GENERIC GALOIS EXTENSIONS FOR FAMILIES OF FINITE GROUPS

Shuvra Gupta

A DISSERTATION

in

Mathematics

Presented to the Faculties of the University of Pennsylvania

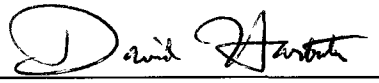
in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

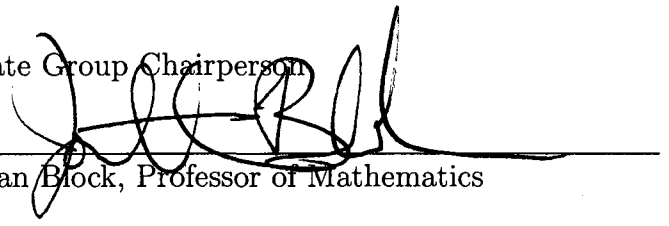
2010

Supervisor of Dissertation



David Harbater, Christopher H. Browne Distinguished Professor in the School of Arts and Sciences

Graduate Group Chairperson



Jonathan Block, Professor of Mathematics

Dissertation Committee
Florian Pop, Professor of Mathematics
David Harbater, Christopher H. Browne Distinguished Professor in the School of Arts and Sciences
Tony Pantev, Professor of Mathematics

Acknowledgments

I would like to take this opportunity to thank several individuals and institutions without whose presence this thesis would not have seen the light of the day.

I would like to thank my advisor, Prof. David Harbater for his patience and for carefully looking through several versions of previous drafts.

I would like to thank Prof. Florian Pop, Prof. Ted Chinburg, Prof. Moshe Jarden, Prof. Joseph Oesterlé, Prof. Daniel Krashen and Prof. David Harari for their intellectual generosity and for the many helpful conversations that I have had the privilege to have with them. My sincere gratitude to Prof. Steve Shatz for being a pillar of support and for being the person to whom one could always turn for both mathematical and non-mathematical advice.

Thanks to Armin Holschbach for his friendship and the several mathematical discussions I have had with him – I could always rely on him to give me a patient hearing even when I churned out mathematical nonsense.

Thanks to Prof. Herman Gluck, for all his help and his infectious enthusiasm.

Thank you to Prof. Ron Donagi and Prof. Tony Pantev for kindly consenting to be on one of my dissertation committees (at short and very short) notices and to Prof. Angela Gibney and Prof. Jonathan Block for being on my Oral Exam Committee.

Life in the department can be lonely but thanks to the wonderful support of our office – Ms. Janet Burns, Ms. Monica Pallanti, Ms. Paula Scarborough and Ms. Robin Toney, things were always lively. Their help was especially important over the last couple of months when things were not going exactly the way I desired. I will definitely remember the many wonderful conversations that I have had with Paula. A very special thanks to Ms. Linda Laws for her very warm welcomes to the library.

I would like to take this opportunity to thank the University of Pennsylvania for its help and support over the past five years, and to the Chennai Mathematical Institute for introducing me to this subject that I have grown to love. In particular, I would like to thank Prof. C. S. Aravinda and Prof. Shiva Shankar for being there for me throughout my undergraduate days.

Thanks to a wonderful host of friends who made sure that I never felt away from home (and to name a few): Aaron, Andrew, Asher, David (Favero), David (Fithian), Dragos, Pranav, Stefano, Toby, Umut and Vittorio.

A very sincere thanks to the late Mr. Todd Craun, Katie and Will for helping me at times when no one else was there to help me.

At times, graduate school can be a very lonely pursuit and keeping oneself grounded is difficult. My thanks to all my rowing friends and coaches at Riley Rowing, Wharton Crew and Bachelors Barge Club, especially Joe and Michael – it is because of the sport and their company that I managed to keep my sanity even when I felt I was losing it.

Thanks to the wonderful city of Philadelphia for being my home-away-from-home and allowing me to enjoy everything it had to offer: its museums, its parks, its wonderful orchestra and so many other delights that makes it Philadelphia.

My thanks to my folks and family, both in the US (especially my cousins in New Jersey) and in India who always prayed for me and supported me even when I lost faith in myself.

However, I have kept the most important word of thanks for the last. Words are not enough to express the gratitude and debt I owe to my parents for bringing me up in spite of all the hardships that lay in their paths, and for protecting and nurturing me to make me who I am today. Everything good that you see in me today is because of them. Of course, my brother Shuva has been much more than a brother – he has been a friend, philosopher, guide, sparring partner(!) and it is because of him that I so cherish my childhood memories. My late grandfather, Sasankha Sekhar Gupta, M. B. E. has been my inspiration because of his personal story, his achievements, his principles and I am sure he is watching every course that I take – this thesis is dedicated to his loving memory.

ABSTRACT

GENERIC GALOIS EXTENSIONS FOR FAMILIES OF FINITE GROUPS

Shuvra Gupta

David Harbater, Advisor

We study the existence of generic Galois extensions for two families of finite groups. We first look at the case of central extensions of symmetric groups and we show that such groups have generic Galois extensions over any field of characteristic zero. One of the crucial tools required in this case is from the theory of quadratic forms, which enables us to solve embedding problems. Rather than solving embedding problems for one field extension at a time, we do this for an entire family of extensions. This is done by using a one-one correspondence between monic polynomials (whose splitting fields are under consideration) and points in affine space. One of the consequences of this result is an if-and-only-if criterion as to when certain families of nonabelian groups have generic Galois extensions. The other family of finite groups in our consideration are dihedral groups. By showing that the problem can be understood by looking at the case of dihedral 2-groups and dihedral groups of order $2n$ for n odd, we reduce the problem to easier problems. We then discuss a proof for the case of $2n$ with n odd. We also give an example for the case of the dihedral group of order 8.

Contents

1 Introduction **1**

1.1 Overview 1

1.2 Outline of thesis 2

1.3 Notation and Some Definitions 2

2 Historical Background **4**

2.1 Noether's Problem 4

2.2 Generic Galois Extensions 6

2.3 Arithmetic Lifting Property 8

3 Embedding Problems and Quadratic Forms **10**

3.1 Group Extensions 10

3.2 Embedding Problems 13

3.3 Trace Forms and Witt Invariants 15

4 Central Extensions of Symmetric Groups **17**

4.1 Reduction Step 19

4.2 Adaptation of work of Mestre 23

4.3 Generic Galois Extensions 30

4.4 Extensions of S_n by 2-groups 40

5 Dihedral groups **52**

5.1 Dihedral 2-groups 52

5.2 General Dihedral Groups 55

6 Further Investigation and Future Plans **60**

Chapter 1

Introduction

1.1 Overview

Given a group G and a field k, David Saltman ([29], Theorem 5.3) showed that a parameter space of all G-Galois extensions of k always exists. If such a parameter space is rational, i.e. birational to projective space of some dimension over k, we say that there is a generic Galois extension for G over k.

More precisely, G is said to have a *generic Galois extension* over k if there exists a purely transcendental extension K/k and a versal G-torsor T over K. In this thesis, I show generic Galois extensions exist for central extensions of A_n and S_n over any field of characteristic zero and show the existence of "generic tractable extensions" (a notion of Saltman that is more general than generic Galois extensions) for dihedral 2-groups over any field of characteristic zero containing

$\sqrt{-1}$. Since an arbitrary dihedral group can be studied in terms of its "2-part" and its "odd part", we use earlier work of Saltman and others to construct some explicit examples. This suggests an approach to constructing generic Galois extensions for all dihedral groups. The above results strengthen earlier results of Jean-François Mestre ([24]), Jack Sonn ([36]), Bernat Plans ([26], [27]), Elena Black ([2], [3]) and Saltman ([29]).

1.2 Outline of thesis

This thesis is organised in the following way: In Chapter 2 we present historical background; in Chapter 3, we discuss some of the existing methods and their adaptations that we use in our proofs; in Chapter 4, we discuss our proof showing the existence of generic Galois extensions for central extensions of symmetric groups; in Chapter 5, we discuss our results related to the existence of generic Galois extensions for dihedral groups and finally in Chapter 6, we discuss some possible future research plans.

1.3 Notation and Some Definitions

- $\mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group of order n written additively.
- C_n denotes the cyclic group of order n written multiplicatively.
- S_n denotes the symmetric group acting as permutations of a set of n objects.

The alternating group, A_n denotes the subgroup of all even permutations.

- $D_m \cong \langle x, y | x^m = 1, y^2 = 1, xy = yx^{-1} \rangle$ denotes the dihedral group of order $2m$.
- i denotes an imaginary square root of -1.
- ζ_q denotes a primitive qth root of unity.
- For a group G, we denote by G' the first derived (or commutator) subgroup of G.
- For a field k, the absolute Galois group $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ will be denoted by G_k.

Chapter 2

Historical Background

In this chapter, we place the problems that we are interested in in historical context and also explain how they are related to other problems.

2.1 Noether's Problem

One of the first approaches to the Inverse Galois Problem was to first realise a finite group G over $\mathbb{Q}(t)$, or more generally $\mathbb{Q}(t_1, t_2, \ldots, t_n)$, the field of rational functions in several variables, and then use Hilbert's Irreducibility Theorem ([35], Chap. 3) to specialise to an extension over $\mathbb{Q}$ with the same Galois group.

Proceeding along these lines, Emmy Noether in 1913 asked the following question which is now known as Noether's Problem: if G is a finite group and V a faithful representation of G over k, then is the field of invariant rational functions $k(V)^G$ rational over k?

In particular, let G act faithfully by permutations on a finite set of indeterminates $x_1, \ldots, x_n$. Let G act on $k(x_1, \ldots, x_n)$ by acting trivially on k and by permuting the variables x_i. Then, is the field of invariants $k(x_1, \ldots, x_n)^G$ purely transcendental over k? If the answer to the above question is positive for a group and if k is Hilbertian (e.g. $\mathbb{Q}$), then using Hilbert's Irreducibility Theorem, G can be realised as a Galois group over k. For example, let $G = S_n$ act on $\mathbb{Q}(x_1, \ldots, x_n)$ by acting trivially on $\mathbb{Q}$ and permuting the indices of the indeterminates. Then we know that the field of invariants is indeed purely transcendental and is generated over $\mathbb{Q}$ by the elementary symmetric polynomials σ_i in n variables. Fischer ([11]), Voskresenskii ([40]), Endo–Miyata ([10]) and others have shown positive answers to Noether's Problem in other cases.

However, the answer to the question is not always in the positive. Richard Swan ([38]) showed that $\mathbb{Q}(x_1, \ldots, x_n)^G$ is not purely transcendental when G is a cyclic group of order n for $n = 47,\ 113$ and 233. Later, Hendrik Lenstra ([22]) showed that the answer is negative for $G = \mathbb{Z}/8\mathbb{Z}$ with $k = \mathbb{Q}$. He also gave a criterion for the problem to have a positive answer for an abelian group G. In the process, he showed that any group containing $\mathbb{Z}/8\mathbb{Z}$ has a negative answer to Noether's Problem over $\mathbb{Q}$. Negative examples over algebraically closed fields were later given by Saltman ([30]) and Emmanuel Peyre ([25]).

2.2 Generic Galois Extensions

One of the conseqences of a positive answer to Noether's Problem for a group G over a Hilbertian field k was not just the realisability of G as a Galois group over k but also the "parametrisation" of all G-Galois extensions of k. In 1980, Saltman defined ([29], Definition 1.1) the notion of generic Galois extensions. Using them, he gave a different explanation as to why groups containing $\mathbb{Z}/8\mathbb{Z}$ gave negative answers to Noether's problem. We recall that an extension of rings S/R is said to be *Galois* with Galois group G if $S^G = R$ and $S \otimes_R S \cong \oplus_{g \in G} S$. The geometric interpretation of the second condition is that as a morphism of schemes, Spec $S \to$ Spec R is étale. We say a G-Galois extension of rings S/R is a generic Galois extension for G over k if R is of the form $k[x_1, \ldots, x_n][\frac{1}{s}]$ where $s \in k[x_1, \ldots, x_n] \backslash \{0\}$, and for any G-Galois extension (of algebras) L/K where K is some field extension of k, there exists a ("specialisation") map $\phi : R \to K$ such that $L \cong S \otimes_\phi K$ with the isomorphism respecting the G-action. The polynomial s is inverted to remove the branch locus of the map so that our extension becomes étale and hence Galois. As an example, we can consider the space of $\mathbb{Z}/2\mathbb{Z}$ extensions of a field k of characteristic not equal to 2. Any quadratic extension of k is of the form $k(\sqrt{a})$ where $a \in k^\times$ (because we are now considering Galois extensions of rings). So, here our parameter space is $\mathbb{A}^1_k \backslash \{0\}$ which is rational.

Saltman ([29], Theorem 5.1) showed that if a group G has a positive answer

to Noether's Problem over a field k, then there exists a generic Galois extension for G over k. He also showed that if there exists a generic Galois extension for G over k, then the Grünwald–Wang theorem (see [42], p. 479) holds for G over k; i.e. in the above notation $H^1(K,G) \to \prod_{i=1,\ldots,m} H^1(K_i,G)$ is surjective where $K_1,\ldots,K_m$ are the completions of K with respect to m inequivalent real-valued valuations of K. So, let S/R be a generic Galois extension for G over k as above, and K/k an extension. Let $K_1,\ldots,K_m$ denote the completions of K with respect to its inequivalent real valued valuations. Now if for each $i = 1,\ldots,m$, there is a G-Galois extension L_i/K_i, then there is a G-Galois extension L/K. Thus, using Shianghaw Wang's ([41]) counterexample reference to Grünwald's Theorem, which showed that the map $H^1(\mathbb{Q},\mathbb{Z}/8\mathbb{Z}) \to \prod_p H^1(\mathbb{Q}_p,\mathbb{Z}/8\mathbb{Z})$ is not surjective, Saltman deduced that any abelian group containing $\mathbb{Z}/8\mathbb{Z}$ will yield a negative answer to Noether's Problem over $\mathbb{Q}$, and that any abelian group not containing an element of order 8 has a generic Galois extension over $\mathbb{Q}$. As a consequence of Swan's earlier result that $\mathbb{Z}/47\mathbb{Z}$ has a negative answer to Noether's Problem over $\mathbb{Q}$, he had thus shown that the existence of a generic Galois extension for a group G over a field k is strictly weaker than a positive answer to Noether's Problem for G over k.

2.3 Arithmetic Lifting Property

In 1954, Shafarevich showed that every solvable group can be realised as a Galois group over $\mathbb{Q}$. (His proof was incomplete for the case of 2-groups but he outlined a method to complete the proof and it was completed by Alexander Schmidt and Kay Wingberg in [37] .) The obvious next question was to think about the realisability of simple groups. Until very recent work of Khare-Larsen-Savin (of which I will talk about more in §6), the principal way to realise simple groups was in the following fashion. By Riemann's Existence Theorem, we know every group can be realised as a Galois group over $\mathbb{P}^1_{\mathbb{C}}$. The Galois extension can then be descended to an extension over $\mathbb{P}^1_{\mathbb{Q}}$ by a method called *rigidity*, and then using Hilbert Irreducibility Theorem, we can realise the group as a Galois group over $\mathbb{Q}$. However, for rigidity to work for all (simple) groups, one has to know that every (simple) group G can be realised as a Galois group of a regular extension $L/\mathbb{Q}(T)$ i.e. $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$. This prompted Sybilla Beckmann ([1]) to ask whether given a group G, every G-Galois extension $L/\mathbb{Q}$ arises as a specialisation of some regular extension of $\mathbb{Q}(T)$ or equivalently, some absolutely irreducible Galois branched covering of $\mathbb{P}^1_{\mathbb{Q}}$. The above question can also be asked for fields k other than $\mathbb{Q}$. If the question has an affirmative answer, we say G satisfies the *Arithmetic Lifting Property* over k. Beckmann answered it in the positive for abelian groups and symmetric groups and Elena Black ([2]) answered it in the positive for dihedral groups of order $2n$ where n is odd. In [3] (Proposition 1.2), she showed that if

there is a generic Galois extension for G over k, then G satisfies the Arithmetic Lifting Property over k. The existence of generic Galois extensions is a strictly stronger property because $\mathbb{Z}/8\mathbb{Z}$ does not have a generic Galois extension over $\mathbb{Q}$ whereas it does satisfy the Arithmetic Lifting Property.

An interesting result of Pierre Dèbes ([6], Proposition 1.2) relates the Arithmetic Lifting Property to the Regular Inverse Galois Problem. For a given group G and a field k, he shows that if G satisfies the Arithmetic Lifting Property over every regular extension of $k(T)$, then G is a Galois group of a regular extension $L/k(T)$.

Chapter 3

Embedding Problems and Quadratic Forms

3.1 Group Extensions

Definition 3.1.1. An extension $1 \to A \to \widetilde{G} \to G \to 1$ of G by A is *central* if $A \subset Z(\widetilde{G})$, where $Z(\widetilde{G})$ denotes the centre of $\widetilde{G}$. Further, we say that the extension is *stem* if $A \subset Z(\widetilde{G}) \cap \widetilde{G}'$.

Definition 3.1.2. The *Schur multiplier* of a finite group G is defined as $H_2(G, \mathbb{Z})$, the second homology group of G with coefficients in the integers.

If the group G is finite and one considers only stem extensions, then there is a largest size for such a group $\widetilde{G}$, and for every $\widetilde{G}$ of that size the subgroup A is isomorphic to the Schur multiplier of G. If the finite group G is moreover perfect,

then $\widetilde{G}$ is unique up to isomorphism and is itself perfect. Such $\widetilde{G}$ are often called *universal perfect central extensions* (or more briefly, *universal central extension*) of G, or *covering group* (as it is a discrete analog of the universal covering space in topology). We note that there is no largest central extension because we always have the central extension $1 \to A \to G \times A \to G \to 1$ for any finite abelian group A and so, this gives us a central extension of arbitrary size.

Stem extensions have the nice property that any lift of a generating set of G is a generating set of $\widetilde{G}$. If the group G is presented in terms of a free group F on a set of generators, and a normal subgroup R generated by a set of relations on the generators, so that $G \cong F/R$, then the covering group itself can be presented in terms of F but with a smaller normal subgroup S such that $\widetilde{G} \cong F/S$.

We shall now discuss a bit about extensions of A_n and S_n and in our discussion of the cohomology of A_n and S_n, we will closely follow the notation of [35], §9.1.3.

The cohomology group $H^2(G, A)$ classifies equivalence classes of extensions $1 \to A \to \widetilde{G} \to G \to 1$ of G by A. It is easy to see that

$$\begin{aligned} H^1(S_n, \mathbb{Z}/2\mathbb{Z}) &\cong \mathbb{Z}/2\mathbb{Z} \text{ for } n \geq 2, \\ H^2(S_n, \mathbb{Z}/2\mathbb{Z}) &\cong \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \text{ for } n \geq 4. \end{aligned}$$

The non-trivial element in $H^1(S_n, \mathbb{Z}/2\mathbb{Z})$ is the signature homomorphism

$$\epsilon_n : S_n \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

The cohomology group $H^2(S_n, \mathbb{Z}/2\mathbb{Z})$ $(n \geq 4)$ has a $\mathbb{Z}/2\mathbb{Z}$-basis given by $\epsilon_n \cdot \epsilon_n$ (where $\cdot$ corresponds to the cup product in cohomology) and an element s_n where

s_n corresponds to the central extension $1 \to \mathbb{Z}/2\mathbb{Z} \to \widetilde{S_n} \to S_n \to 1$ that is characterised by the following two properties:

1. A transposition in S_n lifts to an element of order 2 in $\widetilde{S_n}$, and
2. A product of two disjoint transpositions lifts to an element of order 4 in $\widetilde{S_n}$.

The element $\epsilon_n \cdot \epsilon_n$ corresponds to the extension $S_n' \cong S_n \times_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/4\mathbb{Z}$ which can similarly be characterised by the following two properties:

1. A transposition in S_n lifts to an element of order 4, and
2. A product of two disjoint transpositions lifts to an element of order 2.

Thus, the four possible extensions of S_n by $\mathbb{Z}/2\mathbb{Z}$ are $S_n \times \mathbb{Z}/2\mathbb{Z}$ (corresponding to the identity in $H^2(S_n, \mathbb{Z}/2\mathbb{Z})$), S_n', $\widetilde{S_n}$ and $\widehat{S_n}$, where $\widehat{S_n}$ is characterised by the following two properties:

1. A transposition in S_n lifts to an element of order 4, and
2. A product of two disjoint transpositions lifts to an element of order 4.

The inclusion $A_n \hookrightarrow S_n$ gives rise to a restriction map $H^1(S_n, \mathbb{Z}/2\mathbb{Z}) \to H^1(A_n, \mathbb{Z}/2\mathbb{Z})$ and the image of ϵ_n under this restriction map is zero. The cohomology group $H^2(A_n, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (for $n \geq 4$) and is generated by a_n, the image of s_n under the restriction map $H^1(S_n, \mathbb{Z}/2\mathbb{Z}) \twoheadrightarrow H^1(A_n, \mathbb{Z}/2\mathbb{Z})$. The element a_n corresponds to $\widetilde{A_n}$, the unique non-trivial extension $1 \to \mathbb{Z}/2\mathbb{Z} \to \widetilde{A_n} \to A_n \to 1$. More concretely, it can be realised as the group which fits in the

following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \widetilde{A_n} & \longrightarrow & A_n & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathrm{Spin}(n) & \longrightarrow & SO(n) & \longrightarrow & 1 \end{array}$$

where $A_n \hookrightarrow SO(n)$ by considering elements of A_n as permutation matrices and $\mathrm{Spin}(n)$ is the double cover of $SO(n)$. The group $\widetilde{A_n}$ is an index 2 subgroup of $\widetilde{S_n}$.

3.2 Embedding Problems

For any field k, let G_k denote its absolute Galois group. A Galois extension K/k with Galois group G is then determined by an epimorphism $\phi : G_k \to G$ with $\ker(\phi) = \mathrm{Gal}(\overline{k}/K)$. Given a group extension $1 \to A \to \widetilde{G} \xrightarrow{\pi} G \to 1$, we can ask about the existence of a homomorphism $\tilde{\phi} : G_k \to \widetilde{G}$ lifting ϕ such that the following diagram commutes.

$$\begin{array}{ccccccccc} & & & & & & G_k & & \\ & & & & & \overset{\tilde{\phi}}{\swarrow} & \downarrow \phi & & \\ 1 & \longrightarrow & A & \longrightarrow & \widetilde{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

This is called the *embedding problem* $\mathrm{Emb}(\phi, \pi)$ given by ϕ and π. The embedding problems is also sometimes referred to as $\mathrm{Emb}(K/k, \pi)$. The homomorphism $\tilde{\phi}$ is called a *(weak) solution* to the embedding problem $\mathrm{Emb}(\phi, \pi)$ and the corresponding field $L := \overline{k}^{\ker(\tilde{\phi})}$ a *solution field* of $\mathrm{Emb}(\phi, \pi)$. We note that $\tilde{\phi}$ determines L but not vice-versa. If $\tilde{\phi}$ is a surjection, then $\tilde{\phi}$ and L are called a *proper solution* and a

proper solution field respectively. In the latter case, we can "embed" our G-Galois extension K/k in the $\widetilde{G}$-Galois extension L/k. The obstruction to the existence of a weak solution is the pullback $\phi^*(\gamma) \in H^2(G_k, A)$, where $\gamma \in H^2(G, A)$ is the class of the group extension $\widetilde{G}$. Let γ denote the cohomology class in $H^2(G, A)$ corresponding to the group extension above and let ϕ be as above. Then, it is easy to see that the embedding problem $\mathrm{Emb}(\phi, \pi)$ has a solution if and only if the image $\phi^*(\gamma)$ of γ, under the pullback $\phi^* : H^2(G, A) \to H^2(G_k, A)$, is trivial in $H^2(G_k, A)$. The element $\phi^*(\gamma)$ is often referred to as the *obstruction* to the embedding problem because it is the obstruction to lifting the homomorphism ϕ to $\tilde{\phi}$.

As an example, we can look at the $\mathbb{Z}/2\mathbb{Z}$-Galois extension $\mathbb{Q}(i)/\mathbb{Q}$. It can be shown that this extension cannot be embedded in a $\mathbb{Z}/4\mathbb{Z}$-Galois extension of $\mathbb{Q}$. One argument using class field theory is that the maximal abelian extension ramified only at 2 has group $\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ with the $\mathbb{Z}/2\mathbb{Z}$ factor obtained by adjoining i and the $\mathbb{Z}_2$-factor coming from taking 2-power roots of 5. In fact, using an easy argument from quadratic forms, we can show that a $\mathbb{Z}/2\mathbb{Z}$-Galois extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ can be embedded in a $\mathbb{Z}/4\mathbb{Z}$-Galois extension if and only if a is the sum of two squares in $\mathbb{Q}$.

3.3 Trace Forms and Witt Invariants

A *quadratic form* of dimension n over a field k is a homogeneous polynomial f of degree 2 in n variables over k.

Let E be an étale algebra of finite rank n over k, i.e. a product of separable field extensions of k with the sum of the degrees of the extensions equalling n. Étale algebras E of rank n are in bijective correspondence with conjugacy classes of homomorphisms $\phi : G_k \to S_n$. The correspondence is as follows: given E, let $h(E)$ be the set of k-algebra homomorphisms from E to k^{sep}. The set $h(E)$ has cardinality n and the natural action of G_k gives a permutation action on $h(E)$, thus giving us the desired homomorphism $\phi : G_k \to S_n$ (after a choice of identification of $h(E)$ with $\{1, 2, \ldots, n\}$). Conversely, E can be constructed as the twist of the split algebra $k^n = k \times k \times \cdots \times k$ by the 1-cocycle $\phi : G_k \to S_n = \text{Aut}(k^n)$.

For any such E, the *trace form* q_E is the non-degenerate quadratic form on E defined by $q_E(x) = \text{Tr}_{E/k}(x^2)$.

Let q be a non-degenerate quadratic form over k ($\text{char}(k) \neq 2$) of rank $n \geq 1$. By choosing an appropriate basis, we can write $q = \sum_{i=1}^{n} \alpha_i X_i^2$, with $\alpha_i \in k^\times$. Then, we define the Stiefel-Whitney classes w_i as the i-th elementary symmetric

polynomial in the (α_j) computed in the commutative ring $H^*(G_k, \mathbb{Z}/2\mathbb{Z})$:

$$\begin{aligned} w_0 &= 1, \\ w_1 &= \sum_i (\alpha_i) = (\alpha_1 \cdots \alpha_n) = \text{Discriminant}(q), \\ w_2 &= \sum_{i<j} (\alpha_i) \cdot (\alpha_j), \\ &\vdots \\ w_n &= (\alpha_1) \cdot (\alpha_2) \cdot \cdots \cdot (\alpha_n), \\ \text{and } w_i &= 0 \text{ if } i < 0 \text{ or } i > n. \end{aligned}$$

It is known that these cohomology classes w_i are indeed invariants of q; i.e. they are independent of our choice of α_i, and the second Stiefel-Whitney class w_2 is called the Hasse-Witt invariant.

Chapter 4

Central Extensions of Symmetric Groups

Hilbert in the early 1900s showed that the alternating groups A_n and the symmetric groups S_n could be realised as Galois groups over any field of characteristic zero. To do this, he first showed that S_n has a positive answer to Noether's Problem over any field of characteristic zero. He then showed that A_n could be realised by studying the ramification behaviour of S_n-Galois extensions. However, the answer to the Noether problem for alternating groups A_n is not known for $n > 5$. The A_5 case was shown by Takashi Maeda ([23]) and his proof relies on some explicit combinatorial facts about the linear representations of A_5.

In [24], Mestre used a theorem of Serre which we mention later (Theorem 4.2.1) to show that the group $\widetilde{A_n}$ can be realised as a regular Galois group over $\mathbb{Q}(T)$.

Leila Schneps ([32]) used his work to explicitly construct some $\widetilde{A_n}$-Galois regular extensions of $\mathbb{Q}(T)$. Mestre's argument can in fact be extended to show that $\widetilde{A_n}$ satisfies the Arithmetic Lifting Property over $\mathbb{Q}$. Building on Mestre, Sonn ([36]) showed that any central extension of S_n can be realised as a Galois group of a regular extension of $\mathbb{Q}(T)$, and Plans ([26]) showed that central extensions of A_n satisfy the Arithmetic Lifting Property. The goal of this chapter is to prove the existence of generic Galois extensions for central extensions of S_n over any field of characteristic zero, provided the kernel has a generic extension. One of the consequences of this is that such central extensions of symmetric groups can be realised as Galois groups of regular extensions of $\mathbb{Q}(T)$, and hence they can be realised as Galois groups of infinitely many pairwise disjoint extensions of $\mathbb{Q}$. Our approach will be very similar to the approach taken by Plans in **??**.

We prove:

Theorem 4.0.1. *Let k be a field of characteristic zero and let $1 \to A \to G \xrightarrow{\pi} S_n \to 1$ be a finite central extension. If A has a generic Galois extension over k, then so does G.*

Corollary 4.0.2. *For any natural number n, the groups S_n', $\widetilde{S_n}$ and $\widehat{S_n}$ (cf. 3.1) have generic Galois extensions over any field k of characteristic zero.*

Proof. Recall that the kernel of the map $G \to S_n$ when G is one of S_n', $\widetilde{S_n}$ or $\widehat{S_n}$ is $\mathbb{Z}/2\mathbb{Z}$, which has a generic Galois extension over k (e.g., by [29], Theorem 2.1). Hence, S_n', $\widetilde{S_n}$ or $\widehat{S_n}$ have generic Galois extensions for all n. □

Our method of proof of Theorem 4.0.1 will be as follows:

Step 1: We will show that any G as above can be decomposed as a direct product of two groups G_1 and G_2 where G_1 is a central extension of S_n by a 2-group and G_2 is an odd order subgroup of A.

Step 2: Using an inductive argument, we will prove the above theorem for groups of the form G_1.

Step 3: We will show that the product of two groups having generic Galois extensions has a generic Galois extension and use that to prove our theorem.

The proof of Step 1 will be done in Section 4.1 and the proof of Steps 2 and 3, and hence Theorem 4.0.1 will be done in Section 4.4. We will also give some examples and consequences of the theorem in §4.4.

4.1 Reduction Step

We first show that it is enough to consider the case when the kernel A is a 2-group. The proof is motivated by ([21], Theorem 6), where they show that the realisability of every finite central extension of S_n as a Galois group over a number field k can be reduced to the case where the Galois groups are certain (central) extensions of S_n by 2-groups. Our goal is to express G as a product $G_1 \times G_2$ where G_1 is an extension of S_n by a 2-group and G_2 is a subgroup of A.

Proposition 4.1.1. *Let* $1 \to A \to G \xrightarrow{\pi} S_n \to 1$ *be a central extension of* S_n *by*

a group A. Then G can be expressed as a product $G_1 \times G_2$ where G_1 is a central extension of S_n by a 2-group and G_2 is an odd order subgroup of A.

Proof. Let $B \subset A$ be the unique Sylow 2-subgroup of A. We claim that there exists $g \in G$ such that $g^2 \in B$ and such that $\langle \pi(g) \rangle \cdot A_n = S_n$. In other words, we are asking for a $g \in G$ such that $\pi(g)$ is an odd element of S_n and $\pi(g)$ has order 2 in S_n. Since π is a surjection, we know there exists an element $h \in G$ such that $\pi(h)$ is a transposition. Now, the order of h must be even and hence is of the form $2^a \cdot b$ where b is odd and $a \geq 1$. It is easy to see that $g = h^b$ satisfies the claim.

Let us define the subgroup $K \subset G$ as follows: $K = B \cdot \langle g \rangle \cdot G' = \{b \cdot g^i \cdot h | b \in B, i \in \mathbb{Z}, h \in G'\} \subset G$. The product $B \cdot \langle g \rangle$ is a subgroup as B is central and then $B \cdot \langle g \rangle \cdot G'$ is a subgroup because G' is normal. We claim that $K \cap A = B$. We notice that B is a normal subgroup of G as it is central, and so we consider the following exact sequence obtained by taking quotients by B:

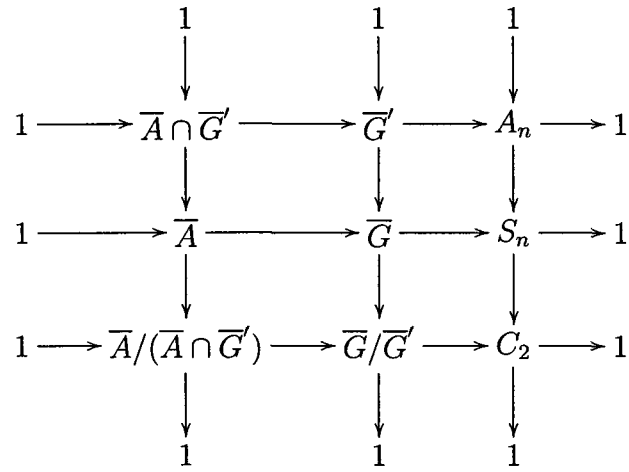
$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\pi} & S_n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & A/B & \longrightarrow & G/B & \longrightarrow & S_n & \longrightarrow & 1 \\
 & & \| & & \| & & \| & & \\
1 & \longrightarrow & \overline{A} & \longrightarrow & \overline{G} & \longrightarrow & S_n & \longrightarrow & 1
\end{array}$$

We notice that the bottom horizontal sequence gives us a central extension of S_n with the added condition that the kernel has odd order. Let $\overline{K}$ and $\overline{B} \cong \langle 1 \rangle$ denote the images of K and B respectively under the vertical map from $G \twoheadrightarrow \overline{G} = G/B$. Also, let $\overline{g}$ be the image of g under the above map. We consider the short

exact sequence

$$1 \to \overline{A} \to \overline{G} \to S_n \to 1$$

and then take quotients by $\overline{G}'$. Thus, we get the following commutative diagram:



The top horizontal exact sequence gives us a central extension of A_n, and by our earlier discussion $\overline{A} \cap \overline{G}'$ is contained in the Schur multiplier (cf. Definition 3.1.2) of A_n. By [14], p. 152, the Schur multiplier of A_n is a 2-group. But as $\overline{A} \cap \overline{G}' \subset \overline{A}$, we have $|\overline{A} \cap \overline{G}'|$ is odd. Therefore, $\overline{A} \cap \overline{G}' = \{1\}$. Also $\overline{K} = \overline{B} \cdot \langle \overline{g} \rangle \cdot \overline{G}' \cong \langle \overline{g} \rangle \cdot \overline{G}'$ is a subgroup of $\overline{G}$ because $\overline{G}'$ is normal; and it has cardinality $2 \cdot |\overline{G}'|$ because $\overline{g}$ has order 2 and $\langle \overline{g} \rangle \cap \overline{G}' = \{1\}$. Furthermore, $\overline{K} \cap \overline{A} = (\langle \overline{g} \rangle \cdot \overline{G}') \cap \overline{A} = \{1\}$ because $\langle \overline{g} \rangle \cap \overline{A} = \{1\}$ (since $\overline{g}$ maps to an odd element in S_n under π and $\overline{A}$ is in the kernel of π) and our earlier result $\overline{A} \cap \overline{G}' = \{1\}$. Since, $\overline{K} \cap \overline{B} \subset \overline{K} \cap \overline{A}$, we have $\overline{K} \cap \overline{B} = \{1\}$ and hence $K \cap A = B$.

Now, we can write $A \cong B \times C$ as a product where C is the odd part of the abelian group A because A is abelian and $|B|$ and $|C| = [A : B]$ are relatively

prime. Here, $K \cdot C \subset G$ is a subgroup because C is central, and hence normal. We want to show that $C \cdot K = G$ and moreover, $C \times K = G$.

First, we have

$$\begin{aligned} C \cap K &= (C \cap A) \cap K \\ &= C \cap (A \cap K) \\ &= C \cap B \\ &= \{1\}. \end{aligned}$$

Also,

$$\begin{aligned} C \cdot K &= C \cdot B \cdot \langle g \rangle \cdot G' \\ &= A \cdot \langle g \rangle \cdot G'. \end{aligned}$$

Now, we know the map $\langle g \rangle \cdot G' \to S_n$ is surjective, i.e. every class in G/A has a representative in $\langle g \rangle \cdot G'$, we get that

$$\begin{aligned} C \cdot K &= A \cdot \langle g \rangle \cdot G' \\ &\cong A \times G/A \end{aligned}$$

That shows that $C \cdot K$ has cardinality the same as $|A \times G/A| = |G|$; but since $C \cdot K \subset G$, we get that $C \cdot K = G$.

Using this with the fact that $C \cap K = \{1\}$ and the fact that C is central in G, we get that $G \cong C \times K$. Now taking $G_1 = K$ and $G_2 = C$ concludes the proof of the proposition. $\square$

4.2 Adaptation of work of Mestre

We recall from §3.1 the element $s_n \in H^2(S_n, \mathbb{Z}/2\mathbb{Z})$ corresponding to a central extension of S_n. Then, Jean-Pierre Serre ([33], Théorème 1) proved the following:

Theorem 4.2.1. *Let E be an étale k-algebra of rank n and discriminant d associated to a homomorphism $\phi : G_k \to S_n$, and let q_E denote the trace form of E. Then:*

1. $w_1(q_E) = \phi^*(\epsilon_n)$, *and*
2. $w_2(q_E) = \phi^*(s_n) + (2) \cdot (d)$.

One of the consequences of the above theorem is that it relates the obstruction to the embedding problem, $\phi^*(s_n)$ to the discriminant and Hasse-Witt invariant of the trace form.

Suppose $G = \phi(G_k)$ is contained in A_n; i.e. d is a square. Then, by the above theorem, $w_1(q_E) = 0$ and $w_2(q_E) = \phi^*(a_n)$, where $\phi^*(a_n)$ is the obstruction (cf. §3.2) to lifting the homomorphism $G_k \to A_n$ to a homomorphism $G_k \to \widetilde{A_n}$. Thus the homomorphism $\phi : G_k \to A_n$ lifts to a homomorphism $G_k \to \widetilde{A_n}$ if and only if $w_2(q_E) = 0$. So, we have the following corollary:

Corollary 4.2.2. *An extension E/k of degree n with Galois group A_n can be embedded in an $\widetilde{A_n}$-extension if and only if $w_2(q_E) = 0$.*

Mestre ([24], Théorème 2) used this to show the following result:

Theorem 4.2.3. *The group $\widetilde{A_n}$ can be realised as a Galois group of a regular extension of $\mathbb{Q}(T)$ for all n.*

Definition 4.2.4. Let k be a field and $k(T)$ be the function field in one variable over k. We say a quadratic form q over $k(T)$ is *constant* (or *independent of* T) if it is $k(T)$-equivalent to a quadratic form over k.

More generally, let k be a field and let $K = k(T)$ be the corresponding rational function field. Further, let n be a positive integer relatively prime to the characteristic of k. Let M be a G_k-module such that n annihilates M, i.e. $nM = 0$ and assume that the canonical homomorphism $H^i(k, M) \to H^i(K, M)$ is injective. An element of $H^i(K, M)$ is said to be *constant* if it belongs to $H^i(k, M)$.

Let n be an odd positive integer greater than 1 and let A be the polynomial ring $\mathbb{Z}[A_1, A_2, \ldots, A_n]$ with $A_1, A_2, \ldots, A_n$ formal parameters, let K the quotient field of A. Let $\overline{K}$ be the algebraic closure of K and let $P(X)$ be the polynomial $X^n + A_1X^{n-1} + \cdots + A_{n-1}X + A_n \in K[X]$.

Keeping the same notation as above, Mestre proved the following proposition (Proposition 1) in [24]:

Proposition 4.2.5. *(a) There exists a unique primitive polynomial $Q \in A[X]$ of degree less than or equal to $n-1$ such that there exists a polynomial $R \in A[X]$ satisfying the relation $PQ' - P'Q = R^2$. The polynomials Q and R are of degree $n-1$, and have no common factor in $A[X]$. The polynomial R is defined up to sign and its roots $r_1, r_2, \ldots, r_{n-1} \in \overline{K}$ are distinct.*

(b) Moreover, let $F_T(X) \in A[T][X]$ *be the polynomial defined by* $F_T(X) = P(X) - T \cdot Q(X)$ *where* T *is a new indeterminate. The discriminant of* $F_T(X)$ *is equal to* $\Delta(P) \cdot S(T)^2$ *where* $S(T)$ *is an element of* $A[T]$ *of degree* $n-1$ *with simple roots. For* $1 \leq i \leq n-1$, *let* $T_i = \frac{P(r_i)}{Q(r_i)}$. *The values* T_i *are pairwise distinct, and are the roots of* S. *The polynomial* $F_{T_i}(X)$ *admits* r_i *as a triple root, and its other roots are simple.*

Definition 4.2.6. Let $v_0, t_1, \ldots, t_n, w_0, u_1, \ldots, u_n$ be algebraically independent over $\mathbb{Z}$ and let

$$\begin{aligned} f(X) &= v_0(X-t_1)\cdots(X-t_n) &&= v_0X^n + \cdots + v_n, \\ g(X) &= w_0(X-u_1)\cdots(X-u_m) &&= w_0X^m + \cdots + w_m. \end{aligned}$$

be two polynomials. Then, the *resultant* of $f(X)$ and $g(X)$ is defined to be

$$\mathrm{Res}(f,g) = v_0^m w_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(t_i - u_j).$$

Remark 4.2.7. Given a field k and two polynomials $f(X), g(X) \in k[X]$, it seems *a priori* that the resultant of the two lies in an algebraic closure $\overline{k}$ of k but it can be shown that the resultant in fact, lies in k. One way to do so is by using an equivalent definition of the resultant (cf. [5], §3.3.2) which expressses it as the determinant of a matrix whose entries are the coefficients of the polynomials and hence, it follows from that the $\mathrm{Res}(f,g) \in k$.

Another way to see it is using Galois Theory. If the characteristic of k is zero, then the splitting field of $f(X) \cdot g(X)$ is Galois, and the Galois group of the

splitting field of acts on the resultant and leaves it invariant. Hence, the resultant lies in k.

If the characteristic of k is $p > 0$, then we need to consider the additional case of purely inseparable extensions. If one of the polynomials has a factor of the form $X^p - \alpha = (X - \alpha^{\frac{1}{p}})^p$ with $\alpha \in K$, then the resultant will have a factor of the form $(\alpha^{\frac{1}{p}} - \beta)^p = \alpha - \beta^p$ which again ensures that the resultant lies in k.

Let $P(X), Q(X), R(X)$ and $S(T)$ be as in Proposition 4.2.5. Let $J(A_1, A_2, \ldots A_n)$ denote the product of the leading coefficients of $S(T)$ and $\Delta(R) \cdot \Delta(S) \cdot \mathrm{Res}(Q, R)$. We note that by Proposition 4.2.5(a), $Q(X)$ and $R(X)$ have no common roots, $R(X)$ has distinct roots; and by Proposition 4.2.5(b), $S(T)$ has distinct roots. Hence, $J(A_1, A_2, \ldots A_n)$ is a nonzero element of A.

Remark 4.2.8. $P_\alpha(X)$ is the polynomial in $k[X]$ obtained from $P(X)$ by specialising A_i to $\alpha_i \in k$. Similarly, Q_α, R_α and S_α are the specialisations of Q, R and S. Also $F_{T,\alpha}(X) = P_\alpha(X) - T \cdot Q_\alpha(X)$.

Let k be a field of characteristic zero. Then, along the lines of Mestre's definition of H-general, we can define:

Definition 4.2.9. ([24], p. 488) If $\alpha_1, \alpha_2, \ldots, \alpha_n \in k$, the polynomial $P_\alpha(X) = X^n + \alpha_1 X^{n-1} + \cdots \alpha_n$ is called *J-general* if $J(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$, where $J(A_1, A_2, \ldots, A_n)$ is as above.

Remark 4.2.10. If P_α is J-general, it follows that Q_α and R_α satisfy the conditions of Proposition 4.2.5.

Remark 4.2.11. The polynomial $P_\alpha(X) = X^n - X$ is J-general. This is because we see that if we take $Q_\alpha(X) = n^2X^{n-1} - (n-2)^2$ and $R_\alpha(X) = nX^{n-1} + (n-2)$, then they satisfy $P'_\alpha(X)Q_\alpha(X) - P_\alpha(X)Q'_\alpha(X) = R(X)^2$.

$$\begin{aligned} & P'_\alpha(X)Q_\alpha(X) - P_\alpha(X)Q'_\alpha(X) \\ = \; & (nX^{n-1} - 1)(n^2X^{n-1} - (n-2)^2) - (X^n - X)(n^2(n-1)X^{n-2}) \\ = \; & n^2X^{2n-2} + 2n(n-1)X^{n-1} + (n-2)^2 \\ = \; & (nX^{n-1} + (n-2))^2. \end{aligned}$$

Clearly, $P_\alpha(X)$ and $R_\alpha(X)$ have no common factor, and $R_\alpha(X)$ has distinct roots. Further, $\Delta(P_\alpha(X) - T \cdot Q_\alpha(X)) = \Delta(P_\alpha(X))(1 + n^n(n-2)^{n-2}T^{n-1})^2$, and again it is clear that $1 + n^n(n-2)^{n-2}T^{n-1}$ has no repeated roots.

Using the correspondence between polynomials and points in affine space, we define

$$\mathcal{Z} := \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n | x_n = 0\} \tag{4.2.1}$$

to be the set which corresponds to the set of all monic polynomials of degree n whose constant term is 0. Also, by abuse of terminology, we will often refer to the polynomial corresponding to a point in $\mathbb{A}^n(k)$ as a polynomial in $\mathbb{A}^n(k)$.

We also define the Zariski-open subset $\mathcal{Y} \subset \mathbb{A}^n$ as follows:

$$\mathcal{Y} := \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{A}^n | J(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0\}. \tag{4.2.2}$$

By Remark 4.2.10 above, for any polynomial $P_\alpha(X) \in \mathcal{Y}(k)$, the corresponding specialised polynomials Q_α and R_α satisfy the conditions of Proposition 4.2.5.

Mestre ([24], Proposition 2) then shows:

Proposition 4.2.12. *Let k be a field of characteristic zero. Let $P_\alpha(X) \in k[X]$ be an J-general polynomial of degree n, and let $F_{T,\alpha}(X) = P_\alpha(X) - T \cdot Q_\alpha(X) \in k[X,T]$ keeping the notation as above. Then the Galois group of the splitting field of $F_{T,\alpha}(X)$ over $k(T)$ is A_n if $\Delta(P_\alpha(X))$ is a square in k, and is S_n otherwise.*

He ([24], Proposition 3) also shows:

Proposition 4.2.13. *Let $P_\alpha(X)$ be as in Proposition 4.2.12, and let $L = k(T)[X]/(F_{T,\alpha}(X))$. Then the trace form $q_L = \mathrm{Tr}_{L/k(T)}(x^2)$ is constant (cf. Definition 4.2.4).*

Now, we have a rational map $\mathcal{M} : \mathbb{A}^n \times \mathbb{A}^1 \dashrightarrow \mathbb{A}^n$ (with the $\mathcal{M}$ standing for Mestre) which is defined over $\mathbb{Q}$ given by

$$\mathcal{M}(P,T) = F_T(X) \tag{4.2.3}$$

keeping the notation as in Proposition 4.2.5. The rationality of the map follows from the fact that for the generic polynomial P, the polynomial Q has coefficients in A and hence $\mathcal{M}$ is given by polynomial equations. Also, we know that if for polynomials $P_\alpha(X)$ lying in the open subset $\mathcal{Y} \subset \mathbb{A}^n$, $F_{T,\alpha}$ satisfies the conditions of Proposition 4.2.5.

Moreover, we have the following lemma:

Lemma 4.2.14. *The map $\mathcal{M}|_{\mathcal{Z}\times\mathbb{A}^1}$ is birational, i.e., there exists a birational inverse $E = (E_1, E_2) : \mathbb{A}^n \dashrightarrow \mathcal{Z} \times \mathbb{A}^1$ such that $E_1|_{\mathcal{Z}} = \mathrm{id}_{\mathcal{Z}}$ as rational maps.*

Proof. Let us denote by $Q_{F_T}(X)$ and $R_{F_T}(X)$ the polynomials obtained if we apply Mestre's Proposition 4.2.5 to the polynomial $F_T(X) = P(X) - T \cdot Q(X)$ instead of the polynomial $P(X)$.

Now,

$$\begin{aligned} & F_T'(X)Q(X) - Q'(X)F_T(X) \\ = \; & (P'(X) - T \cdot Q'(X))Q(X) - Q'(X)(P(X) - T \cdot Q(X)) \\ = \; & P'(X)Q(X) - Q'(X)P(X) \\ = \; & R(X)^2. \end{aligned}$$

Also, $Q(X)$ has no common factor with $F_T(X)$ as it does not have any common factor with $P(X)$. Thus, we see that $Q(X)$ also satisfies the hypothesis of Proposition 4.2.5 for the polynomial $F_T(X)$. Since, by Proposition 4.2.5(a), there exists a unique primitive $Q_{F_T}(X)$, it follows that $Q(X)$ is a multiple of $Q_{F_T}(X)$ viz., $Q(X) = Q_{F_T}(X)G(\underline{A}, T)$, where $G(\underline{A}, T)$ is a polynomial in T and the A_i.

Recall that polynomials in $\mathcal{Z}$ have zero constant term and hence $P(0) = 0$.

Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{A}^n(k)$. Then, by our correspondence between points in affine space and monic polynomials of degree n, the tuple α corresponds to the polynomial $P_\alpha(X) = X^n + \alpha_1 X^{n-1} + \ldots \alpha_n$, which is a specialisation of the generic polynomial $P(X)$. We now define:

$$\begin{aligned} & E_1(\alpha) \\ = \; & E_1(P_\alpha(X)) \\ := \; & P_\alpha(X) - \tfrac{P_\alpha(0)}{Q_\alpha(0)} Q_\alpha(X) \end{aligned}$$

We note that E_1 is a rational map because the coefficients of $Q_\alpha(X)$ are expressed as polynomials in the coefficients of $P_\alpha(X)$ because the same holds for $Q(X)$ and $P(X)$.

Once we know $P(X)$, we can recover T as follows:

$$\begin{aligned} & E_2(F_T(X)) \\ := & \ \frac{-F_T(0)}{Q0} \\ = & \ \frac{-P(0)+T\cdot Q(0)}{Q(0)} \\ = & \ \frac{T\cdot Q(0)}{Q(0)} \text{ (because } P(0)=0) \\ = & \ T. \end{aligned}$$

Thus, it is clear that $\mathcal{M}|_{\mathcal{Z}\times\mathbb{A}^1}$ is a birational map and there exists a birational inverse $E = (E_1, E_2) : \mathbb{A}^n \dashrightarrow \mathcal{Z} \times \mathbb{A}^1$ such that $E_1|_{\mathcal{Z}} = \mathrm{id}_{\mathcal{Z}}$ as rational maps. □

4.3 Generic Galois Extensions

Let k be a field of characteristic zero and let G be a finite group. We defined earlier the notion of a generic Galois extension for G over k. We shall define a notion of a "relative" generic Galois extension and then we will then show that both are equivalent. Most of the results in this section are well known following the works of Saltman, DeMeyer, McKenzie and Plans.

Definition 4.3.1. ([16], Definition 0.1.1) Let $f(\underline{X}, T) \in k(\underline{X})[T]$ (where $\underline{X} = (X_1, X_2, \ldots, X_n)$) be a monic polynomial and let E denote the splitting field of $f(\underline{X}, T)$. We say $f(\underline{X}, T)$ is a *generic polynomial for G over the field k* if:

(i) $E/k(\underline{X})$ is Galois with Galois group G.

(ii) If L/K is any field extension with Galois group G, where K is any field containing k, then there exist $\underline{a} \in K^n$ such that the splitting field of $f(\underline{a}, T)$ is L, where $\underline{a} = (a_1, a_2, \ldots, a_n)$.

Definition 4.3.2. ([29], p. 275) A finite group G is said to have the *lifting property* over k if for any field extension K/k and a G-Galois extension L/K and R a local k-algebra with maximal ideal M and $R/M \cong K$, then there exists a (not necessarily local) k-algebra S such that S is a G-Galois extension of R and $S/MS \cong L$.

Let $\widetilde{G} \xrightarrow{\pi} G$ denote a fixed epimorphism of finite groups and let A denote its kernel. The embedding problem given by π and a G-Galois extension (of k-algebras) S/R will be denoted $(S/R, \pi)$. A G-Galois extension S/R such that the embedding problem has a proper solution will be called a $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension. If π is clear in the context, we will omit the π in $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension.

The following definitions are motivated by the notion of "descent-generic" polynomials ([16], p. 21).

Definition 4.3.3. ([27], Definition 2.1) A $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension S/R is called a *generic Galois extension for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k if:

(i) R is of the form $k[\underline{X}][\frac{1}{f}]$ for some set of indeterminates $\underline{X} = (X_1, \ldots, X_m)$ and some $f \in k[\underline{X}] \backslash \{0\}$, and

(ii) for any field K containing k and a $(\tilde{G} \xrightarrow{\pi} G)$-Galois extension L/K, then

there exists a homomorphism $\phi : R \to K$ of k-algebras (called a *specialisation*) such that L/K is Galois isomorphic to the natural G-Galois extension $S \otimes_\phi K/K$ obtained by specialising S/R.

Definition 4.3.4. ([27], Definition 2.2) A monic polynomial $f(\underline{X}, T) \in k(\underline{X})[T]$ is called a *generic polynomial for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k if:

(i) $f(\underline{X}, U)$ is a separable polynomial and its splitting field over $k(\underline{X})$ is a $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension of $k(\underline{X})$.

(ii) If L/K is a $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension of fields containing k, then there exists $\underline{x} \in K^n$ such that the polynomial $f(\underline{x}, T) \in K[T]$ is separable and its splitting field over K is L.

Definition 4.3.5. ([27], Definition 2.3) Let $\widetilde{G} \xrightarrow{\pi} G$ be as above. We say that $\widetilde{G} \xrightarrow{\pi} G$ has the *lifting property* over k if for every local k-algebra R with maximal ideal M, and every $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension of fields L/K with $K = R/M$, there exists a $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension S/R such that $S \otimes_R K \cong L$.

Remark 4.3.6. If we take $\widetilde{G} = G$ and $\pi = \mathrm{id}_G$, then the above "relative" definitions correspond to the usual concepts.

We make a remark here about the composition of solutions to embedding problems because we will be using it in the proof of the next theorem.

Remark 4.3.7. The term composition refers to the composition of solutions to embedding problems (as in [13], §1.15) and corresponds to the Baer sum of group

extensions. More explicitly, we are saying that there exists an A-Galois extension M_2/K such that L'/K is isomorphic (as $\widetilde{G}$-Galois extensions) to the following $\widetilde{G}$-Galois extension.

Let us first consider $M_2 \otimes_K M_1'/K$, which we can view as an $(A \times \widetilde{G})$-Galois extension via the action

$$(a, g)(l_1 \otimes l_2) := a(l_1) \otimes g(l_2).$$

Now, if A_1 denotes the kernel of the epimorphism

$$\begin{aligned} A \times \widetilde{G} &\to \widetilde{G}, \\ (a, g) &\mapsto ag, \end{aligned}$$

then $(M_2 \otimes_K M_1')^{A_1}/K$ is a $\widetilde{G}$-Galois extension (which is a solution to the embedding problem $(L/K, \pi)$) via the corresponding isomorphism $\widetilde{G} \cong (A \times \widetilde{G})/A_1$. This $\widetilde{G}$-Galois extension is the one which must be isomorphic to L'/K.

The following is listed as Proposition 2.5 in [27]:

Theorem 4.3.8. *Let k be a field of characteristic zero. Let $1 \to A \to \widetilde{G} \xrightarrow{\pi} G \to 1$ be a short exact sequence of finite groups. Assume that A is contained in the centre of $\widetilde{G}$ and also assume that A has a generic Galois extension over k. Then the following assertions are equivalent:*

(i) There exists a generic Galois extension for $\widetilde{G}$ over k.

(ii) There exists a generic polynomial for $\widetilde{G}$ over k.

(iii) The group $\widetilde{G}$ has the lifting property over k.

(iv) There exists a generic Galois extension for $\widetilde{G} \xrightarrow{\pi} G$ over k.

(v) There exists a generic polynomial for $\widetilde{G} \xrightarrow{\pi} G$ over k.

(vi) The lifting property holds for $\widetilde{G} \xrightarrow{\pi} G$ over k.

Proof. The equivalences $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ are well known and are available in several places e.g. in [9]. The proofs of $(iv) \implies (vi)$ and $(v) \implies (vi)$ can be easily obtained from them. Also, it is clear that $(i) \implies (iv)$. And, we will prove a stronger form of $(i) \implies (v)$ in the next lemma, Lemma 4.3.9. To complete the proof of the theorem, we prove $(vi) \implies (iii)$.

To prove $(i) \implies (iii)$**:** Suppose $\widetilde{G}$ has a generic Galois extension over k. Then, there is a k-algebra R and an extension S/R such that:

(i) S/R is Galois with group $\widetilde{G}$.

(ii) $R = k[t_1, \ldots, t_m][\frac{1}{u}]$ for some $0 \neq u \in k[t_1, \ldots, t_m]$ and indeterminates $t_1, \ldots, t_m$.

(iii) For any field extension K/k and any $\widetilde{G}$-Galois extension L/K, there exists a homomorphism $\phi : R \to K$ such that $L \cong S \otimes_\phi K$ as Galois extensions of K.

We want to show that if K is any field containing k and L/K any $\widetilde{G}$-Galois extension of fields and T is a local k-algebra with maximal ideal M and $T/M = K$, then there exists a $\widetilde{G}$-Galois extension T'/T such that $T' \cong T/M \cong L$.

Let T be a local k-algebra with maximal ideal M. Let $K = T/M$ and assume

L/K is a $\widetilde{G}$-Galois extension. Let $\phi : R \to K$ be a homomorphism with $L \cong S \otimes_\phi K$. We are given $R = k[t_1, \ldots, t_m][\frac{1}{u}]$. Let $a_i = \phi(t_i)$ and we choose $b_i \in T$ such that b_i is a preimage of a_i. We define $\psi : R \to T$ by setting $\psi(t_i) = b_i$. Note that $\psi(u)$ is invertible because T is local. Since $S \otimes T \otimes T/M \cong S \otimes K \cong L$, we see that $T' = S \otimes_\psi T$ defines a lifting for L/K.

To prove $(ii) \implies (iii)$: Suppose $\widetilde{G}$ has a generic polynomial over k. Then, there exist indeterminates $t_1, \ldots, t_m$ and a separable polynomial $g(t1, ..., tm)(x) \in k(t_1, \ldots, t_m)[x]$ whose Galois group is G such that: If K is a field containing k and L/K is a Galois extension of fields with Galois group $\widetilde{G}$, then there exist $a_1, \ldots, a_m \in K$ such that the splitting field of the separable polynomial $g(a_1, \ldots, a_m)(x) \in K[x]$ is L.

We want to show that if K is any field containing k and L/K any $\widetilde{G}$-Galois extension of fields and R is a local k-algebra with maximal ideal M and $R/M = K$, then there exists a $\widetilde{G}$-Galois extension S/R such that $S \cong R/M \cong L$.

For $i = 1, \ldots, m$ let $r_i \in R$ be a preimage of a_i under the natural map $R \to R/M$. We note that $g(r_1, \ldots, r_m)(x) \in R[x]$ is separable over R since it is separable over R/M when its coefficients are reduced modulo M. Let u be the product of the discriminant of $g(t_1, \ldots, t_m)(x)$ and the denominators of the coefficients of $g(t_1, \ldots, t_m)(x)$ expressed in lowest terms. The assignment $t_i \mapsto r_i$ induces $\phi : k[t_1, \ldots, t_m][\frac{1}{u}] \to R$, since the substitution $t_i \mapsto a_i$ gives a well-defined image $g(a_1, \ldots, a_m)(x) \in K[x]$ and since the separability of $g(x) \in R[x]$ implies

that the image of the discriminant is a unit in R. If $\beta_1, \ldots, \beta_n$ are the roots of $g(t_1, \ldots, t_m)(x)$ in a splitting field, then $T = k[t_1, \ldots, t_m][\frac{1}{u}][\beta_1, \ldots, \beta_n]$ is a splitting ring of $g(t_1, \ldots, t_m)(x)$ over $k[t_1, \ldots, t_m][\frac{1}{u}]$ and the Galois group of T over $k[t_1, \ldots, t_m][\frac{1}{u}]$ is G. Now, $S = T \otimes_{k[t_1,\ldots,t_m][\frac{1}{u}]} R$ is a Galois extension of R with Galois group $\widetilde{G}$ and $S \otimes_R R/M$ is a Galois extension of $R/M = K$ with Galois group $\widetilde{G}$. Moreover, $g(a_1, \ldots, a_m)(x)$ splits in $S \otimes_R R/M$ and so by uniqueness of splitting fields, $S \otimes_R R/M \cong L$.

To prove $(vi) \implies (iii)$**:** Let R be a local k-algebra with maximal ideal M and residue field $K = R/M$ and let L'/K be a given $\widetilde{G}$-Galois extension of fields.

We define $L = L'^A$. Then, L/K is a G-Galois extension and L'/K is a proper solution to the embedding problem $(L/K, \pi)$. Now by (vi), we know the existence of a $(\widetilde{G} \xrightarrow{\pi} G)$-Galois extension S/R such that $S \otimes_R K \cong L$ as G-Galois extensions.

Let T_1'/R be a $\widetilde{G}$-Galois extension which is a solution to the embedding problem $(S/R, \pi)$ and we define $M' := T_1' \otimes_R K$ to be the specialisation. Clearly, the extension M'/K (obtained above by specialisation) is a solution the embedding problem $(L/K, \pi)$.

Since L'/K and M'/K are solutions to the same embedding problem $(L/K, \pi)$, it follows from [13], Theorem 3.15.4 and our assumption that A is central in G that L'/K must be Galois isomorphic to the the composition (see Remark 4.3.7) of M'/K and a solution the the trivial central embedding problem $(L/K, A \times G \rightarrow G)$.

On the other hand, since we assume that A has a generic extension over k and consequently has the lifting property over k, there exists an A-Galois extension T_2/R such that $T_2 \otimes_R K \cong M_2$ (where M_2 is from Remark 4.3.7) as A-Galois extensions of K.

Thus $T_2 \otimes_R T_1'$ is a $(A \times \widetilde{G})$-Galois extension and $(T_2 \otimes_R T_1') \otimes_R K \cong M_2 \otimes_K M_1'$ as Galois extensions of K.

Further, as above $(T_2 \otimes_R T_1')^{A_1}/R$ is a $\widetilde{G}$-Galois extension, and certainly $(T_2 \otimes_R T_1')^{A_1} \otimes_R K \cong L'$ as Galois extensions of K.

That concludes the proof of $(vi) \implies (iii)$ and hence the proof of the theorem.

□

Lemma 4.3.9. *([27], Lemma 2.8) Let k and $1 \to A \to \widetilde{G} \xrightarrow{\pi} G \to 1$ be as in the hypothesis of Theorem 4.3.8. Then, the following are equivalent:*

(i) There exists a generic Galois extension for $\widetilde{G}$ over k.

(ii) Given a transitive embedding $G \hookrightarrow S_n$, there exists a generic polynomial $F(\underline{U}; X)$ for $\widetilde{G} \xrightarrow{\pi} G$ over k with the following additional properties:

(a) $\deg_X(F(\underline{U}; X)) = n$ and $\mathrm{Gal}_{k(\underline{U})}(F)$ (the Galois group of the splitting field of F over $k(\underline{U})$) is conjugate to G in S_n.

(b) For every subgroup $H \subset G$ and every $(\pi^{-1}(H) \xrightarrow{\pi} H)$-Galois extension L/K of fields containing k, there exists $\underline{v} \in K^m$ such that the polynomial $F(\underline{v}; X) \in K[X]$ is separable, its splitting field over K is L and the

permutation action of H (arising from the embedding $H \hookrightarrow G \hookrightarrow S_n$) on the set of roots of $F(\underline{v}; X)$ (after a choice of a suitable ordering) coincides with the Galois action of H (from the given H-Galois extension L/K).

Proof. It is enough to prove $(i) \implies (ii)$. We recall that k is of characteristic zero and hence infinite.

We let $R := k[\underline{U}][\frac{1}{u}]$ be a localised polynomial ring over k, and let $\widetilde{S}/R$ be a generic extension for $\widetilde{G}$ over k. We can assume that $\widetilde{S}/R$ has a normal basis $\underline{\alpha} = \{\alpha_{\tilde{g}}\}_{\tilde{g} \in \widetilde{G}}$. Moreover, given a set of indeterminates $\underline{Y} = \{Y_{\tilde{g}}\}_{\tilde{g} \in \widetilde{G}}$ and a non-zero polynomial $d(\underline{Y}) \in k[\underline{Y}]$, we can assume too that $d(\underline{\alpha})$ is a unit in S. This follows from [7], Lemma 3.

For every $g \in G$, we define

$$\beta_g := \sum_{\tilde{g} \in \pi^{-1}(g)} \alpha_{\tilde{g}}.$$

We notice that $\{\beta_g\}_{g \in G}$ is a normal basis for the extension $\widetilde{S}^A/R$, which is generic for $\widetilde{G} \xrightarrow{\pi} G$ over k.

Let $G_1 \subset G$ be the stabiliser of 1 with respect to the faithful, transitive action (which is fixed) of G on $\{1, 2, \ldots, n\}$. Given a set $\{g_1, g_2, \ldots, g_n\}$ of representatives of the left cosets of G_1 in G, we define:

$$\gamma_i := \sum_{g \in g_i G_1} \beta_g, \quad i \in \{1, 2, \ldots, n\}.$$

We are going to show that (ii) holds with the polynomial

$$F(\underline{U}; X) := \prod_{1 \leq i \leq n} (X - \gamma_i)$$

which is an element of $k[\{\beta_g\}_{g \in G}]^G[X] \subset R[X]$ and whose discriminant can be assumed to be a unit in R. We will henceforth make that assumption.

Now, property (a) follows trivially and so we give an argument as to why the polynomial satisfies property (b).

Given a subgroup $H \subset G$, let us define $\widetilde{H} := \pi^1(H)$ and let $\pi_H : \widetilde{H} \to H$ denote the restriction of π to $\widetilde{H}$. Suppose we are given a $(\widetilde{H} \to H)$-Galois extension L/K of fields containing k.

We recall the following definition of induced Galois extensions:

Definition 4.3.10. ([29], p. 253) A G-Galois extension *induced* from the H-Galois extension L/K and the inclusion $H \subset G$ is isomorphic to $\mathrm{Ind}_H^G(L)/K = \prod_{1 \leq i \leq [G:H]=r} L$ with the G-Galois action as follows: Let $\{s_1, s_2, \ldots, s_r\}$ be a set of representatives of the left cosets of H in G. If $g \in G$ satisfies $gs_i = s_j h \in s_j H$, then the j^{th} component of $g((l_1, \ldots, l_r))$ is $h(l_i)$.

Since we assume that the embedding problem $(L/K, \pi_H)$ is properly solvable, so must the embedding problem $(\mathrm{Ind}_H^G(L)/K, \pi)$. More precisely, if L'/K is a solution to the embedding problem $(L/K, \pi_H)$, then we can check that $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(L')/K$ is a solution to the embedding problem $(\mathrm{Ind}_H^G(L)/K, \pi)$.

Then, because the G-Galois extension $\widetilde{S}^A/R$ is generic for $\widetilde{G} \xrightarrow{\pi} G$ over k,

there exists a specialization $\phi : R \to K$ such that $\mathrm{Ind}_H^G(L)/K$ and $\widetilde{S}^C \otimes_\phi K/K$ are isomorphic as G-Galois extensions.

Now, let $\underline{v} := \phi(\underline{U}) \in K^m$.

We note that the polynomial (obtained by specialisation) $F(\underline{v}; X) \in K[X]$ must be separable, since its discriminant belongs to $\phi(R^*)$.

Now, we can show that L is the splitting field of $F(\underline{v}; X)$ over K as follows (motivated by [7], Theorem 2). The elements $\{\gamma_i \otimes 1\}_{1 \leq i \leq n}$ generate the K-algebra $\widetilde{S}^A \otimes_\phi K$ and they satisfy

$$F(\underline{v}; X) = \prod_i (X - (\gamma_i \otimes 1)).$$

Thus if,

$$f : \widetilde{S}^C \otimes_\phi K \xrightarrow{\cong} \mathrm{Ind}_H^G(L) = \prod_{1 \leq i \leq r} L$$

defines a isomorphism of G-Galois extensions of K, and let us denote by $\theta_i \in L$ the first component of $f(\gamma_i \otimes 1) \in \prod_{1 \leq i \leq r} L$, then $L = K[\theta_1, \ldots, \theta_n]$ and $F(\underline{v}; X) = \prod_i (X - \theta_i)$.

Moreover, the given (Galois) action on $\{\theta_i\}_i$ is conjugate in S_n to the fixed H-Galois action on $\{1, \ldots, n\}$. In fact, if we choose $\sigma_1 = \mathrm{id}$, then the H-Galois actions on $\{\theta_i\}_i$ and on $\{\gamma_i\}_i$ coincide. □

4.4 Extensions of S_n by 2-groups

We will prove:

Lemma 4.4.1. *Let k and G be as in Theorem 4.0.1, $n \geq 2$ and assume in addition that A is a 2-group. Then, there exists a generic Galois extension for G over k if there exists a generic Galois extension for $\pi^{-1}(S_{n-1})$ where S_{n-1} is the subgroup of S_n consisting of the permutations of the first $n-1$ letters.*

We note however that by Theorem 4.3.8 above, it suffices to prove the following theorem:

Lemma 4.4.2. *Let k be a field of characteristic zero and let $1 \to A \to G \to S_n \to 1$ be a finite central extension with A a 2-group. If $\pi^{-1}(S_{n-1}) \to S_{n-1}$ has a generic polynomial over k, then $G \to S_n$ has a generic polynomial over k.*

Definition 4.4.3. As above, let G be a central extension of S_n by a 2-group A. We say a polynomial $f(X) \in k[X]$ is a *G-good* polynomial over k if:

1. The discriminant of $f(X)$ is not a square in k; or equivalently, the Galois group of the splitting field of $f(X)$ over k is not a subgroup of A_n, and

2. If L denotes the splitting field of $f(X)$ over k and H its Galois group, then the embedding problem $(L/k, \pi_H)$ has a proper solution, where π_H is as follows:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & A & \longrightarrow & \pi^{-1}(H) & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & S_n & \longrightarrow & 1
\end{array}$$

Remark 4.4.4. The first condition for f being G-good is that the discriminant of f is not a square, which is the same as saying that the first Stiefel-Whitney class

of the trace form of the splitting field of f is non-trivial in $k^\times/k^{\times 2}$.

The second for f being G-good is the same as saying that the obstruction to the embedding problem vanishes; and by using Serre's Theorem 4.2.1, it follows that the obstruction can be expressed in terms of the discriminant and Hasse-Witt invariant of the trace form.

Hence, whether a polynomial is G-good or not is entirely determined by its trace form. In particular, if two polynomials have the same trace forms (of their respective splitting fields), then either both are G-good or neither is.

In the proof of Lemma 4.4.2, we need a proposition about the density of G-good polynomials, the proof of which relies on the following result of DeMeyer ([7], Lemma 3):

Lemma 4.4.5. *Let R be a local F-algebra, let S be a Galois extension of R with group G, and let G act as a transitive subgroup of permutations on $y_1, y_2, \ldots, y_n$. Then, there exists $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset S$ so that*

1. $S = R[\alpha_1, \ldots, \alpha_n]$.
2. $\sigma(\alpha_i) = \alpha_j$ *if and only if* $\sigma(y_i) = y_j$ *for all* $1 \leq i, j \leq n, \sigma \in G$.
3. $g(t) = \prod_{i=1}^{n}(t - \alpha_i) \in R[t]$ *is a separable polynomial.*
4. *For any given* $q(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ *the* α_i *can be chosen so that* $q(\alpha_1, \ldots, \alpha_n) \in S^\times$.

Remark 4.4.6. There is a typographical error in the statement of the lemma in DeMeyer's original paper. Condition (2) of the lemma should read $\sigma(y_i) = y_j$ instead of $\sigma(y_j) = y_j$.

We use the above lemma to prove the following proposition:

Proposition 4.4.7. *Let L/K be a $(G \to S_n)$-Galois extension. The set of G-good polynomials of degree n which have L/K as a splitting field is dense in $\mathbb{A}^n(K)$.*

Proof. First of all, if a polynomial has L/K as a splitting field, it is a G-good polynomial because L/K is a $(G \to S_n)$-Galois extension. Hence, it is enough to show that the set of all polynomials of degree n which have L/K as a splitting field is dense in $\mathbb{A}^n(K)$. We also know that the basic open sets of $\mathbb{A}^n(K)$ are the complements of the zero sets $V(f) = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) | f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\}$ for polynomials $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$.

Now, going back to the hypothesis of the proposition we take $F = K$, $S = L$, $R = K$ and $G = S_n$. Then, by the proposition, given any polynomial q as above, there exists $\alpha_1, \ldots, \alpha_n \in L$ such that $q(\alpha_1, \ldots, \alpha_n) \neq 0$ and L/K is the splitting field of $g(t)$.

To show that the set of polynomials of degree n with L/K as a splitting field is dense in $\mathbb{A}^n(K)$, it is enough to show that given any polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, there exists a point $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{A}^n(k)$ (which corresponds to the monic polynomial $g(t) = t^n + \beta_1 t^{n-1} + \beta_2 t^{n-2} + \ldots \beta_{n-1} t + \beta_n$ of degree n)

such that $f(\beta_1, \ldots, \beta_n) \neq 0$ (i.e., $(\beta_1, \ldots, \beta_n) \notin V(f)$) and $g(t)$ has splitting field L/K.

Let $\Sigma_1(y_1, y_2, \ldots, y_n), \Sigma_2(y_1, y_2, \ldots, y_n), \ldots, \Sigma_n(y_1, y_2, \ldots, y_n) \in K[y_1, y_2, \ldots, y_n]$ be the n symmetric polynomials in $y_1, y_2, \ldots, y_n$. Now, take $q(y_1, y_2, \ldots, y_n) = f(\Sigma_1, \Sigma_2, \ldots, \Sigma_n)$. Clearly, $q(y_1, y_2, \ldots, y_n) \in K[y_1, y_2, \ldots, y_n]$. Now, by the above paragraph there exists $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ such that $q(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ and such that $g(t) = \prod_{i=1}^{n}(t - \alpha_i) = t^n + \beta_1 t^{n-1} + \ldots \beta_{n-1}t + \beta_n$, where $\beta_i = \Sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$, has splitting field L/K. Also, $q(\alpha_1, \alpha_2, \ldots, \alpha_n) = f(\Sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \Sigma_n(\alpha_1, \ldots, \alpha_n)) = f(\beta_1, \ldots, \beta_n) \neq 0$, which is exactly what we required. Hence, the set of G-good polynomials of degree n with splitting field L/K is dense in $\mathbb{A}^n(K)$. □

Proof. (of Lemma 4.4.2.) First of all, by work of Serre and Sonn, we can reduce it to the case when n is odd. In this case, we use an approach similar to that in [27], Theorem 3.1. By assumption, there is a generic polynomial for $\pi^{-1}(S_{n-1}) \to S_{n-1}$ over k. By using $(v) \implies (ii)$ of Theorem 4.3.8, there is a generic Galois extension for $\pi^{-1}(S_{n-1})$. Thus by Lemma 4.3.9, there is a generic polynomial $F(\underline{U}, X)$ for $\pi^{-1}(S_{n-1}) \to S_{n-1}$ satisfying both the properties in Lemma 4.3.9(ii), and in particular having degree $n - 1$.

We recall that given a monic polynomial $\prod_{1 \leq i \leq m}(X - \alpha_i)$ of degree m, its Tschirnhaus transformation (see [16], p. 141) with respect to a polynomial $g(X)$ of degree less than m is the polynomial $\prod_{1 \leq i \leq m}(X - g(\alpha_i))$. Let

$\underline{S} = (S_1, \ldots, S_{n-1})$ be a set of indeterminates and let us define $F_{\underline{S}}(\underline{U}, X)$ as the Tschirnhaus transformation of $F(\underline{U}, X)$ with respect to the polynomial $g_S(X) = S_1 X^{n-2} + \ldots S_{n-2} X + S_{n-1}$. Substituting $F(U; X)$ for f and $X - g(Z)$ for g in the definition of resultant (Definition 4.2.6), we get that

$$F_{\underline{S}}(\underline{U}, X) = \text{res}(F(\underline{U}, Y), X - g_S(Y)) \in k(\underline{U}, \underline{S})[X]$$

where the resultant is taken with respect to Y.

It follows from the definition of the Tschirnhaus transformation that the polynomials $F_{\underline{S}}(\underline{U}, X)$ and $F(\underline{U}, X)$ have the same splitting field over $k(\underline{U}, \underline{S})$ and they satisfy $F(\underline{U}, X) = F_{\underline{s}}(\underline{U}, X)$ for the specialisation $s = (0, \ldots, 0, 1, 0)$. Since the polynomial $F(\underline{U}, X)$ was generic to begin with, the polynomial $F_{\underline{S}}(\underline{U}, X) \in k(\underline{U}, \underline{S})[X]$ is also generic for $\pi^{-1}(S_{n-1}) \to S_{n-1}$ over k.

We now claim that every G-good polynomial (cf. Definition 4.4.3) $f(X)$ of degree $n-1$ over a field K/k arises as a specialisation $F_{\underline{s}}(\underline{v}, X)$ for some $\underline{v} \in K^m$ and $\underline{s} \in K^{n-1}$. Since f is G-good, the Galois group of its splitting field is a subgroup of S_{n-1}. The second condition of being G-good implies that the splitting field can be embedded in an $\pi^{-1}(S_{n-1})$-Galois extension. But then by Lemma 4.3.9(b), f occurs as a specialisation $F(\underline{v}; X)$ for some $\underline{v} \in K^m$. Hence every G-good polynomial of degree $n-1$ arises as a specialisation of the polynomial $F_{\underline{S}}(\underline{U}; X)$.

By Proposition 4.4.7, it follows that the set of G-good polynomials of degree n with coefficients in a field k is a Zariski-dense subset in $\mathbb{A}^n(k)$, the set of all

monic polynomials of degree n. In fact, we have shown more: If L/k is a $G \to S_n$ extension, then the set of G-good polynomials of degree n which have L/k as a splitting field is dense in $\mathbb{A}^n(k)$.

Now, $\mathcal{Y}(\mathbb{Q}) \cap \mathcal{Z}(\mathbb{Q}) \neq \emptyset$ (for the definition of $\mathcal{Y}$ and $\mathcal{Z}$, cf. (4.2.2) and (4.2.1)). This is because first $X^n - X$ lies in $\mathcal{Z}(\mathbb{Q})$ as its constant term is zero and second, by Remark 4.2.11 the polynomial $X^n - X$ lies in $\mathcal{Y}(\mathbb{Q})$.

Since $\mathcal{Y}$ is Zariski-open in $\mathbb{A}^n$ and $\mathcal{Y}(\mathbb{Q}) \cap \mathcal{Z}(\mathbb{Q}) \neq \emptyset$, we know that $\mathcal{Y}(\mathbb{Q}) \cap \mathcal{Z}(\mathbb{Q})$ is a nonempty subset of $\mathcal{Z}(\mathbb{Q})$.

Let B denote the polynomial $X \cdot F_{\underline{S}}(\underline{U}, X)$. We first note that $F_{\underline{S}}(\underline{U}, X)$ is a G-good polynomial if and only if B is also a G-good polynomial. This is because whether a polynomial is G-good depends only on its splitting field, and in this case the splitting field of B is the same as the splitting field of $F_{\underline{S}}(\underline{U}, X)$.

We have shown above that $F_{\underline{S}}(\underline{U}, X)$ specialises to any G-good polynomial of degree $n-1$ (over k). Therefore B specialises to any G-good polynomial of degree n with zero constant coefficient (because $B = X \cdot F_{\underline{S}}(\underline{U}, X)$), and so B specialises to any G-good polynomial in $\mathcal{Z}(k)$.

We claim that the G-good polynomials are dense in $\mathcal{Z}(k)$. To show this, we first note our earlier remark that $X \cdot F$ is G-good if and only if F is G-good. Hence, the G-good polynomials in $\mathcal{Z}(k)$ are in one-to-one correspondence with the G-good polynomials of degree $n-1$ in $\mathbb{A}^{n-1}(k)$. But, we know the G-good polynomials of degree $n-1$ are dense in $\mathbb{A}^{n-1}(k)$ and hence, the G-good polynomials are dense

in $\mathcal{Z}(k)$, thus proving the claim.

Thus, there exists a G-good polynomial which lies in $\mathcal{Z}(k) \cap \mathcal{Y}(k)$. Thus, there exists a polynomial in $\mathcal{Y}(k)$ to which $B = X \cdot F_{\underline{S}}(\underline{U}, X)$ specialises but that implies that B lies in $\mathcal{Y}(k(\underline{U}, \underline{S}))$. The last conclusion follows because if B does not lie in $\mathcal{Y}(k(\underline{U}, \underline{S}))$, then B satisfies the polynomial H; but that would imply the specialisation of B also satisfies H, contradicting the fact that the specialisation of B lies in $\mathcal{Y}(k)$.

Let us consider the polynomial $\mathcal{M}(B, T)$ as a polynomial over the field $k(\underline{U}, \underline{S}, T)$. We claim that it is generic for $G \to S_n$ over k.

We claim that $\mathcal{M}(B, T)$ is a G-good polynomial over $k(\underline{U}, \underline{S}, T)$. We know B is an element of $\mathcal{Y}(k(\underline{U}, \underline{S}))$ and so, by Proposition 4.2.13, the trace form of the splitting field of $\mathcal{M}(B, T)$ is constant i.e., independent of T. Choosing $T = 0$, we see $\mathcal{M}(B, 0) = B$, which is a G-good polynomial. Since the trace form was independent of T, we get that the trace form of the splitting field of $\mathcal{M}(B, T)$ is the same as the trace form of the splitting field of $\mathcal{M}(B, 0)$; and hence $\mathcal{M}(B, T)$ is a G-good polynomial by Remark 4.4.4, thus proving the claim.

Further, because $\mathcal{M}(B, T)$ has degree n, we know that the Galois group of its splitting field is contained inside S_n. Since B lies in $\mathcal{Y}(k(\underline{U}, \underline{S}))$ and the discriminant of B is not a square, by Proposition 4.2.12, it also contains S_n and hence, the Galois group must be S_n. We now want to show that it is a generic polynomial for $G \to S_n$.

Let K/k be any field extension and let L/K be any $(G \to S_n)$-Galois extension. Let f be a polynomial in $K[X]$ for which the extension L/K is a splitting field. Now, L/K is Galois with Galois group S_n and so f satisfies the first condition of being G-good. Also, since L/K embeds into a G-Galois extension, it satisfies the second condition of being G-good, and hence f is a G-good polynomial of degree n. Hence, we have shown that any polynomial which has L/K as a splitting field is G-good. Using this fact together with the fact that the G-good polynomials with coefficients in K are dense in $\mathbb{A}^n(K)$, we can choose f such that $(\mathcal{M} \circ (E_1, E_2))$ is defined on f. Then, by Lemma 4.2.14, $(\mathcal{M} \circ (E_1, E_2))(f) = f$ and $E_1(f) \in \mathcal{Z}(K)$. (The maps E_1 and E_2 were defined in Lemma 4.2.14.)

We now claim that $E_1(f)$ is a G-good polynomial over K of degree n. By definition, $\mathcal{M}(E_1(f), 0) = E_1(f)$; and by Lemma 4.2.14, $\mathcal{M}(E_1(f), E_2(f)) = f$. Also, by Proposition 4.2.13, we know that the trace form of the splitting field of $\mathcal{M}(E_1(f), T)$ is independent of T and so the trace form of the splitting field of $E_1(f)$ is the same as the trace form of the splitting field of f. Since f was G-good, that implies $E_1(f)$ is G-good, proving the claim.

Also, as $E_1(f)$ belongs to $\mathcal{Z}(K)$, it has zero constant coefficient and can be written as $X \cdot g(X)$, where $g(X)$ is a G-good polynomial (because as we argued earlier, $g(X)$ is G-good if and only if $X \cdot g(X)$ is G-good). Thus, $E_1(f)$ can be written as $X \cdot F_{\underline{s}}(\underline{v}; X)$ for certain specialisations $\underline{s} \in K^m$ and $\underline{v} \in K^{n-1}$ (because every G-good polynomial can be written as the specialisation of $F_{\underline{S}}(\underline{U}; X)$).

Thus, we have that $\mathcal{M}(B,T)$ under the specialisation $\underline{U} \mapsto \underline{v}$, $\underline{S} \mapsto \underline{s}$ and $T \mapsto E_2(f)$ gives us the polynomial f thus completing the proof. □

Theorem 4.4.8. *([29], Theorem 2.1) An abelian group A has a generic Galois extension over k if $k(\zeta_q)/k$ is cyclic, where q is the highest power of 2 dividing the order of A.*

Lenstra ([22]) gave an if-and-only-if criterion as to when an abelian group has a positive answer to the Noether problem over $\mathbb{Q}$. Later, Saltman ([29]) gave an if-and-only-if criterion as to when an abelia group has a generic Galois extension over any field of characteristic zero. Motivated by Remark 3.6 in [27], the following proposition gives us an if-and-only-if criterion as to when certain nonabelian groups have generic Galois extensions over a field of characteristic zero:

Proposition 4.4.9. *Let $1 \to A \to G \xrightarrow{\pi} S_3 \to 1$ be a finite central extension. Then, G has a generic Galois extension if and only if G has no element of order 8.*

Proof. Using Theorem 4.4.8 together with Theorem 5.11 in [29] (which states that an abelian group with an element of order a power of 2 which is greater than 8 cannot have a generic Galois extension over $\mathbb{Q}$) , we get that an abelian group A has a generic Galois extension over $\mathbb{Q}$ if and only if A does not have an element of order 8. Now, if G is a finite central extension of S_3, then $\pi^{-1}(S_2)$ is an abelian

group which contains a 2-Sylow subgroup of G. As a consequence of Lemma 4.4.1, the group G has a generic Galois extension over $\mathbb{Q}$ if and only if $\pi^{-1}(S_2)$ has a generic Galois extension over $\mathbb{Q}$, which by our above comments holds if and only if $\pi^{-1}(S_2)$ does not contain an element of order 8, which is satisfied if and only if G does not contain an element of order 8.

□

The following theorem is stated as Theorem 1.5 in [29]:

Theorem 4.4.10. *Let G_1 and G_2 be finite groups which have generic Galois extensions over a field k. Then, $G = G_1 \times G_2$ has a generic Galois extension over a field k.*

Proof. Let S_1/R_1 and S_2/R_2 be generic Galois extensions for G_1 and G_2 over k respectively. Then, taking $S = S_1 \otimes_k S_2$ and $R = R_1 \otimes_k R_2$, we claim that S/R is a generic Galois extension for G over k. As S_1/R_1 is G_1-Galois and as S_2/R_2 is G_2-Galois, S/R is G-Galois. Now, we have to show that every G-Galois extension of K where K is any field containing k occurs as a specialisation of S/R. Let L/K be a G-Galois extension i.e. $G_1 \times G_2$-Galois extension. So, L is the compositum of two linearly disjoint fields L_1 and L_2 which are Galois over K with Galois groups G_1 and G_2 respectively. Therefore, they can be realised as specialisations ϕ_1 and ϕ_2 of R_1 and R_2 respectively. Therefore, the specialisation $\phi_1 \otimes \phi_2$ of $R_1 \otimes R_2$ gives us the extension L/K, and hence we are done. □

Proof. (of Theorem 4.0.1.) First, we showed in Proposition 4.1.1 that any G (as in the statement of the theorem) can be written as $G_1 \times G_2$ with G_1 a central extension of S_n by a 2-group and $G_2 \subset A$ has odd order.

Second, since G_2 is an odd order abelian group, it can be written as a product of odd order cyclic groups. By Theorem 4.4.8, a cyclic group of odd order (say m) has a generic Galois extension over k (because the corresponding q is just 1 when the order of the group is odd), and thus by Theorem 4.4.10, G_2 has a generic Galois extension.

Third, in Lemma 4.4.1 we showed that G_1 has a generic extension over k if $\pi^{-1}(G_1)$ has a generic extensions over k. Repeatedly using the lemma, we get that G_1 has a generic extension over k if A (the kernel) has an extension over k. But A has a generic extension by hypothesis, hence G_1 does also.

Finally, by Theorem 4.4.10, we conclude that G can be chosen to have a generic Galois extension over k as G_1 and G_2 have generic Galois extensions over k. $\square$

Chapter 5

Dihedral groups

5.1 Dihedral 2-groups

We will use Kiming's work ([18]) to study the existence of generic Galois extensions for some small dihedral 2-groups. Kiming used "explicit" class field theory to characterise some families of extensions over k where k is a field of characteristic different from 2. In particular, he shows ([18], Theorem 5) that any D_4-Galois extension of k has one of the following forms:

- $k(\sqrt{a}, \sqrt{a-1}, \sqrt{c(a+\sqrt{a})})/k$ where $a, c \in k^\times$ and such that none of $a, a-1, a(a-1)$ is a square in k.
- $k(\sqrt{-1}, \sqrt{c}a^{1/4})/k$ where $a, c \in k^\times$ are such that none of $-1, a, -a$ is a square in k.

We next show that because of the above, we can obtain a generic Galois extension for D_4 over k. (Note that the existence of generic Galois extensions over $\mathbb{Q}$ for the group D_4 and D_8 had already been shown by Elena Black in [2].)

Proposition 5.1.1. *If k is a field with characteristic different from 2, then D_4 has a generic Galois extension over a field k.*

Proof. Consider the following extension over k

$$k\left(\sqrt{a}, \sqrt{ae^2 - d^2}, \sqrt{c(ae + d\sqrt{a})}\right)/k$$

where $a, c, d, e \in k^\times$ such that none of a, b, ab is a square in $k^\times$ where $b = ae^2 - d^2$. It is easy to see that the above extension is Galois with Galois group D_4. We claim that, in fact, any D_4-Galois extension of k can be obtained as a specialisation of the above. By Kiming's result mentioned above, it is enough to show that each of those families can be realised as a specialisation of the above family, and we shall show that. To realise the first family, we look at the following specialisation:

$$\begin{aligned} a &\rightsquigarrow a \\ c &\rightsquigarrow c \\ d &\rightsquigarrow 1 \\ e &\rightsquigarrow 1, \end{aligned}$$

and to realise the second family, we look at the following specialisation:

$$\begin{aligned} a &\rightsquigarrow a \\ c &\rightsquigarrow c \\ d &\rightsquigarrow 1 \\ e &\rightsquigarrow 0. \end{aligned}$$

Thus, we have parametrised all D_4-Galois extensions of a field of characteristic different from 2.

We now claim that the D_4-Galois extension

$$k\left(\sqrt{Z}, \sqrt{X^2 - Y^2 Z}, \sqrt{X + Y\sqrt{Z}}\right) / k(X, Y, Z).$$

is a generic Galois extension for D_4 over k. Specialising the above as follows:

$$\begin{aligned} X &\rightsquigarrow cae \\ Y &\rightsquigarrow cd \\ Z &\rightsquigarrow a \end{aligned}$$

gives us the extension at the beginning of the proof which parametrised all D_4-Galois extensions, and hence the above is indeed a generic extension. □

Let $q = 2^d$ and k be a field with $\mathrm{char}(k) \neq 2$. Further, assume that $\zeta_q \in k$. Then, Elena Black proved:

Proposition 5.1.2. *([3], Proposition 2.1) D_q has a generic Galois extension over k.*

5.2 General Dihedral Groups

We now switch our attention to general dihedral groups i.e. not necessarily 2-groups. Elena Black ([2]) proved in her thesis that any dihedral group D_n, with n odd has the arithmetic lifting property. We will show that in fact any such D_n has a generic extension over any field k of characteristic zero.

Saltman proved the following theorem (Theorem 3.5) in [29]:

Theorem 5.2.1. *Let M and H be finite groups of relatively prime order, and assume M is abelian. Suppose that there are generic Galois extensions for M and H over k. Then there is a generic Galois extension, over k, for any semidirect product $M \rtimes H$.*

Corollary 5.2.2. *If n is odd, $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ has a generic Galois extension over $\mathbb{Q}$, and hence over $\mathbb{Q}(i)$, and more generally over any field of characteristic zero.*

We now study the group structure of dihedral groups – in particular, we want to decompose a dihedral group in terms of smaller dihedral groups. We give a proof of the following elementary lemma, for lack of an explicit reference.

Given a general dihedral group D_m where $q = 2^d$ is the highest power of 2 dividing m, i.e. $m = q \cdot n$ with n odd, we have the following decomposition:

Lemma 5.2.3. *(a) If $d = 1$, then $D_m \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.*

(b) If $d > 1$, then $D_m \cong D_n \times_{\mathbb{Z}/2\mathbb{Z}} D_q$, where the maps from D_m and D_n to $\mathbb{Z}/2\mathbb{Z}$

are the obvious ones.

Proof. We look at the following presentation for D_m:

$$\langle \alpha, \beta | \alpha^m = \beta^2 = (\alpha\beta)^2 = 1 \rangle.$$

Sending α to α^n and β to β induces a well-defined endomorphism $\phi_n : D_m \to D_m$, whose image is isomorphic to D_q. Now if n and q are coprime, the homomorphism $D_m \to D_n \times_{\mathbb{Z}/2\mathbb{Z}} D_q$ induced by $\phi_q : D_m \to D_n$ and $\phi_n : D_m \to D_q$ is bijective by the Chinese Remainder Theorem. (The natural maps $D_n \to \mathbb{Z}/2\mathbb{Z}$ and $D_q \to \mathbb{Z}/2\mathbb{Z}$ are given by $\alpha \mapsto 0$ and $\beta \mapsto 1$ where α and β are the generators as in the above presentation.)

In the special case where n is odd and q is 2, the kernel $\{1, \alpha^n\}$ of $\phi_2 : D_{2n} \to D_{2n}$ lies in the center of D_{2n}; therefore, the map $\mathrm{im}(\phi_2) \times \ker(\phi_2) \to D_{2n}$ is a homomorphism. As $\ker(\phi_2) \cap \mathrm{im}(\phi_2) = \{1\}$ and $\ker(\phi_2) \cong \mathbb{Z}/2\mathbb{Z}$, we have $\mathrm{im}(\phi_2) \cong D_n$ and so we get an isomorphism

$$D_n \times \mathbb{Z}/2\mathbb{Z} \to D_{2n}.$$

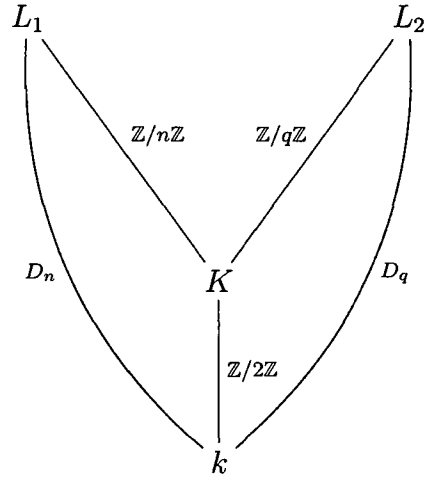
Another proof for the second assertion is as follows: In the special case where n is odd and $q = 2$, D_q is just the Klein four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, thus $G \times_{\mathbb{Z}/2\mathbb{Z}} D_2 \cong G \times \mathbb{Z}/2\mathbb{Z}$ for any group G. In particular, $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$. □

We thus have:

Proposition 5.2.4. *If n is odd, D_{2n} has a generic Galois extension over $\mathbb{Q}$, and hence over any field of characteristic zero.*

Proof. The theorem follows trivially from Theorem 4.4.8, Theorem 4.4.10 and Lemma 5.2.3(a). □

We now try to understand the structure of D_m-Galois extensions when 4 divides m. Any D_m-Galois extension of k will look like the following:



Because of the structure of D_m (Lemma 5.2.3(b)), a D_m-Galois extension of a field k is the compositum of a D_n-Galois extension and a D_q-Galois extension with a common quadratic subextension, where q is the highest power of 2 dividing m.

We know that there exists a generic Galois extension for D_n, and hence we get the $\mathbb{Z}/2\mathbb{Z}$ subextension by taking the invariants of the generic extension under the action of the subgroup $\mathbb{Z}/n\mathbb{Z}$ of D_n. So, if we could find a generic Galois extension for D_q satisfying suitable embedding properties (viz. having the same quadratic subextension as the generic D_n-Galois extension), then we could get a generic Galois extension for D_m. Moreover, the generic Galois extension would

be the fibre product of the generic Galois extensions of D_n and D_q fibred over the common quadratic subextension.

That brings us to the following proposition:

Proposition 5.2.5. *Suppose G_1, G_2 and G_3 are three finite groups with epimorphisms from both G_1 and G_2 to G_3. Further, suppose that both these epimorphisms split. Then, if all the three groups have generic Galois extensions over a field k, then so does $G_1 \times_{G_3} G_2$.*

Proof. The proof is similar to Theorem 4.4.10 and follows from Theorem 3.1 of [29]. □

The above, along with Proposition 5.2.3(b) and Theorem 4.4.8 gives us:

Proposition 5.2.6. *If n is odd, then D_{4n} has a generic Galois extension over any field k of characteristic zero.*

In concluding, we have the following theorem about the existence of generic Galois extensions for a general dihedral group:

Theorem 5.2.7. *Let D_m be a dihedral group with q being the highest power of 2 dividing m. Then D_m has a generic extension over any field k of characteristic zero containing the q^{th} roots of unity.*

Proof. If $q = 2$, we have already shown in Proposition 5.2.4 that D_{2n} has a generic Galois extension over k. If $q > 2$, by Lemma 5.2.3(b), $D_m \cong D_n \times_{\mathbb{Z}/2\mathbb{Z}} D_q$ and the

epimorphisms $D_n \to \mathbb{Z}/2\mathbb{Z}$ and $D_q \to \mathbb{Z}/2\mathbb{Z}$ are both split. Thus, by Proposition 5.2.5, Proposition 5.2.2 and Proposition 5.1.2, we are done. □

Although we can show the existence of generic Galois extensions over $\mathbb{Q}$ for small dihedral 2-groups, we do not have a result as of now which shows the existence of generic Galois extensions over $\mathbb{Q}$ for a general dihedral 2-group. However, one of my future research plans (cf. §6) is to show that we do have something slightly weaker – namely the family of dihedral extensions are "tractable" under certain conditions on the base field.

Chapter 6

Further Investigation and Future Plans

Generalisation to fields of characteristic not equal to 2. I would like to generalise the theorems about central extensions of symmetric and alternating groups from fields of characteristic zero to fields of characteristic not equal to 2. I can generalise most of the results used in the proof from characteristic zero to characteristic not equal to 2. However, Mestre's original result, which is an ingredient of the proof, does not hold in finite characteristic. That is why we interpret Mestre's result more geometrically, by looking at the correspondence between monic polynomials of degree n and affine n-space. We could then try to prove the result over fields of characteristic not equal to 2. We have to exclude fields of characteristic 2 because most of the results we use from the theory of

quadratic forms fail to hold over such fields.

The dihedral group of order 16 Even though one knows from the work of Black that D_8 has a generic Galois extension over $\mathbb{Q}$, it is very difficult to write one down explicitly.

Using techniques similar to the one we used earlier for D_4, we can use Kiming's work ([18]) again to show that the D_8-Galois extensions of k, where k is a field of characteristic zero are:

- $k(\sqrt{-1}, \sqrt{c\sqrt{a}}, \sqrt{(e+d\sqrt{a})\sqrt{c\sqrt{a}}})/k$ where $a, c \in k^\times$, none of $-1, a, -a$ is a square in k, $(a, 2) = 1$ and d and e are solutions in k to the equation $2 = d^2 - ae^2$.
- $k(\sqrt{a}, \sqrt{a-1}, \sqrt{2cf}, \sqrt{k \cdot \frac{1}{g}(2cf + h\sqrt{2cf})})/k$ with certain conditions on the parameters.

The first goal is to combine these two families into one family and write down the generic Galois extension explicitly.

By studying the embedding problem for quadratic extensions into the generic Galois extension for D_8, we can then hope to prove the following:

D_{8n} has a generic Galois extension over any field k of characteristic zero.

Arbitrary Dihedral Groups. I would like to answer the question about the existence of generic Galois extensions over $\mathbb{Q}(i)$ for dihedral groups. As I mentioned in §5.2, the crucial part of the problem is understanding dihedral 2-groups

and so I am trying to answer the question in that case. Once we understand this case, the case of arbitrary dihedral groups will reduce to solving some embedding problems. Finally, if we want to bring down the base field to $\mathbb{Q}$, we can study the ramification behaviour of the generic extensions over $\mathbb{Q}(i)$ and see if the ramification locus is equivariant under the action of the cyclotomic group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. If it is, we can use methods similar to those in [12] to descend the generic extension from $\mathbb{Q}(i)$ to $\mathbb{Q}$.

Essential dimension. In [4], Joe Buhler and Zinovy Reichstein defined "essential dimension" for a finite group G over a field k. The essential dimension for G over k is the minimal dimension of a parameter space of G-Galois extensions over k. For example, we know by Kummer Theory that any $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ for $a, b \in \mathbb{Q}^\times$; and hence the essential dimension of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$ is 2. In my study of dihedral 2-group extensions of $\mathbb{Q}(i)$, I have constructed a certain 2-dimensional family of extensions with Galois group D_q, and I can also show that the essential dimension of D_q over $\mathbb{Q}(i)$ is 2. This implies that my family is a dense subspace of the "parameter space" of D_q-extensions. It remains to determine whether there are D_q-Galois extensions which are missed by the family that I constructed. If not, then my family would indeed be a generic Galois extension. More generally, studying the the essential dimension for a finite group G would help us construct generic Galois extensions for G.

Generic Tractable Extensions We know from the work of Saltman that for any finite group G and any field k, there does not always exist a generic Galois extension for G over k. However, we have shown that there always exists a G-Galois extension S'/R' which parametrises all G-Galois extensions L/K where K/k is a field extension. The issue, however is, that R' may not always be rational.

Saltman, in [29] (p. 261) introduces the notion of generic tractable extensions and proves their existence in the case of cyclic groups. We give a more general definition of generic tractable extensions which agrees with that of Saltman in the case of cyclic groups. We say a generic tractable extension exists for a group G over a field k if there exists a a versal G-torsor with a rational base and which parametrises an open subset of the G-Galois extensions parametrised by the "parameter space".

We would like to prove the following theorem for generic tractable extensions Let k be a field of characteristic zero containing a primitive fourth root of unity e.g. $\mathbb{Q}(i)$. Then D_q has a generic tractable extension over k.

There are three main parts in the proof of the theorem:

1. To show that the essential dimension of D_q is 2.
2. To construct a family of D_q extensions over a 2-dimensional rational base.
3. Show that our 2-dimensional family embeds in the parameter space.

Here Step 3 seems to be the most difficult part.

Arithmetic and Algebraic obstructions. Even when generic extensions

do not exist, we can study the nature of the obstructions – they are usually either arithmetic (e.g. Gruenwald-Wang) or algebraic (e.g. ones arising from division algebras). The question about existence of generic Galois extensions then becomes a question about the vanishing of these obstructions. Understanding these obstructions would then tell us the smallest possible field over which generic Galois extensions could possibly exist. For example, in the case of algebraic obstructions, it would be the smallest field over which the division algebra becomes trivial. I am studying these obstructions in the case of dihedral groups and am planning to understand them for other families of finite groups.

Galois Representations and Work of Khare–Larsen–Savin. I am very interested in understanding the theory of Galois representations and also in using it to attack problems in Galois theory. In particular, I am interested in pursuing methods similar to [43], [19] and [20]. The above are the first instances of simple groups being realised over $\mathbb{Q}$ without using "rigidity". In [20], among other things, Chandrasekhar Khare, Michael Larsen and Gordan Savin construct a continuous irreducible representation $\rho : G_{\mathbb{Q}} \to GL_n(\overline{\mathbb{Q}_l})$ that is unramified outside l, the infinite place ∞ and another auxiliary prime q with certain conditions on the image. They then use these to realise some groups of Lie type as Galois groups over $\mathbb{Q}$. However unlike rigidity, their work realises groups as Galois groups over $\mathbb{Q}$ and not $\mathbb{Q}(t)$. I am interested in pursuing generalisations of their results to $\mathbb{Q}(t)$ (with $\mathbb{Q}$ algebraically closed in the extension) instead of $\mathbb{Q}$. The approach Khare, Larsen

and Savin use involves constructing an automorphic form of the required type and then asserting the existence of Galois representations for automorphic forms. It might be difficult to generalise this approach to $\mathbb{Q}(t)$ as there is no good theory of automorphic forms over $\mathbb{Q}(t)$. However, Richard Taylor, using a method of Ravi Ramakrishna, constructs similar Galois representations in [39] using Čebotarev density theorems, Tate's duality and Euler characteristic theorems. I think his method is more amenable to a generalisation over $\mathbb{Q}(t)$ and am very interested in pursuing that possibility.

Bibliography

[1] S. Beckmann, Is Every Extension of $\mathbb{Q}$ the Specialization of a Branched Covering?, Journal of Algebra, **164(2)** (1994), 430 – 451.

[2] E. Black, Arithmetic Lifting of Dihedral Groups, Journal of Algebra, **203(1)** (1998), 12 – 29.

[3] E. Black, Deformations of Dihedral 2-group Extensions over Fields, Transactions of the American Mathematical Society, **351(8)** (1999), 3229 – 3241.

[4] J. Buhler and Z. Reichstein, On the essential dimension of a finite group, Compositio Math., **106(2)** (1997), 159–179.

[5] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics (Volume 138), Springer–Verlag, Berlin, 1993.

[6] P. Dèbes, Galois covers with prescribed fibers: the Beckmann-Black problem, Ann. Scuola Norm. Pisa Cl. Sci.(4), **28(2)** (1999), 273–286.

[7] F. DeMeyer, Generic Polynomials, J. Algebra, **84(2)** (1983), 441–448.

[8] F. DeMeyer and E. Ingraham, Separable Algebras over Commutative Rings, Lecture Notes in Mathematics (No. 181), Springer-Verlag, Berlin, 1971.

[9] F. DeMeyer, T.McKenzie, On Generic Polynomials, J. Algebra, **261(2)** (2003), 327 – 333.

[10] S. Endô and T. Miyata, Quasipermutation modules over finite groups I, J. Math. Soc. Japan, **25** (1973), 397 – 421.

[11] E. Fischer, Die Isomorphie der Invariantenkörper der endlichen abelschen Gruppen linearer Transformationen, Nachr. d. Ges. d. Wiss. zu Göttingen, (1915), 77 – 80.

[12] D. Harbater, Galois coverings of the arithmetic line, in: Number Theory (New York, 1984–1985), Lecture Notes in Math. (Vol. 1240), Springer–Verlag, Berlin, 1987, pp. 165–195.

[13] V. V. Ishkhanov, B. B. Lur'e and D. K. Faddeev, The Embedding Problem in Galois Theory, Translations of Mathematical Monographs (Volume 165), American Mathematical Society, Providence, Rhode Island, 1997.

[14] I. M. Isaacs, Finite Group Theory, Graduate Studies in Mathematics (Volume 92), American Mathematical Society, Providence, Rhode Island, 2008.

[15] S. Garibaldi, A. Merkurjev and J. -P. Serre, Cohomological Invariants in Galois Cohomology, University Lecture Series (Volume 28), American Mathematical Society, Providence, Rhode Island, 2003.

[16] C. U. Jensen, A. Ledet and N. Yui, Generic Polynomials, Constructive Aspects of the Inverse Galois Problem, Mathematical Sciences Research Institute Publications (Volume 45), Cambridge University Press, Cambridge, United Kingdom, 2002.

[17] G. Kemper, Generic Polynomials are descent-generic, Manuscripta Mathematica, **105(1)** (2001), 139 – 141.

[18] I. Kiming, Explicit Classifications of Some 2-Extensions of a Field of Characteristic Different from 2, Canadian Journal of Mathematics, **42(5)** (1990), 825 – 855.

[19] C. Khare, M. Larsen and G. Savin, Functoriality and the inverse Galois problem, Compos. Math., **144(3)** (2008), 541–564.

[20] ———, Functoriality and the inverse Galois Problem II: groups of type B_n and G_2, to appear in Ann. Fac. Sci. Toulouse Math (2008). Available at: `http://front.math.ucdavis.edu/0807.0861`.

[21] D. Kotlar, M.Schacher and J. Sonn, Central Extensions of Symmetric Groups as Galois Groups, Journal of Algebra, **124** (1989), 183 – 198.

[22] H. W. Lenstra Jr., Rational functions invariant under a finite abelian group, Invent. Math., **25** (1974), 299–325.

[23] T. Maeda, Noether's Problem for A_5, Journal of Algebra, **125(2)**, 418 – 430.

[24] J.-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A_n}$, Journal of Algebra, **131** (1990), 483 – 495.

[25] E. Peyre, Unramified cohomology of degree 3 and Noether's Problem, Invent. Math., **171(1)** (2008), 191–225.

[26] B. Plans, Central Embedding Problems, the Arithmetic Lifting Property, and Tame Extensions of $\mathbb{Q}$, International Mathematics Research Notices, **23** (2003), 1249 – 1267.

[27] B. Plans, Generic Galois Extensions for $SL_2(\mathbb{F}_5)$ over $\mathbb{Q}$, Mathematical Research Letters, **14(3)** (2007), 443 – 452.

[28] D. J. Saltman, Azumaya Algebras with Involution, Journal of Algebra, **52** (1978), 526 – 539.

[29] ———, Generic Galois Extensions and Problems in Field Theory, Advances in Mathematics, **43** (1982), 250 – 283.

[30] ———, Noether's Problem over an algebraically closed field, Invent. Math., **77(1)** (1984), 71–84.

[31] ———, Lectures on division algebras, CBMS Regional Conference Series in Mathematics (Number 94), American Mathematical Society, Providence, Rhode Island, 1999.

[32] L. Schneps, Explicit construction of extensions of $\mathbb{Q}(t)$ of Galois group $\widetilde{A_n}$, J. Algebra, **146(1)** (1992), 117 – 123.

[33] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Commentarii Mathematici Helvetici, **59** (1984), 651 – 679.

[34] ———, Galois Cohomology, Springer-Verlag, Berlin, 1997.

[35] ———, Topics in Galois Theory, Research Notes in Mathematics (Volume 1), A K Peters, Ltd., Wellesley, Massachussetts, 2008.

[36] J. Sonn, Central Extensions of S_n as Galois Groups of Regular Extensions of $\mathbb{Q}(T)$, Journal of Algebra, **140** (1991), 355 – 359.

[37] A. Schmidt and K. Wingberg, Šafarevič's theorem on solvable groups as Galois groups, (1998). Available at: `http://www.math.uiuc.edu/Algebraic-Number-Theory/0136/`.

[38] R. G. Swan, Invariant functions and a problem of Steenrod, Invent. Math., **7** (1969), 148–158.

[39] R. Taylor, On icosahedral Artin representations II, Amer. J. Math., **125(3)** (2003), 549–566.

[40] V. E. Voskresenskii, Rationality of certain algebraic tori (Russian), English translation: Math. USSR Izv., **5** (1971), 1049 – 1056.

[41] S. Wang, A counter-example to Grunwald's theorem, Ann. of Math.(2), **49** (1948) 1008–1009.

[42] ———, On Grunwald's theorem, Ann. of Math.(2), **51** (1950), 471–484.

[43] G. Wiese, On projective linear groups over finite fields as Galois groups over the rational numbers, in: Modular Forms in Schiermonnikoog, B. Edixhoven, G. van der Geer and B. Moonen (eds.), Cambridge University Press, 2008, 343–350.