mathbb{P}$, and $q = p^e$ denotes a power of p . Then the map

$$\phi := \phi_q : K \rightarrow K, \quad a \mapsto a^q,$$

is called the (ordinary) *Frobenius endomorphism*, and the pair (K, ϕ_q) a *Frobenius field* or *F-field* for short. The fixed field K^ϕ of ϕ is then a subfield of \mathbb{F}_q .

A pair (M, Φ) consisting of a K -vector space M and a ϕ -semilinear map $\Phi : M \rightarrow M$, that is, a map with the properties

$$\Phi(x + y) = \Phi(x) + \Phi(y) \quad \text{and} \quad \Phi(ax) = \phi(a)\Phi(x) \quad (1.1)$$

for all $x, y \in M$ and $a \in K$ is called an (ordinary) *Frobenius module*, or *F-module* for short, over (K, ϕ) . It is called a *trivial F-module* if M has a Φ -invariant basis.

Now let L/K be an F-field extension with Frobenius endomorphism ϕ_L , and $M_L := L \otimes M$ with the Frobenius endomorphism $\Phi_L := \phi_L \otimes \Phi$ the extended F-module. Then we call

$$\text{Sol}_L^\Phi(M) := \{x \in M_L \mid \Phi_L(x) = x\}$$

the *solution space of M over L* . If (M_L, Φ_L) is trivial in the above sense, then (L, ϕ_L) is called a *solution field of M* . We will usually suppress the index and write ϕ, Φ in place of ϕ_L and Φ_L .

Now assume that M has finite dimension n over K and let $B = \{b_1, \dots, b_n\}$ denote an ordered K -basis. Then there exists a representing matrix $D = D_B(\Phi) \in K^{n \times n}$ of Φ with $\Phi(B) = B \cdot D$ (where B is considered as a row vector). In the case that $D \in \text{GL}_n(K)$ we call (M, Φ) *dualizable*. Then the representing matrix of the dual Frobenius endomorphism Φ^* on the dual space M^* with respect to the dual basis B^* is given by

$$D_{B^*}(\Phi^*) = (D^{-1})^t. \quad (1.2)$$

Finally, (M, Φ) is called a *cyclic F-module* if there exists a Φ -cyclic element x in M , i.e., if the set $\{\Phi^i(x) \mid i \in \mathbb{N}\}$ contains a basis of M .

Remark. If (M, Φ) is an F-module over (K, ϕ) with basis $B = \{b_1, \dots, b_n\}$ and if $\tilde{B} := B \cdot C$ with $C \in \mathrm{GL}_n(K)$ is a further basis of M , then the representing matrices $D_B(\Phi)$ and $D_{\tilde{B}}(\Phi)$ satisfy

$$D_{\tilde{B}}(\Phi) = C^{-1} D_B(\Phi) \phi(C). \quad (1.3)$$

Then $D_{\tilde{B}}(\Phi)$ is called a ϕ -equivalent matrix to $D_B(\Phi)$.

Proposition 1.1. *Let (M, Φ) be an F-module over an F-field (K, ϕ) with $\dim_K(M) = n$. Then for all F-extension fields $(L, \phi_L) \geq (K, \phi)$ with fixed field $k := L^{\phi_L}$ the solution space $\mathrm{Sol}_L^\Phi(M)$ is a k -vector space with $\dim_k(\mathrm{Sol}_L^\Phi(M)) \leq n$.*

Proof. Obviously $W := \mathrm{Sol}_L^\Phi(M)$ is a k -vector space. Assume $\dim_k(W) > n$. Then there exists a minimal set of vectors $S = \{x_1, \dots, x_m\} \subset M_L$ of cardinality $m > 0$ which is linearly independent over k and linearly dependent over L . By minimality x_1, \dots, x_{m-1} are linearly independent over L . Thus

$$x_m = \sum_{i=1}^{m-1} a_i x_i \quad \text{with } a_i \in L$$

and not all a_i in k . But then the Φ -image satisfies

$$x_m = \sum_{i=1}^{m-1} \phi(a_i) x_i = 0.$$

Subtracting the second equation from the first shows that the L -linearly independent subset $\{x_1, \dots, x_{m-1}\}$ of S is linearly dependent over L , leading to a contradiction. \square

The next result shows that every dualizable F-module over K possesses a minimal solution field which defines a finite Galois extension of K .

Theorem 1.2. *Let (M, Φ) be a dualizable F-module over an F-field (K, ϕ) . Then:*

(a) *There exists an F-extension field $(N, \phi) \geq (K, \phi)$ of (K, ϕ) with dimension $\dim_k(\mathrm{Sol}_N^\Phi(M)) = n = \dim_K(M)$, where $k = N^\phi$.*

(b) *If N in (a) is minimal then N/K is a finite Galois extension (and determined uniquely inside an algebraic closure \bar{K} of K).*

Proof. Let $\phi = \phi_q$. Then we have $L^\phi \leq \mathrm{IF}_q$ for every F-extension field $(L, \phi) \geq (K, \phi)$ and hence $\phi(y) = y$ for $y \in L^\phi$. Now let $B = \{b_1, \dots, b_n\}$ be a basis of M over K and $D := D_B(\Phi) \in \mathrm{GL}_n(K)$ the representing matrix of Φ with respect to B . Then every solution vector $\sum_{i=1}^n b_i y_i \in \mathrm{Sol}_L^\Phi(M)$ with $y_i \in L$ satisfies

$$By = \Phi(By) = \Phi(B)\phi(y) = B \cdot D \cdot \phi(y),$$

where $y = (y_1, \dots, y_n)^t$ and $\phi(y) = (y_1^q, \dots, y_n^q)^t =: y^q$. This yields an algebraic system of equations $y - Dy^q = 0$ for y_1, \dots, y_n .

Now let \bar{K} be an algebraic closure of K with the Frobenius endomorphism $\bar{\phi} = \bar{\phi}_q$. Then the solution set S in \bar{K}^n of the above system of equations $\mathbf{y} - D\mathbf{y}^q = 0$ is finite by Proposition 1.1. As the projective variant of this algebraic system of equations has no solutions on the infinite hyperplane, the theorem of Bezout in $\mathbb{P}^n(\bar{K})$ shows that, counting multiplicities, there exist exactly q^n solutions in \bar{K}^n (see Šafarevič (1994), Ch. IV.2.1). The Jacobian matrix of $\mathbf{y} - D\mathbf{y}^q = 0$ is the identity matrix I_n . Thus all solutions are regular points on S and have multiplicity one (see Iitaka (1982), §2.6). Hence S consists of exactly q^n simple solutions $\mathbf{y}_1, \dots, \mathbf{y}_{q^n}$, which by Proposition 1.1 form an \mathbb{F}_q -vector space. The field $N := K(y_{ij})$ generated by the components y_{ij} of all vectors $\mathbf{y}_i = (y_{i1}, \dots, y_{in})^t \in \bar{K}^n$, $1 \leq i \leq q^n$, together with the restriction $\phi_N := \bar{\phi}_q|_N$ is then a solution field of (M, Φ) , and we have $\mathbb{F}_q \leq N$.

Now obviously N is minimal inside \bar{K} with these properties and according to the Remark before Proposition 1.1 independent of the choice of basis. Since all solutions of the algebraic system of equations $\mathbf{y} - D\mathbf{y}^q = 0$ in \bar{K}^n are simple, N/K is moreover separable and normal, hence Galois. \square

A linearly independent system of solutions $\mathbf{y}_1, \dots, \mathbf{y}_n \in N^n$ of $D\mathbf{y}^q = \mathbf{y}$ is called a *fundamental system of solutions*, and the matrix $Y := (\mathbf{y}_1, \dots, \mathbf{y}_n)$ is a *fundamental solution matrix*. It is characterized by the property that $\phi_N(Y) = D^{-1}Y$. With this we obtain the following characterization of solutions fields:

Corollary 1.3. *Let (K, ϕ) be an F -field with $K^\phi = \mathbb{F}_q$. Then (N, ϕ) is a minimal solution field of a dualizable F -module (M, Φ) over (K, ϕ) if and only if:*

- (1) *there exists a matrix $Y = (y_{ij})_{i,j=1}^n \in \mathrm{GL}_n(N)$ with $\phi_N(Y) = D^{-1}Y$, and*
- (2) *we have $N = K(Y)$, i.e., N/K is generated by the entries y_{ij} of Y .*

Such a characterization of minimal solution fields is well-known from the Galois theory of linear differential and difference equations (see e.g. van der Put and Singer (1997)).

1.2 Cyclic Frobenius Modules

If (K, ϕ) is a Frobenius field with $\phi = \phi_q$ then the matrix

$$\Delta_q(z_1, \dots, z_n) := \begin{pmatrix} z_1 & \dots & z_n \\ z_1^q & \dots & z_n^q \\ \vdots & & \vdots \\ z_1^{q^{n-1}} & \dots & z_n^{q^{n-1}} \end{pmatrix} \quad \text{with } z_1, \dots, z_n \in K,$$

is called *Moore matrix*, and its determinant $\det(\Delta_q(z_1, \dots, z_n))$ the *Moore determinant* of z_1, \dots, z_n . It is well-known that z_1, \dots, z_n are linearly independent over $k := K^\phi$ if and only if $\det(\Delta_q(z_1, \dots, z_n)) \neq 0$ (see Goss (1996), Cor. 1.3.4). In the theory of Frobenius modules the Moore matrix hence plays the role of the Vandermonde matrix. In particular we have (see Goss (1996), Lemma 1.3.6):

Proposition 1.4. Let (K, ϕ) be an F -field with $\phi = \phi_q$, and $z_1, \dots, z_n \in K$ linearly independent over $k := K^\phi$. Then the polynomial

$$f(X) := \det(\Delta_q(z_1, \dots, z_n, X)) / \det(\Delta_q(z_1, \dots, z_n)) \in K[X]$$

satisfies

$$f(X) = \prod_{z \in S} (X - z) \quad \text{with} \quad S = \mathbb{F}_q \langle z_1, \dots, z_n \rangle.$$

Polynomials of this kind with an \mathbb{F}_q -vector space as solution set are called *q -additive polynomials* (resp. \mathbb{F}_q -linear polynomials in Goss (1996), or q -polynomials in Smith (1995)). They have the special form

$$f(X) = \sum_{i=0}^n a_i X^{q^i}$$

(compare Goss (1996), Cor. 1.2.2). Here, $f(X)$ is separable if and only if $a_0 \neq 0$, i.e., if the solution space S has dimension n over \mathbb{F}_q .

Now we can answer the question on sufficient conditions to guarantee that an F -module possesses cyclic elements.

Theorem 1.5. Let (M, Φ) be a dualizable F -module over an F -field (K, ϕ) with $\phi = \phi_q$ such that $\dim_K(M) = n$. If $|K| > \binom{q^n}{2}$ then M is a cyclic F -module.

Proof. In a first step we choose a basis $B = \{b_1, \dots, b_n\}$ of M and consider the corresponding representing matrix $D := D_B(\Phi)$. Further we let N/K be a minimal solution field of (M, Φ) with fundamental matrix $Y = (y_{ij})_{i,j=1}^n = (\mathbf{y}_1, \dots, \mathbf{y}_n) \in \mathrm{GL}_n(N)$. Then we have $\phi(Y) = D^{-1}Y$ by Corollary 1.3. Now let Q denote the ideal in $K[X_1, \dots, X_n]$ generated by $(X_1^q, \dots, X_n^q)^t - D^{-1}(X_1, \dots, X_n)^t$. Then by Theorem 1.2 the factor ring $R := K[X_1, \dots, X_n]/Q$ has dimension $\dim_K(R) = q^n$. If K has more than $\binom{q^n}{2}$ elements, by Kreuzer and Robbiano (2000), Prop. 3.7.22, there exist elements $c_i \in K$ such that $X := X_1 - \sum_{i=2}^n c_i X_i$ is in normal 1-position, i.e., so that the first components of all solutions are pairwise distinct (see Kreuzer and Robbiano (2000), Def. 3.7.21). This transformation corresponds to the base change

$$B \mapsto \tilde{B} := (b_1 + \sum_{i=2}^n c_i b_i, b_2, \dots, b_n) := B \cdot C,$$

and the corresponding fundamental solution matrix is given by $\tilde{Y} := (\tilde{\mathbf{y}}_1, \dots, \tilde{\mathbf{y}}_n) = C^{-1}Y$.

In a second step we apply the Buchberger algorithm with respect to the anti-lexicographical ordering to the system of equations in X, X_2, \dots, X_n given by Q . Since the first components of the solutions are pairwise distinct we then obtain a Gröbner basis of the form

$$f(X) = \sum_{i=0}^{q^n} \tilde{a}_i X^i \quad \text{and} \quad X_j = f_j(X) \in K[X] \quad \text{for } j = 2, \dots, n$$

with suitable $\tilde{a}_i \in K$. By Theorem 1.2 the solution space of $f(X)$ is given by the \mathbb{F}_q -vector space \tilde{S} of the first components of the solutions $\tilde{\mathbf{y}}_i = (\tilde{y}_{i1}, \dots, \tilde{y}_{in})^t$, $1 \leq i \leq n$, of $\tilde{\mathbf{y}}^q = \tilde{D}^{-1}\tilde{\mathbf{y}}$ with $\tilde{D} = D_{\tilde{B}}(\Phi)$. Thus we obtain $f(X) = \prod_{\tilde{z} \in \tilde{S}} (X - \tilde{z})$, and moreover $f(X)$ is q -additive and separable, say $f(X) = \sum_{i=0}^n a_i X^{q^i}$ with $a_0 \neq 0$. Every basis $\{z_1, \dots, z_n\}$ of \tilde{S} can now be completed via $\tilde{z}_{ij} := f_j(z_i)$ to a basis $\tilde{z}_1 = (z_1, \tilde{z}_{12}, \dots, \tilde{z}_{1n}), \dots, \tilde{z}_n = (z_n, \tilde{z}_{n2}, \dots, \tilde{z}_{nn})$ of $\text{Sol}_N^\Phi(M)$. Thus $\tilde{z}_1, \dots, \tilde{z}_n$ are linear combinations of $\tilde{y}_1, \dots, \tilde{y}_n$. So there exists a matrix $C' \in \text{GL}_n(\mathbb{F}_q)$ with $\tilde{Z} := (\tilde{z}_1, \dots, \tilde{z}_n) = \tilde{Y} C'$, and \tilde{Z} is by definition also a fundamental solution matrix of (M, Φ) , with respect to \tilde{B} .

In the third step we show first that there exists a matrix $\tilde{C} \in \text{GL}_n(K)$ with $Z := \Delta_q(z_1, \dots, z_n) = \tilde{C} \cdot \tilde{Z}$. For the first row of this matrix the choice $\tilde{c}_{1j} = \delta_{1j}$ will obviously do. Since

$$\phi(Z) = \phi(\tilde{C})\phi(\tilde{Z}) = \phi(\tilde{C})\tilde{D}^{-1}\tilde{Z}$$

we can take the first row of \tilde{D}^{-1} for the second row of \tilde{C} . By induction we see that the i th row of \tilde{C} is given by the first row of $\phi^{i-1}(\tilde{D}^{-1}) \cdots \tilde{D}^{-1}$. This proves the existence of a matrix $\tilde{C} \in K^{n \times n}$ with $Z = \tilde{C} \tilde{Z}$. Moreover this is invertible due to $\det(Z) \neq 0$. By the base change $\tilde{B} \mapsto \bar{B} := \tilde{B} \tilde{C}^{-1}$ the Moore matrix Z becomes the fundamental solution matrix of (M, Φ) with respect to the basis $\bar{B} = (\bar{b}_1, \dots, \bar{b}_n)$. In particular we have

$$\phi(Z) = \tilde{D}^{-1}Z \quad \text{and} \quad \Phi(\bar{B}) = \bar{B} \cdot \bar{D}$$

with

$$\bar{D}^{-1} = \begin{pmatrix} 0 & 1 & & \\ & \ddots & & \\ & & 1 & \\ -a_0 & -a_1 & \dots & -a_{n-1} \end{pmatrix} \quad \text{respectively} \quad \bar{D} = \begin{pmatrix} -\frac{a_1}{a_0} & \dots & -\frac{a_{n-1}}{a_0} & -\frac{1}{a_0} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}.$$

From this we obtain

$$\Phi(\bar{b}_1) = \bar{b}_2 - \frac{a_1}{a_0} \bar{b}_1, \dots, \Phi(\bar{b}_{n-1}) = \bar{b}_n - \frac{a_{n-1}}{a_n} \bar{b}_1$$

and thus the required Φ -cyclicity of \bar{b}_1 . \square

By Theorem 1.5 in particular all F -modules over an algebraic function field K are cyclic since there $|K| = \infty$. The monic q -additive polynomial

$$f(X) = \frac{\det(\Delta_q(z_1, \dots, z_n, X))}{\det(\Delta_q(z_1, \dots, z_n))} = \prod_{\tilde{z} \in \tilde{S}} (X - \tilde{z})$$

constructed in the proof, whose zeroes are precisely the vector space consisting of the first components of the solution space, will be called the *characteristic polynomial of the F -module*. According to the proof of Theorem 1.5 it satisfies:

Corollary 1.6. Let (M, Φ) be a dualizable F -module over (K, ϕ) and $f(X)$ the characteristic polynomial of (M, Φ) (with respect to a basis in normal 1-position). Then the splitting field N/K of $f(X)$ is the minimal solution field of (M, Φ) (inside \bar{K}).

Using the representing matrix $\bar{D} = D_{\bar{B}}(\Phi)$ in the proof of Theorem 1.5 one sees that every q -additive polynomial $f(X)$ occurs as the characteristic polynomial of a Frobenius module. In this situation we also write D_f in place of \bar{D} , and the corresponding F -module (M, Φ) is called the *F -module associated to $f(X)$* and denoted (M_f, Φ) . The inverse $A_f := D_f^{-1}$ of $\bar{D} = D_f$ is the *companion matrix* of $f(X)$.

1.3 Galois Groups

In this subsection we attach to every dualizable F -module a linear group as Galois group and derive an important upper bound for these.

Proposition 1.7. Let (M, Φ) be a dualizable F -module over (K, ϕ) with solution field N and $Y, \tilde{Y} \in \mathrm{GL}_n(N)$ two fundamental solution matrices of (M, Φ) with respect to the same basis. Then there exists a matrix $C \in \mathrm{GL}_n(N^\phi)$ with $\tilde{Y} = Y \cdot C$.

Proof. Let $\phi = \phi_q$, so $N^\phi = \mathbb{F}_q$. Since the columns of Y as well as of \tilde{Y} consist of the coordinate vectors of a basis of the solution space $\mathrm{Sol}_N^\Phi(M)$, which is an \mathbb{F}_q -vector space, the matrix C is just the corresponding base change matrix on the coordinate vector space. \square

Corollary 1.8. Let (K, ϕ) be an F -field and (N, ϕ) a minimal solution field of an F -module over K as in Proposition 1.7. Then the Galois group $\mathrm{Gal}(N/K)$ is isomorphic to a subgroup of $\mathrm{GL}_n(N^\phi)$.

Proof. Let $Y \in \mathrm{GL}_n(N)$ be a fundamental solution matrix of the F -module (M, Φ) (with respect to a basis B of M). Then for $\gamma \in \mathrm{Gal}(N/K)$, $\gamma(Y)$ is again a fundamental solution matrix. By Proposition 1.7 there hence exists a matrix $C_\gamma \in \mathrm{GL}_n(N^\phi)$ with $\gamma(Y) = Y \cdot C_\gamma$. This induces a faithful representation

$$\Gamma : \mathrm{Gal}(N/K) \rightarrow \mathrm{GL}_n(N^\phi), \quad \gamma \mapsto C_\gamma. \quad \square$$

The representation of $\mathrm{Gal}(N/K)$ into $\mathrm{GL}_n(q)$ is also called the *Galois group of the F -module (M, Φ)* (with respect to a given basis of M) and denoted by $\mathrm{Gal}(M, \Phi)$.

Remark. The Galois group of (M, Φ) restricts, via

$$\gamma(z_1, \dots, z_n) := (z_1, \dots, z_n)C_\gamma \quad \text{for } z_i = y_{1i},$$

to the solution space V of the first solution components and so directly furnishes a faithful permutation representation on the zeroes of the characteristic polynomial.

In the next theorem we use the language of linear algebraic groups, see e.g. Springer (1998), Ch. 2.1. It gives an extremely useful upper bound for the Galois group $\text{Gal}(M, \Phi)$ of a Frobenius module.

Theorem 1.9 (Upper Bound Theorem). *Let (M, Φ) be a dualizable F -module over the F -field (K, ϕ) with $\phi = \phi_q$ and $K^\phi = \mathbb{F}_q$. Further let \mathbf{G} be a connected linear algebraic group defined over \mathbb{F}_q . If there exists a basis B of M with $D_B(\Phi) \in \mathbf{G}(K)$, then the Galois group of the F -module satisfies*

$$\text{Gal}(M, \Phi) \leq \mathbf{G}(\mathbb{F}_q).$$

Proof. In the proof we utilize the modified Lang isogeny

$$\pi : \mathbf{G}(K^{\text{sep}}) \longrightarrow \mathbf{G}(K^{\text{sep}}), \quad (x_{ij}) \mapsto \phi_q((x_{ij})) (x_{ij})^{-1},$$

over the separable closure K^{sep} of K . As \mathbf{G} is a connected linear algebraic group, π is surjective by the Theorem II.1.1 of Lang–Steinberg. So there exists a matrix $Y = (y_{ij}) \in \mathbf{G}(K^{\text{sep}})$ with $\pi(Y) = D^{-1}$ for $D = D_B(\Phi) \in \mathbf{G}(K)$, respectively $Y^q = D^{-1} \cdot Y$. That is, Y is a fundamental solution matrix of (M, Φ) . By Corollary 1.3 the field $N = K(Y)$ is a minimal solution field of (M, Φ) . Since $\gamma(Y) = Y \cdot C_\gamma$ for $\gamma \in \text{Gal}(N/K)$ we have that C_γ not only lies in $\text{GL}_n(q)$, but also in $\mathbf{G}(N)$. Thus $C_\gamma \in \mathbf{G}(\mathbb{F}_q)$ for all $\gamma \in \text{Gal}(N/K)$. \square

The existence of such a non-trivial upper bound for the Galois group is special to positive characteristic and does not have an analogue in characteristic zero.

In the following examples we assume that $K = \mathbb{F}_p(t)$ is a rational function field in one variable and $\phi = \phi_p$.

Example 1.1. The simplest example of a connected linear algebraic group is the multiplicative group \mathbb{G}_m with $\mathbb{G}_m(K) = K^\times$. We let (M, Φ) be a 1-dimensional F -module with $D_B(\Phi) = (t^{-1}) \in \mathbb{G}_m(K)$. Then by Corollary 1.8 the Galois group of (M, Φ) is a subgroup of $\mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^\times$. We obtain the characteristic polynomial from $X^p = \phi(X) = tX$ as

$$f(X) = X^p - tX = X(X^{p-1} - t) \in K[X],$$

where the second factor $X^{p-1} - t \in K[X]$ is irreducible. Thus the minimal solution field N has degree $p - 1$ over K , and $\text{Gal}(M, \Phi) = \mathbb{F}_p^\times$. \square

Example 1.2. Now consider the additive group \mathbb{G}_a and let (M, Φ) be a 2-dimensional F -module over K with $D_B(\Phi) = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \in \mathbb{G}_a(K)$. Then by Theorem 1.9 the Galois group of (M, Φ) is a subgroup of $\mathbb{G}_a(\mathbb{F}_p) \cong (\mathbb{F}_p, +)$. From

$$\Phi \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

we obtain that $X_1^p = X_1 + tX_2$ and $X_2^p = X_2$, so for $X = X_1$ the characteristic polynomial is

$$f(X) = X^{p^2} - (t^{p-1} + 1)X^p + t^{p-1}X.$$

This factorises as

$$f(X) = \prod_{c \in \mathbb{F}_p} (X^p - X - ct)$$

into a product of irreducible Artin–Schreier polynomials of degree p . So the Galois group of (M, Φ) contains at least p elements, and we deduce that $\text{Gal}(M, \Phi) = \text{IF}_p$. \square

Example 1.3. As final example we consider the group $\mathbf{G} = \text{SL}_2$. For this let (M, Φ) be a 2-dimensional \mathbf{F} -module over K with $D_B(\Phi) = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \in \text{SL}_2(K)$. Thus the Galois group G of (M, Φ) is a subgroup of $\text{SL}_2(p)$. With $X = X_1$ we obtain the characteristic polynomial

$$f(X) = X^{p^2} - tX^p + X = X(X^{p^2-1} - tX^{p-1} + 1) \in K[X].$$

As the second factor is irreducible, $p^2 - 1$ must divide $|G|$. Now we specialize $t \mapsto 2$ and $X^{p-1} \mapsto Y$. Then the second factor becomes

$$Y^{p+1} - 2Y + 1 = (Y - 1)(Y^p + \dots + Y - 1),$$

where again the second factor is irreducible. By the Dedekind Criterion (Corollary I.9.3) the solution field N then contains an intermediate field L/K of degree p . So $|G|$ is even divisible by $p(p^2 - 1)$, which implies that $G = \text{SL}_2(p)$. \square

1.4 Effective Frobenius Modules

In this section we are concerned with the question under which conditions on a Frobenius module (M, Φ) we are in the favorable situation that the containment of $D_B(\Phi)$ in a certain linear algebraic group $\mathbf{G}(K)$ already determines the Galois group, i.e., the upper bound in Theorem 1.9 is attained.

For simplification we introduce the following definition: a dualizable \mathbf{F} -module (M, Φ) over (K, ϕ) is called *effective* if there exists a linear algebraic group \mathbf{G} defined over K^ϕ and a basis B of M such that

$$D_B(\Phi) \in \mathbf{G}(K) \quad \text{and} \quad \text{Gal}(M, \Phi) \cong \mathbf{G}(K^\phi).$$

Obviously the three \mathbf{F} -modules given in the examples at the end of the previous section are effective \mathbf{F} -modules.

Proposition 1.10. *Let (K, ϕ) be an \mathbf{F} -field with $K \geq \overline{\text{IF}}_p$ and (M, Φ) a dualizable \mathbf{F} -module with basis B . Further let \mathbf{G} be a linear algebraic group over K with*

$D_B(\Phi) \in \mathbf{G}(K)$. Then there exists a matrix $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ such that with $\tilde{B} = BC$ the matrix $D_{\tilde{B}}(\Phi)$ lies in the connected component $\mathbf{G}^\circ(K)$ of \mathbf{G} .

Proof. By a theorem of Borel and Serre the connected component \mathbf{G}° of \mathbf{G} has a finite supplement \mathcal{H} in \mathbf{G} , i.e., \mathcal{H} is a finite linear algebraic group over $\overline{\mathbb{F}}_p$ (see for example Wehrfritz (1973), Lemma 10.10). So $D = D_B(\Phi)$ can be factorized into the product $D = D_0 \cdot C_0$ with $D_0 \in \mathbf{G}^\circ(K)$ and $C_0 \in \mathcal{H}(\overline{\mathbb{F}}_p)$. As C_0 defines a trivial \mathbf{F} -module over $\overline{\mathbb{F}}_p$, there exists $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ with $C_0^{-1} = \phi(C)C^{-1}$. Then for the basis $\tilde{B} := B \cdot C$ of M we obtain by (1.3)

$$D_{\tilde{B}}(\Phi) = C^{-1} D_B(\Phi) \phi(C) = C^{-1} D_0 C.$$

Thus $D_{\tilde{B}}(\Phi)$ is contained in the connected component $\mathbf{G}^\circ(K)$ of \mathbf{G} . \square

Corollary 1.11. *If a Frobenius module (M, Φ) with $D_B(\Phi) \in \mathbf{G}(K)$ is effective, then the linear algebraic group \mathbf{G} is connected.*

Proof. Let (M, Φ) be an effective \mathbf{F} -module over (K, ϕ) with $D_B(\Phi) \in \mathbf{G}(K)$ and $\mathrm{Gal}(M, \Phi) = \mathbf{G}(\mathbb{F}_q)$. By Proposition 1.10 we may assume without loss of generality that $D_B(\Phi)$ lies in the connected component $\mathbf{G}^\circ(\overline{\mathbb{F}}_q K)$. So we have $\mathrm{Gal}(M, \Phi) \leq \mathbf{G}^\circ(\overline{\mathbb{F}}_q)$ by Theorem 1.9, so by effectiveness that $\mathbf{G} = \mathbf{G}^\circ$. \square

There remains the question under which conditions \mathbf{F} -modules are effective, whose Galois group is the group of \mathbb{F}_q -rational points of a connected linear algebraic group \mathbf{G} ? Does this always hold, for example, if $K/\overline{\mathbb{F}}_p$ is an algebraic function field in one variable? The answer seems to be unknown.

2 Computation of the Galois Group

In the first four sections we present an algorithm for the computation of the Galois group of a q -additive polynomial in finitely many steps. Unfortunately the necessary calculations can become quite cumbersome for larger Galois groups. For this reason in the fifth section we derive lower bounds for the Galois group, which are similar in flavor to the Dedekind Criterion (see Corollary I.9.3). Agreement of the upper bound from Theorem 1.9 with the composite of all lower bounds then renders the algorithmic determination of the Galois group superfluous. In the subsequent sections this method will usually prove successful. The first four sections follow the thesis of Garcia Lopez (2010), while the last one is based upon Matzat (2003) with the multivariate version presented in Albert and Maier (2011).

2.1 An Invariant Theoretic Criterion

Let K be a (at first) arbitrary field and V a K -vector space with basis $B = \{b_1, \dots, b_n\}$. Then the *symmetric algebra* $\text{Sym}_K(V)$ will be denoted by $K[V]$, and its field of fractions by $K(V)$. It is well-known that $K[V]$ is isomorphic to a polynomial ring $K[t_1, \dots, t_n]$ in linearly independent forms t_1, \dots, t_n on the dual vector space V^* , and we have $K(V) \cong K(t_1, \dots, t_n)$. In the following t_1, \dots, t_n usually denote the bidual basis of a given basis B in $V^{**} \cong V \subset K[V]$. In case L is a field containing K , we write $L[V]$ or $L[t_1, \dots, t_n]$ for $L \otimes_K K[V]$.

Now let G be a subgroup of the general linear group $\text{GL}(V) \cong \text{GL}_n(K)$. Then $\gamma \in G$ acts on the coordinates $\mathbf{v} = (v_1, \dots, v_n)^t$ of $v = \sum_{i=1}^n v_i b_i \in V$ via $\mathbf{v} \mapsto C_\gamma \mathbf{v}$ with a matrix $C_\gamma \in \text{GL}_n(K)$. Consequently, $\gamma \in G$ also acts on the polynomials $f(t_1, \dots, t_n)$ in $K[V] \cong K[t_1, \dots, t_n]$ via $\gamma(f(t_1, \dots, t_n)) = f((t_1, \dots, t_n)C_\gamma)$. The K -algebra of G -invariant polynomials in $K[V]$ is called the *ring of invariants* $K[V]^G$, and the field of G -invariant rational functions in $K(V)$ the *field of invariants* $K(V)^G$.

In the standard literature on invariant theory (e.g. Smith (1995), Derksen and Kemper (2002) etc.) usually $K[V]$ stands for $\text{Sym}_K(V^*)$ with the inverse action of G on V^* . The use of $K[V] := \text{Sym}_K(V)$ in this monograph has the advantage that the action of G on a basis b_1, \dots, b_n of V and its bidual basis t_1, \dots, t_n in $V^{**} \cong V \subset K[V]$ agree. Since statements on invariants do not depend on whether the action of G is ordinary or inverse, the results from invariant theory cited in the sequel hold for $K[V] \cong \text{Sym}_K(V) \cong \text{Sym}_K(V^{**})$ as well as for $\text{Sym}_K(V^*)$.

The first statements needed from invariant theory are collected in the following

Remarks. (1) If H is a subgroup of $G \leq \text{GL}(V)$ then we clearly have

$$K[V]^H \geq K[V]^G \quad \text{and} \quad K(V)^H \geq K(V)^G.$$

(2) If $G \leq \mathrm{GL}(V)$ is a finite group, then

$$K(V)^G = \mathrm{Frac}(K[V]^G).$$

This is shown for example in Smith (1995), Prop. 1.2.4.

The best known example of an invariant ring is obtained from the natural permutation representation of the symmetric group S_n as the group $G \leq \mathrm{GL}_n(K)$ of permutation matrices. Here $K[V]^G$ is the ring of symmetric polynomials over K . This is itself a polynomial ring, generated over K for example by the elementary symmetric polynomials

$$s_i := \sum_{1 \leq j_1 < \dots < j_i \leq n} \prod_{k=1}^i t_{j_k} \quad \text{for } 1 \leq i \leq n.$$

An analogue for q -additive polynomials is given by the Dickson algebra. For this let V be an n -dimensional vector space over $K \geq \mathbb{F}_q$ and $G = \mathrm{GL}_n(q)$. Then the polynomial

$$f_{q,n}(X) := \prod_{t \in W} (X - t) \quad \text{with } W := \mathbb{F}_q \langle t_1, \dots, t_n \rangle$$

is q -additive by our observations in Paragraph 1. So it has the form

$$f_{q,n}(X) = \sum_{i=0}^n d_{q,n}^{(i)} X^{q^n - q^{n-i}} \quad \text{with } d_{q,n}^{(0)} = 1.$$

The non-trivial coefficients $d_i := d_{q,n}^{(i)}$, $1 \leq i \leq n$, of $f_{q,n}(X)$ are G -invariant homogeneous polynomials in t_1, \dots, t_n of degree $q^n - q^{n-i}$. They are called *Dickson invariants*. Obviously $K(V) = K(t_1, \dots, t_n)$ is the splitting field of $f_{q,n}(X)$ over $K(\mathbf{d}) = K(d_1, \dots, d_n) \leq K(V)^G$. So the d_1, \dots, d_n are algebraically independent over K and $K(V)/K(\mathbf{d})$ is Galois with Galois group H a subgroup of G . Since

$$[K(V) : K(\mathbf{d})] \geq \prod_{i=1}^n (q^n - q^{n-i}) = |G|$$

we even have $H = G$ and the invariant field $K(V)^G$ is generated over K by the Dickson invariants:

$$K(V)^G = K(d_1, \dots, d_n).$$

Thus the roots of the *Dickson polynomial*

$$f_{q,n}(X) = \sum_{i=0}^n d_i X^{q^n - q^{n-i}} \quad \text{with } d_0 = 1 \tag{2.1}$$

generate the Galois extension $K(\mathbf{t})/K(\mathbf{d})$ with group $\mathrm{GL}_n(q)$. (This indeed is a *generic polynomial* in the sense of Jensen, Ledet and Yui (2002), compare Example (1.1.2).)

By the Theorem of Dickson (see Smith (1995), Thm. 8.1.5) the polynomial subring $K[\mathbf{d}]$ of $K[V]^G$ is already the full ring of invariants of G , i.e., we have

$$K[V]^G = K[d_1, \dots, d_n].$$

This is also called the *Dickson algebra of degree n over K* in this context. It constitutes the starting point for the algorithm for the computation of the Galois group of a q -additive polynomial that we will present here.

Now let K again be an arbitrary field, V an n -dimensional K -vector space and $H \leq G \leq \mathrm{GL}_n(K)$ linear groups with finite index $(G : H) = m$. Then $F_H \in K(V)^H$ is called a *G -relative H -invariant* if F_H is a primitive element of the extension $K(V)^H/K(V)^G$. If $\sigma_1, \dots, \sigma_m$ is a system of representatives for the cosets of H in G then

$$\mathrm{Res}_{G/H}^{F_H}(X) := \prod_{j=1}^m (X - \sigma_j(F_H))$$

is called a *G -relative resolvent for H* . This will now be used in the case of q -additive polynomials.

Proposition 2.1. *Let $K \geq \mathbb{F}_q$ be a field, $f(X) \in K[X]$ a separable q -additive polynomial and $\mathbf{z} := (z_1, \dots, z_n)$ an ordered \mathbb{F}_q -basis of the zero space $V \subset K^{\mathrm{sep}}$ of $f(X)$. Further let $G_{\mathbf{z}} := \mathrm{Gal}_{\mathbf{z}}(f)$ be the representation of the Galois group of $f(X)$ with respect to the basis \mathbf{z} with $G_{\mathbf{z}} \leq G \leq \mathrm{GL}_n(q)$. If then $H \leq G$ is a subgroup of G , $F_H \in K[V]^H$ a G -relative H -invariant and $\rho_{\mathbf{z}} : K[V] \rightarrow \bar{K}$ the specialization homomorphism determined by $t_i \mapsto z_i$, then*

$$\mathrm{Res}_{G/H}^{F_H(\mathbf{z})}(X) := \rho_{\mathbf{z}}(\mathrm{Res}_{G/H}^{F_H}(X)) \in K[X].$$

Proof. We write

$$\mathrm{Res}_{G/H}^{F_H}(X) = \sum_{i=0}^m a_i(\mathbf{t}) X^i \in K[V]^G[X].$$

Then for $\gamma \in \mathrm{Gal}(f)$ with corresponding representing matrix $C_{\gamma} \in \mathrm{Gal}_{\mathbf{z}}(f)$ we have

$$\gamma(\mathrm{Res}_{G/H}^{F_H(\mathbf{z})}(X)) = \sum_{i=0}^m \gamma(\rho_{\mathbf{z}}(a_i(\mathbf{t}))) X^i = \sum_{i=0}^m \rho_{\mathbf{z}}(a_i(\mathbf{t}) C_{\gamma}) X^i = \sum_{i=0}^m \rho_{\mathbf{z}}(a_i(\mathbf{t})) X^i.$$

So the elements $\rho_{\mathbf{z}}(a_i(\mathbf{t}))$ all lie in the fixed field $N^{\mathrm{Gal}(f)}$ under $\mathrm{Gal}(f)$ of the splitting field N of $f(X)$ and hence in K . \square

The next theorem is a q -additive analogue of the Theorem of Stauduhar, which plays a central role in the computation of Galois groups in characteristic zero (compare also Stroth (1998), §17).

Theorem 2.2. Assume the notations in Proposition 2.1. Furthermore assume that the specialized G -relative H -resolvent $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ is separable. Then $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ has a zero in K if and only if $\text{Gal}_{\mathbf{z}}(f)$ is conjugate in G to a subgroup of H .

Proof. We first assume that $\text{Gal}_{\mathbf{z}}(f)$ is G -conjugate to a subgroup of H , that is, there exists $\sigma \in G$ with $\text{Gal}_{\mathbf{z}}(f) \leq \sigma H \sigma^{-1}$. Clearly $\sigma(F_H)$ is a G -relative $\sigma H \sigma^{-1}$ -invariant. Thus we have for all $\gamma \in \text{Gal}(f)$ that

$$\gamma(\rho_{\mathbf{z}}(F_H(\mathbf{t}))) = \rho_{\mathbf{z}}(F_H(\mathbf{t}C_{\gamma})) = \rho_{\mathbf{z}}(\gamma(F_H)).$$

So, $a := \rho_{\mathbf{z}}(\gamma(F_H))$ is invariant under $\text{Gal}(f)$ und thus is a zero of $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ in K .

For the converse assume that $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ has a zero $a \in K$. Then there exists a coset $\sigma H \in G/H$ with $\rho_{\mathbf{z}}(\sigma(F_H)) = a \in K$. We now assume that $\text{Gal}_{\mathbf{z}}(f)$ is not a subgroup of $\sigma H \sigma^{-1}$. Then there exists $C_{\gamma} \in \text{Gal}_{\mathbf{z}}(f) \setminus \sigma H \sigma^{-1}$ with $\gamma(\sigma(F_H)) \neq \sigma(F_H)$. Due to

$$\rho_{\mathbf{z}}(\gamma(\sigma(F_H))) = \gamma(\rho_{\mathbf{z}}(\sigma(F_H))) = \gamma(a) = a$$

this gives a contradiction to the separability of $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$. \square

Our proof of Theorem 2.2 also leads to the following observation:

Remark. The assertion of Theorem 2.2 remains true in the inseparable case if $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ either has no zero, or has at least one simple zero in K .

We are now faced with the task to determine suitable G -relative H -invariants $F_H \in K[V]^H$.

2.2 Computation of Homogeneous Invariants

We first show how to reduce the computation of G -relative H -invariants $F_H \in K[V]^H$ to the case $K = \mathbb{F}_q$.

Proposition 2.3. Let $K \geq \mathbb{F}_q$ be a field and $H < G \leq \text{GL}_n(q)$ subgroups of $\text{GL}_n(q)$. Then we have:

- (a) There exists a primitive element F_H of $K(V)^H / K(V)^G$ with $F_H \in \mathbb{F}_q[V] = \mathbb{F}_q[t_1, \dots, t_n]$.
- (b) If $H < G$ is maximal then there also exists a G -relative H -invariant $F_H \in \mathbb{F}_q[V]$ that is homogeneous in t_1, \dots, t_n .

Proof. Part (a) follows immediately from the translation theorem of Galois theory starting from the corresponding field extension $\mathbb{F}_q(V)^H / \mathbb{F}_q(V)^G$. Part (b) is obtained from that by decomposition into homogeneous components. \square

According to Proposition 2.3 we may now restrict ourselves to the computation of homogeneous G -relative H -invariants over \mathbb{F}_q . By the Remark (1) in Section 2.1 we have $\mathbb{F}_q[V]^H \geq \mathbb{F}_q[V]^G$ and thus $\mathbb{F}_q[V]_d^H \geq \mathbb{F}_q[V]_d^G$ for the corresponding homogeneous components in degree d . From this we obtain immediately:

Corollary 2.4. *Let $G \leq \mathrm{GL}_n(q)$ and $H < G$ a maximal subgroup. Then there exists a homogeneous G -relative H -invariant F_H of degree d if and only if*

$$\dim_{\mathbb{F}_q}(\mathbb{F}_q[V]_d^H) \neq \dim_{\mathbb{F}_q}(\mathbb{F}_q[V]_d^G).$$

The computation of bases of $\mathbb{F}_q[V]_d^H$ and $\mathbb{F}_q[V]_d^G$ is always possible with algorithms from constructive invariant theory, for example with the linear algebra method of Kemper described in Derksen and Kemper (2002), Ch. 3.3.1. If the index $(G : H)$ is prime to the characteristic of the underlying fields, then the homogeneous G -relative H -invariants of degree d are just given by the elements which are not fixed under the *relative Reynolds operator*

$$R_{G/H} : \mathbb{F}_q[V]_d^H \longrightarrow \mathbb{F}_q[V]_d^G, \quad f \mapsto \frac{1}{(G : H)} \sum_{\sigma \in G/H} \sigma(f).$$

Starting with a basis of $\mathbb{F}_q[V]_d^H$ these can also be determined in this simple fashion (for this see Derksen and Kemper (2002), Algorithm 3.1.1).

2.3 Specialization of Relative Resolvents

In this section we describe an algorithm for the computation of the Galois group of a q -additive polynomial. This works inductively along a chain of maximal subgroups. For this we make the following induction hypothesis: Let $K \geq \mathbb{F}_q$ be a field, $f(X) \in K[X]$ a separable q -additive polynomial, $V \subset K^{\mathrm{sep}}$ the vector space of zeroes of $f(X)$ and $\mathbf{z} = (z_1, \dots, z_n)$ an \mathbb{F}_q -basis of V . We assume that $\mathrm{Gal}_{\mathbf{z}}(f) \leq G$ and that $H < G$ is a maximal subgroup of G of index $(G : H) = m$. Further let $F_H \in \mathbb{F}_q[V]^H$ be a G -relative H -invariant with (without loss of generality) $\rho_{\mathbf{z}}(F_H) \in K$ (respectively $G_{\mathbf{z}} \leq H$) and $\mathrm{Res}_{G/H}^{F_H(\mathbf{z})}(X) \in K[X]$.

With the symmetric bilinear form

$$\beta : \mathbb{F}_q(V)^H \times \mathbb{F}_q(V)^H \longrightarrow \mathbb{F}_q(V)^G, \quad (g, h) \mapsto \sum_{\sigma \in G/H} \sigma(gh),$$

over $\mathbb{F}_q(V)^G$ we introduce the symmetric matrix

$$\mathrm{Col}_{G/H}^{F_H} := \begin{pmatrix} \beta(F_H^0, F_H^0) & \dots & \beta(F_H^0, F_H^{m-1}) \\ \vdots & & \vdots \\ \beta(F_H^{m-1}, F_H^0) & \dots & \beta(F_H^{m-1}, F_H^{m-1}) \end{pmatrix},$$

which we call the *G-relative Colin matrix of F_H* in view of the precursor work of Colin (1995) in characteristic zero. This enjoys the following property:

Proposition 2.5. *Let $F_H \in \mathbb{F}_q[V]^H$ be a G-relative H-invariant and $g \in \mathbb{F}_q[V]^H$ arbitrary. Then there exist $x_j \in \mathbb{F}_q(V)^G$ with*

$$g = \sum_{j=0}^{m-1} x_j F_H^j.$$

Here, x_0, \dots, x_{m-1} are solutions of the linear system of equations

$$(\beta(F_H^0, g), \dots, \beta(F_H^{m-1}, g))^t = \text{Col}_{G/H}^{F_H}(x_0, \dots, x_{m-1})^t.$$

Proof. The first part of the assertion follows from the fact that F_H is a primitive element of the extension $\mathbb{F}_q(V)^H / \mathbb{F}_q(V)^G$, the second from the linearity of $\beta(F_H^i, g)$ in the second argument:

$$\beta(F_H^i, g) = \sum_{j=0}^{m-1} \beta(F_H^i, F_H^j) x_j.$$

□

After this preparation we come to the principal result of this section:

Theorem 2.6. *Under our inductive assumption we have:*

- (a) *The determinant of the G-relative Colin matrix of F_H is different from zero: $\det(\text{Col}_{G/H}^{F_H}) \neq 0$.*
- (b) *The specialized resolvent $\text{Res}_{G/H}^{F_H(x)}(X)$ is separable if and only if the determinant of the specialized Colin matrix satisfies $\det(\text{Col}_{G/H}^{F_H(x)}) \neq 0$.*

Proof. Let $\sigma_1, \dots, \sigma_m$ be a system of coset representatives of H in G . Then

$$\beta(F_H^i, F_H^j) = \sum_{l=1}^m \sigma_l(F_H^i F_H^j) = \sum_{l=1}^m \sigma_l(F_H^i) \sigma_l(F_H^j).$$

This leads to the following factorization of the Colin matrix:

$$\text{Col}_{G/H}^{F_H} = \begin{pmatrix} 1 & \dots & 1 \\ \sigma_1(F_H) & \dots & \sigma_m(F_H) \\ \vdots & & \vdots \\ \sigma_1(F_H^{m-1}) & \dots & \sigma_m(F_H^{m-1}) \end{pmatrix} \begin{pmatrix} 1 & \dots & \sigma_1(F_H^{m-1}) \\ \vdots & & \vdots \\ 1 & \dots & \sigma_m(F_H^{m-1}) \end{pmatrix}.$$

So $\det(\text{Col}_{G/H}^{F_H})$ is the square of the determinant of the Vandermonde matrix in $\sigma_1(F_H), \dots, \sigma_m(F_H)$ and hence different from zero.

If moreover the polynomial $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ is separable, then its discriminant

$$D(\text{Res}_{G/H}^{F_H(\mathbf{z})}) = \prod_{i < j} (\rho_{\mathbf{z}}(\sigma_i(F_H)) - \rho_{\mathbf{z}}(\sigma_j(F_H)))^2$$

does not vanish and by the above coincides with the determinant of the specialized Colin matrix $\det(\text{Col}_{G/H}^{F_H})$. \square

As an immediate consequence we obtain:

Corollary 2.7. *If $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ is separable the specializations of the invariants $g \in \mathbb{F}_q[V]^H$ are computable successively using Proposition 2.5.*

As a means to facilitate the computation of the specialized Colin matrix we observe the following:

Proposition 2.8. *The specialized Colin matrix $\text{Col}_{G/H}^{F_H(\mathbf{z})}$ can be computed directly from the coefficients of the specialized relative resolvent $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ using the Newton identities.*

Proof. The specialized G -relative resolvent $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ has the form

$$\text{Res}_{G/H}^{F_H(\mathbf{z})}(X) = \prod_{i=1}^m (X - \sigma_i(\rho_{\mathbf{z}}(F_H))) = X^m + \sum_{i=1}^m (-1)^i a_i X^{m-i} \in K[X]$$

with the elementary symmetric polynomials

$$a_i = s_i(\sigma_1(\rho_{\mathbf{z}}(F_H)), \dots, \sigma_m(\rho_{\mathbf{z}}(F_H))),$$

whose values we assume to be given. The entries of the specialized Colin matrix have the form

$$\beta(\rho_{\mathbf{z}}(F_H^i, F_H^j)) = \sum_{l=1}^m \sigma_l(\rho_{\mathbf{z}}(F_H^{i+j})).$$

So they are power sums in the $\sigma_l(\rho_{\mathbf{z}}(F_H))$. The latter can be computed recursively from the a_1, \dots, a_m using the Newton identities. \square

It now remains to understand how the assumptions on separability of the specialized resolvent $\text{Res}_{G/H}^{F_H(\mathbf{z})}(X)$ can be guaranteed. This is the aim of the next section.

2.4 Linear Tschirnhaus Transformations

Let $K \geq \mathbb{F}_q$ be a field, $f \in K[X]$ a separable q -additive polynomial and $\mathbf{z} = (z_1, \dots, z_n)$ a basis of the \mathbb{F}_q -vector space of zeroes $V \subset K^{\text{sep}}$. If $0 \neq g \in K[X]$

is a further q -additive polynomial then

$$\theta_g(f)(X) := \prod_{(a_1, \dots, a_n) \in \mathbb{F}_q^n} \left(X - \sum_{i=1}^n a_i g(z_i) \right) \in K^{\text{sep}}[X]$$

is called the *linear Tschirnhaus transform of f with respect to g* . Clearly $\theta_g(f)(X)$ is again a q -additive polynomial and it satisfies $\theta_g(f)(X) \in K[X]$ because of the invariance of its coefficients under $\text{Gal}(f)$.

Proposition 2.9. *Let $f, g \in K[X]$ be as above. If the Tschirnhaus transform $\theta_g(f)(X)$ is separable then the splitting fields and hence the Galois groups of f and $\theta_g(f)$ over K agree.*

Proof. Let N be the splitting field of $f(X)$ over K , so $z_i \in N$. Let $\tilde{f} := \theta_g(f)$ denote the linear Tschirnhaus transform of f with respect to g . Then $g(\mathbf{z}) := (g(z_1), \dots, g(z_n))$ is a generating system of \tilde{V} in the splitting field \tilde{N} of $\tilde{f}(X)$ over K . Because \tilde{f} is separable, \tilde{V} is an n -dimensional \mathbb{F}_q -vector space and $g(z_1), \dots, g(z_n)$ are linearly independent elements thereof. As N/K is Galois and $\tilde{N} \leq N$, the extension N/\tilde{N} is also Galois. Now let $\tilde{\sigma} \in \text{Gal}(N/\tilde{N})$. Then there exists $C = (c_{ij})_{i,j=1}^n \in \text{GL}_n(q)$ with

$$\tilde{\sigma}(z_j) = \sum_{i=1}^n c_{ij} z_i \quad \text{for } j = 1, \dots, n.$$

As $g(z_j) \in \tilde{N}$ it is invariant under $\tilde{\sigma}$. Hence we see that

$$g(z_j) = \tilde{\sigma}(g(z_j)) = \sum_{i=1}^n c_{ij} g(z_i).$$

Consequently, $C = I_n$, and so $\tilde{\sigma} = \text{id}_N$, whence $N = \tilde{N}$ and $\text{Gal}(f) = \text{Gal}(\tilde{f})$. \square

The next result shows the existence of a linear Tschirnhaus transform which possesses a separable specialized resolvent and thus solves the problem posed at the end of the previous subsection.

Theorem 2.10. *Let $K \geq \mathbb{F}_q$ be an infinite field, $f(X) \in K[X]$ a q -additive polynomial, $V \subset K^{\text{sep}}$ the vector space of zeroes of $f(X)$ and $\mathbf{z} = (z_1, \dots, z_n)$ an \mathbb{F}_q -basis of V . Further let $\text{Gal}_{\mathbf{z}}(f) \leq G \leq \text{GL}_n(q)$, $H \leq G$ a subgroup of G and $F_H \in K[V]^H$ a G -relative H -invariant. Then there exists a q -additive polynomial $g(X) \in K[X]$ with respect to which the Tschirnhaus transform of $f(X)$ preserves the Galois group and whose specialized resolvent is separable, i.e., we have*

$$\text{Gal}_{g(\mathbf{z})}(\theta_g(f)) \cong \text{Gal}_{\mathbf{z}}(f) \quad \text{and} \quad D(\text{Res}_{G/H}^{F_H(g(\mathbf{z}))}) \neq 0.$$

Proof. Let again N denote the splitting field of $f(X)$ over K and $\Delta_q(z_1, \dots, z_n) \in \text{GL}_n(N)$ the Moore matrix with basis elements z_i of the vector space of zeroes V .

With these for $N[\mathbf{X}] := N[X_1, \dots, X_n]$ we define the ring automorphism

$$\psi : N[\mathbf{X}] \rightarrow N[\mathbf{X}], \quad X_i \mapsto T_i := \sum_{j=1}^n z_i^{q^{j-1}} X_j.$$

As $\det(\Delta_q(z_1, \dots, z_n)) \neq 0$ the T_1, \dots, T_n are also algebraically independent over N and

$$F(X) := \prod_{\mathbf{c} \in \mathbb{F}_q^n} \left(X - \sum_{i=1}^n c_i T_i \right)$$

is a (general) q -additive polynomial of degree q^n . Consequently the discriminant $D(F)$ of $F(X)$ is a non-zero polynomial in X_1, \dots, X_n , say $D(F) = h(X_1, \dots, X_n) \in N[\mathbf{X}]$. As T_1, \dots, T_n are algebraically independent over N , $\text{Res}_{G/H}^{F_H(T_1, \dots, T_n)}(X)$ is separable. So there exists a polynomial $\tilde{h}(X_1, \dots, X_n) \in N[\mathbf{X}]$ with $\tilde{h}(X_1, \dots, X_n) := D(\text{Res}_{G/H}^{F_H(T_1, \dots, T_n)}) \neq 0$. But then also the product $d(\mathbf{X}) := h(\mathbf{X}) \cdot \tilde{h}(\mathbf{X}) \in N[\mathbf{X}]$ is non-zero. As $|K| = \infty$ by assumption there exist $a_i \in K$ with $d(a_0, \dots, a_{n-1}) \neq 0$. If we now set $g(X) := \sum_{k=0}^{n-1} a_k X^{q^k}$ then the discriminants $D(\theta_g(f)) = h(a_0, \dots, a_{n-1})$ and $D(\text{Res}_{G/H}^{F_H(g(\mathbf{z}))}) = \tilde{h}(a_0, \dots, a_{n-1})$ are non-zero. Thus the claim follows by Proposition 2.9. \square

Remark. The conclusion of Theorem 2.10 remains correct for finite fields K whenever we have $|K| > m(m-1)$, where $m = (G : H)$ (see Garcia Lopez (2010), Ch. 5).

Obviously by successive specialization $X_i \mapsto a_{i-1}$ we can find in finitely many steps elements $a_0, \dots, a_{n-1} \in K$ with $d(a_0, \dots, a_{n-1}) \neq 0$. From this we finally obtain:

Corollary 2.11. *Let $K \geq \mathbb{F}_q$ and $f(X) \in K[X]$ a q -additive polynomial, then the Galois group $\text{Gal}(f)$ of $f(X)$ over K can be computed in finitely many steps.*

Proof. This follows from Theorem 2.2 by induction along a chain of maximal subgroups. To improve the separability condition step by step one has to use the auxiliary results developed in Sections 2.3 and 2.4, thus possibly moving to Tschirnhaus transforms with better separability properties. This can be achieved with finitely many calculations. \square

2.5 The Modular Dedekind Criterion

In this last section we derive also lower bounds for the Galois group of a q -additive polynomial. In the case of agreement with the upper bound from Theorem 1.9 these render superfluous the sometimes rather cumbersome application of the algorithm for the computation of Galois groups described above.

We assume here that (K, ϕ_q) is an F-field with $\mathbb{F}_q \leq K$. Further let v be a non-trivial Krull valuation on K with valuation ring \mathcal{O}_v , valuation ideal $\mathfrak{P}_v \triangleleft \mathcal{O}_v$ and residue field $k_v := \mathcal{O}_v/\mathfrak{P}_v$ (see Engler and Prestel (2005), Ch. 2.1). If K/\mathbb{F}_q is finitely generated and the transcendence degree of K/\mathbb{F}_q agrees with the rank of the valuation v , then k_v/\mathbb{F}_q is a finite extension (see Engler and Prestel (2005), Cor. 3.4.4) and thus k_v is a finite field. The canonical homomorphism $\mathcal{O}_v \rightarrow k_v$ will usually be denoted by ρ_v .

Theorem 2.12 (Modular Dedekind Criterion). *Let (K, ϕ_q) be an F-field with valuation v , valuation ring \mathcal{O}_v , valuation ideal \mathfrak{P}_v and finite residue field k with $[k : \mathbb{F}_q] = m$. Further let (M, Φ) be a dualizable F-module over K with basis $B = \{b_1, \dots, b_n\}$ and $D := D_B(\Phi) \in \mathrm{GL}_n(\mathcal{O})$. Let $D_{\mathfrak{P}} := \rho_v(D) \in \mathrm{GL}_n(K)$ denote the image of D under the canonical morphism ρ_v . Then we have:*

(a) *The Galois group $\mathrm{Gal}(M, \Phi) \leq \mathrm{GL}_n(q)$ contains elements that are $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate to*

$$\hat{D} := D_{\mathfrak{P}} \phi_q(D_{\mathfrak{P}}) \cdots \phi_q^{m-1}(D_{\mathfrak{P}}).$$

(b) *If \mathbf{G} is a connected linear algebraic group defined over \mathbb{F}_q and if D lies in $\mathbf{G}(\mathcal{O})$ then $\mathrm{Gal}(M, \Phi)$ contains an element which is $\mathbf{G}(\overline{\mathbb{F}}_q)$ -conjugate to \hat{D} .*

Proof. Let N/K be a minimal solution field of (M, Φ) and $Y := (y_{ij})_{i,j=1}^n \in \mathrm{GL}_n(N)$ a fundamental solution matrix of (M, Φ) , so that $\phi_q(Y) = D^{-1}Y$. Further let \tilde{v} be an extension of the valuation v to N with valuation ring $\tilde{\mathcal{O}}$, valuation ideal $\tilde{\mathfrak{P}}$ and residue field \tilde{k} (according to Engler and Prestel (2005), Thm. 3.1.2). As $D^{-1} \in \mathrm{GL}_n(\tilde{\mathcal{O}})$ it follows from the ultrametric triangle inequality for \tilde{v} that the y_{ij} as well as $\det(Y)$ and $\det(Y^{-1})$ lie in $\tilde{\mathcal{O}}$. So the reduction $\tilde{Y}_{\tilde{\mathfrak{P}}} := \rho_{\tilde{v}}(Y) \in \mathrm{GL}_n(\tilde{k})$ is well-defined and we have $\tilde{Y}_{\tilde{\mathfrak{P}}} = D_{\mathfrak{P}} \phi_q(Y_{\tilde{\mathfrak{P}}})$. By Corollary 1.3 the field $N_{\tilde{\mathfrak{P}}} := k(\tilde{Y}_{\tilde{\mathfrak{P}}}) \leq \tilde{k}$ is a minimal solution field of the reduced F-module $(V_{\mathfrak{P}}, \rho_v \circ \Phi)$ with the reduced vector space $V_{\mathfrak{P}} \cong k^n$.

By assumption the residue field k has finite degree m over \mathbb{F}_q . Hence $\mathrm{Gal}(N_{\tilde{\mathfrak{P}}}/k)$ is cyclic and generated by the Frobenius automorphism $\phi_{\mathfrak{P}} = \phi_q^m$. From this we obtain

$$Y_{\tilde{\mathfrak{P}}} = D_{\tilde{\mathfrak{P}}} \phi_{\mathfrak{P}}(Y_{\tilde{\mathfrak{P}}}) \quad \text{with} \quad D_{\tilde{\mathfrak{P}}} = D_{\mathfrak{P}} \phi_q(D_{\mathfrak{P}}) \cdots \phi_q^{m-1}(D_{\mathfrak{P}}).$$

Setting $C_{\tilde{\mathfrak{P}}} := Y_{\tilde{\mathfrak{P}}}^{-1} D_{\tilde{\mathfrak{P}}}^{-1} Y_{\tilde{\mathfrak{P}}}$ this gives

$$\phi_{\mathfrak{P}}(Y_{\tilde{\mathfrak{P}}}) = Y_{\tilde{\mathfrak{P}}} C_{\tilde{\mathfrak{P}}},$$

whence $C_{\tilde{\mathfrak{P}}}$ is the representing matrix of $\phi_{\mathfrak{P}}$, and $C_{\tilde{\mathfrak{P}}} \in \mathrm{GL}_n(q)$.

Now let K_h be the decomposition field of v in N/K . Then the residue class map from $\mathrm{Gal}(N/K_h)$ to $\mathrm{Gal}(\tilde{k}/k)$ is surjective (by Engler and Prestel (2005), Lemma 5.2.6). Hence the extension $\tilde{\phi}_{\mathfrak{P}} := \phi_q^m$ of $\phi_{\mathfrak{P}}$ to $\mathrm{Gal}(\tilde{k}/k)$ has a preimage $\phi \in \mathrm{Gal}(N/K_h) \leq \mathrm{Gal}(N/K)$. For this there exists a matrix $C_{\phi} \in \mathrm{GL}_n(q)$ with $\phi(Y) = Y \cdot C_{\phi}$. Via the natural epimorphism $\rho_{\tilde{v}}$ we obtain from this

$$\tilde{\phi}_{\mathfrak{P}}(Y_{\tilde{\mathfrak{P}}}) = \phi_{\mathfrak{P}}(Y_{\tilde{\mathfrak{P}}}) = Y_{\tilde{\mathfrak{P}}} C_{\phi},$$

which implies that $C_{\phi} = C_{\tilde{\mathfrak{P}}}$. Part (a) of the theorem follows.

Under the assumptions in part (b) we have $Y \in \mathbf{G}(K^{\text{sep}})$ by the Theorem II.1.1 of Lang–Steinberg. Application of the canonical map then gives $Y_{\tilde{\mathfrak{P}}} \in \mathbf{G}(\overline{\mathbb{F}}_q)$ and $\phi_{\mathfrak{P}}(Y_{\tilde{\mathfrak{P}}}) \in \mathbf{G}(\overline{\mathbb{F}}_q)$, since \mathbf{G} is defined over \mathbb{F}_q . As $C_{\tilde{\mathfrak{P}}} = Y_{\tilde{\mathfrak{P}}} D_{\tilde{\mathfrak{P}}}^{-1} Y_{\tilde{\mathfrak{P}}}$ this shows that C_ϕ is conjugate to $D_{\tilde{\mathfrak{P}}}^{-1} \in \mathbf{G}(\mathbb{F}_q)$ inside $\mathbf{G}(\tilde{k}) \leq \mathbf{G}(\overline{\mathbb{F}}_q)$. \square

Here we are particularly interested in those representing matrices D with coefficients in $\mathbb{F}_q[t_1, \dots, t_r] =: R$ and in specializations $t_i \mapsto a_i \in \mathbb{F}_q$. For this let $\mathfrak{A} := (t_1 - a_1, \dots, t_r - a_r) \triangleleft R$ be the corresponding maximal ideal and $R_{\mathfrak{A}}$ the localization of R at \mathfrak{A} with maximal ideal $\mathfrak{A}R_{\mathfrak{A}}$. Then by a theorem of Chevalley there exist valuations v on $K = \mathbb{F}_q(t_1, \dots, t_r)$ with $\mathcal{O}_v \supseteq R_{\mathfrak{A}}$ and $\mathfrak{P}_v \cap R_{\mathfrak{A}} = \mathfrak{A}R_{\mathfrak{A}} = (t_1 - a_1, \dots, t_r - a_r)$ (see e.g. Engler and Prestel (2005), Thm. 3.1.1), for example the map

$$v : \mathbb{F}_q(t_1, \dots, t_r)^\times \rightarrow \mathbb{Z}^r, \quad f(t_1, \dots, t_r) \mapsto (\text{ord}_{(t_1 - a_1)}(f), \dots, \text{ord}_{(t_r - a_r)}(f)),$$

of $\mathbb{F}_q(\mathbf{t})^\times$ into the lexicographically ordered abelian group \mathbb{Z}^r given by the multiplicities of $(t_i - a_i)$ in $f(\mathbf{t})$. For this the residue field k_v coincides with \mathbb{F}_q , so we have

$$\mathcal{O}_v/\mathfrak{P}_v = k_v \cong \mathbb{F}_q \cong R_{\mathfrak{A}}/\mathfrak{A}R_{\mathfrak{A}} \cong \mathbb{F}_q[t_1, \dots, t_r]/(t_1 - a_1, \dots, t_r - a_r).$$

In this special case we obtain from Theorem 2.12:

Corollary 2.13. *Let $K = \mathbb{F}_q(t_1, \dots, t_r)$ be a rational function field in r variables over \mathbb{F}_q with Frobenius endomorphism $\phi = \phi_q$. Further let (M, Φ) be an n -dimensional dualizable F -module over K with basis B and representing matrix $D = D_B(\Phi) \in \text{GL}_n(\mathbb{F}_q[t_1, \dots, t_r])$. Then for all $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_q^r$ with $\det(D(a_1, \dots, a_r)) \neq 0$, $\text{Gal}(M, \Phi)$ contains elements $C_{\mathbf{a}} \in \text{GL}_n(\overline{\mathbb{F}}_q)$ which are $\text{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate to $D(\mathbf{a})$.*

The group generated by the elements $C_{\mathbf{a}}$ in Corollary 2.13 usually already gives quite good lower bounds for $\text{Gal}(M, \Phi)$, as will become apparent in the following paragraphs.

As first applications we continue our Examples 1.1 to 1.3 from Paragraph 1, so again $K = \mathbb{F}_p(t)$ and $\phi = \phi_p$.

Example 2.1. First let (M, Φ) be the 1-dimensional F -module over K with $D := D_B(\Phi) = (t^{-1})$. Then a primitive element $w \in \mathbb{F}_p^\times$ also satisfies $\langle D^{-1}(w) \rangle = \mathbb{F}_p^\times$. So $\text{Gal}(M, \Phi)$ contains the group $\mathbb{G}_m(\mathbb{F}_p)$ by Theorem 2.12. \square

Example 2.2. Now let (M, Φ) be a 2-dimensional F -module over K with $D_B(\Phi) = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}$. Then $\text{Gal}(M, \Phi)$ contains by Corollary 2.13 an element conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, of order p , so it contains a copy of the group $\mathbb{G}_a(\mathbb{F}_p)$. \square

Example 2.3. Finally let (M, Φ) be the \mathbb{F} -module over K with $D := D_B(\Phi) = \begin{pmatrix} t^{-1} & -1 \\ 0 & t \end{pmatrix}$. So D lies in the Borel subgroup $B_2(\mathbb{F}_p(t))$ of upper triangular matrices in $\mathrm{SL}_2(\mathbb{F}_p(t))$. According to Theorem 1.9 the Galois group $\mathrm{Gal}(M, \Phi)$ is then a subgroup of $B_2(\mathbb{F}_p)$ with $|B_2(\mathbb{F}_p)| = p(p-1)$. As $D(1) \in \mathrm{GL}_2(\mathbb{F}_p)$ has order p and $D(w)$ has order $p-1$, we obtain that $|\mathrm{Gal}(M, \Phi)| \geq |B_2(\mathbb{F}_p)|$ and hence $\mathrm{Gal}(M, \Phi) \cong B_2(\mathbb{F}_p)$. \square

3 Polynomials for Split Groups of Lie Type

In this paragraph we construct polynomials over $\mathbb{F}_q(\mathbf{t}) = \mathbb{F}_q(t_1, \dots, t_n)$ with Galois group $\mathbf{G}(\mathbb{F}_q)$ a split group of Lie type, where \mathbf{G} is one of the linear groups SL_{n+1} , Sp_{2n} , SO_{2n+1} , SO_{2n} or G_2 respectively. For this we utilize Frobenius modules whose representing matrix lies in the natural representation of \mathbf{G} over $\mathbb{F}_q(\mathbf{t})$ and which is sufficiently general. The results presented here are mostly taken from the thesis of Albert and form part of the joint publication Albert and Maier (2011).

3.1 Linear Groups SL_{n+1}

We start with some preparatory observations. For the construction of sufficiently general representing matrices $D = D_B(\Phi)$ in $\mathbf{G}(\mathbb{F}_q(t_1, \dots, t_n))$ we use so-called Steinberg cross sections. Their importance is demonstrated by the following result, which we will not prove here as it is not used in the sequel (see Steinberg (1965), Thm. 1.4).

Theorem 3.1 (Steinberg cross section). *Let \mathbf{G} be a (connected) semisimple linear algebraic group of simply connected type of rank n over a field k , $\mathbf{T} \leq \mathbf{G}$ a maximal torus and $\alpha_1, \dots, \alpha_n$ a system of simple roots of \mathbf{G} with respect to \mathbf{T} with $\omega_1, \dots, \omega_n \in N_{\mathbf{G}}(\mathbf{T})$ mapping to the corresponding simple reflections in the Weyl group $N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$, and with corresponding root subgroups $\mathbf{X}_1, \dots, \mathbf{X}_n \leq \mathbf{G}$. Then*

$$S := \prod_{i=1}^n \mathbf{X}_i \omega_i := \mathbf{X}_1 \omega_1 \cdots \mathbf{X}_n \omega_n$$

contains representatives of all regular conjugacy classes of \mathbf{G} .

The set S in Theorem 3.1 will be called a *Steinberg cross section of \mathbf{G}* . As an algebraic variety it is isomorphic to an n -dimensional k -vector space (Steinberg (1965), Thm. 7.1). In the sequel we will only use its construction. The property of being a section then offers a good chance to find sufficiently general specializations. This will be verified explicitly in each application.

Remark. According to Theorem 3.1 the set S is an n -parameter family $S(t_1, \dots, t_n)$ in $\mathbf{G}(\overline{\mathbb{F}_q})$, and so can be considered as an element of $\mathbf{G}(\mathbb{F}_q(\mathbf{t}))$.

As an easy example we first compute a Steinberg cross section of SL_{n+1} .

Proposition 3.2. *The group $\mathbf{G}_{A_n} := \mathrm{SL}_{n+1}$ possesses a Steinberg cross section of the form*

$$S_{A_n}(t_1, \dots, t_n) = \begin{pmatrix} -t_1 & \dots & -t_n & 1 \\ -1 & & & 0 \\ & \ddots & & \vdots \\ & & -1 & 0 \end{pmatrix}$$

with characteristic polynomial

$$h_{A_n}(t_1, \dots, t_n) = X^{n+1} + \sum_{i=1}^n (-1)^{i-1} t_i X^{n+1-i} + (-1)^{n+1}.$$

Proof. According to Section II.1.2, the $\epsilon_i - \epsilon_{i-1}$, $1 \leq i \leq n$, form a system of simple roots for a root system of type A_n . The corresponding root subgroups have the form $X_i = X_{i,i+1} = \{\text{Id} + t_i I_{i,i+1} \mid t_i \in \mathbb{F}_q\}$ with Weyl group representatives $\omega_i = \text{diag}(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 1, \dots, 1)$, where the block of size 2 occurs in positions $(i, i+1)$. With this we get

$$X_i(t_i)\omega_i = \text{diag}(1, \dots, 1, \begin{pmatrix} -t_i & 1 \\ -1 & 0 \end{pmatrix}, 1, \dots, 1)$$

again with the 2-block at positions $(i, i+1)$. From this induction over j yields

$$S_j := \prod_{i=1}^j X_i(t_i)\omega_i = \begin{pmatrix} -t_1 & \dots & -t_j & 1 \\ -1 & & & 0 \\ \ddots & & \vdots & \\ & -1 & 0 & \\ & & 1 & 0 \\ & & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

and thus for $j = n$ the expression for $S_{A_n}(t_1, \dots, t_n)$ as claimed. The computation of the characteristic polynomial is straightforward. \square

To be able to successfully apply the Modular Dedekind Criterion we need generating systems $(\gamma_1, \dots, \gamma_s)$ of $G(\mathbb{F}_q)$ with the property that for all $\text{GL}_n(\overline{\mathbb{F}}_q)$ -conjugates $\tilde{\gamma}_i \in G(\mathbb{F}_q)$ of γ_i the tuple $(\tilde{\gamma}_1, \dots, \tilde{\gamma}_s)$ also generates $G(\mathbb{F}_q)$. Such generating systems will be called *robust* (with respect to $\text{GL}_n(\overline{\mathbb{F}}_q)$). Such a robust generating system $(\gamma_1, \dots, \gamma_s) \in G(\mathbb{F}_q)^s$ occurs for example if there exists no proper subgroup of $G(\mathbb{F}_q)$ containing elements with all element orders occurring for $\gamma_1, \dots, \gamma_n$. For the groups $G_{A_n}(\mathbb{F}_q)$ robust systems are provided by the next result which essentially goes back to Malle, Saxl and Weigel (1994).

Proposition 3.3. *Let $n \geq 1$ and q be a prime power.*

- (a) *The group $G_{A_n}(\mathbb{F}_q) = \text{SL}_{n+1}(q)$ possesses cyclic maximal tori T_1 and T_2 of orders $(q^{n+1}-1)/(q-1)$ and q^n-1 respectively.*
- (b) *For $(n, q) \notin \{(1, 2), (1, 3), (1, 4), (1, 7), (1, 9)\}$ pairs (γ_1, γ_2) of generators of T_1, T_2 form robust generating systems of $G_{A_n}(\mathbb{F}_q)$.*
- (c) *In the cases excluded in (b), a robust system $(\gamma_1, \gamma_2, \gamma_3)$ is obtained by adding an element γ_3 of order $\gcd(2, p-1)p$.*

Proof. We first consider the case $n = 1$, that is, the groups $\text{SL}_2(q)$. Then assertions (a) and (b) easily follow from the Theorem of Dickson (see Huppert (1967),

Kap. II, Satz 8.27), since by order considerations no proper subgroups can contain conjugates of both γ_1, γ_2 . In the excluded cases the same holds using a third element γ_3 of order $\gcd(2, p-1)p$.

In the general case $n > 1$ part (a) follows from Malle, Saxl and Weigel (1994), Tab. III, and part (b) from Malle, Saxl and Weigel (1994), proof of Thm. 3.1 (second paragraph). In the special case of $\mathrm{SL}_4(2) \cong A_8$ the elements γ_1, γ_2 have orders 7, 15 respectively, which again cannot both lie in a proper subgroup. \square

This allows us to prove the following result:

Theorem 3.4. *Let $n \geq 1$.*

- (a) *The Frobenius module (M_{A_n}, Φ) over $K = \mathbb{F}_q(t_1, \dots, t_n)$ with representing matrix $D_B(\Phi) = S_{A_n}(t_1, \dots, t_n)$ is dualizable.*
- (b) *The Galois group of M_{A_n}, Φ is $\mathrm{SL}_{n+1}(q)$.*
- (c) *The corresponding Galois extension $N/\mathbb{F}_q(\mathbf{t})$ is geometric and generated by the zeroes of the characteristic polynomial of (M_{A_n}, Φ)*

$$f_{A_n}(X) = X^{q^n+1} + \sum_{i=1}^n (-1)^i t_i X^{q^i} + (-1)^{n+1} X.$$

Proof. The F-module (M_{A_n}, Φ) is dualizable as $\det(S_{A_n}(\mathbf{t})) \neq 0$ by Proposition 3.2. By Theorem 1.9 its Galois group $G := \mathrm{Gal}(M_{A_n}, \Phi)$ is a subgroup of $\mathrm{SL}_{n+1}(q)$ since $S_{A_n}(\mathbf{t}) \in \mathbf{G}_{A_n}(\mathbb{F}_q(\mathbf{t}))$.

The generators γ_1, γ_2 from Proposition 3.3 possess the Jordan normal forms $\mathrm{diag}(v, v^q, \dots, v^{q^n})$ over $\overline{\mathbb{F}}_q$ with an element $v \in \overline{\mathbb{F}}_q^\times$ of order $(q^{n+1}-1)/(q-1)$, respectively $\mathrm{diag}(w, w^q, \dots, w^{q^{n-1}}, w^{-\frac{q^n-1}{q-1}})$ with w of order q^n-1 . Consequently the conjugacy classes of γ_1 and γ_2 in $\mathbf{G}(\overline{\mathbb{F}}_q)$ are both determined by their characteristic polynomials $h_j(X)$, $j = 1, 2$. Write

$$h_j(X) = X^{n+1} + \sum_{i=1}^n (-1)^{i+1} c_{ij} X^{n+1-i} + (-1)^{n+1}$$

with coefficient vector $\mathbf{c}_j = (c_{1j}, \dots, c_{nj}) \in \mathbb{F}_q^n$. Specializing $\mathbf{t} = (t_1, \dots, t_n)$ in $h_{A_n}(\mathbf{t})$ to \mathbf{c}_j we obtain that $S_{A_n}(\mathbf{c}_j) = D(\mathbf{c}_j)$ is a $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate of γ_j , hence also a generator of a torus conjugate to T_j . Apart from the listed exceptions these form a robust generating system for $\mathrm{SL}_{n+1}(q)$ by Proposition 3.3.

In the special cases we have $n = 1$. Then the specialization $S_{A_1}(\pm 2) = D(\pm 2)$ leads to an element γ_3 conjugate to $\begin{pmatrix} \pm 2 & 1 \\ -1 & 0 \end{pmatrix}$. Since its characteristic polynomial equals $h_3(X) = X^2 \pm 2X + 1$ and $\gamma_3^2 \neq I_2$ in case of odd characteristic, γ_3 has order $2p$, respectively p in characteristic 2. Thus here (b) follows from Proposition 3.3(c).

It remains to calculate the characteristic polynomial of (M_{A_n}, Φ) . This is obtained from the non-linear system of equations

$$S_{A_n}(\mathbf{t})(X_1^q, \dots, X_{n+1}^q)^t = (X_1, \dots, X_{n+1})^t$$

by solving for $X := X_1$. We have

$$\begin{aligned} -\sum_{i=1}^n t_i X_i^q + X_{n+1}^q &= X_1 = X \quad \text{and} \\ -X_i^q &= X_{i+1} \quad \text{resp.} \quad X_{i+1} = (-1)^i X^{q^i} \quad \text{for } i = 1, \dots, n. \end{aligned}$$

From this we conclude that

$$-\sum_{i=1}^n t_i (-1)^{i-1} X^{q^i} + (-1)^n X^{q^{n+1}} = X,$$

which is the polynomial given in (b).

The geometricity of $N/\mathbb{F}_q(\mathbf{t})$ finally follows from the fact that all specializations used in the proof are compatible with extensions of constants and thus the elements generate the same group after extension of constants. \square

Remark. By the Hilbert irreducibility theorem (Theorem IV.1.1) Theorem 3.4 also yields Galois extensions over $\mathbb{F}_q(t)$ with Galois group $\mathrm{SL}_{n+1}(q)$. In the non-exceptional cases of Proposition 3.3 such extensions can very easily be given explicitly, for example by the specialization

$$t_i \mapsto c_{i1} + t(c_{i2} - c_{i1})$$

(in the notation of the previous proof). Indeed, after the further specialization $t \mapsto 0$, respectively $t \mapsto 1$ we arrive at the robust generators γ_1, γ_2 .

Corollary 3.5. *The fixed field of the center $\mathcal{Z}(\mathrm{SL}_{n+1}(q))$ in the Galois extension N/K in Theorem 3.4 is a Galois extension over $\mathbb{F}_q(\mathbf{t})$ with group $\mathrm{L}_{n+1}(q)$. It is generated over K by the roots of*

$$\bar{f}_{A_n}(Y) = Y^{\frac{q^{n+1}-1}{q-1}} + \sum_{i=1}^n (-1)^i t_i Y^{\frac{q^i-1}{q-1}} + (-1)^{n+1}.$$

Proof. The irreducible polynomial $\bar{f}_{A_n}(Y)$ arises by dividing $f_{A_n}(Y)$ by X and then substituting X^{q-1} by Y . Let L be the intermediate field generated by the roots of $\bar{f}_{A_n}(Y)$. Since $\mathcal{Z}(\mathrm{SL}_{n+1}(q))$ acts on the root space V of $f_{A_n}(Y)$ by scalar multiplication with suitable elements $c \in \mathbb{F}_q^\times$, it acts trivially on the roots of $\bar{f}_{A_n}(Y)$. Hence L is contained in the fixed field of $\mathcal{Z}(\mathrm{SL}_{n+1}(q))$, and its non-trivial Galois group is a factor group of $\mathrm{SL}_{n+1}(q)/\mathcal{Z}(\mathrm{SL}_{n+1}(q))$, so $\mathrm{Gal}(L/K) \cong \mathrm{L}_{n+1}(q)$. \square

The polynomial $f_{A_n}(X)$ in Theorem 3.4(c) is obtained from the Dickson polynomial (2.1) by specializing the Dickson invariant d_{n+1} to $(-1)^{n+1}$. (The specialization $d_{n+1} \mapsto (-1)^{n+1} t_{n+1}^{q-1}$ would lead to a generic polynomial for $\mathrm{SL}_{n+1}(q)$). This follows from the Theorem of Dickson (Smith (1995), Thm. 8.1.1) that

$$\mathbb{F}_q[V]^{\mathrm{SL}_{n+1}(q)} = \mathbb{F}_q[d_1, \dots, d_n, g_{n+1}] \quad \text{with} \quad g_{n+1}^{q-1} = d_{n+1}$$

in combination with a result of Kemper and Mattig on generic polynomials explained in Jensen, Ledet and Yui (2002), Prop. 1.1.3.)

Further specializations $t_i \mapsto 0$ for $i = 1, \dots, n-1$ in $f_{A_n}(X)$ and $\tilde{f}_{A_n}(Y)$ respectively give the nice $\mathrm{SL}_{n+1}(q)$ - and $\mathrm{L}_{n+1}(q)$ -polynomials of Abhyankar (1994).

3.2 Symplectic Groups

We next turn our attention to the symplectic groups $\mathrm{Sp}_{2n}(q)$, $n \geq 2$, with q any prime power. First we construct a Steinberg cross section.

Proposition 3.6. *The groups $\mathbf{G}_{C_n}(\mathrm{IF}_q) := \mathrm{Sp}_{2n}(q)$ possess a Steinberg cross section of the form*

$$S_{C_n}(t_1, \dots, t_n) = \left(\begin{array}{cc|cc} -t_1 & \dots & -t_{n-1} & -t_n & 1 \\ 1 & & & & \\ & \ddots & & & \\ & & 1 & 0 & \\ \hline & & & -t_{n-1} & 0 \ 1 \\ & & & \vdots & \ddots \ \ddots \\ & & -t_1 & & 1 \\ & & -1 & & 0 \end{array} \right).$$

Its characteristic polynomial is given by the symmetric polynomial

$$h_{C_n}(X) = X^{2n} + \sum_{i=1}^{n-1} t_i X^{2n-i} + t_n X^n + \sum_{i=1}^{n-1} t_i X^i + 1.$$

Proof. In the groups $\mathbf{G}_{C_n} = \mathrm{Sp}_{2n}$ the root subgroups and corresponding simple reflections for $i = 1, \dots, n-1$ have the form

$$\mathbf{X}_i(t_i) = \mathrm{diag}(1, \dots, 1, \begin{pmatrix} 1 & -t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1),$$

$$\omega_i = \mathrm{diag}(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1),$$

where the 2-blocks are at position $(i, i+1)$, and symmetrically at $(2n-i-1, 2n-i)$. For $i = n$ we have

$$\mathbf{X}_n(t_n) = \mathrm{diag}(1, \dots, 1, \begin{pmatrix} 1 & t_n \\ 0 & 1 \end{pmatrix}, 1, \dots, 1),$$

$$\omega_n = \mathrm{diag}(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1),$$

with the 2-block in middle position $(n, n+1)$ (see Digne and Michel (1991), §15.2). From this we obtain

$$\mathbf{X}_i(t_i)\omega_i = \text{diag}(1, \dots, 1, \begin{pmatrix} -t_i & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} t_i & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1), \quad \text{for } i < n,$$

respectively

$$\mathbf{X}_n(t_n)\omega_n = \text{diag}(1, \dots, 1, \begin{pmatrix} t_n & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1).$$

Induction then easily gives the stated expression for $S_{C_n}(t_1, \dots, t_n)$.

To calculate the characteristic polynomial of $S_{C_n}(t_1, \dots, t_n)$ we first eliminate the strictly lower triangular entries in the upper left hand and the lower right hand block to obtain a matrix

$$\tilde{C} = \begin{pmatrix} g_1 & t_2 & \dots & t_n & -1 \\ g_2 & & * & * & \\ \ddots & & \vdots & \vdots & \\ & g_n & -1 & & \\ h_{n-1} & X^n & & & \\ \vdots & & \ddots & & \\ h_0 & & & & X \end{pmatrix}$$

with $t_0 := 1$, $g_i := \sum_{j=0}^i t_j X^{i-j}$ and $h_i := \sum_{j=0}^i t_j X^j$. Under consideration of the factors used for the twofold triangulation this leads to

$$h_{C_n}(X) = \det \begin{pmatrix} g_n & -1 \\ h_{n-1} & X^n \end{pmatrix} = X^n \sum_{i=0}^n t_i X^{n-1} + \sum_{i=1}^{n-1} t_i X^i$$

which is the claimed expression. \square

A robust generating system for $\text{Sp}_{2n}(q)$ can be deduced from Guralnick and Malle (2012):

Proposition 3.7. *Let $n \geq 3$.*

(a) *The group $G_{C_n}(\mathbb{F}_q) = \text{Sp}_{2n}(q)$ possesses maximal tori T_1, T_2 of orders $q^n + 1$ and $(q^{n-1} + 1)(q + 1)$ respectively.*

(b) *Any pair (γ_1, γ_2) of regular elements of T_1, T_2 of maximal order forms a robust generating pair.*

Proof. The existence of maximal tori of the given orders is immediate by Malle and Testerman (2011), Prop. 25.3, for example. The assertion in (b) follows from Guralnick and Malle (2012), Cor. 3.4. Indeed, let H be generated by γ_1, γ_2 as in the statement. As $n \geq 3$ any two elements of the given orders generate an irreducible subgroup of $\text{GL}_{2n}(q)$. Easy order considerations show that the only possibility for H is as in Guralnick and Malle (2012), Cor. 3.4(1). As by assumption $H \leq \text{Sp}_{2n}(q)$, we either have $H = \text{Sp}_{2n}(q)$ as claimed, or q is even and $H \leq \text{GO}_{2n}^\pm(q)$. But the order of $\text{GO}_{2n}^+(q)$ is not divisible by $q^n + 1$, while

$\mathrm{GO}_{2n}^-(q)$ does not contain tori of order $(q^{n-1} + 1)(q + 1)$ (see again Malle and Testerman (2011), Prop. 25.3), hence no regular elements with that centralizer. Note that γ_1 has Jordan normal form $\mathrm{diag}(v, v^q, \dots, v^{q^{n-1}}, v^{-q^{n-1}}, \dots, v^{-q}, v^{-1})$ over $\overline{\mathbb{F}}_q$ for some element $v \in \overline{\mathbb{F}}_q^\times$ of orders $q^n + 1$, while γ_2 has Jordan normal form $\mathrm{diag}(v, v^q, \dots, v^{q^{n-2}}, w, w^{-1}, v^{-q^{n-2}}, \dots, v^{-q}, v^{-1})$ for suitable elements $v, w \in \overline{\mathbb{F}}_q^\times$ of orders $q^{n-1} + 1, q + 1$ respectively. \square

With these preparations we are in a position to prove the Galois realizations:

Theorem 3.8. *Let $n \geq 3$.*

- (a) *The Frobenius module (M_{C_n}, Φ) over $K = \mathbb{F}_q(t_1, \dots, t_n)$ with representing matrix $D_B(\Phi) = S_{C_n}(t_1, \dots, t_n)$ is dualizable.*
- (b) *The Galois group of (M_{C_n}, Φ) is $\mathrm{Sp}_{2n}(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial of (M_{C_n}, Φ)*

$$f_{C_n}(X) = X^{q^{2n}} + \sum_{i=1}^{n-1} t_{n-i}^{q^i} X^{q^{n+i}} + t_n X^{q^n} + \sum_{i=1}^{n-1} t_i X^{q^i} + X.$$

Proof. From Proposition 3.6 we see that (M_{C_n}, Φ) is dualizable and $\mathrm{Sp}_{2n}(q)$ is an upper bound for its Galois group. The elements γ_1, γ_2 from Proposition 3.7(b) yield a robust generating system of $\mathrm{Sp}_{2n}(q)$. According to the proof of Proposition 3.7 not only h_{C_n} but also the characteristic polynomials of γ_1 and γ_2 possess symmetric coefficients; so the t_i can be specialized so that h_{C_n} becomes the characteristic polynomial of γ_1 or γ_2 . This yields elements that are $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate to the γ_i .

It remains to compute the characteristic polynomial of (M_{C_n}, Φ) . It is obtained from the algebraic system of equations

$$S_{C_n}(X_1^q, \dots, X_{2n}^q)^t = (X_1, \dots, X_{2n})^t$$

by solving for $X := X_1$. The individual equations yield

$$-\sum_{i=1}^n t_i X_i^q - t_n X_n^q + X_{n+1}^q = X_1 = X,$$

$$X_{i-1}^q = X_i \quad \text{resp.} \quad X_i = X^{q^{i-1}} \quad \text{for } i = 1, \dots, n,$$

$$-t_{n-i} X_n^q + X_{n+i+1}^q = X_{n+i} \quad \text{for } i = 1, \dots, n-1,$$

$$-X_n^q = X_{2n} \quad \text{resp.} \quad X_{2n} = -X^{q^n}.$$

From this we get by induction

$$\begin{aligned} X_{2n-j} &= - \sum_{i=0}^{j-1} t_{j-i}^{q^i} X^{q^{n+i}} - X^{q^{n+j}} \quad \text{for } j = 0, \dots, n-1, \\ X_{n+1} &= - \sum_{i=0}^{n-1} t_{n-i}^{q^{i-1}} X^{q^{n+i-1}} - X^{q^{2n-1}}. \end{aligned}$$

Substitution into the first equation then yields the stated characteristic polynomial. The geometricity of the Galois extension follows as in Theorem 3.4. \square

Corollary 3.9. *The fixed field of the center $\mathcal{L}(\mathrm{Sp}_{2n}(q))$ in the Galois extension N/K in Theorem 3.8 gives a Galois extension over $\mathbb{F}_q(t)$ with group $S_{2n}(q)$. It is generated over K by the roots of the projective version $\tilde{f}_{C_n}(Y)$ of $f_{C_n}(X)$ which arises by dividing $f_{C_n}(X)$ by X and substituting Y for X^{q-1} .*

The nice polynomials of Abhyankar (1996b) for $\mathrm{Sp}_{2n}(q)$ and $S_{2n}(q)$ over $\mathbb{F}_q(t, u)$ can be obtained from $f_{C_n}(X)$ respectively $\tilde{f}_{C_n}(Y)$ by specializing $t_i \mapsto 0$ for $i = 1, \dots, n-2$ (see also Abhyankar and Loomis (1998, 1999)).

We close by pointing out that Elkies (1997), using a completely different method, obtained essentially the same polynomial for $\mathrm{Sp}_{2n}(q)$.

3.3 Odd-Dimensional Orthogonal Groups

Here we consider the groups $\mathrm{SO}_{2n+1}(q)$. As $\mathrm{SO}_{2n+1}(2^l) \cong \mathrm{Sp}_{2n}(2^l)$ we may restrict ourselves to the case of odd q . We start again with the construction of a Steinberg cross section. For this we introduce an additional parameter s which will allow us later to find specializations into suitable classes modulo squares.

Proposition 3.10. *The groups $\mathrm{G}_{B_n}(\mathbb{F}_q) = \mathrm{SO}_{2n+1}(q)$ with q odd possess a Steinberg cross section of the form*

$$S_{B_n}(t_1, \dots, t_n, s) = \left(\begin{array}{cc|c} -t_1 & -st_2 & \dots & -st_{n-1} & \frac{s}{2}t_n^2 & st_n & -s \\ 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & 0 & & \\ & & & & -t_n & -1 & \\ \hline & & & & -t_{n-1} & 0 & 0 & 1 \\ & & & & \vdots & & & \ddots \\ & & & & -\frac{t_1}{s} & & & 1 \\ \hline & & & & -\frac{1}{s} & & & 0 \end{array} \right).$$

Its characteristic polynomial $h_{B_n}(X)$ has the anti-symmetric form

$$\frac{1}{s} h_{B_n}(X) = \sum_{i=0}^n (s_{i-1} + s_i) X^{2n+1-i} - \sum_{i=0}^n (s_{i-1} + s_i) X^i$$

with $s_{-1} = 0$, $s_0 = \frac{1}{s}$, $s_1 = \frac{t_1}{s}$, $s_i = t_i$ for $i = 2, \dots, n-1$ and $s_n = \frac{1}{2}t_n^2$.

Proof. For the computation of the Steinberg cross section we use the root subgroups

$$X_i(t_i) = \text{diag}(1, \dots, 1, \begin{pmatrix} 1 & -t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1), \quad \text{for } i = 1, \dots, n-1,$$

$$X_n(t_n) = \text{diag}(1, \dots, 1, \begin{pmatrix} 1 & -t_n & -\frac{1}{2}t_n^2 \\ 0 & 1 & t_n \\ 0 & 0 & 1 \end{pmatrix}, 1, \dots, 1)$$

with the 2-blocks at positions $(i, i+1)$ and symmetrically at $(2n+1-i, 2n+2-i)$, and the 3-block at position $(n, n+1, n+2)$. As representatives for the simple reflections we choose

$$\omega_1 = \text{diag}(\begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 0 & 1 \\ \frac{1}{s} & 0 \end{pmatrix}),$$

$$\omega_i = \text{diag}(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1), \quad \text{for } i = 2, \dots, n-1,$$

and

$$\omega_n = \text{diag}(1, \dots, 1, \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, 1, \dots, 1).$$

Here, the 2-blocks are in positions $(i, i+1)$ and $(2n+1-i, 2n+2-i)$, and the 3-block is in the central position $(n, n+1, n+2)$. From this an easy induction yields the claimed expression for the Steinberg cross section.

The characteristic polynomial of $S_{B_n}(t_1, \dots, t_n, s)$ can be computed as shown in the proof of Proposition 3.7. After suitable transformations we obtain

$$\begin{aligned} h_{B_n}(X) &= \det \begin{pmatrix} g_n & -st_n & s \\ t_n & X+1 & 0 \\ h_{n-1} & 0 & X^n \end{pmatrix} \\ &= g_n(X)(X+1)X^n - st_n^2 X^n - s(X+1)h_{n-1}(X) \\ &= \left(\sum_{i=0}^n ss_i X^{n-i} \right) (X+1)X^n - 2ss_n X^n - s(X+1) \left(\sum_{i=0}^{n-1} s_i X^i \right) \end{aligned}$$

with the corresponding g_n, h_{n-1} . □

Next, we need a robust system of generators.

Proposition 3.11. Let q be odd and $n \geq 3$.

- (a) The groups $\mathbf{G}_{\mathrm{B}_n}(\mathrm{IF}_q) = \mathrm{SO}_{2n+1}(q)$ possess cyclic maximal tori $\mathsf{T}_1, \mathsf{T}_2$ of orders $q^n + 1, q^n - 1$ respectively.
- (b) Any pair of generators (γ_1, γ_2) of T_1 and T_2 is a robust generating system of $\mathbf{G}_{\mathrm{B}_n}(\mathrm{IF}_q)$.

Proof. Part (a) follows from Malle, Saxl and Weigel (1994), Tab. III. Generators γ_i of T_i have Jordan normal form $\mathrm{diag}(v, v^q, \dots, v^{q^{n-1}}, 1, v^{-q^{n-1}}, \dots, v^{-q}, v^{-1})$ over $\overline{\mathrm{IF}}_q$ for elements $v \in \overline{\mathrm{IF}}_q^\times$ of orders $q^n + 1, q^n - 1$ respectively. Part (b) then follows from Malle, Saxl and Weigel (1994), proof of Thm. 3.1 (fourth paragraph). \square

After these preparations the proof of the next result proceeds as usually.

Theorem 3.12. Let q be odd and $n \geq 3$.

- (a) The F -module (M_{B_n}, Φ) over $K = \mathrm{IF}_q(t_1, \dots, t_n, s)$ with the representing matrix $D_B(\Phi) = S_{\mathrm{B}_n}(t_1, \dots, t_n, s)$ is dualizable.
- (b) The Galois group of (M_{B_n}, Φ) is $\mathrm{SO}_{2n+1}(q)$.
- (c) The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial $f_{\mathrm{B}_n}(X)$ of (M_{B_n}, Φ) , given by

$$\begin{aligned} s^{-q} f_{\mathrm{B}_n}(X) = & - \sum_{i=0}^n (s_{i-1}^q + t_n^{q-1} s_i) X^{q^i} + (t_{n-1}^q t_n^{q-1} - \frac{1}{2} t_n^{2q}) X^{q^{n+1}} \\ & + \sum_{i=2}^{n+1} (s_{n-i+1}^{q^i} + t_n^{q-1} s_{n-i}^{q^i}) X^{q^{n+i}} \end{aligned}$$

with the s_i from Proposition 3.10.

Proof. Part (a) and the assertion that the group $\mathrm{SO}_{2n+1}(q)$ is an upper bound for the Galois group follow directly from Proposition 3.11 and Theorem 1.9.

From the shape of the Jordan normal forms of γ_1 and γ_2 given in the proof of Proposition 3.11 it is immediate that the characteristic polynomials of γ_1 and γ_2 are anti-symmetric. As $h_{\mathrm{B}_n}(X)$ is not generically anti-symmetric, it still remains to verify that it specializes to both of these characteristic polynomials. For this let

$$h(X) = X^{2n+1} + \sum_{i=0}^{n-1} a_i X^{2n-i} + a_n X^n - \sum_{i=0}^{n-1} a_i X^i - 1$$

be the characteristic polynomial of γ_1 or γ_2 . Then specialization of the coefficients of $h_{\mathrm{B}_n}(X)$ leads to the system of equations

$$\begin{aligned} a_1 &= 1 + t_1, \quad a_2 = 1 + st_2, \\ a_i &= s(t_{i-1} + t_i) \text{ for } i = 3, \dots, n-1 \text{ and } a_n = st_{n-1} + \frac{1}{2} st_n^2. \end{aligned}$$

The first $n-1$ of these equations can be solved inductively for the t_i , and the last one is of the form $\frac{s}{2} t_n^2 = u \in \mathrm{IF}_q$. By a suitable choice of the class of s modulo squares, we can also guarantee this latter condition.

The geometricity of N/K follows as in the proof of Theorem 3.4. The computation of the characteristic polynomial $f_{B_n}(X)$ from

$$S_{B_n}(X_1^q, \dots, X_{2n+1}^q)^t = (X_1, \dots, X_{2n+1})^t$$

is achieved according to the example in the proof of Theorem 3.8. \square

3.4 Even-Dimensional Orthogonal Groups $SO_{2n}^+(q)$

For the even-dimensional orthogonal groups $SO_{2n}^+(q)$ for simplicity we will only consider the case when q is odd. Moreover, whenever convenient we will assume that $n \geq 4$, since in smaller rank the groups are either not simple or isomorphic to other groups treated before. As in the odd-dimensional case we introduce an additional parameter for the Steinberg cross section, which originates from the freedom of choice of Weyl group representatives.

Proposition 3.13. *For odd q the group $G_{D_n}(\mathbb{F}_q) = SO_{2n}^+(q)$ possesses a Steinberg cross section $S_{D_n}(t_1, \dots, t_n, s)$ of the form*

$$\left(\begin{array}{cccccc|cc} -t_1 & -st_2 & \dots & -st_{n-2} & -st_{n-1} & t_n & st_n & -st_{n-1} & -s \\ 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & t_n & 0 & & 1 & \\ \hline & & & & -t_{n-1} & 1 & 0 & 0 & \\ & & & & -t_{n-2} & & 0 & 1 & \\ & & & & \vdots & & & \ddots & \ddots \\ & & & & -\frac{t_1}{s} & & & 0 & 1 \\ & & & & -\frac{1}{s} & & & & 0 \end{array} \right).$$

Its characteristic polynomial $h_{D_n}(X)$ has the symmetric form

$$\frac{1}{s} h_{D_n}(X) = \sum_{i=0}^{n-1} (s_i - s_{i-2}) X^{2n-i} - (2t_{n-2} + t_{n-1}^2 + t_n^2) X^n + \sum_{i=0}^{n-1} (s_i - s_{i-2}) X^i$$

with $s_{-2} = s_{-1} = 0$, $s_0 = \frac{1}{s}$, $s_1 = \frac{t_1}{s}$, $s_i = t_i$ for $i = 2, \dots, n-2$ and $s_{n-1} = t_{n-1} t_n$.

Proof. Proceeding as for Proposition 3.10 we first choose root subgroups

$$X_i(t_i) = \text{diag}(1, \dots, 1, \begin{pmatrix} 1 & -t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}, 1, \dots, 1), \quad \text{for } i = 1, \dots, n-1,$$

$$\mathbf{X}_n(t_n) = \text{diag}(1, \dots, 1, \begin{pmatrix} 1 & 0 & -t_n & 0 \\ 0 & 1 & 0 & t_n \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, 1, \dots, 1),$$

as well as

$$\omega_1 = \text{diag}\left(\begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 0 & 1 \\ \frac{1}{s} & 0 \end{pmatrix}\right),$$

$$\omega_i = \text{diag}(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1), \quad \text{for } i = 2, \dots, n-1,$$

and

$$\omega_n = \text{diag}(1, \dots, 1, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, 1, \dots, 1)$$

with the 2-blocks at positions $(i, i+1)$ and symmetrically at $(2n-i, 2n+1-i)$, respectively with a 4-block in the middle position (see Malle and Testerman (2011), Ex. 11.7). From this an easy induction yields $S_j := \mathbf{X}_1(t_1)\omega_1 \cdots \mathbf{X}_j(t_j)\omega_j$ for $j = 1, \dots, n-1$ and thus finally $S_n = S_{D_n}(t_1, \dots, t_n, s)$ as given above.

Performing the transformation described in Proposition 3.6 one obtains the characteristic polynomial

$$h_{D_n}(X) = \det \begin{pmatrix} g_{n-1} & -st_n & st_{n-1} & s \\ -t_n & X & -1 & 0 \\ t_{n-1} & -1 & X & 0 \\ h_{n-2} & 0 & 0 & X^{n-1} \end{pmatrix}$$

of $S_{D_n}(X)$ with

$$g_{n-1}(X) = s \sum_{i=0}^{n-1} s_i X^{n-1-i} \quad \text{and} \quad h_{n-2}(X) = \sum_{i=0}^{n-2} s_i X^i,$$

which equals

$$(X^{n+1} - X^{n-1})g_{n-1}(X) - s(t_n^2 + t_{n-1}^2)X^n + 2st_n t_{n-1} X^{n-1} - s(X^2 - 1)h_{n-2}(X).$$

Expanding gives the claimed formula. \square

Robust generating systems for G_{D_n} are given as follows:

Proposition 3.14. *Let $n \geq 4$ and q be odd.*

(a) *The group $G_{D_n}(\mathbb{F}_q) = \text{SO}_{2n}^+(q)$ has maximal tori T_1, T_2 of orders $(q^{n-1} + 1) \cdot (q + 1)$ and $q^n - 1$ when n is odd, respectively of orders $(q^{n-1} + 1)(q + 1)$ and $(q^{\frac{n}{2}} + (-1)^{\frac{n}{2}})^2$ when n is even.*

(b) *Any two elements γ_1 of T_1 and γ_2 of T_2 of maximal order form a robust generating system of G_{D_n} .*

Proof. The existence of the T_i follows from Malle, Saxl and Weigel (1994), Tab. III. The first torus, which we consider for all n , is generated by elements γ_1 with Jordan normal form $\text{diag}(v, v^q, \dots, v^{q^{n-2}}, w, w^{-1}, v^{-q^{n-2}}, \dots, v^{-1})$ over $\overline{\mathbb{F}}_q$, where $v, w \in \overline{\mathbb{F}}_q^\times$ have orders $q^{n-1} + 1$ and $q + 1$ respectively. (In particular T_1 is not cyclic.) For odd n the second torus T_2 is cyclic, generated by elements γ_2 with Jordan normal form $\text{diag}(v, \dots, v^{q^{n-1}}, v^{-q^{n-1}}, \dots, v^{-1})$ over $\overline{\mathbb{F}}_q$, where $v \in \overline{\mathbb{F}}_q^\times$ has order $q^n - 1$. For even n , T_2 is generated by elements γ_2 with Jordan normal form

$$\text{diag}(v, v^q, \dots, v^{q^{\frac{n}{2}-1}}, w, \dots, w^{q^{\frac{n}{2}-1}}, w^{-q^{\frac{n}{2}-1}}, \dots, w^{-1}, v^{-q^{\frac{n}{2}-1}}, \dots, v^{-1})$$

over $\overline{\mathbb{F}}_q$. Here both v, w are elements of $\overline{\mathbb{F}}_q^\times$ of order $q^{\frac{n}{2}} + (-1)^{\frac{n}{2}}$. (Hence in this case T_2 is not cyclic either.)

Part (b) of the assertion follows from Malle, Saxl and Weigel (1994), proof of Thm. 3.1 (Paragraphs 8 and 9). (The only exceptional case occurring there is $\text{SO}_4^+(2)$, but we assume here that q is odd.) \square

Theorem 3.15. Assume that $n \geq 4$ and q is odd.

- (a) The F -module (M_{D_n}, Φ) over $K = \mathbb{F}_q(t_1, \dots, t_n, s)$ with representing matrix $D_B(\Phi) = S_{D_n}(t_1, \dots, t_n, s)$ is dualizable.
- (b) The Galois group of (M_{D_n}, Φ) is $\text{SO}_{2n}^+(q)$.
- (c) The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial $f_{D_n}(X)$ of (M_{D_n}, Φ) , which is given by

$$\begin{aligned} \frac{1}{s^{q^2}} f_{D_n}(X) = & \sum_{i=0}^{n-1} (-d^{q-1} t_n^q s_i + (t_{n-1}^{q^2} - d^{q-1} t_{n-1}) s_{i-1}^q + t_n^q s_{i-2}^{q^2}) X^{q^i} \\ & + ((d^{q-1} t_{n-1} - t_{n-1}^{q^2}) s_{n-1}^q + (s_{n-2}^{q^2} - 2d^{q-1} t_{n-1}^{q+1} - d^q - d^{q-1} s_{n-2}^q) t_n^q) X^{q^n} \\ & - (2t_{n-1}^{q^2} t_n^{q^2+q} + t_n^q s_{n-1}^{q^2} + (t_{n-1}^{q^2} - d^{q-1} t_{n-1}) s_{n-2}^{q^2} - d^{q-1} t_n^q s_{n-3}^{q^2}) X^{q^{n+1}} \\ & - \sum_{i=2}^n (t_n^q s_{n-i}^{q^i+1} + t_{n-1}^{q^2} - d^{q-1} t_{n-1}) s_{n-i-1}^{q^2+1} - d^{q+1} t_n^q s_{n-i-2}^{q^i+1}) X^{q^{n+i}} \end{aligned}$$

with the s_i as given in Proposition 3.13 and $d := t_n^{q+1} - t_{n-1}^{q+1}$.

Proof. The assertion in (a) as well as the fact that $\text{SO}_{2n}^+(q)$ is an upper bound for $\text{Gal}(M_{D_n}, \Phi)$ follow directly from Proposition 3.13 and Theorem 1.9.

To show that $\text{SO}_{2n}^+(q)$ is also a lower bound for $\text{Gal}(M_{D_n}, \Phi)$ it suffices to find specializations of $S_{D_n}(t_1, \dots, t_n, s)$ to elements $\tilde{\gamma}_i \in \text{SO}_{2n}^+(q)$ such that suitable powers of the $\tilde{\gamma}_i$ are $\text{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate to the γ_i in Proposition 3.14(b), since then $(\tilde{\gamma}_1, \tilde{\gamma}_2)$ form a robust generating system of $\text{SO}_{2n}^+(q)$. Obviously the characteristic polynomials of both γ_1 and γ_2 are symmetric, that is, of the form

$$h(X) = X^{2n} + \sum_{i=1}^{n-1} a_i X^{2n-i} + a_n X^n + \sum_{i=1}^{n-1} a_i X^i + 1 = \prod_{i=1}^n (X - c_i)(X - \frac{1}{c_i})$$

with suitable $a_i \in \mathbb{F}_q$ and $c_i \in \overline{\mathbb{F}}_q^\times$. We claim that $h_{D_n}(X)$ can be specialized to any such a symmetric polynomial $h(X)$. This leads to the system of equations

$$\begin{aligned} a_0 &= 1, a_1 = t_1, a_2 = st_2 - 1, a_3 = st_3 - t_1, \\ a_i &= s(t_i - t_{i-2}) \quad \text{for } i = 4, \dots, n-2, \\ a_{n-1} &= s(t_n t_{n-1} - t_{n-3}), a_n = -s(t_n^2 + t_{n-1}^2 - 2t_{n-2}). \end{aligned}$$

Elimination of t_1, \dots, t_{n-1} yields the following biquadratic equation for t_n

$$t_n^4 + \frac{u}{s} t_n^2 + \left(\frac{v}{s}\right)^2 = 0,$$

where

$$u = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} a_{n-2i} \quad \text{and} \quad v = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} a_{n-1-2i}.$$

If the discriminant $\frac{1}{s^2}(u^2 - 4v^2)$ of the underlying quadratic polynomial is a square in \mathbb{F}_q , say $u^2 - 4v^2 = c^2$, we find $t_n^2 = \frac{-u \pm c}{2s}$. With a suitable choice of $s \in \mathbb{F}_q$ such a t_n can hence be found in \mathbb{F}_q . It remains to show that $u^2 - 4v^2$ is in fact a square in \mathbb{F}_q . For this we first note the following identities:

$$-u + 2v = (-1)^{n+1} h(-1), \quad -u - 2v = -h(1).$$

Multiplying these we obtain

$$u^2 - 4v^2 = (-1)^n h(1)h(-1) = \prod_{i=1}^n \frac{(1+c_i)^2(1-c_i)^2}{c_i^2},$$

which visibly is a square in \mathbb{F}_q .

The specialization just constructed maps the Steinberg section $S_{D_n}(t_1, \dots, t_n, s)$ to an element $\tilde{\gamma}_1$, resp. $\tilde{\gamma}_2 \in \mathrm{SO}_{2n}^+(q)$ which has the same characteristic polynomial as γ_1, γ_2 respectively. According to the multiplicative Jordan decomposition the order of $\tilde{\gamma}_i$ is then the order of γ_i multiplied by a power of the characteristic p . As the order of γ_i is prime to p , there is some power of $\tilde{\gamma}_i$ of order prime to p and with the same characteristic polynomial as γ_i and which is hence $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ -conjugate to γ_i .

The geometricity of N/K is obtained as in the proof of Theorem 3.4. Finally the characteristic polynomial of (M_{D_n}, Φ) is computed from the algebraic system of equations

$$S_{D_n}(t_1, \dots, t_n, s)(X_1^q, \dots, X_{2n}^q)^t = (X_1, \dots, X_{2n})^t$$

by solving for $X := X_1$. □

Remark. The projective variant $\bar{f}_{D_n}(Y)$ of $f_{D_n}(X)$ generates a geometric Galois extension with group $\mathrm{PSO}_{2n}^+(q)$ over K (compare Corollary 3.5).

3.5 The Dickson Groups $G_2(q)$

For the Dickson group $G_2(q)$ with q odd we use its smallest 7-dimensional representation over IF_q . Its image is contained inside the orthogonal group $\text{SO}_8^+(q)$ (see Malle (2003), and Albert and Maier (2011), Ch. 6.2). With this one obtains:

Proposition 3.16. *For q odd the group $G_2(q)$ possesses a Steinberg cross section of the form*

$$S_{G_2}(t, u) = \begin{pmatrix} -t & -u & 1 & . & . & . & . \\ -1 & . & . & . & . & . & . \\ . & -t^2 & . & -t & u & 1 & . \\ . & -2t & . & -1 & . & . & . \\ . & 1 & . & . & . & . & . \\ . & . & . & . & -t & . & -1 \\ . & . & . & . & 1 & . & . \end{pmatrix}.$$

Its characteristic polynomial is given by

$$\begin{aligned} h_{G_2}(X) = (X-1)(X^6 + (t+2)X^5 + (2+2t-u)X^4 + (2+2t-2u-t^2)X^3 \\ + (2+2t-u)X^2 + (t+2)X + 1). \end{aligned}$$

Proof. We use the following root subgroups and representatives of simple reflections for the computation of the Steinberg cross section (see Malle (2003)):

$$\begin{aligned} X_1(t) &= \text{diag}\left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -t^2 \\ 0 & 1 - 2t \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}\right), \\ X_2(t) &= \text{diag}(1, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, 1, \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}, 1), \\ \omega_1 &= \text{diag}\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right), \\ \omega_2 &= \text{diag}(1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 1, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, 1). \end{aligned}$$

The Steinberg cross section in the statement is obtained by expanding the product

$$S_{G_2}(t, u) = X_1(t)\omega_1 X_2(u)\omega_2.$$

Its characteristic polynomial can be determined by elementary calculations. \square

Proposition 3.17. (a) *The group $G_2(q)$ with q odd contains elements γ_1, γ_2 of orders $q^2 \pm q + 1$.*

(b) *For $q \neq 3$ any two such elements form a robust generating pair.*

(c) *For $q = 3$ there exists an element $\gamma_3 \in G_2(3)$ of order 8 such that $(\gamma_1, \gamma_2, \gamma_3)$ is a robust generating system.*

Proof. For (a) let $v \in \overline{\mathbb{F}_q}^\times$ be an element of order $q^2 + q + 1$, $q^2 - q + 1$ respectively. Then the characteristic polynomial $g_v(x)$ of $\text{diag}(v, v^q, v^{q^2}, v^{-q^2}, v^{-q}, v^{-1})$ is symmetric in $\mathbb{F}_q[X]$, i.e., it has the form

$$g_v(X) = X^6 - a_1 X^5 + a_2 X^4 - a_3 X^3 + a_2 X^2 - a_1 X + 1,$$

with

$$\begin{aligned} a_1 &= v + v^q + v^{q^2} + v^{-q^2} + v^{-q} + v^{-1}, \\ a_2 &= v^{1-q} + v^{1+q} + v^{1-q^2} + v^{1+q^2} + v^{q-q^2} + v^{q+q^2} + v^{-q-q^2} + v^{q^2-q} \\ &\quad + v^{-1-q^2} + v^{q^2-1} + v^{-1-q} + v^{q-1} + 3, \\ a_3 &= v^2 + v^{2q} + v^{2q^2} + v^{-2q^2} + v^{-2q} + v^{-2} + 2 - 2a_1 = 2a_2 - 2 + a_1^2 - 2a_1. \end{aligned}$$

Since here a_3 satisfies the same relations as in the second factor of $h_{G_2}(X)$, we have that $h_v(X) := (X - 1)g_v(X)$ can be obtained as a specialization over \mathbb{F}_q from $h_{G_2}(X)$. Consequently $G_2(q)$ contains an element γ_v with characteristic polynomial $h_v(X)$. This has Jordan normal form $\text{diag}(v, v^q, v^{q^2}, 1, v^{-q^2}, v^{-q}, v^{-1})$ over $\overline{\mathbb{F}_q}$ and hence order $q^2 + q + 1$, respectively $q^2 - q + 1$.

For the proof of (b) as in Section II.4.3, we use the list of maximal subgroups compiled by Kleidman (1988b). According to this for $q > 3$ there is no maximal subgroup containing elements of both orders $q^2 + q + 1$ and $q^2 - q + 1$. For $q = 3$ there is no such subgroup which additionally contains a third element of order 8 (see Conway et al. (1985), p. 60). Such an element is obtained via the specialization $(t, u) \mapsto (0, 1)$. \square

Theorem 3.18. *Let q be odd.*

- (a) *The F -module (M_{G_2}, Φ) over $K = \mathbb{F}_q(t, u)$ with representing matrix $D_B(\Phi) = S_{G_2}(t, u)$ is dualizable.*
- (b) *The Galois group of (M_{G_2}, Φ) is $G_2(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial of (M_{G_2}, Φ)*

$$\begin{aligned} f_{G_2}(X) &= X^{q^7} + (t^{q^2-q} + t^{q^3})X^{q^6} + (t^{2q^2-q} - u^{q^2})X^{q^5} - (u^q t^{q^2-q} + t^{2q^2})X^{q^4} \\ &\quad + (t^{q^2+q} + u^q)X^{q^3} + (ut^{q^2-q} - t^q)X^{q^2} - (t^{q^2-q+1} + 1)X^q - t^{q^2-q}X. \end{aligned}$$

Proof. The dualizability of (M_{G_2}, Φ) follows from Proposition 3.16. Application of Theorem 1.9 shows that $G_2(q)$ is an upper bound for $\text{Gal}(M_{G_2}, \Phi)$. Proposition 3.17 with Corollary 2.13 then gives that $G_2(q)$ is also a lower bound for the Galois group, whence $\text{Gal}(M_{G_2}, \Phi) \cong G_2(q)$.

The geometricity of N/K follows as in Theorem 3.4. The characteristic polynomial $f_{G_2}(X)$ finally can be computed with the Buchberger algorithm (in anti-lexicographical ordering) from the system of algebraic equations

$$S_{G_2}(t, u)(X_1^q, \dots, X_7^q)^t = (X_1, \dots, X_7)^t$$

with $X := X_1$. □

For the easier case of even prime powers q one may use the 6-dimensional representation of $G_2(q)$ over \mathbb{F}_q embedding it into $Sp_6(q)$ (see Malle (2003), resp. Albert and Maier (2011), Ch. 6.2). With this one obtains in a similar way a Steinberg cross section of the form

$$S_{G_2}^{\text{even}}(t, u) = \begin{pmatrix} t & u & 1 & \dots & \\ 1 & \dots & \dots & \dots & \\ \cdot & t^2 & \cdot & u & 1 \\ \cdot & 1 & \dots & \dots & \\ \cdot & \dots & t & \cdot & 1 \\ \cdot & \dots & 1 & \dots & \end{pmatrix}.$$

This satisfies:

Proposition 3.19. *Let q be even.*

- (a) *The F -module (M_{G_2}, Φ) over $K = \mathbb{F}_q(t, u)$ with $D_B(\Phi) = S_{G_2}^{\text{even}}(t, u)$ is dualizable.*
- (b) *The Galois group of (M_{G_2}, Φ) is $G_2(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial of (M_{G_2}, Φ)*

$$f_{G_2}(X) = X^{q^6} + t^{q^2} X^{q^5} + u^q X^{q^4} + t^{2q} X^{q^3} + u X^{q^2} + t X^q + X.$$

The proof is left as an exercise to the interested reader; it can also be found in Albert and Maier (2011), Ch. 6.2.

Somewhat more complicated polynomials for the groups $G_2(q)$ over $\mathbb{F}_q(t, u)$ had already been constructed in a similar fashion by Malle (2003), Thms. 4.1 and 4.3.

Due to the large degrees of their minimal faithful representations, similar computations for the large exceptional groups of types F_4, E_6, E_7 and E_8 become rather unwieldy and thus corresponding polynomials have not (yet) been constructed.

4 Polynomials for Twisted Groups of Lie Type

In order to realize twisted groups of Lie type as Galois groups over $\mathbb{F}_q(\mathbf{t})$ we need a twisted variant of the upper bound from Theorem 1.9 and a corresponding replacement for the Steinberg cross section, which we will call a pseudo Steinberg cross section. Using this we will realize the unitary groups ${}^2A_n(q) = \mathrm{SU}_{n+1}(q)$, the orthogonal groups ${}^2D_n(q) = \mathrm{SO}_{2n}^-(q)$ for q odd, the Suzuki groups ${}^2B_2(q^2)$, the Ree groups ${}^2G_2(q^2)$ and the Steinberg triality groups ${}^3D_4(q)$ for q odd as Galois groups. Moreover we compute generating polynomials for the corresponding Galois extensions. These results are all taken from the thesis of Maier and form part of Albert and Maier (2011).

4.1 The Special Unitary Groups $\mathrm{SU}_n(q)$

Twisted groups of Lie type are defined as fixed point groups of simple algebraic groups under Steinberg endomorphisms. Let \mathbf{G} be a linear algebraic group defined over \mathbb{F}_q and $\varphi : \mathbf{G} \rightarrow \mathbf{G}$ an endomorphism such that some power φ^r is the Frobenius endomorphism ϕ_q on \mathbf{G} . Then φ is a *Steinberg endomorphism of \mathbf{G}* . Note that then the group of fixed points \mathbf{G}^φ under φ satisfies $\mathbf{G}^\varphi \leq \mathbf{G}^{\phi_q} = \mathbf{G}(\mathbb{F}_q)$.

For the realization of twisted groups of Lie type we need a replacement for the Steinberg cross section which takes into account Steinberg morphisms. The basis for this is yielded by Maier's variant of the upper bound in Theorem 1.9 (see Albert and Maier (2011), Thm. 3.3):

Theorem 4.1 (Twisted Upper Bound Theorem). *Let \mathbf{G} be a connected linear algebraic group over \mathbb{F}_q with a Steinberg endomorphism $\varphi : \mathbf{G} \rightarrow \mathbf{G}$ such that $\varphi^r = \phi_q$ for some $r \in \mathbb{N}$. If (M, Φ) is an F -module over $K \geq \mathbb{F}_q$ with basis B and if the representing matrix $D_B(\Phi)$ has the form*

$$D_B(\Phi) = D_0 \varphi(D_0) \cdots \varphi^{r-1}(D_0)$$

for some $D_0 \in \mathbf{G}(K)$, then $\mathrm{Gal}(M, \Phi) \leq \mathbf{G}^\varphi$.

Proof. The starting point is again the Theorem II.1.1 of Lang–Steinberg which guarantees the existence of a matrix $Y \in \mathbf{G}(\overline{\mathbb{F}}_q)$ with $\varphi(Y) = D_0^{-1}Y$. This satisfies

$$\begin{aligned} \phi_q(Y) &= \varphi^r(Y) = \varphi^{r-1}(D_0^{-1}Y) = \varphi^{r-1}(D_0^{-1})\varphi^{r-1}(Y) \\ &= \varphi^{r-1}(D_0^{-1}) \cdots \varphi(D_0^{-1})D_0^{-1}Y = D_B(\Phi)^{-1}Y. \end{aligned}$$

By Theorem 1.9 there is an embedding

$$\mathrm{Gal}(M, \Phi) \longrightarrow \mathbf{G}(\mathbb{F}_q), \quad \gamma \mapsto C_\gamma := Y^{-1}\gamma(Y).$$

Since φ and γ commute and $D_0 \in \mathbb{G}(K)$ is γ -invariant we obtain

$$\begin{aligned}\varphi(C_\gamma) &= \varphi(Y^{-1}\gamma(Y)) = \varphi(Y^{-1})\varphi(\gamma(Y)) = \varphi(Y^{-1})\gamma(\varphi(Y)) \\ &= Y^{-1}D_0\gamma(D_0^{-1}Y) = Y^{-1}\gamma(Y) = C_\gamma.\end{aligned}$$

So $C_\gamma \in \mathbb{G}(\mathbb{F}_q)$ is φ -invariant for every $\gamma \in \text{Gal}(M, \Phi)$ and thus lies in \mathbb{G}^φ . \square

The special unitary groups can be obtained as fixed points $\text{SU}_n(q) := \text{SL}_n^\varphi$ under the Steinberg endomorphism

$$\varphi : \text{SL}_n \rightarrow \text{SL}_n, \quad C \mapsto J \cdot (\phi_q(C)^t)^{-1} \cdot J,$$

where $J := \text{antidiag}(1, \dots, 1)$. Here clearly we have $\varphi^2 = \phi_{q^2}$. We now construct a replacement $S_{\text{U}_n}(t_1, \dots, t_n)$ in $\text{SU}_n(q)$ for the Steinberg cross section of the form $D_0\varphi(D_0)$, which will contain $m := \lfloor \frac{n}{2} \rfloor$ root subgroups of $\text{SL}_n(q^2)$. It is called a *pseudo Steinberg cross section*. An easy calculation shows that in the notation of Proposition 3.2 we have $\varphi(\omega_i) = \omega_{n-i}$ and $\varphi(\mathbf{X}_i(t_i)) = \mathbf{X}_{n-i}(t_i^{-q})$. Thus $\prod_{i=1}^m \mathbf{X}_i(t_i)\omega_i$ seems like a good choice for D_0 .

Proposition 4.2. (a) For $n = 2m + 1 \geq 3$ the group $\mathbb{G}_{\text{U}_n}^\varphi = \text{SU}_n(q)$, $(n, q) \neq (3, 2)$, possesses a pseudo Steinberg cross section of the form

$$S_{\text{U}_n}(t_1, \dots, t_m) = \left(\begin{array}{cc|c} -t_1^q & \dots & -t_{m-1}^q & -t_m^q & | & (-1)^m \\ 1 & & & & | & \\ \ddots & & & & | & \\ & 1 & & 0 & | & \\ \hline & & & (-1)^m t_m & | & 1 \\ & & & (-1)^m t_{m-1} & | & 0 & 1 \\ & & & \vdots & | & \ddots & \ddots \\ & & & (-1)^m t_1 & | & 0 & 1 \\ & & & (-1)^m & | & & 0 \end{array} \right).$$

Its characteristic polynomial is given by

$$h_{\text{U}_n}(X) = X^{2m+1} + \sum_{i=1}^m t_i^q X^{2m+1-i} - \sum_{i=1}^m t_i X^i - 1.$$

(b) For $n = 2m \geq 4$ the group $\mathbf{G}_{\mathrm{U}_n}^\varphi = \mathrm{SU}_n(q)$ possesses a pseudo Steinberg cross section of the form

$$S_{\mathrm{U}_n}(t_1, \dots, t_m) = \left(\begin{array}{cc|c} -t_1^q & \cdots & -t_{m-2}^q & -t_{m-1}^q & -t_m^q & (-1)^m \\ 1 & & & & & \\ \ddots & & 1 & & & \\ & & & (-1)^m t_m & 1 & \\ & & & (-1)^m t_{m-1} & 0 & \\ \vdots & & & & & \ddots \ddots \\ & & & (-1)^m t_1 & & 1 \\ & & & (-1)^m & & 0 \end{array} \right).$$

Its characteristic polynomial is given by

$$\begin{aligned} h_{\mathrm{U}_n}(X) = X^{2m} + \sum_{i=1}^{m-1} (t_i^q - t_{i-1}^q) X^{2m-i} + & (-t_{m-1} - t_{m-1}^q + (-1)^m t_m^{q+1}) X^m \\ + \sum_{i=1}^{m-1} (t_i - t_{i-1}) X^i + 1 & \quad \text{with } t_0 = 1. \end{aligned}$$

Proof. In the case $n = 2m + 1$ in order to simplify our calculations we prefer to use

$$D_0 = \begin{pmatrix} I_m & & & \\ & (-1)^m & 1 & \\ & (-1)^m t_1 & 0 & 1 \\ & \vdots & & \ddots \\ & (-1)^m t_{m-1} & & 1 \\ & (-1)^m t_m & & 0 \end{pmatrix} \quad \text{with} \quad \varphi(D_0) = \begin{pmatrix} -t_1^q & \cdots & -t_m^q & (-1)^m \\ 1 & & & \\ \ddots & & 1 & 0 \\ & & & I_m \end{pmatrix}$$

instead of $X_1(t_1)\omega_1 \cdots X_m(t_m)\omega_m = \begin{pmatrix} S_{\mathrm{A}_m} & 0 \\ 0 & I_m \end{pmatrix}$. Then we obtain $S_{\mathrm{U}_n}(t_1, \dots, t_m)$ in (a) as the product $D_0 \cdot \varphi(D_0)$. Its characteristic polynomial is most easily calculated with the methods from Propositions 3.6 and 3.10.

In the case $n = 2m$ we vary the above D_0 by replacing the identity matrix I_m therein by I_{m-1} . Setting $S_{\mathrm{U}_n}(t_1, \dots, t_m) := D_0 \varphi(D_0)$ we obtain the pseudo Steinberg cross section of $\mathrm{SU}_n(q)$ given in (b) with the characteristic polynomial $h_{\mathrm{U}_n}(X)$ as stated. \square

Proposition 4.3. For $n > 2$ we have:

- (a) The groups $\mathbf{G}_{\mathrm{U}_n} = \mathrm{SU}_n(q)$ possess cyclic maximal tori $\mathsf{T}_1, \mathsf{T}_2$ of orders $\frac{q^n - (-1)^n}{q+1}$ and $q^{n-1} - (-1)^{n-1}$.
- (b) For $(n, q) \notin \{(3, 2), (4, 3), (6, 2)\}$ any two generators (γ_1, γ_2) of $\mathsf{T}_1, \mathsf{T}_2$ form a robust generating system of $\mathbf{G}_{\mathrm{U}_n}$.

(c) Adding an element γ_3 of order 8 respectively 9 in the case $(n, q) = (4, 3)$, respectively $(n, q) = (6, 2)$, the triple $(\gamma_1, \gamma_2, \gamma_3)$ is a robust generating system of \mathbf{G}_{U_n} .

Proof. Assertion (a) follows from Malle, Saxl and Weigel (1994), Tab. III. Part (b) for $(n, q) \in \{(3, 3), (3, 5), (5, 2)\}$ can be read off immediately from Conway et al. (1985), pp. 14, 34 and 72. For the other (n, q) in (b) the proof is given in Malle, Saxl and Weigel (1994), Thm. 3.1 (third paragraph). In the remaining cases $(n, q) \in \{(4, 3), (6, 2)\}$ in (c) a robust system as claimed is obtained using Conway et al. (1985), pp. 54 and 115. \square

For the proof of our main result the following observation will be useful:

Lemma 4.4. *Let $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + (-1)^n \in \mathbb{F}_{q^2}[X]$ be a separable polynomial with the property that $x \in \overline{\mathbb{F}}_q$ is a zero of f if and only if $-x^q$ is. Then we have $a_i = -a_{n-i}^q$ for all $1 \leq i \leq n-1$.*

Proof. The symmetry relation among the coefficients follows directly from the symmetry of the zeroes $x_1, \dots, x_n \in \overline{\mathbb{F}}_q$ using the product relation $x_1 \cdots x_n = 1$. \square

This completes our preparations for the proof of the main result of this section.

Theorem 4.5. *Let $n > 2$ and q be a prime power, with $(n, q) \neq (3, 2)$. Then with $m := \lfloor \frac{n}{2} \rfloor$ we have:*

- (a) *The F -module (M_{U_n}, Φ) over $K = \mathbb{F}_{q^2}(t_1, \dots, t_m)$ with the representing matrix $D_B(\Phi) = S_{U_n}(t_1, \dots, t_m)$ is dualizable.*
- (b) *The Galois group of (M_{U_n}, Φ) is $SU_n(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial $f_{U_n}(X)$ of (M_{U_n}, Φ) , given by*

$$f_{U_n}(X) = X^{(q^2)^{2m+1}} + \sum_{i=1}^m t_i^{(q^2)^{m+1-i}} X^{(q^2)^{2m+1-i}} - \sum_{i=1}^m t_i^q X^{(q^2)^i} - X$$

for $n = 2m + 1$,

$$f_{U_n}(X) = X^{(q^2)^{2m}} + \sum_{i=1}^{m-1} (t_i^{(q^2)^{m+1-i}} - t_m^{q^3-q} t_{i-1}^{(q^2)^{m+i-1}}) X^{(q^2)^{2m+1-i}} \\ + (-t_{m-1}^{q^2} t_m^{q^3-q} - t_{m-1}^{q^3} + (-1)^m t_m^{q^2(q+1)}) X^{(q^2)^m}$$

$$+ \sum_{i=1}^{m-1} (-t_{i-1}^{q^3} + t_m^{q^3-q} t_i^q) X^{(q^2)^i} + t_m^{q^3-q} X$$

for $n = 2m$

where $t_0 = 1$.

Proof. Part (a) again follows directly from the shape of $D_B(\Phi)$ in Proposition 4.2, as does the claim that $SU_n(q)$ is an upper bound for $\text{Gal}(M_{U_n}, \Phi)$ by Theorem 4.1.

For (b) it remains to show that $S_{U_n}(t_1, \dots, t_m)$ can be specialized to a robust generating system of $SU_n(q)$. For this let first $n = 2m + 1$ be odd. Then $h_{U_n}(X)$ is by Proposition 4.2(a) a general polynomial with the symmetry property from Lemma 4.4. The elements γ_1, γ_2 from Proposition 4.3(b) have Jordan normal forms

$$\begin{aligned} & \text{diag}(v_1, v_1^{-q}, v_1^{q^2}, \dots, v_1^{(-q)^{n-1}}), \\ & \text{diag}(v_2, v_2^{-q}, \dots, v_2^{(-q)^{n-2}}, v_2^{-1+q-q^2+\dots-(-q)^{n-2}}) \end{aligned}$$

with elements $v_i \in \overline{\mathbb{F}_q}^\times$ of the same order as γ_i (see Malle, Saxl and Weigel (1994)). Thus the characteristic polynomials of γ_1 and γ_2 also enjoy the symmetry property from Lemma 4.4. Consequently $h_{U_n}(X)$ possesses specializations to the characteristic polynomials of γ_1 and γ_2 . The same specializations applied to $S_{U_n}(t_1, \dots, t_m)$ then yield a robust generating system of $SU_n(q)$. In the case $n = 2m$ the characteristic polynomials of γ_1, γ_2 both have the shape

$$X^n + \sum_{i=1}^{m-1} a_i^q X^{n-i} + a_m X^m + \sum_{i=1}^{m-1} a_i X^i + 1$$

with $a_i \in \mathbb{F}_{q^2}$ and $a_m \in \mathbb{F}_q$. Such a polynomial is obtained from $h_{U_n}(X)$ by the specialization $t_i \mapsto u_i$ with

$$u_i = 1 + \sum_{j=1}^i a_j \quad \text{for } 1 \leq i \leq m-1 \quad \text{and} \quad u_m^{q+1} = (-1)^m (a_m + u_{m-1} + u_{m-1}^q).$$

This is possible since the right hand side of the last equation is an element of \mathbb{F}_q and hence a $q+1$ st power in \mathbb{F}_{q^2} . The corresponding statement also holds for γ_3 in the two exceptional cases in Proposition 4.3(c). Thus these specializations $t_i \mapsto u_i$ of $S_{U_n}(t_1, \dots, t_m)$ lead to a robust generating system (γ_1, γ_2) respectively $(\gamma_1, \gamma_2, \gamma_3)$ of $SU_n(q)$. Hence, in both cases, n odd and n even, $SU_n(q)$ is also a lower bound for $\text{Gal}(V_{U_n}, \Phi)$ by Corollary 2.13.

The generating polynomial for the corresponding Galois extension is finally obtained by solving the algebraic system of equations

$$S_{U_n}(X_1^{q^2}, \dots, X_m^{q^2})^t = (X_1, \dots, X_m)^t$$

for $X := X_1$. Its geometricity ensues as in Theorem 3.4. \square

Remark. With the methods of the subsequent section it is also possible to construct Frobenius modules (\tilde{M}_{U_n}, Φ) of dimension $2n$ with Galois group $SU_n(q)$ over $\mathbb{F}_q(t_1, \dots, t_n)$. For this the computation of a generating additive polynomial turns out to be difficult (see Albert and Maier (2011), Ch. 5.1). A general method for the descent of ground fields will be presented in Paragraph 5.

Corollary 4.6. *The fixed field of the center $\mathcal{Z}(\mathrm{SU}_n(q))$ in the Galois extension N/K in Theorem 4.5 gives a Galois extension over $\mathbb{F}_{q^2}(\mathbf{t})$ with the simple group $\mathrm{U}_n(q)$. It is generated by the roots of the projective variant $\bar{f}_{\mathrm{U}_n}(Y)$ of $f_{\mathrm{U}_n}(X)$.*

The nice polynomials for $\mathrm{SU}_n(q)$ and $\mathrm{U}_n(q)$ presented by Abhyankar (1996a) for n odd and by Abhyankar and Inglis (2001) for n even can be obtained from the polynomials $f_{\mathrm{U}_n}(X)$ in Theorem 4.5 and $\bar{f}_{\mathrm{U}_n}(Y)$ in Corollary 4.6 by specializing $t_i \mapsto 0$ for $i = 1, \dots, m-1$ (and possibly changing the sign at X or Y , respectively).

4.2 The Orthogonal Groups $\mathrm{SO}_{2n}^-(q)$

In order to obtain polynomials which can easily be calculated, in the case of orthogonal groups $\mathrm{SO}_{2n}^-(q)$ (with q odd) we replace the natural $2n$ -dimensional representation of $\mathrm{G}_{\mathrm{D}_n}$ by the one of the linear algebraic group $\mathrm{G}_{\mathrm{O}_{2n}}$ obtained by field restriction. (Thus this section can also be regarded as an explicit precursor example for the method of field restriction presented in the next paragraph.) As we have $\mathrm{G}_{\mathrm{O}_{2n}}(\mathbb{F}_q) = \mathrm{SO}_{2n}^-(q)$ this will yield a Galois extension with the group $\mathrm{SO}_{2n}^-(q)$ over $\mathbb{F}_q(t)$ (instead of over $\mathbb{F}_{q^2}(t)$).

The orthogonal group $\mathrm{SO}_{2n}^-(q)$ is defined as the fixed point subgroup in SO_{2n} under the Steinberg endomorphism

$$\varphi : \mathrm{SO}_{2n} \longrightarrow \mathrm{SO}_{2n}, \quad C \mapsto N^{-1}\phi_q(C)N,$$

where $N = \mathrm{diag}(1, \dots, 1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1)$ with a central 2-block (see Malle and Testerman (2011), Ex. 22.9(2)). This clearly satisfies $\varphi^2 = \phi_{q^2}$. In order to construct a linear group $\mathrm{G}_{\mathrm{O}_{2n}}$ with $\mathrm{G}_{\mathrm{O}_{2n}}(\mathbb{F}_q) = \mathrm{SO}_{2n}^+(q^2)^\varphi = \mathrm{SO}_{2n}^-(q)$ we choose an element $y \in \mathbb{F}_{q^2}$ with $y^q = -y$. This satisfies $\mathbb{F}_{q^2} = \mathbb{F}_q(y)$. As $y^2 \in \mathbb{F}_q$ we then obtain an \mathbb{F}_q -linear embedding

$$\lambda : \mathbb{F}_{q^2}(\mathbf{t}) \longrightarrow \mathbb{F}_q(\mathbf{t})^{2 \times 2}, \quad a(\mathbf{t}) + yb(\mathbf{t}) \mapsto \begin{pmatrix} a(\mathbf{t}) & y^2b(\mathbf{t}) \\ b(\mathbf{t}) & a(\mathbf{t}) \end{pmatrix} \in \mathbb{F}_q(\mathbf{t})^{2 \times 2}$$

and from this a homomorphic embedding

$$\Lambda : \mathrm{GL}_{2n}(\mathbb{F}_{q^2}(\mathbf{t})) \longrightarrow \mathrm{GL}_{4n}(\mathbb{F}_q(\mathbf{t})), \quad (c_{ij}) \mapsto (\lambda(c_{ij})).$$

Here the image $\mathcal{H}(\mathbb{F}_q(\mathbf{t})) := \Lambda(\mathrm{GL}_{2n}(\mathbb{F}_{q^2}(\mathbf{t})))$ is a linear algebraic group defined over \mathbb{F}_q , although Λ is not a morphism in the sense of algebraic geometry.

The non-trivial generating element $\psi \in \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ satisfies $\psi(y) = y^q = -y$. This extends to $\Lambda(\mathrm{GL}_{2n}(\mathbb{F}_{q^2}(\mathbf{t})))$ via

$$\Psi : \mathcal{H}(\mathbb{F}_q(\mathbf{t})) \longrightarrow \mathcal{H}(\mathbb{F}_q(\mathbf{t})), \quad \begin{pmatrix} a_{ij}(\mathbf{t}) & y^2b_{ij}(\mathbf{t}) \\ b_{ij}(\mathbf{t}) & a_{ij}(\mathbf{t}) \end{pmatrix} \mapsto \begin{pmatrix} a_{ij}(\mathbf{t}) & -y^2b_{ij}(\mathbf{t}) \\ -b_{ij}(\mathbf{t}) & a_{ij}(\mathbf{t}) \end{pmatrix}.$$

With this the defining relation $C = N^{-1}\phi_q(C)N$ of $\mathrm{SO}_{2n}^-(q)$ can be transferred inside $\mathrm{SO}_{2n}^+(q^2)$ to $\mathcal{H}(\mathbb{F}_q(\mathbf{t}))$ as $\Lambda(C) = \Lambda(N)^{-1}\Psi(C)\Lambda(N)$. For $C = a_{ij}(\mathbf{t}) + yb_{ij}(\mathbf{t}) \in \mathrm{GL}_{2n}(\mathbb{F}_{q^2}(\mathbf{t}))$ we now write

$$\det(C) = f(a_{ij}(\mathbf{t}), b_{ij}(\mathbf{t})) + yg(a_{ij}(\mathbf{t}), b_{ij}(\mathbf{t})) =: f(C) + yg(C)$$

with polynomials $f, g \in \mathbb{F}_q[X_{ij}, Y_{ij}]$. With this let

$$\begin{aligned} \mathsf{G}_{\mathrm{O}_{2n}}(\overline{\mathbb{F}_q(\mathbf{t})}) := \{C \in \mathcal{H}(\overline{\mathbb{F}_q(\mathbf{t})}) \mid & f(C) = 1, g(C) = 0, \tilde{C}\Lambda(J)C = \Lambda(J), \\ & C = \Lambda(N)^{-1}\Psi(C)\Lambda(N)\}; \end{aligned}$$

here \tilde{C} is obtained from C by blockwise transposition of all of its 2×2 -blocks. This is a linear algebraic group defined over \mathbb{F}_q .

Proposition 4.7. *For $n \geq 4$ and odd q the linear algebraic group $\mathsf{G}_{\mathrm{O}_{2n}}$ satisfies:*

- (a) $\mathsf{G}_{\mathrm{O}_{2n}}(\mathbb{F}_q) \cong \mathrm{SO}_{2n}^-(q)$ and $\mathsf{G}_{\mathrm{O}_{2n}}(\mathbb{F}_q(\mathbf{t})) \cong \mathrm{SO}_{2n}^-(\mathbb{F}_{q^2}(\mathbf{t}))$,
- (b) $\mathsf{G}_{\mathrm{O}_{2n}}(\overline{\mathbb{F}_q(\mathbf{t})}) \cong \mathrm{SO}_{2n}(\overline{\mathbb{F}_q(\mathbf{t})})$; in particular $\mathsf{G}_{\mathrm{O}_{2n}}$ is connected.

Proof. The two claims in (a) follow directly from the definition of $\mathsf{G}_{\mathrm{O}_{2n}}$. Clearly there exists a natural isomorphism over $\overline{\mathbb{F}_q(\mathbf{t})}$ of the form

$$\mathsf{G}_{\mathrm{O}_{2n}} \cong \{(C_1, C_2) \in \mathrm{SO}_{2n} \times \mathrm{SO}_{2n} \mid C_1 = N^{-1}C_2N\}.$$

This shows that $\mathsf{G}_{\mathrm{O}_{2n}}(\overline{\mathbb{F}_q(\mathbf{t})}) \cong \mathrm{SO}_{2n}(\overline{\mathbb{F}_q(\mathbf{t})})$ is connected. \square

We can now easily obtain a pseudo Steinberg cross section for $\mathrm{SO}_{2n}^-(q)$ from the one for $\mathrm{SO}_{2n}^+(q)$ in Proposition 3.13 by replacing t_{n-1} and t_n by $t_{n-1} + yt_n$ and $-t_{n-1} + yt_n$ respectively.

Corollary 4.8. *Let $n \geq 4$. The group $\mathrm{SO}_{2n}^-(q)$ with q odd possesses a pseudo Steinberg cross section of the form*

$$S_{\mathrm{O}_{2n}}(t_1, \dots, t_n, s) := S_{\mathrm{D}_n}(t_1, \dots, t_{n-2}, t_{n-1} + yt_n, -t_{n-1} + yt_n, s),$$

with characteristic polynomial

$$h_{\mathrm{O}_{2n}}(X) = h_{\mathrm{D}_n}(t_1, \dots, t_{n-2}, t_{n-1} + yt_n, -t_{n-1} + yt_n, s)(X).$$

Proof. By definition

$$\mathrm{SO}_{2n}^-(\mathbb{F}_{q^2}(\mathbf{t})) = \{C \in \mathrm{SO}_{2n}^+(\mathbb{F}_{q^2}(\mathbf{t})) \mid N^{-1}\phi_q(C)N = C\}.$$

These matrices have the form

$$C = \begin{pmatrix} & a_1 & \psi(a_1) & & \\ & C_1 & \vdots & \vdots & C_2 \\ & & a_{n-1} & \psi(a_{n-1}) & \\ b_1 & \dots & b_n & c_n & \dots & c_1 \\ \psi(b_1) & \dots & \psi(c_n) & \psi(b_n) & \dots & \psi(c_1) \\ & & d_{n-1} & \psi(d_{n-1}) & & \\ & C_3 & \vdots & \vdots & C_4 \\ & & d_1 & \psi(d_1) & & \end{pmatrix} \quad \text{with} \quad \begin{aligned} C_i &\in \mathbb{F}_q(\mathbf{t})^{n-1 \times n-1}, \\ a_i, b_i, c_i, d_i &\in \mathbb{F}_{q^2}(\mathbf{t}). \end{aligned}$$

So according to Proposition 3.13

$$S_{D_n}(t_1, \dots, t_{n-2}, t_{n-1} + yt_n, -t_{n-1} + yt_n, s)$$

is an element of $\mathrm{SO}_{2n}^-(\mathbb{F}_{q^2}(\mathbf{t}, s))$ and hence also a pseudo Steinberg cross section of $\mathrm{SO}_{2n}^-(q)$. \square

Proposition 4.9. *Let $n \geq 4$ and q be odd. Then:*

- (a) *The group $\mathrm{SO}_{2n}^-(q)$ possesses maximal tori T_1 and T_2 of orders $q^n + 1$ and $(q^{n-1} + 1)(q - 1)$.*
- (b) *Any two elements γ_1, γ_2 of maximal order in T_1, T_2 respectively form a robust generating pair of $\mathrm{SO}_{2n}^-(q)$.*

Proof. Assertion (a) can be found in Malle, Saxl and Weigel (1994), Tab. III. The elements in T_1, T_2 have Jordan normal forms $\mathrm{diag}(v, v^q, \dots, v^{q^{n-1}}, v^{-q^{n-1}}, \dots, v^{-1})$ with $v^{q^n+1} = 1$, resp. $\mathrm{diag}(v, v^q, \dots, v^{q^{n-2}}, w, w^{-1}, v^{-q^{n-2}}, \dots, v^{-1})$ with $v^{q^{n-1}+1} = 1$ and $w^{q-1} = 1$.

Assertion (b) follows from Malle, Saxl and Weigel (1994), proof of Thm. 3.1 (Paragraph 7). (Note that we assume q to be odd here.) \square

Theorem 4.10. *Let $n \geq 4$ and q be odd.*

- (a) *The F -module $(M_{O_{2n}}, \Phi)$ over $K = \mathbb{F}_q(t_1, \dots, t_n, s)$ with representing matrix $D_B(\Phi) = \Lambda(S_{O_{2n}}(t_1, \dots, t_n, s))$ is dualizable.*
- (b) *The Galois group of $(M_{O_{2n}}, \Phi)$ over K is $\mathrm{SO}_{2n}^-(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial of $(M_{O_{2n}}, \Phi)$.*

Proof. As in the proof of Theorem 4.5 it only remains to show that $\Lambda(S_{O_{2n}}(\mathbf{t}, s))$ can be specialized to elements of maximal order in the two tori T_1 and T_2 from Proposition 4.9. These then form a robust system of generators for $\mathrm{G}_{O_{2n}}(\mathbb{F}_q) \cong \mathrm{SO}_{2n}^-(q)$. Since the upper bound from Theorem 1.9 and the lower bound from Corollary 2.13 do agree we then conclude that $\mathrm{Gal}(M_{O_{2n}}, \Phi) \cong \mathrm{SO}_{2n}^-(q)$.

For simplicity we first work with the $2n$ -dimensional natural representation $S_{O_{2n}}(\mathbf{t}, s)$ instead of the $4n$ -dimensional $\Lambda(S_{O_{2n}}(\mathbf{t}, s))$. According to Proposition 4.9 the characteristic polynomials $h_\gamma(X)$ of $\gamma \in \{\gamma_1, \gamma_2\}$ are separable polynomials in

$\mathbb{F}_q[X]$ and symmetric, since with $x \in \overline{\mathbb{F}}_q$ also x^{-1} is a zero of $h_\gamma(X)$. In particular it suffices to identify the $h_\gamma(X)$ as specializations of $h_{O_{2n}}(X)$. For this let

$$h_\gamma(X) = \sum_{i=0}^{2n} a_i X^i \quad \text{with} \quad a_{2n-i} = a_i \in \mathbb{F}_q.$$

By Proposition 3.13 and Corollary 4.8 we have

$$\frac{1}{s} h_{O_{2n}}(X) = \sum_{i=0}^{n-1} (\tilde{s}_i - \tilde{s}_{i-2}) (X^{2n-i} + X^i) - (2\tilde{t}_{n-2} + \tilde{t}_{n-1}^2 + \tilde{t}_n^2) X^n$$

with $\tilde{t}_{n-1} = t_{n-1} + yt_n$, $\tilde{t}_n = -t_{n-1} + yt_n$, $\tilde{s}_{-2} = \tilde{s}_{-1} = 0$, $\tilde{s}_0 = \frac{1}{s}$, $\tilde{s}_1 = \frac{t_1}{s}$, $\tilde{s}_i = t_i$ for $i = 2, \dots, n-2$, and $\tilde{s}_{n-1} = \tilde{t}_{n-1}\tilde{t}_n = y^2 t_n^2 - t_{n-1}^2$. From this we reach $h_\gamma(X)$ by specializing the t_i to u_i and s to $r \in \mathbb{F}_q$ such that

$$\begin{aligned} u_1 &= a_1, \quad ru_i = (a_i + a_{i-2} + \dots) \quad \text{for } i = 2, \dots, n-2, \\ r(y^2 u_n^2 - u_{n-1}^2) &= ru_{n-1} + a_{n-1} = a_{n-1} + a_{n-3} + \dots, \\ r(y^2 u_n^2 + u_{n-1}^2) &= -u_{n-2} - \frac{1}{2}a_n = -\frac{1}{2s}a_n - \frac{1}{s}(a_{n-2} + a_{n-4} + \dots). \end{aligned}$$

Since

$$h_\gamma(1) = -4ru_{n-1}^2 \quad \text{and} \quad h_\gamma(-1) = (-1)^{n-1} 4ry^2 u_n^2$$

this is possible if and only if

$$(-1)^n h_\gamma(1) h_\gamma(-1) y^2 = y^2 \prod_{i=1}^n \frac{(1-x_i)^2(1+x_i)^2}{x_i^2} = y^2 \prod_{i=1}^n (x_i^{-1} - x_i)^2$$

is a square in \mathbb{F}_q , that is, if $z := y \prod_{i=1}^n (x_i^{-1} - x_i)$ is an element of \mathbb{F}_q . But the latter is easily verified using the zeroes of $h_{\gamma_1}(X)$ and $h_{\gamma_2}(X)$ given in Proposition 4.9.

Since the u_i and r are elements of \mathbb{F}_q , Λ commutes with the specialization $t_i \mapsto u_i$. So $\Lambda(\gamma_1)$ and $\Lambda(\gamma_2)$ also form a robust generating system of $\Lambda(SO_{2n}^-(q))$. \square

In fact, the characteristic polynomials of $h(\gamma)$, $\gamma \in \{\gamma_1, \gamma_2\}$ can easily be computed. As will be shown in Corollary 5.3 they can be obtained as the product

$$h_{\Lambda(\gamma)}(X) = h_\gamma(X) h_\gamma^\psi(X) = h_\gamma(X)^2.$$

Remark. The generating additive polynomial in Theorem 4.10(c) is computable explicitly from

$$\Lambda(SO_{2n}(t_1, \dots, t_n, s))(X_1^q, \dots, X_{4n}^q)^t = (X_1, \dots, X_{4n})^t$$

with $X := X_1$, but it extends over more than half a page. The interested reader can find it in Albert and Maier (2011), Thm. 5.3. Its projective variant generates a geometric Galois extension with group $PSO_{2n}^-(q)$ over K .

4.3 The Suzuki Groups ${}^2\mathrm{B}_2(q^2)$

The Suzuki groups are best defined as fixed point subgroups inside the 4-dimensional symplectic group $\mathbf{G}_{\mathbb{C}} := \mathbf{G}_{\mathrm{C}_2} = \mathrm{Sp}_4(k)$ over an algebraically closed field k of characteristic 2. According to a result of Chevalley (see Geck (2003), Thm. 3.3.6) there exists a uniquely determined isomorphism of algebraic groups

$$\begin{aligned}\varphi : \mathbf{G}_{\mathbb{C}} &\rightarrow \mathbf{G}_{\mathbb{C}}, A(t_1, \dots, t_4) := \begin{pmatrix} 1 & t_1 & t_3 + t_1 t_2 & t_4 + t_1 t_3 \\ 0 & 1 & t_2 & t_3 \\ 0 & 0 & 1 & t_4 \\ 0 & 0 & 0 & t_1 \end{pmatrix} \\ &\mapsto A' := \begin{pmatrix} 1 & t_2 & t_4 & t_3^2 + t_2 t_4 \\ 0 & 1 & t_1^2 & t_4 + t_1^2 t_2 \\ 0 & 0 & 1 & t_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

with $\varphi(A^t) = (A')^t$. This satisfies

$$\varphi^2(A(t_1, t_2, t_3, t_4)) = A(t_1^2, t_2^2, t_3^2, t_4^2),$$

hence $\varphi^2 = \phi_2$. Setting

$$\varphi_q := \varphi \circ \phi_{2l} \quad \text{for } q^2 = 2^{2l+1}$$

(see Section II.4.5), then in analogy to the previous section we obtain $\varphi_q^2 = \phi_{q^2}$, i.e., φ_q is a (twisted) Steinberg morphism of $\mathbf{G}_{\mathbb{C}}$. Its group of fixed points

$${}^2\mathrm{B}_2(q^2) := \mathbf{G}_{\mathbb{C}}^{\varphi_q} \quad \text{with } q^2 = 2^{2l+1}$$

is the Suzuki group as in Section II.4.5 of order $q^4(q^2 - 1)(q^4 + 1)$.

Proposition 4.11. *The Suzuki group ${}^2\mathrm{B}_2(q^2)$ for $q^2 = 2^{2l+1}$ and $l \geq 1$ has a pseudo Steinberg cross section*

$$S_{\mathrm{Suz}}(t) := \begin{pmatrix} t & t^{2^{l+1}} & 1 & . \\ 1 & . & . & . \\ . & t & . & 1 \\ . & 1 & . & . \end{pmatrix}$$

of the form $S_{\mathrm{Suz}}(t) = D_0 \cdot \varphi_q(D_0)$. Its characteristic polynomial is given by

$$h_{\mathrm{Suz}}(X) = X^4 + t X^3 + t^{2l+1} X^2 + t X + 1.$$

Proof. We use the root subgroups $\mathbf{X}_1, \mathbf{X}_2$ and the Weyl group representatives ω_1, ω_2 for $\mathrm{Sp}_4(q^2)$ from the proof of Proposition 3.6 for $n = 2$. These satisfy

$$\begin{aligned}\varphi_q(\mathbf{X}_1(t)) &= \mathbf{X}_2(t^{2^{l+1}}), & \varphi_q(\omega_1) &= \omega_2, \\ \varphi_q(\mathbf{X}_2(t)) &= \mathbf{X}_1(t^{2^l}), & \varphi_q(\omega_2) &= \omega_1.\end{aligned}$$

So if we set $D_0 := \mathbf{X}_1(t)\omega_1$ then with

$$S_{\text{Suz}}(t) := D_0 \cdot \varphi_q(D_0) = \mathbf{X}_1(t)\omega_1 \mathbf{X}_2(t^{2^l+1})\omega_2$$

we obtain the stated pseudo Steinberg cross section as well as its characteristic polynomial. \square

Proposition 4.12. *For $q^2 = 2^{2l+1}$ with $l \geq 1$ we have:*

- (a) *The Suzuki group ${}^2\text{B}_2(q^2)$ has cyclic maximal tori $\mathbf{T}_1, \mathbf{T}_2$ of respective orders $q^2 \pm 2^{l+1} + 1$.*
- (b) *Any two generators of \mathbf{T}_1 and \mathbf{T}_2 form a robust generating system of ${}^2\text{B}_2(q^2)$.*

Proof. Both claims follows almost immediately from the table of maximal subgroups of ${}^2\text{B}_2(q^2)$ determined by Suzuki (1962). \square

After these preparations we can now formulate the main result of this section.

Theorem 4.13. *For $q^2 = 2^{2l+1}$ with $l \geq 1$ we have:*

- (a) *The F -module (M_{Suz}, Φ) over $K = \overline{\mathbb{F}_{q^2}}(t)$ with representing matrix $D_B(\Phi) = S_{\text{Suz}}(t)$ is dualizable.*
- (b) *The Galois group of (M_{Suz}, Φ) over K is ${}^2\text{B}_2(q^2)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial of (M_{Suz}, Φ)*

$$f_{\text{Suz}}(X) = X^{q^8} + t^{q^2} X^{q^6} + t^{2^{l+1}} X^{q^4} + t X^{q^2} + X.$$

Proof. Again for parts (a) and (b) we only need to verify that ${}^2\text{B}_2(q^2)$ is a lower bound for $\text{Gal}(M_{\text{Suz}}, \Phi)$. For this let $v_1, v_2 \in \overline{\mathbb{F}_2}$ be elements of orders $q^2 \pm 2^{l+1} + 1$. As $(q^2 + 2^{l+1} + 1)(q^2 - 2^{l+1} + 1) = q^4 + 1$, their minimal polynomials $h_i(X)$ over \mathbb{F}_{q^2} have the form

$$\begin{aligned} h_i(X) &= (X - v_i)(X - v_i^{q^2})(X - v_i^{q^4})(X - v_i^{q^6}) \\ &= (X - v_i)(X - v_i^{q^2})(X - v_i^{-1})(X - v_i^{-q^2}). \end{aligned}$$

Thus, these are symmetric polynomials, i.e.,

$$h_i(X) = X^4 + a_i X^3 + b_i X^2 + a_i X + 1$$

with $a_i = v_i + v_i^{-1} + v_i^{q^2} + v_i^{-q^2} \in \mathbb{F}_{q^2}$ and $b_i = v_i^{1+q^2} + v_i^{-1-q^2} + v_i^{-1+q^2} + v_i^{1-q^2} \in \mathbb{F}_{q^2}$. Since

$$a_i^{2^{l+1}} = v_i^{1+q^2} + v_i^{-1-q^2} + v_i^{q^4+q^2} + v_i^{-q^4-q^2} = b_i$$

both $h_i(X)$ are specializations of $h_{\text{Suz}}(X)$ for $t \mapsto a_i$. According to Proposition 4.11 the same specializations, applied to the matrix $S_{\text{Suz}}(t)$, yield a robust generating system of ${}^2\text{B}_2(q^2)$. So ${}^2\text{B}_2(q^2)$ is a lower bound for $\text{Gal}(M_{\text{Suz}}, \Phi)$ by Corollary 2.13.

Again a generating polynomial is obtained by elimination from the algebraic system of equations

$$S_{\text{Suz}}(t)(X_1^{q^2}, \dots, X_4^{q^2})^t = (X_1, \dots, X_4)^t$$

with $X := X_1$. □

Remark. The assertion of Theorem 4.13 continues to hold in the solvable case $q^2 = 2$. This was checked in Garcia Lopez (2010) with the algorithm for the computation of Galois groups of additive polynomials presented in Paragraph 2.

4.4 The Ree Groups ${}^2G_2(q^2)$

Here we start from the simple algebraic group $G_G := G_{G_2}(k)$ over an algebraically closed field k of characteristic 3. Then by Section II.4.2, there exists a Steinberg morphism

$$\varphi_q : G_G \longrightarrow G_G, \quad \text{with } \varphi_q^2 = \phi_{q^2} \text{ for } q^2 = 3^{2l+1}$$

(compare also Kemper, Lübeck and Magaard (2001)). Its fixed point subgroup is called the Ree group

$${}^2G_2(q^2) := G_G^{\varphi_q} \quad \text{with } q^2 = 3^{2l+1},$$

of order $q^6(q^2 - 1)(q^6 + 1)$. For this a pseudo Steinberg cross section can be determined completely analogously to the case of the Suzuki groups in the previous section:

Proposition 4.14. *For the Ree groups ${}^2G_2(q^2)$ with $q^2 = 3^{2l+1}$, $l \geq 0$,*

$$S_{\text{Ree}}(t) := S_{G_2}(t, t^{3^l+1})$$

is a pseudo Steinberg cross section of the form $S_{\text{Ree}}(t) = D_0 \cdot \varphi_q(D_0)$. Its characteristic polynomial is given by

$$h_{\text{Ree}}(X) = h_{G_2}(t, t^{3^l+1})(X).$$

Proof. We use the root subgroups X_1, X_2 and Weyl group representatives of $G_2(q^2)$ in the proof of Proposition 3.16. They satisfy

$$\begin{aligned} \varphi_q(X_1(t)) &= X_2(t^{3^l+1}), & \varphi_q(\omega_1) &= \omega_2, \\ \varphi_q(X_2(t)) &= X_1(t^{3^l}), & \varphi_q(\omega_2) &= \omega_1 \end{aligned}$$

(see Steinberg (1967), p. 178). With $D_0 := \mathbf{X}_1(t)\omega_1$ then

$$S_{\text{Ree}}(t) := D_0 \cdot \varphi_q(D_0) = \mathbf{X}_1(t)\omega_1 \mathbf{X}_2(t^{3^l+1})\omega_2$$

gives the stated pseudo Steinberg cross section as well as its characteristic polynomial. \square

Proposition 4.15. *For $q^2 = 3^{2l+1}$ with $l \geq 0$ we have:*

- (a) *The Ree group ${}^2G_2(q^2)$ has cyclic maximal tori T_1 and T_2 of orders $q^2 \pm 3^{l+1} + 1$.*
- (b) *For $l > 0$ any two generators of T_1 and T_2 form a robust generating system of ${}^2G_2(q^2)$.*
- (c) *For $q^2 = 3$ every triple $(\gamma_1, \gamma_2, \gamma_3)$ of elements of ${}^2G_2(3)$ of orders 6, 7, and 9 is a robust generating system.*

Proof. Assertions (a) and (b) follow directly from the list of maximal subgroups given in Kleidman (1988b). The claim in (c) is easily checked for example using Conway et al. (1985), p. 6. \square

Theorem 4.16. *For $q^2 = 3^{2l+1}$ with $l \geq 0$ we have:*

- (a) *The F -module (M_{Ree}, Φ) over $K = \overline{\mathbb{F}}_{q^2}(t)$ with representing matrix $D_B(\Phi) = S_{\text{Ree}}(t)$ is dualizable.*
- (b) *The Galois group of (M_{Ree}, Φ) over K is ${}^2G_2(q^2)$.*
- (c) *The corresponding Galois extension N/K is geometric and is generated by the zeroes of the characteristic polynomial $f_{\text{Ree}}(X)$ of (M_{Ree}, Φ) , which is given by*

$$f_{\text{Ree}}(X) = f_{G_2}(t, t^{3^l+1})(X).$$

Proof. By our previous considerations it only remains to show that $S_{\text{Ree}}(t)$ specializes to a robust generating system of ${}^2G_2(q^2)$. In the case when $l = 0$, so $q^2 = 3$, the specializations $t \mapsto 0, 1, -1$ yield elements of orders 6, 9, 7 respectively and thus by Proposition 4.16(c) a robust generating system. For $l \geq 1$ we choose primitive roots of unity v_1, v_2 in $\overline{\mathbb{F}}_q$ of orders $q^2 \pm 3^{l+1} + 1$ and then follow the lines of the argument in the proof of Theorem 4.13. \square

4.5 The Steinberg Triality Groups ${}^3D_4(q)$

We next consider the triality groups ${}^3D_4(q)$ for odd q . Here our starting point is the group $G := G_{D_4} = SO_8(k)$ over an algebraically closed field k of odd characteristic, respectively its projective version $\bar{G} := G/\mathcal{L}(G) \cong P\mathrm{SO}_8(k)$. Denoting the images of root subgroups X_i of G in \bar{G} by \bar{X}_i , there exists an automorphism φ of algebraic

groups uniquely determined up to inner automorphisms such that

$$\varphi : \bar{G} \longrightarrow \bar{G}, \quad \text{with } \varphi(\bar{X}_2) = \bar{X}_2 \text{ and } \varphi : \bar{X}_1 \rightarrow \bar{X}_3 \rightarrow \bar{X}_4 \rightarrow \bar{X}_1$$

(see Deriziotis and Michler (1987)). The Steinberg triality groups are then obtained as fixed point subgroups of the endomorphisms $\varphi_q := \varphi \circ \phi_q$:

$${}^3D_4(q) := \bar{G}^{\varphi_q} \quad \text{with } \varphi_q^3 = \phi_{q^3}.$$

By construction these are subgroups of $\mathrm{PSO}_8^+(q^3)$. The full preimage of ${}^3D_4(q)$ in $\mathrm{SO}_8^+(q^3)$ will be denoted by $\mathcal{H}(q)$. This is a direct product of ${}^3D_4(q)$ with $\mathcal{Z}(\mathrm{SO}_8^+(q^3))$. In contrast to Section 3.4 here we choose

$$\omega_i := X_i(-1)X_{-i}(1)X_i(-1)$$

as representatives for the simple reflections for SO_8 , where X_{-i} denotes the negative root subgroup of X_i . Then for the projective image \bar{D}_0 of

$$D_0 := X_1(t)\omega_1 X_2(u)\omega_2 \in \mathrm{SO}_8^+(\mathrm{IF}_{q^3}(t, u))$$

we obtain

$$\begin{aligned} \varphi_q(\bar{D}_0) &= \bar{X}_3(t^q)\bar{\omega}_3\bar{X}_2(u^q)\bar{\omega}_2, \\ \varphi_q^2(\bar{D}_0) &= \bar{X}_4(t^{q^2})\bar{\omega}_4\bar{X}_2(u^{q^2})\bar{\omega}_2. \end{aligned}$$

Thus, $\bar{S}_{\mathrm{Tri}}(t, u) := \bar{D}_0\varphi_q(\bar{D}_0)\varphi_q^2(\bar{D}_0)$ is a pseudo Steinberg cross section for ${}^3D_4(q)$ and

$$S_{\mathrm{Tri}}(t, u) := X_1(t)\omega_1 X_2(u)\omega_2 X_3(t^q)\omega_3 X_2(u^q)\omega_2 X_4(t^{q^2})\omega_4 X_2(u^{q^2})\omega_2$$

is a preimage of $\bar{S}_{\mathrm{Tri}}(t, u)$ in $\mathrm{SO}_8^+(\mathrm{IF}_{q^3}(t, u))$. Explicit calculation shows that

$$S_{\mathrm{Tri}}(t, u) = \begin{pmatrix} t & * & -t^q + u^{q+1} & t^{q^2} & u & -u^{q^2} & 1 & . \\ -1 & . & . & . & . & . & . & . \\ . & t^{q^2} - u^{q^2+q} & -u^q & . & -1 & . & . & . \\ . & u^{q^2} & 1 & . & . & . & . & . \\ . & t^q & . & -u^q & . & 1 & . & . \\ . & u & . & -1 & . & . & . & . \\ . & t & . & . & . & . & . & -1 \\ . & 1 & . & . & . & . & . & . \end{pmatrix}$$

with $* = -(t^{q^2}u + t^q u^{q^2} - u^{q^2+q+1})$. This achieves the proof of the first part of the next statement:

Proposition 4.17. *The image $\bar{S}_{\mathrm{Tri}}(t, u)$ of $S_{\mathrm{Tri}}(t, u)$ in $\mathrm{PSO}_8^+(q^3)$ is a pseudo Steinberg cross section for ${}^3D_4(q)$. Its characteristic polynomial is symmetric and has*

the form

$$\begin{aligned} h_{\text{Tri}}(X) = & X^8 + (-t + u^q)(X^7 + X) \\ & + (-t^{q^2}u - tu^q - t^q u^{q^2} + u^{1+q+q^2})(X^6 + X^2) \\ & + (t - t^{q+q^2} - u^{1+q^2} - u^q + t^q u + t^{q^2} u^{q^2})(X^5 + X^3) \\ & + (-2 + 2tu^q + u^2 + u^{2q^2} - 2u^{1+q+q^2} + t^{2q} + t^{2q^2})X^4 + 1. \end{aligned}$$

Proof. During the computation of the coefficients of $h_{\text{Tri}}(X)$ from $S_{\text{Tri}}(t, u)$ it turns out that these are symmetric, i.e., that $h_{\text{Tri}}(X) = \sum_{i=0}^8 a_i X^i$ with $a_{8-i} = a_i$. \square

Proposition 4.18. (a) *The group ${}^3\text{D}_4(q)$ has a cyclic maximal torus \bar{T}_1 of order $q^4 - q^2 + 1$ and a bicyclic maximal torus \bar{T}_2 of order $(q^2 + q + 1)^2$.*

(b) *Every pair of elements $\bar{\gamma}_1, \bar{\gamma}_2$ of \bar{T}_1, \bar{T}_2 of maximal order is a robust generating system of ${}^3\text{D}_4(q)$.*

Proof. Both assertions are immediate from the list of maximal subgroups of ${}^3\text{D}_4(q)$ determined in Kleidman (1988a). Here elements of \bar{T}_1 have preimages in $\mathcal{H}(q)$ with Jordan normal form

$$\text{diag}(v_1, v_1^{q^3}, v_1^{-q^3+q^2+q-1}, v_1^{q^2-q}, v_1^{-q^2+q}, v_1^{q^3-q^2-q+1}, v_1^{-q^3}, v_1^{-1}),$$

respectively

$$\text{diag}(v_2, v_2^{-1}v_3, v_2^{-1}v_3^{1+q}, v_2^{-2q-1}v_3^q, v_2^{2q+1}v_3^{-q}, v_2v_3^{-q-1}, v_2v_3^{-1}, v_2^{-1}),$$

where v_1 is a primitive root of unity of order $q^4 - q^2 + 1$, and v_2, v_3 are roots of unity of order $q^2 + q + 1$ in $\overline{\mathbb{F}_q}^\times$ (see Deriziotis and Michler (1987), Table 1.1). \square

In order to recognize elements of maximal (odd) order in the preimages T_i in $\mathcal{H}(q)$ of \bar{T}_i as specializations of $S_{\text{Tri}}(t, u)$ the following observation of P. Müller is very useful:

Lemma 4.19. *For every $y, z \in \mathbb{F}_q$ with q odd there exists $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ with*

$$\text{tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x(x+y)) + \mathcal{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x) = z.$$

Proof. The minimal polynomial of an element $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ over \mathbb{F}_q has the form

$$g_x(X) = (X - x)(X - x^q)(X - x^{q^2}) = X^3 - a(x)X^2 + b(x)X - c(x)$$

with $a(x) = x + x^q + x^{q^2}$, $b(x) = x^{1+q} + x^{q+q^2} + x^{q^2+1}$ and $c(x) = x^{1+q+q^2}$. So for $y \in \mathbb{F}_q$ we have

$$\text{tr}(x(x+y)) = a(x)^2 - 2b(x) + ya(x).$$

We hence need to find an element $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ with $-c(x) = a(x)^2 - 2b(x) + ya(x) - z$. For this it suffices to prove the existence of elements $a, b \in \mathbb{F}_q$ such that

$$f_{a,b}(X) := X^3 - aX^2 + bX + (a^2 - 2b + ya - z)$$

is irreducible in $\mathbb{F}_q[X]$. Indeed, then every zero x of $f_{a,b}(X)$ is a solution to our problem. We first observe that there certainly is $a \in \mathbb{F}_q$ with

$$f_{a,b}(2) = 8 - 4a + a^2 + ya - z \neq 0$$

(independent of $b \in \mathbb{F}_q$). Furthermore, for every $v \in \mathbb{F}_q \setminus \{2\}$ there exists a unique $b \in \mathbb{F}_q$ satisfying $f_{a,b}(v) = 0$. So there are at most $q - 1$ elements $b \in \mathbb{F}_q$ such that $f_{a,b}(X)$ (with a as chosen above) has a zero in $\mathbb{F}_q \setminus \{2\}$. Thus, we can find $b \in \mathbb{F}_q$ for which $f_{a,b}(X)$ has no zero in \mathbb{F}_q and hence is irreducible. \square

Corollary 4.20. *Let q be odd. Then for $i = 1, 2$ the characteristic polynomials $h_i(X) := h_{\gamma_i}(X)$ are specializations of $h_{\text{Tri}}(X)$.*

Proof. According to Proposition 4.18 the characteristic polynomials $h_i(X)$ of preimages $\gamma_i \in \mathcal{H}(q)$ of $\bar{\gamma}_i$ of odd order are symmetric for $i = 1, 2$, i.e., they are of the form

$$h_i(X) = X^8 + a_i(X^7 + X) + b_i(X^6 + X^2) + c_i(X^5 + X^3) + d_i X^4 + 1$$

with coefficients in \mathbb{F}_{q^3} . Moreover we have $b_i \in \mathbb{F}_q$, and

$$c_i = -a_i^{q^2+q} - a_i \quad \text{and} \quad d_i = a_i^{2q} + a_i^{2q^2} - 2b_i - 2,$$

as can be seen by elementary calculations. Now let $x_i \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ be the solutions from Lemma 4.19 for $(y, z) = (a_i^{q^2}, -b_i)$. Then the specializations

$$\sigma_i : \mathbb{F}_{q^3}[t, u] \longrightarrow \mathbb{F}_{q^3}, \quad t \mapsto -a_i - x_i^q, \quad u \mapsto -x_i,$$

satisfy

$$\sigma_i(a) = \sigma_i(-t + u^q) = a_i + x_i^q - x_i^q = a_i,$$

$$\sigma_i(b) = -\text{tr}(x_i(x_i + a_i^{q^2})) - \mathcal{N}(-x_i) = b_i.$$

Using the above formulas for c_i and d_i this yields

$$\sigma_i(c) = c_i \quad \text{and} \quad \sigma_i(d) = d_i$$

for the corresponding coefficients a, b in $h_{\text{Tri}}(X)$. Hence we have $\sigma_i(h_{\text{Tri}}(X)) = h_i(X)$. Consequently $S_{\text{Tri}}(t, u)$ can be specialized to elements $\tilde{\gamma}_i \in \mathcal{H}(q)$, $i = 1, 2$, with characteristic polynomial $h_i(X)$. \square

For the construction of a Frobenius module for ${}^3\mathrm{D}_4(q)$ we use the 64-dimensional natural linear representation

$$\psi : \mathrm{PSO}_8(\overline{\mathrm{IF}_q(t,u)}) \longrightarrow \mathrm{GL}_{64}(\overline{\mathrm{IF}_q(t,u)})$$

given by conjugation.

Theorem 4.21. *Let q be odd.*

- (a) *The F -module (M_{Tri}, Φ) with $D_B(\Phi) = \psi(\bar{S}_{\mathrm{Tri}})$ over $K = \mathrm{IF}_{q^3}(t,u)$ is dualizable.*
- (b) *The Galois group of (M_{Tri}, Φ) is ${}^3\mathrm{D}_4(q)$.*
- (c) *The corresponding Galois extension N/K is geometric and can be generated by the zeroes of the characteristic polynomial of (M_{Tri}, Φ) .*

Proof. It suffices to show that $\psi(\bar{S}_{\mathrm{Tri}}(t,u))$ can be specialized to a robust generating system of $\psi({}^3\mathrm{D}_4(q))$. By Corollary 4.20, $S_{\mathrm{Tri}}(t,u)$ has specializations $\tilde{\gamma}_1, \tilde{\gamma}_2 \in \mathcal{H}(q)$ with characteristic polynomial $h_i(X)$, for $i = 1, 2$. Their images $\bar{\gamma}_i$ in ${}^3\mathrm{D}_4(q)$ have order divisible by $q^4 - q^2 + 1, q^2 + q + 1$ respectively and thus by Proposition 4.18 form a robust generating pair of ${}^3\mathrm{D}_4(q)$. As ψ commutes with the specializations σ_i , this property is preserved by passage to the 64-dimensional representation of ${}^3\mathrm{D}_4(q)$. \square

The calculation of the generating polynomial of N/K of degree $(q^3)^{64}$ from the equation

$$\psi(\bar{S}_{\mathrm{Tri}})(X_1^{q^3}, \dots, X_{64}^{q^3})^t = (X_1, \dots, X_{64})^t$$

is possible in principle but at present seems out of reach computationally.

5 Field Restriction in Modular Galois Theory

Modular Galois theory has not only the advantage of the existence of non-trivial upper bounds for Galois groups, which has no analogue in characteristic zero, but also possesses the method of field restriction. Here one starts from a Galois extension N/K with group $\mathbf{G}(k)$ over a field of constants $k = \mathbb{F}_q$, which is given by an effective Frobenius module (M, Φ) over K , that is, the representing matrix of the Frobenius operator Φ is an element of $\mathbf{G}(K)$. Then via field restriction the underlying representation of the linear algebraic group \mathbf{G} over \mathbb{F}_q can be transformed to a representation over \mathbb{F}_p . Since this transformation is compatible with specializations used to derive lower bounds, this results for example in the fact that all Galois realizations from the previous two sections over the natural field of definition \mathbb{F}_q of \mathbf{G} can even be realized over the prime field \mathbb{F}_p ; the corresponding generating polynomials are much harder to compute then, though. This method also seems to have been in the intention of Abhyankar in his paper Abhyankar and Keskar (2001). Our presentation here follows Stichel (2014).

5.1 Base Field Reduction

We start with an overview on some known results concerning field restriction. For this let K be a field, say $K = \mathbb{F}_p(t_1, \dots, t_n)$, and L/K a finite field extension as for example $L = \mathbb{F}_q(t_1, \dots, t_n)$ with $q = p^l$. Then the following fact is known from the theory of linear algebraic groups:

Theorem 5.1. *Let K be a field, L/K a finite Galois extension and $\mathbf{G} = \mathbf{G}_L$ a linear algebraic group over L . Then we have:*

(a) *There exists a linear algebraic group $\mathbf{G}^* = \mathbf{G}_K^*$ over K and an L -homomorphism $\Psi : \mathbf{G}_K^* \rightarrow \mathbf{G}_L$ with the following universal mapping property: for all affine varieties \mathcal{Y}_K over K with an L -morphism $\Upsilon : \mathcal{Y}_K \rightarrow \mathbf{G}_L$ there exists exactly one K -morphism $\Delta : \mathcal{Y}_K \rightarrow \mathbf{G}_K^*$ with $\Upsilon = \Psi \circ \Delta$.*

$$\begin{array}{ccc} \mathcal{Y}_K & \xrightarrow{\Delta} & \mathbf{G}_K^* \\ & \searrow \Upsilon & \swarrow \Psi \\ & \mathbf{G}_L & \end{array}$$

(b) *If Υ in (a) is an L -homomorphism, then Δ is an L -homomorphism.*

(c) *If \mathbf{G}_L in (a) is connected then \mathbf{G}_K^* is also connected.*

Proof. The proof is composed of several result in Springer (1998), namely of Thm. 11.4.16 with Exerc. 11.4.20(1) for (a), of Prop. 12.4.2 for (b) and of Exerc. 12.4.7(3) for (c). \square

Remark. From the construction of \mathbf{G}^* , with $G = \text{Gal}(L/K)$ we obtain the relation

$$K[\mathbf{G}^*] \cong \left(\bigotimes_{\sigma \in G} L[\mathbf{G}^\sigma] \right)^G$$

between the coordinate rings.

The algebraic group \mathbf{G}_K^* given by Theorem 5.1 is said to be obtained by *field restriction with respect to L/K from \mathbf{G}_L* . By the universal property it is determined uniquely up to K -isomorphisms. More precisely we may also denote it as

$$\text{Res}_K^L(\mathbf{G}_L) := \mathbf{G}_K^*.$$

It enjoys the following properties:

Corollary 5.2. *Let L/K be a finite Galois extension with group $G = \text{Gal}(L/K)$, \mathbf{G} a linear algebraic group over L and $\mathbf{G}^* = \text{Res}_K^L(\mathbf{G})$. Then:*

- (a) $\mathbf{G}^*(K^{\text{sep}}) \cong \mathbf{G}(K^{\text{sep}} \otimes_K L)$.
- (b) $\mathbf{G}^*(L) \cong \prod_{\sigma \in G} \mathbf{G}^\sigma(L)$ and Ψ is the projection onto the factor indexed by the identity element of G .

Proof. Again the results are taken from Springer (1998), Ch. 12.4.4 for (a), and Prop 11.4.22 and Ch. 12.4.5 for (b). \square

In order to make field restriction somewhat more concrete we choose a basis y_1, \dots, y_l of L/K . Then there exists a K -linear isomorphism

$$\lambda : L \longrightarrow \bigoplus_{i=1}^l Ky_i, \quad \sum_{i=1}^l a_i y_i \mapsto a_1 y_1 + \dots + a_l y_l,$$

inducing for all $m \geq 1$ a K -linear embedding

$$\Lambda : \text{GL}_m(L) \longrightarrow \text{GL}_{ml}(K), \quad \gamma \in \text{Aut}(L^m) \mapsto \Lambda(\gamma) \in \text{Aut}(K^{ml}),$$

with matrices γ with respect to a basis x_1, \dots, x_m and $\Lambda(\gamma)$ with respect to the basis $\{x_i y_j\}$. With these notations we obtain:

Corollary 5.3. *Let L/K be a finite Galois extension with group G and \mathbf{G} a linear algebraic group over L . Then:*

- (a) $\mathbf{G}^*(K) \cong \Lambda(\mathbf{G}(L))$ as groups.
- (b) For any $A \in \mathbf{G}(L)$ the characteristic polynomial of $\Lambda(A)$ splits as

$$h_{\Lambda(A)}(X) = \prod_{\sigma \in G} h_{A^\sigma}(X).$$

Proof. Let $\mathbf{H}_K := \Lambda(\mathbf{G}(L))$ be the finite linear algebraic group defined over K and $\Upsilon : \mathbf{H}_K \rightarrow \mathbf{G}$ the embedding defined over L . Then by Theorem 5.1 there exists a

K -homomorphism $\Delta : \mathsf{H}_K \rightarrow \mathsf{G}^*$ with $\Psi \circ \Delta = \Upsilon$. From this we obtain a sequence of homomorphisms

$$\mathsf{H}_K \xrightarrow{\Delta} \mathsf{G}^*(K) \hookrightarrow \mathsf{G}^*(L) \xrightarrow{\psi} \prod_{\sigma \in G} \mathsf{G}^\sigma(L),$$

where ψ , according to Corollary 5.2(b), is the projection onto the factor with $\sigma = 1$. Due to $\Psi \circ \Delta = \Upsilon$ we hence have $\Lambda(\mathsf{G}(L)) \cong \mathsf{G}(L)$, and Δ is injective. As moreover ψ is injective on $\mathsf{G}^*(K)$ by Springer (1998), Prop. 12.4.6, we have $\mathsf{G}(L) \cong \mathsf{G}^*(K)$. This shows (a).

Assertion (b) follows immediately from Corollary 5.2(b), as taking the characteristic polynomial is compatible with extension of constants. \square

5.2 Application to Groups of Lie Type

We start with a typical example, namely the Galois extension N/L with group $\mathsf{G}_{A_n}(\mathbb{F}_q) = \mathrm{SL}_{n+1}(q)$ constructed in Section 3.1. This originated from a Frobenius module (M_{A_n}, Φ) with $D_B(\Phi) = S_{A_n}(t_1, \dots, t_n)$ over $L = \mathbb{F}_q(t_1, \dots, t_n)$. Now we choose a basis y_1, \dots, y_l of $\mathbb{F}_q/\mathbb{F}_p$, which is also a basis of L/K for $K = \mathbb{F}_p(t_1, \dots, t_n)$, and replace the transcendentals t_i by $t_i^* := \sum_{j=1}^l t_{ij} y_j$ with new transcendentals t_{ij} . Then from Proposition 3.2 we obtain the characteristic polynomial

$$h_{A_n}(t_1^*, \dots, t_n^*) = X^{n+1} + \sum_{i=1}^n (-1)^{i-1} t_i^* X^{n+1-i} + (-1)^{n+1}.$$

Let us write $\mathbf{t}^* = (t_1^*, \dots, t_n^*)$ and $\underline{\mathbf{t}} = (t_1, \dots, t_n)$. The Λ -image of the Steinberg cross section $S_{A_n}(t_1, \dots, t_n)$ will be denoted by

$$S_{A_n}^*(\underline{\mathbf{t}}) := \Lambda(S_{A_n}(\mathbf{t}^*)) \in \mathsf{G}^*(\mathbb{F}_p(\underline{\mathbf{t}}))$$

with $\mathsf{G}^* = \mathrm{Res}_K^L(\mathrm{SL}_{n+1})$, and its characteristic polynomial by

$$h_{A_n}^*(\underline{\mathbf{t}}) := \prod_{\sigma \in G} h_{A_n}^\sigma(\mathbf{t}^*)$$

where $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Here, the Galois action is given by $\sigma(t_i^*) = \sum_{j=1}^l t_{ij} \sigma(y_j)$.

Now let $(M_{A_n}^*, \Phi)$ be the $l(n+1)$ -dimensional F-module over $K^* = \mathbb{F}_p(\underline{\mathbf{t}})$ with $D_B(\Phi) = S_{A_n}^*(\underline{\mathbf{t}}) \in \Lambda(\mathrm{SL}_{n+1}(\mathbb{F}_q(\mathbf{t}^*)))$. This is obviously dualizable. Now SL_{n+1} is connected, hence so is $\mathrm{Res}_K^L(\mathrm{SL}_{n+1})$ by Theorem 5.1(c). Thus $\mathrm{Gal}(M_{A_n}^*, \Phi)$

by Theorem 1.9 becomes a subgroup of $\mathbf{G}^*(\mathbb{F}_p) \cong \Lambda(\mathrm{SL}_{n+1}(q)) \cong \mathrm{SL}_{n+1}(q)$. We now want to compare the lower bounds. For this let (γ_1, γ_2) , respectively $(\gamma_1, \gamma_2, \gamma_3)$ be the robust generating system of $\mathrm{SL}_{n+1}(q)$ from Proposition 3.3. Due to $\Lambda(\mathbf{G}(\mathbb{F}_q)) \cong \mathbf{G}^*(\mathbb{F}_p) \cong \mathbf{G}(\mathbb{F}_q)$ their images $\Lambda(\gamma_i)$ form a robust generating system of $\Lambda(\mathrm{SL}_{n+1}(q))$. Now let $t_i \mapsto c_i \in \mathbb{F}_q$ denote the specialization in Theorem 3.4, which maps $S_{A_n}(\mathbf{t})$ to an element conjugate to γ_1 , and write $c_i = \sum_{j=1}^l c_{ij} y_j$ with $c_{ij} \in \mathbb{F}_p$. Then the specialization $t_{ij} \mapsto c_{ij} \in \mathbb{F}_p$ maps $S_{A_n}^*(\mathbf{t})$ to an element that is $\Lambda(\mathrm{GL}_{n+1}(q))$ -conjugate to $\Lambda(\gamma_1)$. The analogous observation applies to γ_2 and γ_3 . So by Corollary 2.13 the group $\Lambda(\mathrm{SL}_{n+1}(q))$ is also a lower bound for $\mathrm{Gal}(M_{A_n}^*, \Phi)$. Consequently, we have

$$\mathrm{Gal}(M_{A_n}^*, \Phi) = \mathrm{SL}_{n+1}(q),$$

and $\mathrm{SL}_{n+1}(q)$ occurs as the Galois group of a geometric Galois extension over $K^* = \mathbb{F}_p(t_{11}, \dots, t_{nl})$.

Completely analogous considerations lead to the following statement:

Theorem 5.4. *Let \mathbf{G} be one of the groups of Lie type*

$$\begin{aligned} \mathrm{SL}_{n+1}(q), \mathrm{Sp}_{2n}(q), \mathrm{SO}_{2n+1}(q), \mathrm{SO}_{2n}^+(q), G_2(q), \mathrm{SU}_n(q), \\ \mathrm{SO}_{2n}^-(q), {}^2\mathrm{B}_2(q^2), {}^2\mathrm{G}_2(q^2), {}^3\mathrm{D}_4(q) \end{aligned}$$

with their corresponding representations in $\mathrm{GL}_m(\tilde{q})$ as considered in Paragraphs 3 and 4 (where $\tilde{q} = q$ or $\tilde{q} = q^2$ according to the cases). Then writing $\tilde{q} = p^l$ we have:

- (a) *The Frobenius module $(M_{\mathbf{G}}^*, \Phi)$ with $D_B(\Phi) = S_{\mathbf{G}}^*(\mathbf{t}) \in \Lambda(\mathbf{G}(\mathbb{F}_{\tilde{q}}(\mathbf{t}^*)))$ over $K^* = \mathbb{F}_p(\mathbf{t})$ is dualizable.*
- (b) *The Galois group $\mathrm{Gal}(M_{\mathbf{G}}^*, \Phi)$ over K^* is $\mathbf{G}(\mathbb{F}_{\tilde{q}})$.*
- (c) *The corresponding Galois extension N^*/K^* is generated by a characteristic polynomial of $(M_{\mathbf{G}}^*, \Phi)$. It can be computed from the algebraic system*

$$S_{\mathbf{G}}^*(\mathbf{t})(X_1^p, \dots, X_{ml}^p)^t = (X_1, \dots, X_{ml})^t.$$

Proof. The proof can in all cases be achieved in complete analogy to the above example of $\mathrm{SL}_{n+1}(q)$. Here s should — if it occurs — be split up as $s = \sum_{j=1}^l s_j y_j$ into the additional transcendentals s_1, \dots, s_l . \square

5.3 Explicit Polynomials for $\mathrm{SL}_{n+1}(q)$

In this section we present polynomials for some special Galois extensions obtained by field restriction.

We start with the group $\mathbf{G}_{A_n}(\mathbb{F}_q) = \mathrm{SL}_{n+1}(q)$ for $q = 4$. For this let $\mathbb{F}_4 = \mathbb{F}_2(x)$ with $x^2 + x = 1$, and set $t_i^* = t_i + u_i x$. Then we have

$$S_{A_n}^*(\mathbf{t}, \mathbf{u}) = \Lambda(S_{A_n}(\mathbf{t}^*)) = \begin{pmatrix} t_1 & \dots & t_n & 1 & u_1 & \dots & u_n & 0 \\ 1 & & & 0 & & & & \\ & \ddots & & & & & & \\ & & 1 & 0 & & & & \\ u_1 & \dots & u_n & 0 & t_1 + u_1 & \dots & t_n + u_n & 1 \\ & & & & 1 & & & 0 \\ & & & & & \ddots & & \\ & & & & & & 1 & 0 \end{pmatrix}.$$

From the corresponding system of algebraic equations

$$S_{A_n}^*(\mathbf{t}, \mathbf{u})(X_1^2, \dots, X_{n+1}^2, Y_1^2, \dots, Y_{n+1}^2)^t = (X_1, \dots, Y_{n+1})^t$$

one obtains the equations

$$\begin{aligned} \sum_{i=1}^n t_i X_i^2 + X_{n+1}^2 + \sum_{i=1}^n u_i Y_i^2 &= X_1, \quad X_i^2 = X_{i+1} \text{ for } i = 1, \dots, n, \\ \sum_{i=1}^n u_i X_i^2 + \sum_{i=1}^n (t_i + u_i) Y_i^2 + Y_{n+1}^2 &= Y_1, \quad Y_i^2 = Y_{i+1} \text{ for } i = 1, \dots, n. \end{aligned}$$

This first yields $X_i = X^{2^{i-1}}$, $Y_i = Y^{2^{i-1}}$ for $X = X_1$, $Y = Y_1$, and then we obtain from Theorem 5.4:

Proposition 5.5. *Let $f(X)$ respectively $g(Y)$ be the polynomial which is obtained by elimination of Y resp. of X from the system*

$$\begin{aligned} \sum_{i=1}^n t_i X^{2^i} + X^{2^{n+1}} + \sum_{i=1}^n u_i Y^{2^i} &= X, \\ \sum_{i=1}^n u_i X^{2^i} + \sum_{i=1}^n (t_i + u_i) Y^{2^i} + Y^{2^{n+1}} &= Y. \end{aligned}$$

Then the field $N_{A_n}^$ generated over $\mathbb{F}_2[\mathbf{t}, \mathbf{u}]$ by the zeroes of f , respectively g , has Galois group*

$$\mathrm{Gal}(N_{A_n}^*/\mathbb{F}_2(\mathbf{t}, \mathbf{u})) \cong \mathrm{SL}_{n+1}(4).$$

Example 5.1. For $n = 1$, $t_1 = t$ and $u_1 = u$ the equations in Proposition 5.5 read

$$tX^2 + X^4 + uY^2 = X, \quad uX^2 + (t+u)Y^2 + Y^4 = Y,$$

from which one first obtains

$$Y^2 = \frac{1}{u}(X^4 + tX^2 + X) \quad \text{and} \quad Y^2 = u^2X^4 + (t+u)^2Y^4 + Y^8$$

and from this by replacing Y^2 in the second equation the polynomial

$$\begin{aligned} X^{16} + (t^4 + t^2u^2 + u^4)X^8 + (t^4u^2 + u^4t^2 + u^6 + u^3 + 1)X^4 \\ + (u^2t^2 + u^3t + u^4)X^2 + u^3X = 0. \end{aligned}$$

By Proposition 5.5 this has Galois group $\mathrm{SL}_2(4)$ over $\mathrm{IF}_2(t, u)$. \square

The second example concerns the groups $\mathbf{G}_{\mathrm{A}_n}(\mathrm{IF}_q) = \mathrm{SL}_{n+1}(q)$ with $q = p^2 \neq 4$. Here let $\mathrm{IF}_q = \mathrm{IF}_p(x)$ with $x^2 = y \in \mathrm{IF}_p$ and $t_i^* = t_i + xu_i$. Then according to Proposition 3.2 we get

$$S_{\mathrm{A}_n}^*(\mathbf{t}, \mathbf{u}) = \begin{pmatrix} -t_1 & \dots & -t_n & 1 & -u_1y & \dots & -u_ny & 0 \\ -1 & & & & 0 & & & \\ & \ddots & & & & & & \\ & & -1 & 0 & & & & \\ -u_1 & \dots & -u_n & 0 & -t_1 & \dots & -t_n & 1 \\ & & & & -1 & & & 0 \\ & & & & & \ddots & & \\ & & & & & & -1 & 0 \end{pmatrix}.$$

The system of algebraic equations

$$S_{\mathrm{A}_n}^*(\mathbf{t}, \mathbf{u})(X_1^p, \dots, X_{n+1}^p, Y_1^p, \dots, Y_{n+1}^p)^t = (X_1, \dots, Y_{n+1})^t$$

then leads to the equations

$$\begin{aligned} -\sum_{i=1}^n t_i X_i^p + X_{n+1}^p - \sum_{i=1}^n u_i y Y_i^p &= X_1, \quad -X_i^p = X_{i+1} \text{ for } i = 1, \dots, n, \\ -\sum_{i=1}^n u_i X_i^p - \sum_{i=1}^n t_i Y_i^p + Y_{n+1}^p &= Y_1, \quad -Y_i^p = Y_{i+1} \text{ for } i = 1, \dots, n. \end{aligned}$$

From this one finds $X_i = (-1)^{i-1}X^{p^{i-1}}$ for $X = X_1$ and $Y_i = (-1)^{i-1}Y^{p^{i-1}}$ for $Y = Y_1$. This shows:

Proposition 5.6. *Assume $p > 2$ and let $f(X)$ respectively $g(Y)$ be the polynomial which is obtained by elimination of Y resp. of X from the system*

$$X + \sum_{i=1}^n (-1)^{i-1} t_i X^{p^i} + (-1)^n X^{p^{n+1}} + \sum_{i=1}^n (-1)^{i-1} u_i y Y^{p^i} = 0,$$

$$Y + \sum_{i=1}^n (-1)^{i-1} u_i X^{p^i} + \sum_{i=1}^n (-1)^{i-1} t_i Y^{p^i} + (-1)^n Y^{p^{n+1}} = 0.$$

Then the field $N_{A_n}^*$ generated over $\mathbb{F}_p[\mathbf{t}, \mathbf{u}]$ by the zeroes of f , respectively of g , has Galois group

$$\text{Gal}(N_{A_n}^*/\mathbb{F}_p(\mathbf{t}, \mathbf{u})) \cong \text{SL}_{n+1}(p^2).$$

Example 5.2. We again give explicit polynomials for $\text{SL}_2(p^2)$, $p > 2$. For this let $n = 1$, $t = t_1$ and $u = u_1$. Then the equations in Proposition 5.6 become

$$X + tX^p - X^{p^2} + uyY^p = 0, \quad Y + uX^p + tY^p - Y^{p^2} = 0.$$

From these by elimination of X one obtains the polynomial

$$\begin{aligned} Y^{p^4} - (t^{p^2} + t^p u^{p^2-p}) Y^{p^3} + (t^{2p} u^{p^2-p} - y u^{p^2+p} - u^{p^2-1} - 1) Y^{p^2} \\ + (t^p u^{p^2-p} + t u^{p^2-1}) Y^p + u^{p^2-1} Y \end{aligned}$$

with Galois group $\text{SL}_2(p^2)$ over $\mathbb{F}_p(t, u)$ for $p \neq 2$. □

VI Rigid Analytic Methods

The solution of the inverse problem of Galois theory over the field $\mathbb{C}(t)$ was achieved by a blend of topological and analytical methods. A similar approach is possible for any ground field complete with respect to a non-archimedean valuation. The suitable analytic structures are provided by the so-called rigid analytic spaces. They satisfy a GAGA-principle, which makes it possible to recover algebraic structures from analytic constructions. This replaces the Riemann Existence Theorem in the complex case. In the first paragraph we collect some definitions and results on rigid analytic geometry and sketch a proof of the GAGA-principle for covers of the rigid analytic projective line.

With these prerequisites it is then possible to solve the inverse problem for the rational function field over a complete ultrametric field. This includes in particular the rational function field over the field \mathbb{Q}_p of p -adic numbers. The solution is achieved by a cut and paste process mimicking the complex case. Further we solve the inverse problem over $\overline{\mathbb{F}}_p(t)$ for any prime p by specializing Galois extensions of $\overline{\mathbb{F}}_p((u))(t)$. The result is due to Harbater (1984), who used formal geometry instead of rigid analytic geometry. Harbater (1995a) and Pop (1995) later showed how to solve sufficiently many embedding problems over $\overline{\mathbb{F}}_p(t)$ in order to conclude the freeness of the absolute Galois group of this field from the Freiheitssatz of Iwasawa.

In the third paragraph we show how to construct large free quotients of fundamental groups of function fields over complete ultrametric fields with explicit information on the action of the Galois group, following Pop (1994). Using the gluing procedure, one first obtains free products of finite groups as Galois groups, and then, taking a suitable projective limit, also free groups. This is used in the fourth paragraph to solve embedding problems over function fields over large fields as introduced by Pop (1996). This allows to prove that the absolute Galois group of a countable Hilbertian PAC-field is free profinite, generalizing Theorem IV.3.8.

In the final paragraph, we first prove the projectivity of the fundamental group of an affine curve. We then state the conjecture of Abhyankar (1957) concerning the finite quotients of the fundamental group in positive characteristic with fixed number of ramification points, and give some hints on the recent proof by Raynaud (1994).

for the case of the affine line of this conjecture (see also Saïdi (2000)). Finally we prove the reduction of the general case to the 1-point case, due to Harbater (1994a), following Pop (1995).

1 Results from Rigid Analytic Geometry

Rigid analytic spaces are best defined locally via their algebras of holomorphic functions, the Tate algebras. We then introduce coherent sheaves on rigid analytic spaces and sketch a proof of the 1-dimensional GAGA-theorem. The definitions and results in this paragraph, unless otherwise stated, are taken from Fresnel and van der Put (1981) or Bosch, Güntzer and Remmert (1984).

1.1 Tate Algebras

In the whole paragraph, k denotes a field complete with respect to a valuation with corresponding ultrametric absolute value $|\cdot| : k \rightarrow \mathbb{R}$. The valuation ring and valuation ideal are

$$k^0 := \{z \in k \mid |z| \leq 1\}, \quad k^{00} := \{z \in k \mid |z| < 1\}, \quad (1.1)$$

with residue class field k^0/k^{00} . For an integer $n \geq 1$ we define

$$T_n := T_n(k) := k\langle Z_1, \dots, Z_n \rangle := \left\{ \sum_{\mathbf{j} \in \mathbb{N}_0^n} a_{\mathbf{j}} \mathbf{Z}^{\mathbf{j}} \mid a_{\mathbf{j}} \in k, \lim_{\sum_i j_i \rightarrow \infty} (a_{\mathbf{j}}) = 0 \right\}, \quad (1.2)$$

the ring of convergent power series in the n indeterminates $\mathbf{Z} = (Z_1, \dots, Z_n)$ on the unit disc with respect to the ultrametric absolute value $|\cdot|$, where $\mathbf{Z}^{\mathbf{j}} := Z_1^{j_1} \cdots Z_n^{j_n}$, and $\mathbf{j} = (j_1, \dots, j_n)$. Now

$$\left\| \sum_{\mathbf{j} \in \mathbb{N}_0^n} a_{\mathbf{j}} \mathbf{Z}^{\mathbf{j}} \right\| := \max\{|a_{\mathbf{j}}| \mid \mathbf{j} \in \mathbb{N}_0^n\}$$

defines a norm on the algebra T_n . As for k above, we set

$$T_n(k)^0 := \{f \in T_n(k) \mid \|f\| \leq 1\}, \quad T_n(k)^{00} := \{f \in T_n(k) \mid \|f\| < 1\}.$$

Then the residue ring $T_n(k)^0/T_n(k)^{00}$ is canonically isomorphic to the polynomial ring in n indeterminates over the residue class field k^0/k^{00} .

A *Tate algebra* A over k is a finite extension of $T_n(k)$ for some n . Here finite extension means that A is finitely generated as a T_n -module. The following properties of Tate algebras can be proved by elementary calculations, using an analogue of the Weierstraß division and preparation theorem. For a proof see Fresnel and van der Put (1981), Thm. II.3, or Bosch, Güntzer and Remmert (1984), 5.2.6, 6.1.2, 6.1.3 and 6.2.4.

Theorem 1.1. (a) *Tate algebras are Noetherian rings.*

(b) *T_n is a unique factorization domain.*

(c) *For any maximal ideal \mathfrak{m} of T_n , T_n/\mathfrak{m} is a finite extension of k .*

- (d) Every Tate algebra has the form $A = T_n/\mathfrak{a}$ for some n and some ideal $\mathfrak{a} \triangleleft T_n$.
- (e) Algebra homomorphisms between Tate algebras are continuous; all Banach norms on a Tate algebra are equivalent.

Let A be a Tate algebra over k . By Theorem 1.1(d) there exist n and $\mathfrak{a} \triangleleft T_n$ with $A = T_n/\mathfrak{a}$, where $T_n = k\langle Z_1, \dots, Z_n \rangle$. We can then define

$$A\langle Y_1, \dots, Y_m \rangle := k\langle Z_1, \dots, Z_n, Y_1, \dots, Y_m \rangle / (\mathfrak{a} \cdot k\langle Z_1, \dots, Z_n, Y_1, \dots, Y_m \rangle)$$

for any finite set $\{Y_1, \dots, Y_m\}$ of further indeterminates. This is independent of the choice of presentation for A . By $\text{Sp}(A)$ we denote the set of maximal ideals of A . For $f \in A$ and $\mathfrak{m} \in \text{Sp}(A)$ we define $f(\mathfrak{m})$ to be the image of f in A/\mathfrak{m} . By Theorem 1.1(c) and (d), A/\mathfrak{m} is a finite field extension of k , so the absolute value $|\cdot|$ has a unique extension to A/\mathfrak{m} and it makes sense to speak of $|f(\mathfrak{m})|$. We define a topology on $\mathcal{X} = \text{Sp}(A)$, to be generated by the sets of the form $\mathcal{U}_f := \{\mathfrak{m} \in \mathcal{X} \mid |f(\mathfrak{m})| \leq 1\}$, where f runs over A . A subset $\mathcal{R} \subseteq \text{Sp}(A)$ is called a *rational subset* (in \mathcal{X}) if there exist $f_0, \dots, f_n \in A$ with

$$\mathcal{R} = \{\mathfrak{m} \in \text{Sp}(A) \mid |f_i(\mathfrak{m})| \leq |f_0(\mathfrak{m})| \text{ for } 1 \leq i \leq n\} \quad (1.3)$$

and A is generated by f_0, \dots, f_n as an ideal: $A = (f_0, \dots, f_n)$.

To each rational subset $\mathcal{R} \subseteq \text{Sp}(A)$ we associate the Tate algebra

$$B := A\langle X_1, \dots, X_n \rangle / (f_1 - X_1 f_0, \dots, f_n - X_n f_0). \quad (1.4)$$

The canonical homomorphism $\varphi : A \rightarrow B$ induces a homeomorphism $\text{Sp}(\varphi) : \text{Sp}(B) \rightarrow \mathcal{R} \subseteq \text{Sp}(A)$, such that B satisfies the following universal mapping property: For any homomorphism $\psi : A \rightarrow C$ of Tate algebras with $\text{Sp}(\psi)(\text{Sp}(C)) \subseteq \mathcal{R}$ there exists a unique homomorphism $\tau : B \rightarrow C$ such that $\tau \circ \varphi = \psi$. In particular, a rational subset \mathcal{R} is of the form $\text{Sp}(B)$ for some Tate algebra B which is independent of the choice of the elements f_0, \dots, f_n used to present \mathcal{R} (see Fresnel and van der Put (1981), Lemme III.1.2). We write $\mathcal{O}_{\mathcal{X}}(\mathcal{R}) := B$, where $\mathcal{X} = \text{Sp}(A)$, and call it the *ring of holomorphic functions on \mathcal{R}* . The following properties of rational sets are elementary (see Fresnel and van der Put (1981), Lemme III.1.3, or Bosch, Güntzer and Remmert (1984), 7.2.3, 7.2.4).

Proposition 1.2. (a) If $\mathcal{R}_1, \mathcal{R}_2$ are rational in $\mathcal{X} = \text{Sp}(A)$, then so is $\mathcal{R}_1 \cap \mathcal{R}_2$, and we have $\mathcal{O}_{\mathcal{X}}(\mathcal{R}_1 \cap \mathcal{R}_2) = \mathcal{O}_{\mathcal{X}}(\mathcal{R}_1) \hat{\otimes}_A \mathcal{O}_{\mathcal{X}}(\mathcal{R}_2)$.

(b) If $\mathcal{R}_1 \subseteq \mathcal{R}_2 \subseteq \mathcal{X}$, and \mathcal{R}_1 is rational in \mathcal{R}_2 , while \mathcal{R}_2 is rational in \mathcal{X} , then \mathcal{R}_1 is also rational in \mathcal{X} .

Here $\hat{\otimes}_A$ denotes the complete tensor product, see Bosch, Güntzer and Remmert (1984), 2.1.7.

1.2 Rigid Analytic Spaces

Let A be a Tate algebra. In order to obtain the right notion of sheaves on the space $\mathcal{X} = \text{Sp}(A)$ of maximal ideals of A we introduce a Grothendieck topology (see for example Bosch, Güntzer and Remmert (1984), 9.1). For this let the *admissible subsets* of \mathcal{X} be the finite unions of rational subsets. The *admissible coverings* are the finite coverings by admissible subsets. It can be verified that this defines a Grothendieck topology T on \mathcal{X} (see Bosch, Güntzer and Remmert (1984), 9.1.4). Then by Proposition 1.2 a (pre-) sheaf of rings on T is given by $\mathcal{R} \mapsto \mathcal{O}_{\mathcal{X}}(\mathcal{R})$ for rational subsets $\mathcal{R} \subseteq \mathcal{X}$. For any finitely generated A -module M define \tilde{M} to be the presheaf with $\mathcal{R} \mapsto \tilde{M}(\mathcal{R}) := M \otimes_A \mathcal{O}_{\mathcal{X}}(\mathcal{R})$. The non-trivial fact that these define sheaves was first proved by Tate (see Fresnel and van der Put (1981), Thm. III.2.2, or Bosch, Güntzer and Remmert (1984), 8.2.1):

Theorem 1.3 (Tate). *Let A be a Tate algebra, M a finitely generated A -module. Then every admissible covering of $\mathcal{X} = \text{Sp}(A)$ is acyclic for the (pre-) sheaf \tilde{M} . In particular, $\mathcal{O}_{\mathcal{X}}$ and \tilde{M} are sheaves.*

The ringed space $(\text{Sp}(A), T, \mathcal{O}_{\text{Sp}(A)})$ is called an *affinoid analytic space*, with structure sheaf (or sheaf of holomorphic functions) $\mathcal{O}_{\text{Sp}(A)}$.

More generally, a ringed space $(\mathcal{X}, T, \mathcal{O}_{\mathcal{X}})$ consisting of a space \mathcal{X} with a Grothendieck topology T and a sheaf $\mathcal{O}_{\mathcal{X}}$ on \mathcal{X} is called a *rigid analytic space*, if there exists an admissible covering $\{\mathcal{X}_i \mid i \in I\}$ of \mathcal{X} such that $(\mathcal{X}_i, T|_{\mathcal{X}_i}, \mathcal{O}_{\mathcal{X}}|_{\mathcal{X}_i})$ is an affinoid analytic space for all $i \in I$. A *morphism of rigid analytic spaces* is by definition a morphism of locally ringed spaces with Grothendieck topology.

An important method for constructing rigid analytic spaces is by gluing. For this we first define a *gluing datum*. This consists of a family $\{\mathcal{X}_i \mid i \in I\}$ of affinoid analytic spaces, with rational subsets $\mathcal{X}_{ij} \subseteq \mathcal{X}_i$ and isomorphisms of analytic spaces $\varphi_{ji} : \mathcal{X}_{ij} \xrightarrow{\sim} \mathcal{X}_{ji}$ for all $i, j \in I$, satisfying the following properties:

- (1) $\mathcal{X}_{ii} = \mathcal{X}_i$, $\varphi_{ii} = \text{Id}_{\mathcal{X}_i}$ for all $i \in I$,
- (2) φ_{ij} is inverse to φ_{ji} for all $i, j \in I$,
- (3) $\varphi_{kj} \circ \varphi_{ji} = \varphi_{ki}$ on $\mathcal{X}_{ij} \cap \mathcal{X}_{ik}$ for all $i, j, k \in I$.

Note that $\mathcal{X}_{ij} = \mathcal{X}_{ji} = \emptyset$ is allowed. Gluing data define rigid analytic spaces:

Proposition 1.4 (Gluing of Spaces). *Let $\{\mathcal{X}_i \mid i \in I\}$, $\{\mathcal{X}_{ij}, \varphi_{ij} \mid i, j \in I\}$ be a gluing datum. Then there exists a rigid analytic space $(\mathcal{X}, T, \mathcal{O}_{\mathcal{X}})$ unique up to isomorphism with the following properties:*

- (a) *there exist homeomorphisms $\psi_i : \mathcal{X}_i \rightarrow \psi_i(\mathcal{X}_i) \subseteq \mathcal{X}$ onto open subsets of \mathcal{X} ,*
- (b) *$\mathcal{X} = \bigcup_{i \in I} \psi_i(\mathcal{X}_i)$ is an admissible covering,*
- (c) *$\psi_i(\mathcal{X}_{ij}) = \psi_j(\mathcal{X}_{ji}) = \psi_i(\mathcal{X}_i) \cap \psi_j(\mathcal{X}_j)$, and $\varphi_{ji} = \psi_j^{-1} \circ \psi_i$ on \mathcal{X}_{ij} for all $i, j \in I$,*
- (d) *ψ_i induces an isomorphism between the structure sheaf $\mathcal{O}_{\mathcal{X}_i}$ and $\mathcal{O}_{\mathcal{X}}|_{\mathcal{X}_i}$.*

For a proof see Bosch, Güntzer and Remmert (1984), 9.3.2. Similarly, morphisms of rigid analytic spaces may be glued (see loc. cit., 9.3.3).

Proposition 1.5 (Gluing of Morphisms). *Let \mathcal{X} and \mathcal{Y} be analytic spaces with admissible coverings $\{\mathcal{X}_i \mid i \in I\}$, $\{\mathcal{Y}_i \mid i \in I\}$. Let $\{\varphi_i : \mathcal{Y}_i \rightarrow \mathcal{X}_i \mid i \in I\}$ be analytic morphisms such that φ_i and φ_j have same restriction to $\mathcal{Y}_i \cap \mathcal{Y}_j$ for all $i, j \in I$. Then there exists a unique analytic morphism $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ with $\varphi|_{\mathcal{Y}_i} = \varphi_i$ for all $i \in I$.*

A rigid analytic space $(\mathcal{X}, T, \mathcal{O}_{\mathcal{X}})$ is called *connected* if the only idempotent global sections of $\mathcal{O}_{\mathcal{X}}$ are the constants 0 and 1. The following criteria for connectedness will be used in subsequent constructions:

Lemma 1.6. *Let $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ be an admissible covering of a rigid analytic space by connected analytic spaces \mathcal{X}_i such that $\mathcal{X}_1 \cap \mathcal{X}_2$ is non-empty. Then \mathcal{X} is connected.*

Proof. Let $f \in \mathcal{O}_{\mathcal{X}}(\mathcal{X})$ be an idempotent global section. Then for $i = 1, 2$ the restriction $f|_{\mathcal{X}_i}$ is an idempotent global section on \mathcal{X}_i , hence constant since \mathcal{X}_i is connected. Restriction to the non-empty intersection $\mathcal{X}_1 \cap \mathcal{X}_2$ shows that these two constants must in fact coincide. Thus f is constant, proving the connectedness of \mathcal{X} . \square

This will be particularly interesting for the gluing of spaces:

Corollary 1.7. *In the setting of Proposition 1.4 assume that all the \mathcal{X}_i are connected, and for each pair $i, j \in I$ there exists a sequence $i = i_1, i_2, \dots, i_n = j$ of indices in I such that $\mathcal{X}_{i_m, i_{m+1}} \neq \emptyset$ for $m = 1, \dots, n - 1$. Then \mathcal{X} is connected.*

Proof. Induction on the length of a chain of indices as in the assumption, with Lemma 1.6 as induction base, shows the following: if $f \in \mathcal{O}_{\mathcal{X}}(\mathcal{X})$ is idempotent then for any pair $i, j \in I$ the two constant functions $f|_{\mathcal{X}_i}, f|_{\mathcal{X}_j}$ agree. Thus any idempotent global section on \mathcal{X} is constant. \square

Lemma 1.8. *Let $\mathcal{X} = \bigcup_{i=0}^n \mathcal{X}_i$ be an admissible covering of a connected analytic space such that $\mathcal{X}_0 \cap \mathcal{X}_i$ is connected for $i = 1, \dots, n$ and $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ for $1 \leq i < j \leq n$. Then \mathcal{X}_0 is connected.*

Proof. Let $f_0 \in \mathcal{O}_{\mathcal{X}_0}(\mathcal{X}_0)$ be an idempotent global section. Since $\mathcal{X}_0 \cap \mathcal{X}_i$ is connected, the restriction $f_0|_{\mathcal{X}_0 \cap \mathcal{X}_i} = a_i$ is constant. Let $f_i \in \mathcal{O}_{\mathcal{X}_i}(\mathcal{X}_i)$ be the constant function a_i for $1 \leq i \leq n$. Then by Proposition 1.4 (Gluing of Spaces) the f_i , $i = 0, \dots, n$, may be glued to a function $f \in \mathcal{O}_{\mathcal{X}}(\mathcal{X})$ which is idempotent since the f_i are. But \mathcal{X} is connected, so f is constant, and hence $f_0 = f|_{\mathcal{X}_0}$ is constant as well. \square

We conclude this section with some standard examples of affinoid analytic spaces.

Example 1.1 (Discs). Let k be algebraically closed. By Theorem 1.1(c) we then have $T_1/\mathfrak{m} \cong k$ for every $\mathfrak{m} \in \mathcal{X} = \mathrm{Sp}(k\langle Z \rangle) = \mathrm{Sp}(T_1)$. For $z \in k$ with $|z| > 1$ the element $Z - z$ is invertible in T_1 , so it does not generate a proper ideal of T_1 . We

may hence identify the topological space $\mathcal{X} = \text{Sp}(T_1)$ with $k^0 = \{z \in k \mid |z| \leq 1\}$ via the map $(Z - z)T_1 \mapsto z$. In particular, T_1 is the ring of holomorphic functions on the unit disc k^0 . By suitable translation and scaling, this gives the holomorphic functions on discs centered at arbitrary points.

More generally we thus obtain that the topological space $\mathcal{X} = \text{Sp}(T_n)$ can be identified with the polydisc

$$\{\mathbf{z} = (z_1, \dots, z_n) \in k^n \mid |z_i| \leq 1 \text{ for } 1 \leq i \leq n\}. \quad \square$$

Example 1.2 (Circles). We write

$$k\langle Z, Z^{-1} \rangle = \left\{ \sum_{i=-\infty}^{\infty} a_i Z^i \mid a_i \in k, \lim_{|i| \rightarrow \infty} (a_i) = 0 \right\} \quad (1.5)$$

for the Tate algebra $k\langle Z_1, Z_2 \rangle / (Z_1 Z_2 - 1)$. If again k is assumed to be algebraically closed, $\text{Sp}(k\langle Z, Z^{-1} \rangle)$ can be naturally identified with the unit circle $\{z \in k \mid |z| = 1\}$ by the same recipe as in Example 1.1. \square

Example 1.3 (Annuli). A third important type of affinoid analytic spaces is given by annuli. They are obtained from Tate algebras

$$A := k\langle Z_1, Z_2 \rangle / (Z_1 Z_2 - z_0) \quad \text{where } 0 < |z_0| < 1.$$

If k is algebraically closed, A can be naturally identified with the annulus $\{z \in k \mid |z_0| \leq |z| \leq 1\}$ as in the previous examples. \square

1.3 Analytification of Algebraic Varieties

We have seen above how a rigid analytic space can be obtained by gluing. The other important mechanism for the construction of analytic spaces is by analytification of algebraic varieties. We start with the case of projective space.

Let $\mathbb{P}^n(k)$ be the n -dimensional projective space over k . By Example 1.1, the polydiscs

$$\mathcal{U}_i := \{(z_0, \dots, z_n) \mid |z_i| \geq |z_j| \text{ for } 0 \leq j \leq n\}$$

have associated Tate algebras T_n . These are clearly rational and cover the projective space. The \mathcal{U}_i with structure sheaves $\mathcal{O}_{\mathcal{U}_i}$ together with $\mathcal{U}_{ij} = \mathcal{U}_{ji} := \mathcal{U}_i \cap \mathcal{U}_j$ and the identity maps $\varphi_{ij} = \text{Id}_{\mathcal{U}_{ij}}$ form a gluing datum. By the Gluing of Spaces (Proposition 1.4) we obtain the structure of a rigid analytic space $\mathcal{X} := \mathbb{P}^n(k)^{\text{an}} := \bigcup_{i=0}^n \mathcal{U}_i$ on $\mathbb{P}^n(k)$ with structure sheaf $\mathcal{O}_{\mathcal{X}}(\mathcal{U}_i) := \mathcal{O}_{\mathcal{U}_i}$.

More generally, let k be algebraically closed and \mathcal{X}/k an algebraic variety. Then there exists a canonical analytification of \mathcal{X} . By the Gluing Proposition 1.4, it suffices to construct this in the case that \mathcal{X} is affine. Then \mathcal{X} can be identified with a closed subset of k^n for some n , and there exists an ideal $\mathfrak{a} = (f_1, \dots, f_s)$ of

$k[Z_1, \dots, Z_n]$ with

$$\mathcal{X} = \{\mathbf{z} \in k^n \mid f_1(\mathbf{z}) = \dots = f_s(\mathbf{z}) = 0\}.$$

Let $q \in k$ with $0 < |q| < 1$. Then

$$\mathcal{X}_m := \{\mathbf{z} \in \mathcal{X} \subseteq \mathbb{A}^n(k) \mid |z_i| \leq |q|^{-m} \text{ for } 1 \leq i \leq n\}$$

can be identified with the affinoid analytic space defined by the Tate algebra

$$A_m := k\langle Z_1, \dots, Z_n \rangle / (f_1(q^{-m}Z), \dots, f_s(q^{-m}Z))$$

via

$$\mathcal{X}_m \longrightarrow \mathrm{Sp}(A_m), \quad \mathbf{z} \mapsto (Z_1 - q^m z_1, \dots, Z_n - q^m z_n).$$

The \mathcal{X}_m form an inductive system and may be glued together since \mathcal{X}_m is rational inside \mathcal{X}_{m+1} . We obtain $\mathcal{X}^{\mathrm{an}} := \bigcup_m \mathcal{X}_m$ and $\mathcal{O}(\mathcal{X}^{\mathrm{an}}) = \varprojlim \mathcal{O}(\mathcal{X}_m)$. It can be proved that this analytification of \mathcal{X} is independent of the chosen embedding $\mathcal{X} \hookrightarrow k^n$ (see Bosch, Güntzer and Remmert (1984), 9.3.4, or Fresnel and van der Put (1981), III.4.5). Via the preceding construction we may and will from now on identify the points $\mathcal{P} \in \mathcal{X}$ of algebraic varieties \mathcal{X} and their rigid analytic versions $\mathcal{X}^{\mathrm{an}}$.

Let \mathcal{X} be a rigid analytic space. A sheaf \mathcal{F} of $\mathcal{O}_{\mathcal{X}}$ -modules is called a *coherent sheaf*, if there exists an admissible covering $\{\mathcal{X}_i \mid i \in I\}$ of \mathcal{X} by affinoid analytic spaces \mathcal{X}_i such that $\mathcal{F}(\mathcal{X}_i)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}(\mathcal{X}_i)$ -module and

$$\mathcal{F}|_{\mathcal{X}_i} = \widetilde{\mathcal{F}(\mathcal{X}_i)} \quad \text{for all } i \in I.$$

As in the algebraic case there is a simple characterization of coherent sheaves on affinoid spaces (see Fresnel and van der Put (1981), Thm. III.6.2, or Bosch, Güntzer and Remmert (1984), 9.4.3):

Theorem 1.9. *Let \mathcal{X} be an affinoid analytic space and \mathcal{F} a coherent sheaf. Then $\mathcal{F}(\mathcal{X})$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$ -module and $\mathcal{F} \cong \widetilde{\mathcal{F}(\mathcal{X})}$.*

The GAGA-principle compares coherent algebraic and analytic sheaves. We first explain how coherent sheaves on an algebraic variety can be analytified. It suffices to do this in the affine case.

Let k be algebraically closed, $\mathcal{X} = \mathrm{Spec}(R)$ an affine algebraic variety over k and \mathcal{F} an algebraic coherent sheaf on \mathcal{X} . Let $\{\mathrm{Sp}(B_i) \mid i \in I\}$ be a basis of the Grothendieck topology on the analytification $\mathcal{X}^{\mathrm{an}}$. We define a presheaf $\mathcal{F}^{\mathrm{an}}$ on $\mathcal{X}^{\mathrm{an}}$ by setting $\mathcal{F}^{\mathrm{an}}(\mathrm{Sp}(B_i)) := \mathcal{F}(\mathcal{X}) \otimes_R B_i$ for $i \in I$. Then this defines a coherent analytic sheaf on $\mathcal{X}^{\mathrm{an}}$ (see Köpf (1974), Bem. 3.2). Furthermore, if $\varphi : \mathcal{F} \rightarrow \mathcal{G}$ is a morphism of coherent sheaves on \mathcal{X} , then

$$\varphi_{\mathrm{Sp}(B_i)}^{\mathrm{an}} := \varphi \otimes B_i : \mathcal{F}(\mathcal{X}) \otimes B_i \rightarrow \mathcal{G}(\mathcal{X}) \otimes B_i \quad \text{for } i \in I$$

defines a morphism $\varphi^{\text{an}} : \mathcal{F}^{\text{an}} \rightarrow \mathcal{G}^{\text{an}}$ of analytic coherent sheaves (see Köpf (1974), Satz 3.1). This analytification satisfies (see loc. cit. Satz 3.6):

Proposition 1.10. *Let $0 \rightarrow \mathcal{F}_1 \rightarrow \mathcal{F}_2 \rightarrow \mathcal{F}_3 \rightarrow 0$ be an exact sequence of coherent \mathcal{X} -sheaves. Then the associated sequence of coherent \mathcal{X}^{an} -sheaves $0 \rightarrow \mathcal{F}_1^{\text{an}} \rightarrow \mathcal{F}_2^{\text{an}} \rightarrow \mathcal{F}_3^{\text{an}} \rightarrow 0$ is also exact.*

Proof. Since exactness of sequences of sheaves is a local property, it suffices to consider the case where $\mathcal{X} = \text{Spec}(R)$ is affine. The \mathcal{F}_i are coherent, so the sequence $0 \rightarrow \mathcal{F}_1(\mathcal{X}) \rightarrow \mathcal{F}_2(\mathcal{X}) \rightarrow \mathcal{F}_3(\mathcal{X}) \rightarrow 0$ of R -modules is also exact. The flatness of $R \rightarrow B$ for rational subsets $\text{Sp}(B) \subset \mathcal{X}^{\text{an}}$ (see Fresnel and van der Put (1981), Thm. III.7.2) now shows that the sequence $0 \rightarrow \mathcal{F}_1(\mathcal{X}) \otimes_R B \rightarrow \mathcal{F}_2(\mathcal{X}) \otimes_R B \rightarrow \mathcal{F}_3(\mathcal{X}) \otimes_R B \rightarrow 0$ is also exact, hence the result follows by the construction of the analytification. \square

1.4 The GAGA-Principle for $\mathbb{P}^1(k)^{\text{an}}$

For our purposes the most important fact on rigid analytic spaces is the GAGA-principle. Over \mathbb{C} this was proved by Serre (1956). This was adapted to the rigid analytic setting by Köpf (1974). We will only need the statement for subspaces of $\mathbb{P}^1(k)$. For this let $\mathbb{P}^1(k)^{\text{an}}$ denote the analytification of the 1-dimensional (algebraic) projective line $\mathbb{P}^1(k)$ over k . We fix the covering

$$\mathbb{P}^1(k)^{\text{an}} = \mathcal{X}_1 \cup \mathcal{X}_2, \quad \text{with } \mathcal{X}_1 = \{z \in k \mid |z| \leq 1\}, \mathcal{X}_2 = \{z \in k \mid |z| \geq 1\},$$

and let $\mathcal{X}_{12} := \mathcal{X}_1 \cap \mathcal{X}_2 = \{z \in k \mid |z| = 1\}$. With respect to this covering for any integer n we define the *twisted structure sheaf* $\mathcal{O}_{\mathcal{X}}(n)$ by

$$\mathcal{U} \mapsto \{(f_1, f_2) \in \mathcal{O}_{\mathcal{X}}(\mathcal{X}_1 \cap \mathcal{U}) \oplus \mathcal{O}_{\mathcal{X}}(\mathcal{X}_2 \cap \mathcal{U}) \mid f_1 = Z^n f_2 \text{ on } \mathcal{X}_{12} \cap \mathcal{U}\} \quad (1.6)$$

for admissible open subsets $\mathcal{U} \subseteq \mathbb{P}^1(k)^{\text{an}}$. (See Fresnel and van der Put (1981), III.8.5, for the fact that this is an invertible coherent sheaf, and any invertible coherent sheaf is isomorphic to one of this type.)

The following result was shown to us by M. van der Put:

Proposition 1.11. *Let \mathcal{F} be a coherent sheaf on $\mathbb{P}^1(k)^{\text{an}}$. Then there exists $n > 0$ such that $\mathcal{F}(n) := \mathcal{F} \otimes \mathcal{O}_{\mathcal{X}}(n)$ is generated by global sections.*

Proof. Since \mathcal{X}_i , $i = 1, 2$, is an affinoid analytic space, the restriction of \mathcal{F} to \mathcal{X}_i is isomorphic to \tilde{M}_i for some finitely generated $\mathcal{O}(\mathcal{X}_i)$ -module M_i by Theorem 1.9. Let $\mathcal{F}(\mathcal{X}_i) = \langle a_{i1}, \dots, a_{ir} \rangle$ be a generating system of M_i . Denote by ρ_i the restriction maps $\rho_i : \mathcal{F}(\mathcal{X}_i) \rightarrow \mathcal{F}(\mathcal{X}_{12})$. Then by the coherence of \mathcal{F} we see that

$\mathcal{F}(\mathcal{X}_{12}) = \langle \rho_i(a_{i1}), \dots, \rho_i(a_{ir}) \rangle$ for $i = 1, 2$. Let $U, V \in \mathcal{O}(\mathcal{X}_{12})^{r \times r}$ be matrices with

$$\begin{aligned} V \cdot (\rho_1(a_{11}), \dots, \rho_1(a_{1r}))^t &= (\rho_2(a_{21}), \dots, \rho_2(a_{2r}))^t, \\ U \cdot (\rho_2(a_{21}), \dots, \rho_2(a_{2r}))^t &= (\rho_1(a_{11}), \dots, \rho_1(a_{1r}))^t, \end{aligned}$$

so that $VU(\rho_2(a_{21}), \dots, \rho_2(a_{2r}))^t = (\rho_2(a_{21}), \dots, \rho_2(a_{2r}))^t$. By Example 1.2, the Tate algebra of \mathcal{X}_{12} is given by $\mathcal{O}(\mathcal{X}_{12}) = \{\sum_{i=-\infty}^{\infty} c_i Z^i \mid \lim_{|i| \rightarrow \infty} (c_i) = 0\}$. Thus clearly for any $\epsilon > 0$ there exists $n := n(\epsilon) \in \mathbb{N}$ and

$$V' \in \mathrm{GL}_r(\{\sum_{i=-n}^{\infty} c_i Z^i \mid \lim_{i \rightarrow \infty} (c_i) = 0\})$$

such that $\|(V - V')U\| < \epsilon$. By Fresnel and van der Put (1981), Lemme III.6.3, (a special case of the Lemma of Cartan) for ϵ suitably small there then exist $V_i \in \mathrm{GL}_r(\mathcal{O}(\mathcal{X}_i))$, $i = 1, 2$, with

$$\mathrm{Id} - (V - V')U = \rho_1(V_1)^{-1} \rho_2(V_2).$$

Hence we get $\rho_1(V_1)V'(\rho_1(a_{11}), \dots, \rho_1(a_{1r}))^t = \rho_2(V_2)(\rho_2(a_{21}), \dots, \rho_2(a_{2r}))^t$. By construction we have $Z^n V' = \rho_1(\tilde{V})$ for some matrix $\tilde{V} \in \mathrm{GL}_r(\mathcal{O}(\mathcal{X}_1))$. In particular we see that

$$\rho_1(V_1 \tilde{V}(a_{11}, \dots, a_{1r})^t) = Z^n \rho_2(V_2(a_{21}, \dots, a_{2r})^t).$$

Thus $V_1 \tilde{V}(a_{11}, \dots, a_{1r})^t \in \mathcal{F}(\mathcal{X}_1)$ and $V_2(a_{21}, \dots, a_{2r})^t \in \mathcal{F}(\mathcal{X}_2)$ satisfy the compatibility condition (1.6) for $\mathcal{F}(n)$; since $\mathcal{F}(n)$ is a sheaf, there exists a global section (b_1, \dots, b_r) having these two elements as projections. Finally, $V_1 \tilde{V}$ and V_2 are invertible, and the result follows. \square

We now formulate the GAGA-principle for the 1-dimensional projective analytic space $\mathbb{P}^1(k)^{\mathrm{an}}$, and sketch a proof closely following the one given by Serre (1956) for the general complex analytic case (see also Fresnel and van der Put (2004), Ch. 9.3.1).

Theorem 1.12 (GAGA for \mathbb{P}^1). *Let k be a field complete with respect to a non-archimedean valuation.*

(a) *Let \mathcal{G} be an algebraic coherent sheaf on the 1-dimensional projective space $\mathbb{P}^1(k)$. Then analytification yields an isomorphism of the global sections $\mathcal{G}(\mathbb{P}^1(k))$ and $\mathcal{G}^{\mathrm{an}}(\mathbb{P}^1(k)^{\mathrm{an}})$.*

(b) *Let \mathcal{F}, \mathcal{G} be algebraic coherent sheaves on $\mathbb{P}^1(k)$. Then every analytic homomorphism $\mathcal{F}^{\mathrm{an}} \rightarrow \mathcal{G}^{\mathrm{an}}$ is induced by a unique algebraic homomorphism $\mathcal{F} \rightarrow \mathcal{G}$.*

(c) *For every coherent analytic sheaf \mathcal{F} on $\mathbb{P}^1(k)^{\mathrm{an}}$ there exists an algebraic coherent sheaf \mathcal{G} on $\mathbb{P}^1(k)$ unique up to isomorphism with $\mathcal{G}^{\mathrm{an}} \cong \mathcal{F}$.*

Outline of proof. Let \mathcal{G} be an algebraic coherent sheaf on $\mathcal{X} := \mathbb{P}^1(k)$ and $\mathcal{G}^{\mathrm{an}}$ its analytification on $\mathcal{X}^{\mathrm{an}} := \mathbb{P}^1(k)^{\mathrm{an}}$. Then there exist canonical homomorphisms $\epsilon^i : H^i(\mathcal{X}, \mathcal{G}) \rightarrow H^i(\mathcal{X}^{\mathrm{an}}, \mathcal{G}^{\mathrm{an}})$ of cohomology groups for all $i \geq 0$ compatible with

short exact sequences, that is, for any short exact sequence $0 \rightarrow \mathcal{G}_1 \rightarrow \mathcal{G}_2 \rightarrow \mathcal{G}_3 \rightarrow 0$ of coherent \mathcal{X} -sheaves all squares in the diagram

$$\begin{array}{ccccccc} H^i(\mathcal{X}, \mathcal{G}_1) & \rightarrow & H^i(\mathcal{X}, \mathcal{G}_2) & \rightarrow & H^i(\mathcal{X}, \mathcal{G}_3) & \rightarrow & H^{i+1}(\mathcal{X}, \mathcal{G}_1) \\ \downarrow \epsilon_1^i & & \downarrow \epsilon_2^i & & \downarrow \epsilon_3^i & & \downarrow \epsilon_1^{i+1} \\ H^i(\mathcal{X}^{\text{an}}, \mathcal{G}_1^{\text{an}}) & \rightarrow & H^i(\mathcal{X}^{\text{an}}, \mathcal{G}_2^{\text{an}}) & \rightarrow & H^i(\mathcal{X}^{\text{an}}, \mathcal{G}_3^{\text{an}}) & \rightarrow & H^{i+1}(\mathcal{X}^{\text{an}}, \mathcal{G}_1^{\text{an}}) \end{array} \quad (1.7)$$

commute (see Köpf (1974), Satz 3.10). To prove (a) one shows more generally that ϵ^i is an isomorphism for all $i \geq 0$, the assertion being the special case $i = 0$. For the structure sheaf $\mathcal{O} = \mathcal{O}(\mathcal{X}^{\text{an}})$ the cohomology groups can be computed explicitly on both sides: they vanish for $i > 0$, and the global sections are equal to k (see Köpf (1974), Thm. 4.6). Now the machinery of Serre's proof can be applied in this setting: First, one considers the twisted structure sheaves $\mathcal{G} = \mathcal{O}(n)$, $n \in \mathbb{Z}$. To any point P of \mathcal{X}^{an} is associated an exact sequence

$$0 \rightarrow \mathcal{O}(n-1) \rightarrow \mathcal{O}(n) \rightarrow \mathcal{O}_P(n) \rightarrow 0$$

where \mathcal{O}_P is supported by the single point P , and similarly for the analytifications. Taking cohomology the associated diagrams (1.7) allow to use induction on n by applying the snake lemma, see Köpf (1974), Hilfssatz 4.10.

Now let \mathcal{G} be an algebraic coherent sheaf on \mathcal{X} . By Hartshorne (1977), Cor. II.5.18, there exist $n, r \in \mathbb{N}$ and a surjective morphism $\mathcal{O}^r \rightarrow \mathcal{G}(n)$ of coherent sheaves. By loc. cit., Prop. II.5.7, the kernel is again coherent, so we have an exact sequence

$$0 \rightarrow \mathcal{N} \rightarrow \mathcal{O}^r \rightarrow \mathcal{G}(n) \rightarrow 0$$

of coherent \mathcal{X} -sheaves. Taking global sections of this sequence and its analytification yields long exact sequences of cohomology connected by diagram (1.7). The snake lemma now allows to apply descending induction on i to show the bijectivity of ϵ^i . Part (a) follows.

For (b) we consider the coherent sheaf $\mathcal{A} = \text{Hom}(\mathcal{F}, \mathcal{G})$ of homomorphisms from \mathcal{F} to \mathcal{G} , and its analytic version $\mathcal{B} = \text{Hom}(\mathcal{F}^{\text{an}}, \mathcal{G}^{\text{an}})$. Analytification yields an injection $\iota : \mathcal{A}^{\text{an}} \rightarrow \mathcal{B}$. If $\mathcal{A}_{\mathcal{P}} = \text{Hom}_{\mathcal{O}_{\mathcal{P}}}(\mathcal{F}_{\mathcal{P}}, \mathcal{G}_{\mathcal{P}})$ denotes the stalk of \mathcal{A} at a point $\mathcal{P} \in \mathbb{P}^1(k)$, then by definition

$$\mathcal{A}_{\mathcal{P}}^{\text{an}} = \text{Hom}_{\mathcal{O}_{\mathcal{P}}}(\mathcal{F}_{\mathcal{P}}, \mathcal{G}_{\mathcal{P}}) \otimes_{\mathcal{O}_{\mathcal{P}}} \mathcal{O}_{\mathcal{P}}^{\text{an}}.$$

Since \mathcal{F}^{an} is coherent, the stalk of \mathcal{B} at \mathcal{P} is given by

$$\mathcal{B}_{\mathcal{P}} = \text{Hom}_{\mathcal{O}_{\mathcal{P}}^{\text{an}}}(\mathcal{F}_{\mathcal{P}} \otimes_{\mathcal{O}_{\mathcal{P}}} \mathcal{O}_{\mathcal{P}}^{\text{an}}, \mathcal{G}_{\mathcal{P}} \otimes_{\mathcal{O}_{\mathcal{P}}} \mathcal{O}_{\mathcal{P}}^{\text{an}}).$$

The ring $\mathcal{O}_{\mathcal{P}}$ is local and Noetherian, so its completion $\hat{\mathcal{O}}_{\mathcal{P}}$ is faithfully flat over $\mathcal{O}_{\mathcal{P}}$ (see Matsumura (1980), Thm. 56). Since the completions of $\mathcal{O}_{\mathcal{P}}$ and $\mathcal{O}_{\mathcal{P}}^{\text{an}}$ coincide, the descent property of faithful flatness shows that $\mathcal{O}_{\mathcal{P}}^{\text{an}}$ is faithfully flat over $\mathcal{O}_{\mathcal{P}}$. This implies the bijectivity of $\iota_{\mathcal{P}}$. It follows that first ι , and then the

composition

$$\mathcal{A}(\mathbb{P}^1(k)) \longrightarrow \mathcal{A}^{\text{an}}(\mathbb{P}^1(k)^{\text{an}}) \xrightarrow{\iota} \mathcal{B}(\mathbb{P}^1(k)^{\text{an}})$$

with the isomorphism from part (a), applied to the coherent sheaf \mathcal{A} , are also bijective. Now the global sections $\mathcal{A}(\mathbb{P}^1(k))$ of \mathcal{A} are the homomorphisms from \mathcal{F} to \mathcal{G} , and similarly for \mathcal{B} , showing part (b).

For part (c) let \mathcal{F} be an analytic coherent sheaf on $\mathbb{P}^1(k)^{\text{an}}$. By Proposition 1.11 there exists $n \in \mathbb{N}$ such that $\mathcal{F}(n)$ is generated by global sections. Thus for a suitable r we obtain a surjective morphism $(\mathcal{O}^{\text{an}})^r \rightarrow \mathcal{F}(n)$ of coherent sheaves. By Bosch, Güntzer and Remmert (1984), 9.4.3, Prop. 2, the kernel of a morphism of coherent sheaves is again coherent, so there exists a coherent sheaf \mathcal{N} completing the exact sequence

$$0 \longrightarrow \mathcal{N} \longrightarrow (\mathcal{O}^{\text{an}})^r \longrightarrow \mathcal{F}(n) \longrightarrow 0. \quad (1.8)$$

Applying Proposition 1.11 again to the coherent sheaf \mathcal{N} we get a surjection $(\mathcal{O}^{\text{an}})^s \rightarrow \mathcal{N}(m)$ for suitable $s, m \in \mathbb{N}$, which together with (1.8) yields an exact sequence

$$(\mathcal{O}^{\text{an}})^s \longrightarrow (\mathcal{O}^{\text{an}})^r(m) \longrightarrow \mathcal{F}(n+m) \longrightarrow 0. \quad (1.9)$$

By part (b) the morphism $\varphi : (\mathcal{O}^{\text{an}})^s \rightarrow (\mathcal{O}^{\text{an}})^r(m)$ comes from a uniquely determined algebraic morphism ψ . Thus (1.9) induces a sequence

$$\mathcal{O}^s \xrightarrow{\psi} \mathcal{O}^r(m) \longrightarrow \mathcal{G} \longrightarrow 0 \quad (1.10)$$

of algebraic sheaves, with coherent \mathcal{G} . In particular with Proposition 1.10 we obtain that $\mathcal{G}^{\text{an}} = \mathcal{F}(n+m)$, hence $\mathcal{F} = \mathcal{G}(-n-m)^{\text{an}}$ as claimed. To prove uniqueness, assume that $\mathcal{G}_1, \mathcal{G}_2$ are two algebraic coherent sheaves with analytification \mathcal{F} . Then there exists an analytic isomorphism $\varphi : \mathcal{G}_1^{\text{an}} \rightarrow \mathcal{G}_2^{\text{an}}$, which by part (b) is induced by an algebraic morphism $\psi : \mathcal{G}_1 \rightarrow \mathcal{G}_2$ with $\psi^{\text{an}} = \varphi$. With the kernel \mathcal{A} and the cokernel \mathcal{B} we obtain an exact sequence of coherent sheaves

$$0 \longrightarrow \mathcal{A} \longrightarrow \mathcal{G}_1 \xrightarrow{\mu} \mathcal{G}_2 \longrightarrow \mathcal{B} \longrightarrow 0.$$

By analytification Proposition 1.10 shows that $\mathcal{A}^{\text{an}} = \mathcal{B}^{\text{an}} = 0$. Looking at the global sections this forces $\mathcal{A} = \mathcal{B} = 0$, hence $\mu : \mathcal{G}_1 \rightarrow \mathcal{G}_2$ is an isomorphism. \square

A morphism $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ of rigid analytic spaces is called *finite* if there exists an admissible affinoid covering $\{\mathcal{X}_i \mid i \in I\}$ of \mathcal{X} , such that $\{\varphi^{-1}(\mathcal{X}_i) \mid i \in I\}$ is an admissible covering of \mathcal{Y} and the associated morphisms $\varphi_{\mathcal{X}_i}^* : \mathcal{O}_{\mathcal{X}}(\mathcal{X}_i) \rightarrow \mathcal{O}_{\mathcal{Y}}(\varphi^{-1}(\mathcal{X}_i))$ of Tate algebras are finite. Here a morphism $\varphi^* : A \rightarrow B$ is called *finite*, if B is a finitely generated A -module via φ^* .

Corollary 1.13. *Let $\varphi : \mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ be a finite morphism of analytic spaces.*

(a) *There exists a finite algebraic morphism of algebraic varieties $\psi : \tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)$ whose analytification is isomorphic to $\varphi : \mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$.*

(b) Let $\tilde{\varphi} : \mathcal{Y} \rightarrow \mathcal{X}$ be finite. Then there exists a finite morphism of algebraic varieties $\tilde{\psi} : \tilde{\mathcal{Y}} \rightarrow \tilde{\mathcal{X}}$ with $\tilde{\psi}^{\text{an}} = \tilde{\varphi}$.

Proof. The direct image $\mathcal{F} := \varphi_*(\mathcal{O}_{\mathcal{X}})$ of the structure sheaf on \mathcal{X} is a coherent sheaf on $\mathbb{P}^1(k)^{\text{an}}$ (see Bosch, Güntzer and Remmert (1984), 9.4.4, Prop. 3). Thus by Theorem 1.12(c) there exists an algebraic sheaf \mathcal{G} on $\mathbb{P}^1(k)$ with $\mathcal{G}^{\text{an}} = \mathcal{F}$. By construction \mathcal{F} is a sheaf of rings. The multiplication defines an analytic morphism $v : \mathcal{F} \otimes \mathcal{F} \rightarrow \mathcal{F}$ of coherent analytic sheaves. By Theorem 1.12(b) this is induced by an algebraic morphism $\mu : \mathcal{G} \otimes \mathcal{G} \rightarrow \mathcal{G}$ with $\mu^{\text{an}} = v$. Since, as in the proof of Theorem 1.12, all ring extensions are faithfully flat, the morphism μ has the properties of a multiplication, thus making \mathcal{G} into a sheaf of rings. Now $\tilde{\mathcal{X}}_1 = \text{Spec}(\mathcal{G}(\mathbb{P}^1(k) \setminus \{\infty\}))$ and $\tilde{\mathcal{X}}_2 = \text{Spec}(\mathcal{G}(\mathbb{P}^1(k) \setminus \{0\}))$ may be glued to an algebraic covering $\tilde{\mathcal{X}} := \text{Spec}(\mathcal{G}) = \tilde{\mathcal{X}}_1 \cup \tilde{\mathcal{X}}_2$ of $\mathbb{P}^1(k)$ (see Hartshorne (1977), Ex. III.5.17) with analytification $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)^{\text{an}}$, proving (a).

In part (b) the morphisms φ and $\varphi \circ \tilde{\varphi} : \mathcal{Y} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ are analytifications of algebraic morphisms by part (a). Moreover $\tilde{\varphi}$ induces a morphism $\tilde{\varphi}_* : \varphi_*(\mathcal{O}_{\mathcal{X}}) \rightarrow (\varphi \circ \tilde{\varphi})_*(\mathcal{O}_{\mathcal{Y}})$ commuting with the multiplication on these two sheaves of algebras. By Theorem 1.12(b) this is induced by an algebraic morphism $\varphi_*(\mathcal{O}_{\mathcal{X}}) \rightarrow (\varphi \circ \tilde{\varphi})_*(\mathcal{O}_{\tilde{\mathcal{Y}}})$ of sheaves of algebras (see part (a)). This defines an algebraic morphism $\tilde{\psi} : \tilde{\mathcal{Y}} \rightarrow \tilde{\mathcal{X}}$ with analytification $\tilde{\varphi} : \mathcal{Y} \rightarrow \mathcal{X}$. \square

2 The Inverse Problem over $\mathbb{Q}_p(t)$ and $\overline{\mathbb{F}}_p(t)$

In this paragraph we mimic the cut and paste approach for the solution of the inverse problem over $\mathbb{C}(t)$ via topological methods to obtain a similar result for any field complete with respect to an ultrametric valuation. The complex analytic structure is replaced by the rigid analytic structure introduced in Paragraph 1, but otherwise the proofs closely follow the complex example. The main results are the solution of the inverse problem over $\mathbb{Q}_p(t)$ and over $\overline{\mathbb{F}}_p(t)$ and the freeness of the fundamental group of $\overline{\mathbb{F}}_p(t)$ for any prime p .

2.1 Induced Covers

Let k be complete with respect to an ultrametric valuation. Let $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ be a morphism of rigid analytic spaces over k . The group $\text{Deck}(\varphi)$ is defined to be the group of analytic automorphisms σ of \mathcal{Y} with $\varphi = \varphi \circ \sigma$. The cover $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ is called a *Galois cover* if the quotient $\mathcal{Y}/\text{Deck}(\varphi)$ exists and is isomorphic to \mathcal{X} . For any subgroup $G \leq \text{Deck}(\varphi)$ we say that $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ is *G -equivariant*; if moreover G acts regularly on the generic fibres of φ we say for brevity that $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ is *Galois with group G* . We will be interested primarily in connected Galois covers (with respect to the Grothendieck topology, or, equivalently, with respect to the Zariski topology, see Bosch, Güntzer and Remmert (1984), 9.1.4), since these lead to Galois extensions of function fields.

Proposition 2.1. *Let G be a finite group, $H \leq G$ a subgroup, and $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ a Galois cover with group H . Then there exists a unique Galois cover*

$$\text{Ind}_H^G(\varphi) : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \mathcal{X} \quad (2.1)$$

with group G with an H -morphism $\iota : \mathcal{Y} \rightarrow \text{Ind}_H^G(\mathcal{Y})$ such that $\varphi = \text{Ind}_H^G(\varphi) \circ \iota$.

If $H_1 \leq H_2 \leq G$ is a chain of subgroups, then as G -covers

$$\text{Ind}_{H_1}^G(\mathcal{Y}) \cong \text{Ind}_{H_2}^G(\text{Ind}_{H_1}^{H_2}(\mathcal{Y})).$$

Proof. Let $\text{Ind}_H^G(\mathcal{Y}) := G/H \times \mathcal{Y} = \cup_{\sigma_i \in G/H} (\sigma_i, \mathcal{Y})$ be the disjoint union of copies of \mathcal{Y} indexed by a system of coset representatives σ_i of H in G , where the representative for H is chosen to be 1. Then G acts on $\text{Ind}_H^G(\mathcal{Y})$ in a natural way via

$$\sigma : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \text{Ind}_H^G(\mathcal{Y}), \quad (\sigma_i, y) \mapsto (\sigma_j, \tau(y)),$$

for $\sigma \in G$ with $\sigma\sigma_i = \sigma_j\tau$ for $\tau \in H$. This defines a G -cover $\text{Ind}_H^G(\varphi) : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \mathcal{X}$, $(\sigma_i, y) \mapsto y$. Further the embedding

$$\iota : \mathcal{Y} \xrightarrow{\sim} \mathcal{Y}_1 \hookrightarrow \text{Ind}_H^G(\mathcal{Y})$$

yields an H -morphism ι with $\varphi = \text{Ind}_H^G(\varphi) \circ \iota$.

For the uniqueness, let $\varphi_{\mathcal{X}} : \mathcal{Z} \rightarrow \mathcal{X}$ be another Galois cover with group G and with H -morphism $\iota_{\mathcal{X}} : \mathcal{Y} \rightarrow \mathcal{Z}$. We define

$$\psi : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \mathcal{Z}, \quad (\sigma_i, y) \mapsto \psi(y) := \sigma_i(\iota_{\mathcal{X}}(y)),$$

a G -equivariant morphism with $\iota_{\mathcal{X}} = \psi \circ \iota$. Since the roles of \mathcal{Z} and $\text{Ind}_H^G(\mathcal{Y})$ are interchangeable, we obtain a G -equivariant isomorphism $\psi : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \mathcal{Z}$. The remaining statements in the proposition are now easy consequences of the above construction. \square

The cover $\text{Ind}_H^G(\varphi) : \text{Ind}_H^G(\mathcal{Y}) \rightarrow \mathcal{X}$ is called the *induced cover* of $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ from H to G . Note that such covers are not connected whenever H is a proper subgroup of G . It is easy to see that on the side of Tate algebras, induction corresponds to taking direct products of isomorphic copies. Thus induced covers do not in general yield extensions of function fields on the algebraic side. The induced cover $\text{Ind}_1^G(\mathcal{X}) \rightarrow \mathcal{X}$ is called the *trivial cover* of \mathcal{X} of group G .

Proposition 2.2. *Let K/k be a function field in one variable. Let $\mathcal{X} \rightarrow \mathbb{P}^1(k)$ be a projective normal geometrically integral model of $K/k(t)$ and $\mathcal{X}^{\text{an}} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ the covering of analytic spaces obtained from it by analytification. Then \mathcal{X}^{an} is a trivial cover above some affinoid subset of $\mathbb{P}^1(k)^{\text{an}}$ if and only if there exists a prime divisor $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ of degree 1 which splits completely in $K/k(t)$.*

Proof. First assume that the prime divisor $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ of degree 1 splits completely in $K/k(t)$. Without loss of generality we may take \mathfrak{P} to be the numerator divisor of (t) . Then $\mathcal{X} \rightarrow \mathbb{P}^1(k)$ is unramified in a small neighborhood of $0 \in \mathbb{P}^1(k)$, hence locally is defined by an equation $f(t, X) = 0$ such that $f(0, X) = \prod_{i=1}^n (X - z_i)$ splits into linear factors over k . By the analytification procedure described in Example 1.3, the cover $\mathcal{X}^{\text{an}} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ is given locally near 0 by the morphism of Tate algebras $k\langle Z \rangle \rightarrow k\langle Z, X \rangle / f(Z, X)$. By Hensel's Lemma we have $f(Z, X) = \prod_{i=1}^n (X - f_i(Z))$ for certain $f_i(Z) \in k\langle Z \rangle$ in a small neighborhood of 0. But

$$k\langle Z, X \rangle / \left(\prod_{i=1}^n (X - f_i(Z)) \right) \cong \bigoplus_{i=1}^n k\langle Z \rangle,$$

hence \mathcal{X}^{an} is equal to $\cup_{i=1}^n \text{Sp}(k\langle Z \rangle)$ close to 0, which is a trivial cover of $\text{Sp}(k\langle Z \rangle)$.

Conversely if $\mathcal{X}^{\text{an}} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ is a trivial cover above $\{z \in k \mid |z| \leq 1\}$, the local Tate algebra is a direct sum $\bigoplus_{i=1}^n k\langle Z \rangle$, thus equal to the analytification of a function algebra defined by a polynomial with k -rational zeroes at some point of the unit disc. The corresponding extension of function fields $K/k(t)$ then has a prime divisor which splits completely. \square

2.2 The Inverse Problem over Complete Ultrametric Fields

For $a, b \in k$ we denote by

$$\mathcal{D}(a, b) := \{z \in k \mid |z - a| \leq |b|\} \quad \text{and} \quad \mathcal{D}(a, b)^\circ := \{z \in k \mid |z - a| < |b|\}$$

the *closed* respectively *open ultrametric discs*. (Note that both are open as well as closed for the topology induced by the ultrametric valuation of k .)

The fundamental building blocks for arbitrary Galois covers are cyclic covers with a base point.

Proposition 2.3. *Let k be a field complete with respect to an ultrametric valuation and $n \in \mathbb{N}$. Then there exists a connected Galois cover $\mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ of analytic spaces with cyclic Galois group Z_n of order n , which is a trivial cover above $\mathbb{P}^1(k)^{\text{an}} \setminus \mathcal{D}(0, 1)^\circ$.*

Proof. We just have to translate the results of Chapter III.4 on cyclic extensions to the present setting. It is clearly enough to prove the result for n the power of a prime p . If p is different from the characteristic of k , then by Theorem III.4.5 there exists a cyclic geometric Galois extension $K/k(t)$ in which the denominator divisor \mathfrak{P}_∞ of (t) splits completely. If the characteristic of k equals p , Corollary III.4.8 gives the same result. Application of Proposition 2.2 completes the proof. \square

The main result is now achieved by gluing the cyclic Galois covers.

Proposition 2.4. *Let k be a field complete with respect to an ultrametric valuation. Then for every finite group G there exists a connected Galois cover $\mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ with group G , which is a trivial cover above $\mathbb{P}^1(k)^{\text{an}} \setminus \mathcal{D}(0, 1)^\circ$.*

Proof. We follow the proof given by Liu (1995). For cyclic groups, the assertion is just Proposition 2.3. By induction it then suffices to show, if $G = \langle H_1, H_2 \rangle$ is generated by two subgroups for both of which the assertion holds, then it also holds for G . Let $\varphi_i : \mathcal{X}_i \rightarrow \mathbb{P}^1(k)^{\text{an}}$, $i = 1, 2$, be the coverings with group H_i whose existence is assumed. For a fixed $q \in k$, $0 < |q| < 1$, the discs

$$\mathcal{D}_1 := \mathcal{D}(0, q^2), \quad \mathcal{D}_2 := \mathcal{D}(q, q^2)$$

are disjoint. We write $\mathcal{D}_1^\circ := \mathcal{D}(0, q^2)^\circ$ and $\mathcal{D}_2^\circ := \mathcal{D}(q, q^2)^\circ$. By change of coordinates we may and will assume that φ_i is a trivial cover above $\mathbb{P}^1(k)^{\text{an}} \setminus \mathcal{D}_i^\circ$. Let $\mathcal{D}_0 := \mathbb{P}^1(k)^{\text{an}} \setminus (\mathcal{D}_1^\circ \cup \mathcal{D}_2^\circ)$ and $\tilde{\mathcal{X}}_i := \varphi_i^{-1}(\mathcal{D}_i)$. Above \mathcal{D}_i , $i = 1, 2$, let $\mathcal{Y}_i := \text{Ind}_{H_i}^G(\tilde{\mathcal{X}}_i)$ be induced covers and above \mathcal{D}_0 let $\mathcal{Y}_0 := \text{Ind}_1^G(\mathcal{D}_0)$ be the induced covering of the identical covering. For $i = 1, 2$ both coverings $\mathcal{Y}_0 \rightarrow \mathcal{D}_0$ and $\mathcal{Y}_i \rightarrow \mathcal{D}_i$ are trivial on the intersection $\mathcal{D}_0 \cap \mathcal{D}_i = \mathcal{D}_i \setminus \mathcal{D}_i^\circ$ and therefore isomorphic to each other on this intersection. We may thus apply the Gluing Propositions 1.4 and 1.5 to deduce the existence of a G -equivariant analytic cover $\mathcal{Y} \rightarrow \mathbb{P}^1(k)^{\text{an}}$.

By construction, \mathcal{Y}_0 is a disjoint union of connected subspaces $\mathcal{Y}_{0,\sigma}$ for $\sigma \in G$, while \mathcal{Y}_i , $i = 1, 2$, is a disjoint union of connected spaces $\mathcal{Y}_{i,\tau}$ for $\tau \in G/H_i$. But if

$\sigma \in \tau H_i$ then $\mathcal{Y}_{0,\sigma} \cap \mathcal{Y}_{i,\tau} \neq \emptyset$. Since H_1 and H_2 generate G , Corollary 1.7 shows that \mathcal{Y} is connected, and $\mathcal{Y} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ is Galois with group G . By construction, its restriction to $\mathbb{P}^1(k)^{\text{an}} \setminus \mathcal{D}(0,1)^\circ$ is a trivial cover since $\mathcal{D}_1 \cup \mathcal{D}_2 \subseteq \mathcal{D}(0,1)^\circ$. \square

Theorem 2.5 (Harbater (1987)). *Let k be a field complete with respect to an ultrametric valuation. Then the inverse Galois problem over $k(t)$ has a positive solution.*

Proof. Let G be a finite group. Then by Proposition 2.4 there exists an analytic connected Galois cover $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ with group G . By the GAGA-principle Corollary 1.13 this is the analytification of an algebraic connected Galois cover $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)$ with Galois group G . The function field $N = k(\tilde{\mathcal{X}})$ of $\tilde{\mathcal{X}}$ then yields a Galois extension of $k(t) = k(\mathbb{P}^1(k))$ with Galois group G . \square

Corollary 2.6. *The inverse Galois problem over $\mathbb{Q}_p(t)$ has a positive solution.*

Remark. Together with Corollary I.1.7 the above Corollary shows that the inverse problem of Galois theory is solved for rational function fields over all completions of \mathbb{Q} . By Theorem 2.5 the corresponding result holds more generally for rational function fields over the completions of arbitrary global fields.

When choosing rational ramification points for the cyclic extensions glued in Proposition 2.4, Corollary 2.6 yields Galois extensions defined over the field $\mathbb{Q}'_p := \mathbb{Q}_p \cap \bar{\mathbb{Q}}$ of algebraic p -adic numbers, thus solving the inverse problem over $\mathbb{Q}'_p(t)$ (see Harbater (1987), Cor. 2.11).

2.3 The Inverse Problem over $\overline{\mathbb{F}}_p(t)$

By a standard specialization argument it is possible to derive a solution of the inverse Galois problem over $\overline{\mathbb{F}}_p(t)$ from the above result for complete non-archimedean fields.

Theorem 2.7 (Harbater (1984)). *The inverse Galois problem over $\overline{\mathbb{F}}_p(t)$ has a positive solution.*

Proof. The power series field $k := \overline{\mathbb{F}}_p((u))$ is complete ultrametric, so by Theorem 2.5 for any finite group G there exists a connected algebraic Galois cover $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)$ with group G . This cover is already defined over a finitely generated extension ring $R = \overline{\mathbb{F}}_p[x_1, \dots, x_s]$ of $\overline{\mathbb{F}}_p$, yielding a cover $\varphi : \tilde{\mathcal{X}}_R \rightarrow \mathbb{P}^1(R)$ with smooth generic fiber which becomes isomorphic to $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k)$ after base change to k . Since $\overline{\mathbb{F}}_p$ is algebraically closed, there exist infinitely many $\overline{\mathbb{F}}_p$ -rational points on $\tilde{\mathcal{X}}_R$. By the Bertini–Noether Theorem (see Fried and Jarden (1986), Prop. 8.8) infinitely many of these give specializations such that $\tilde{\mathcal{X}}_R$ remains irreducible, i.e., there exists a maximal ideal $\mathfrak{m} \triangleleft R$, with $R/\mathfrak{m} \cong \overline{\mathbb{F}}_p$, such that $\tilde{\mathcal{X}}_R \times_{\mathbb{P}^1(R)} \mathbb{P}^1(\overline{\mathbb{F}}_p) \rightarrow \mathbb{P}^1(\overline{\mathbb{F}}_p)$ is connected with Galois group G . The function field of this cover yields a Galois extension of $\overline{\mathbb{F}}_p(t)$ with the desired Galois group. \square

A refinement of the above argument makes it possible to solve split embedding problems over $K = \overline{\mathbb{F}}_p(t)$ and thus to show that the absolute Galois group of such fields K is free profinite of countable rank.

2.4 The Conjecture of Šafarevič for $\overline{\mathbb{F}}_p(t)$

The conjecture of Šafarevič (see IV, 3.3) states that the absolute Galois group of \mathbb{Q}^{ab} is free profinite of countable rank. In the usual analogy between number fields and function fields over finite fields, one is led to ask a similar question for $\overline{\mathbb{F}}_p(t)$, the maximal cyclotomic extension of $\mathbb{F}_p(t)$. In this case the rigid analytic methods yield a positive answer, found by Harbater (1995a) and Pop (1995). The simplified proof presented here, which only uses gluing arguments from Paragraph 1, was found independently by Haran and Völklein (1996) and van der Put.

We start by solving certain split geometric embedding problems $\mathcal{E}(\varphi, \kappa)$ (see Ch. IV.1 for the notation).

Proposition 2.8. *Let k be a complete ultrametric field and $\mathcal{E}(\varphi, \kappa)$ a finite split geometric embedding problem over $k(t)$ with fixed field N of $\ker(\varphi)$. If there exists a prime divisor $\mathfrak{P} \in \mathbb{P}(k(t)/k)$ which splits completely in $N/k(t)$, then $\mathcal{E}(\varphi, \kappa)$ has a proper geometric solution.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ a finite split embedding problem over $k(t)$ belonging to the split exact sequence

$$1 \longrightarrow H = \ker(\kappa) \longrightarrow \tilde{G} = H \rtimes G \longrightarrow G = \text{Gal}(N/k(t)) \longrightarrow 1.$$

By Proposition 2.2 for $u \in k$ with $|u| < 1$ the analytification \mathcal{X} of a suitable model of $N/k(t)$ may be taken such that its restriction $\mathcal{X}_1 \rightarrow \mathcal{D}_1 := \mathcal{D}(0, u^2)$ is connected with group G and trivial above $\mathcal{D}_1 \setminus \mathcal{D}_1^\circ$. Further, by Proposition 2.4 there exists a connected cover $\mathcal{X}_2 \rightarrow \mathcal{D}_2 := \mathcal{D}(u, u^2)$ with group $H = \ker(\kappa)$ which is a trivial cover above $\mathcal{D}_2 \setminus \mathcal{D}_2^\circ$. Let $\mathcal{Y}_1 := \text{Ind}_G^{\tilde{G}}(\mathcal{X}_1)$, $\mathcal{Y}_2 := \text{Ind}_H^{\tilde{G}}(\mathcal{X}_2)$, and $\mathcal{Y}_0 := \text{Ind}_1^{\tilde{G}}(\mathcal{D}_0)$ for $\mathcal{D}_0 := \mathbb{P}^1(k)^{\text{an}} \setminus (\mathcal{D}_1^\circ \cup \mathcal{D}_2^\circ)$. This is a special case of the setup in the proof of Proposition 2.4. In particular, \mathcal{Y}_i , $i = 0, 1, 2$, may be glued to a connected cover $\mathcal{Y} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ with group $\tilde{G} = \langle H, G \rangle$.

Since H is a system of coset representatives of G in \tilde{G} , by the construction in the proof of Proposition 2.1 we have $\mathcal{Y}_1 = H \times \mathcal{X}_1 = \cup_{\tau \in H} \mathcal{X}_{1,\tau}$ with H -action $\rho(\mathcal{X}_{1,\tau}) := \mathcal{X}_{1,\rho\tau}$. Thus the canonical map $\mathcal{X}_1 = \mathcal{X}_{1,1} \rightarrow \mathcal{Y}_1/H$ is an isomorphism. Similarly we have $\mathcal{Y}_2 = \cup_{\sigma \in G} \mathcal{X}_{2,\sigma}$, with $\tau(\sigma, x) = (\sigma, t^\sigma(x))$ for $(\sigma, x) \in \mathcal{X}_{2,\sigma}$ and $\tau \in H$. Thus

$$(\bigcup_{\sigma \in G} \mathcal{X}_{2,\sigma})/H = \bigcup_{\sigma \in G} (\mathcal{X}_{2,\sigma}/H) = \bigcup_{\sigma \in G} \mathcal{D}_{2,\sigma} = \text{Ind}_1^G(\mathcal{D}_2),$$

where $\mathcal{D}_{2,\sigma} = \mathcal{X}_{2,\sigma}/H \cong \mathcal{D}_2$. Moreover we trivially have $\mathcal{Y}_0/H = \text{Ind}_1^G(\mathcal{D}_0)$. This shows that \mathcal{Y}/H coincides with the trivial cover $\text{Ind}_1^G(\mathcal{D}_0 \cup \mathcal{D}_2)$ above $\mathcal{D}_0 \cup \mathcal{D}_2$, while it equals $\mathcal{X}_1 \rightarrow \mathcal{D}_1$ above \mathcal{D}_1 . It follows that $\mathcal{Y}/H \cong \mathcal{X}$.

Via the GAGA-principle (Corollary 1.13), $\mathcal{Y} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ corresponds to a connected Galois cover $\tilde{\mathcal{Y}} \rightarrow \mathbb{P}^1(k)$ with group \tilde{G} , such that the extension of function fields $k(\tilde{\mathcal{Y}})/k(t)$ contains $N/k(t)$ as a Galois subextension. Since by construction $\tilde{\sigma} \in \tilde{G}$ acts via $\kappa(\tilde{\sigma})$ on the quotient $\mathcal{Y}/H \cong \mathcal{X}$ this yields a proper solution of $\mathcal{E}(\varphi, \kappa)$. \square

Extension of constants now allows to obtain the following consequence of Proposition 2.8 and Theorem 2.7:

Corollary 2.9. *Every split embedding problem over $\overline{\mathbb{F}}_p(t)$ has a proper solution.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be an embedding problem over $\overline{\mathbb{F}}_p(t)$ and N the fixed field of $\ker(\varphi)$ with Galois group $G = \varphi(\Gamma)$. Without loss of generality we may assume that $N/\overline{\mathbb{F}}_p(t)$ is unramified at the denominator divisor \mathfrak{P}_∞ of t , and hence \mathfrak{P}_∞ splits completely. Extension of constants with the complete field $k := \overline{\mathbb{F}}_p((u))$ transforms $\mathcal{E}(\varphi, \kappa)$ to a geometric embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ with $N^* = Nk$ and $\text{Gal}(N^*/k(t)) \cong G$ with a prime divisor \mathfrak{P}_∞^* which splits completely. Since the power series field k is complete ultrametric, by Proposition 2.8 the split embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ possesses a proper geometric solution. Let $\tilde{N}^*/k(t)$ be a solution field, such that $\text{Gal}(\tilde{N}^*/k(t)) \cong \tilde{G}$, and $\tilde{\mathcal{Y}}^* \rightarrow \mathbb{P}^1(k)$ a corresponding normal model. By the argument in the proof of Theorem 2.7 there exists a specialization of $\tilde{\mathcal{Y}}^* \rightarrow \mathbb{P}^1(k)$ to a connected cover $\tilde{\mathcal{Y}} \rightarrow \mathbb{P}^1(\overline{\mathbb{F}}_p)$, i.e., with $\text{Gal}(\tilde{N}/\overline{\mathbb{F}}_p(t)) \cong \tilde{G}$, where $\tilde{N} := \overline{\mathbb{F}}_p(\tilde{\mathcal{Y}})$. Since N^* was obtained from N by extension of constants, any such specialization of $\tilde{\mathcal{Y}}$ will be such that \tilde{N} contains N and is a solution field of the original embedding problem $\mathcal{E}(\varphi, \kappa)$. It gives a solution $\tilde{\varphi}$ by the reasoning in the proof of Theorem IV.1.5(a). \square

Theorem 2.10 (Harbater (1995a), Pop (1995)). *The absolute Galois group of $\overline{\mathbb{F}}_p(t)$ is free profinite of countable rank.*

Proof. By the Theorem of Tsen (Theorem IV.1.11(a)) the absolute Galois group $\Gamma := \Gamma_{\overline{\mathbb{F}}_p(t)}$ of $\overline{\mathbb{F}}_p(t)$ is projective. Since $\overline{\mathbb{F}}_p(t)$ is countable, Γ can have at most countable rank. Thus by the Freiheitssatz of Iwasawa (Theorem IV.1.13) the result is proved if every finite embedding problem for Γ has a proper solution. By the Theorem of Ikeda (Theorem IV.1.9) it even suffices to properly solve split embedding problems. But these always have proper solutions by Corollary 2.9. \square

Corollary 2.11. *Let k be an algebraically closed countable field, K/k a function field in one variable. Then Γ_K is a free profinite group (of countable rank).*

Proof. In characteristic 0 this is Theorem I.2.2, while in positive characteristic it follows from the previous Theorem 2.10 since subgroups of finite index of free profinite groups of countable rank are again free of countable rank. \square

Remark. The above corollary even holds without restriction on the cardinality of k . Then the rank of Γ_K is equal to the cardinality of k . This can be proved by showing that the number of solutions to the embedding problems considered in the proof of Theorem 2.10 is equal to the cardinality of k and then invoking a result of Melnicov (1980) (see Pop (1995), Thm A and Cor. on p. 556, as well as Harbater (1995a), Lemma 4.3 and Thms. 3.5, 3.6 and 4.4, for the details, and for a more general assertion where the ramification can be controlled).

3 Free Quotients of the Fundamental Group

The structure of the fundamental group of $\mathbb{C}(t)$ is well known by the Riemann Existence Theorem. If \mathbb{C} is replaced by a non-algebraically closed field which is complete with respect to a non-archimedean valuation, no comparable result is known at present. In this section we give at least partial information by constructing a large free factor of the fundamental group, using rigid analytic methods, on which the action of the Galois group of the field of constants can be described explicitly.

3.1 Free Composites of Galois Extensions

Let k be complete with respect to an ultrametric valuation and $K = k(t)$. We consider a finite family $\mathcal{M} = \{N_i/K \mid i \in I\}$, $|I| < \infty$, of finite Galois extensions N_i of K inside a fixed algebraic closure \bar{K} of K , regular over k . Let $\tilde{\mathcal{Y}}_i$ be the normalization of $\mathbb{P}^1(k)$ in N_i , and $\varphi_i : \tilde{\mathcal{Y}}_i \rightarrow \mathbb{P}^1(k)$ the corresponding covering of curves. Denote by $\mathcal{X} := \mathbb{P}^1(k)^{\text{an}}$, $\mathcal{Y}_i := \tilde{\mathcal{Y}}_i^{\text{an}}$ for $i \in I$, the rigid analytifications. Now \mathcal{M} is called a *compatible family* if moreover there exists an admissible covering $\{\mathcal{U}\} \cup \{\mathcal{U}_i \mid i \in I\}$ of \mathcal{X} by affinoid spaces such that

- (1) the \mathcal{U}_i , $i \in I$, are non-empty and pairwise disjoint,
- (2) φ_i has no ramification above \mathcal{U} and \mathcal{U}_j for $i \neq j$,
- (3) the preimage $\mathcal{V}_i := \varphi_i^{-1}(\mathcal{U}_i) \subseteq \mathcal{Y}_i$ of \mathcal{U}_i is connected,
- (4) the preimage $\partial\mathcal{V}_i := \varphi_i^{-1}(\partial\mathcal{U}_i)$ of $\partial\mathcal{U}_i := \mathcal{U} \cap \mathcal{U}_i$ contains an admissible subset $\partial\mathcal{U}_{i,1}$ which is isomorphic to $\partial\mathcal{U}_i$ via φ_i .

The above conditions can be interpreted as controlling the ramification locus of the geometric field extensions $N_i/k(t)$: in a certain sense, they have to be sufficiently separated.

The conditions (1)–(4) have some obvious consequences. First, the $\partial\mathcal{U}_i$ are non-empty since $\mathbb{P}^1(k)^{\text{an}}$ is connected, and pairwise disjoint since the \mathcal{U}_i are. Thus the union $\partial\mathcal{U} := \cup \partial\mathcal{U}_i$ is disjoint. The analytic projective line \mathcal{X} can be recovered by gluing $\cup \mathcal{U}_i$ with \mathcal{U} along $\partial\mathcal{U}$. Further, assumption (2) implies that the N_i/K are linearly disjoint. Indeed, the extension $(N_i \cap N_j)/K$ is unramified for $i \neq j$, hence trivial since there exist no unramified field extension of $K = k(t)$.

Proposition 3.1. *Let k be complete with respect to an ultrametric valuation, $K = k(t)$, $\mathcal{M} = \{N_i/K \mid i \in I\}$ a compatible family with composite $N = \prod_{i \in I} N_i$ and Galois groups $G_i = \text{Gal}(N_i/K)$. Then there exists a geometric Galois extension M/K with Galois group $\Pi := (\times_{i \in I} G_i)^\wedge$ the profinite completion of the free product of the G_i , having N/K as a subextension.*

Proof. Since \mathcal{M} is compatible, there exists an admissible covering $\{\mathcal{U}\} \cup \{\mathcal{U}_i \mid i \in I\}$ of \mathcal{X} satisfying (1) to (4). The automorphism group $G_i^* := \text{Deck}(\varphi_i)$ is anti-isomorphic to the Galois group G_i of N_i/K . For $\sigma \in G_i^*$ we define $\partial\mathcal{U}_{i,\sigma} :=$

$\sigma(\partial\mathcal{U}_{i,1})$. Then by our assumptions the $\partial\mathcal{U}_{i,\sigma}$ for $\sigma \in G_i^*$ are connected and pairwise disjoint subsets of $\partial\mathcal{V}_i$, and $\bigcup_{\sigma \in G_i^*} \partial\mathcal{U}_{i,\sigma}$ is a G_i^* -invariant admissible covering of $\partial\mathcal{V}_i$. Furthermore, for $\sigma, \tau \in G_i^*$ we have $\tau(\partial\mathcal{U}_{i,\sigma}) = \partial\mathcal{U}_{i,\tau\sigma}$. In other words, $\partial\mathcal{V}_i \cong \text{Ind}_1^{G_i^*}(\partial\mathcal{U}_i)$.

Let now Ψ be the kernel in the natural exact sequence

$$1 \longrightarrow \Psi \longrightarrow \Pi \longrightarrow \prod_{i \in I} G_i = \text{Gal}(N/K) \longrightarrow 1. \quad (3.1)$$

Let $\Lambda \leq \Psi$ be an open normal subgroup of Π and H the quotient group

$$1 \longrightarrow \Lambda \longrightarrow \Pi \xrightarrow{\kappa} H \longrightarrow 1.$$

The G_i are naturally embedded into Π and their images generate Π topologically. This implies $H = \langle \kappa(G_i) \mid i \in I \rangle$, and since $\Lambda \leq \Psi$ and $\Pi/\Psi \cong \prod G_i$ we have $\kappa(G_i) \cong G_i$. We write H^* for the opposite group of H . Let $\tilde{\mathcal{U}} := \text{Ind}_1^{H^*}(\mathcal{U})$ and $\tilde{\mathcal{V}}_i := \text{Ind}_{G_i^*}^{H^*}(\mathcal{V}_i)$. So by definition

$$\tilde{\mathcal{U}} = H^* \times \mathcal{U} = \bigcup_{\tau \in H^*} \mathcal{U}_\tau, \quad \tilde{\mathcal{V}}_i = H^*/G_i^* \times \mathcal{V}_i = \bigcup_{\tau \in H^*/G_i^*} \mathcal{V}_{i,\tau}, \quad (3.2)$$

and according to Proposition 2.1 the elements $\sigma \in H^*$ act on $\tilde{\mathcal{U}}$ and $\tilde{\mathcal{V}}$ via

$$\sigma(\tau, \mathcal{U}) = (\sigma\tau, \mathcal{U}), \quad \sigma(\tau, \mathcal{V}_i) = (\tau', \sigma'(\mathcal{V}_i)),$$

where $\sigma\tau = \tau'\sigma'$ for some $\sigma' \in G_i^*$. We now glue $\tilde{\mathcal{U}}$ and $\tilde{\mathcal{V}}_i$, $i \in I$, over

$$\partial\tilde{\mathcal{U}} := \text{Ind}_1^{H^*}(\partial\mathcal{U}) = \bigcup_{\tau \in H^*} \bigcup_{i \in I} \partial\mathcal{U}_{i,\tau} \quad (3.3)$$

and

$$\partial\tilde{\mathcal{V}}_i := \text{Ind}_{G_i^*}^{H^*}(\partial\mathcal{V}_i) = \bigcup_{\tau \in H^*/G_i^*} \partial\mathcal{V}_{i,\tau} = \bigcup_{\tau \in H^*/G_i^*} \bigcup_{\sigma \in G_i^*} \partial\mathcal{U}_{i,\sigma\tau} \quad (3.4)$$

by identifying $\partial\mathcal{U}_{i,\sigma_i\tau_i}$ in (3.4) with $\partial\mathcal{U}_{i,\tau_i\sigma_i}$ in (3.3). By the Gluing Propositions 1.4 and 1.5 this yields an H^* -equivariant analytic cover $\mathcal{Y}_H \rightarrow \mathcal{X}$. By the same reasoning as in the proof of Proposition 2.4 this is connected since H is generated by the $\kappa(G_i)$. Further, $\mathcal{Y}_H/H^* \cong \mathcal{X}$, so the cover is Galois with group H^* . By the GAGA-principle (Corollary 1.13(b)) this is the analytification of a connected algebraic cover $\tilde{\mathcal{Y}}_H \rightarrow \mathbb{P}^1(k)$ with Galois group H^* and factoring through the $\tilde{\mathcal{V}}_i$. The corresponding extension N_H/K of function fields is geometric by Proposition 2.2 since $\mathcal{Y}_H \rightarrow \mathcal{X}$ is the trivial cover above \mathcal{U} .

For a sequence of epimorphisms

$$\Pi \xrightarrow{\kappa} H \xrightarrow{\kappa'} H',$$

with corresponding analytic spaces $\mathcal{Y}_H, \mathcal{Y}_{H'}$, by construction $\mathcal{Y}_H / \ker(\kappa')$ is canonically isomorphic to $\mathcal{Y}_{H'}$. Thus the above construction yields a projective system $\{\mathcal{Y}_H \rightarrow \mathcal{X}\}_H$ of analytic covers and $\{\tilde{\mathcal{Y}}_H \rightarrow \mathbb{P}^1(k)\}_H$ of connected algebraic covers. For the corresponding geometric function field extensions N_H/K this translates to an injective system, with projective system of Galois groups $H = \text{Gal}(N_H/K)$. Taking the direct limit yields a geometric field extension $M := \cup_H N_H$, with Galois group Π over K , which contains the composite N of the N_i . \square

3.2 Galois Action

We now refine the procedure of the first section to accommodate an additional Galois action. Let k_0 be a complete ultrametric field, k/k_0 a finite Galois extension with group G , $K_0 = k_0(t)$, $K = kK_0 = k(t)$ and $\mathcal{X} = \mathbb{P}^1(k)^{\text{an}}$. A compatible family $\mathcal{M} = \{N_i/K \mid i \in I\}$ with respect to K/k is called a *G-compatible family* if moreover

- (5) \mathcal{M} is $\Gamma_{K_0} := \text{Gal}(\bar{K}_0/K_0)$ -invariant,
- (6) the admissible covering $\{\mathcal{U}\} \cup \{\mathcal{U}_i \mid i \in I\}$ of \mathcal{X} is G -invariant.

Since the composite $N := \prod N_i$ is Galois over K_0 by assumption (3), we have an exact sequence

$$1 \longrightarrow \text{Gal}(N/K) \longrightarrow \text{Gal}(N/K_0) \longrightarrow G \longrightarrow 1$$

of Galois groups, which splits since $\mathbb{P}^1(k)$ has k -rational points. A group theoretic section $v : G \rightarrow \text{Gal}(N/K_0)$ of this sequence of Galois groups is called an *\mathcal{M} -section*, if for all $i \in I$ the connected component $\partial\mathcal{U}_{i,1}$ of $\partial\mathcal{U}_i$ (which is isomorphic to $\partial\mathcal{U}_i$ via φ_i) is invariant under (the opposite group of) the stabilizer of N_i in $v(G)$.

Lemma 3.2. *Let $v : G \rightarrow \text{Gal}(N/K_0)$ be an \mathcal{M} -section for the G -compatible family \mathcal{M} . Then there exists a labeling $\partial\mathcal{U}_{i,\sigma}$, $\sigma \in G_i^*$, of the connected components of $\partial\mathcal{U}_i$ such that for all $\rho \in G^*$ we have*

$$\rho(\partial\mathcal{U}_{i,\sigma}) = \partial\mathcal{U}_{j,\rho\sigma}, \quad \text{where } j \text{ is defined by } {}^\rho\sigma := \rho\sigma\rho^{-1} \in G_j^*.$$

Proof. It is clearly sufficient to prove this for a G -orbit on \mathcal{M} . For such an orbit we choose a fixed N_i with stabilizer H_i in G . Then we may label the components of $\partial\mathcal{U}_i$ by $\sigma \in G_i^*$, starting from the component $\partial\mathcal{U}_{i,1}$ of $\partial\mathcal{U}_i$ fixed by H_i , whose existence is guaranteed by the fact that v is an \mathcal{M} -section, such that

$$\sigma'(\partial\mathcal{U}_{i,\sigma}) = \partial\mathcal{U}_{i,\sigma'\sigma}$$

for all $\sigma, \sigma' \in G_i^*$. Next, for $\rho \in G^*$ and j with $N_j = N_i^\rho$, we set $\partial\mathcal{U}_{j,\tau} := \rho(\partial\mathcal{U}_{i,\sigma})$, where $\tau = {}^\rho\sigma \in G_j^*$ for $\sigma \in G_i$. To show that this labeling is well-defined it is clearly sufficient to consider the case $i = j$, and $\rho = 1$. But then ρ lies in H_i and stabilizes

$\partial\mathcal{U}_{i,1}$. This yields

$$\rho(\partial\mathcal{U}_{i,\sigma}) = \rho(\sigma(\partial\mathcal{U}_{i,1})) = {}^\rho\sigma(\rho(\partial\mathcal{U}_{i,1})) = {}^\rho\sigma(\partial\mathcal{U}_{j,1}) = \partial\mathcal{U}_{j,{}^\rho\sigma},$$

proving the assertion. \square

Any section $v : G \rightarrow \text{Gal}(N/K_0)$ defines an action of G on $\text{Gal}(N/K) \cong \prod_{i \in I} G_i$ and thus also on $\Pi = (\times_{i \in I} G_i)^\wedge$. With respect to this we can speak of the semidirect product $\Pi \rtimes G$.

Theorem 3.3. *Let \mathcal{M} be a G -compatible family and v an \mathcal{M} -section. Then the field extension M/K constructed in Proposition 3.1 is Galois over K_0 and v can be extended to $v_{\mathcal{M}} : G \rightarrow \text{Gal}(M/K_0)$ such that*

$$1 \longrightarrow \text{Gal}(M/K) \longrightarrow \text{Gal}(M/K_0) \longrightarrow G \longrightarrow 1$$

is canonically isomorphic to

$$1 \longrightarrow \Pi \longrightarrow \Pi \rtimes G \longrightarrow G \longrightarrow 1,$$

where $\Pi \rtimes G$ is defined with respect to the action induced by v .

Proof. Let Ψ be the kernel of $\Pi \rightarrow \prod_{i \in I} G_i$ as in (3.1). We show that the construction in Proposition 3.1 of the universal field extension M of K attached to \mathcal{M} is compatible with the action of G . Let $\Lambda \leq \Psi$ be an open G -invariant normal subgroup of Π and $H = \Pi/\Lambda$ the quotient group. We identify $H \rtimes G \cong (\Pi \rtimes G)/\Lambda$. It now suffices to prove that the fixed field N_H of Λ in M is normal over K_0 and the section $v : G \rightarrow \text{Gal}(N/K_0)$ may be prolonged to a section $v_H : G \rightarrow \text{Gal}(N_H/K_0)$ such that the sequence

$$1 \rightarrow \text{Gal}(N_H/K) \rightarrow \text{Gal}(N_H/K_0) = \text{Gal}(N_H/K).v_H(G) \rightarrow \text{Gal}(K/K_0) \rightarrow 1$$

becomes canonically isomorphic to

$$1 \longrightarrow H \longrightarrow H \rtimes G \longrightarrow G \longrightarrow 1. \quad (3.5)$$

We may define a natural action of G^* as group of analytic automorphisms on $\tilde{\mathcal{U}}$ and $\bigcup_{i \in I} \tilde{\mathcal{V}}_i$ as in (3.2): For $\rho \in G^*$ let

$$\begin{aligned} \rho(\tau, x) &= ({}^\rho\tau, \rho(x)) \quad \text{for } (\tau, x) \in H^* \times \mathcal{U} = \tilde{\mathcal{U}}, \\ \rho(\tau, x) &= ({}^\rho\tau, \rho(x)) \in H_j^* \times \mathcal{V}_j \quad \text{for } (\tau, x) \in H_i^* \times \mathcal{V}_i \text{ and } {}^\rho\tau \in G_j^*, \end{aligned} \quad (3.6)$$

where we have identified H^*/G_i^* with the kernel H_i^* of the canonical epimorphism $H^* \rightarrow G_i^*$. In this action H^* is normalized by G^* , extending the action on $\prod_{i \in I} G_i$ via v and thus defining a semidirect product $H \rtimes G^*$ with section v_H extending v . Furthermore, by the construction in Lemma 3.2 the action (3.6) of G^* is compatible with the gluing as in the proof of Proposition 3.1 used to define \mathcal{Y}_H . So we obtain an action of $H^* \rtimes G^*$ as a group of analytic automorphisms of \mathcal{Y}_H with $\mathcal{Y}_H/H^* \cong \mathcal{X}$.

This shows that the exact sequence

$$1 \longrightarrow \text{Deck}(\mathcal{Y} \rightarrow \mathcal{X}) \longrightarrow \text{Deck}(\mathcal{Y} \rightarrow \mathcal{X}_0) \longrightarrow \text{Deck}(\mathcal{X} \rightarrow \mathcal{X}_0) \longrightarrow 1$$

is canonically isomorphic to (3.5). Let N_H denote the function field of the corresponding cover $\tilde{\mathcal{Y}}_H \rightarrow \mathbb{P}^1(k)$ of algebraic curves existing by Corollary 1.13(b). Then by the above N_H is Galois over K_0 with group

$$\text{Gal}(N_H/K_0) = \text{Gal}(N_H/K) \rtimes v_H(G) \cong H \rtimes G.$$

This proves that the procedure in the proof of Proposition 3.1 can be made compatible with the Galois action by G . Going to the projective limit of the covers \mathcal{Y}_H , respectively the injective limit of the field extensions N_H , we obtain the assertion of the theorem. \square

3.3 A Free Quotient of the Algebraic Fundamental Group

We now show that G -compatible families with good sections exist in one important case. In this section we assume that the characteristic of the residue class field of k_0 with respect to the ultrametric valuation equals the characteristic of k_0 . The more general case of mixed characteristic is studied in Pop (1994).

Let k_0 be a complete ultrametric field. A finite set

$$\mathcal{S} = \{\mathcal{P}_1, \mathcal{Q}_1, \dots, \mathcal{P}_r, \mathcal{Q}_r\} \subset \mathbb{P}^1(\bar{k}_0)$$

of $2r$ points of $\mathbb{P}^1(\bar{k}_0)$ stable under Γ_{k_0} with corresponding set of prime divisors $\mathbf{S} = \{\mathfrak{P}_1, \mathfrak{Q}_1, \dots, \mathfrak{P}_r, \mathfrak{Q}_r\} \subset \mathbb{P}(\bar{k}_0(t)/\bar{k}_0)$ is called *pairwise adjusted* (with respect to k_0) if there exists a finite Galois extension k/k_0 with group $G = \text{Gal}(k/k_0)$ such that

- (7) the set of pairs $\{(\mathcal{P}_i, \mathcal{Q}_i) \mid i = 1, \dots, r\}$ forms a system of imprimitivity for the action of Γ_{k_0} ,
- (8) there exists an admissible covering $\{\mathcal{U}\} \cup \{\mathcal{U}_i \mid i \in I\}$ of $\mathcal{X} = \mathbb{P}^1(k)^{\text{an}}$ with $\mathcal{P}_i, \mathcal{Q}_i \in \mathcal{U}_i$ satisfying (1) of Section 3.1 and (6) of Section 3.2, and a G -invariant family of $G_{\mathfrak{P}_i}$ -equivariant analytic isomorphisms

$$\{\theta_i : \mathcal{U}_i \xrightarrow{\sim} \mathcal{D}(0, 1) \mid i \in I\}$$

with $\theta_i(\mathcal{P}_i) = 0$, $\theta_i(\mathcal{Q}_i) \in \mathcal{D}(0, 1)^\circ$ and $\theta_i(\mathcal{U}_i \cap \mathcal{U}) = \mathcal{D}(0, 1) \setminus \mathcal{D}(0, 1)^\circ$, where $G_{\mathfrak{P}_i}$ denotes the decomposition group of \mathfrak{P}_i in G .

Lemma 3.4. *Let $\mathcal{S} = \{\mathcal{P}_1, \mathcal{Q}_1, \dots, \mathcal{P}_r, \mathcal{Q}_r\}$ be pairwise adjusted. Furthermore, let $\mathbf{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$ with $n_i = n_j$ if \mathcal{P}_i and \mathcal{P}_j are G -conjugate. Then for all suitably large k/k_0 there exists a G -compatible family $\mathcal{M} = \{N_i/k(t) \mid 1 \leq i \leq r\}$ such that for all $i \in I$ the extension $N_i/k(t)$ is only ramified in $\{\mathfrak{P}_i, \mathfrak{Q}_i\}$ and has Galois group $\text{Gal}(N_i/k(t)) \cong Z_{n_i}$.*

Proof. We fix $\mathbf{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$ with $n_i = n_j$ if \mathcal{P}_i and \mathcal{P}_j are G -conjugate. Denote by m the p -prime part of the least common multiple of the n_i , $i = 1, \dots, r$, where p is the characteristic of k_0 . Assume that k contains the m -th roots of unity. In Proposition 2.3 we constructed a connected cyclic Galois cover $\tilde{\mathcal{Y}}_i$ of $\mathcal{D}(0, 1)$ with group Z_{n_i} . For the p -part of n_i we replace the Galois extension from Corollary III.4.8 by the cyclic Galois extension of $k(t)$ in Theorem III.4.7 described by the specialization $\mathbf{t} \mapsto (1/(t(t-1)), 0, \dots, 0)$ and again denote by $\tilde{\mathcal{Y}}_i$ the connected cyclic Galois cover obtained by analytification. As before, this is a trivial cover above some open disc. Now by construction in all cases the corresponding cyclic Galois extension $\tilde{N}_i/k(t)$ is totally ramified in two points and $\text{Gal}(\tilde{N}_i/k(t))$ is generated by the inertia elements σ_i, τ_i at the two ramification points subject to the relation $\sigma_i \tau_i = 1$. Furthermore Γ_k acts via the cyclotomic character as $\sigma_i^\delta = \sigma_i^{c(\delta)}$ for $\delta \in \Gamma_k$. Via θ_i^{-1} the cover $\tilde{\mathcal{Y}}_i \rightarrow \mathcal{D}(0, 1)$ may be transported to a Galois cover $\mathcal{Y}_i \rightarrow \mathcal{U}_i$ with group $G_i \cong Z_{n_i}$ trivial above $\partial \mathcal{U}_i := \mathcal{U}_i \cap \mathcal{U}$. Above $\mathcal{U}'_i := \mathcal{U} \cup \bigcup_{j \neq i} \mathcal{U}_j$ we consider the trivial cover $\text{Ind}_1^{G_i}(\mathcal{U}'_i)$. Gluing above $\partial \mathcal{U}_i = \mathcal{U}_i \cap \mathcal{U}'_i$ gives a connected Galois cover $\varphi_i : \mathcal{Y}_i \rightarrow \mathcal{X}$ with group Z_{n_i} . By the GAGA-principle this gives rise to a family $\mathcal{M} = \{N_i/k(t) \mid i = 1, \dots, r\}$ of cyclic Galois extensions of $k(t)$ with groups Z_{n_i} . More precisely, $N_i/k(t)$ is generated by a root of

$$x^{(n_i)_{p'}} - \frac{t - q_i}{t - p_i} = 0 \quad (3.7)$$

together with the coordinates of a solution \mathbf{x} of

$$\mathbf{x}^p - \mathbf{x} = (1/((t - p_i)(t - q_i)), 0, \dots, 0) \quad (3.8)$$

in the Witt ring $\mathbb{W}(\overline{k(t)})$ of Witt vectors of length $(n_i)_p$. Here p_i (respectively q_i) is such that \mathfrak{P}_i is the numerator divisor of $(t - p_i)$ (respectively \mathfrak{Q}_i is the numerator divisor of $(t - q_i)$).

The compatibility of the family \mathcal{M} is clear from the definitions. It remains to show that \mathcal{M} is $\Gamma_{k_0(t)}$ -invariant. But this follows since $N_i = N_{i'}^\delta$ if $\delta(\mathcal{P}_i) = \mathcal{P}_{i'}$ for all $\delta \in \Gamma_{k_0(t)}$ and from property (8). \square

After these preparations we can prove a result of Pop (1994) which may be thought of giving one half of the Riemann Existence Theorem in the case of a base field k_0 complete with respect to a non-archimedean valuation, but with precise information on the action of Γ_{k_0} on the free normal subgroup (compare with Theorem I.2.6).

Theorem 3.5 (Pop (1994)). *Let k_0 be a field complete with respect to a non-archimedean valuation such that the characteristic of k_0 equals the characteristic of the residue class field with respect to this valuation. Further let $\mathcal{S} = \{\mathcal{P}_1, \mathcal{Q}_1, \dots, \mathcal{P}_r, \mathcal{Q}_r\} \subset \mathbb{P}^1(\bar{k}_0)$ be pairwise adjusted. Then the arithmetic fundamental group $\pi_1^{\text{alg}}(\mathbb{P}^1(\bar{k}_0) \setminus \mathcal{S}) \rtimes \Gamma_{k_0}$ has a quotient $\Pi \rtimes \Gamma_{k_0}$ such that*

$$\Pi = \langle \alpha_1, \beta_1, \dots, \alpha_r, \beta_r \mid \alpha_i \beta_i = 1 \text{ for } 1 \leq i \leq r \rangle^\wedge, \quad (3.9)$$

where the elements α_i, β_i are generators of inertia groups above the ramified prime divisors $\mathfrak{P}_i, \mathfrak{Q}_i$ for $1 \leq i \leq r$.

Furthermore, Γ_{k_0} acts on Π via the cyclotomic character c as

$$\alpha_i^\delta = \alpha_{(i)\delta}^{c(\delta)} \quad \text{for } \delta \in \Gamma_{k_0}. \quad (3.10)$$

Proof. Let $\mathbf{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$ be Γ_{k_0} -invariant, i.e., with $n_i = n_j$ whenever \mathfrak{P}_i and \mathfrak{P}_j lie in the same orbit under the action of Γ_{k_0} . Let $k_{\mathbf{n}}$ be the cyclotomic extension of k_0 with those p -prime roots of unity whose order divides one of the n_i , and set $K_{\mathbf{n}} := k_{\mathbf{n}}(t)$. Then by Lemma 3.4 there exists a G -compatible family $\mathcal{M}_{\mathbf{n}} = \{N_{\mathbf{n},i}/K_{\mathbf{n}} \mid 1 \leq i \leq r\}$ of cyclic Galois extensions with groups $G_i := \text{Gal}(N_{\mathbf{n},i}/K_{\mathbf{n}}) = Z_{n_i}$.

We next show that there exists an $\mathcal{M}_{\mathbf{n}}$ -section. By construction the G_i are generated by inertia elements σ_i, τ_i subject to $\sigma_i \tau_i = 1$, and Γ_{k_0} and hence $G_{\mathbf{n}} := \text{Gal}(K_{\mathbf{n}}/k_0(t))$ act on these via

$$\sigma_i^\delta = \sigma_{(i)\delta}^{c(\delta)}, \quad \text{where } \delta^{-1}(\mathfrak{P}_i) = \mathfrak{P}_{i(\delta)} \text{ for } \delta \in \Gamma_{K_0}.$$

In particular the extension

$$1 \longrightarrow \text{Gal}(N_{\mathbf{n}}/K_{\mathbf{n}}) \longrightarrow \text{Gal}(N_{\mathbf{n}}/k_0(t)) \longrightarrow G_{\mathbf{n}} \longrightarrow 1$$

with $N_{\mathbf{n}} := \prod_{i=1}^r N_{\mathbf{n},i}$ splits. Let \mathfrak{P} be the denominator divisor of (t) . By the Remark after Theorem I.3.5 together with Proposition I.3.1 this provides a section from Γ_{k_0} to $\Gamma_{k_0(t)}$ and thus a section $v_{\mathbf{n}} : G_{\mathbf{n}} \rightarrow \text{Gal}(N_{\mathbf{n}}/k_0(t))$, after possibly extending $k_{\mathbf{n}}$ by a finite step. We claim that $v_{\mathbf{n}}$ is an $\mathcal{M}_{\mathbf{n}}$ -section. For this let $H_i \leq G_{\mathbf{n}}$ be the stabilizer of $N_{\mathbf{n},i}$ (via $v_{\mathbf{n}}$) and write $k_i := k^{H_i}$ for the fixed field in k . The analytic spaces \mathcal{Y}_i can be regarded as analytic spaces over k_i and (the opposite group of) H_i acts on \mathcal{Y}_i by analytic automorphisms. Let \mathcal{Y}'_i be the preimage under φ_i of \mathcal{U}'_i , an admissible H_i -invariant subset of \mathcal{Y}_i . Thus H_i permutes the connected components of \mathcal{Y}'_i , and this action is the same as the one on the formal power series solutions of equations (3.7) and (3.8). But these clearly have solutions in the decomposition field of \mathfrak{P} as can be seen by Hensel's lemma. Thus $v_{\mathbf{n}}$ is an $\mathcal{M}_{\mathbf{n}}$ -section.

Hence Theorem 3.3 applies to the $G_{\mathbf{n}}$ -compatible family $\mathcal{M}_{\mathbf{n}}$ and the $\mathcal{M}_{\mathbf{n}}$ -section $v_{\mathbf{n}}$ to yield a Galois extension $M_{\mathbf{n}}$ of $K_{\mathbf{n}}$ with group

$$\Pi_{\mathbf{n}} := \text{Gal}(M_{\mathbf{n}}/K_{\mathbf{n}}) = \left(\bigtimes_{i=1}^r Z_{n_i} \right)^{\wedge}. \quad (3.11)$$

The system of G -invariant tuples $\mathbf{n} \in \mathbb{N}^r$ is projective, and since the above constructions were all canonical, starting from the pairwise adjusted set S , we obtain an injective system of field extensions

$$\{\bar{k}_0 M_{\mathbf{n}} \mid \mathbf{n} \in \mathbb{N}^r \text{ is } G\text{-invariant}\}$$

of $\bar{k}_0(t)$ with projective system of Galois groups $\{\Pi_{\mathbf{n}}\}$ from (3.11). The limit over the $\Pi_{\mathbf{n}}$ is clearly given by Π in (3.9). The action of Γ_{k_0} on Π is obtained from the corresponding action on the intermediate levels. \square

4 Large Fields

In this paragraph we study a class of fields for which the inverse Galois problem has a positive solution. This includes rational function fields over PAC-fields and over complete fields as special cases. As an application the absolute Galois group of a Hilbertian PAC-field of arbitrary characteristic is shown to be free profinite.

4.1 Existentially Closed Fields

Let K^*/K be an extension of fields. Then K is *existentially closed in K^** if for every Zariski-closed subset A of $\mathbb{A}^n(K)$, $A(K^*) \neq \emptyset$ implies $A(K) \neq \emptyset$. This notion is transitive in the following sense: if $K_1 \leq K_2 \leq K_3$ is a tower of fields and K_i is existentially closed in K_{i+1} for $i = 1, 2$, then K_1 is existentially closed in K_3 . Conversely, if K_1 is existentially closed in K_3 , then at least K_1 is also existentially closed in K_2 .

Lemma 4.1. *Let K^*/K be an arbitrary field extension such that K^* has a K -rational place. Then K^* is regular over K .*

Proof. Let $\wp : K^* \rightarrow K \cup \{\infty\}$ be the K -rational place of K^* . Let $\sum_{i=1}^n a_i f_i = 0$ with $a_i \in \bar{K}$ in an algebraic closure \bar{K} of K and $f_i \in K^*$. Denote by $\bar{\wp} : \bar{K}^* \rightarrow \bar{K} \cup \{\infty\}$ the extension of \wp with $\bar{\wp}(a) = a$ for all $a \in \bar{K}$. Let $j \in \{1, \dots, n\}$ be such that f_j is the element with the largest order of pole. Then $\bar{\wp}(f_i/f_j) \in K$ and hence

$$\bar{\wp}\left(\sum_{i=1}^n a_i f_i/f_j\right) = \sum_{i=1}^n a_i \bar{\wp}(f_i/f_j) = 0,$$

but $\bar{\wp}(f_j/f_j) \neq 0$ which shows that a_1, \dots, a_n are linearly dependent over K . Thus \bar{K} and K^* are linearly disjoint. \square

Thus in particular, if K is existentially closed in K^* then K^* is a regular extension of K .

Existentially closed field extensions behave well with respect to regular solutions of split embedding problems:

Proposition 4.2. *Let K be existentially closed in K^* . Let $\mathcal{E}(\varphi, \kappa)$ be a finite split embedding problem over K and $\mathcal{E}(\varphi^*, \kappa^*)$ the corresponding embedding problem over K^* obtained by extension of constants with K^* . Then $\mathcal{E}(\varphi, \kappa)$ has a regular proper solution if and only if $\mathcal{E}(\varphi^*, \kappa^*)$ has a regular proper solution.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be a finite split embedding problem over K and N the fixed field of $\ker(\varphi)$ with Galois group $G = \varphi(\Gamma)$. Since K^*/K is regular, extension of constants with K^* transforms $\mathcal{E}(\varphi, \kappa)$ to an embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ with $N^* = NK^*$ and $\text{Gal}(N^*/K^*) \cong G$. Let $\tilde{\varphi}$ be a regular proper solution of $\mathcal{E}(\varphi, \kappa)$,

with solution field $\tilde{N}/K(t)$ which we may assume to be linearly disjoint from K^* over K . The composition of the restriction map from $\text{Gal}(\overline{K^*(t)}/K^*(t))$ to $\text{Gal}(\overline{K^*K(t)}/K^*(t))$ with the conjugate of $\tilde{\varphi}$ by the natural isomorphism from $\text{Gal}(\overline{K(t)}/K(t))$ to $\text{Gal}(K^*\overline{K(t)}/K^*(t))$ then gives a regular proper solution $\tilde{\varphi}^*$ of $\mathcal{E}(\varphi^*, \kappa^*)$ with solution field $\tilde{N}^* := \tilde{N}K^*$.

So now let $\tilde{\varphi}^*$ be a regular proper solution of $\mathcal{E}(\varphi^*, \kappa^*)$ with solution field $\tilde{N}^*/K^*(t)$ and $\text{Gal}(\tilde{N}^*/K^*(t)) \cong \tilde{G}$. Let y be a primitive element of $\tilde{N}^*/K^*(t)$ and $f(t, Y)$ the minimal polynomial of y over $K^*(t)$. Then there exists a finitely generated subfield $K(\mathbf{x})$, $\mathbf{x} = (x_1, \dots, x_r)$, of K^* such that $f(t, Y) = f_1(t, \mathbf{x}, Y) \in K(t)[\mathbf{x}][Y]$ generates a Galois extension of $K(t, \mathbf{x})$ with group \tilde{G} . Since K^*/K is regular, so is $K(\mathbf{x})/K$, hence the algebraic variety $V = \text{Spec}(K[\mathbf{x}])$ is absolutely irreducible. By the Bertini-Noether Theorem (Fried and Jarden (1986), Prop. 8.8) there exists a Zariski-open subset $U \subseteq V$ such that for $\mathbf{u} \in U$ the polynomial $f_1(t, \mathbf{u}, Y)$ remains irreducible with group \tilde{G} . Since K is existentially closed in K^* the set U contains a K -rational point \mathbf{u}_0 . Then the splitting field of $f_1(t, \mathbf{u}_0, Y)$ is a geometric Galois extension $\tilde{N}/K(t)$ with group \tilde{G} since $f_1(t, \mathbf{u}, Y)$ is absolutely irreducible. By the argument used in the proof of Theorem IV.1.5(a) it can be seen to solve the embedding problem $\mathcal{E}(\varphi, \kappa)$. \square

The following property of Henselian fields will be used in the sequel:

Proposition 4.3. *Let K be a Henselian field and \hat{K} its completion. If \hat{K}/K is a separable extension, then K is existentially closed in \hat{K} .*

Proof. Let $\mathbf{x} = (x_1, \dots, x_n)$ be a \hat{K} -rational point of some closed affine set A . Let $\mathbf{y} = (y_1, \dots, y_n)$ be a separating transcendence basis (see Fried and Jarden (1986), Lemma 9.5) of $K(\mathbf{x})/K$ and z a primitive element of the finite separable extension $K(\mathbf{x})/K(\mathbf{y})$ which is integral over $K[\mathbf{y}]$. Thus there exists an irreducible polynomial $f(Y, Z) \in K[Y, Z]$ with $f(y, z) = 0$ and $f'(y, z) \neq 0$. Since K is dense in \hat{K} , there exist points in K arbitrarily close to \mathbf{y} and z . As K is Henselian, there exist $\mathbf{a}, b \in K$ with $f(\mathbf{a}, b) = 0$. This gives a specialization of \mathbf{y}, z to K and hence a specialization of \mathbf{x} to a K -rational point of A . \square

4.2 Characterization of Large Fields

A field k is called *large* if every absolutely irreducible curve over k with a simple k -rational point has infinitely many k -rational points. Note that this is equivalent to the property: Every function field of one variable over k that has a k -rational point has infinitely many k -rational points. The class of large fields contains a number of interesting examples:

Proposition 4.4. *The following fields are large:*

- (a) all PAC-fields,
- (b) all real closed fields,
- (c) all Henselian fields.

Proof. The first assertion is immediate from the definition of PAC-fields.

For (b) let \mathcal{C} be an absolutely irreducible curve over the real closed field k with a simple k -rational point. Let $f(X, Y) \in k[X, Y]$ be the equation for a model of an affine part of \mathcal{C} such that $(0, 0)$ becomes the simple k -rational point. Thus there exists a small neighborhood \mathcal{U} of 0 such that $f(0, y)$ takes positive as well as negative values for $y \in \mathcal{U}$. Hence for all small enough x_0 the polynomial $f(x_0, y)$ also takes positive and negative values in a neighborhood of $y = 0$. By the mean value theorem this implies the existence of a simple zero y_0 of $f(x_0, y)$, hence the existence of infinitely many k -rational points on \mathcal{C} , proving (b).

Let k be Henselian, $f(X, Y) \in k[X, Y]$ the equation for a model of an affine part of an absolutely irreducible curve \mathcal{C} over k and (x, y) with $f(x, y) = 0$ a simple point. Since k is Henselian, for all x' sufficiently close to x in the topology induced by the Henselian valuation of k , there exists $y' \in k$ with $f(x', y') = 0$ such that (x', y') is again simple. \square

Remark. According to Pop (1996) the field \mathbb{Q}^{tr} of all totally real numbers as well as the totally p -adic fields are also large. It is not known whether \mathbb{Q}^{ab} is large.

Lemma 4.5. *Let k be a field. Then the extension $k((u))/k(u)^h$ of the field of formal power series over the Henselization of $k(u)$ with respect to the place $\wp_u : u \mapsto 0$ is separable.*

Proof. We may assume that the characteristic p of k is positive. According to Fried and Jarden (1986), Lemma 9.5, $k((u))/k(u)^h$ is separable if $k((u))$ and $(k(u)^h)^{\frac{1}{p}}$ are linearly disjoint over $k(u)$. Since $k(u)^h$ is separable algebraic over $k(u)$ this holds if $k((u))$ and $(k(u))^{\frac{1}{p}}$ are linearly disjoint. Any finite subextension of $(k(u))^{\frac{1}{p}}/k(u)$ is contained in a field $L = k(a_1^{\frac{1}{p}}, \dots, a_n^{\frac{1}{p}})(u^{\frac{1}{p}})$ for suitable $a_1, \dots, a_n \in k$. To prove linear disjointness of L and $k((u))$ it suffices to check that $[Lk((u)) : k((u))] = [L : k(u)]$. Clearly the residue field extensions of $L/k(u)$ and $Lk((u))/k((u))$ with respect to \wp coincide. Since moreover in both field extensions the value group is enlarged by the factor p we conclude $[Lk((u)) : k((u))] \geq [L : k(u)]$ and hence the result. \square

We can now give the following connection with existentially closed field extensions due to Pop (1996).

Theorem 4.6. *For a field k , the following are equivalent:*

- (1) *k is large.*
- (2) *k is existentially closed in the field of formal power series $k((u))$.*

Proof. First assume that k is large. Since $k((u))/k$ has the rational place $\wp_u : u \mapsto 0$ it follows from Lemma 4.1 that $k((u))/k$ is a regular extension.

Let $k(u)^h$ denote the Henselization of $k(u)$ with respect to the place \wp_u . Then $k((u))$ is the completion of $k(u)^h$, and since $k((u))/k(u)^h$ is separable by Lemma 4.5 it suffices by Proposition 4.3 to show that k is existentially closed in $k(u)^h$. Let $\mathbf{x} = (x_1, \dots, x_r)$ be a $k(u)^h$ -rational point of some Zariski-closed affine

set \mathcal{A} . Then the field $k(\mathbf{x})$ generated by the coordinates is a finitely generated algebraic extension of $k(u)$, so is a function field of one variable over k . By construction $k(\mathbf{x})$ has a rational point, so by assumption it has infinitely many rational points. At all but finitely many of these, \mathbf{x} is finite, so specialization yields infinitely many points in $\mathcal{A}(k)$.

Conversely, assume that k is existentially closed in $k((u))$. Let \mathcal{C} be an absolutely irreducible curve over k and $f(x, y) = 0$ a model for an affine part of \mathcal{C} containing a simple k -rational point, with coordinates (x_1, y_1) say. We claim that then \mathcal{C} has infinitely many k -rational points. Indeed, assume by induction that we found points with coordinates $(x_1, y_1), \dots, (x_n, y_n)$. Consider the Zariski-closed affine set \mathcal{A} defined by the equations

$$f(X, Y) = 0, \quad Z_i(X - x_i) = 1 \quad \text{for } i = 1, \dots, n.$$

By setting $X := x_1 + u^m$ for m sufficiently large we see that \mathcal{A} has a point in the Henselian field $k((u))$. Since k is existentially closed in $k((u))$ this implies that \mathcal{A} has a k -rational point (x, y, z_1, \dots, z_n) , so $(x_{n+1}, y_{n+1}) := (x, y)$ yields a k -rational point of \mathcal{C} with $x_{n+1} \neq x_i$ for $i = 1, \dots, n$. This shows that k is large. \square

4.3 Split Embedding Problems over Large Fields

Proposition 4.7. *Let k be a large field. Then every finite split embedding problem over $k((u))$ has a regular proper solution.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be a finite split embedding problem over $K := k((u))$ and N the fixed field of $\ker(\varphi)$ with Galois group $G = \varphi(\Gamma)$. It suffices to find a proper solution of the lifted embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ over $K^* := K(t)$ with fixed field $N^* = N(t)$ of φ^* and $G^* = \text{Gal}(N^*/K^*) \cong G$ such that N is algebraically closed in the solution field. Let $\gamma_1, \dots, \gamma_r$ be generators of the kernel H and set $C_i := \langle \gamma_i \rangle$. Let $\{C_{i,\sigma} \mid 1 \leq i \leq r, \sigma \in G^*\}$ be a set of copies of the C_i with isomorphisms $\iota_{i,\sigma} : C_{i,\sigma} \xrightarrow{\sim} C_i$. We denote by $\gamma_{i,\sigma}$ the preimages under $\iota_{i,\sigma}$ of γ_i . Let

$$\Phi := (\underset{\substack{1 \leq i \leq r \\ \sigma \in G^*}}{\times} C_{i,\sigma})^\circ$$

be the profinite completion of the free product of the $C_{i,\sigma}$. Then G^* acts on Φ via $(\gamma_{i,\tau\sigma})^\tau = \gamma_{i,\sigma}$. We denote the semidirect product of Φ and G^* with respect to this action by \hat{G}^* . By construction there is a natural epimorphism from \hat{G}^* onto \tilde{G} , so it suffices to solve the split embedding problem $\mathcal{E}(\varphi^*, \hat{\kappa}^*)$ associated to

$$1 \longrightarrow \Phi \longrightarrow \hat{G}^* \longrightarrow G^* \longrightarrow 1 \tag{4.1}$$

where $\hat{\kappa}^*$ is the composite of the natural epimorphism $\hat{G}^* \rightarrow H \rtimes G^*$ with κ^* .

Let $\{x_\sigma \in N \mid \sigma \in G^*\}$ be a normal basis of N^*/K^* and choose $a_i \in K^*$ such that all $x_{i,\sigma} := a_i x_\sigma$ are distinct for $1 \leq i \leq r$, $\sigma \in G^*$. Further let $b_i \in K^*$ be different from a_i . If the b_i are close enough to the a_i in the topology induced by the ultrametric topology of K then the set of pairs $\mathcal{S} := \{(x_{i,\sigma}, y_{i,\sigma})\}$ with $y_{i,\sigma} := b_i x_\sigma$ is pairwise adjusted in the sense of Paragraph 3.

By Theorem 3.5 there exists a quotient $\Pi \rtimes \Gamma_{K^*}$ of the arithmetic fundamental group of $\mathbb{P}^1(\bar{K}^*) \setminus \mathcal{S}$ with

$$\Pi = \langle \alpha_{i,\sigma}, \beta_{i,\sigma} \mid \alpha_{i,\sigma} \beta_{i,\sigma} = 1, 1 \leq i \leq r, \sigma \in G^* \rangle,$$

Γ_{K^*} acts on Π via the cyclotomic character c as in (3.5), and the $\alpha_{i,\sigma}$, $\beta_{i,\sigma}$ are generators of the inertia groups above the prime divisors corresponding to $x_{i,\sigma}$, $y_{i,\sigma}$ respectively. Then the epimorphism

$$\psi : \Pi \rightarrow \Phi, \quad \psi(\alpha_{i,\sigma}) := \gamma_{i,\sigma}^{c(\sigma)},$$

satisfies

$$\psi(\alpha_{i,\sigma})^\delta = (\gamma_{i,\sigma}^{c(\sigma)})^\delta = \gamma_{i,\delta^{-1}\sigma}^{c(\sigma)} = \gamma_{i,\delta^{-1}\sigma}^{c(\delta)c(\delta^{-1}\sigma)} = \psi(\alpha_{i,\delta^{-1}\sigma}^{c(\delta)}) = \psi(\alpha_{i,\sigma}^\delta).$$

Thus ψ is compatible with the action of $G^* \cong \text{Gal}(N^*/K^*)$ and we obtain a commutative diagram with surjective vertical arrows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \Pi & \longrightarrow & \Pi \rtimes \Gamma_{K^*} & \longrightarrow & \Gamma_{K^*} \longrightarrow 1 \\ & & \psi \downarrow & & \psi \rtimes \varphi^* \downarrow & & \varphi^* \downarrow \\ 1 & \longrightarrow & \Phi & \longrightarrow & \Phi \rtimes G^* & \longrightarrow & G^* \longrightarrow 1. \end{array} \quad (4.2)$$

In particular $\tilde{\varphi}^* := \psi \rtimes \varphi^*$ gives a solution for the embedding problem (4.1) such that N is algebraically closed in the solution field and thus the proof is complete. \square

Theorem 4.8 (Pop (1996)). *Let k be a large field. Then every finite split embedding problem $\mathcal{E}(\varphi, \kappa)$ over k has a regular proper solution. In particular every finite group occurs as the Galois group of a geometric Galois extension of the rational function field $k(t)$.*

Proof. Let $\mathcal{E}(\varphi, \kappa)$ be a finite split embedding problem over k and $\mathcal{E}(\varphi^*, \kappa^*)$ the corresponding embedding problem obtained by extension of constants with $k^* := k((u))$. By Proposition 4.7 this has a proper regular solution. Since k is existentially closed in k^* by Theorem 4.6, this implies the existence of a proper regular solution of $\mathcal{E}(\varphi, \kappa)$ by Proposition 4.2. \square

If moreover k is Hilbertian we obtain from Theorem IV.1.5(a):

Corollary 4.9. *Every finite split embedding problem over a Hilbertian large field has a proper solution.*

4.4 Application to Hilbertian PAC-Fields

As an easy consequence we obtain the following generalization of Theorem IV.3.10 to arbitrary characteristic:

Theorem 4.10 (Pop (1996)). *The absolute Galois group of a countable Hilbertian PAC-field is free profinite of countable rank.*

Proof. This follows as in the proof of Theorem IV.3.10 since by Proposition 4.4 a PAC-field is large, and by Corollary 4.9 every finite split embedding problem over a Hilbertian large field has a proper solution. \square

Remark. Together with the result of Roquette (see Fried and Jarden (1986), Prop. 24.38) this allows the following characterization of Hilbertian PAC-fields: A countable PAC-field is Hilbertian if and only if its absolute Galois group is free profinite of countable rank.

5 On the Fundamental Group with Restricted Ramification

In contrast to the situation in characteristic zero described in Chapter I.1, the fundamental group $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ of an algebraic curve \mathcal{X} with finite $\emptyset \neq \mathcal{S} \subseteq \mathcal{X}$ over an algebraically closed field k of positive characteristic is not free. Here we first show that at least the projectivity of the fundamental group in the case of restricted ramification remains true, then we discuss the recent solution of Abhyankar's conjecture.

5.1 Projectivity

In this section we show that at least the pro- p -factor groups $\pi_1^{(p)}(\mathcal{X} \setminus \mathcal{S})$ of $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$ for an algebraic curve \mathcal{X} with finite $\emptyset \neq \mathcal{S} \subseteq \mathcal{X}$ are free. As a consequence we obtain the projectivity of $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S})$. The first partial result is an immediate consequence of the Grothendieck Specialization Theorem:

Proposition 5.1. *Let K/k be a rational function field in one variable over an algebraically closed field k , \mathbb{S} a finite subset of $\mathbb{P}(K/k)$ with $|\mathbb{S}| > 1$, and $p \in \mathbb{P}$ different from the characteristic of k . Then the Galois group $\text{Gal}(M_{\mathbb{S}}^{(p)}/K)$ of the maximal p -extension $M_{\mathbb{S}}^{(p)}/K$ unramified outside \mathbb{S} is a free pro- p -group of rank $|\mathbb{S}| - 1$.*

Proof. This follows by an application of the Grothendieck Specialization Theorem I.10.6 to the free fundamental groups $\pi_1^{\text{alg}}(\mathcal{X} \setminus \mathcal{S}) = \text{Gal}(M_{\mathbb{S}}/K)$ of rank $|\mathbb{S}| - 1 = |\mathcal{S}| - 1$ in Theorem I.1.3. \square

Remark. According to Section I.1.4 the corresponding result remains true for function fields K/k of genus $g > 0$ and with $|\mathbb{S}| \geq 1$. In this case the rank equals $|\mathbb{S}| + 2g - 1$.

For convenience we introduce the following notation. Let K/k be an algebraic function field of one variable. Let M be a Galois extension of K with group Γ . A homomorphism φ from Γ to a finite group G is called *ramified* in $\mathfrak{P} \in \mathbb{P}(K/k)$ if \mathfrak{P} is ramified in the Galois extension $M^{\ker(\varphi)}/K$, and is called unramified otherwise. The proof of the following theorem was communicated to us by J.-P. Serre.

Theorem 5.2. *Let K/k be an algebraic function field in one variable over an algebraically closed field k of characteristic $p > 0$ and \mathbb{S} a nonempty finite subset of $\mathbb{P}(K/k)$. Then the Galois group $\text{Gal}(M_{\mathbb{S}}^{(p)}/K)$ of the maximal p -extension unramified outside \mathbb{S} is a free pro- p -group of infinite rank (equal to the cardinality of field k).*

Proof. We first show the freeness of the pro- p -group $\Gamma_K^{(p)}(\mathbb{S}) := \text{Gal}(M_{\mathbb{S}}^{(p)}/K)$. For this it suffices to verify that $H^2(\Gamma_K^{(p)}(\mathbb{S}), \mathbb{Z}_p) = 0$ with trivial action of $\Gamma_K^{(p)}(\mathbb{S})$

on Z_p (see for example Serre (1964), Ch. I, §4, Prop. 21 and Cor. 2 to Prop. 24). Let \mathcal{O} be the set of open normal subgroup in $\Gamma_K^{(p)}(\mathbb{S})$ and φ_O for $O \in \mathcal{O}$ the restriction map from $\Gamma_K^{(p)}(\mathbb{S})$ to $G_O := \text{Gal}((M_{\mathbb{S}}^{(p)})^O/K)$. Then

$$\Gamma_K^{(p)}(\mathbb{S}) = \varprojlim (\varphi_O(\Gamma_K^{(p)}(\mathbb{S})/O))_{O \in \mathcal{O}} = \varprojlim (G_O)_{O \in \mathcal{O}}$$

and hence also (compare Serre (1964), Ch. I, §2, Prop. 8)

$$H^2(\Gamma_K^{(p)}(\mathbb{S}), Z_p) = \varinjlim (\varphi_O^*(H^2(G_O, Z_p)))_{O \in \mathcal{O}}. \quad (5.1)$$

Thus from Theorem IV.6.1 with the subsequent Remark the vanishing of (5.1) follows from the solvability of all finite central embedding problems with kernel Z_p inside $M_{\mathbb{S}}^{(p)}/K$.

So let $\varphi : \Gamma_K^{(p)}(\mathbb{S}) \rightarrow G = \text{Gal}(N/K)$ be an epimorphism onto a finite group G and

$$1 \longrightarrow Z_p \xrightarrow{\iota} \tilde{G} \xrightarrow{\kappa} G \longrightarrow 1$$

be a central group extension with kernel Z_p , $\rho : \Gamma_K^{(p)} \rightarrow \Gamma_K^{(p)}(\mathbb{S})$ the restriction map from the Galois group of the maximal p -extension $M^{(p)}/K$ to the Galois group of the maximal p -extension $M_{\mathbb{S}}^{(p)}/K$ unramified outside \mathbb{S} and $\psi := \varphi \circ \rho$. By the Theorem of Tsen (Theorem IV.1.11(a)) $\Gamma_K^{(p)}$ is a projective (and hence free) profinite group. Thus the embedding problem $\mathcal{E}(\psi, \kappa)$ possesses a solution $\tilde{\psi} : \Gamma_K^{(p)} \rightarrow \tilde{G}$. In what follows we will modify this solution so that it is unramified outside \mathbb{S} and hence factors through $\Gamma_K^{(p)}(\mathbb{S})$. Therefor we denote by \mathbf{T} the finite set of ramified places of $\tilde{\psi}$ not belonging to \mathbb{S} , and by \tilde{N} the solution field of $\tilde{\psi}$. Then $\tilde{\psi}$ induces for every $\mathfrak{P} \in \mathbf{T}$ an epimorphism of local Galois groups

$$\tilde{\psi}_{\mathfrak{P}} : I(\tilde{\mathfrak{P}}/\mathfrak{P}) \cong \Gamma_{K_{\mathfrak{P}}}^{(p)} \rightarrow \text{Gal}(\tilde{N}_{\tilde{\mathfrak{P}}}/K_{\mathfrak{P}}) \cong Z_p.$$

(This is uniquely determined by \mathfrak{P} up to inner automorphisms of $\Gamma_K^{(p)}$.) The local Galois extensions $\tilde{N}_{\tilde{\mathfrak{P}}}/K_{\mathfrak{P}}$ are generated by Artin-Schreier-equations $f_{\mathfrak{P}}(X) = X^p - X - x_{\mathfrak{P}}$ with $x_{\mathfrak{P}} \in K_{\mathfrak{P}}$. By the Strong Approximation Theorem (see for example Hasse (1980), Ch. 24) there exists $x \in K$ such that $\text{ord}_{\mathfrak{P}}(x - x_{\mathfrak{P}})$ is large for all $\mathfrak{P} \in \mathbf{T}$ and $\text{ord}_{\mathfrak{P}}(x) \geq 0$ for $\mathfrak{P} \in \mathbb{P}(K/k) \setminus (\mathbb{S} \cup \mathbf{T})$. The zeroes of $f(X) = X^p - X - x \in K[X]$ then generate a Galois extension L/K with group Z_p whose localizations $L_{\mathfrak{P}}$ for $\mathfrak{P} \in \mathbf{T}$ coincide with $\tilde{N}_{\tilde{\mathfrak{P}}}$ by Krasner's Lemma (see Artin (1967), Ch. 2, Thm. 9), and which by Theorem III.4.7 are trivial for $\mathfrak{P} \in \mathbb{P}(K/k) \setminus (\mathbb{S} \cup \mathbf{T})$. Thus there exists an epimorphism

$$\chi : \Gamma_K^{(p)} \longrightarrow \text{Gal}(L/K) \cong Z_p$$

whose localizations $\chi_{\mathfrak{P}}$ for $\mathfrak{P} \in \mathbb{P}(K/k) \setminus \$$ agree with $\tilde{\psi}_{\mathfrak{P}}$. Since $Z_p \leq \mathcal{L}(\tilde{G})$ the map

$$\tilde{\chi} : \Gamma_K^{(p)} \rightarrow \tilde{G}, \quad \gamma \mapsto \chi(\gamma)^{-1} \tilde{\psi}(\gamma),$$

is a homomorphism which is unramified outside $\$$ by construction. Hence $\tilde{\chi}$ factors through $\Gamma_K^{(p)}(\$)$ and defines a homomorphism

$$\tilde{\varphi} : \Gamma_K^{(p)} \rightarrow \tilde{G} \quad \text{with } \kappa \circ \tilde{\varphi} = \varphi$$

since $\kappa \circ \iota = 0$. This shows the solvability of $\mathcal{E}(\varphi, \kappa)$ and hence the freeness of $\Gamma_K^{(p)}(\$)$.

Since the Artin-Schreier-equations $f(X) = X^p - X - x \in K[X]$ generate different fields for elements x in different classes of $(K, +)$ modulo the subgroup $\{x^p - x \mid x \in K\}$, the rank of $\Gamma_K^{(p)}(\$)$ is at least the cardinality of K , and hence equal to it. \square

Remark. In the case $\$ = \emptyset$ the Galois group $\text{Gal}(M_{\$}^{(p)}/K)$ is again a free pro- p -group. But its rank is now finite and equal to the rank of the Hasse-Witt matrix of K/k (see Šafarevič (1947), Thm. 2).

As a consequence of the preceding theorem we obtain the result announced at the beginning of this section:

Theorem 5.3. *Let K/k be an algebraic function field in one variable over an algebraically closed field k and $\$$ a nonempty subset of $\mathbb{P}(K/k)$. Then the Galois group $\text{Gal}(M_{\$}/K)$ of the maximal Galois extension unramified outside $\$$ is a projective profinite group.*

Proof. By definition we have to verify that every finite embedding problem $\mathcal{E}(\varphi, \kappa)$ for $\Gamma_K(\$) := \text{Gal}(M_{\$}/K)$ has a solution $\tilde{\varphi}$ with $\kappa \circ \tilde{\varphi} = \varphi$ (see Section IV.1.5). By the reduction theorem of Nobusawa (Theorem IV.5.1) it suffices to solve Frattini embedding problems, and by induction over the chief factors of the nilpotent Frattini group, even embedding problems with p -elementary abelian kernel H (see also Fried and Jarden (1986), Lemma 20.9). First let p be equal to the characteristic of K . Then by the Theorem IV.8.2 of Kochendörffer we may restrict ourselves to the solvability of embedding problems $\mathcal{E}(\varphi_p, \kappa_p)$ belonging to a Sylow p -subgroup G_p of $G = \varphi(\Gamma_K(\$))$, where $\varphi_p : \Gamma_L(\$) \rightarrow G_p$ denotes the epimorphism belonging to the fixed field L of $G_p = \kappa(\tilde{G}_p)$. Observe that by the proof of Theorem IV.8.2 a solution field of $\mathcal{E}(\varphi, \kappa)$ can be found inside the Galois closure over K of a solution field of $\mathcal{E}(\varphi_p, \kappa_p)$ such that with $\mathcal{E}(\varphi_p, \kappa_p)$ also $\mathcal{E}(\varphi, \kappa)$ possesses a solution unramified outside $\$$. But the embedding problems $\mathcal{E}(\varphi_p, \kappa_p)$ even have proper solutions since $\Gamma_L^{(p)}(\$)$ is free profinite of infinite rank by the above theorem. With a similar argument we obtain solutions of the corresponding embedding problems in characteristic different from p because here $\Gamma_L^{(p)}(\$)$ is free of finite rank by Proposition 5.1 and the subsequent Remark. \square

By Proposition 5.1 and Theorem 5.2 the group $\text{Gal}(M_{\mathbb{S}}/K)$ is not a free profinite group if K has positive characteristic, in spite of the fact that its cohomological dimension equals 1.

5.2 Embedding Problems with p -Kernel

A further very useful result for the study of the fundamental group with restricted ramification in positive characteristic is the following strengthening of the embedding Theorem IV.8.3 to embedding problems with restricted ramification going back to Serre.

Theorem 5.4 (Serre (1990)). *Let k be an algebraically closed field of characteristic p and $\mathcal{E}(\varphi, \kappa)$ a finite geometric embedding problem over $K = k(t)$ whose kernel H is a p -group. Assume that the ramification points of the Galois extension $N/k(t)$ for the quotient G are contained in the nonempty set $\mathbb{S} \subset \mathbb{P}(k(t)/k)$. Then $\mathcal{E}(\varphi, \kappa)$ has a proper geometric solution whose solution field $\tilde{N}/k(t)$ is only ramified in \mathbb{S} .*

Sketch of proof. By assumption the epimorphism $\varphi : \Gamma_K \rightarrow G$ factors through the Galois group $\Gamma_K(\mathbb{S}) := \text{Gal}(M_{\mathbb{S}}/K)$ of the maximal Galois extension of K unramified outside \mathbb{S} . Therefore without loss of generality we can replace Γ_K by $\Gamma_K(\mathbb{S})$. By induction along a chief series we may assume that the kernel H is an elementary abelian p -group. Since $\Gamma_K(\mathbb{S})$ by Theorem 5.3 is a projective profinite group the embedding problem $\mathcal{E}(\varphi, \kappa)$ is solvable. To obtain a proper solution by the Theorem IV.1.9 of Ikeda it is enough to solve properly split embedding problems with the same kernel H . The problem therefore is reduced to properly solving split embedding problems with elementary abelian p -kernel H inside $\Gamma_K(\mathbb{S})$.

Via the semidirect product $H \rtimes G$ and φ the group H becomes a $\Gamma_K(\mathbb{S})$ -module. It is easy to verify that $\mathcal{E}(\varphi, \kappa)$ has a proper solution if and only if the inflation $\varphi^*(H^1(G, H))$ of $H^1(G, H)$ is properly contained in $H^1(\Gamma_K(\mathbb{S}), H)$. Therefore the assertion follows from the fact proved by Serre (1990), Prop. 4, that $H^1(\Gamma_K(\mathbb{S}), H)$ is an infinite dimensional \mathbb{F}_p -vector space. \square

5.3 The Conjecture of Abhyankar for the Affine Line

Apart from the result in the previous sections, almost nothing is known about the fundamental group in the case of restricted ramification. Its structure even depends on the choice of the set \mathcal{S} of ramification points, as the following example shows: Let $p > 2$ and $\mathcal{P}_i \in \mathbb{P}^1(k)$ such that $\mathcal{I}_i := \{0, 1, \infty, \mathcal{P}_i\}$ has ordinary respectively supersingular j -invariant for $i = 1, 2$ (see for example Silverman (1986), Ch. V). It is shown in Harbater (1994b), Thm. 1.8, that in fact $\pi_1^{\text{alg}}(\mathbb{P}^1(k) \setminus \mathcal{I}_i)$ are non-isomorphic for $i = 1, 2$.

At present the only information in this situation comes from the conjecture of Abhyankar (1957), which describes the set of finite factor groups of the fundamental group. This was proved by Raynaud (1994) in the case of one ramification point and genus zero, and then by Harbater (1994a) in general. To formulate the conjecture, we introduce the following notations. Let G be a finite group and p a prime number. Then $O^{p'}(G)$ is the normal subgroup of G generated by the Sylow p -subgroups of G , hence $G/O^{p'}(G)$ is the largest factor group of G of order prime to p . A group G with $G = O^{p'}(G)$ is called a *quasi- p -group*. Thus quasi- p -groups are generated by their elements of p -power order. For $G_p \leq G$ a Sylow p -subgroup of a finite group G define

$$O(G, G_p) := \langle H \mid H < G \text{ is quasi-}p, H \cap G_p \text{ is a Sylow } p\text{-subgroup of } H \rangle.$$

The Abhyankar conjecture for the affine line, which was proved by Raynaud, can be stated as follows:

Theorem 5.5 (Raynaud (1994)). *Let k be an algebraically closed field of characteristic $p \neq 0$ and G a finite group. Then G occurs as the Galois group of an unramified connected cover of the affine line over k if and only if G is a quasi- p -group.*

The proof of this result goes beyond the scope of the present book. Let us just give an informal description of the steps Raynaud uses in his proof (see also Harbater (1995b) for an introduction). Let k be an algebraically closed field of characteristic p and G a finite quasi- p -group with Sylow p -subgroup G_p . Then an induction argument together with the Theorem I.10.6 of Grothendieck easily shows that Theorem 5.5 is implied by the following three assertions:

- (a) Let $H \triangleleft G$ be a p -group. If G/H occurs as the Galois group of an unramified cover of the affine line over k then so does G .
- (b) If $G = O(G, G_p)$ and all proper quasi- p -subgroups of G occur as the Galois group of an unramified cover of the affine line over k , then so does G .
- (c) If $G \neq O(G, G_p)$ and G has no non-trivial normal p -subgroup, then G occurs as the Galois group of an unramified cover of the affine line over k .

The three alternatives enumerated above require three quite different approaches. Part (a) is solved by Theorem 5.4 or Theorem 5.3 respectively.

The proof of case (b) is achieved by gluing suitable rigid analytic spaces. Let H_1, \dots, H_r be the proper quasi- p subgroups of G such that $H_i \cap G_p$ is a Sylow p -subgroup of H_i . By assumption, for each of these there exists an unramified Galois cover $\mathcal{X}_i \rightarrow \mathbb{A}^1(K)$ with group H_i , where $K = k((u))$. Moreover it may be reached that the inertia groups above infinity are conjugate to subgroups Q_i of G_p . Thus the restriction of \mathcal{X}_i to an annulus \mathcal{A}_i centered around ∞ splits into a disjoint union of copies of Q_i -covers $\mathcal{B}_i \rightarrow \mathcal{A}_i$. Now choose r points $\mathcal{P}_1, \dots, \mathcal{P}_r \in \mathbb{A}^1(K)$ and copies of the annuli \mathcal{A}_i centered around the \mathcal{P}_i such that the union of the discs \mathcal{D}_i corresponding to the annuli \mathcal{A}_i is disjoint and $\mathbb{A}^1(K)$ contains a point in each component of $\mathbb{A}^1(K) \setminus (\cup_{i=1}^r \mathcal{A}_i \cup \{\mathcal{P}_1, \dots, \mathcal{P}_r\})$. Then possibly after replacing K by a finite separable extension there exists a Galois cover $\mathcal{Y} \rightarrow \mathbb{A}^1(K) \setminus \{\mathcal{P}_1, \dots, \mathcal{P}_r\}$ with group G_p whose restriction to each \mathcal{A}_i is a disjoint union of copies of $\mathcal{B}_i \rightarrow \mathcal{A}_i$.

The proof of this fact proceeds by induction on the order of G_p and uses étale cohomology. Induction to G and pasting each \mathcal{X}_i to \mathcal{Y} over \mathcal{A}_i yields a cover with group $G = O(G, G_p)$, which is connected by the assumption in case (b).

In case (c) let R be a complete discrete valuation ring with residue field k and with field of fractions K of characteristic zero. Such a ring can be constructed using Witt vectors (see for example Serre (1979), §5, Thm. 3). By Theorem 2.5 there exists a geometric Galois extension of $K(t)$ with group G . Since G is a quasi- p -group, so generated by elements of p -power order, the proof of Proposition 2.4 shows that we may moreover assume that the inertia groups are (cyclic) p -groups. Using the theory of semistable reduction it is possible to choose K and R such that the corresponding covering $\mathcal{Y} \rightarrow \mathcal{X} = \mathbb{P}^1(K)$ has an R -model $\mathcal{Y}_R \rightarrow \mathcal{X}_R$ with semistable reduction and such that \mathcal{X}_R is a blow-up of $\mathbb{P}^1(R)$. Since \mathcal{X}_R is a model of the projective line the special fiber \mathcal{X}_k has to be a tree of projective lines over k . The strict transform e' of \mathcal{X} in $\mathbb{P}^1(k)$ will be taken as the origin of the tree \mathcal{X}_k . To each irreducible component c of \mathcal{Y}_k is associated its stabilizer D_c , the decomposition group with respect to the generic point of c , and the pointwise stabilizer I_c , the inertia group. It is shown by Raynaud (1994), 6.3, that \mathcal{X}_R can be chosen such that the inertia group I_c at each component c of \mathcal{Y}_k is a p -group and I_c is non-trivial unless c lies above a terminal component of \mathcal{X}_k . There exists a partial ordering on the tree \mathcal{X}_k with the terminal components maximal and the base component e' minimal. This allows to construct an analogous partially ordered subtree T of \mathcal{Y}_k , chosen such that $G_e = G$ for the preimage e of e' . Here for c a component of T we define $G_c := \langle O^{p'}(D_d) \mid d \in T, d \geq c \rangle$.

If $c \in T$ is maximal with $G_c = G$ then using that we are not in case (a) one can show by group theoretic arguments that either $I_c = 1$ or $G = G_c \subseteq O(G, G_p)$ for some Sylow p -subgroup G_p of G . But the latter case cannot happen in (c) (it was treated in (b)). Thus $I_c = 1$ and c must be a terminal component with $D_c = G$. Since c is terminal, its image c' in \mathcal{X}_k is a projective line which intersects the other components in a single point. By deleting this point we obtain an unramified cover of the affine line with group G .

5.4 The General Case of the Conjecture of Abhyankar

Abhyankar (1957) posed the following conjecture on finite quotients of the fundamental group of an affine smooth connected curve \mathcal{C} over an algebraically closed field of characteristic p : If \mathcal{C} is obtained by removing $s > 0$ points from a projective connected normal curve of genus g then G occurs as a quotient of the algebraic fundamental group of \mathcal{C} if and only if $G/O^{p'}(G)$ is generated by $2g + s - 1$ elements. This general form of the conjecture was proved by Harbater (1994a) with formal geometric methods, building on Raynaud's result for the affine line. We sketch a proof of this given subsequently by Pop (1995), which essentially reduces it to the case of the affine line. The following result is a special case of Cor. 4.2.6 in Raynaud (1994); its proof will not be given here.

Theorem 5.6. Let

$$1 \longrightarrow H \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

be an exact sequence of finite groups where H is a p -group. Let k be a complete ultrametric field, $\emptyset \neq \mathcal{S} \subset \mathbb{P}^1(k)^{\text{an}}$ a finite set, $\mathcal{D} \subseteq \mathbb{P}^1(k)^{\text{an}}$ affinoid such that each connected component of $\mathbb{P}^1(k)^{\text{an}} \setminus \mathcal{D}$ contains a point of \mathcal{S} . Assume given a Galois covering $\mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ with group G which is unramified outside \mathcal{S} and trivial over \mathcal{D} , and a Galois covering $\mathcal{Y} \rightarrow \mathcal{D}$ with group H . Then there exists a connected Galois covering $\mathcal{Z} \rightarrow \mathbb{P}^1(k)^{\text{an}}$ with group \tilde{G} unramified outside \mathcal{S} isomorphic to $\text{Ind}_H^{\tilde{G}}(\mathcal{Y})$ over \mathcal{D} such that the quotient by H is isomorphic to the covering $\mathcal{X} \rightarrow \mathbb{P}^1(k)^{\text{an}}$.

This allows to prove a generalization of Theorem 5.4 from p -kernel to quasi- p -kernel.

Theorem 5.7 (Pop (1995)). *Let k be an algebraically closed field of characteristic p and $\mathcal{E}(\varphi, \kappa)$ a finite geometric embedding problem over $k(t)$ such that the ramification points of the Galois extension $N/k(t)$ for the quotient G are contained in the nonempty set $\mathbb{S} \subset \mathbb{P}(k(t)/k)$. Assume that there exists an analytic Galois cover $\psi : \mathcal{Y} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group H unramified outside $\infty \in \mathbb{P}^1(k^*)^{\text{an}}$ such that the decomposition groups of points above ∞ are the Sylow p -subgroups of H . Then $\mathcal{E}(\varphi, \kappa)$ has a proper geometric solution whose solution field $\bar{N}/k(t)$ is only ramified in \mathbb{S} .*

Proof. We first reduce the assertion to embedding problems of a very special type. By the Theorem of Ikeda (Theorem IV.1.9) since the Galois group of the maximal extension of $k(t)$ unramified outside \mathbb{S} is projective by Theorem 5.3 we may assume that $\mathcal{E}(\varphi, \kappa)$ is split. Let H_p be a Sylow p -subgroup of H . Since all Sylow p -subgroups of H are H -conjugate, we have $(\mathcal{N}_{\tilde{G}}(H_p) : \mathcal{N}_H(H_p)) = (\tilde{G} : H) = |G|$, so we obtain an induced embedding problem $\mathcal{E}(\varphi, \kappa_1)$

$$1 \longrightarrow \mathcal{N}_H(H_p) \longrightarrow \mathcal{N}_{\tilde{G}}(H_p) \longrightarrow G \longrightarrow 1$$

for the normalizers of H_p , where $\kappa_1 = \kappa|_{\mathcal{N}_{\tilde{G}}(H_p)}$. By Theorem 5.3 the Galois group of the maximal extension field of $k(t)$ unramified outside \mathbb{S} is projective. Thus $\mathcal{E}(\varphi, \kappa_1)$ has a solution φ_1 , with solution field N_1 , say, such that $N_1/k(t)$ is unramified outside \mathbb{S} . With $G_1 := \text{Gal}(N_1/k(t))$ we obtain a further induced embedding problem $\mathcal{E}(\varphi_1, \kappa')$

$$1 \longrightarrow H \longrightarrow \tilde{G} \times_G G_1 \longrightarrow G_1 \longrightarrow 1$$

again with kernel H by construction. Thus any (proper, geometric) solution of $\mathcal{E}(\varphi', \kappa')$ ramified only in \mathbb{S} gives rise to a (proper, geometric) solution of $\mathcal{E}(\varphi, \kappa)$ only ramified in \mathbb{S} . Moreover $\mathcal{E}(\varphi', \kappa')$ is still split, and by construction G_1 normalizes a Sylow p -subgroup of H . We are thus reduced to solving split embedding problems $\mathcal{E}(\varphi, \kappa)$ such that G normalizes a Sylow p -subgroup H_p of H .

As in the proof of Theorem 2.10 it suffices to solve the induced embedding problem $\mathcal{E}(\varphi^*, \kappa^*)$ obtained from $\mathcal{E}(\varphi, \kappa)$ by extension of constants with the com-

plete ultrametric field $k^* := k((u))$. Note that if we have found a solution field $\tilde{N}^*/k(u)(t)$ ramified only in \mathbb{S} , then the same is true for the specialized solution field $\tilde{N}/k(t)$.

So let now $\mathcal{E}(\varphi, \kappa)$ be a split embedding problem over $k^*(t)$ such that G normalizes a Sylow p -subgroup H_p of the kernel H and N^* the fixed field of $\ker(\varphi)$. Via analytification of suitable curves $N^*/k^*(t)$ corresponds to an analytic Galois cover $\varphi : \mathcal{X} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group G unramified outside a set $\mathcal{S} \subset \mathbb{P}^1(k^*)^{\text{an}}$.

We first construct an analytic Galois cover $\mathcal{Z} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group the semidirect product $H_p \cdot G$ ramified in at most $|\mathcal{S}| + 1$ points. For this, the cover $\psi : \mathcal{Y} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ is subdivided into several parts. Let \mathcal{D}_0 be a disc in $\mathbb{P}^1(k^*)^{\text{an}}$ around 0 and $\mathcal{Y}_1 = \psi^{-1}(\mathcal{D}_0)$, $\mathcal{Y}_2 = \psi^{-1}(\mathbb{P}^1(k^*)^{\text{an}} \setminus \mathcal{D}_0^\circ)$ and

$$\partial \mathcal{Y}_1 := \partial \mathcal{Y}_2 = \mathcal{Y}_1 \cap \mathcal{Y}_2 = \psi^{-1}(\partial \mathcal{D}_0),$$

where from now on for discs $\mathcal{D}(a, b)$ we will write $\partial \mathcal{D}(a, b)$ for $\mathcal{D}(a, b) \setminus \mathcal{D}(a, b)^\circ$. Then by a suitable choice of the uniformizing parameter for $\mathbb{P}^1(k^*)^{\text{an}}$ we may assume that the following hold. Let $y \in \mathcal{Y}_2$ be a preimage of ∞ with decomposition group equal to H_p and \mathcal{Y}_0 the connected component of \mathcal{Y}_2 containing y . Then \mathcal{Y}_2 is the disjoint union of $(H : H_p)$ copies of \mathcal{Y}_0 ,

$$\mathcal{Y}_2 = \bigcup_{\tau \in H/H_p} \tau \mathcal{Y}_0,$$

$\mathcal{Y}_0 \rightarrow \mathbb{P}^1(k^*)^{\text{an}} \setminus \mathcal{D}_0^\circ$ is connected Galois with group H_p and $\partial \mathcal{Y}_0 := \mathcal{Y}_0 \cap \partial \mathcal{Y}_1 \rightarrow \partial \mathcal{D}_0$ is still a connected Galois cover with group H_p which moreover is unramified. Furthermore, by Lemma 1.8 the covering $\mathcal{Y}_1 \rightarrow \mathcal{D}_0$ is connected and Galois with group H .

Next for all $\mathcal{P} \in \mathcal{S}$ we choose disjoint small discs $\mathcal{D}_{\mathcal{P}}$ around \mathcal{P} in $\mathbb{P}^1(k^*)^{\text{an}}$ such that the preimage $\mathcal{U}' = \varphi^{-1}(\mathcal{D}')$ in \mathcal{X} of the complement

$$\mathcal{D}' := \mathbb{P}^1(k^*)^{\text{an}} \setminus \bigcup_{\mathcal{P} \in \mathcal{S}} \mathcal{D}_{\mathcal{P}}^\circ$$

is the trivial covering $\text{Ind}_1^G(\mathcal{D}')$ of \mathcal{D}' with Galois group G (which is possible after a suitable finite separable extension of k^* by Proposition 2.2). We fix a point $\mathcal{P} \in \mathcal{S}$ and choose a point $\tilde{\mathcal{P}} \neq \mathcal{P}$ in $\mathcal{D}_{\mathcal{P}}^\circ$ having only k^* -rational, distinct preimages in \mathcal{X} (after a suitable finite separable extension of k^*). Let $\tilde{\mathcal{D}} \subset \mathcal{D}_{\mathcal{P}}^\circ$ be a small disc containing $\tilde{\mathcal{P}}$ and not containing \mathcal{P} . Since $\tilde{\mathcal{D}}$ is analytically isomorphic to \mathcal{D}_0 , from one piece of \mathcal{Y} we obtain a connected Galois cover $\mathcal{Y}_1 \rightarrow \mathcal{D}_0 \xrightarrow{\sim} \tilde{\mathcal{D}}$ with group H . Its restriction to $\partial \tilde{\mathcal{D}}$ decomposes into connected components isomorphic to $\partial \mathcal{Y}_0$, which gives a connected unramified Galois cover $\partial \mathcal{Y}_0 \rightarrow \partial \tilde{\mathcal{D}}$ with group H_p .

We have thus obtained the Galois cover $\mathcal{X} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group G , trivial over $\mathcal{D}' \cup \partial \tilde{\mathcal{D}}$, and a Galois cover of $\mathcal{D}' \cup \partial \tilde{\mathcal{D}}$ with group H_p given by $\text{Ind}_1^{H_p}(\mathcal{U}')$ above \mathcal{D}' and by $\partial \mathcal{Y}_0$ above $\partial \tilde{\mathcal{D}}$. By Raynaud's Theorem 5.6 there exists a connected

Galois cover $\mathcal{X} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group \tilde{G}_p ramified only in \mathcal{S} and some further point in $\tilde{\mathcal{D}}^\circ$, isomorphic to $\text{Ind}_{\tilde{G}_p}^{\tilde{G}_p}(\mathcal{U}')$ above \mathcal{D}' and to $\text{Ind}_{H_p}^{\tilde{G}_p}(\partial\mathcal{Y}_0)$ above $\partial\tilde{\mathcal{D}}$. Let $\tilde{\mathcal{D}}' = \mathbb{P}^1(k^*)^{\text{an}} \setminus \tilde{\mathcal{D}}^\circ$ and \mathcal{V}' its preimage in \mathcal{X} . Then \mathcal{V}' is a connected Galois cover of $\tilde{\mathcal{D}}'$ with group \tilde{G}_p unramified outside $\mathcal{S} \subset \tilde{\mathcal{D}}'$.

We are now ready to construct the Galois cover of $\mathbb{P}^1(k^*)^{\text{an}}$ with group \tilde{G} solving $\mathcal{E}(\varphi, \kappa)$. Let $\tilde{\mathcal{X}}_1 = \text{Ind}_{\tilde{G}_p}^{\tilde{G}}(\mathcal{V}')$ above $\tilde{\mathcal{D}}'$. Then restriction to $\partial\tilde{\mathcal{D}}'$ yields

$$\text{Ind}_{\tilde{G}_p}^{\tilde{G}}(\partial\mathcal{V}') \cong \text{Ind}_{\tilde{G}_p}^{\tilde{G}_p}(\text{Ind}_{H_p}^{\tilde{G}_p}(\partial\mathcal{Y}_0)) \cong \text{Ind}_{H_p}^{\tilde{G}}(\partial\mathcal{Y}_0)$$

with the preimage $\partial\mathcal{V}'$ of $\partial\tilde{\mathcal{D}}'$, by the construction of \mathcal{X} . Further, let $\tilde{\mathcal{X}}_2 = \text{Ind}_H^{\tilde{G}}(\mathcal{Y}_1)$ above $\tilde{\mathcal{D}} \cong \mathcal{D}_0$. Its restriction to $\partial\tilde{\mathcal{D}} = \partial\tilde{\mathcal{D}}'$ is \tilde{G} -equivariantly isomorphic to

$$\text{Ind}_H^{\tilde{G}}(\partial\mathcal{Y}_1) \cong \text{Ind}_H^{\tilde{G}}(\text{Ind}_{H_p}^H(\partial\mathcal{Y}_0)) \cong \text{Ind}_{H_p}^{\tilde{G}}(\partial\mathcal{Y}_0).$$

Hence by the Gluing Proposition 1.4 the two covers $\tilde{\mathcal{X}}_1$ and $\tilde{\mathcal{X}}_2$ may be glued above $\partial\tilde{\mathcal{D}}'$ to give a Galois cover $\tilde{\mathcal{X}} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group \tilde{G} . This cover is connected since \tilde{G} is generated by \tilde{G}_p and H , and it is only ramified in \mathcal{S} since $\mathcal{V}' \rightarrow \tilde{\mathcal{D}}'$ is only ramified in \mathcal{S} , while $\mathcal{Y}_1 \rightarrow \tilde{\mathcal{D}}$ is unramified by construction. Further, the quotient of $\tilde{\mathcal{X}}$ by H is isomorphic to $\mathcal{X} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$, thus $\tilde{\mathcal{X}}$ solves the embedding problem $\mathcal{E}(\varphi, \kappa)$. \square

Remark. If H is a quasi- p -group then by the Theorem 5.5 of Raynaud there exists an analytic Galois cover $\psi : \mathcal{Y} \rightarrow \mathbb{P}^1(k^*)^{\text{an}}$ with group H unramified outside $\infty \in \mathbb{P}^1(k^*)^{\text{an}}$. Further by Raynaud (1994), Cor. 2.2.6, this may be chosen such that the Sylow p -subgroups of H are the decomposition groups of points above ∞ . Thus, the preceding Theorem 5.7 applies if the kernel H is a quasi- p -group. On the other hand, starting with abelian p -groups, Theorem 5.7 allows to give an alternative proof of the Theorem 5.4 of Serre.

We can now state the version of Abhyankar's conjecture for ramified extensions of the projective line; the general result for function fields in one variable is given in Harbater (1994a) and Pop (1995).

Theorem 5.8 (Raynaud (1994), Harbater (1994a)). *Let k be an algebraically closed field of characteristic p , and $\mathbb{S} \subseteq \mathbb{P}(k(t)/k)$ a finite set of cardinality s . Then G occurs as a Galois group over $k(t)$ unramified outside \mathbb{S} if and only if $G/O^{p'}(G)$ occurs as the Galois group of an extension of $\mathbb{C}(t)$ unramified outside a set of cardinality s , i.e., $G/O^{p'}(G)$ is generated by $s - 1$ elements.*

Proof. With the above preparations, this result is easy to obtain. In fact, first assume that G occurs as a Galois group over $k(t)$ unramified outside of \mathbb{S} . Then the p -prime group $G/O^{p'}(G)$ also is a factor group of $\pi_1^{\text{alg}}(\mathbb{P}(k(t)/k) \setminus \mathbb{S})$, hence by the theorem of Grothendieck (Theorem I.10.6) already occurs over $\mathbb{C}(t)$ with the same number of ramification points.

Conversely, let \tilde{G} be a finite group such that $G := \tilde{G}/O^{p'}(\tilde{G})$ occurs as a Galois group of an extension of $\mathbb{C}(t)$ unramified outside a set of cardinality s . Then again by the theorem of Grothendieck the p -prime group G also occurs as a Galois group of a field extension $N/k(t)$ unramified outside a set $\$$ of cardinality s . Let $\mathcal{E}(\varphi, \kappa)$ be the embedding problem associated to the group extension $\tilde{G} = O^{p'}(\tilde{G}) \cdot G$ and the Galois extension $N/k(t)$ with $\text{Gal}(N/k(t)) \cong G$. Then by Theorem 5.7 and the subsequent Remark $\mathcal{E}(\varphi, \kappa)$ has a proper solution whose solution field is again ramified at most in $\$$. \square

Appendix: Example Polynomials

In this appendix we list example polynomials whose roots generate regular extension fields of $\mathbb{Q}(t)$, respectively number fields over \mathbb{Q} with given Galois group of small permutation degree. The first set of examples realizes most of the equivalence types of transitive permutation groups of degree less than 12 as regular Galois groups over $\mathbb{Q}(t)$. (There are 301 inequivalent transitive permutation groups of degree 12.) Most of these results are new. In the second table, we collect the known explicit regular Galois realizations of primitive non-solvable permutation groups of degree at most 31 over $\mathbb{Q}(t)$ from the literature. For both sets of tables the results were mainly obtained by the rigidity method described in Chapter I and descent arguments.

Finally, we give example polynomials generating number fields over \mathbb{Q} with given Galois group of permutation degree at most 14. For degree less than 12, these were either found by a random search, and then the Galois group was verified by the Galois group recognition programs in several computer algebra systems, or they were obtained by specializing the parametric realizations from the first set of tables. (Such specializations tend to have larger field discriminant.) The polynomials of degree 12 to 14 are taken from Klüners and Malle (2000, 2002). The polynomials listed in this table were chosen so that their coefficient sum is small.

1 Regular Realizations for Transitive Groups of Degree Less than 12

Here we give polynomials generating regular field extensions of $\mathbb{Q}(t)$ with Galois groups most of the transitive permutation groups of degree less than 12. The generic formulas for polynomials with symmetric or alternating group of arbitrary degree are given separately. In all other cases the groups are numbered according to the list in Butler and McKay (1983), so that a polynomial $f_{n,i}$ has Galois group the transitive permutation group of degree n denoted by T_i in loc. cit.

Table 1.1 Symmetric and alternating groups

S_n	$x^n - t(nx - n + 1)$
A_n	$\begin{cases} f_{S_n}(x, 1 - (-1)^{n(n-1)/2}nt^2) & \text{for } n \equiv 1 \pmod{2} \\ f_{S_n}(x, 1/(1 + (-1)^{n(n-1)/2}(n-1)t^2)) & \text{for } n \equiv 0 \pmod{2} \end{cases}$

Table 1.2 Degree 4

$f_{4,3}$	$x^4 - 2x^2 + t$
$f_{4,2}$	$x^4 + tx^2 + 1$
$f_{4,1}$	$x^4 + tx^3 - 6x^2 - tx + 1$

Table 1.3 Degree 5

$f_{5,3}$	$x^5 + 10x^3 + 5tx^2 - 15x + t^2 - t + 16$
$f_{5,2}$	$x^2(x+1)^2(x+2) - (x-2)^2(x-1)t$
$f_{5,1}$	$x(x^2 - 25)^2 + (x^4 - 20x^3 - 10x^2 + 300x - 95)t^2 - 4(x-3)^2t^4$

Table 1.4 Degree 6

$f_{6,14}$	$x^6 - 2x^5 + (5x^2 - 6x + 2)t$
$f_{6,13}$	$x^6 - (3x - 2)^2t$
$f_{6,12}$	$f_{6,14}(x, 1 - 5t^2)$
$f_{6,11}$	$x^6 - (3x^2 + 1)t/4$
$f_{6,10}$	$f_{6,13}(x, 1/(t^2 + 1))$
$f_{6,9}$	$f_{6,13}(x, 1 - t^2)$
$f_{6,8}$	$f_{6,11}(x, 1/(1 - 3t^2))$
$f_{6,7}$	$f_{6,11}(x, t^2)$
$f_{6,6}$	$f_{6,11}(x, 3t^2 + 1)$
$f_{6,5}$	$f_{6,13}(x, -12t^2(3t^2 + 1))$
$f_{6,4}$	$f_{6,11}(x, (t^2 + 3)^2/(t^2 - 3)^2)$
$f_{6,3}$	$x^2(x^2 + 3)^2 + 4t$
$f_{6,2}$	$f_{6,3}(x, 3t^2 + 1)$
$f_{6,1}$	$x^6 + (3x^2 + 4)^2(3t^2 + 1)$

Table 1.5 Degree 7

$f_{7,5}$	$(x^4 - 3x^3 - x + 4)(x^3 - x + 1) - x^2(x - 1)t$
$f_{7,4}$	$x^7 + 28x^6 + 63x^5 + 1890x^3 + 3402x^2 - 5103x + 33534 + x(x^6 - 63x^4 - 3402x - 5103)t + 13122t^2$
$f_{7,3}$	see Smith (1993)
$f_{7,2}$	$f_{7,4}(x, (t^3 - 27t^2 - 9t + 27)/(3(t^3 + t^2 - 9t - 1)))$

$f_{7,1}$	$x^7 - 21\phi_7(t)x^5 - 7\phi_7(t)(10t^3 + 5t^2 - 5t - 3)x^4 - 7(15t^6 + 15t^5 - 20t^4 - 27t^3 - 13t^2 - 6t - 13)\phi_7(t)x^3 - 7(12t^9 + 18t^8 - 30t^7 - 63t^6 - 35t^5 - 14t^4 - 35t^3 + 2t^2 + 31t + 16)\phi_7(t)x^2 - 7(t-1)\phi_7(t)(5t^{11} + 15t^{10} - 5t^9 - 62t^8 - 93t^7 - 91t^6 - 126t^5 - 166t^4 - 113t^3 - 30t^2 - 8t - 12)x - (6t^{15} + 15t^{14} - 35t^{13} - 126t^{12} - 63t^{11} + 70t^{10} - 91t^9 - 271t^8 + 131t^7 + 427t^6 + 126t^5 - 84t^4 + 175t^3 + 189t^2 - 29t - 97)\phi_7(t)$
-----------	--

Table 1.6 Degree 8

$f_{8,48}$	$x^4(x-2)^2(x^2+x+2)-(x-1)^2(x^2+x+1)t$
$f_{8,47}$	$x^8 - (4x-3)^2 t$
$f_{8,46}$	$f_{8,47}(x, t^2 + 1)$
$f_{8,45}$	$f_{8,47}(x, 1/(1-t^2))$
$f_{8,44}$	$x^8 + (4x^2 + 3)t$
$f_{8,43}$	$x^6(x^2-x+7) - 108(x-1)t$
$f_{8,42}$	$f_{8,47}(x, -1/(12t^2(3t^2-1)))$
$f_{8,41}$	$(x^2-2)^4 - 2^6(2x-3)^2t/3^3$
$f_{8,40}$	$x^4(x^4-8x^2+18)-27t$
$f_{8,39}$	$f_{8,44}(x, 3t^2)$
$f_{8,38}$	$f_{8,44}(x, 1/(3t^2+1))$
$f_{8,37}$	$x^8 + 6x^7 + 3(7x^2 + 6x + 36)(7t^2 + 144)$
$f_{8,36}$	$(f_{9,32}(x, 0) - f_{9,32}(t, 0))/(x-t)$
$f_{8,35}$	$f_{8,44}(x, -27t^2(t-1)/4)$
$f_{8,34}$	$f_{8,41}(x, 1-t^2)$
$f_{8,33}$	$f_{8,41}(x, 1/(3t^2+1))$
$f_{8,32}$	$f_{8,40}(x, -3t^2)$
$f_{8,31}$	$f_{8,44}(x, 27(t^2-1)^2/(t^2+3)^3)$
$f_{8,30}$	$x^4(x^4+4x^2+6) - (4x^2+1)(3t^2+2)^2(3t^2-1)/4$
$f_{8,29}$	$f_{8,44}(x, 27t^2(t^2-1)^2/4)$
$f_{8,28}$	$f_{8,44}(x, 27t^4(t^2+1)/4)$
$f_{8,27}$	$f_{8,44}(x, 27(t^2+4)/(4(t^2+3)^3))$
$f_{8,26}$	$f_{8,40}(x, 27t^2(t-1)/((3t+1)(3t-2)^2))$
$f_{8,25}$	see Smith (1993)
$f_{8,24}$	$(x^2+x+1)^4 - (2x+1)^2 t$
$f_{8,23}$	$x^2(x^2+396)^2(x^2+11) - (x^2+4)^2(x^2+256)t$
$f_{8,22}$	$f_{8,41}(x, 27t^2/(4(t^2-1)^3))$
$f_{8,21}$	$x^8 + 2(t^2-1)x^6 + (3t^4-t^2)x^4 + 2(t^6+t^4)x^2 + t^8 + t^6$
$f_{8,20}$	$f_{8,41}(x, 27t^4(t^2+1)/4)$

$f_{8,19}$	$f_{8,41}(x, 27(t^2 + 4)/(4(t^2 + 3)^3))$
$f_{8,18}$	$f_{8,41}(x, 27(t^2 - 1)^2/(t^2 + 3)^3)$
$f_{8,17}$	$(x^4 + 4x^3 - 6x^2 - 4x + 1)^2 - 16x^2(x^2 - 1)^2 t$
$f_{8,16}$	$f_{8,40}(x, -27(t^2 + 2)^2/(t^4(4t^2 + 9)))$
$f_{8,15}$	$x^8 + 8x^6 + 4(4t - 11)x^4 + 8(t - 3)(t - 2)x^2 + t(t - 3)^2$
$f_{8,14}$	$f_{8,24}(x, 1 - 3t^2)$
$f_{8,13}$	$f_{8,24}(x, 1/(3t^2 + 1))$
$f_{8,12}$	$f_{8,23}(x, -t^2)$
$f_{8,11}$	$f_{8,15}(x, t^2)$
$f_{8,10}$	$f_{8,41}(x, 2^2 3^3 t^4 (t^2 + 9)(t^2 + 1)/(t^2 + 3)^6)$
$f_{8,9}$	$f_{8,24}(x, -27t^2(t - 1)/4)$
$f_{8,8}$	$f_{8,15}(x, (8t^2 + 3)/(2t^2 + 1))$
$f_{8,7}$	$f_{8,15}(x, 4/(t^2 + 1))$
$f_{8,6}$	$f_{8,15}(x, 2t^2 + 3)$
$f_{8,5}$	$x^8 - 4(t^2 + 2)(t^2 + 1)x^6 + 2(3t^2 + 1)(t^2 + 1)(t^2 + 2)^2 x^4 - 4(t^2 + 2)^2(t^2 + 1)^3 x^2 t^2 + (t^2 + 2)^2(t^2 + 1)^4 t^4$
$f_{8,4}$	$(x^4 - 6x^2 + 1)^2 + 16x^2(x^2 - 1)^2 t$
$f_{8,3}$	$f_{8,24}(x, 27(t^2 - 1)^2/(t^2 + 3)^3)$
$f_{8,2}$	$f_{8,24}(x, 27(t^2 + 4)/(4(t^2 + 3)^3))$
$f_{8,1}$	$x^8 - 4(t^4 + 1)x^6 + 2(4t^2 + 1)(t^4 + 1)x^4 - 4(t^2 + 1)(t^4 + 1)t^2 x^2 + (t^4 + 1)t^4$

Table 1.7 Degree 9

$f_{9,32}$	$x^9 - 3x^8 + 4x^7 - 28x^6 + 126x^5 - 266x^4 + 308x^3 - t x^2 + (3t - 539)x - 4t + 805$
$f_{9,31}$	$x^4(x + 1)^3(x + 3)^2 - 4/27(3x + 1)^3 t$
$f_{9,30}$	$x^4(x - 3)^2(x^3 - 3x^2 - 12) + 2^8 t$
$f_{9,29}$	$f_{9,31}(x, t^2)$
$f_{9,28}$	$f_{9,31}(x, 1/(3t^2 + 1))$
$f_{9,27}$	$f_{9,32}(x, (t^3 - 6t^2 + 3t + 1)/(t^3 - 3t + 1))$
$f_{9,26}$	$(x^3 - 19x^2 + 97x - 27)(x^2 - 4x - 7)^3 + 16/27x^2(x - 7)t$
$f_{9,25}$	$f_{9,30}(x, 1/(3t^2 + 1))$
$f_{9,24}$	$x^6(x^3 + 9x + 6) - 4(3x + 2)^3 t$
$f_{9,23}$	$f_{9,26}(x, -(43923t^2 + 18225)/(3t^2 + 1))$
$f_{9,22}$	$f_{9,24}(x, 1/(3t^2 + 1))$
$f_{9,21}$	$x^4(x + 1)^2(x + 2)^2(x + 3) - 1/3^5 x^2(9x^2 + 20x + 12)t + 1/3^9 t^2$
$f_{9,20}$	$f_{9,24}(x, 3t^2 + 1)$
$f_{9,19}$	$(f_{10,35}(x, 0)(t - 1)^2 - f_{10,35}(t, 0)(x - 1)^2)/(x - t)$
$f_{9,18}$	$x^6(x + 1)^2(x - 2) + 4/27(3x + 2)^3 t$
$f_{9,17}$	$f_{9,21}(x, 2^5/(3t^2 + 1))$

$f_{9,16}$	$(x^2 + x - 2)^4(x - 4) + 2^4 3^3 x^3 t$
$f_{9,15}$	
$f_{9,14}$	
$f_{9,13}$	$f_{9,18}(x, 1/(3t^2 + 1))$
$f_{9,12}$	$f_{9,18}(x, -t^2)$
$f_{9,11}$	$f_{9,18}(x, 3t^2 + 1)$
$f_{9,10}$	$(x^6 + 3x^4 + 10x^3 + 6x + 25)(x^3 + 3x^2 + 2) + (x - 1)(x + 2) \cdot (x^3 - 3x^2 - 6x - 1) \cdot (x^4 - 7x^3 + 6x^2 - 13x - 14)t/9 + 18t^2$
$f_{9,9}$	$f_{9,16}(x, t^2 + 1)$
$f_{9,8}$	$f_{9,16}(x, t^2)$
$f_{9,7}$	$(x^3 + 27x^2 - 9x - 27)(x^2 + 3)^3 - 27/4(x^2 - 1)^2 x(x^2 - 9)(3t^2 + 49)$
$f_{9,6}$	$f_{9,21}(x, 96(t^2 - 9)^2 t^2 / ((t^4 - 2t^2 + 49)(3t^2 + 1)))$
$f_{9,5}$	$f_{9,16}(x, (t^2 + 1)^2 / (t^2 - 1)^2)$
$f_{9,4}$	$f_{9,16}(x, 1/(3t^2 + 1)^2)$
$f_{9,3}$	$f_{9,10}(x, -(t^3 + 6t^2 + 3t - 1)/(t^3 - 3t - 1))$
$f_{9,2}$	$x^9 - 6(t^2 + 3)x^7 - 6x^6 t + 9(t^4 + 9t^2 + 9)x^5 + 24t(t^2 + 3)x^4 - (4t^6 + 69t^4 + 213t^2 + 81)x^3 - 216t^3 x^2 + 12t^2(3t^4 - 11t^2 + 21)x - 8t^3$
$f_{9,1}$	$x^9 - 27\phi_9(t)x^7 - 54t(t^2 - 1)\phi_9(t)x^6 + 243\phi_9(t)(2t^4 + t^3 - t^2 + 1)x^5 + 243t(t^2 - 1)\phi_9(t) \cdot (4t^4 + 2t^3 - t^2 + t + 3)x^4 - 81(33t^8 + 33t^7 - 26t^6 - 6t^5 + 69t^4 + 16t^3 - 36t^2 - 3t + 10) \cdot \phi_9(t)x^3 - 2187t(t^2 - 1)(2t^8 + 2t^7 - t^6 - t^5 + 4t^4 + 3t^3 - t^2 + 1)\phi_9(t)x^2 + 729(2t^3 + 1)(3t^9 + 9t^8 + 2t^7 - 14t^6 + 17t^4 + t^3 - 9t^2 - t + 1)\phi_9(t)x + 243\phi_9(t)(36t^{13} + 18t^{12} - 60t^{11} + 30t^{10} + 64t^9 - 81t^8 - 9t^7 + 87t^6 - 36t^5 - 54t^4 + 21t^3 + 15t^2 - 3t - 1)$

Table 1.8 Degree 10

$f_{10,43}$	$x^{10} - (5x - 4)^2 t$
$f_{10,42}$	$f_{10,43}(x, 1/(t^2 + 1))$
$f_{10,41}$	$f_{10,43}(x, 1 - t^2)$
$f_{10,40}$	$f_{10,43}(x, -20t^2(5t^2 - 1))$
$f_{10,39}$	$x^{10} - 5^5(x^2 + 4)t$
$f_{10,38}$	$f_{10,39}(x, 1/(t^2 + 1))$
$f_{10,37}$	$(x^2 - 4)^5 - 5^5 x^2 t$
$f_{10,36}$	$f_{10,39}(x, 1 - 5t^2)$
$f_{10,35}$	$x^{10} - 2x^9 + 9x^8 - 729(x - 1)^2 t$
$f_{10,34}$	$f_{10,39}(x, 4(t^2 + t - 1)^2 / (5(t^2 + 1)^2))$
$f_{10,33}$	$(x - 2)^2(x^2 + x - 1)^4 - (380x^6 - 784x^5 + 300x^4 + 360x^3 - 315x^2 + 60x + 4)t + 4(5x - 4)^2 t^2$
$f_{10,32}$	$f_{10,35}(x, t^2)$
$f_{10,31}$	$f_{10,35}(x, 1/(2t^2 + 1))$

$f_{10,30}$	$f_{10,35}(x, 1 - 2t^2)$
$f_{10,29}$	$x^{10} + 10x^6 - 5tx^4 - 15x^2 - t^2 + t - 16$
$f_{10,28}$	$(x - 2)(x - 1)(x^4 + x^3 + 6x^2 - 4x + 1)(x^2 + x - 1)^2 + (4x^5 - 20x^2 + 15x - 2) \cdot (10x^3 - 10x^2 + 1)t + (5x - 4)(8x^5 - 40x^2 + 35x - 8)t^2$
$f_{10,27}$	$f_{10,33}(x, -t/(4(t^2 - 1)))$
$f_{10,26}$	$f_{10,35}(x, (t^2 - 2)^2/(t^2 + 2)^2)$
$f_{10,25}$	$f_{10,39}(x, 2^8t^2/((t^4 + 6t^2 + 25)(t^2 + 1)^4))$
$f_{10,24}$	$f_{10,29}(x, t(t - 8)/(t^2 - 1))$
$f_{10,23}$	$x^2(x^4 - 25)^2 + (x^8 - 20x^6 - 10x^4 + 300x^2 - 95)t - 4(x^2 - 3)^2t^2$
$f_{10,22}$	$x^{10} + 5^5(x^2 + 256)^4t$
$f_{10,21}$	$(x^2 + 9x + 24)^2(x^2 + 4x + 64)^2(x^2 - 6x + 144) - 5^5x^4(x + 8)^2t/4$
$f_{10,20}$	
$f_{10,19}$	$(x^2 + 1)^4(x^2 + 16) - 5(x^7 + 11x^5 - 15x^4 - 5x^3 + 38x^2 - 15x - 7)t + (x^5 + 10x^3 - 15x - 15x^2 + 28)t^2$
$f_{10,18}$	$f_{10,28}(x, t^2)$
$f_{10,17}$	
$f_{10,16}$	$f_{10,23}(x, t^2 - 95/36)$
$f_{10,15}$	$f_{10,23}(x, 95/(t^2 - 36))$
$f_{10,14}$	$f_{10,23}(x, t^2) = f_{5,1}(x^2, t)$
$f_{10,13}$	$(x^2 - 5)^5 - 5^5(x^2 + 5x + 6)^4t/4$
$f_{10,12}$	$f_{10,22}(x, 1/(1 - t^2))$
$f_{10,11}$	$f_{10,22}(x, 1 - 5t^2)$
$f_{10,10}$	$f_{10,21}(x, 4(3t^2 + 32)/(4t^2 + 1))$
$f_{10,9}$	$f_{10,21}(x, -4(5t^2 - 32))$
$f_{10,8}$	$f_{10,23}(x, (7t^2 - 24t + 7)^2/(36(t^2 - 1)^2))$
$f_{10,7}$	$f_{10,13}(x, 1 - 5t^2)$
$f_{10,6}$	$f_{10,19}(x, -4/(5t^4 + 5t^2 + 1))$
$f_{10,5}$	$f_{10,22}(x, -4t^5(t - 10)/(5^5(t^2 + 2t + 5)))$
$f_{10,4}$	$f_{10,13}(x, -4t^5(t - 10)/(5^5(t^2 + 2t + 5)))$
$f_{10,3}$	$f_{10,22}(x, -(11t^2 + 4t - 11)(t^2 + 4t - 1)^5/(5^5(t^2 + 1)^2(t^2 - 1)^4))$
$f_{10,2}$	$x^{10} - 2(t^2 - 125)x^8 + (t^2 - 125)(t^2 - 4t - 65)x^6 - 4(t^2 - 125)^2(t - 10)x^4 + 4(t^2 - 14t + 25)(t^2 - 125)^2x^2 - 64(2t - 25)(t^2 - 125)^2$
$f_{10,1}$	$x^{10} - 20\phi_{10}(t)x^8 + 10(7t^4 - 7t^3 + 17t^2 - 17t + 12)\phi_{10}(t)x^6 - 25(4t^8 - 8t^7 + 12t^6 - 16t^5 + 25t^4 - 46t^3 + 67t^2 - 38t + 9)\phi_{10}(t)x^4 + 5\phi_{10}(t)(13t^{12} - 39t^{11} + 18t^{10} + 50t^9 - 125t^8 + 376t^7 - 453t^6 - 214t^5 + 1050t^4 - 1125t^3 + 613t^2 - 164t + 18)x^2 - \phi_{10}(t)(-1 - 3t + 32t^2 - 36t^3 - 10t^4 + 34t^5 - 13t^6 - 8t^7 + 4t^8)^2$

Table 1.9 Degree 11

$f_{11,6}$	$(f_{M_{12}}(x, 0)(2t - 1)^2 - f_{M_{12}}(t, 0)(2x - 1)^2)/(x - t)$
$f_{11,5}$	$x^{11} - 3x^{10} + 7x^9 - 25x^8 + 46x^7 - 36x^6 + 60x^4 - 121x^3 + 140x^2 - 95x + 27 + x^2(x - 1)^3 t$
$f_{11,4}$	
$f_{11,3}$	$x^{11} - 11(t^2 + 11)x^9 + 44(t^2 + 11)^2 x^7 - 77(t^2 + 11)^3 x^5 + 55(t^2 + 11)^4 x^3 - 11(t^2 + 11)^5 x - 2t(t^2 + 11)^5$
$f_{11,2}$	
$f_{11,1}$	$x^{11} - 55\phi_{11}(t)x^9 - 11(30t^5 + 15t^4 - 30t^3 - 25t^2 - 4t + 3)\phi_{11}(t)x^8 - 11(90t^{10} + 90t^9 - 240t^8 - 350t^7 - 229t^6 - 97t^5 + 35t^4 + 13t^3 - 42t^2 - 42t - 75)\phi_{11}(t)x^7 - 11(168t^{15} + 252t^{14} - 840t^{13} - 1750t^{12} - 1218t^{11} - 242t^{10} + 880t^9 + 1265t^8 + 880t^7 + 836t^6 + 572t^5 + 437t^4 + 430t^3 + 224t^2 + 78t - 36)\phi_{11}(t)x^6 - 11(210t^{20} + 420t^{19} - 1680t^{18} - 4550t^{17} - 2723t^{16} + 2118t^{15} + 7971t^{14} + 11976t^{13} + 9282t^{12} + 6555t^{11} + 6523t^{10} + 5466t^9 + 6103t^8 + 4089t^7 - 422t^6 - 2128t^5 - 1887t^4 - 722t^3 + 355t^2 + 508t + 452)\phi_{11}(t)x^5 - 11(180t^{25} + 450t^{24} - 2100t^{23} - 7000t^{22} - 3080t^{21} + 10615t^{20} + 27060t^{19} + 40865t^{18} + 32857t^{17} + 10109t^{16} - 2398t^{15} - 10128t^{14} - 6994t^{13} - 882t^{12} - 14413t^{11} - 33099t^{10} - 42438t^9 - 36861t^8 - 18117t^7 - 550t^6 + 6589t^5 + 2640t^4 - 1063t^3 - 958t^2 - 648t + 117)\phi_{11}(t)x^4 - 11(105t^{30} + 315t^{29} - 1680t^{28} - 6650t^{27} - 1659t^{26} + 20003t^{25} + 44905t^{24} + 64445t^{23} + 44116t^{22} - 34353t^{21} - 102124t^{20} - 135499t^{19} - 138713t^{18} - 92626t^{17} - 79067t^{16} - 119189t^{15} - 147399t^{14} - 166843t^{13} - 136359t^{12} - 38237t^{11} + 44396t^{10} + 74899t^9 + 52267t^8 + 2031t^7 - 22096t^6 - 12051t^5 + 3115t^4 + 7001t^3 + 1543t^2 - 1896t - 1160)\phi_{11}(t)x^3 - 11(40t^{35} + 140t^{34} - 840t^{33} - 3850t^{32} - 154t^{31} + 19008t^{30} + 39600t^{29} + 49203t^{28} + 14520t^{27} - 120945t^{26} - 280357t^{25} - 348952t^{24} - 314514t^{23} - 145540t^{22} + 29359t^{21} + 33825t^{20} - 27126t^{19} - 75933t^{18} - 85096t^{17} + 57717t^{16} + 276738t^{15} + 420112t^{14} + 438965t^{13} + 296100t^{12} + 50632t^{11} - 97383t^{10} - 69608t^9 + 16104t^8 + 68277t^7 + 54527t^6 - 3025t^5 - 25355t^4 - 7986t^3 + 3117t^2 + 2302t - 84)\phi_{11}(t)x^2 - 11(9t^{40} + 36t^{39} - 240t^{38} - 1250t^{37} + 227t^{36} + 9128t^{35} + 17905t^{34} + 16150t^{33} - 12716t^{32} - 122980t^{31} - 290048t^{30} - 377822t^{29} - 311551t^{28} + 1083t^{27} + 489620t^{26} + 744371t^{25} + 662921t^{24} + 433805t^{23} + 172463t^{22} + 209836t^{21} + 561407t^{20} + 810964t^{19} + 909892t^{18} + 777874t^{17} + 289801t^{16} - 197823t^{15} - 430310t^{14} - 356065t^{13} - 11405t^{12} + 252280t^{11} + 230131t^{10} + 47388t^9 - 93665t^8 - 90187t^7 - 24467t^6 + 19479t^5 + 19576t^4 - 4165t^3 - 5861t^2 + 1587t + 999) \cdot \phi_{11}(t)x - (10t^{45} + 45t^{44} - 330t^{43} - 1925t^{42} + 792t^{41} + 19448t^{40} + 36036t^{39} + 13761t^{38} - 83787t^{37} - 449020t^{36} - 1138951t^{35} - 1569333t^{34} - 1270152t^{33} + 131912t^{32} + 3449677t^{31} + 7101292t^{30} + 8022157t^{29})$

	$\begin{aligned} & +6359584t^{28} + 2562879t^{27} - 1238875t^{26} + 266530t^{25} + 4792381t^{24} \\ & + 7758954t^{23} + 9292575t^{22} + 6341588t^{21} + 107481t^{20} - 3610200t^{19} \\ & - 4999456t^{18} - 3552868t^{17} + 1494614t^{16} + 4899972t^{15} + 3760834t^{14} \\ & + 620191t^{13} - 2831935t^{12} - 4464948t^{11} - 2695792t^{10} - 670956t^9 \\ & - 36608t^8 + 325281t^7 + 187935t^6 + 13585t^5 + 170786t^4 + 81906t^3 \\ & - 42372t^2 - 19548t + 243) \phi_{11}(t) \end{aligned}$
--	---

2 Regular Realizations for Nonsolvable Primitive Groups

Here we collect regular realizations for primitive non-solvable permutation groups of degree d with $12 \leq d \leq 31$. Simple groups in this range for which no polynomial over $\mathbb{Q}(t)$ is known to date are $L_2(16)$, M_{23} , $L_2(25)$ and $L_2(27)$. The polynomials were taken from Häfner (1992), König (2015), Malle (1987, 1988a, 1993a), Malle and Matzat (1985), Matzat (1987), Matzat and Zeh-Marschke (1986) and Müller (2012). We also present surprisingly small polynomials of degree 100 with groups $\text{Aut}(\text{HS})$ and HS taken from Barth and Wenz (2016). A polynomial of degree 266 for the Janko group J_2 has been obtained in Barth and Wenz (2017). In addition we give the polynomial with Galois group Z_{16} from Dentzer (1995a).

Table 2.1 Primitive groups

M_{12}	$x^{12} + 44x^{11} + 754x^{10} + 6060x^9 + 18870x^8 - 28356x^7 - 272184x^6 - 57864x^5 + 1574445x^4 - 92960x^3 - 1214416x^2 + 1216456x - 304119 - 492075(2x - 1)^2 t$
$\text{PGL}_2(11)$	$(x^3 - 66x - 308)^4 - 9t(11x^5 - 44x^4 - 1573x^3 + 1892x^2 + 57358x + 103763) - 3t^2(x - 11)$
$L_2(11)$	$f_{\text{PGL}_2(11)}(x, 2^8 3^5 / (11t^2 + 1))$
$L_3(3)$	$(x^6 - 6x^4 + 64x^3 - 36x^2 + 216)(x^4 + 8x^3 - 108x^2 + 432x - 540) \cdot (x^3 - 18x^2 + 54x - 108) - (3x^4 - 28x^3 + 108x^2 - 216x + 108)^2 \cdot (x^4 + 8x^3 + 108)t$
$\text{PGL}_2(13)$	$(x^3 - x^2 + 35x - 27)^4(x^2 + 36) - 4(x^2 + 39)^6(7x^2 - 2x + 247)t/27$
$L_2(13)$	$f_{\text{PGL}_2(13)}(x, 1/(39t^2 + 1))$
$\text{PGL}_2(17)$	$(x^3 - 7x^2 + 5x - 2)^6 - (x^{17} - 17x^{15} + 34x^{14} + 85x^{13} - 408x^{12} + 289x^{11} + 1190x^{10} - 2907x^9 + 1462x^8 + 3281x^7 - 5780x^6 + 3196x^5 + 238x^4 - 646x^3 - 68x^2 + 120x - 16)t + t^2$
$L_2(17)$	$f_{\text{PGL}_2(17)}(x, 2^2 3^3 17 / (t^2 - 17))$
$\text{PGL}_2(19)$	$(x^5 + 26x^4 + 69x^3 + 108x^2 + 68x + 16)^4 - (x^{19} - 38x^{17} - 38x^{16} + 513x^{15} + 1064x^{14} - 2299x^{13} - 9538x^{12} - 5358x^{11} + 24358x^{10} + 55081x^9 + 35416x^8 - 40204x^7 - 105374x^6 - 98496x^5 - 41040x^4 + 3648x^3 + 11552x^2 + 4352x + 512)t + t^2$
$L_2(19)$	$f_{\text{PGL}_2(19)}(x, 2^8 19 / (t^2 + 19))$
$\text{P}\Gamma\text{L}_3(4)$	$(x^3 - 9x^2 - 21x + 5)^5(x + 1)^5x - t(20x^5 + 89x^4 + 68x^3 - 50x^2 + 16x + 1)^3 \cdot (x^5 + 57x^4 + 330x^3 + 914x^2 + 1509x + 1125)$
$L_3(4).3$	see König (2015)
$L_3(4).2_2$	$(f_{\text{Aut}(M_{22})}(x, 0)(t^2 - t + 3)^{11} - (f_{\text{Aut}(M_{22})}(t, 0)(x^2 - x + 3)^{11}) / (t - x)$
$L_3(4)$	see König (2015)

$\text{Aut}(\text{M}_{22})$	$(5x^4 + 34x^3 - 119x^2 + 212x - 164)^4(19x^3 - 12x^2 + 28x + 32)^2 - 2^{22}(x^2 - x + 3)^{11}t$
M_{22}	$f_{\text{Aut}(\text{M}_{22})}(x, 1/(11t^2 + 1))$
M_{24}	$4(48x^{10} - 192x^9 - 256x^8 + 1104x^7 + 520x^6 - 1276x^5 - 64x^4 - 776x^3 - 1117x^2 + 391x + 52)^2(x^2 + 1) + (16x^{12} - 96x^{11} - 144x^{10} + 928x^9 + 520x^8 - 1744x^7 - 1008x^6 - 1712x^5 - 791x^4 + 2154x^3 + 1121x^2 + 1098x - t)^2$
$\text{PGL}_2(23)$	$(x^8 + 3x^7 + 37x^6 - 24x^5 + 121x^4 + 333x^3 + 429x^2 + 216x + 36)^3 - (2x^{24} + x^{23} - 322x^{22} + 1219x^{21} + 1863x^{20} + 4094x^{19} + 99084x^{18} + 197501x^{17} + 877910x^{16} + 1337726x^{15} + 3132117x^{14} + 8697795x^{13} + 15394935x^{12} + 16590866x^{11} + 4182642x^{10} + 6982731x^9 + 36934642x^8 + 43085601x^7 + 13510591x^6 - 9423054x^5 - 10152936x^4 - 4024080x^3 - 824688x^2 - 85536x - 3456)t + (x^{24} - 7x^{23} + 69x^{22} - 460x^{21} - 1564x^{20} - 3289x^{19} + 11017x^{18} + 19159x^{17} - 20792x^{16} - 269307x^{15} - 650440x^{14} - 547124x^{13} + 609937x^{12} + 2106294x^{11} + 2682306x^{10} + 1410682x^9 - 856612x^8 - 1557215x^7 - 609132x^6 + 135079x^5 + 225814x^4 + 113436x^3 + 33764x^2 + 5904x + 496)t^2 - (x^{23} + 23x^{20} + 23x^{19} + 23x^{18} + 161x^{17} + 368x^{16} + 529x^{15} + 575x^{14} + 1610x^{13} + 3036x^{12} + 2668x^{11} + 2300x^{10} + 3542x^9 + 5428x^8 + 2599x^7 - 1748x^6 - 1265x^5 + 345x^4 - 598x^2 - 252x - 16)t^3 + t^4$
$\text{L}_2(23)$	$f_{\text{PGL}_2(23)}(x, (23 - 3^3t^2)/(t^2 + 23))$
$\text{U}_4(2).2$	$(x^3 + 6x^2 - 8)^9 - 2^4 3^{12} x^6 (x^2 + 5x + 4)^4 (x - 2) t$
$\text{U}_4(2)$	$(x^3 + 6x^2 - 8)^9 - 2^4 3^{12} x^6 (x^2 + 5x + 4)^4 (x - 2) (3t^2 + 1)$
$\text{S}_6(2)$	$(x^4 - 10x^2 - 8x + 1)^7 - x^3(x^2 + 3x + 1)^5 t$
$\text{U}_3(3).2$	$(x^6 - 6x^5 - 435x^4 - 308x^3 + 15x^2 + 66x + 19)^4(x^4 + 20x^3 + 114x^2 + 68x + 13) - 2^2 3^9(x^2 + 4x + 1)^{12}(2x + 1)t$
$\text{U}_3(3)$	$f_{\text{U}_3(3).2}(x, 1/(t^2 + 1))$
$\text{PGL}_2(29)$	$(x^5 - 7x^4 + 8x^3 - 17x^2 + 9x - 6)^6 - t(x^{29} + 29x^{26} - 29x^{25} + 29x^{24} + 290x^{23} - 638x^{22} + 899x^{21} + 464x^{20} - 4118x^{19} + 8323x^{18} - 9686x^{17} - 899x^{16} + 20532x^{15} - 46197x^{14} + 55477x^{13} - 36801x^{12} - 8584x^{11} + 66874x^{10} - 100601x^9 + 105560x^8 - 73602x^7 + 34017x^6 - 2349x^5 - 11745x^4 + 10962x^3 - 6264x^2 + 1944x - 432) + t^2$
$\text{L}_2(29)$	$f_{\text{PGL}_2(29)}(x, 2^2 3^3 29/(t^2 - 29))$
$\text{PSL}_5(2)$	$(x^5 - 95x^4 - 110x^3 - 150x^2 - 75x - 3)^3(x^5 + 4x^4 - 38x^3 + 56x^2 + 53x - 4)^3(x - 3) - 3^4 t(x^2 - 6x - 1)^8(x^2 - x - 1)^4(x + 2)^4 x$
$\text{Aut}(\text{HS})$	$(x^4 - 5)^5(x^8 - 20x^6 + 60x^5 - 70x^4 + 100x^2 - 100x + 25)^{10} - t(7x^5 - 30x^4 + 30x^3 + 40x^2 - 95x + 50)^4(2x^{10} - 20x^9 + 90x^8 - 240x^7 + 435x^6 - 550x^5 + 425x^4 - 100x^3 - 175x^2 + 250x - 125)^4(2x^{10} + 5x^8 - 40x^6 + 50x^4 - 50x^2 + 125)^4$
HS	$f_{\text{Aut}(\text{HS})}(x, (5t^2 + 1)/2^8)$

Table 2.2 The cyclic group Z_{16}

Z_{16}	$\begin{aligned} & x^{16} - 2^4 \phi_{16}(t) x^{14} + 2^4 (16t^6 - 14t^4 + 6t^2 + 5) \phi_{16}(t) x^{12} \\ & - 2^6 (24t^{12} - 28t^{10} + 6t^8 + 36t^6 - 31t^4 + 13t^2 + 2) \phi_{16}(t) x^{10} \\ & + 2^5 (128t^{18} - 120t^{16} - 144t^{14} + 560t^{12} - 488t^{10} + 144t^8 + 164t^6 \\ & - 136t^4 + 56t^2 + 1) \phi_{16}(t) x^8 \\ & - 2^8 (16t^{22} + 16t^{20} - 120t^{18} + 208t^{16} - 108t^{14} - 64t^{12} + 164t^{10} \\ & - 128t^8 + 73t^6 - 20t^4 + 3t^2 + 2) t^2 \phi_{16}(t) x^6 \\ & + 2^8 (64t^{24} - 192t^{22} + 208t^{20} + 80t^{18} - 432t^{16} \\ & + 520t^{14} - 316t^{12} + 112t^{10} + 18t^8 - 66t^6 + 67t^4 - 26t^2 + 5) t^4 \phi_{16}(t) x^4 \\ & - 2^{10} (32t^{22} - 112t^{20} + 160t^{18} - 72t^{16} - 84t^{14} + 144t^{12} - 86t^{10} + 28t^8 \\ & - 17t^6 + 17t^4 - 7t^2 + 1) t^6 \phi_{16}(t) x^2 \\ & + 2^8 (8t^{10} - 16t^8 + 12t^6 - 4t^2 + 1) t^8 \phi_{16}(t) \end{aligned}$
----------	--

3 Realizations over \mathbb{Q} for Transitive Groups of Degree up to 14

This last set of tables contains polynomials generating field extensions of \mathbb{Q} with transitive Galois group of degree less than fifteen. The polynomials are mainly taken from the database Klüners and Malle (2002), which contains polynomials for all but two transitive groups up to degree 23; see also Klüners and Malle (2000).

Table 3.1 Degree 2

T_1	T_2	$x^2 + x + 1$
-------	-------	---------------

Table 3.2 Degree 3

T_2	S_3	$x^3 - x - 1$
T_1	T_3	$x^3 - x^2 - 2x + 1$

Table 3.3 Degree 4

T_5	S_4	$x^4 - x + 1$
T_4	A_4	$x^4 - 2x^3 + 2x^2 + 2$
T_3	D_4	$x^4 - x^3 - x^2 + x + 1$
T_2	V_4	$x^4 - x^2 + 1$
T_1	T_4	$x^4 + x^3 + x^2 + x + 1$

Table 3.4 Degree 5

T_5	S_5	$x^5 - x^3 - x^2 + x + 1$
T_4	A_5	$x^5 + x^4 - 2x^2 - 2x - 2$
T_3	F_{20}	$x^5 + x^4 + 2x^3 + 4x^2 + x + 1$
T_2	D_5	$x^5 - x^3 - 2x^2 - 2x - 1$
T_1	T_5	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$

Table 3.5 Degree 6

T_{16}	S_6	$x^6 - x^4 - x^3 + x + 1$
T_{15}	A_6	$x^6 - x^3 - 3x^2 - 1$
T_{14}	$\text{PGL}_2(5)$	$x^6 - 2x^5 + 4x + 2$
T_{13}	$3^2 \cdot D_4$	$x^6 + x^5 - x^2 - x + 1$
T_{12}	$L_2(5)$	$x^6 - 2x^5 - 5x^2 - 2x - 1$
T_{11}	$2 \times S_4$	$x^6 - x^4 + 1$
T_{10}	$3^2 \cdot 4$	$x^6 + x^5 + x^4 + x^3 - 4x^2 + 5$
T_9	$3^2 \cdot 2^2$	$x^6 - x^3 + 2$
T_8	$S_4/4$	$x^6 - x^4 + 2x^2 + 2$
T_7	S_4/V_4	$x^6 - x^2 - 1$
T_6	$2 \times A_4$	$x^6 - 3x^2 + 1$
T_5	$3 \times S_3$	$x^6 - 3x^3 + 3$
T_4	A_4	$x^6 + x^4 - 2x^2 - 1$
T_3	D_6	$x^6 - x^3 - 1$
T_2	S_3	$x^6 + 3$
T_1	6	$x^6 - x^3 + 1$

Table 3.6 Degree 7

T_7	S_7	$x^7 + x^3 - x^2 + 1$
T_6	A_7	$x^7 - 2x^6 + 2x + 2$
T_5	$L_3(2)$	$x^7 - 7x + 3$
T_4	F_{42}	$x^7 - 2$
T_3	F_{21}	$x^7 - 8x^5 - 2x^4 + 16x^3 + 6x^2 - 6x - 2$
T_2	D_7	$x^7 + 7x^3 - 7x^2 + 7x + 1$
T_1	7	$x^7 - x^6 - 12x^5 + 7x^4 + 28x^3 - 14x^2 - 9x - 1$

Table 3.7 Degree 8

T_{50}	S_8	$x^8 + x^4 + x + 1$
T_{49}	A_8	$x^8 - 8x^3 + 10$
T_{48}	$2^3 \cdot L_3(2)$	$x^8 - 2x^7 + 8x - 2$
T_{47}	$S_4 \wr 2$	$x^8 - 5x - 5$
T_{46}		$x^8 - 8x^3 - 8x^2 + 1$
T_{45}		$x^8 - 3x^4 - 2x^2 - 4x - 1$
T_{44}	$2 \wr S_4$	$x^8 - x^2 - 1$
T_{43}	$PGL_2(7)$	$x^8 - x^7 + 7x^6 - 4x + 4$
T_{42}	$A_4 \wr 2$	$x^8 - 2x^7 + 6x^4 + 4$
T_{41}		$x^8 + 4x^7 - 2x^4 - 4x^2 + 2$
T_{40}		$x^8 + 4x^6 - 9$
T_{39}	$2^3 \cdot S_4$	$x^8 + x^2 + 1$
T_{38}	$2 \wr A_4$	$x^8 + 2x^6 + 2x^4 + 2$
T_{37}	$L_2(7)$	$x^8 - 4x^7 + 7x^6 - 7x^5 + 7x^4 - 7x^3 + 7x^2 + 5x + 1$
T_{36}	$2^3 \cdot 7.3$	$x^8 + x^7 + x^6 - 3x^5 + 5x^4 + 5x^3 - 7x + 9$
T_{35}	$2 \wr 2 \wr 2$	$x^8 + 2x^6 + 2$
T_{34}		$x^8 - x^7 + 2x^6 - x^5 - 2x^4 + 4x^3 - 6x + 4$
T_{33}		$x^8 - 4x^5 + 12x^4 - 8x^2 + 12x + 9$
T_{32}		$x^8 + x^6 + 3x^2 + 4$
T_{31}	$2 \wr 2^2$	$x^8 + 4x^6 - 8x^2 - 1$
T_{30}		$x^8 - 4x^6 + 4x^4 - 2$
T_{29}	$2^3 \cdot D_4$	$x^8 - x^6 + x^2 + 1$
T_{28}		$x^8 + 4x^6 + 2$
T_{27}	$2 \wr 4$	$x^8 - 8x^4 + 8x^2 - 2$
T_{26}		$x^8 + x^4 + 2$
T_{25}	$2^3 \cdot 7$	$x^8 - 4x^7 + 8x^6 - 6x^5 + 2x^4 + 6x^3 - 3x^2 + x + 3$
T_{24}	$S_4 \times 2$	$x^8 - 4x^2 + 4$
T_{23}	$GL_2(3)$	$x^8 - 6x^4 - x^2 - 3$
T_{22}		$x^8 - x^4 + 4$
T_{21}		$x^8 - 2x^6 + x^4 + 5$
T_{20}		$x^8 - 3x^6 - x^4 + 3x^2 + 1$
T_{19}		$x^8 + 4x^4 - 4x^2 + 1$
T_{18}	$2^2 \wr 2$	$x^8 - x^6 + 2x^2 + 1$
T_{17}	$4 \wr 2$	$x^8 - 2x^4 + 2$
T_{16}		$x^8 + 4x^4 + 2$
T_{15}		$x^8 + 3$
T_{14}	S_4	$x^8 + 4x^6 + 4x^2 + 4$
T_{13}	$A_4 \times 2$	$x^8 + 2x^6 + 3x^4 - 3x^2 + 1$

T_{12}	$\text{SL}_2(3)$	$x^8 + 9x^6 + 23x^4 + 14x^2 + 1$
T_{11}		$x^8 + 9$
T_{10}		$x^8 - 2x^6 + 4x^4 - 3x^2 + 1$
T_9	$D_4 \times 2$	$x^8 + 4x^4 + 1$
T_8		$x^8 - 2$
T_7		$x^8 - 15x^4 + 10x^2 + 5$
T_6	D_8	$x^8 + 2$
T_5	Q_4	$x^8 + 12x^6 + 36x^4 + 36x^2 + 9$
T_4	D_4	$x^8 + 3x^4 + 1$
T_3	2^3	$x^8 - x^4 + 1$
T_2	4×2	$x^8 + 1$
T_1	8	$x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1$

Table 3.8 Degree 9

T_{34}	S_9	$x^9 + x^5 - x^2 + 1$
T_{33}	A_9	$x^9 - 3x^3 + x + 2$
T_{32}	$\Gamma\text{L}_2(8)$	$x^9 + x^7 + 2x^5 + 4x^3 - x^2 + x + 1$
T_{31}	$S_3 \wr S_3$	$x^9 - x^8 + 2x^2 - x + 1$
T_{30}		$x^9 + 2x^5 - 4x^4 + 4x^3 - 4x^2 + x - 1$
T_{29}		$x^9 - 3x^6 - 5x^5 + 5x^2 - 1$
T_{28}	$S_3 \wr 3$	$x^9 - 2x^6 - 4x^3 + 3x + 1$
T_{27}	$L_2(8)$	$x^9 + x^7 - 4x^6 - 12x^4 - x^3 - 7x^2 - x - 1$
T_{26}	$3^2 \cdot \text{GL}_2(3)$	$x^9 - x^7 + 5x^6 + x^5 - 2x^4 + 4x^3 + 3x^2 - x - 1$
T_{25}		$x^9 - 3x^6 + 9x^5 - 9x^4 - 27x^3 + 9x + 1$
T_{24}		$x^9 - 2x^6 - 2$
T_{23}	$3^2 \cdot \text{SL}_2(3)$	$x^9 - 3x^8 + x^6 + 15x^5 - 13x^4 - 3x^3 + 4x - 1$
T_{22}		$x^9 - 3x^6 + 3$
T_{21}		$x^9 - 6x^3 - 6$
T_{20}	$3 \wr S_3$	$x^9 - x^6 - 2x^3 + 1$
T_{19}		$x^9 - 3x^8 + 18x^5 + 18x^4 - 27x + 9$
T_{18}		$x^9 - x^3 - 1$
T_{17}	$3 \wr 3$	$x^9 + x^8 - 10x^7 - 14x^6 + 20x^5 + 36x^4 - 18x^2 - 8x - 1$
T_{16}	$3^2 \cdot D_4$	$x^9 - x^8 - x^5 - x^4 + 3x^3 + 2x^2 - 1$
T_{15}	$3^2 \cdot 8$	$x^9 - 4x^8 + 8x^7 - 32x^5 + 80x^4 - 104x^3 + 80x^2 - 34x + 8$
T_{14}	$3^2 \cdot Q_4$	$x^9 - 12x^5 + 132x - 128$
T_{13}		$x^9 - 3x^3 - 1$
T_{12}		$x^9 - 2x^8 + x^5 - 3x^3 + 4x^2 - 12x + 8$
T_{11}	$3^2 \cdot 6$	$x^9 - x^6 + 5x^3 + 1$
T_{10}	9.6	$x^9 - 2$
T_9	$3^2 \cdot 4$	$x^9 + 2x^7 - 3x^6 + x^5 - x^4 + 64x^3 - x - 1$
T_8	S_3^2	$x^9 + 3x^3 - 1$
T_7	$3^2 \cdot 3$	$x^9 - 3x^8 - 21x^7 + 78x^5 + 69x^4 - 21x^3 - 39x^2 - 12x - 1$
T_6	9.3	$x^9 - 14x^7 + 63x^5 - 98x^3 + 42x - 7$
T_5	$3^2 \cdot 2$	$x^9 - 3x^6 - 3x^3 - 1$
T_4	$S_3 \times 3$	$x^9 - 3x^6 - 6x^3 - 1$
T_3	D_9	$x^9 - 9x^6 + 27x^3 - 3$
T_2	3^2	$x^9 - 15x^7 + 4x^6 + 54x^5 - 12x^4 - 38x^3 + 9x^2 + 6x - 1$
T_1	9	$x^9 - 9x^7 + 27x^5 - 30x^3 + 9x - 1$

Table 3.9 Degree 10

T_{45}	S_{10}	$x^{10} - x^3 - 1$
T_{44}	A_{10}	$x^{10} - 2x^9 + 3x^5 - 4$
T_{43}	$S_5 \wr 2$	$x^{10} + 3x^6 - 2x^5 + 1$
T_{42}		$x^{10} + 5x^8 - 5x^7 + 5x^6 - 7x^5 - 5x^4 - 10x^2 - 4$
T_{41}		$x^{10} - 2x^9 - x^6 + x^4 - 4x^2 + 2x - 1$
T_{40}	$A_5 \wr 2$	$x^{10} - x^9 - x^4 - 4x^3 + 4x^2 - x - 1$
T_{39}	$2 \wr S_5$	$x^{10} - x^2 + 1$
T_{38}		$x^{10} - 3x^8 + 2x^2 + 2$
T_{37}	$2^4 \cdot S_5$	$x^{10} - x^2 - 1$
T_{36}	$2 \wr A_5$	$x^{10} + x^4 - 2x^2 + 3$
T_{35}	$\text{PGL}_2(9)$	$x^{10} - 4x^9 + 6x^8 + 12x^2 + 16x + 8$
T_{34}	$2^4 \cdot A_5$	$x^{10} + 4x^4 + x^2 - 4$
T_{33}	$(5.4) \wr 2$	$x^{10} + 6x^6 + 8x^5 - 35x^2 + 24x + 16$
T_{32}	S_6	$x^{10} - 2x^9 + x^8 - 9x^2 + 2x - 1$
T_{31}	M_{10}	$x^{10} - 2x^9 + 9x^8 - 54x^2 + 108x - 54$
T_{30}	$\text{PGL}_2(9)$	$x^{10} - 2x^9 + 9x^8 - 7x^2 + 14x - 7$
T_{29}	$2 \wr (5.4)$	$x^{10} + 10x^6 + 5$
T_{28}		$x^{10} - 10x^7 + 10x^6 + 36x^5 + 50x^4 - 10x^3 - 1$
T_{27}		$x^{10} + 3x^6 - 2x^5 + x^2 + 2x + 1$
T_{26}	$L_2(9)$	$x^{10} - x^9 + 3x^8 - 6x^7 + 3x^6 - 3x^5 - 3x^3 - 6x^2 - 8x - 1$
T_{25}		$x^{10} + 10x^6 - 5$
T_{24}	$2^4 \cdot 5.4$	$x^{10} + 5x^6 + 5x^2 - 1$
T_{23}	$2 \wr (5.2)$	$x^{10} - 5x^4 - 3$
T_{22}	$S_5 \times 2$	$x^{10} + 4x^2 + 4$
T_{21}	$D_5 \wr 2$	$x^{10} + x^6 - 2x^5 - x^4 + 3x^2 - 2x + 1$
T_{20}	$5^2 \cdot Q_4$	$x^{10} - 10x^8 + 35x^6 - 4x^5 - 50x^4 + 20x^3 + 25x^2 - 20x - 17$
T_{19}	$5^2 \cdot D_4$	$x^{10} - 10x^8 + 35x^6 - 2x^5 - 50x^4 + 10x^3 + 25x^2 - 10x + 2$
T_{18}	$5^2 \cdot 8$	$x^{10} + 60x^6 - 208x^5 + 850x^2 - 8000x - 4672$
T_{17}		$x^{10} + x^5 + 2$
T_{16}		$x^{10} - 5x^4 + 15$
T_{15}	$2^4 \cdot 5.2$	$x^{10} - 5x^4 - 4x^2 - 1$
T_{14}	$2 \wr 5$	$x^{10} + x^8 - 4x^6 - 3x^4 + 3x^2 + 1$
T_{13}	S_5 / D_6	$x^{10} - x^9 - x^8 + 3x^6 - x^5 - 2x^4 + 3x^3 - x^2 - x + 1$
T_{12}	S_5 / A_4	$x^{10} + 2x^9 + 3x^8 - x^6 - 2x^5 - x^4 + 3x^2 + 2x + 1$
T_{11}	$A_5 \times 2$	$x^{10} + x^8 - 4x^2 + 4$
T_{10}	$5^2 \cdot 4$	$x^{10} - 2x^5 - 4$
T_9	$5^2 \cdot 2^2$	$x^{10} - x^9 - 5x^8 + 11x^6 + 4x^5 - 10x^4 + 25x^2 + 5x - 5$
T_8	$2^4 \cdot 5$	$x^{10} - 4x^8 + 2x^6 + 5x^4 - 2x^2 - 1$
T_7	A_5	$x^{10} - x^8 - 4x^7 - 3x^6 - 2x^5 + 8x^3 - 2x - 1$
T_6	$5 \wr 2$	$x^{10} - x^9 + 3x^7 - 3x^6 + x^5 + 5x^4 - x^3 + 2x^2 + 3x + 1$
T_5	2×5.4	$x^{10} + 2$
T_4	5.4	$x^{10} - 5$
T_3	D_{10}	$x^{10} - 3x^4 + 2x^2 + 1$
T_2	D_5	$x^{10} + 5x^8 + 15x^6 + 20x^4 + 25x^2 + 15$
T_1	10	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Table 3.10 Degree 11

T_8	S_{11}	$x^{11} + x^6 + x^4 + 1$
T_7	A_{11}	$x^{11} - 6x^8 + 4x^5 - 3x^3 + 2$
T_6	M_{11}	$x^{11} - 4x^{10} + 60x^7 - 108x^6 + 72x^5 - 360x^4 + 3636x - 1944$
T_5	$L_2(11)$	$x^{11} - 2x^{10} + x^9 - 5x^8 + 13x^7 - 9x^6 + x^5 - 8x^4 + 9x^3 - 3x^2 - 2x + 1$
T_4	F_{110}	$x^{11} - 3$
T_3	F_{55}	$x^{11} - 33x^9 + 396x^7 - 2079x^5 + 4455x^3 - 2673x - 243$
T_2	D_{11}	$x^{11} - x^{10} + 5x^8 + 8x^5 + 6x^4 - x^3 + x^2 + 3x + 1$
T_1	11	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6 - 56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$

Table 3.11 Degree 12

S_{12}	$x^{12} - x + 1$
A_{12}	$x^{12} + 3x^8 + 3x^4 + 4x^3 + 4$
T_{299}	$x^{12} + x^2 - 2x + 1$
T_{298}	$x^{12} - 72x^2 - 120x - 50$
T_{297}	$x^{12} - 2x^7 + 7x^6 + x^2 - 2x + 1$
T_{296}	$x^{12} - x^7 - 7x^6 - 5x^4 - x^2 + x + 1$
M_{12}	$x^{12} - 375x^8 - 3750x^6 - 75000x^3 + 228750x^2 - 750000x + 1265625$
T_{294}	$x^{12} + 4x^9 - 6x^7 + 2$
T_{293}	$x^{12} - x^6 - x^2 - 1$
T_{292}	$x^{12} - 3x^{11} + 5x^9 - 3x^8 + 3x^7 + 2x^6 - 6x^5 - 3x^4 + 1$
T_{291}	$x^{12} - 12x^9 - 9x^8 - 64x^3 - 144x^2 - 108x - 27$
T_{290}	$x^{12} + 3x^{10} - x^9 + 2x^6 - 3x^5 + 9x^4 - 3x^3 + 3x + 1$
T_{289}	$x^{12} - 4x^9 + 2x^6 + 4x^4 + 1$
T_{288}	$x^{12} - 4x^{11} + 4x^{10} - 50x^4 + 120x^3 - 112x^2 + 48x - 8$
T_{287}	$x^{12} - 3x^8 + 2x^6 + 3$
T_{286}	$x^{12} - x^6 - 3x^4 - 1$
T_{285}	$x^{12} - 4x^2 + 4$
T_{284}	$x^{12} - 12x^9 - 9x^8 + 64x^3 + 144x^2 + 108x + 27$
T_{283}	$x^{12} - 8x^9 + 24x^6 + 144x^5 + 96x^3 + 144x^2 + 48$
T_{282}	$x^{12} - x^{11} + 3x^{10} - x^9 + 6x^8 + 6x^6 - 2x^5 + 7x^4 + 4x^3 + 4x^2 + x + 1$
T_{281}	$x^{12} - x^{11} + x^{10} - 2x^8 + 3x^7 - 3x^5 + 3x^4 - 2x^3 + 3x^2 - x + 1$
T_{280}	$x^{12} - 4x^{11} + 6x^{10} - 2x^9 - 5x^8 + 6x^7 - 4x^5 + 2x^4 + 2$
T_{279}	$x^{12} - 4x^{11} + 4x^{10} + 4x^7 - 6x^6 - 4x^5 + 36x^2 + 36x + 9$
T_{278}	$x^{12} + 20x^8 - 80x^6 + 50x^4 - 320x^3 - 912x^2 + 1280x + 800$
T_{277}	$x^{12} + 3x^6 + 3x^2 + 4$
T_{276}	$x^{12} + 192x^6 - 288x^5 + 108x^4 + 256x^3 - 576x^2 + 432x - 108$
T_{275}	$x^{12} + x^{10} - 9x^9 + 11x^8 - 11x^7 + 17x^6 - 7x^5 + 2x^4 + x + 1$
T_{274}	$x^{12} - x^8 + 2x^6 - 4x^3 + 1$
T_{273}	$x^{12} - 12x^9 + 9x^8 + 192x^3 - 432x^2 + 324x - 81$
M_{11}	$x^{12} + 6x^{11} + 15x^{10} + 28x^9 + 36x^8 + 6x^7 - 75x^6 - 108x^5 + 18x^4 + 82x^3 + 3x^2 - 6x + 5$
T_{271}	$x^{12} - 135x^8 - 180x^7 + 399x^6 + 918x^5 + 693x^4 + 352x^3 + 216x^2 + 96x + 16$
T_{270}	$x^{12} + x^{10} + 4x^2 - 1$
T_{269}	$x^{12} - 2x^{10} - 6x^8 + 14x^6 + x^4 - 8x^3 + 1$
T_{268}	$x^{12} + 4x^9 - 3x^8 - 64x^3 + 144x^2 - 108x + 27$

T_{267}	$x^{12} + 12x^{10} - 8x^9 + 54x^8 - 48x^7 + 132x^6 - 72x^5 - 33x^4 - 32x^3 + 8$
T_{266}	$x^{12} + x^{10} - 4x^9 - 2x^8 - 3x^7 + 4x^5 + 2x^3 - 2x^2 - x + 1$
T_{265}	$x^{12} - 8x^{10} + 7x^9 + 8x^8 - 7x^7 - 15x^6 + 21x^5 + 8x^4 - 14x^3 - 8x^2 + 7x + 1$
T_{264}	$x^{12} - 4x^{11} + 6x^{10} - 3x^9 - 2x^8 + 3x^7 - 2x^5 + x^4 + x^3 - x^2 + 1$
T_{263}	$x^{12} - 162x^4 - 432x^3 - 432x^2 - 192x - 32$
T_{262}	$x^{12} + 18x^8 - 24x^7 + 8x^6 - 81x^4 + 216x^3 - 216x^2 + 96x - 16$
T_{261}	$x^{12} + 2x^6 - 4x^5 + x^4 + 1$
T_{260}	$x^{12} - 3x^2 + 3$
T_{259}	$x^{12} - 12x^{10} + 54x^8 - 110x^6 + 93x^4 - 4x^3 - 18x^2 + 12x - 8$
T_{258}	$x^{12} - x^3 - 3$
T_{257}	$x^{12} + 4x^{10} - 4x^2 + 4$
T_{256}	$x^{12} + 4x^{10} - 5x^2 + 5$
T_{255}	$x^{12} - 2x^8 - 6x^6 + 9x^4 - 1$
T_{254}	$x^{12} + 6x^{10} - 12x^9 - 54x^7 + 24x^6 + 180x^4 + 156x^3 + 216x^2 + 72x + 18$
T_{253}	$x^{12} - 4x^9 - 3x^8 - 32x^6 - 48x^5 - 18x^4 + 64x^3 + 144x^2 + 108x + 27$
T_{252}	$x^{12} - 12x^9 + 27x^8 + 12x^6 - 36x^5 + 27x^4 - 16x^3 + 36x^2 + 9$
T_{251}	$x^{12} + 48x^6 - 72x^5 + 27x^4 + 64x^3 - 144x^2 + 108x - 27$
T_{250}	$x^{12} + 3x^2 + 5$
T_{249}	$x^{12} - 12x^{10} + 54x^8 - 108x^6 + 81x^4 - 8x^3 + 24x + 8$
T_{248}	$x^{12} + 324x^6 - 648x^5 + 675x^4 - 744x^3 + 648x^2 - 288x + 48$
T_{247}	$x^{12} - 8x^9 + 24x^6 + 162x^4 - 32x^3 + 16$
T_{246}	$x^{12} + 81x^4 - 216x^3 + 216x^2 - 96x + 16$
T_{245}	$x^{12} - 12x^{10} - 54x^8 - 72x^7 + 96x^6 + 9x^4 + 200x^3 + 108x^2 - 4$
T_{244}	$x^{12} - 3x^{11} - 6x^{10} + 13x^9 + 6x^8 - 15x^7 + 5x^6 - 15x^5 + 15x^4 + 5x^3 - 5$
T_{243}	$x^{12} - 9x^8 - 12x^7 - 4x^6 - 81x^4 - 216x^3 - 216x^2 - 96x - 16$
T_{242}	$x^{12} - 4x^9 + 18x^8 - 4x^6 - 36x^5 + 81x^4 + 16x^3 + 108x^2 + 16$
T_{241}	$x^{12} + x^{10} - 3x^8 - x^6 + 6x^4 - 3$
T_{240}	$x^{12} + 6x^8 + 4x^6 - 4$
T_{239}	$x^{12} - 12x^9 + 9x^8 - 32x^6 + 48x^5 - 18x^4 - 64x^3 + 144x^2 - 108x + 27$
T_{238}	$x^{12} + 6x^{10} + 9x^8 - 8$
T_{237}	$x^{12} + 10x^2 + 5$
T_{236}	$x^{12} + x^4 + 2x^2 + 1$
T_{235}	$x^{12} + 3x^8 - 4x^6 + 2$
T_{234}	$x^{12} + x^9 + 3x^3 + 4$
T_{233}	$x^{12} - 4x^3 - 6$
T_{232}	$x^{12} - 13x^8 - 26x^7 - 11x^6 + 6x^5 + 25x^4 + 78x^3 + 114x^2 + 76x + 19$
T_{231}	$x^{12} - x^{11} + 2x^9 - x^8 - 4x^7 + 5x^6 - x^5 - x^4 - x^3 + 4x^2 - 3x + 1$
T_{230}	$x^{12} + x^{10} - 3x^8 + 4x^4 + 1$
T_{229}	$x^{12} - 18x^{10} - 22x^9 + 102x^8 + 180x^7 - 96x^6 - 90x^5 + 81x^4 - 30x^3 - 54x^2 + 3$
T_{228}	$x^{12} + 4x^{11} + 3x^{10} - 2x^9 + 11x^8 + 30x^7 + 14x^6 - 11x^5 + 12x^4 + 30x^3 + x^2 - 9x - 1$
T_{227}	$x^{12} + 2x^{10} + x^8 - 4x^4 + 3$
T_{226}	$x^{12} - 3x^8 - 6x^2 + 1$
T_{225}	$x^{12} - 3x^{10} + 2x^6 + 2x^4 - 3$
T_{224}	$x^{12} + 4x^8 + 6x^6 - 6x^2 + 2$
T_{223}	$x^{12} - 6x^{10} + 12x^6 - 9$
T_{222}	$x^{12} - 4x^6 + 3x^2 - 1$
T_{221}	$x^{12} - 2x^{10} - x^8 + 6x^6 - x^4 - 4x^2 - 1$

T_{220}	$x^{12} - 4x^9 - 12x^8 + 34x^6 - 12x^5 + 45x^4 + 42x^2 + 10$
T_{219}	$x^{12} + 2x^6 + x^2 + 1$
T_{218}	$x^{12} - 2x^{11} + 22x^9 - 88x^7 + 176x^5 - 176x^3 + 64x + 4$
T_{217}	$x^{12} - 4x^9 + 2$
T_{216}	$x^{12} - 12x^{10} - 8x^9 + 162x^4 + 432x^3 + 432x^2 + 192x + 32$
T_{215}	$x^{12} - 3x^{10} + x^9 - 81x^8 + 54x^7 - 36x^6 + 27x^5 + 72x^4 - 107x^3 + 54x^2 - 12x + 1$
T_{214}	$x^{12} - 12x^9 + 18x^8 - 56x^6 + 138x^4 - 96x^3 + 72x^2 + 72$
T_{213}	$x^{12} - x^3 - 1$
T_{212}	$x^{12} - 12x^{10} - 18x^8 - 96x^7 - 132x^6 - 63x^4 - 64x^3 + 72x^2 - 16$
T_{211}	$x^{12} + 90x^8 + 120x^7 + 40x^6 + 405x^4 + 1080x^3 + 1080x^2 + 480x + 80$
T_{210}	$x^{12} - 4x^9 + 8x^6 - 36x^5 + 105x^4 - 120x^3 + 90x^2 - 36x + 9$
T_{209}	$x^{12} - 8x^9 + 18x^8 - 24x^7 + 24x^6 - 33x^4 - 16x^3 - 48x - 8$
T_{208}	$x^{12} - 3x^{10} + 3x^6 + 3x^4 + 3$
T_{207}	$x^{12} - x^{11} + x^9 - x^7 - x^6 + 2x^5 - x^4 - 3x^3 + 3x^2 - 2x + 1$
T_{206}	$x^{12} - 12x^9 + 15x^8 - 12x^5 + 18x^4 - 64x^3 + 96x^2 - 36x + 9$
T_{205}	$x^{12} - 208x^6 - 312x^5 - 117x^4 - 832x^3 - 1872x^2 - 1404x - 351$
T_{204}	$x^{12} - 6x^9 + 18x^8 + 48x^6 + 108x^4 - 32x^3 - 72x + 24$
T_{203}	$x^{12} - 2x^6 + x^4 + 1$
T_{202}	$x^{12} - 4x^6 + 9x^4 + 4$
T_{201}	$x^{12} + 3x^{10} - 12x^2 + 24$
T_{200}	$x^{12} + 6x^{10} + 9x^8 - 12$
T_{199}	$x^{12} - 2x^{10} - 4x^8 - x^6 + x^4 + 4$
T_{198}	$x^{12} - 2x^{10} - x^8 + 6x^4 - 4x^2 + 2$
T_{197}	$x^{12} + 4x^6 - 9x^4 + 8$
T_{196}	$x^{12} - 2x^8 - 4x^6 + 6x^4 + 4x^2 - 1$
T_{195}	$x^{12} + 4x^{10} + 2x^8 - 4x^6 + 4$
T_{194}	$x^{12} + 2x^{10} + 2x^9 - x^8 - 2x^7 + 4x^6 - 12x^5 + 6x^4 + 2x^3 + 18x^2 + 27$
T_{193}	$x^{12} + 6x^6 + 6x^4 + 3$
T_{192}	$x^{12} - 6x^{10} + x^8 + 36x^6 - 30x^4 - 28x^2 + 18$
T_{191}	$x^{12} + x^{10} + 2x^8 - x^6 + 2x^4 - 3x^2 + 1$
T_{190}	$x^{12} + 2x^{10} - 13x^8 + 36x^6 + 15x^4 - 38x^2 - 19$
T_{189}	$x^{12} - 6x^8 + 12x^4 + 13x^2 + 5$
T_{188}	$x^{12} - 2x^{10} + 5x^6 + 5x^2 - 1$
T_{187}	$x^{12} + 8x^6 - 9x^2 + 1$
T_{186}	$x^{12} - x^{10} - x^2 - 1$
T_{185}	$x^{12} - x^4 - 2$
T_{184}	$x^{12} + x^8 + 9x^6 + 9x^4 + 7x^2 + 1$
T_{183}	$x^{12} - 7x^6 - 10x^4 - 5x^2 + 1$
T_{182}	$x^{12} - 8x^9 + 6x^8 + 20x^6 - 24x^5 + 18x^4 - 16x^3 + 24x^2 + 8$
T_{181}	$x^{12} - 18x^8 - 36x^6 - 72x^5 + 54x^4 - 144x^3 - 216x^2 - 72$
T_{180}	$x^{12} - 2x^{10} + 5x^8 - 8x^6 + 6x^4 - 4x^2 + 1$
$L_2(11)$	$x^{12} + x^{11} - 8x^{10} - 29x^9 + 48x^8 + 51x^7 - 5x^6 + 275x^5 + 642x^4 + 208x^3 + 308x^2 + 41x + 2$
T_{178}	$x^{12} - x^9 + 4x^3 - 1$
T_{177}	$x^{12} - 4x^9 + 4x^3 + 2$
T_{176}	$x^{12} + 4x^6 - 8x^3 + 8$
T_{175}	$x^{12} - 2x^{11} + 4x^{10} - 2x^9 + 4x^7 - 3x^6 + 2x^5 + x^2 - 2x + 1$
T_{174}	$x^{12} + 12x^{10} + 54x^8 + 20x^6 - 447x^4 - 384x^3 - 792x^2 - 1152x - 368$

T_{173}	$x^{12} - 36x^8 - 48x^7 - 32x^6 + 162x^4 - 288x^2 + 128$
T_{172}	$x^{12} + 12x^{10} - 6x^9 - 54x^7 - 157x^6 + 210x^4 + 174x^3 + 234x^2 + 252x + 118$
T_{171}	$x^{12} - 8x^9 - 36x^8 - 72x^5 + 81x^4 + 64x^3 - 144x^2 + 64$
T_{170}	$x^{12} - x^9 + 2x^6 + 4x^3 + 3$
T_{169}	$x^{12} - 8x^3 + 18$
T_{168}	$x^{12} - 10x^6 - 12x^3 - 2$
T_{167}	$x^{12} - 3x^3 + 3$
T_{166}	$x^{12} + 18x^{10} + 135x^8 + 348x^6 + 63x^4 - 512x^3 - 270x^2 + 729$
T_{165}	$x^{12} - 16x^9 + 12x^8 + 256x^3 - 576x^2 + 432x - 108$
T_{164}	$x^{12} + 4x^9 + 6x^7 + 8x^6 - 54x^5 + 88x^3 - 57x^2 - 90x + 111$
T_{163}	$x^{12} - x^8 - 2x^6 + x^4 - 2x^2 + 1$
T_{162}	$x^{12} - 2x^8 - 8x^6 + 14x^4 - 16x^2 + 4$
T_{161}	$x^{12} + 3x^{10} + 18x^2 + 9$
T_{160}	$x^{12} + x^{10} + x^8 + x^6 - 4x^4 + 5$
T_{159}	$x^{12} + 4x^{10} - 4x^8 - 24x^6 - x^4 + 32x^2 + 8$
T_{158}	$x^{12} - x^8 - 2x^6 + 2x^2 + 1$
T_{157}	$x^{12} - 8x^9 + 24x^7 + 44x^6 - 51x^4 + 48x^3 - 72x^2 + 16$
T_{156}	$x^{12} - 2x^9 + 2$
T_{155}	$x^{12} - 2x^{10} - 3x^8 + 2$
T_{154}	$x^{12} - 2x^6 + 12x^4 - 6x^2 + 7$
T_{153}	$x^{12} + 2x^{10} + 8x^2 + 8$
T_{152}	$x^{12} - 4x^8 - 2x^6 + 4x^4 - 1$
T_{151}	$x^{12} - 3x^8 - 2$
T_{150}	$x^{12} - x^6 - 3x^4 + 2x^2 + 2$
T_{149}	$x^{12} - 9x^4 - 6$
T_{148}	$x^{12} + 3x^{10} + 3x^8 + x^6 - 3$
T_{147}	$x^{12} - 3x^8 - 8$
T_{146}	$x^{12} - 2x^{10} - x^8 - 2x^6 - 2x^4 - 8x^2 + 8$
T_{145}	$x^{12} + 6x^8 + 4x^6 - 18x^4 - 24x^2 - 8$
T_{144}	$x^{12} + 6x^{10} + 4x^8 - 24x^6 - 21x^4 + 22x^2 + 4$
T_{143}	$x^{12} - 6x^{10} + 24x^8 - 56x^6 + 93x^4 - 90x^2 + 51$
T_{142}	$x^{12} + 3x^8 + 4x^6 + 6x^4 + 3$
T_{141}	$x^{12} + 3x^8 - 3$
T_{140}	$x^{12} - x^4 - 4$
T_{139}	$x^{12} + 3x^{10} + 3x^2 + 1$
T_{138}	$x^{12} - x^4 + 1$
T_{137}	$x^{12} + x^8 - 2x^6 - x^4 - 1$
T_{136}	$x^{12} - x^{10} + 4x^2 + 1$
T_{135}	$x^{12} - 18x^8 - 24x^6 + 27x^4 + 36x^2 - 6$
T_{134}	$x^{12} - 7x^{10} + 14x^8 - 21x^4 + 7x^2 + 7$
T_{133}	$x^{12} - 8x^9 + 162x^8 - 372x^7 + 20x^6 + 432x^5 - 63x^4 - 212x^3 - 36x^2 + 24x + 56$
T_{132}	$x^{12} - x^{10} - 11x^9 + 99x^8 - 45x^7 - 117x^6 - 27x^5 + 90x^4 + 36x^3 + 9x + 18$
T_{131}	$x^{12} - 2x^{11} - x^{10} + 9x^9 - 7x^8 - 11x^7 + 20x^6 + x^5 - 19x^4 + 8x^3 + 6x^2 - 5x + 1$
T_{130}	$x^{12} - 2x^9 + x^6 + 6x^3 + 3$
T_{129}	$x^{12} - 6x^{10} - 2x^9 + 3x^8 - 30x^7 + 8x^6 + 90x^5 + 36x^4 - 24x^3 + 6x - 1$
T_{128}	$x^{12} - 12x^{10} - 22x^9 + 57x^8 - 72x^6 + 30x^5 + 15x^4 - 30x^3 + 6x + 1$
T_{127}	$x^{12} - 16x^9 + 18x^8 - 72x^6 + 36x^5 - 36x^4 - 76x^3 - 72x - 62$
T_{126}	$x^{12} + x^8 + x^6 - 2x^4 - x^2 + 1$

T_{125}	$x^{12} - 2x^8 - 2x^6 + x^4 + 2x^2 - 1$
T_{124}	$x^{12} + 4x^{10} + 10x^6 + 5$
T_{123}	$x^{12} - 2x^{10} + 10x^6 - 8x^2 + 1$
T_{122}	$x^{12} - 2x^{11} - 3x^{10} - 6x^9 + 21x^8 - 32x^7 + 37x^6 - 16x^5 + 11x^4 + 32x^3 - x^2 + 20x + 1$
T_{121}	$x^{12} - x^9 + 2x^3 + 1$
T_{120}	$x^{12} - 2x^9 - 6x^3 + 9$
T_{119}	$x^{12} - 8x^6 - 8x^3 - 2$
T_{118}	$x^{12} + 8x^6 - 8x^3 + 2$
T_{117}	$x^{12} - 2x^9 + x^6 + 5$
T_{116}	$x^{12} - 2x^9 + 4x^3 + 4$
T_{115}	$x^{12} - 2x^8 + 3x^4 - 4$
T_{114}	$x^{12} - x^4 - 1$
T_{113}	$x^{12} - x^4 + 4$
T_{112}	$x^{12} - 3x^8 + 9x^4 + 1$
T_{111}	$x^{12} - 6x^8 + 68x^6 + 105x^4 + 36x^2 + 12$
T_{110}	$x^{12} + x^8 - x^6 - x^4 - 1$
T_{109}	$x^{12} + x^{10} - 4x^2 + 1$
T_{108}	$x^{12} - 3x^8 - 4x^6 + 6x^4 + 4$
T_{107}	$x^{12} + 6x^{10} + 3x^8 - 28x^6 - 21x^4 + 30x^2 + 5$
T_{106}	$x^{12} + 3x^{10} - 2x^8 - 9x^6 + 5x^2 + 1$
T_{105}	$x^{12} - 7x^{10} + 7x^8 + 14x^6 - 16x^4 - 5x^2 + 5$
T_{104}	$x^{12} + 6x^{10} + 12x^8 + 8x^6 - 3x^4 - 6x^2 - 1$
T_{103}	$x^{12} + 3x^{10} - x^6 + 3x^2 + 1$
T_{102}	$x^{12} - 5x^{10} + 20x^8 - 70x^6 + 145x^4 - 280x^2 + 208$
T_{101}	$x^{12} - 3x^{10} - 3x^2 + 1$
T_{100}	$x^{12} - x^{10} + x^8 + 4x^6 - x^4 - x^2 - 1$
T_{99}	$x^{12} - 76x^8 + 325x^6 - 380x^4 + 125$
T_{98}	$x^{12} - 64x^{10} - 231x^8 + 740x^6 - 481x^4 + 37$
T_{97}	$x^{12} + x^8 + 9x^4 + 1$
T_{96}	$x^{12} - 3x^4 - 4$
T_{95}	$x^{12} - x^{10} + 3x^6 - 2x^4 - 3x^2 + 1$
T_{94}	$x^{12} - 57x^8 - 38x^6 + 318x^4 - 204x^2 + 17$
T_{93}	$x^{12} + 10x^{10} + 28x^8 + 6x^6 - 43x^4 + 6x^2 + 3$
T_{92}	$x^{12} - 9x^4 - 9$
T_{91}	$x^{12} + 5x^{10} + 9x^8 + 8x^6 + 2x^4 - 12x^2 + 16$
T_{90}	$x^{12} + 2x^{10} - x^6 + 2x^2 + 1$
T_{89}	$x^{12} - 3x^4 + 1$
T_{88}	$x^{12} - 6x^8 - 4x^6 - 3x^4 - 18x^2 + 3$
T_{87}	$x^{12} + 6x^{10} + 9x^8 - 4x^6 - 12x^4 + 1$
T_{86}	$x^{12} + 2x^8 - 2$
T_{85}	$x^{12} - 3x^{11} - 3x^{10} + 15x^9 - 15x^8 - 33x^7 + 29x^6 + 15x^5 - 30x^4 - 128x^3 - 30x^2 + 198x + 48$
T_{84}	$x^{12} - 6x^{10} + 4x^9 + 21x^8 - 12x^7 - 52x^6 - 16x^3 + 48x^2 + 16$
T_{83}	$x^{12} + 3x^6 - x^3 + 3$
T_{82}	$x^{12} - 12x^{10} + 54x^8 - 116x^6 + 129x^4 - 72x^2 - 16$
T_{81}	$x^{12} + x^6 + 2$

T_{80}	$x^{12} - 90x^8 + 160x^6 - 135x^4 + 7200x^2 - 80$
T_{79}	$x^{12} + 4x^{10} + 6x^8 + 4x^6 + 2$
T_{78}	$x^{12} - x^9 + x^3 + 1$
T_{77}	$x^{12} - 2x^6 + 5x^2 + 1$
T_{76}	$x^{12} + 2x^8 + 5x^4 + 6x^2 + 1$
T_{75}	$x^{12} + 7x^8 + 7x^4 + 8x^2 + 1$
T_{74}	$x^{12} - x^{10} + 2x^8 + 4x^6 - 3x^4 - 3x^2 + 1$
T_{73}	$x^{12} - 3x^{11} + 4x^{10} - x^8 - 6x^7 + 20x^6 - 10x^5 + 8x^4 + 24x^3 + 3x^2 + 12x + 9$
T_{72}	$x^{12} - 6x^{10} - 10x^9 + 36x^8 - 116x^6 + 720x^5 + 696x^4 - 2440x^3 - 720x^2 + 1200x + 880$
T_{71}	$x^{12} - 4x^9 + 4x^6 + 3$
T_{70}	$x^{12} + 9x^6 - 18x^3 + 9$
T_{69}	$x^{12} - 3x^{10} - 2x^8 + 9x^6 - 5x^2 + 1$
T_{68}	$x^{12} + x^{10} + 6x^8 + 3x^6 + 6x^4 + x^2 + 1$
T_{67}	$x^{12} - x^8 - x^6 - x^4 + 1$
T_{66}	$x^{12} + 6x^{10} + 12x^8 + 8x^6 - 3$
T_{65}	$x^{12} - 3x^4 + 4$
T_{64}	$x^{12} + 3x^8 - 16$
T_{63}	$x^{12} - 6x^{10} + 104x^6 + 93x^4 + 18x^2 + 4$
T_{62}	$x^{12} - 3x^{10} + 3x^8 - x^6 + 4x^4 - 4x^2 + 1$
T_{61}	$x^{12} - 3x^4 - 1$
T_{60}	$x^{12} - 4x^8 - 9x^4 + 4$
T_{59}	$x^{12} - 6x^{10} + 6x^8 - 4x^6 - 3x^4 + 3$
T_{58}	$x^{12} - 12x^8 - 14x^6 + 9x^4 + 12x^2 + 1$
T_{57}	$x^{12} + 38x^{10} + 533x^8 + 3474x^6 + 10574x^4 + 12740x^2 + 4225$
T_{56}	$x^{12} - 2x^{10} + x^6 - 2x^2 + 1$
T_{55}	$x^{12} + 2x^{10} - 97x^8 - 360x^6 - 345x^4 - 50x^2 + 25$
T_{54}	$x^{12} - 6x^8 + 9x^4 + 2$
T_{53}	$x^{12} + 2x^8 - 16x^6 + 4x^4 + 8$
T_{52}	$x^{12} - 3x^4 - 6$
T_{51}	$x^{12} + 6x^8 + 9x^4 + 3$
T_{50}	$x^{12} - 3x^4 + 6$
T_{49}	$x^{12} + 3x^8 - 4x^6 - 3x^4 - 1$
T_{48}	$x^{12} + 8x^4 + 1$
T_{47}	$x^{12} - 6x^{10} + 20x^9 - 72x^7 + 128x^6 - 96x^5 + 45x^4 - 8x^3 - 18x^2 + 12x - 2$
T_{46}	$x^{12} - 4x^{11} + 6x^{10} + 4x^9 - 21x^8 + 40x^7 - 28x^6 - 8x^5 + 25x^4 - 28x^3 + 10x^2 - 4x - 1$
T_{45}	$x^{12} - 3x^9 - 18x^8 - 24x^6 - 9x^5 + 69x^4 - x^3 + 3x - 1$
T_{44}	$x^{12} - 6x^6 - 10x^3 - 6$
T_{43}	$x^{12} - 6x^9 + 10x^6 + 4x^3 + 2$
T_{42}	$x^{12} - x^6 + 7$
T_{41}	$x^{12} - x^9 - 6x^6 + x^3 + 1$
T_{40}	$x^{12} - 7x^{10} + 24x^8 - 36x^6 + 24x^4 + 13x^2 + 1$
T_{39}	$x^{12} - 4x^6 + 2$
T_{38}	$x^{12} + x^6 - 3$
T_{37}	$x^{12} + x^6 + 4$
T_{36}	$x^{12} - 2x^9 - 2x^3 + 1$
T_{35}	$x^{12} - x^9 - x^6 + x^3 + 1$

T_{34}	$x^{12} + 12x^{10} + 54x^8 + 108x^6 + 81x^4 + 16$
T_{33}	$x^{12} + 2x^8 + 58x^6 + 301x^4 + 174x^2 + 25$
T_{32}	$x^{12} + 7x^{10} - x^8 - 23x^6 - x^4 + 7x^2 + 1$
T_{31}	$x^{12} + 6x^{10} - 23x^8 - 210x^6 - 360x^4 - 50x^2 + 25$
T_{30}	$x^{12} - 7x^{10} - 14x^8 + 115x^6 - 70x^4 - 175x^2 + 125$
T_{29}	$x^{12} - 45x^8 + 50x^6 + 225x^4 - 375x^2 + 125$
T_{28}	$x^{12} + 2$
T_{27}	$x^{12} + 12x^{10} + 68x^8 + 220x^6 + 392x^4 + 360x^2 + 148$
T_{26}	$x^{12} - 9x^8 - 8x^6 - 9x^4 + 1$
T_{25}	$x^{12} + 5x^8 + 6x^4 + 1$
T_{24}	$x^{12} - 2x^8 - 7x^4 + 16$
T_{23}	$x^{12} - 4x^4 + 4$
T_{22}	$x^{12} - 5x^{10} + 7x^8 - 6x^7 - 17x^6 - 6x^5 + 7x^4 - 5x^2 + 1$
T_{21}	$x^{12} + 3x^8 - 4x^6 + 3x^4 + 1$
T_{20}	$x^{12} - 4x^9 + 72x^8 - 84x^7 + 236x^6 - 144x^5 + 324x^4 - 192x^3 + 72x^2 + 8$
T_{19}	$x^{12} + 24x^{10} + 196x^8 + 600x^6 + 452x^4 + 112x^2 + 8$
T_{18}	$x^{12} + 2x^6 + 4$
T_{17}	$x^{12} + 4x^8 + 4x^6 + 5x^4 + 12x^2 + 2$
T_{16}	$x^{12} - x^6 + 4$
T_{15}	$x^{12} + 3$
T_{14}	$x^{12} - 9x^6 + 27$
T_{13}	$x^{12} - 3$
T_{12}	$x^{12} + x^6 - 27$
T_{11}	$x^{12} - 8x^6 + 8$
T_{10}	$x^{12} + 9$
T_9	$x^{12} + 3x^8 + 4x^6 + 3x^4 + 1$
T_8	$x^{12} - 6x^{10} - 8x^9 + 9x^8 + 12x^7 - 20x^6 + 9x^4 - 24x^3 - 4$
T_7	$x^{12} + 4x^{10} - x^8 - x^4 + 4x^2 + 1$
T_6	$x^{12} + 2x^{10} - 6x^8 + 2x^6 - 6x^4 + 2x^2 + 1$
T_5	$x^{12} - 80x^{10} + 1820x^8 - 13680x^6 + 29860x^4 - 2720x^2 + 32$
T_4	$x^{12} + 6x^8 + 26x^6 - 63x^4 + 162x^2 + 81$
T_3	$x^{12} + 36$
T_2	$x^{12} - x^6 + 1$
T_1	$x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

Table 3.12 Degree 13

T_9	S_{13}	$x^{13} - x + 1$
T_8	A_{13}	$x^{13} + 156x - 144$
T_7	$L_3(3)$	$x^{13} + x^{12} + 40x^{10} + 13x^9 - 99x^8 + 180x^7 - 468x^6 - 468x^5 + 1644x^4 - 912 + 24x + 24$
T_6	F_{156}	$x^{13} - 2$
T_5	F_{78}	$x^{13} + 3x^9 - 10x^8 - 3x^7 + 5x^6 - 20x^5 - 11x^4 + 2x^3 - 10x^2 - 10x - 3$
T_4	F_{52}	$x^{13} + 13x^{10} - 26x^8 + 13x^7 + 52x^6 - 39x^4 + 26x^2 + 13x + 2$
T_3	F_{39}	$x^{13} - 39x^{11} + 468x^9 - 1989x^7 - 507x^6 + 2886x^5 + 1443x^4 - 624x^3 - 234x^2 + 3$
T_2	D_{13}	$x^{13} - 2x^{12} + 4x^{10} - 5x^9 + x^8 + 5x^7 - 11x^6 + 19x^5 - 22x^4 + 16x^3 - 10x^2 + 6x - 1$
T_1	13	$x^{13} - x^{12} - 24x^{11} + 19x^{10} + 190x^9 - 116x^8 - 601x^7 + 246x^6 + 738x^5 - 215x^4 - 291x^3 + 68x^2 + 10x - 1$

Table 3.13 Degree 14

S_{14}	$x^{14} - x - 1$
A_{14}	$x^{14} - 9x^7 + 49x^5 - 90$
T_{61}	$x^{14} + x^2 - 2x + 1$
T_{60}	$x^{14} - 7x^8 - 6x^7 + 49x^2 + 84x + 36$
T_{59}	$x^{14} - 96x^7 - 1568x^2 + 2304$
T_{58}	$x^{14} - 7x^8 + 6x^7 + 784x^2 - 1344x + 576$
T_{57}	$x^{14} - x^2 + 1$
T_{56}	$x^{14} + 14x^8 - 24$
T_{55}	$x^{14} - x^2 - 1$
T_{54}	$x^{14} + 7x^6 + 4$
T_{53}	$x^{14} + 7x^8 - 7x^6 - 9$
T_{52}	$x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - 4x^8 + 6x^7 - 5x^5 + 5x^4 + x^3 - 4x^2 + 1$
T_{51}	$x^{14} - 7x^2 - 3$
T_{50}	$x^{14} - 2x^8 - 5x^6 - 3x^2 - 4$
T_{49}	$x^{14} - 4x^6 + 4$
T_{48}	$x^{14} + 7x^6 + 21x^2 + 50$
T_{47}	$x^{14} + 2x^{12} - 2x^{10} + x^6 - 8x^4 + 5x^2 + 2$
T_{46}	$x^{14} + 5x^{10} - 4x^8 + 2$
T_{45}	$x^{14} - 7x^{12} - 14x^{11} + 21x^{10} + 84x^9 + 35x^8 - 69x^7 + 7x^6 + 84x^5 + 7x^4 + 77x^3 + 133x^2 + 35x + 58$
T_{44}	$x^{14} - 8x^{10} - 2x^8 + 16x^6 + 6x^4 - 6x^2 - 2$
T_{43}	$x^{14} + 3x^{12} - 4x^8 + x^6 - 3x^2 + 1$
T_{42}	$x^{14} + 7x^{12} - 7x^{10} - 49x^8 + 7x^6 + 49x^4 - 49x^2 + 9$
T_{41}	$x^{14} - 2x^{12} - 2x^{10} + x^8 + 6x^6 - x^2 - 4$
T_{40}	$x^{14} + 2x^{12} - 14x^8 + 35x^6 - 21x^4 - 7x^2 + 7$
$PGL_2(13)$	$x^{14} - x^{13} - 26x^{10} + 65x^6 + 13x^5 - 52x^2 - 12x - 1$
T_{38}	$x^{14} - 7x^8 - 14x^6 - 7$
T_{37}	$x^{14} - 28x^{11} - 28x^9 + 196x^8 - 2x^7 + 392x^6 + 616x^4 - 392x^3 + 14x^2 + 56x + 9$
T_{36}	$x^{14} - 35x^{12} - 133x^{11} + 469x^{10} + 1239x^9 + 742x^8 - 3604x^7 + 47138x^6 - 85351x^5 + 168028x^4 - 156394x^3 + 158718x^2 - 72149x + 42751$
T_{35}	$x^{14} - 9x^{12} + 17x^{10} + 29x^8 - 49x^6 - 67x^4 - 21x^2 - 1$
T_{34}	$x^{14} - 3x^{12} + 4x^8 + x^6 - 3x^2 - 1$
T_{33}	$x^{14} + 14x^{10} + 28x^8 - 35x^6 + 784x^4 - 140x^2 - 4$
T_{32}	$x^{14} - 14x^{12} + 77x^{10} - 210x^8 + x^7 + 294x^6 - 7x^5 - 196x^4 + 14x^3 + 49x^2 - 7x + 2$
T_{31}	$x^{14} - 7x^{12} + 91x^8 - 192x^7 - 126x^5 - 1519x^4 + 1218x^3 + 8827x^2 + 11046x + 5484$
$L_2(13)$	$x^{14} - 6x^{13} + 13x^{12} - 338x^9 + 845x^8 + 17576x^4 + 70304x + 35152$
T_{29}	$x^{14} + 12x^{12} + 41x^{10} + 26x^8 - 59x^6 - 64x^4 + 9x^2 + 17$
T_{28}	$x^{14} + 7x^6 + 7x^4 + 7x^2 - 1$
T_{27}	$x^{14} + 7x^8 - 14x^6 + 7$
T_{26}	$x^{14} - 28x^{11} + 280x^{10} + 567x^9 + 5061x^8 + 2273x^7 - 735x^6 + 33908x^5 + 40348x^4 - 3192x^3 + 36855x^2 + 119196x + 75141$

T_{25}	$x^{14} + 42x^{12} - 42x^{11} + 525x^{10} - 896x^9 + 2422x^8 - 2536x^7 + 1225x^6 + 742x^5 - 994x^4 + 560x^3 - 28x^2 - 168x + 56$
T_{24}	$x^{14} - 3x^7 + 6$
T_{23}	$x^{14} - 14x^{12} + 77x^{10} - 210x^8 - 11x^7 + 294x^6 + 77x^5 - 196x^4 - 154x^3 + 49x^2 + 77x + 29$
T_{22}	$x^{14} + 42x^{12} - 840x^{11} + 4473x^{10} - 77728x^9 + 235648x^8 - 2601696x^7 + 6832756x^6 - 48638016x^5 + 124211584x^4 - 490172256x^3 + 802837840x^2 - 1497646080x + 723639232$
T_{21}	$x^{14} - x^{12} - 12x^{10} + 7x^8 + 28x^6 - 14x^4 - 9x^2 - 1$
T_{20}	$x^{14} - 2x^{13} - 4x^{12} + x^{11} + 6x^9 + 10x^8 - x^7 + 6x^6 - 13x^4 - 15x^3 - 5x^2 + x - 1$
T_{19}	$x^{14} + 10x^8 + 8x^6 - 4x^4 + 2$
T_{18}	$x^{14} + 4x^{12} - 30x^{10} + 8x^8 + 60x^6 + 8x^4 - 24x^2 - 8$
T_{17}	$x^{14} + 11x^{12} + 53x^{10} + 15x^8 - 149x^6 + 89x^4 - x^2 - 3$
T_{16}	$x^{14} - 14x^{10} + 14x^8 + 22x^7 + 21x^6 + 49x^4 - 154x^3 + 77x^2 - 154x + 149$
T_{15}	$x^{14} - 87x^{12} + 1456x^{10} - 256x^9 - 8563x^8 + 3448x^7 + 18032x^6 - 9890x^5 - 11776x^4 + 5198x^3 + 3128x^2 - 506x - 184$
T_{14}	$x^{14} - 2x^7 + 8$
T_{13}	$x^{14} + 4x^{13} + 10x^{11} + 39x^{10} + 28x^9 - 13x^8 + 34x^7 + 126x^6 - 36x^5 + 29x^4 - 24x^3 + 38x^2 - 16x + 4$
T_{12}	$x^{14} + 35x^{12} + 210x^{11} + 735x^{10} + 2849x^9 + 10150x^8 + 45655x^7 + 94570x^6 + 98455x^5 - 199381x^4 - 344400x^3 + 647395x^2 + 4094650x + 1010645$
T_{11}	$x^{14} - 5x^{12} - 11x^{10} + 25x^8 + 27x^6 - 23x^4 - 17x^2 - 1$
T_{10}	$x^{14} + 14x^8 - 84x^6 + 84x^4 + 21x^2 - 9$
T_9	$x^{14} + 7x^{12} - 49x^{10} - 245x^8 + 588x^6 + 294x^4 - 7$
T_8	$x^{14} - x^{12} - 3x^{11} + 5x^{10} + 5x^9 - 5x^8 - 9x^7 + x^6 + 14x^5 - 2x^4 - 7x^3 + x^2 + 1$
T_7	$x^{14} + 2$
T_6	$x^{14} + 13x^{12} + 31x^{10} - 9x^8 - 54x^6 - 3x^4 + 23x^2 - 1$
T_5	$x^{14} - x^7 + 2$
T_4	$x^{14} + 7$
T_3	$x^{14} + 6x^{12} + 7x^{10} + x^8 - 3x^6 + x^4 + 3x^2 + 1$
T_2	$x^{14} + 8x^{12} + 22x^{10} + 8x^8 - 55x^6 - 48x^4 + 64x^2 + 71$
T_1	$x^{14} + 25x^{12} + 214x^{10} + 767x^8 + 1194x^6 + 686x^4 + 53x^2 + 1$

References

- Abhyankar, S.S. (1957): Coverings of algebraic curves. Amer. J. Math. **79**, 825–856
- Abhyankar, S.S. (1994): Nice equations for nice groups. Israel J. Math. **88**, 1–23
- Abhyankar, S.S. (1996a): Again nice equations for nice groups. Proc. Amer. Math. Soc. **124**, 2967–2976
- Abhyankar, S.S. (1996b): More nice equations for nice groups. Proc. Amer. Math. Soc. **124**, 2977–2991
- Abhyankar, S.S., Inglis, N.J. (2001): Galois groups of some vectorial polynomials. Trans. Amer. Math. Soc. **353**, 2941–2869
- Abhyankar, S.S., Keskar, P.H. (2001): Descent principle in modular Galois theory. Proc. Indian Acad. Sci. Math. **11**, 139–149
- Abhyankar, S.S., Loomis, P.A. (1998): Once more nice equations for nice groups. Proc. Amer. Math. Soc. **126**, 1885–1896
- Abhyankar, S.S., Loomis, P.A. (1999): Twice more nice equations for nice groups. Pp. 63–76 in: Applications of curves over finite fields (Seattle, WA, 1997), Contemp. Math., 245, Amer. Math. Soc., Providence, RI, 1999
- Albert, M., Maier, A. (2011): Additive polynomials for finite groups of Lie type. Israel J. Math. **186**, 125–195
- Artin, E. (1925): Theorie der Zöpfe. Abh. Math. Sem. Univ. Hamburg **4**, 47–72
- Artin, E. (1947): Theory of braids. Ann. of Math. **48**, 101–126
- Artin, E. (1967): Algebraic numbers and algebraic functions. Gordon and Breach, New York
- Aschbacher, M. (1986): Finite group theory. Cambridge University Press, Cambridge
- Aschbacher, M. et al. (eds.) (1984): Proceedings of the Rutgers group theory year, 1983–1984. Cambridge University Press, Cambridge
- Auslander, M., Brumer, A. (1968): Brauer groups of discrete valuation rings. Indag. Math. **30**, 286–296
- Barth, D., Wenz, A. (2016): Explicit Belyi maps over \mathbb{Q} having almost simple primitive monodromy groups. Preprint, arXiv:1703.02848

- Barth, D., Wenz, A. (2017): Belyi map for the sporadic group J_1 . Preprint, arXiv:1704.06419
- Bayer-Fluckiger, E. (1994): Galois cohomology and the trace form. *Jahresber. Deutsch. Math.-Verein.* **96**, 35–55
- Beckmann, S. (1989): Ramified primes in the field of moduli of branched coverings of curves. *J. Algebra* **125**, 236–255
- Beckmann, S. (1991): On extensions of number fields obtained by specializing branched coverings. *J. reine angew. Math.* **419**, 27–53
- Belyi, G.V. (1979): On Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.* **43**, 267–276 (Russian) [English transl.: *Math. USSR Izv.* **14** (1979), 247–256]
- Belyi, G.V. (1983): On extensions of the maximal cyclotomic field having a given classical Galois group. *J. reine angew. Math.* **341**, 147–156
- Benson, D.J. (1991): Representations and cohomology I. Cambridge University Press, Cambridge
- Beynon, W.M., Spaltenstein, N. (1984): Green functions of finite Chevalley groups of type E_n ($n = 6, 7, 8$). *J. Algebra* **88**, 584–614
- Birman, J.S. (1975): Braids, links and mapping class groups. Princeton University Press, Princeton
- Borel, A. (1991): Linear algebraic groups. Springer, New York
- Borel, A. et al. (1970): Seminar on algebraic groups and related finite groups. LNM **131**, Springer, Berlin
- Bosch, S., Güntzer, U., Remmert, R. (1984): Non-archimedean analysis. Springer, Berlin Heidelberg New York
- Breuer, T., Malle, G., O’Brien, E. (2016): Reliability and reproducibility of Atlas information. Submitted
- Brieskorn, E., Saito, K. (1972): Artin-Gruppen und Coxeter-Gruppen. *Invent. Math.* **17**, 245–271
- Bruen, A.A., Jensen, C.U., Yui, N. (1986): Polynomials with Frobenius groups of prime degree as Galois groups. *J. Number Theory* **24**, 305–359
- Butler, G., McKay, J. (1983): The transitive groups of degree up to eleven. *Comm. Algebra* **11**, 863–911
- Cartan, H., Eilenberg, S. (1956): Homological algebra. Princeton University Press, Princeton
- Carter, R.W. (1985): Finite groups of Lie type: Conjugacy classes and complex characters. John Wiley and Sons, Chichester
- Carter, R.W. (1989): Simple groups of Lie type. John Wiley and Sons, Chichester
- Chang, B., Ree, R. (1974): The characters of $G_2(q)$. Pp. 395–413 in: *Symposia Mathematica XIII*, London
- Chow, W.-L. (1948): On the algebraic braid group. *Ann. of Math.* **49**, 654–658
- Cohen, A.M. et al. (1992): The local maximal subgroups of exceptional groups of Lie type, finite and algebraic. *Proc. London Math. Soc.* **64**, 21–48
- Cohen, D.B. (1974): The Hurwitz monodromy group. *J. Algebra* **32**, 501–517
- Colin, A. (1995): Formal computation of Galois groups with relative resolvents. Pp. 169–182 in: *Lecture Notes in Comput. Sci.*, 948, Springer, Berlin

- Conway, J.H. et al. (1985): *Atlas of finite groups*. Clarendon Press, Oxford
- Cooperstein, B.N. (1981): Maximal subgroups of $G_2(2^n)$. *J. Algebra* **70**, 23–36
- Crespo, T. (1989): Explicit construction of A_n type fields. *J. Algebra* **127**, 452–461
- Dèbes, P., Fried, M.D. (1990): Arithmetic variation of fibers in families of covers I. *J. reine angew. Math.* **404**, 106–137
- Deligne, P., Lusztig, G. (1976): Representations of reductive groups over finite fields. *Ann. of Math.* **103**, 103–161
- Delone, B.N., Faddeev, D.K. (1944): Investigations in the geometry of the Galois theory. *Math. Sb.* **15(57)**, 243–284 (Russian with English summary)
- Demuškin, S.P., Šafarevič, I.R. (1959): The embedding problem for local fields. *Izv. Akad. Nauk. Ser. Mat.* **23**, 823–840 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **27**, 267–288 (1963)]
- Dentzer, R. (1989): Projektive symplektische Gruppen $\mathrm{PSp}_4(p)$ als Galoisgruppen über $\mathbb{Q}(t)$. *Arch. Math.* **53**, 337–346
- Dentzer, R. (1995a): Polynomials with cyclic Galois group. *Comm. Algebra* **23**, 1593–1603
- Dentzer, R. (1995b): On geometric embedding problems and semiabelian groups. *Manuscripta Math.* **86**, 199–216
- Deriziotis, D.I. (1983): The centralizers of semisimple elements of the Chevalley groups E_7 and E_8 . *Tokyo J. Math.* **6**, 191–216
- Deriziotis, D.I., Michler, G.O. (1987): Character table and blocks of finite simple triality groups ${}^3D_4(q)$. *Trans. Amer. Math. Soc.* **303**, 39–70
- Derksen, H., Kemper, G. (2002): Computational invariant theory. Springer Verlag, Berlin
- Dettweiler, M. (2003): Middle convolution functor and Galois realizations. Pp. 143–158 in: K. Hashimoto et al. Eds: *Galois theory and modular forms*. Kluwer
- Dettweiler, M. (2004): Plane curve complements and curves on Hurwitz spaces. *J. reine angew. Math.* **573**, 19–43
- Dettweiler, M., Reiter, S. (1999): On rigid tuples in linear groups. *J. Algebra* **222**, 550–560
- Dettweiler, M., Reiter, S. (2000): An algorithm of Katz and its applications to the inverse Galois problem. *J. Symb. Comput.* **30**, 761–798
- Dew, E. (1992): Fields of moduli of arithmetic Galois groups. PhD-thesis, University of Pennsylvania
- Digne, F., Michel, J. (1991): Representations of finite groups of Lie type. LMS Student Texts **21**, Cambridge University Press, Cambridge
- Digne, F., Michel, J. (1994): Groupes réductifs non connexes. *Ann. scient. Éc. Norm. Sup.* **27**, 345–406
- van den Dries, L., Ribenboim, P. (1979): Application de la théorie des modèles aux groupes de Galois de corps de fonctions. *C. R. Acad. Sci. Paris* **288**, A789–A792
- Douady, A. (1964): Détermination d'un groupe de Galois. *C. R. Acad. Sci. Paris* **258**, 5305–5308
- Elkies, N.D. (1997): Linearized algebra and finite groups of Lie type I: Linear and symmetric groups. *Contemp. Math.* **245**, 77–108
- Engler, A.J., Prestel, A. (2005): *Valued fields*. Springer Verlag, Berlin

- Enomoto, H. (1976): The characters of the finite Chevalley groups $G_2(q)$, $q = 3^f$. *Japan. J. Math.* **2**, 191–248
- Enomoto, H., Yamada, H. (1986): The characters of $G_2(2^n)$. *Japan. J. Math.* **12**, 325–377
- Faddeev, D.K. (1951): Simple algebras over a field of algebraic functions of one variable. *Trudy Mat. Inst. Steklov* **38**, 190–243 (Russian) [English transl.: Amer. Math. Soc. Transl. II **3**, 15–38 (1956)]
- Fadell, E. (1962): Homotopy groups of configuration spaces and the string problem of Dirac. *Duke Math. J.* **29**, 231–242
- Fadell, E., Van Buskirk, J. (1962): The braid groups of E^2 and S^2 . *Duke Math. J.* **29**, 243–257
- Feit, W. (1984): Rigidity of $\text{Aut}(\text{PSL}_2(p^2))$, $p \equiv \pm 2 \pmod{5}$, $p \neq 2$. Pp. 351–356 in: M. Aschbacher et al. (eds.) (1984)
- Feit, W. (1989): Some finite groups with nontrivial centers which are Galois groups. Pp. 87–109 in: Group Theory, Proceedings of the 1987 Singapore Conference. W. de Gruyter, Berlin-New York
- Feit, W., Fong, P. (1984): Rational rigidity of $G_2(p)$ for any prime $p > 5$. Pp. 323–326 in: M. Aschbacher et al. (eds.) (1984)
- Fleischmann, P., Janiszczak, I. (1993): The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7 . *Comm. Algebra* **21**, 93–161
- Folkers, M. (1995): Lineare Gruppen ungerader Dimension als Galoisgruppen über \mathbb{Q} . IWR-Preprint 95-41, Universität Heidelberg
- Forster, O. (1981): Lectures on Riemann surfaces. Springer, New York
- Franz, W. (1931): Untersuchungen zum Hilbertschen Irreduzibilitätsatz. *Math. Z.* **33**, 275–293
- Fresnel, J., van der Put, M. (1981): Géométrie analytique rigide et applications. Birkhäuser, Basel
- Fresnel, J., van der Put, M. (2004): Rigid analytic geometry and its applications. Birkhäuser, Boston
- Fried, M.D. (1977): Fields of definition of function fields and Hurwitz families — Groups as Galois groups. *Comm. Algebra* **5**, 17–82
- Fried, M.D. (1984): On reduction of the inverse Galois problem to simple groups. Pp. 289–301 in: M. Aschbacher et al. (eds.) (1984)
- Fried, M.D., Biggers, R. (1982): Moduli spaces of covers and the Hurwitz monodromy group. *J. reine angew. Math.* **335**, 87–121
- Fried, M.D., Dèbes, P. (1990): Rigidity and real residue class fields. *Acta Arithmetica* **56**, 291–323
- Fried, M.D., Jarden, M. (1986): Field arithmetic. Springer, Berlin
- Fried, M.D., Völklein, H. (1991): The inverse Galois problem and rational points on moduli spaces. *Math. Ann.* **290**, 771–800
- Fried, M.D., Völklein, H. (1992): The embedding problem over a Hilbertian PAC-field. *Ann. of Math.* **135**, 469–481
- Fried, M.D. et al. (eds.) (1995): Recent developments in the inverse Galois problem. Contemporary Math. vol. 186, Amer. Math. Soc., Providence

- Fröhlich, A. (1985): Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants. *J. reine angew. Math.* **360**, 84–123
- Frohardt, D., Guralnick, R., Hoffman, C., Magaard, K. (2016): Exceptional low genus actions of finite groups. Preprint
- Frohardt, D., Magaard, K. (2001): Composition factors of monodromy groups. *Ann. of Math.* **154**, 327–345
- Garcia Lopez, F. (2010): An algorithm for computing Galois groups of additive polynomials. Preprint
- Geck, M. (2003): An introduction to algebraic geometry and algebraic groups. Oxford University Press, Oxford
- Geyer, W.-D., Jarden, M. (1998): Bounded realization of ℓ -groups over global fields. *Nagoya Math. J.* **150**, 13–62
- Gille, P. (2000): Le groupe fondamental sauvage d'une courbe affine in characteristic p . Pp. 217–231 in: Bost, J.-L. et al. eds.: Courbes semi-stables et groupe fondamental en géométrie algébrique. Birkhäuser, Basel
- Gillette, R., Van Buskirk, J. (1968): The word problem and consequences for the braid groups and mapping class groups of the 2-sphere. *Trans. Amer. Math. Soc.* **131**, 277–296
- Goss, D. (1996): Basic structures of function field arithmetic. Springer, Berlin
- Granboulan, L. (1996): Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24} . *Experimental Math.* **5**, 3–14
- Grothendieck, A. (1971): Revêtements étales et groupe fondamental. Springer, Berlin
- Guralnick, R.M., Lübeck, F., Yu, J. (2016): Rational rigidity for $F_4(p)$. *Adv. Math.* **302**, 48–58
- Guralnick, R.M., Malle, G. (2012): Simple groups admit Beauville structures. *J. London Math. Soc.* **85**, 694–721
- Guralnick, R.M., Malle, G. (2014): Rational rigidity for $E_8(p)$. *Compos. Math.* **150**, 1679–1702
- Guralnick, R.M., Thompson, J.G. (1990): Finite groups of genus zero. *J. Algebra* **131**, 303–341
- Häfner, F. (1992): Einige orthogonale und symplektische Gruppen als Galoisgruppen über \mathbb{Q} . *Math. Ann.* **292**, 587–618
- Hansen, V.L. (1989): Braids and coverings. Cambridge University Press, Cambridge
- Haraoka, Y. (1994): Finite monodromy of Pochhammer equation. *Ann. Inst. Fourier* **44**, 767–810
- Haran, D., Völklein, H. (1996): Galois groups over complete valued fields. *Israel J. Math.* **93**, 9–27
- Harbater, D. (1984): Mock covers and Galois extensions. *J. Algebra* **91**, 281–293
- Harbater, D. (1987): Galois coverings of the arithmetic line. In: Chudnovsky, D.V. et al. (eds.): Number Theory, New York 1984–1985. Springer, Berlin
- Harbater, D. (1994a): Abhyankar's conjecture on Galois groups over curves. *Invent. Math.* **117**, 1–25

- Harbater, D. (1994b): Galois groups with prescribed ramification. Pp. 35–60 in: N. Childress and J. Jones (eds.): Arithmetic Geometry. Contemporary Math. vol. 174, Amer. Math. Soc., Providence
- Harbater, D. (1995a): Fundamental groups and embedding problems in characteristic p . Pp. 353–369 in: M. Fried et al. (eds.) (1995)
- Harbater, D. (1995b): Fundamental groups of curves in characteristic p . Pp. 656–666 in: Proc. Int. Congress of Math., Zürich 1994, Birkhäuser
- Hartshorne, R. (1977): Algebraic geometry. Springer, Berlin Heidelberg New York
- Hasse, H. (1948): Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers I. Math. Nachr. **1**, 40–61
- Hasse, H. (1980): Number theory. Springer, Berlin
- Hecke, E. (1935): Die eindeutige Bestimmung der Modulfunktionen q -ter Stufe durch algebraische Eigenschaften. Math. Ann. **111**, 293–301
- Higman, D., McLaughlin, J. (1965): Rank 3 subgroups of finite symplectic and unitary groups. J. reine angew. Math. **218**, 174–189
- Hilbert, D. (1892): Über die Irreducibilität ganzer rationaler Functionen mit ganzzähligen Coeffizienten. J. reine angew. Math. **110**, 104–129
- Hilton, P.J., Stammbach, U. (1971): A course in homological algebra. Springer, New York
- Hoechsmann, K. (1968): Zum Einbettungsproblem. J. reine angew. Math. **229**, 81–106
- Hoyden-Siedersleben, G. (1985): Realisierung der Jankogruppen J_1 und J_2 als Galoisgruppen über \mathbb{Q} . J. Algebra **97**, 14–22
- Hoyden-Siedersleben, G., Matzat, B.H. (1986): Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpern. J. Algebra **101**, 273–285
- Hunt, D.C. (1986): Rational rigidity and the sporadic groups. J. Algebra **99**, 577–592
- Huppert, B. (1967): Endliche Gruppen I. Springer, Berlin
- Huppert, B., Blackburn, N. (1982): Finite groups II. Grundlehren **242**, Springer, Berlin
- Hurwitz, A. (1891): Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten. Math. Ann. **39**, 1–61
- Ihara, Y. (1991): Braids, Galois groups, and some arithmetic functions. Pp. 99–120 in: Proc. Int. Congress of Math., Kyoto 1990, Springer
- Ihara, Y. et al. (eds.) (1989): Galois groups over \mathbb{Q} . Springer, New York
- Iitaka, S. (1982): Algebraic geometry. Springer Verlag, Berlin
- Ikeda, M. (1960): Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren. Abh. Math. Sem. Univ. Hamburg **24**, 126–131
- Inaba, E. (1944): Über den Hilbertschen Irreduzibilitätssatz. Japan. J. Math. **19**, 1–25
- Ishkhanov, V.V., Lure, B.B., Faddeev, D.K. (1997): The embedding problem in Galois theory. Amer. Math. Soc., Providence
- Iwasawa, K. (1953): On solvable extensions of algebraic number fields. Ann. of Math. **58**, 548–572

- Jacobson, N. (1980): Basic algebra II. W. H. Freeman, New York
- Jensen, C., Ledet, A., Yui, N. (2002): Generic polynomials. Constructive aspects of the inverse Galois problem. Cambridge University Press, Cambridge
- Kantor, W.M. (1979): Subgroups of classical groups generated by long root elements. *Trans. Amer. Math. Soc.* **248**, 347–379
- Katz, N. (1996): Rigid local systems. Annals of Math. Studies 139, Princeton University Press, Princeton
- Kemper, G., Lübeck, F., Magaard, K. (2001): Matrix generators for the Ree groups ${}^2G_2(q)$. *Comm. Algebra* **29**, 407–415
- Kleidman, P.B. (1987): The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra* **110**, 173–242
- Kleidman, P.B. (1988a): The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups. *J. Algebra* **115**, 182–199
- Kleidman, P.B. (1988b): The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$ and of their automorphism groups. *J. Algebra* **117**, 30–71
- Kleidman, P.B., Liebeck, M. (1990): The subgroup structure of the finite classical groups. LMS lecture notes **129**, Cambridge University Press, Cambridge
- Klein, F. (1884): Vorlesungen über das Ikosaeder. Teubner, Leipzig
- Klein, F., Fricke, R. (1890): Vorlesungen über die Theorie der elliptischen Modulfunktionen I. Teubner, Leipzig
- Klüners, J., Malle, G. (2000): Explicit Galois realization of transitive groups of degree up to 15. *J. Symbolic Comput.* **30**, 675–716
- Klüners, J., Malle, G. (2002): A Database for Number Fields. <http://galoisdb.math.upb.de/>
- Kochendörffer, R. (1953): Zwei Reduktionssätze zum Einbettungsproblem für abelsche Algebren. *Math. Nachr.* **10**, 75–84
- König, J. (2015): Computation of Hurwitz spaces and new explicit polynomials for almost simple Galois groups. *Math. Comp.*, to appear
- König, J. (2016): On rational functions with monodromy group M_{11} . *J. Symbolic Comput.* **79**, 372–383
- Köpf, U. (1974): Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen. *Schriftenreihe Math. Inst. Univ. Münster*, 2. Serie, Heft **7**
- Kreuzer, M., Robbiano, L. (2000): Computational commutative algebra I. Springer Verlag, Berlin
- Krull, W., Neukirch, J. (1971): Die Struktur der absoluten Galoisgruppe über dem Körper $\mathbb{IR}(t)$. *Math. Ann.* **193**, 197–209
- Kucera, J. (1994): Über die Brauergruppe von Laurentreihen- und rationalen Funktionenkörpern und deren Dualität mit K -Gruppen. Dissertation, Universität Heidelberg
- Kuyk, W. (1970): Extensions de corps Hilbertiens. *J. Algebra* **14**, 112–124
- Landazuri, V., Seitz, G.M. (1974): On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32**, 418–443
- Lang, S. (1982): Introduction to algebraic and abelian functions. Springer, New York

- Ledet, A. (2000): On a theorem of Serre. Proc. Amer. Math. Soc. **128**, 27–29
- Ledet, A. (2005): Brauer type embedding problems. Amer. Math. Soc., Providence
- Liebeck, M.W., Seitz, G.M. (1999): On finite subgroups of exceptional algebraic groups. J. Reine Angew. Math. **515**, 25–72
- Liu, Q. (1995): Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(t)$, d'après Harbater. Pp. 261–265 in: M. Fried et al (eds.) (1995)
- Lübeck, F., Malle, G. (1998): (2,3)-generation of exceptional groups. J. London Math. Soc. **59**, 109–122
- Lusztig, G. (1977): Representations of finite Chevalley groups. CBMS Regional Conference Series in Mathematics **39**
- Lusztig, G. (1980): On the unipotent characters of the exceptional groups over finite fields. Invent. Math. **60**, 173–192
- Lusztig, G. (1984): Characters of reductive groups over a finite field. Annals of Math. Studies **107**, Princeton University Press, Princeton
- Lyndon, R.C., Schupp, P.E. (1977): Combinatorial group theory. Springer, Berlin
- Madan, M., Rzedowski-Calderon, M., Villa-Salvador, G. (1996): Galois extensions with bounded ramification in characteristic p . Manuscripta Math. **90**, 121–135
- Malle, G. (1986): Exzeptionelle Gruppen vom Lie-Typ als Galoisgruppen. Dissertation, Universität Karlsruhe
- Malle, G. (1987): Polynomials for primitive nonsolvable permutation groups of degree $d \leq 15$. J. Symb. Comp. **4**, 83–92
- Malle, G. (1988a): Polynomials with Galois groups $\text{Aut}(M_{22})$, M_{22} , and $\text{PSL}_3(\text{IF}_4).2$ over \mathbb{Q} . Math. Comp. **51**, 761–768
- Malle, G. (1988b): Exceptional groups of Lie type as Galois groups. J. reine angew. Math. **392**, 70–109
- Malle, G. (1991): Genus zero translates of three point ramified Galois extensions. Manuscripta Math. **71**, 97–111
- Malle, G. (1992): Disconnected groups of Lie type as Galois groups. J. reine angew. Math. **429**, 161–182
- Malle, G. (1993a): Polynom mit Galoisgruppen $\text{PGL}_2(p)$ und $\text{PSL}_2(p)$ über $\mathbb{Q}(t)$. Comm. Algebra **21**, 511–526
- Malle, G. (1993b): Generalized Deligne-Lusztig characters. J. Algebra **159**, 64–97
- Malle, G. (1993c): Green functions for groups of types E_6 and F_4 in characteristic 2. Comm. Algebra **21**, 747–798
- Malle, G. (1996): GAR-Realisierungen klassischer Gruppen. Math. Ann. **304**, 581–612
- Malle, G. (2003): Explicit realization of the Dickson groups $G_2(q)$ as Galois groups. Pacific J. Math. **212**, 157–167
- Malle, G., Matzat, B. H. (1985): Realisierung von Gruppen $\text{PSL}_2(\text{IF}_p)$ als Galoisgruppen über \mathbb{Q} . Math. Ann. **272**, 549–565
- Malle, G., Matzat, B. H. (1999): Inverse Galois theory. Springer Verlag, Berlin-Heidelberg
- Malle, G., Saxl, J., Weigel, T. (1994): Generation of classical groups. Geom. Dedicata **49**, 85–116

- Malle, G., Sonn, J. (1996): Covering groups of almost simple groups as Galois groups over $\mathbb{Q}^{\text{ab}}(t)$. Israel J. Math. **96**, 431–444.
- Malle, G., Testerman, D. (2011): Linear algebraic groups and finite groups of Lie type. Cambridge University Press, Cambridge
- Matsumura, H. (1980): Commutative algebra. Benjamin/Cummings, Reading
- Matzat, B.H. (1979): Konstruktion von Zahlkörpern mit der Galoisgruppe M_{11} über $\mathbb{Q}(\sqrt{-11})$. Manuscripta Math. **27**, 103–111
- Matzat, B.H. (1984): Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. J. reine angew. Math. **349**, 179–220
- Matzat, B.H. (1985a): Zwei Aspekte konstruktiver Galoistheorie. J. Algebra **96**, 499–531
- Matzat, B.H. (1985b): Zum Einbettungsproblem der algebraischen Zahlentheorie mit nicht abelschem Kern. Invent. Math. **80**, 365–374
- Matzat, B.H. (1986): Topologische Automorphismen in der konstruktiven Galoistheorie. J. reine angew. Math. **371**, 16–45
- Matzat, B.H. (1987): Konstruktive Galoistheorie. LNM **1284**, Springer, Berlin
- Matzat, B.H. (1989): Rationality criteria for Galois extensions. Pp. 361–383 in: Y. Ihara et al. (eds.) (1989)
- Matzat, B.H. (1991a): Zöpfe und Galoissche Gruppen. J. reine angew. Math. **420**, 99–159
- Matzat, B.H. (1991b): Frattini-Einbettungsprobleme über Hilbertkörpern. Manuscripta Math. **70**, 429–439
- Matzat, B.H. (1991c): Der Kenntnisstand in der konstruktiven Galoisschen Theorie. Pp. 65–98 in G.O. Michler and C.M. Ringel (eds.) (1991)
- Matzat, B.H. (1992): Zopfgruppen und Einbettungsprobleme. Manuscripta Math. **74**, 217–227
- Matzat, B.H. (1993): Braids and decomposition groups. Pp. 179–189 in: S. David (ed.): Séminaire de théorie des nombres, Paris 1991–1992. Birkhäuser, Boston
- Matzat, B.H. (1995): Parametric solutions of embedding problems. Pp. 33–50 in: M. Fried et al. (eds.) (1995)
- Matzat, B.H. (2003): Frobenius modules and Galois groups. Pp. 233–268 in K. Hashimoto, K. Miyake, H. Nakamura et al. Eds.: Galois theory and modular forms. Kluwer Acad. Publ., Boston, MA
- Matzat, B.H., Zeh-Marschke, A. (1986): Realisierung der Mathieu-Gruppen M_{11} und M_{12} als Galoisgruppen über \mathbb{Q} . J. Number Theory **23**, 195–202
- McLaughlin, J. (1969): Some subgroups of $SL_n(\mathbb{F}_p)$. Ill. J. Math. **13**, 108–115
- Melnikov, O.V. (1980): Projective limits of free profinite groups. Dokl. Akad. Nauk SSSR **24**, 968–970
- Mestre, J.-F. (1990): Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois \tilde{A}_n . J. Algebra **131**, 483–495
- Mestre, J.-F. (1994): Construction d’extensions régulières de $\mathbb{Q}(t)$ à groupes de Galois $SL_2(F_7)$ et \tilde{M}_{12} . C. R. Acad. Sci. **319**, 781–782
- Mestre, J.-F. (1998): Extensions \mathbb{Q} -régulières de $\mathbb{Q}(t)$ de groupes de Galois $6.A_6$ et $6.A_7$. Israel J. Math. **107**, 333–341

- Michler, G.O., Ringel, C.M. (eds.) (1991): Representation theory of finite groups and finite-dimensional algebras. Birkhäuser, Basel
- Mizuno, K. (1977): The conjugate classes of Chevalley groups of type E_6 . *J. Fac. Sci. Univ. Tokyo* **24**, 525–563
- Mizuno, K. (1980): The conjugate classes of unipotent elements of the Chevalley groups E_7 and E_8 . *Tokyo J. Math.* **3**, 391–461
- Monien, H. (2017): The sporadic group J_2 , Hauptmodul and Belyi map. Preprint, arXiv:1703.05200
- Müller, P. (2012): A one-parameter family of polynomials with Galois group M_{24} over $\mathbb{Q}(t)$. Preprint, arXiv:1204.1328
- Nagata, M. (1977): Field theory. Marcel Dekker, New York
- Nakamura, H. (1997): Galois rigidity of profinite fundamental groups. *Sugaku Expositiones* **10**, 195–215
- Narkiewicz, W. (1990): Elementary and analytic theory of algebraic numbers. Springer, Berlin
- Neukirch, J., Schmidt, A. and Wingberg, K. (2000): Cohomology of Number Fields. Springer-Verlag, Berlin.
- Nobusawa, N. (1961): On the embedding problem of fields and Galois algebras. *Abh. Math. Sem. Univ. Hamburg* **26**, 89–92
- Noether, E. (1918): Gleichungen mit vorgeschrriebener Gruppe. *Math. Ann.* **78**, 221–229
- Nori, M.V. (1994): Unramified coverings of the affine line in positive characteristic. Pp. 209–212 in: Bajaj, C.L., ed.: Algebraic geometry and its applications. Springer, New York
- Norton, S.P., Wilson, R.A. (1989): The maximal subgroups of $F_4(2^n)$ and its automorphism group. *Comm. Algebra* **17**, 2809–2824
- Pahlings, H. (1988): Some sporadic groups as Galois groups. *Rend. Sem. Math. Univ. Padova* **79**, 97–107
- Pahlings, H. (1989): Some sporadic groups as Galois groups II. *Rend. Sem. Math. Univ. Padova* **82**, 163–171 [correction: ibid. **85** (1991), 309–310]
- Pochhammer, L. (1870): Über die hypergeometrischen Funktionen n -ter Ordnung. *J. reine angew. Math.* **71**, 312–352
- Pop, F. (1994): $\frac{1}{2}$ Riemann existence theorem with Galois action. Pp. 193–218 in: G. Frey and J. Ritter (eds.): Algebra and number theory. W. de Gruyter, Berlin
- Pop, F. (1995): Étale Galois covers of affine smooth curves. *Invent. Math.* **120**, 555–578
- Pop, F. (1996): Embedding problems over large fields. *Ann. of Math.* **144**, 1–34
- Popp, H. (1970): Fundamentalgruppen algebraischer Mannigfaltigkeiten. Springer, Berlin
- Porsch, U. (1993): Greenfunktionen der endlichen Gruppen $E_6(q)$, $q = 3^n$. Diplomarbeit, Universität Heidelberg
- Przywara, B. (1991): Zopfbahnen und Galoisgruppen. IWR-Preprint 91-01, Universität Heidelberg
- van der Put, M., Singer, M.F. (1997): Galois theory of difference equations. Springer Verlag, Berlin

- Raynaud, M. (1994): Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. *Invent. Math.* **116**, 425–462
- Reichardt, H. (1937): Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. reine angew. Math.* **177**, 1–5
- Reiter, S. (1999): Galoisrealisierungen klassischer Gruppen. *J. reine angew. Math.* **511**, 193–236
- Ribes, L. (1970): Introduction to profinite groups and Galois cohomology. Queen's University, Kingston
- Rzedowski-Calderon, M. (1989): Construction of global function fields with nilpotent automorphism groups. *Bol. Soc. Mat. Mexicana* **34**, 1–10
- Šafarevič, I.R. (1947): On p -extensions. *Math. Sb. Nov. Ser.* **20** (62), 351–363 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **4**, 59–72 (1956)]
- Šafarevič, I.R. (1954a): On the construction of fields with a given Galois group of order ℓ^a . *Izv. Akad. Nauk. SSSR* **18**, 216–296 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **4**, 107–142 (1956)]
- Šafarevič, I.R. (1954b): On an existence theorem in the theory of algebraic numbers. *Izv. Akad. Nauk. SSSR* **18**, 327–334 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **4**, 143–150 (1956)]
- Šafarevič, I.R. (1954c): On the problem of imbedding fields. *Izv. Akad. Nauk. SSSR* **18**, 389–418 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **4**, 151–183 (1956)]
- Šafarevič, I.R. (1954d): Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk. SSSR* **18**, 525–578 (Russian) [English transl.: *Amer. Math. Soc. Transl. II* **4**, 185–237 (1956)]
- Šafarevič, I.R. (1958): The embedding problem for splitting extensions. *Dokl. Akad. Nauk SSSR* **120**, 1217–1219 (Russian)
- Šafarevič, I.R. (1989): Factors of descending central series. *Math. Notes* **45**, 262–264
- Šafarevič, I.R. (1994): Basic algebraic geometry I. Springer Verlag
- Saïdi, M. (2000): Abhyankar's conjecture II: the use of semi-stable curves. Pp. 249–265 in: Bost, J.-L. et al. eds.: *Courbes semi-stables et groupe fondamental en géométrie algébrique*. Birkhäuser, Basel
- Saltman, D.J. (1982): Generic Galois extensions and problems in field theory. *Adv. Math.* **43**, 250–283
- Saltman, D.J. (1984): Noether's problem over algebraically closed fields. *Invent. Math.* **77**, 71–84
- Scharlau, W. (1969): Über die Brauer-Gruppe eines algebraischen Funktionenkörpers einer Variablen. *J. reine angew. Math.* **239/240**, 1–6
- Scharlau, W. (1985): Quadratic and Hermitean forms. Springer, Berlin
- Schneps, L. (1992): Explicit construction of extensions of $\mathbb{Q}(t)$ of Galois group \tilde{A}_n for n odd. *J. Algebra* **146**, 117–123
- Scholz, A. (1929): Über die Bildung algebraischer Zahlkörper mit auflösbarer galoisscher Gruppe. *Math. Z.* **30**, 332–356
- Scholz, A. (1937): Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I. *Math. Z.* **42**, 161–188

- Scott, L. (1977): Matrices and cohomology. *Ann. of Math.* **105**, 473–492
- Seidelmann, F. (1918): Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich. *Math. Ann.* **78**, 230–233
- Seifert, H., Threlfall, W. (1934): Lehrbuch der Topologie. Teubner, Leipzig
- Serre, J.-P. (1956): Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier* **6**, 1–42
- Serre, J.-P. (1959): Groupes algébriques et corps de classes. Hermann, Paris
- Serre, J.-P. (1964): Cohomologie galoisienne. Springer, Berlin
- Serre, J.-P. (1979): Local fields. Springer, New York
- Serre, J.-P. (1984): L'invariant de Witt de la forme $\text{Tr}(x^2)$. *Comment. Math. Helvetici* **59**, 651–679
- Serre, J.-P. (1988): Groupes de Galois sur \mathbb{Q} . Astérisque **161–162**, 73–85
- Serre, J.-P. (1990): Construction de revêtements étals de la droite affine en caractéristique p . *C. R. Acad. Sci. Paris* **311**, 341–346
- Serre, J.-P. (1992): Topics in Galois theory. Jones and Bartlett, Boston
- Shabat, G.B., Voevodsky, V.A. (1990): Drawing curves over number fields. Pp. 199–227 in: P. Cartier et al. (eds.): *The Grothendieck Festschrift III*. Birkhäuser, Boston
- Shatz, S.S. (1972): Profinite groups, arithmetic and geometry. Princeton University Press, Princeton
- Shih, K.-y. (1974): On the construction of Galois extensions of function fields and number fields. *Math. Ann.* **207**, 99–120
- Shih, K.-y. (1978): p -division points on certain elliptic curves. *Compositio Math.* **36**, 113–129
- Shiina, Y. (2003a): Braid orbits related to $\text{PSL}_2(p^2)$ and some simple groups. *Tohoku Math. J.* **55**, 271–282
- Shiina, Y. (2003b): Regular Galois realizations of $\text{PSL}_2(p^2)$ over $\mathbb{Q}(T)$. Pp. 125–142 in: K. Hashimoto et al. Eds: *Galois theory and modular forms*. Kluwer
- Shinoda, K. (1974): The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic 2. *J. Fac. Sci. Univ. Tokyo* **21**, 133–159
- Shoji, T. (1974): The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic $p \neq 2$. *J. Fac. Sci. Univ. Tokyo* **21**, 1–17
- Shoji, T. (1982): On the Green polynomials of a Chevalley group of type F_4 . *Comm. Algebra* **10**, 505–543
- Silverman, J.H. (1986): The arithmetic of elliptic curves. Springer, New York
- Simpson, W., Frame, J. (1973): The character tables for $\text{SL}_3(q)$, $\text{SU}_3(q)$, $\text{PSL}_3(q)$, $\text{U}_3(q)$. *Can. J. Math.* **25**, 486–494
- Smith, G.W. (1991): Generic cyclic polynomials of odd degree. *Comm. Algebra* **19**, 3367–3391
- Smith, G.W. (2000): Some polynomials over $\mathbb{Q}(t)$ and their Galois groups. *Math. Comp.* **69**, 775–796
- Smith, L. (1995): Polynomial invariants of finite groups. A.K. Peters, Wellesley
- Sonn, J. (1990): On Brauer groups and embedding problems over function fields. *J. Algebra* **131**, 631–640

- Sonn, J. (1991): Central extensions of S_n as Galois groups of regular extensions of $\mathbb{Q}(T)$. *J. Algebra* **140**, 355–359
- Sonn, J. (1994a): Brauer groups, embedding problems, and nilpotent groups as Galois groups. *Israel J. Math.* **85**, 391–405
- Sonn, J. (1994b): Rigidity and embedding problems over $\mathbb{Q}^{\text{ab}}(t)$. *J. Number Theory* **47**, 398–404
- Spaltenstein, N. (1982): Caractères unipotents de ${}^3D_4(\mathbb{F}_q)$. *Comment. Math. Helvetica* **57**, 676–691
- Speiser, A. (1919): Zahlentheoretische Sätze aus der Gruppentheorie. *Math. Z.* **5**, 1–6
- Springer, T.A. (1998): Linear algebraic groups. Birkhäuser, Basel
- Steinberg, R. (1965): Regular elements of semi-simple algebraic groups. *Publ. Math. IHES* **25**, 49–80.
- Steinberg, R. (1967): Lectures on Chevalley groups. Yale University
- Steinberg, R. (1968): Endomorphisms of linear algebraic groups. *Mem. Amer. Math. Soc.* **80**, Amer. Math. Soc., Providence
- Stichel, D. (2014): Finite groups of Lie type as Galois groups over $\mathbb{F}_q(t)$. *J. Commut. Algebra* **6**, 587–603
- Stöcker, R., Zieschang, H. (1988): Algebraische Topologie. Teubner, Stuttgart
- Stoll, M. (1995): Construction of semiabelian Galois extensions. *Glasgow Math. J.* **37**, 99–104
- Strambach, K., Völklein, H. (1999): On linearly rigid tuples. *J. reine angew. Math.* **510**, 57–62
- Stroth, G. (1998): Algebra. de Gruyter Verlag, Berlin
- Suzuki, M. (1962): On a class of doubly transitive groups. *Ann. of Math.* **75**, 105–145
- Suzuki, M. (1982): Group theory. Springer, Berlin
- Swallow, J.R. (1994): On constructing fields corresponding to the \tilde{A}_n 's of Mestre for odd n . *Proc. Amer. Math. Soc.* **122**, 85–90
- Swan, R.G. (1969): Invariant rational functions and a problem of Steenrod. *Invent. Math.* **7**, 148–158
- Tate, J. (1962): Duality theorems in Galois cohomology. Pp. 288–295 in: *Proc. Int. Congress of Math.*, Stockholm
- Tate, J. (1966): The cohomology groups of tori in finite Galois extensions of number fields. *Nagoya Math. J.* **27**, 709–719
- Thompson, J.G. (1973): Isomorphisms induced by automorphisms. *J. Austral. Math. Soc.* **16**, 16–17
- Thompson, J.G. (1984a): Some finite groups which appear as $\text{Gal}(L/K)$ where $K \leq \mathbb{Q}(\mu_n)$. *J. Algebra* **89**, 437–499
- Thompson, J.G. (1984b): Primitive roots and rigidity. Pp. 327–350 in: M. Aschbacher et al. (eds.) (1984)
- Thompson, J.G. (1986): Regular Galois extensions of $\mathbb{Q}(x)$, Pp. 210–220 in: Tuan Hsio-Fu (ed.): Group theory, Beijing 1984. Springer, Berlin
- Thompson, J.G., Völklein, H. (1998): Symplectic groups as Galois groups. *J. Group Theory* **1**, 1–58

- Tschebotaröw, N.G., Schwerdtfeger, H. (1950): Grundzüge der Galoisschen Theorie. Noordhoff, Groningen
- Uchida, K. (1980): Separably Hilbertian fields. *Kodai Math. J.* **3**, 83–95
- Vila, N. (1985): On central extensions of A_n as Galois groups over \mathbb{Q} . *Arch. Math.* **44**, 424–437
- Völklein, H. (1992a): Central extensions as Galois groups. *J. Algebra* **146**, 144–152
- Völklein, H. (1992b): $GL_n(q)$ as Galois group over the rationals. *Math. Ann.* **293**, 163–176
- Völklein, H. (1993): Braid group action via $GL_n(q)$ and $U_n(q)$ and Galois realizations. *Israel J. Math.* **82**, 405–427
- Völklein, H. (1994): Braid group action, embedding problems and the groups $PGL_n(q)$ and $PU_n(q^2)$. *Forum Math.* **6**, 513–535
- Völklein, H. (1996): Groups as Galois groups. Cambridge University Press, Cambridge
- Völklein, H. (1998): Rigid generators of classical groups. *Math. Ann.* **311**, 421–438
- Wagner, A. (1978): Collineation groups generated by homologies of order greater than 2. *Geom. Dedicata* **7**, 387–398
- Wagner, A. (1980): Determination of the finite primitive reflection groups over an arbitrary field of characteristic not 2, I–III. *Geom. Dedicata* **9**, 239–253; **10**, 183–189; **10**, 475–523
- Walter, J.H. (1984): Classical groups as Galois groups. Pp. 357–383 in: M. Aschbacher et al. (eds.) (1984)
- Ward, H.N. (1966): On Ree's series of simple groups. *Trans. Amer. Math. Soc.* **121**, 62–89
- Washington, L. (1982): Introduction to cyclotomic fields. Springer, New York
- Wehrfritz, B.A.F. (1973): Infinite linear groups. Springer Verlag, Berlin
- Weigel, T. (1992): Generators of exceptional groups of Lie type. *Geom. Dedicata* **41**, 63–87
- Weil, A. (1956): The field of definition of a variety. *Amer. J. Math.* **78**, 509–524
- Weil, A. (1974): Basic number theory. Springer, New York
- Weissauer, R. (1982): Der Hilbertsche Irreduzibilitätssatz. *J. reine angew. Math.* **334**, 203–220
- Wilson, R.A. (2017): Maximal subgroups of sporadic groups. To appear in: *Finite Simple Groups: Thirty Years of the Atlas and Beyond*, AMS Contemporary Mathematics Series, 2017.
- Wolf, P. (1956): Algebraische Theorie der galoisschen Algebren. VEB Deutscher Verlag der Wissenschaften, Berlin
- Yakovlev, A.V. (1964): The embedding problems for fields. *Izv. Akad. Nauk. SSSR* **28**, 645–660 (Russian)
- Yakovlev, A.V. (1967): The embedding problem for number fields. *Izv. Akad. Nauk. SSSR* **31**, 211–224 (Russian) [English transl.: *Math. USSR Izv.* **1**, 195–208 (1967)]
- Zalesskiĭ, A.E., Serežkin, V.N. (1980): Finite linear groups generated by reflections. *Izv. Akad. Nauk SSSR Ser. Math.* **44**, 1279–1307 (Russian) [English transl.: *Math. USSR Izv.* **17** (1981), 477–503]

- Zassenhaus, H. (1958): Gruppentheorie. Vandenhoeck & Ruprecht, Göttingen
- Zywina, D (2015): The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$. Duke Math. J. **164**, 2253–2292.

Index

- ϕ -equivalent matrix, 386
- accompanying Brauer embedding problem, 350
- accompanying embedding problem, 350
- admissible covering, 451
- admissible subset, 451
- affinoid analytic space, 451
- algebraic fundamental group, 4, 187
- almost character, 127
- arithmetic fundamental group, 10, 197
- (full) Artin braid group, 179
- associated F-module, 390
- AV -rigid, 64
- AV -symmetric, 64
- AV -symmetrized irrationality degree, 64
- basic rigidity theorem, 30
- Belyi triple, 102
- braid cycle theorem, 246
- braid orbit theorem, 215
- braid relations, 181
- Brauer embedding problem, 339
- central embedding problem, 288
- characteristic polynomial of an F-module, 389
- clean Belyi function, 17
- closed ultrametric disc, 462
- coherent sheaf, 454
- cohomologically trivial in dimension i , 361
- companion matrix, 390
- comparison theorem of Tate, 367
- compatible family, 467
- concordance obstruction, 364
- concordant embedding problem, 351
- conformal orthogonal group, 111
- conformal symplectic group, 108
- connected rigid analytic space, 452
- convolution, 251
- coroot, 93
- cyclic F-module, 385
- cyclotomic character, 14
- cyclotomic polynomial, 117
- Dedekind criterion, 72
- Dickson algebra, 396
- Dickson invariants, 395
- Dickson polynomial, 395
- disclosed function field of one variable, 14
- duality theorem of Tate, 354
- dualizable F-module, 385
- effective G -module, 392
- embedding problem, 288
- existentially closed, 474
- extension theorem, 67
- F-field, 385
- F-module, 385
- field of definition, 19
- field of definition with group, 19
- field of invariants, 394
- field of moduli, 30
- field restriction of algebraic groups, 441
- finite embedding problem, 288
- finite morphism, 458
- first embedding obstruction, 364
- fixed point theorem, 53
- Frattini embedding problem, 288
- Frattini embedding theorem, 319
- Freiheitssatz of Iwasawa, 295

- Frobenius endomorphism, 385
 Frobenius field, 385
 Frobenius module, 385
 full symmetry group, 31, 63
 fundamental solution matrix, 387
 fundamental system of solutions, 387
- G -compatible family, 469
 G -realization, 34
 G -relative H -invariant, 396
 G -relative Colin Matrix, 399
 G -relative resolvent, 396
 GA-realization, 36
 GAGA for \mathbb{P}^1 , 456
 Galois group of an F-module, 390
 GAR-realization, 302
 general unitary group, 107
 generating s -system, 26
 generic polynomial, 396
 geometric (proper) solution, 289
 geometric embedding problem, 289
 geometric field extension, 8
 geometrically conjugate, 126
 GL-stable tuple, 260
 gluing datum, 451
 gluing of morphisms, 452
 gluing of spaces, 451
 good reduction modulo p , 88
 Green function, 128
 group of geometric automorphisms, 43
- H_s^V -rigid class vector, 212
 Hasse embedding obstruction, 364
 Hasse-Witt-invariant, 332
 Hilbertian field, 287
 Hilbertian set, 287
 homology, 100
 homomorphism ramified in, 480
 (full) Hurwitz braid group, 181
 Hurwitz classification, 27, 198
 hypothesis (H), 254
- induced cover, 461
 irrationality degree, 28
 irreducible Jordan–Pochhammer tuple, 270
- j -th braid orbit genus, 213
 Jordan–Pochhammer tuple, 270
- k -rational class vector, 319
 k -symmetric class vector, 319
 kernel of an embedding problem, 288
- large field, 475
 Lemma of Scott, 260
 Lemma of Speiser, 201
 linear Tscheirnhaus transform, 401
 linearly rigid tuple, 260
 Lusztig series, 126
- \mathcal{M} -section, 469
 mapping class group, 183
 modular Dedekind criterion, 403
 modular Galois theory, 383
 Moore determinant, 387
 Moore matrix, 387
 morphism of rigid analytic spaces, 451
 multiplication with c , 267
- non-split embedding problem, 288
 normalized structure constant, 36
- open ultrametric disc, 462
 orthogonal group, 110
 orthogonal group of minus type, 115
 orthogonal group of plus type, 111
- \wp -stable, 86
 pairwise adjusted, 471
 Pochhammer transform, 251
 Pochhammer transformation, 251
 primitive linear group, 100
 primitive prime divisor, 118
 primitive translate, 55
 profinite Hurwitz braid group, 189
 profinite Riemann existence theorem, 4
 projective profinite group, 294
 proper solution (field) of an embedding problem, 288
 pseudo algebraically closed, 229
 pseudo Steinberg cross section, 424
 pseudo-reflection, 100
 pure Artin braid group, 179
 pure Hurwitz braid group, 181
- q -additive polynomial, 388
 quasi-central element, 132
 quasi-determinant, 115
 quasi- p -group, 484
- r -fold uncomplete product, 179
 r -fold uncomplete symmetric product, 179
 rational class vector, 29
 rational subset, 450
 rationally rigid class vector, 29
 reduced braid orbit genera, 245

- reflection, 100
 regular solution of an embedding problem, 289
 regularity theorem, 212
 relative Reynolds operator, 398
 rigid analytic space, 451
 rigid braid cycle, 247
 rigid braid cycle theorem, 247
 rigid braid orbit theorem, 216
 rigid class vector, 29
 rigid H_s^V -orbit, 48, 64
 rigid H_s^V -orbit, 212
 rigidity defect, 263
 ring of holomorphic functions, 450
 ring of invariants, 394
 robust generating systems, 407
 root, 93
 s -th V -symmetrized braid orbit genus, 235
 Scholz embedding problem, 374
 Scholz extension, 374
 Scholz solution, 374
 Schur multiplier, 226
 second embedding obstruction, 364
 semiabelian group, 299
 semirational class, 41
 shape function, 226
 socle of an ℓ -Galois extension, 375
 solution field of an embedding problem, 288
 solution field of an F-module, 385
 solution of an embedding problem, 288
 solution space of an F-module, 385
 specialization theorem, 224
 sphere relations, 182
 spinor norm, 110
 split embedding problem, 288
 splitting theorem, 13, 196
 stability condition, 260
 Steinberg cross section, 406
 Steinberg endomorphism, 423
 strictly non-degenerate quadratic form, 332
 strong rigidity theorem, 32
 symmetric algebra, 394
 symmetry group, 31, 63
 symplectic group, 108
 Tate algebra, 449
 thick normal subgroup, 185
 transference, 347
 translation theorem, 58
 transvection, 100
 trivial cover, 461
 trivial F-module, 385
 twisted braid orbit theorem, 239
 twisted rigidity theorem, 50
 twisted structure sheaf, 455
 twisted upper bound theorem, 423
 uniform function, 126
 unipotent character, 127
 uniquely liftable, 318
 unirational function field, 200
 universally central embeddable Galois extension, 328
 unramified, 187
 unramified rational place, 223
 upper bound theorem, 391
 V -configuration, 48, 232
 V -rigid class vector, 48
 V -symmetric, 31
 V -symmetrized braid orbit, 211
 V -symmetrized irrationality degree, 31
 wreath extension, 347