

Big Mod ℓ Monodromy For Families of G Covers

By

Lalit Jain

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

(MATHEMATICS)

at the

UNIVERSITY OF WISCONSIN – MADISON

2016

Date of final oral examination: June 2, 2016

The dissertation is approved by the following members of the Final Oral Committee:

Professor Jordan S. Ellenberg, Mathematics

Professor Nigel Boston, Mathematics and Electrical & Computer Engineering

Professor Daniel Erman, Mathematics

Professor Richard P. Kent, Mathematics

Professor Robert D. Nowak, Electrical & Computer Engineering

Abstract

The monodromy of a family of varieties is a measure of how homology classes vary. Surprisingly, many familiar ideas in number theory, such as Galois representations and Cohen-Lenstra heuristics, are closely linked to the monodromy of specific families. In general, we expect the monodromy of a family to be “big”, i.e. as large as possible subject to any geometrical or algebraic constraints arising from the family. In this thesis I study the monodromy of Hurwitz spaces of G -covers, moduli spaces for branched covers of the projective line with Galois group G . I show that if G is center-free and has trivial Schur multiplier the mod ℓ monodromy will be big as long as the number of branch points of a curve in the family is chosen to be sufficiently large. Along the way the necessary algebraic results, including a generalized equivariant Witt’s lemma, are presented. The proof relies on a characterization of the connected components of Hurwitz Spaces due to Ellenberg, Venkatesh, and Westerland that generalizes an older result of Conway-Parker and Fried-Völklein. Connections to current results on monodromy of cyclic covers are also discussed.

Acknowledgements

I want to begin by thanking my advisor, Professor Jordan Ellenberg for his mentorship and advice both professionally and personally. His flexibility allowed me to explore a broad range of ideas and projects during my PhD. Graduate school would have been much more difficult without his patience, enthusiasm, and encouragement.

I'd also like to give a special thanks to Professor Robert Nowak for allowing me to be involved in his lab and introducing me to machine learning and statistical learning theory. Becoming immersed in these areas has allowed me to think about problems outside the scope of my algebraic training and I am grateful to be able to explore such an exciting new area of research.

Other faculty who were an important part of my experience at UW-Madison include (but is certainly not limited to) Professors Nigel Boston, Daniel Erman, David Zureick-Brown, Melanie Matchett-Wood, Tonghai Yang, Richard Kent, and Robert Harron.

There are several peers I would like to thank for the many hours they spent discussing mathematics, listening to practice talks, and actively collaborating with me. Specifically, Daniel Ross, Nathan Clement, Ed Dewey, Evan Dummit, Márton Hablicsek, Leland Jeffers, and Kevin Jamieson. Many others have provided me emotional support and friendship over the years. These include Eric Hall, Aaron Peterson, Keith D'Souza, Aniruddha Bhargava, Mimansa Vahia, Blake Mason, Rachel Davis and Yongqiang Zhang.

Other people who were kind enough to discuss the ideas of this thesis include Professors Jeff Achter, Rachel Pries, Craig Westerland, Dan Margalit, and T. N. Venkataramana. Thanks to all of you for your suggestions.

Finally (and perhaps most importantly) I have to thank my family for their support through the years. Gudda (my brother Yajit) has been my best friend and sounding board. My parents started me on this path by making sure to teach me math over the dining table or while driving in the car. My journey would have been nearly impossible without the encouragement and resources you all have provided.

List of Figures

1	The Dehn Twist action of γ_i	11
2	Explicit construction of a D_5 cover.	39
3	Homology basis for C	41
4	The curve γ_1 on C	44

Contents

Abstract	i
Acknowledgements	ii
1 Introduction	1
1.1 Monodromy	1
1.2 Examples of Monodromy	2
1.2.1 Hyperelliptic Monodromy	2
1.2.2 Cyclic Covers and Thin Groups	5
1.3 Monodromy of Hurwitz Spaces	6
2 Topological Properties of Hurwitz Spaces	9
2.1 Introduction	9
2.2 Construction of Hurwitz Spaces	10
2.2.1 Braid Groups and Fundamental Groups	10
2.2.2 Braid Groups and Configuration Spaces	13
2.2.3 Nielsen Classes and Hurwitz Spaces	13
2.3 Hurwitz Monodromy Action	17
2.4 Connectedness Results	18
3 The Algebra of Monodromy	20
3.1 Centralizers of Group Actions	20
3.1.1 Alternating Forms	20

3.1.2	Equivariant Witt's Lemma	24
3.1.3	Symplectic centralizers of representations	28
3.2	Transitivity Results	30
3.3	Subgroups of Products of Groups	34
4	Explicit Dihedral Monodromy	38
4.1	Introduction and Topological Construction	38
4.2	Homology of the Cover	40
4.3	The Hurwitz Monodromy group	42
5	Transitivity and Big Monodromy	47
5.1	Problem Statement	47
5.2	Galois Action on Homology	48
5.3	Covers Corresponding to Subspaces	51
5.4	Proof of the Main Monodromy Theorem	55
	Bibliography	59

Chapter 1

Introduction

1.1 Monodromy

Let $X \rightarrow S$ be a proper family of complex Riemann surfaces with S an irreducible manifold. Given a point $s \in S$, the fundamental group $\pi_1(S, s)$ acts linearly on the homology, $H_1(X_s, \mathbb{Z})$, of the fiber X_s . There is an associated monodromy map

$$\rho : \pi_1(S, s) \rightarrow GL(H_1(X_s, \mathbb{Z}))$$

whose image is called the *monodromy group* of the family.

Intuitively, given a loop $\gamma \in \pi_1(S, s)$, the monodromy action takes hold of a homology class of X_s , and “moves” it along the fibers of the points of γ in X . We will also be interested in the mod ℓ -monodromy of ρ given by composing with the natural $\mathbb{Z}/\ell\mathbb{Z}$ quotient,

$$\rho_\ell : \pi_1(S, s) \rightarrow GL(H_1(X_s, \mathbb{Z}/\ell\mathbb{Z})).$$

We are interested in situations where the monodromy group is *big* relative to any constraints. As the most simple example, the monodromy group has to preserve the natural symplectic intersection form on $H_1(X_s, \mathbb{Z})$ so,

$$\text{im } \rho \subset \text{Sp}(H_1(X_s, \mathbb{Z}))$$

where $\mathrm{Sp}(X_s, \mathbb{Z})$ is the subgroup of $GL(H_1(X_s, \mathbb{Z}/\ell\mathbb{Z}))$ preserving the intersection pairing.

As an explicit example of a big monodromy group, for $g > 1$, let $S = M_g$ be the moduli space of genus g curves, and $X = C_g$ to be the universal curve lying over M_g . Then there is a monodromy action $\pi_1(M_g) \rightarrow \mathrm{Sp}(2g, \mathbb{Z})$. The fundamental group of M_g is well known to be the mapping class group Γ_g of genus g surfaces, and the image of this representation is known to be surjective [18, Section 6.3].

However, we will not use big to necessarily mean that the image of monodromy surjects onto the symplectic group. In particular, big could imply that the monodromy lies in a finite index subgroup of the symplectic group or in the mod ℓ case contains a commutator subgroup of a group containing its image. In this thesis we establish big monodromy for families of surfaces that are regular covers of $\mathbb{P}^1(\mathbb{C})$ with a fixed number of branch points and have a specified deck group. Before stating our problem and results, we provide examples of big monodromy computations and applications of these computations

1.2 Examples of Monodromy

1.2.1 Hyperelliptic Monodromy

Recall the definition of configuration space.

Definition 1.2.1. *The configuration space on n points, $\mathrm{Conf}_n(\mathbb{C})$, is the set of unordered tuples of points in $\mathbb{A}^1(\mathbb{C})$.*

Concretely we can realize $\text{Conf}_n(\mathbb{C})$ as an open subset of $\mathbb{A}^1(\mathbb{C})^n$. Indeed,

$$\text{Conf}_n(\mathbb{C}) = \{(b_1, \dots, b_n) | b_i \neq b_j, 1 \leq i, j \leq n\} / S_n.$$

where the symmetric group S_n acts by permuting the coordinates.

In the context of monodromy, we will take $S = \text{Conf}_n(\mathbb{C})$ and X to be the family of hyperelliptic curves whose fiber over a specific configuration $\{b_1, \dots, b_n\}$ is the normalization of the affine curve

$$y^2 = (x - b_1) \cdots (x - b_n)$$

It is well known (and will be discussed further in Chapter 2) that $\pi_1(\text{Conf}_n(\mathbb{C})) \cong \text{Br}_n$, where Br_n is the braid group on n -strands. Hence the natural monodromy representation,

$$\text{Br}_n \rightarrow \text{Sp}(2g, \mathbb{Z})$$

is a symplectic representation of the braid group.

Computing the image of monodromy in this case is a well studied problem. A'Campo [2], shows that the monodromy group is a finite index subgroup of $\text{Sp}(2g, \mathbb{Z})$ contained in the level 2 congruence subgroup and containing the level 4 congruence subgroup. In this case, big monodromy implies that the monodromy group is a finite index subgroup of the symplectic group. Achter-Pries [4], Hall [23], and Yu [41] all independently showed that the mod ℓ -monodromy group is the full symplectic group for $\ell > 2$. Their work was more general and applied to families of curves not just defined over $\mathbb{C}$.

The hyperelliptic monodromy results described above have a natural application in number theory through the Cohen-Lenstra Heuristics that we now quickly describe.

For $D \in \mathbb{N}$, let S_D be the set of quadratic imaginary fields of discriminant less than D . The Cohen-Lenstra conjectures [11] predict that the average number of surjections

from the class group of a quadratic imaginary field to a finite abelian ℓ -group A is 1, i.e.

$$\lim_{D \rightarrow \infty} \frac{\sum_{K \in S_D} |\text{Surj}(C_K, L)|}{|S_D|} = 1$$

The Cohen-Lenstra conjecture is mostly open and there are only known and partial results in the case where $A = \mathbb{Z}/3\mathbb{Z}$ and $A = \mathbb{Z}/4\mathbb{Z}$ [12, 40].

Friedman and Washington [20] formulated an analogous version of the Cohen-Lenstra conjecture for function fields. Let $\mathbb{F}_q$ be a finite field with $(q, \ell) = 1$ and for n odd let $U_n(\mathbb{F}_q)$ be the set of monic polynomials of degree n . Then for a fixed $f(x) \in U_n(\mathbb{F}_q)$, the hyperelliptic curve H_f with affine model $y^2 = f(x)$ is ramified at ∞ and the class group of $\mathbb{F}_q(t)(\sqrt{f})$ can be identified with $\text{Jac}(H_f)$. Then the Friedman-Washington conjecture states that for a finite abelian ℓ group A ,

$$\lim_{n \rightarrow \infty, n: \text{odd}} \frac{\sum_{f \in U_n} |\text{Surj}(\text{Jac}(H_f), A)|}{|U_n(\mathbb{F}_q)|} = 1$$

There is a version for n -even as well that we omit. In the work of Achter [3], and in unpublished work of Yu [41], (see also the notes of Ellenberg [15]) equidistribution results are exploited to show that big monodromy of the hyperelliptic family provides Cohen-Lenstra type results in the case when n is fixed but q is allowed to grow. In particular they prove

$$\lim_{q \rightarrow \infty, q \not\equiv 1 \pmod{\ell}} \frac{\sum_{f \in U_n} |\text{Surj}(\text{Jac} H_f(\mathbb{F}_q), A)|}{|U_n(\mathbb{F}_q)|} = 1.$$

The original Friedman-Washington conjecture is still open however. We refer the reader to the work of Ellenberg, Venkatesh, and Westerland [16] for more information.

1.2.2 Cyclic Covers and Thin Groups

We now consider the case of general cyclic covers of $\mathbb{P}^1(\mathbb{C})$ rather than just hyperelliptic covers. Again take $S = \text{Conf}_n(\mathbb{C})$ and X to be the family of hyperelliptic curves whose fiber over a specific configuration $\{b_1, \dots, b_n\}$ is the normalization of the affine curve

$$y^d = (x - b_1) \cdots (x - b_n)$$

where $d > 2$.

In this case, the monodromy group can not be the full symplectic group. Each fiber has an action of $\mathbb{Z}/d\mathbb{Z}$ coming from the deck group

$$\{(x, y) \rightarrow (x, \zeta_d^i y) : 1 \leq i \leq d\}.$$

In particular the deck group acts on the homology of a fiber and the monodromy group is forced to lie in the subgroup of $\text{Sp}(2g, \mathbb{Z})$ that commutes with the $\mathbb{Z}/d\mathbb{Z}$ action. The monodromy group is forced to be a subgroup of the *symplectic centralizer* of $\mathbb{Z}/d\mathbb{Z}$.

Motivated by *big* monodromy in the hyperelliptic case, it is reasonable to ask whether the monodromy group is an *arithmetic subgroup* of the symplectic centralizer, or alternatively of finite index. Alternatively, we can ask whether the monodromy group can ever be *thin*, i.e. Zariski dense in the symplectic centralizer but of finite index.

Building on work of Deligne and Mostow, McMullen [32] shows that when $d = 4$ and $n = 18$ the monodromy group is indeed thin, providing one of the first examples of a thin group. However when $m \geq 2d$ recent work of Venkataramana [37, 38] shows that the monodromy group is indeed an arithmetic subgroup.

Venkataramana's result implies that the mod ℓ -monodromy group is the full symplectic centralizer for ℓ sufficiently large. In particular we can hope that we might be

able to detect thin-ness by looking mod ℓ . However this is not possible due to a result of Vaserstein and Weisfeiler [31]. They show that for a connected algebraic group G any finitely-generated Zariski-dense subgroup of G will surject onto $G(\mathbb{Z}/p\mathbb{Z})$ for p sufficiently large.

1.3 Monodromy of Hurwitz Spaces

In this report, the families of interest will be *Hurwitz spaces*, moduli spaces of regular covers of $\mathbb{P}^1(\mathbb{C})$. Fix a center-free group G , a choice of conjugacy classes $\mathcal{C} := (\mathcal{C}_1, \dots, \mathcal{C}_k)$, and a tuple of integers $\mathbf{m} := (m_1, \dots, m_k)$. More specifically

Definition 1.3.1. *A cover of type $(G, \mathcal{C}, m)$, will be given by tuple $(E_1, \dots, E_k, f)$ where*

- *Each $E_i \subset \mathbb{C}$ is a subset of size m_i .*
- *$f : \pi_1(\mathbb{P}_{\mathbb{C}}^1 - \bigcup E_i) \twoheadrightarrow G$ is a surjection.*
- *f maps a loop around each point of E_i to $\mathcal{C}_i$.*

Each such surjection gives rise to a G cover of $\mathbb{P}^1(\mathbb{C})$ with specified ramification at the $E = \bigcup E_i$ lying in $\bigcup \mathcal{C}_k$. The space of all such covers is the *Hurwitz space* of connected G -covers and is denoted by $\text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}$. The examples given above of hyperelliptic covers and more general cyclic covers are specific instances of Hurwitz spaces.

For a fixed isomorphism class of $(G, \mathcal{C}, \mathbf{m})$ covers denoted C , there is an associated point $[C] \in \text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}$. As described in the introduction and explicitly described in section 2.3 there is an associated mod ℓ -monodromy representation,

$$\rho_{G, m}^{\mathcal{C}} : \pi_1(\text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}, [C]) \rightarrow \text{Sp}(H_1(C, \mathbb{Z}/\ell\mathbb{Z}))$$

for a prime l . Denote the associated monodromy group by $M_\ell(G)$.

The $\mathbb{F}_\ell$ vector space $V_\ell = H_1(C, \mathbb{Z}/\ell\mathbb{Z})$ carries an symplectic intersection form, and a natural action of G . As in the case of cyclic covers discussed in the previous section, the monodromy group, $M_\ell(G)$, must preserve the form and commute with the action of G , so $M_\ell(G) \subset C_{\text{Sp}(V_\ell)}(G)$, the *symplectic centralizer* of G .

In the mod ℓ case the symplectic centralizer is finite, so finite index is not an effective way to define the word *big*. Instead, we take *big* to mean that the monodromy group contains the commutator subgroup of the symplectic centralizer. We prove the following result.

Theorem (Theorem 5.4.2). *Fix a center-free group G with $H_2(G, \mathbb{Z}) = 0$ and a prime $\ell \nmid 2|G|$. If $\min_i m_i$ sufficiently large, $CHur_{G, \mathbf{m}}^\mathcal{C}$ has big monodromy,*

$$[C_{\text{Sp}(V_\ell)}(G), C_{\text{Sp}(V_\ell)}(G)] \subset M_\ell(G)$$

As described in section 3.1, the symplectic centralizer decomposes as a product of general linear, symplectic, unitary and orthogonal groups. Hence requiring the monodromy group to contain the commutator is analogous to having a subgroup of the general linear group containing the special linear group. This is certainly an adequate notion of a *big* subgroup.

The rough strategy to prove Theorem 5.4.2 is as follows. The monodromy group $M_\ell(G)$ naturally acts on certain G -invariant subspaces of $H_1(C, \mathbb{Z}/\ell\mathbb{Z})$. These subspaces correspond to covers of C in a natural way and using results from [17], we will be able to compute the number of orbits of $M_\ell(G)$ on these subspaces. Subsequently, theorems about transitivity from finite group theory, and projective geometry, will demonstrate that $M_\ell(G)$ is *big* in a natural way.

Note that this approach greatly differs from the methods used in several of the results cited (for example [23, 30]) in previous sections to compute big monodromy. In most of these cases, monodromy is shown to be a large subgroup of the symplectic group by demonstrating the existence of enough transvections. We provide an example in Chapter 4 which emulates such an argument, but the proof of the main theorem uses purely global topological results.

The thesis is broken into four sections. Chapter 2 provides background on Hurwitz spaces and the associated monodromy representations. In Chapter 3, the necessary algebraic tools for the proof of Theorem 5.4.2 are provided. Chapter 4 gives an explicit computation for a specific case of dihedral monodromy by constructing explicit mapping classes acting on a dihedral cover of $\mathbb{P}^1(\mathbb{C})$. The final chapter provides a full proof of the main theorem.

Chapter 2

Topological Properties of Hurwitz Spaces

2.1 Introduction

Informally, Hurwitz spaces parametrizes isomorphism classes of covers of the projective line $\mathbb{P}^1(\mathbb{C})$ with prescribed extra information. This could include data about ramification, degree, or automorphisms (as we are primarily concerned with in this thesis). Hurwitz spaces have a rich history dating back to work of Clebsch, Hurwitz and Lüroth in the 1880's. The study of the topological properties of Hurwitz spaces has been applied with great success to combinatorial group theory, the connectedness of the moduli space of curves M_g [21], the inverse Galois problem [19], and as described in the introduction to the Cohen-Lenstra conjectures [16].

In this section, we provide an introduction to the theory of Hurwitz spaces from a group theoretic point of view. First we introduce the definition of the braid group and its action on Nielsen classes of a group. This is followed up by an explicit definition of Hurwitz spaces and their monodromy action on the homology of a curve. Finally we describe results of Conway-Parker-Fried, and Ellenberg-Venkatesh-Westerland on counting the components of Hurwitz spaces.

The interested reader is pointed to [35], [16], [36] for more information on the constructions in this chapter.

2.2 Construction of Hurwitz Spaces

2.2.1 Braid Groups and Fundamental Groups

In this section we provide a quick summary of many standard facts on mapping class groups of surfaces, braid groups, and configuration spaces. The interested reader is directed to [18] for more information on these topics.

Definition 2.2.1. *Let S be a surface with boundary ∂S . The Mapping Class Group of S , denoted $Mod(S)$ is defined to be the group of isotopy classes of orientation preserving homeomorphisms of S that are the identity on ∂S . In other words,*

$$Mod(S) = Homeo^+(S, \partial S) / Homeo_0(S, \partial S)$$

Fix a decomposition of projective space $\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \cup \{\infty\}$. In addition choose a set of points $\mathbf{b} = \{p_1, \dots, p_n\} \subset \mathbb{A}^1(\mathbb{C})$.

Instead of the whole mapping class group of $\mathbb{P}^1(\mathbb{C})$, we will be interested in understanding the mapping classes of $\mathbb{P}^1(\mathbb{C}) - \mathbf{b}$ fixing ∞ which we denote by β_n . A general homeomorphism of $\mathbb{P}^1(\mathbb{C}) - \mathbf{b}$ can send a neighborhood of one of the punctures contained in $\mathbb{A}^1(\mathbb{C})$ to a neighborhood around ∞ . Treating ∞ as a puncture, β_n can be identified with the index $n + 1$ subgroup of $mod(\mathbb{P}^1(\mathbb{C}) - \mathbf{b} \cup \infty)$ that fixes ∞ . Through stereographic projection through ∞ , β_n can also be identified with the mapping class group of the n -times punctured plane, $Mod(\mathbb{A}^1(\mathbb{C}) - \mathbf{b})$. We can explicitly find a presentation of β_n by studying its connection to *Artin's Braid Group*.

Definition 2.2.2. *Artin's braid group on n strands, is given in terms of generators and relations as*

$$Br_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i \sigma_j = \sigma_j \sigma_i, \text{ if } |i - j| \geq 2, \text{ otherwise } \sigma_{i+1} \sigma_i \sigma_{i+1} = \sigma_i \sigma_{i+1} \sigma_i \rangle$$

The braid group can be identified with the compactly supported mapping classes of $\mathbb{A}^1(\mathbb{C}) - \mathbf{b}$ or alternatively the mapping classes of the closed disk D^2 with n punctures, also denoted $\mathbf{b}$, fixing the boundary of the disk. As shown in Figure 2.2.1 under this isomorphism the action of σ_i is a *Dehn Twist* which acts by a 180° rotation in a neighborhood of p_i, p_{i+1} not containing any other of the points $p_1, \dots, p_n$.

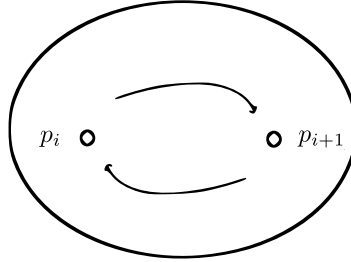


Figure 1: The Dehn Twist action of γ_i .

By taking a small open disc U around $\infty \in \mathbb{P}^1(\mathbb{C})$, we can fix a homeomorphism from $D^2 - \mathbf{b} \rightarrow \mathbb{P}^1(\mathbb{C}) - \mathbf{b} - U$ by mapping the boundary of D^2 , ∂D^2 , to ∂U . This gives rise to a map from $Br_n \rightarrow \beta_n$.

The kernel of this map is generated by the Dehn Twist around a circle in D^2 near ∂D^2 . The subgroup generated by this Dehn twist is the center of B_n and in terms of generators is explicitly given by $\Delta^2 = (\sigma_1 \sigma_2 \cdots \sigma_{n-1})^n$. In particular

$$\beta_n \cong Br_n / \langle \Delta^2 \rangle.$$

We refer the reader to [18, Chapter 9] for more details on this isomorphism.

Having established a presentation for β_n , we now introduce the action of β_n on the free group. Choose a set of pairwise non-intersecting loops $\gamma_i, 1 \leq i \leq n$ based at ∞ such that γ_i winds around p_i once. Then a presentation for the fundamental group of $\mathbb{P}^1(\mathbb{C}) - \mathbf{b}$ is given by,

$$\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) = \langle \gamma_1, \dots, \gamma_n \mid \gamma_1 \cdots \gamma_n = 1 \rangle$$

So in particular $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty)$ is isomorphic to a free group. In general the choice of $\{\gamma_i\}$ is not unique but any other choice of loops $\{\gamma'_i\}$ is related to γ_i by a diffeomorphism fixing ∞ .

Since the action of β_n fixes ∞ , it induces an action on $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty)$

$$\beta_n \rightarrow \text{Aut}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty)),$$

often referred to as the *braiding action on the free group*. By explicitly analyzing the action of each σ_i this action can explicitly be described on γ_i by,

- $\sigma_i \cdot \gamma_i = \gamma_{i+1}$
- $\sigma_i \cdot \gamma_{i+1} = \gamma_i^{-1} \gamma_{i+1} \gamma_i$.

See [39, Theorem 10.13] for a proof.

Since β_n is a quotient of Br_n , we can lift this action to Br_n ,

$$\text{Br}_n \rightarrow \text{Aut}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty))$$

Each braid permutes the points $\{p_1, \dots, p_n\}$, with the generator σ_i transposing p_i, p_{i+1} and leaving the rest of the points fixed. This gives rise to a homomorphism,

$$\text{Br}_n \rightarrow S_n$$

the kernel of this map is often referred to as the *pure braid group*.

2.2.2 Braid Groups and Configuration Spaces

In addition to being identified as a mapping class group, the braid group also has a realization as a fundamental group of configuration space.

Definition 2.2.3. *The configuration space on n points $\text{Conf}_n(\mathbb{C})$ is the set of unordered tuples of distinct points in $\mathbb{A}^1(\mathbb{C})$.*

Concretely we can realize $\text{Conf}_n(\mathbb{C})$ as an open subset of $\mathbb{A}^1(\mathbb{C})^n$.

$$\text{Conf}_n(\mathbb{C}) = \{(b_1, \dots, b_n) | b_i \neq b_j, b_i, b_j \in \mathbb{A}^1(\mathbb{C}), 1 \leq i, j \leq n\} / S_n.$$

where the symmetric group S_n acts by permuting the coordinates.

Intuitively, a loop in $\text{Conf}_n(\mathbb{C})$ is a continuous motion of a set of points that can be realized through a mapping class. So it is not surprising that the fundamental group of configuration space is given by the braid group.

Theorem 2.2.4 ([18, Section 9.1.1]). *Let $c \in \text{Conf}_n(\mathbb{C})$ be an unordered tuple of points, then*

$$\pi_1(\text{Conf}_n(\mathbb{C}), c) \cong Br_n$$

2.2.3 Nielsen Classes and Hurwitz Spaces

In this section we define an action of the braid group on a set that will naturally give rise to a cover of configuration space parametrizing branched covers of $\mathbb{P}^1(\mathbb{C})$.

For a fixed n and group G , the set of *Nielsen classes* of G is,

$$E_n(G) = \{\mathbf{g} = (g_1, \dots, g_n) \in G^n | g_1 \cdots g_n = 1, \langle g_1, \dots, g_n \rangle = G\}.$$

In the notation of the previous sections, assume $\mathbf{b}$ is an ordered tuple of n distinct points in $\mathbb{A}^1(\mathbb{C})$. Let $\text{Surj}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$ denote the set of surjections from $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) \rightarrow G$. Since each such surjection is specified by the images of the generators $\gamma_1, \dots, \gamma_n$, there is a natural bijection between $\text{Surj}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$ and $E_n(G)$.

The action of Br_n on $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty)$ described above induces an action on $\text{Surj}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$. Namely given $\sigma \in \text{Br}_n$, and $\phi \in \text{Surj}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$, $\sigma \cdot \phi = \phi \circ \sigma$. This translates into a *braiding action* on $E_n(G)$, given on the generators by

$$\sigma_i \cdot (g_1, \dots, g_i, g_{i+1}, \dots, g_n) = (g_1, \dots, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \dots, g_n)$$

The braid action specified above naturally gives rise to a topological cover of configuration space whose fibers are Nielsen Classes. By the theory of covering spaces and G -sets, there is a topological space $\text{Chur}_{G,n}$ with a map

$$\text{Chur}_{G,n} \rightarrow \text{Conf}_n(\mathbb{C})$$

where the fiber over a point $(p_1, \dots, p_n)$ can be identified with $E_n(G)$ and the action of $\pi_1(B_n, \mathbf{g})$ on the fiber of $\mathbf{g}$ is isomorphic to its action on $E_n(G)$.

We can also describe the points of $\text{Chur}_{G,n}$ as isomorphism classes of branched connected covers of $\mathbb{P}^1(\mathbb{C})$. We say that a Riemann Surface C is specified by the data of $(G, \mathbf{b}, f, \mathbf{x}, \alpha)$ if

- $\mathbf{b} \subset \mathbb{A}^1(\mathbb{C})$ is a set of n distinct points in the interior of $\mathbb{A}^1(\mathbb{C})$.
- C is connected and $p : C \rightarrow \mathbb{P}^1(\mathbb{C})$ is a covering map branched only at $\mathbf{b}$.
- $\mathbf{x}$ is a point above ∞ .

- $\alpha : G \rightarrow \text{Aut}(f)$ is a specified isomorphism inducing a transitive action of G on each fiber.

We say that a surface C' with data $(G, \mathbf{b}, f', \mathbf{x}', \alpha')$ is isomorphic to C if there is a homeomorphism from $\rho : C \rightarrow C'$ such that $f' \circ \rho = f$, $f(\mathbf{x}) = \mathbf{y}$ and $f \circ \alpha(g) = \alpha'(g) \circ f$ for all $g \in G$.

A given $(G, \mathbf{b}, f, \mathbf{x}, \alpha)$ cover C specifies a surjection $\phi_C : \pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) \rightarrow G$. Indeed since the action of G is transitive on $f^{-1}(\infty)$, every point of $f^{-1}(\infty)$ can be identified with an element of G . So given $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}) \rightarrow \mathbf{b}, \infty)$ the $\phi_C(\gamma) = \tilde{\gamma}(1)$ where $\tilde{\gamma}$ is a lift of γ starting at $\mathbf{x}$ and we identify the end point with an element of G . If $C \cong C'$ then it is easy to check that $\phi_C = \phi_{C'}$.

On the other hand given a Nielsen Class $\mathbf{g} \in E_n(G)$ or the corresponding surjection $\phi_{\mathbf{g}} : \pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) \rightarrow G$, standard covering space theory gives the existence of a connected regular cover $f : C \rightarrow \mathbb{P}^1(\mathbb{C}) - \mathbf{b}$, a basepoint $\mathbf{x} \in C$ with $f(\mathbf{x}) = \infty$ and a transitive action of G on the fiber $f^{-1}(\infty)$. The latter action arises from the action of G on the coset space of $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) / \ker \phi_{\mathbf{g}}$.

Thus we see the points of $\text{Chur}_{G,n}$ above $\mathbf{b} \in \text{Conf}_n(\mathbb{C})$ parametrize isomorphism classes of connected regular covers of $\mathbb{P}^1(\mathbb{C}) - \mathbf{b}$ up to isomorphism in the manner specified above. We refer to such $\text{Chur}_{G,n}$ as the *Hurwitz space* parametrizing covers of type (G, n) .

We can generalize the above construction to track additional data. In addition to fixing G , fix a tuple of conjugacy classes $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_n)$, where $\mathcal{C}_i \subset G$, $1 \leq i \leq n$, and a tuple of positive integers $\mathbf{m} = (m_1, \dots, m_n) \in \mathbb{N}^n$. Let $|\mathbf{m}| = m_1 + \dots + m_n$.

The set of Nielsen classes of type $(G, \mathcal{C}, \mathbf{m})$ is

$$E_{\mathbf{m}}(G, \mathcal{C}) = \{\mathbf{g} = (g_1, \dots, g_{|\mathbf{m}|}) \mid g_1 \cdots g_{|\mathbf{m}|} = 1, \langle g_1, \dots, g_{|\mathbf{m}|} \rangle = G, \text{ and } m_j \text{ of } g_i \text{ lie in } \mathcal{C}_j\}.$$

For a given set of $|\mathbf{m}|$ points $\mathbf{b} \subset \mathbb{A}^1(\mathbb{C})$, let

$$\text{Surj}^{\mathcal{C}}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G) \subset \text{Surj}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$$

denote the set of surjections $\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty) \rightarrow G$ ensuring that loops around m_j of the branch points land in $\mathcal{C}_j$. As in the case of $E_n(G)$, there is a natural bijection between $\text{Surj}^{\mathcal{C}}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$ and $E_{\mathbf{m}}(G, \mathcal{C})$.

The action of the Braid group on Nielsen classes preserves $E_{\mathbf{m}}(G, \mathcal{C})$. As mentioned above, $\text{Surj}^{\mathcal{C}}(\pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{b}, \infty), G)$ and $E_{\mathbf{m}}(G, \mathcal{C})$ are in fact isomorphic as $\text{Br}_{|\mathbf{m}|}$ sets.

In addition there is an analogous Hurwitz space along with a map to configuration space

$$\text{CHur}_{G, \mathbf{m}}^{\mathcal{C}} \rightarrow \text{Conf}_{|\mathbf{m}|}(\mathbb{C})$$

where the fiber above any point $\mathbf{E}$ is the set $E_{\mathbf{m}}(G, \mathcal{C})$. As above, the fiber can be identified with covers of type $(G, \mathbf{E}, f, \mathbf{x}, \alpha)$

- $\mathbf{E} = (E_1, \dots, E_n) \subset \mathbb{A}^1(\mathbb{C})$ is a set of size $m_1 + \dots + m_n$ with $|E_i| = m_i$.
- $f : C \rightarrow \mathbb{P}^1(\mathbb{C})$ is a covering map branched only at the points of $\mathbf{E}$.
- $\mathbf{x}$ is a point above ∞ .
- $\alpha : G \rightarrow \text{Aut}(f)$ is a specified isomorphism acting transitively on a fiber.
- The monodromy of a loop around a point in E_i lands in $\mathcal{C}_i$

In general we will say that the Hurwitz space $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ parametrizes covers of type $(G, \mathcal{C}, \mathbf{m})$. Now that the basic definitions are in place throughout the rest of this chapter we will focus on topological aspects of $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$.

2.3 Hurwitz Monodromy Action

In this section we continue exploring the implications of the action of the braid group on the Nielsen classes $E_{\mathbf{m}}(G, \mathcal{C})$ and define the monodromy action on the homology of a curve.

A priori $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is not connected for a given choice of $(G, \mathcal{C}, \mathbf{m})$. By definition $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ will only be connected if the action of $\text{Br}_{|\mathbf{m}|}$ on $E_{\mathbf{m}}(G, \mathcal{C})$ is transitive. If the action is not transitive, let $\text{Stab}_{\text{Br}_{|\mathbf{m}|}}(\mathbf{g})$ be the stabilizer of some $\mathbf{g} \in E_{\mathbf{m}}(G, \mathcal{C})$. This stabilizer can be identified with the fundamental group (based at $\mathbf{g}$) of the connected component of $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ containing $\mathbf{g}$ identified as a point in the fiber of $\mathbf{E} \in \text{Conf}_{\mathbf{m}}(\mathbb{C})$. This fundamental group is often referred to as the *Hurwitz Monodromy group*. We will say more about the connected components of $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ in the next section. However to simplify exposition, for the rest of this section we assume that $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is connected. In other words assume $\text{Stab}_{\text{Br}_{|\mathbf{m}|}}(\mathbf{g}) \cong \pi_1(\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, \mathbf{g})$. Alternatively, fixing a surface C (up to isomorphism) corresponding to $\mathbf{g}$ as described in the previous section, $\text{Stab}_{\text{Br}_{\mathbf{m}}}(\mathbf{g}) \cong \pi_1(\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, [C])$.

Moving away from combinatorial arguments back to topology, recall from Section 2.2.3 that $\pi_1(\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, C) \subset \text{Br}_m$ can be identified with mapping classes fixing the surjection $\mathbb{P}^1(\mathbb{C}) \rightarrow G$ specified by $\phi_{\mathbf{g}}$. By a universal lifting lemma [24], every such mapping class lifts to a mapping class of C preserving the specified basepoint $\mathbf{x} \in C$

and this lift is unique.

This gives rise to the *monodromy action*

$$\pi_1(\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, [C]) \rightarrow \mathrm{Homeo}^+(C, \mathbf{x}).$$

We are primarily concerned with the induced action on homology,

$$\pi_1(\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, [C]) \rightarrow \mathrm{GL}(H_1(C, \mathbb{Z})).$$

or on cohomology

$$\pi_1(\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, [C]) \rightarrow \mathrm{GL}(H^1(C, \mathbb{Z})).$$

We will return to this monodromy action in the next chapter.

Remark. In this chapter we have taken a very topological approach to constructing the monodromy representation. One can also construct *Hurwitz varieties* as moduli spaces (with a variety structure) of $(G, \mathcal{C}, \mathbf{m})$ covers. In the case when G is center-free the resulting variety is a fine moduli space for $(G, \mathcal{C}, \mathbf{m})$ covers. In this case, $\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ admits a cover by a universal curve where the fiber over a point $[C] \in \mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is the curve C . The monodromy action of this family is more akin to the monodromy action defined in the introduction however it will agree with the monodromy action presented in this section. We refer the reader to [36] for more information.

2.4 Connectedness Results

We finish this chapter with a description of results about connected components of Hurwitz Spaces. As has been explained above, in general $\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ does not need to be connected and the connected components of $\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ correspond to orbits of $\mathrm{Br}_{|\mathbf{m}|}$ on $E_{\mathbf{m}}(G)$. In particular, if the action is transitive then $\mathrm{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is connected.

Computing the number of connected components of Hurwitz spaces $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is a well studied problem with roots in work Clebsch, Lüroth and Hurwitz [26]. In the case of $G = S_n$ and $\mathcal{C} = (\mathcal{C}_1)$ where $\mathcal{C}_1$ is the conjugacy class of transpositions, they showed that $\text{Chur}_{S_n,n}^{\mathcal{C}}$ was connected for any choice of n . Conway and Parke in an appendix of a paper by Fried and Völklein ([19]) show that $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is connected in the case when the *Schur Multiplier* $H_2(G, \mathbb{Z})$ is trivial, $\mathcal{C} = (G - \{e\})$ and n is chosen sufficiently large.

In [17], Ellenberg, Venkatesh and Westerland give a method to compute the connected components of $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$. This is a previously unpublished result of Fried. Given a choice of $\mathcal{C}$ as above, $x \in \cup \mathcal{C}_i$ and $y \in G$ such that x, y commute, define the *universal commutator* $\langle x, y \rangle \in H_2(G, \mathbb{Z})$ as the image of the map $\phi_* : H_2(\mathbb{Z}^2, \mathbb{Z}) \rightarrow H_2(G, \mathbb{Z})$ induced by the map $\phi : \mathbb{Z}^2 \rightarrow G : (m, n) \rightarrow x^m y^n$. Define $H_2(G, \mathcal{C})$ to be the quotient of $H_2(G, \mathbb{Z})/Q_{\mathcal{C}}$ where $Q_{\mathcal{C}}$ is the subgroup generated by all such universal commutators. Then [17] proves

Theorem 2.4.1 (Ellenberg-Venkatesh-Westerland, Fried). *For $\min_i m_i$ sufficiently large, there is a bijection*

$$\pi_0(\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}) \rightarrow H_2(G, \mathcal{C}).$$

In the case of the symmetric group, the quotient above is trivial (the Schur multiplier is generated by commutators) recovering the results mentioned above. In general if $H_2(G, \mathbb{Z})$ is trivial, we can expect $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ to be connected. The theorem gives an effective way to compute the number of components of $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ by finding appropriate quotients of Schur multipliers.

Chapter 3

The Algebra of Monodromy

In this chapter we present several of the algebraic tools that will be needed for the proof of Theorem 5.4.2. This includes an explicit computation of the symplectic centralizer of a symplectic representation, a discussion on transitive subgroups of linear groups, and a characterization of certain subgroups of products of linear groups.

Many of the group theoretic ideas (though not the exact results) in the second section have been used in various other contexts related to monodromy groups and inverse Galois problems. We try to point our connections with the existing literature whenever possible. This chapter is self contained and may be used as a reference for the rest of the thesis.

3.1 Centralizers of Group Actions

3.1.1 Alternating Forms

Let G be an arbitrary group and ℓ a prime such that $\ell \nmid 2|G|$. In this section and the next, we classify the possibilities for the set of matrices that commute with an arbitrary homogenous G -representation that also preserves a symplectic form. Let W be an irreducible $\mathbb{F}_\ell[G]$ module, equipped with a nondegenerate G -invariant form b .

Definition 3.1.1. *A nondegenerate G -invariant form b is an ϵ -form if*

$$b(x, y) = \epsilon b(y, x),$$

where $\epsilon = \pm 1$. In the case where $\epsilon = 1$, we say b is symmetric and when $\epsilon = -1$, b is alternating.

Let the space of G -invariant bilinear forms be denoted by Bil^G and the space of ϵ -forms be denoted by Bil_ϵ^G . Hence, $\text{Bil}_1^G = (\text{Sym}^2 W)^G$ and similarly $\text{Bil}_{-1}^G = (\text{Alt}^2 W)^G$.

Since W is irreducible, Schur's lemma implies that $\text{End}_G(W)$ is a division ring over $\mathbb{F}_\ell$ and hence a finite field. Let $D := \text{End}_G(W)$ and so we can view W as a vector space D . Define $d := [D : \mathbb{F}_\ell]$, so that D is a degree d extension of $\mathbb{F}_\ell$, $D \cong \mathbb{F}_{\ell^d}$.

Denote the map from $W \rightarrow W^\vee$ that sends $x \in W$ to $b(x, \cdot)$ by $\tilde{b}$. There is an adjoint involution on $\text{End}_{\mathbb{F}_\ell}(W)$ induced by b , namely for any $A \in \text{End}_{\mathbb{F}_\ell}(W)$, we define $i_b(A) \in \text{End}_{\mathbb{F}_\ell}(W)$ to be the endomorphism satisfying

$$b(Ax, y) = b(x, i_b(A)y).$$

for all $x, y \in W$. We also define the *symplectic group* of isometries of b ,

$$\text{Sp}(W, b) = \{A \in \text{GL}(W) : b(Ax, Ay) = b(x, y) \text{ for all } x, y \in W\}.$$

Notice that $A \in \text{Sp}(W, b)$ is equivalent to $i_b(A) = A^{-1}$. If $A^\vee : W^\vee \rightarrow W^\vee$ is the map between duals induced by W we can explicitly compute

$$i_b(A) = \tilde{b}^{-1} \circ A^\vee \circ \tilde{b}.$$

Lemma 3.1.2. *The involution i_b preserves $\text{End}_G(W)$.*

Proof. Let $A \in \text{End}_G(W)$ so that $Ag = gA$ for all $g \in G$. Then taking the adjoint of both sides we see that $i_b(g)i_b(A) = i_b(A)i_b(g)$ but since b is G -invariant, $i_b(g) = g^{-1}$. This implies that $i_b(A)$ commutes with the action of G giving the result. $\square$

Lemma 3.1.3. *Let the fixed field of i_b on D be denoted K . There is a bijection $K \cong \text{Bil}_\epsilon^G$ and in particular, $\text{Bil}_\epsilon^G - \{0\}$ is a torsor for K^* . Given h in Bil_ϵ^G there is a $d \in \text{End}_G(W)$ such that*

$$b(\cdot, \cdot) = h(d\cdot, \cdot).$$

In addition, $h \in \text{Bil}_\epsilon^G$, iff $d \in K$.

Proof. We begin by providing a bijection from K to Bil_ϵ^G . Given $k \in K$, consider the non-degenerate form $b_k = b(k\cdot, \cdot)$. This is an ϵ -form since

$$\begin{aligned} b(ky, x) &= \epsilon b(x, ky) \\ &= \epsilon b(i_b(k)x, y) \\ &= \epsilon b(kx, y). \end{aligned}$$

Since k commutes with G , b_k is also G -equivariant. This defines a map of $\mathbb{F}_\ell$ vector spaces, $\phi : K \rightarrow \text{Bil}_\epsilon^G$ given by $\phi(k) = b_k$. Since b is non-degenerate, this map is necessarily injective.

Let h be another ϵ -form. Notice that $\tilde{b}^{-1} \circ \tilde{h} : W \rightarrow W$ is a G -invariant map, so $\tilde{b}^{-1} \circ \tilde{h} = d$ for some $d \in \text{End}_G(W)$. This implies that $h(\cdot, \cdot) = b(d\cdot, \cdot)$. A computation similar to the above shows that $d \in K$, implying the surjectivity of ϕ . $\square$

Two forms $h, g \in \text{Bil}_\epsilon^G$ are considered G -equivalent if there is a $d \in \text{End}_G(W)$ such that $g(x, y) = h(dx, dy) = h(i_h(d)dx, y)$.

Lemma 3.1.4. *One of the following two possibilities must occur.*

- i_b acts trivially on $\text{End}_G(W)$, $\text{Bil}^G \cong \text{Bil}_\epsilon^G$ and there are two classes of G -invariant bilinear forms up to G -equivalence.
- i_b acts nontrivially on $\text{End}_G(W)$, $\text{Bil}^G = (\text{Sym}^2 W)^G \oplus (\text{Alt}^2 W)^G$ and there is a unique class of bilinear epsilon forms up to G -equivalence.

Proof. First, assume that i_b acts trivially on D . Then $D = K$ and every G -invariant bilinear form is an ϵ -form by lemma 2.2. Any form equivalent to b must be of the form $b(d^2 \cdot, \cdot)$, with $d \in \text{End}_G(W)$. Since D is a finite field, $[D^* : (D^*)^2] = 2$. Hence every G -invariant is equivalent to either $b(ax, y)$ or $b(x, y)$ for a a non-square in $\text{End}_G(W)$. So there are two classes of non-equivalent Bil^G forms.

If i_b acts non-trivially, then $[D : K] = 2$ and since $\dim \text{Bil}_\epsilon^G = \dim K$, we see that $\text{Bil}^G = (\text{Sym}^2 W)^G \oplus (\text{Alt}^2 W)^G$ where $\dim(\text{Sym}^2 W)^G = \dim(\text{Alt}^2 W)^G = [D : K]/2$. As before, any form equivalent to b must be of the form $b(i_b(d)d \cdot, \cdot)$. The map $D \rightarrow K : d \rightarrow i_b(d)d$ is surjective since it is just the norm map. So there is a unique class of bilinear epsilon forms up to G -equivalence. $\square$

If the first case occurs, then we say W is *type 1*. If the second case occurs, we say W is *type 2*.

Remark 1. Note that if W is *absolutely irreducible* over $\mathbb{F}_\ell$ if and only if $\text{End}_G(W) = \mathbb{F}_\ell$. In this case we must have that $D = K$ and we must be in case 1, so either $\dim(\text{Sym}^2 W)^G$ or $\dim(\text{Alt}^2 W)^G$ is one.

This theorem is related to the Frobenius-Schur theory for characterizing irreducible real representations. A similar phenomenon happens with real representation. Indeed,

let W be an irreducible $\mathbb{R}$ self-dual representation of a group G , as above,

$$\mathrm{End}_G W \cong (W \otimes W^*)^G \cong (W^* \otimes W^*) \cong (\mathrm{Sym}^2 W)^G \otimes (\mathrm{Alt}^2 W)^G$$

Furthermore, if χ is the character of the representation, then χ must be real valued, and in particular W is isomorphic to $W^\vee$. We can consider $cW = W \otimes \mathbb{C}$, the complexification of W .

Then one of the following occurs,

- $\mathrm{End}_G(W) = \mathbb{R}$: One of $\mathrm{Sym}^2 W$ or $\mathrm{Alt}^2 W$ has dimension 1. This is analogous to part a of the theorem.
- $\mathrm{End}_G(W) = \mathbb{C}$: In this case, $cW = V \oplus \bar{V}$ with $V \not\cong \bar{V}$. As in lemma 3.1.4, either $\dim(\mathrm{Sym}^2 W)^G$ or $\dim(\mathrm{Alt}^2 W)^G$ is two or $\dim(\mathrm{Sym}^2 W)^G = \dim(\mathrm{Alt}^2 W)^G = 1$. (We can actually realize all the bilinear forms on W as the real/complex parts of a Hermitian form on cW .)
- $\mathrm{End}_G W = \mathbb{Z}$: This case has no analogy in the finite field setting. In this case, $cW = V \oplus \bar{V}$ with $V \cong \bar{V}$. Either $\dim(\mathrm{Sym}^2 W)^G = 3, \dim(\mathrm{Alt}^2 W)^G = 1$ or $\dim(\mathrm{Sym}^2 W)^G = 1, \dim(\mathrm{Alt}^2 W)^G = 3$.

3.1.2 Equivariant Witt's Lemma

Now we work more generally, though we still assume $\ell \nmid 2|G|$. Let V be a homogenous $\mathbb{F}_\ell[G]$ representation with isotypic component W so there is an isomorphism (though not a canonical isomorphism!) $V \cong W^k$. We also assume that V carries a non-degenerate alternating form h . We are interested in understanding the *symplectic centralizer*,

$$C_{\mathrm{Sp}(V_\ell)}(G) = \mathrm{Sp}(V, h) \cap \mathrm{End}_G(V),$$

the isometries of h that commute with the action of G . After choosing an isomorphism $V \cong W^k$, by Schur's lemma, we can identify $\text{End}_G(V)$ with $M_k(D)$.

Note that $D := \text{End}_G(W)$ acts on $\text{Hom}_G(W, V)$ by precomposition, $d \cdot \psi = \psi \circ d$. Since D is a field, this endows $\text{Hom}_G(W, V)$ with a k dimensional vector space structure over D .

Given a G -equivariant isomorphism $b : W \rightarrow W^\vee$, which is equivalent to the choice of a G -equivariant bilinear form define a map $\tilde{h}_b$ as follows

$$\tilde{h}_b : \text{Hom}_G(W, V) \times \text{Hom}_G(W, V) \rightarrow \text{End}_G(W)$$

by

$$\tilde{h}_b(\psi, \tau) = b^{-1} \circ \tau^\vee \circ h \circ \psi.$$

Lemma 3.1.5. $\tilde{h}_b$ defines a sesquilinear form on $\text{Hom}_G(W, V)$, i.e.

$$\tilde{h}_b(d\psi + \tau, e\beta) = di_b(e)\tilde{h}_b(\psi, \beta) + i_b(e)\tilde{h}_b(\tau, \beta)$$

for $d, e \in \text{End}_G(W)$ and $\psi, \tau, \beta \in \text{Hom}_G(W, V)$.

Proof. Let $\psi, \tau, \beta \in \text{Hom}_G(W, V)$ be arbitrary maps and let $d, e \in \text{End}_G(W)$. Then

$$\begin{aligned} \tilde{h}_b(d\psi + \tau, e\beta) &= b^{-1} \circ e^\vee \circ \beta \circ \tilde{h}_b \circ \beta \circ (d\psi + \tau) \\ &= b^{-1} \circ e^\vee \circ b \circ (b^{-1} \circ \tau^\vee \circ \tilde{h}_b \circ \psi \circ d + b^{-1} \circ \beta^\vee \circ \tilde{h}_b \circ \tau) \\ &= di_b(e)\tilde{h}_b(\psi, \beta) + i_b(e)\tilde{h}_b(\tau, \beta) \end{aligned}$$

□

There is a map

$$i : \text{End}_G(V) \rightarrow \text{End}_D(\text{Hom}_G(W, V))$$

given by

$$i(A)\psi = A \circ \psi.$$

This is a D equivariant map since

$$i(A)(d \cdot \psi) = A \circ d \cdot \psi = d \cdot A(\psi).$$

This map is clearly injective and I claim it is also surjective. By definition, the size of the left hand side is $|D|^{k^2}$ since $\text{End}_G(V) \cong M_k(D)$. The size of the right hand side is the size of an endomorphism ring of a dimension k vector space over D which is also $|D|^{k^2}$. So every D -endomorphism of $\text{Hom}_G(W, V)$ arises as an ambient G -endomorphism of V .

Lemma 3.1.6. *Let $\text{Isom}(\tilde{h}_b) \subset \text{End}_D(\text{Hom}_G(W, V))$ denote the isometries of the form $\tilde{h}_b$.*

$$\text{Isom}(\tilde{h}_b) = C_{\text{Sp}(V, h)}(G).$$

Proof. From the discussion above, we can identify $\text{Isom}(\tilde{h}_b) \subset \text{End}_G(V)$. Now, $A \in \text{End}_G(V)$ is contained in $\text{Isom}(\tilde{h}_b)$ iff $\tilde{h}_b(A \circ \psi, A \circ \tau) = \tilde{h}_b(\psi, \tau)$. By non-degeneracy of $\tilde{h}_b$ this is true iff $h^{-1} \circ A^\vee \circ h \circ A = \text{id}$ which is equivalent to A being an isometry for h , in other words $A \in \text{Sp}(V, h)$. $\square$

Being able to identify the symplectic centralizer with a group of isometries is a powerful too to explicitly compute it. We can now prove the main theorem of this section.

Theorem 3.1.7. *1. If $(\text{Alt}^2 W)^G = 0$, k must be even, $\tilde{h}_b$ is an alternating form and*

$$C_{\text{Sp}(V_\ell)}(G) \cong \text{Sp}(k, D).$$

2. If $(\text{Alt}^2 W)^G \neq 0$ and W is type 1, $\tilde{h}_b$ is a symmetric form and $C_{\text{Sp}(V_\ell)}(G) \cong O(k, D)$.

3. If $(\text{Alt}^2 W)^G \neq 0$ and W is type 2, $\tilde{h}_b$ is a Hermitian form and $C_{\text{Sp}(V_\ell)}(G) \cong U(k, D)$.

Proof. Since h is an alternating form, note that $h^\vee = -h$ and more generally if b is an ϵ -form, $b^\vee = \epsilon b^{-1}$. So

$$\begin{aligned} i_b(\tilde{h}_b(\psi, \tau)) &= b^{-1} \circ (b^{-1} \psi^\vee \circ h \circ \tau)^\vee \circ b \\ &= b^{-1} \circ \tau^\vee \circ h^\vee \circ \psi \circ (b^{-1})^\vee \circ b \\ &= \epsilon b^{-1} \circ \tau^\vee \circ h^\vee \circ \psi \\ &= -\epsilon \tilde{h}_b(\tau, \psi) \end{aligned}$$

Case 1: $(\text{Alt}^2 W)^G = 0$. In this case, b is necessarily a symmetric form and W is necessarily type 1 so the previous computation implies that $\tilde{h}_b(\tau, \psi) = i_b(\tilde{h}_b(\psi, \tau)) = -\tilde{h}_b(\psi, \tau)$. Hence $\tilde{h}_b$ is a non-degenerate alternating form.

Case 2: $(\text{Alt}^2 W)^G \neq 0$ and W is type 1. In this case, b is necessarily an alternating form, i.e. $\epsilon = -1$, and W is type 1. The above computation implies that $\tilde{h}_b(\tau, \psi) = i_b(\tilde{h}_b(\psi, \tau)) = \tilde{h}_b(\psi, \tau)$. Hence $\tilde{h}_b$ is a non-degenerate symmetric form.

Case 3: $(\text{Alt}^2 W)^G \neq 0$ and W is type 2. Since W is type 2, i_b is a non-trivial involution. Choose b to be a symmetric form, so $\tilde{h}_b(\psi, \tau) = -i_b(\tilde{h}_b(\tau, \psi))$. $\square$

The action of $C_{\text{Sp}(V_\ell)}(G)$ on V , gives rise to a natural action of $C_{\text{Sp}(V_\ell)}(G)$ on $\text{Inj}_G(W^r, V)$, the set of G -equivariant injective homomorphisms, for any $r \leq k$ by post-composition. Given such an injection f , let f^*h be the pullback bilinear form on W , i.e. $f^*h(x, y) = h(f(x), f(y))$.

Corollary 3.1.8 (Equivariant Witt's Lemma). *Choose $r \leq k$ and let $f, g \in \text{Inj}_G(W^r, V)$ such that $f^*h = g^*h$. Then, there exists $A \in C_{\text{Sp}(V_\ell)}(G)$ such that $A \circ f = g$.*

Proof. Let f_i, g_i be the restriction of f, g respectively to the i -th component of W^r . Since $f^*h = g^*h$, we see that $\tilde{h}_b(f_i, f_j) = \tilde{h}_b(g_i, g_j)$. This implies that the r -dimensional subspaces of $\text{End}_G(W, V)$ given by $\langle f_1, \dots, f_r \rangle$ and $\langle g_1, \dots, g_r \rangle$ are isometric. Hence by the previous theorem and Witt's lemma [6, Section 20], there exists an isometry of $\tilde{h}_b$ such that $A \circ f_i = g_i$. The result follows by using Lemma 2.5 to identify the isometries of $\tilde{h}_b$ with $C_{\text{Sp}(V_\ell)}(G)$. $\square$

Corollary 3.1.9. *The number of orbits of $C_{\text{Sp}(V_\ell)}(G)$ on $\text{Inj}_G(W^r, V)$ is $|(Alt^2 W^r)^G|$ for $r < n/2$.*

3.1.3 Symplectic centralizers of representations

In this section we again generalize. Again, let G be a group and let $\text{Irr}_\ell(G)$ denote the isomorphism classes of irreducible representations of G over $\mathbb{F}_\ell$ where $\ell \nmid 2|G|$. Denote the associated G -module to $\rho \in \text{Irr}_\ell(G)$ by W_ρ . By Schur's lemma $D_\rho := \text{End}_G(W_\rho)$ is a finite field extension of $\mathbb{F}_\ell$ so by is a finite field. Let V be a representation of G and denote the multiplicity of W_ρ in V by k_ρ . Then we can decompose V as

$$V \cong \bigoplus_{\rho \in \text{Irr}_\ell(G)} V_\rho$$

where V_ρ is the isotypic component for W_ρ so $V_\rho \cong W_\rho^{k_\rho}$. In addition, assume that there is a non-degenerate G -equivariant alternating form $h : V \times V \rightarrow \mathbb{F}_\ell$. Our goal in this section is to harness the results from the last section to explicitly compute $C_{\text{Sp}(V_\ell)}(G)$.

Since h is nondegenerate and G -invariant, it induces an G -module isomorphism from V to $V^\vee$. When V_ρ is self dual h restricted to V_ρ is non-degenerate.

If V_ρ is not self-dual i.e. $V_\rho \not\cong V_{\rho^\vee}$, the module $V_\rho \oplus V_{\rho^\vee}$ appears as a factor of V . Also h restricted to $V_\rho \oplus V_{\rho^\vee}$ is non-degenerate and $V_\rho, V_{\rho^\vee}$ are maximal isotypic subspaces of the direct sum. This follows from the fact that for $\psi \in \text{Irr}(G), \psi \neq \rho^\vee$ we necessarily have that $V_\psi \perp V_{\rho^\vee}$. Indeed the map $V_\psi \rightarrow V_{\rho^\vee} : x \rightarrow h(x, \cdot)$ is G -equivariant and so must be zero.

When $V_\rho \cong V_{\rho^\vee}$ we will use the notation $M_\rho := V_\rho \oplus V_{\rho^\vee}$. Let $\mathcal{D} \subset \text{Irr}(G)$ denote the set of self dual isotypic components. Then V decomposes as

$$V = \bigoplus_{\rho \in \mathcal{D}} V_\rho \oplus \bigoplus_{\rho \in \text{Irr}(G) - \mathcal{D}} M_\rho$$

Each operator commuting with G must preserve each V_ρ . Pairwise orthogonality of the isotypic components implies

$$C_{\text{Sp}(V_\ell)}(G) = \prod_{\rho \in \mathcal{D}} C_{\text{Sp}(V_\rho)}(G) \times \prod_{\rho \in \text{Irr}(G) - \mathcal{D}} C_{\text{Sp}(M_\rho)}(G)$$

where $\text{Sp}(V_\rho, h)$ is the subgroup of $\text{End}_G(V_\rho)$ that preserve the restriction of h to V_ρ ; $\text{Sp}(M_\rho, h)$ is defined analogously.

Theorem 3.1.10.

$$C_{\text{Sp}(V_\rho)}(G) \cong \begin{cases} \text{Sp}(k_\rho, D_\rho) & (\text{Alt}^2 W_\rho)^G = 0 \\ \text{O}(k_\rho, D_\rho) & (\text{Sym}^2 W_\rho)^G = 0 \\ \text{U}(k_\rho, D_\rho) & \text{otherwise} \end{cases}$$

and

$$C_{\text{Sp}(M_\rho)}(G) \cong \text{GL}(k_\rho, D_\rho)$$

Proof. We first compute the groups $C_{\text{Sp}(M_\rho)}(G)$. Since each element of $C_{\text{Sp}(M_\rho)}(G)$ must necessarily preserve V_ρ and $V_{\rho^\vee}$ it must be a block diagonal matrix $\text{diag}(A, B)$ where

A, B are invertible and $A \in \text{End}_G(V_\rho), B \in \text{End}_G(V_{\rho^*})$. The requirement that this endomorphism also preserve h is equivalent to $[B] = ([A]^T)^{-1}$ with respect to a basis of V_ρ and a dual basis of V_{ρ^*} . Recall that $D_\rho = \text{End}_G(W_\rho)$ is a field, so after choosing a basis we can identify $\text{End}_G(V_\rho) \cong \text{Mat}_{k_\rho}(D)$. Under this identification $C_{\text{Sp}(M_\rho)}(G) \cong \text{GL}(k_\rho, D)$.

The result now follows from Theorem 2.4. $\square$

3.2 Transitivity Results

In this section we review some of the standard properties of classical groups of Lie type. Throughout the following, let $\mathbb{F} := \mathbb{F}_{\ell^k}$ and let $\Gamma(n, \mathbb{F})$ denote one of

$$\{\text{GL}(n, \mathbb{F}), \text{Sp}(n, \mathbb{F}), \text{U}(n, \mathbb{F}), \text{O}(n, \mathbb{F}) | n \geq 5, l \geq 3\}.$$

In this range of n, ℓ all the groups above are pairwise non-isomorphic. In the orthogonal case, we do not distinguish between the groups $O^+(n, \mathbb{F})$ and $O^-(n, \mathbb{F})$, and all the results we state will be true for both cases.

Here are some key properties we exploit, again with our assumption on n, ℓ . Proofs of all the results stated can be found in [22].

Commutators. In all cases the commutator of Γ , denoted Γ' is perfect, i.e., $[\Gamma', \Gamma'] = \Gamma'$.

Note that Γ/Γ' will be a cyclic subgroup as it is a subgroup of $\mathbb{F}^*$

Generation by Elements of order ℓ . In all cases, Γ' is generated by elements of order ℓ . In particular in each case Γ' is generated by transvections. Recall that $\tau \in \Gamma$ is a *transvection* if there is a hyperplane $W \subset \mathbb{F}^n$ such that $\tau|_W = \text{id}_W$ and $\tau v - v \in W$ for all $v \in V$. We explicitly describe these generating sets now.

When $\Gamma = \text{Sp}$ or $\Gamma = \text{U}$, h be the form preserved by Γ , then for any $v \in V$ and $a \in \mathbb{F}_\ell$, $\tau_{a,v}(x) := x + ah(x, v)v$ fixes $v^\perp$ and is contained in Γ .

When $\Gamma = \text{GL}$, $\Gamma' = \text{SL}$ is generated by *elementary matrices*, i.e. matrices with 1's on the diagonal and a single non-zero entry off the diagonal. Each elementary matrix is a transvection fixing the hyperplane spanned by the columns having only a 1 on the diagonal.

Finally, when $\Gamma = \text{O}$, Γ' is generated by transvections known as *Siegel transformations*. The definition of this class of transformations is a bit involved so we refer the reader to the discussion in [22].

Central quotients and Simplicity Define the projective group $\mathbb{P}\Gamma := \Gamma/Z(\Gamma)$. In general, $Z(\Gamma') = \Gamma' \cap Z(\Gamma)$ and $\mathbb{P}\Gamma' := \Gamma'/(Z(\Gamma'))$ are simple. From the above, $\mathbb{P}\Gamma' = [\mathbb{P}\Gamma, \mathbb{P}\Gamma]$ and $\mathbb{P}\Gamma/\mathbb{P}\Gamma'$ is cyclic.

We also have the following lemma,

Lemma 3.2.1. *Let Γ be one of the classical groups, and Γ' the derived subgroup. Then $C_{\mathbb{P}\Gamma}(\mathbb{P}\Gamma')$ is trivial.*

Proof. Let $\bar{t} \in C_{\mathbb{P}\Gamma}(\mathbb{P}\Gamma')$ and $t \in \Gamma$ be any lift of $\bar{t}$. Let $\gamma_1, \gamma_2 \in \Gamma'$ be arbitrary. By assumption, $\gamma_1 t \gamma_1^{-1} t^{-1} \in Z(\Gamma')$. In particular,

$$\begin{aligned} [\gamma_1 \gamma_2, t] &= \gamma_2^{-1} [\gamma_1, t] \gamma_2 [\gamma_2, t] \\ &= [\gamma_1, t] [\gamma_2, t] \in Z(\Gamma'). \end{aligned}$$

So the map $\gamma \rightarrow [\gamma, t]$ is a homomorphism $\Gamma' \rightarrow Z(\Gamma')$. Since $\Gamma' = [\Gamma', \Gamma']$ we see the image of this map must be trivial, so in particular, $[t, \gamma]$ is trivial for all $t \in \Gamma'$. However such an element of Γ is necessarily contained in $Z(\Gamma)$ so the result follows. $\square$

In addition to the basic properties of the classical groups mentioned above, we will need some results on these groups as permutations groups. As a starting example of

the type of transitivity results we employ, consider the following result dependent on the classification of finite simple groups. Any 6 transitive permutation group must be S_n or A_n . More generally, the two transitive and four transitive groups have also been classified [9]. Analogous to the permutation group case, one can ask for a classification of subgroups of affine groups that act singly or doubly transitively on lines, or higher dimensional subspaces. The Cameron and Kantor theorem [10] classifies all two-transitive subgroups of the semi-linear groups. Hering [25] went on to classify all subgroups acting transitively on lines. An older result, due to Perin, classifies subgroups acting transitively on subspaces with dimension at least three.

Theorem 3.2.2 (Perin [33, Theorem 1]).

Let $n \geq 3$ and ℓ odd. Suppose that $H \subset GL(n, \mathbb{F})$ acts transitively on the three dimensional subspaces of $GL(n, \mathbb{F}_{\ell^m})$. Then $SL(n, \mathbb{F}_{\ell^m}) \subset H$.

The *rank* of a transitive permutation group is the number of orbits of the stabilizer of a point. Each of the classical linear groups preserving a form, aka the symplectic, orthogonal and unitary groups, are all rank 3 on the set of isotropic lines. Indeed the orbits of the stabilizer of an isotropic line are given by the line, isotropic lines perpendicular to the line, and isotropic lines not perpendicular to the line. In [33], Perin characterizes such rank 3 subgroups of symplectic and unitary groups which was later followed by a classification of such rank 3 subgroups of orthogonal groups in odd characteristic by Kantor and Liebler [27]. The following theorem is a restatement of their result that will be used heavily in the proof of the main monodromy result.

Theorem 3.2.3 ([33, Theorem 4], [27, Theorem 1.3]).

Let $n \geq 5$ and ℓ odd. Let Γ be one of $U(n, \mathbb{F}_{\ell^k})$, $O(n, \mathbb{F}_{\ell^k})$, or $Sp(n, \mathbb{F}_{\ell^k})$. If $H \subset \Gamma$ acts as a rank 3 permutation group on isotropic lines, then $\Gamma' \subset H$.

Remark 2. In their paper [29], Liebeck, Praeger and Saxl, provide (among many other results) a generalization of the Cameron-Kantor theorem and a classification of subgroups of symplectic groups acting transitively on lines and hyperbolic planes in even and odd characteristic. Abhyankar has used the Cameron-Kantor to solve carious cases of the inverse Galois problem for classical groups. We refer the reader to their paper [29] along with a survey paper of Abhyankar [1] for more information on these types of transitivity results.

Theorem 3.2.4. *Let V be a vector space of dimension n over $\mathbb{F} := \mathbb{F}_{\ell^k}$, for $\ell \neq 2$ and with $n \geq 5$. Let Γ denote one of*

$$Sp(n, \mathbb{F}), U(n, \mathbb{F}), O(n, \mathbb{F}), GL(n, \mathbb{F}).$$

For any $H \subset \Gamma$ such that H has the same set of orbits on $\text{Inj}(\mathbb{F}^r, V)$ as Γ for all $r \in \{1, 2, 3\}$, we have that $\Gamma' \subset H$.

Proof. If $\Gamma = GL(V)$ then by Theorem 3.2.2 and the assumption with $r = 3$ we see that $SL(V) \subset H$. If we can show that H having the same number of orbits as Γ on $\text{Inj}(\mathbb{F}^k, V)$ for $r = 1$ and $r = 2$ implies that H is rank 3 on the set of isotropic lines of V then the result then follows from Theorem 3.2.3 in all other cases.

So, assume let $u, v \in \mathbb{F}^n$ be isotropic vectors spanning independent lines and let Γ be the underlying isometry group of some form h . The orbit of v under the stabilizer of u in Γ , denoted Γ_u , are all isotropic vectors w such that $h(u, v) = h(u, w)$ and u, w are independent. In particular the injections from $\mathbb{F}^2 \rightarrow \mathbb{F}^n$ that map the basis elements to

u, v and u, w respectively are in the same orbit of Γ_u . Since H has the same orbits on injections as Γ , this implies that v is in the same orbit as w . $\square$

3.3 Subgroups of Products of Groups

We will need the following theorems about subgroups of products of groups.

Lemma 3.3.1 (Goursat's Lemma). *Let G_1, G_2 be groups, and let H be a subgroup of $G_1 \times G_2$. Let H_2 and K_1 respectively be the image and kernel of the projection onto the second factor $p_2 : H \rightarrow G_2$, and likewise let H_1, K_2 the image and kernel of the projection onto the first factor $p_1 : H \rightarrow G_1$. Then K_1 is a normal subgroup of H_1 , and K_2 is a normal subgroup of H_2 . There is an isomorphism $\phi : H_1/K_1 \rightarrow H_2/K_2$ and H is the pullback of the graph ϕ under the projection $H_1 \times H_2 \rightarrow H_1/K_1 \times H_2/K_2$.*

The following result about below is a variant of the well-known *Hall's Lemma*. Many versions of this lemma have previously appeared in diverse settings related to monodromy computations before including [14, Dunfield-Thurston], [34, Ribet], and [5, Allcock-Hall].

Theorem 3.3.2. *Suppose that $\Gamma_1, \dots, \Gamma_n$ is a set of finite non-abelian groups such that each $\Gamma'_i := [\Gamma_i, \Gamma_i]$ is simple non-abelian.*

Let $H \subset \Gamma_1 \times \dots \times \Gamma_n$ such that the projection of H onto $\Gamma_i \times \Gamma_j$ contains $\Gamma'_i \times \Gamma'_j$ for all $1 \leq i, j \leq n$. Then $\Gamma'_1 \times \dots \times \Gamma'_n \subset H$.

Proof. Let p_i, p_{ij} denote the projection maps onto Γ_i and $\Gamma_i \times \Gamma_j$ respectively. Set $N := [H, H]$ and note that

$$N \subset \Gamma'_1 \times \dots \times \Gamma'_n.$$

It suffices to show that $N = \Gamma'_1 \times \dots \times \Gamma'_n$.

First note that since Γ'_i is simple non-abelian, Γ'_i is perfect, i.e. $[\Gamma'_i, \Gamma'_i] = \Gamma'_i$. Now

$$\Gamma'_i \times \Gamma'_j = [\Gamma'_i \times \Gamma'_j, \Gamma'_i \times \Gamma'_j] \subset [p_{ij}(H), p_{ij}(H)] \subset \Gamma'_i \times \Gamma'_j$$

so $p_{ij}(N) = [p_{ij}(H), p_{ij}(H)] = \Gamma'_i \times \Gamma'_j$.

We now induct on n . The result is clear for $n = 2$. Denote the kernel of $p_n : N \rightarrow \Gamma_n$ by N_1 . By Goursat's lemma, N_1 is a normal subgroup of the projection of N onto $\Gamma'_1 \times \cdots \times \Gamma'_{n-1}$. By the inductive hypothesis this projection is surjective. Now, because $p_{in}(N) = \Gamma'_i \times \Gamma'_n$, we also have that $\Gamma'_i = p_i(N_1)$ for $1 \leq i \leq n-1$. Every normal subgroup of a product of simple groups that surjects onto each factor is necessary the whole product. Since each Γ'_i is simple we can conclude $N_1 = \Gamma'_1 \times \cdots \times \Gamma'_{n-1}$. Hence by Goursat's lemma, N_2 , the kernel of the projection onto $\Gamma'_1 \times \cdots \times \Gamma'_{n-1}$ must be Γ'_n . Hence we can conclude that $N = \Gamma'_1 \times \cdots \times \Gamma'_n$. $\square$

In the case where the product consists of two different groups we can prove a sharper result. We say that a subgroup H of a product of groups $G_1 \times G_2$ is *diagonally embedded* if H is the graph of an isomorphism $H_1 \rightarrow H_2$ with H_1, H_2 the projections of H to G_1, G_2 respectively.

Theorem 3.3.3. *Suppose that Γ_1 and Γ_2 are groups satisfying the conditions of the previous theorem. In addition assume $C_{\Gamma_i}(\Gamma'_i)$ is trivial.*

Let $H \subset \Gamma_1 \times \Gamma_2$ such that the projection of H onto Γ_1 contains Γ'_1 and that the projection of H onto Γ_2 contains Γ'_2 . Then

- *If $\Gamma'_1 \not\cong \Gamma'_2$ then $\Gamma'_1 \times \Gamma'_2 \subset H$.*
- *If $\Gamma'_1 \cong \Gamma'_2$ then either $\Gamma'_1 \times \Gamma'_2 \subset H$ or H is a diagonally embedded subgroup of $\Gamma_1 \times \Gamma_2$.*

Proof. Let H_1 be the projection of H onto Γ_1 , H_2 the projection of H onto Γ_2 , and N_2 , N_1 the respective kernels. Then by Goursat's lemma $H_1/N_1 \cong H_2/N_2$. For $i = 1, 2$, Γ'_i is simple by assumption and so $N_i \cap \Gamma'_i$ is either Γ'_i or trivial.

If $\Gamma'_2 \cap N_2 = \Gamma'_2$ then H_2/N_2 is abelian. So H_1/N_1 must also be abelian and since $\Gamma'_1 \subset H_1$, $\Gamma'_1 \subset N_1$. So $\Gamma'_1 \times \Gamma'_2 \subset H$.

Now assume $N_2 \cap \Gamma'_2$ is trivial. This implies that N_2 commutes with Γ'_2 which by assumption implies N_2 is trivial. Hence $H_1/N_1 \cong H_2$. However, since H_2 is non-abelian, $\Gamma'_1 \not\subset N_1$ and so $N_1 \cap \Gamma'_1$ is trivial. By similar reasoning as for N_2 , N_1 is trivial and so we can conclude $H_1 \cong H_2$ and that H is a diagonally embedded subgroup.

If we additionally assume that $\Gamma'_1 \not\cong \Gamma'_2$, then H_1 and H_2 will have non-isomorphic composition factors since Γ'_1, Γ'_2 are simple. This is a contradiction. The result follows. $\square$

Finally we will need the following lemma.

Lemma 3.3.4. *Let Γ_i for $1 \leq i \leq n$ be a collection of groups such that*

- $Z(\Gamma'_i) = Z(\Gamma_i) \cap \Gamma'_i$
- *There is a subset $U_i \subset \Gamma'_i$ that generates Γ'_i such that the order of every element of U_i is a prime ℓ with $(\ell, Z(\Gamma_i)) = 1$ for all i .*

Let $\Gamma = \prod_{i=1}^n \Gamma_i$, and let $\rho_i : \Gamma \rightarrow \Gamma_i$ be the projection map onto Γ_i .

Assume that $H \subset \Gamma$ such that $\Gamma'_i \subset \rho_i(H)$. In addition if $\phi : \Gamma \rightarrow \mathbb{P}\Gamma$ is the natural quotient map, then assume that $\prod_{i=1}^n \mathbb{P}\Gamma'_i \subset \phi(H)$. Then $\prod_{i=1}^n \Gamma'_i \subset H$

Proof. Since $\prod_{i=1}^n \mathbb{P}\Gamma'_i \subset \phi(H)$ we see that $\prod_{i=1}^n \Gamma'_i \subset HZ(\Gamma)$. Choose an element $(t_1, \dots, t_n) \in \prod_{i=1}^n U_i$. We can find $(h_1, \dots, h_n) \in H$ and $(z_1, \dots, z_n) \in \prod_{i=1}^n Z(\Gamma_i)$

such that

$$(t_1, \dots, t_n) = (h_1 z_1, \dots, h_n z_n).$$

Now choose k so that $k \cong 1 \pmod{\ell}$ and $|Z(\Gamma_i)| \mid k$ for each i . Raising each side to the k -th power we see that $t_i = h_i^k$ which implies that $(t_1, \dots, t_n) \in H$. This gives the result. $\square$

Unfolding the previous lemma, one of its implications is that if $H \subset \mathrm{GL}(n, \mathbb{F})$ and image of H in $\mathrm{PGL}(n, \mathbb{F})$ contains $\mathrm{PSL}(n, \mathbb{F})$ then $\mathrm{SL}(n, \mathbb{F}) \subset H$.

Chapter 4

Explicit Dihedral Monodromy

Before providing a proof of the main theorem, Theorem 5.4.2, we first discuss a monodromy computation of an explicit family of dihedral covers of $\mathbb{P}^1(\mathbb{C})$. The computation done in this chapter will give us a chance to exercise the algebraic tools appearing in Chapter 3. The techniques in this chapter are motivated by the paper of Looijenga [30].

4.1 Introduction and Topological Construction

Take $G = D_5$, the dihedral group of size 10 with the presentation

$$D_5 = \langle \tau, \sigma \mid \tau^5 = \sigma^2 \sigma \tau = \tau^{-1} \sigma \rangle.$$

Let $\mathcal{C} = (C_\sigma)$ where C_σ , the conjugacy class of σ , is the unique conjugacy class of involutions. Let $\mathbf{m} = (6)$, so we will insist that our cover has 6 branch points. We denote the branch points by $D = \{b_1, b_2, \dots, b_6\}$ and choose a cover of $f : C \rightarrow \mathbb{P}^1(\mathbb{C})$ corresponding to a surjection.

$$\pi_1(\mathbb{P}^1(\mathbb{C}) - D, \infty) \rightarrow G.$$

In the following, we provide a topological construction of C , describe the representation theory of G acting on $H_1(C, \mathbb{F}_\ell)$ and explicitly compute the Hurwitz monodromy of C .

By basic properties of covering maps C is an unramified cover of its quotient by τ , denoted by C' . In turn, C' is a double cover of $\mathbb{P}^1(\mathbb{C})$ with the same branch locus as C . The restriction of σ gives the hyperelliptic involution on C' . Furthermore C' is topologically constructed from C by cutting along an embedded curve, and pasting 5 different copies of C' together along this embedded curve. This construction is explicitly depicted in Figure 4.1.

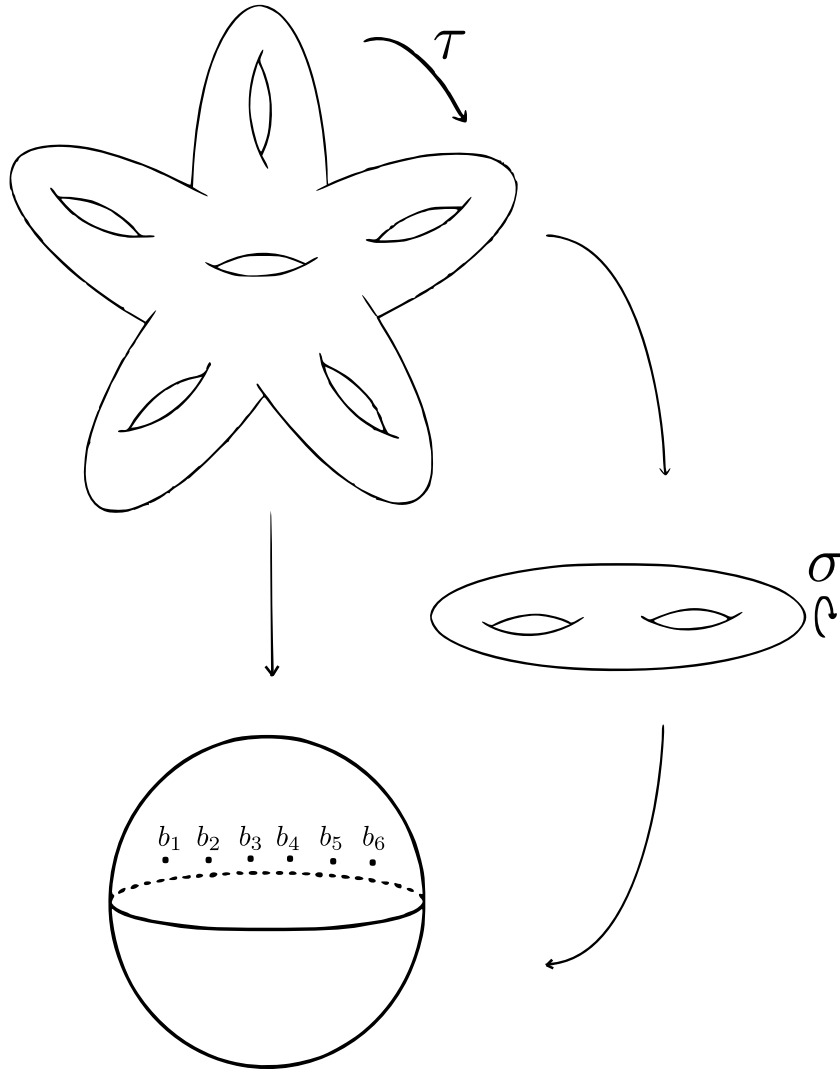


Figure 2: Explicit construction of a D_5 cover.

As can be seen by the above picture or a quick computation using the Riemann-Hurwitz formula, C is a genus 6 curve and C' is a genus 2 hyperelliptic curve. The action of D_5 is also explicitly shown, namely τ rotates the figure counter-clockwise by an angle of $2\pi/5$ and σ performs a rotation around a fixed arm.

4.2 Homology of the Cover

Denote the G representation derived from the Galois action on the homology of C by

$$\rho_C : G \rightarrow GL(H_1(C, \mathbb{Z})).$$

Over $\mathbb{Z}$, D_5 has two one dimensional representations, namely the trivial representation ρ_{triv} and a sign representation ρ_{sign} coming from the restriction of the sign representation when D_5 is viewed as a permutation group on the vertices of a pentagon. It also has a unique four dimensional representation on the trace 0 hyperplane of $\mathbb{Z}^5$. This representation, denoted ρ_4 , is irreducible over $\mathbb{Q}$. However, $\rho_4 \otimes \mathbb{Q}(\sqrt{5})$ splits into the sum of two two-dimensional irreducible representations, ρ_2 and ρ_3 . Over a finite field $\mathbb{F}_\ell$, the behavior of $\rho_4 \otimes \mathbb{F}_\ell$ depends on the splitting of ℓ in $\mathbb{Q}(\sqrt{5})$. By quadratic reciprocity,

$$\rho_4 \otimes \mathbb{F}_\ell = \begin{cases} \rho_4 \otimes \mathbb{F}_\ell & \text{if } \ell = 2, 3 \bmod 5 \text{ the representation remains irreducible} \\ \rho_2 \otimes \mathbb{F}_\ell \oplus \rho_3 \otimes \mathbb{F}_\ell & \text{if } \ell = 1, 4 \bmod 5 \text{ the representation splits} \end{cases}$$

By Theorem 5.2.1 we can explicitly decompose ρ_C in terms of the representations in the previous paragraph, specifically,

$$\rho_C \cong 4\rho_{\text{sign}} \oplus \rho_4 \oplus \rho_4. \tag{4.1}$$

Without invoking Theorem 5.2.1 we can explicitly compute this representation in terms of an explicit homology basis on C . In Figure 4.2, a basis for $H_1(C, \mathbb{Z})$ is given by the simple curves

$$\alpha_1, \dots, \alpha_5, \beta_1, \dots, \beta_5, \delta_1, \delta_2.$$

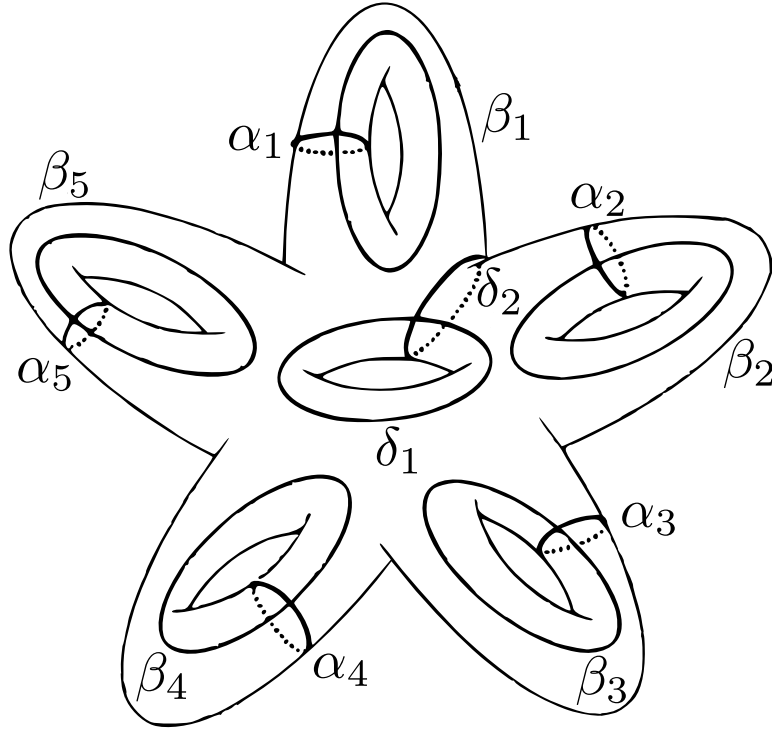


Figure 3: Homology basis for C .

The action of G on this basis is explicitly given by,

$$\tau(\alpha_i) = \alpha_{i+1 \bmod 5}, \tau(\beta_i) = \beta_{i+1 \bmod 5}$$

$$\tau(\delta_1) = \delta_1, \tau(\delta_2) = \delta_2$$

$$\sigma(\alpha_i) = -\alpha_i, \sigma(\beta_i) = -\beta_i$$

$$\sigma(\delta_1) = -\delta_1, \sigma(\delta_2) = -\delta_2$$

Now G acts on the subspaces generated by $\langle \alpha_1, \dots, \alpha_5 \rangle$ and $\langle \beta_1, \dots, \beta_5 \rangle$ by its standard permutation representation. Thus the sign representation in 4.2 expression is generated by

$$S := \langle \alpha_1 + \dots + \alpha_5, \beta_1 + \dots + \beta_5, \delta_1, \delta_2 \rangle.$$

Note that we can also identify S as the τ -invariants of homology, $S = H_1(C, \mathbb{Z})^\tau$.

A basis for the subrepresentation isomorphic to $\rho_4 \oplus \rho_4$ is given by,

$$W := W_1 \oplus W_2$$

where

$$W_1 := \langle \alpha_1 - \alpha_2, \alpha_2 - \alpha_3, \alpha_3 - \alpha_4, \alpha_4 - \alpha_5 \rangle$$

and

$$W_2 := \langle \beta_1 - \beta_2, \beta_2 - \beta_3, \beta_3 - \beta_4, \beta_4 - \beta_5 \rangle.$$

Note that $W_1 \cong W_2$ under the map that sends $\alpha_i - \alpha_{i+1} \rightarrow \beta_i - \beta_{i+1}$.

Hence we see that

$$H_1(C, \mathbb{Z}/\ell\mathbb{Z}) \cong S \oplus W_1 \oplus W_2. \quad (4.2)$$

4.3 The Hurwitz Monodromy group

As discussed in the previous chapter, there is a monodromy action

$$\rho : \pi_1(\text{Chur}_{D_{5,(6)}}^{\mathcal{C}}, [C]) \rightarrow \text{Sp}(H_1(C, \mathbb{Z})).$$

Where $\pi_1(\text{Chur}_{D_{5,(6)}}^{\mathcal{C}}, [C])$ can be identified with mapping classes of $\mathbb{P}^1(\mathbb{C}) - D$ that fix ∞ . We will denote the reduction of $\rho \bmod \ell$ by

$$\rho_\ell : \pi_1(\text{Chur}_{D_{5,(6)}}^{\mathcal{C}}, [C]) \rightarrow \text{Sp}(H_1(C, \mathbb{Z}/\ell\mathbb{Z})).$$

To make the exposition easier we will ignore basepoints.

To compute the monodromy group in this case, we will demonstrate an explicit set of generators. The image of ρ_ℓ , denoted M_{ρ_ℓ} must be contained in $C_{Sp(H_1(C, \mathbb{Z}))}(G)$. We have a decomposition,

$$C_{Sp(H_1(C, \mathbb{Z}))}(G) = C_{Sp(S)}(G) \oplus C_{Sp(W)}(G)$$

where $Sp(S)$ is the restriction of the the G -equivariant symplectic isometries to S , and analogously for $Sp(W)$.

It is straight-forward to see that $\text{Alt}^2 \rho_4 = \text{Alt}^2 \rho_2 = \text{Alt}^2 \rho_3 = 0$ and $\text{Sym}^2 \rho_4 = 2$. Hence by Theorem 3.1.10, $C_{Sp(S)}(D_5) = Sp(4, \mathbb{F}_\ell)$ and

$$C_{Sp(W)}(D_5) = \begin{cases} Sp(2, \mathbb{F}_{\ell^2}) & \text{if } \ell = 2, 3 \bmod 5 \\ Sp(2, \mathbb{F}_\ell) \times Sp(2, \mathbb{F}_\ell) & \text{if } \ell = 1, 4 \bmod 5 \end{cases}$$

Of course, $Sp(2, \mathbb{F}_{\ell^2}) \cong SL(2, \mathbb{F}_{\ell^2})$ and $Sp(2, \mathbb{F}_\ell) \cong SL(2, \mathbb{F}_\ell)$.

We point out a set of curves on C which are especially important. Let γ_i be a curve that wraps around the $i - 1$ and $i + 1$ handles and goes through the center genus. The curve γ_1 is illustrated in Figure 4.3.

Now we single out three specific mapping classes of C ,

- T_α which is a Dehn twist in the union of curves $\alpha_1, \dots, \alpha_5$.
- T_β which is a Dehn twist in the union of curves $\beta_1, \dots, \beta_5$.
- T_γ which is a Dehn twist in the union of curves $\gamma_1, \dots, \gamma_5$.

Because of their symmetric nature, each one of these mapping classes can be seen to commute with the action of G and in fact descends to a mapping class action of $\mathbb{P}^1(\mathbb{C})$

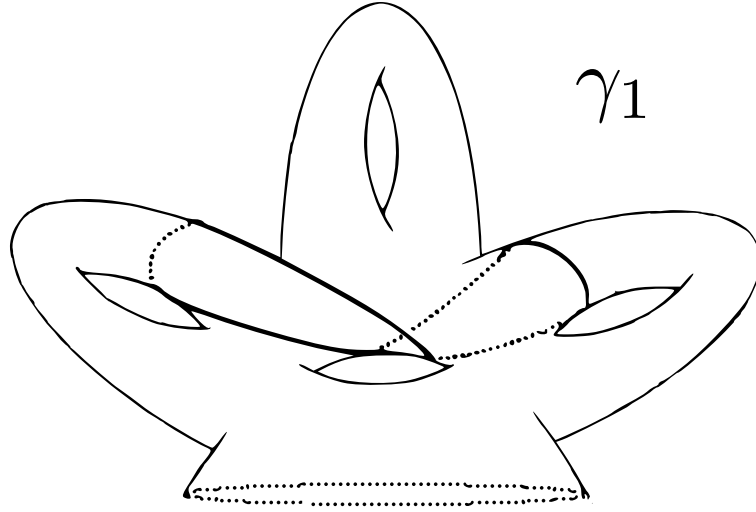


Figure 4: The curve γ_1 on C .

preserving ∞ . Hence all three of these mapping classes lie in the image of ρ_ℓ . In the case of T_α and T_β , these mapping classes correspond to lifts of braids permuting branch points in $\mathbb{P}^1(\mathbb{C})$.

The action of these mapping classes on the explicit basis of W is given for T_α and T_β as

$$\begin{aligned} T_\alpha(\alpha_i - \alpha_{i+1}) &= \alpha_i - \alpha_{i+1}, \\ T_\alpha(\beta_i - \beta_{i+1}) &= \beta_i - \beta_{i+1} + \alpha_i - \alpha_{i+1}, \\ T_\beta(\alpha_i - \alpha_{i+1}) &= \alpha_i - \alpha_{i+1} + \beta_i - \beta_{i+1}, \\ T_\beta(\beta_i - \beta_{i+1}) &= \beta_i - \beta_{i+1}. \end{aligned}$$

Since the curves γ_i are disjoint from the α_i , it is easy to see that the restriction of T_γ to W_1 is trivial. What is a bit more surprising is that $T_\gamma|_{W_2} = 2 - \tau - \tau^{-1}$.

Combining all the previous computations together, we finish this chapter with a

theorem showing that in this specific case we have big monodromy.

Theorem 4.3.1. *If $\ell \cong 2, 3 \pmod{5}$, then $M_{\rho_\ell} = C_{Sp(H_1(C, \mathbb{Z}))}(D_5) = Sp(4, \mathbb{F}_\ell) \oplus Sp(2, \mathbb{F}_{\ell^2})$.*

Remark. From Sage[13] computations, it seems that we still have big monodromy when $\ell \cong 1, 4 \pmod{5}$.

Proof. Throughout this proof, we identify the elements of G with their image in $Sp(H_1(C, \mathbb{F}_\ell))$.

Since $C' = C/\langle \tau \rangle$ we can identify $S = H_1(C, \mathbb{Z})^\tau$, with $H_1(C', \mathbb{Z})$. Hence, the natural projection of M_{ρ_ℓ} to $C_{Sp(S)}(G)$ can be identified with the image of the monodromy action,

$$\text{Chur}_{\mathbb{Z}/2\mathbb{Z}, 6} \rightarrow Sp(H_1(C', \mathbb{Z}/\ell\mathbb{Z}))$$

which is surjective by the results on the monodromy of hyperelliptic curves mentioned in the introduction. Hence M_{ρ_ℓ} surjects onto $C_{Sp(S)}(G)$ under the natural projection map.

Now we compute the projection of M_{ρ_ℓ} in $C_{Sp(S)}(W)$. Denote the image of this projection by $(M_{\rho_\ell})_W$. Because $\ell \cong 2, 3 \pmod{5}$, we know that $\dim \text{Sym}^2 W = \dim W \otimes_G W^* = [\text{End}_G(W) : \mathbb{F}_\ell] = 2$. Clearly,

$$\sigma(\tau + \tau^{-1}) = (\tau + \tau^{-1})\sigma$$

so $\tau + \tau^{-1} \in \text{End}_G(W)$. In particular $[\mathbb{F}_\ell[\tau + \tau^{-1}] : \mathbb{F}_\ell] = 2$ so we see that $\text{End}_G(W) = \mathbb{F}_\ell[\tau + \tau^{-1}]$.

This gives an explicit way to realize the action of T_α, T_β , and T_γ on W as matrices in $C_{Sp(W)}(G) = \text{SL}(2, \mathbb{F}_\ell[\tau + \tau^{-1}])$. We can see that they correspond to the matrices

$$\mathcal{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \mathcal{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \mathcal{G} = \begin{pmatrix} 1 & 2 - \tau - \tau^{-1} \\ 0 & 1 \end{pmatrix}.$$

I claim that these three matrices generate $\mathrm{SL}(2, \mathbb{F}_{\ell^2})$. Firstly note that,

$$\mathcal{S} = \mathcal{B}^{-1} \mathcal{A} \mathcal{A}^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and

$$\mathcal{A} \mathcal{S}^{-1} = \begin{pmatrix} & 1 & & 0 \\ & & & \\ 2 - \tau - \tau^{-1} & & & \\ & & & 1 \end{pmatrix}.$$

In particular we can conclude that $(M_{\rho_\ell})_W$ contains all elementary matrices,

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}[\tau + \tau^{-1}].$$

It is well known that the special linear group is generated by elementary matrices these elementary matrices so in particular, $(M_{\rho_\ell})_W = C_{\mathrm{Sp}(W)}(G)$

Let $\phi : C_{\mathrm{Sp}(W)}(G) \rightarrow C_{\mathrm{Sp}(W)}(G)/Z(C_{\mathrm{Sp}(W)}(G))$ be the natural quotient map. By the above $\phi(M_{\rho_\ell})$ surjects onto each component of

$$\mathbb{P}\mathrm{Sp}(4, \mathbb{F}_\ell) \times \mathbb{P}\mathrm{SL}(2, \mathbb{F}_\ell^2).$$

and so by Theorem 3.3.3, $\mathbb{P}\mathrm{Sp}(4, \mathbb{F}_\ell) \times \mathbb{P}\mathrm{SL}(2, \mathbb{F}_\ell^2) \subset \phi(\mathrm{im} \rho)$ since both factors are simple groups. Hence, by Lemma 3.3.4, we can conclude that $\mathrm{Sp}(4, \mathbb{F}_\ell) \times \mathrm{SL}(2, \mathbb{F}_\ell^2) \subset M_{\rho_\ell}$. $\square$

Chapter 5

Transitivity and Big Monodromy

5.1 Problem Statement

Fix a center-free group G , a tuple of conjugacy classes $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_k)$ and a multidiscriminant $\mathbf{m} = (m_1, \dots, m_k)$. As described in Section 2.2.3, there is a topological space $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ whose points parametrizes surfaces C of type $(G, \mathcal{C}, \mathbf{m})$. We fix such a C and identify the point associated to C in $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ with $[C]$. Assume that that $f : C \rightarrow \mathbb{P}^1(\mathbb{C})$ is the associated covering map and $\mathbf{E}$ is the ramification locus of f .

As described in section 2.3, if $\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}$ is connected, or alternatively if $H_2(G, \mathbb{Z})$ is trivial there is an associated monodromy action. We assume that $H_2(G, \mathbb{Z}) = 0$.

Definition 5.1.1. *For ℓ a prime, there is an associated mod ℓ monodromy map*

$$\rho_{G,m}^{\mathcal{C}} : \pi_1(\text{CHur}_{G,\mathbf{m}}^{\mathcal{C}}, [C]) \rightarrow GL(H_1(C, \mathbb{Z}/\ell\mathbb{Z})).$$

Denote the image of this representation by $M_{\ell}(G)$

The $\mathbb{F}_{\ell}$ vector space $V_{\ell} := H_1(C, \mathbb{Z}/\ell\mathbb{Z})$ carries a symplectic intersection form, and a natural action of G . Since the action of the monodromy group arises through oriented homeomorphisms of C , the elements of $M_{\ell}(G)$ must preserve the symplectic intersection form guaranteeing that $M_{\ell}(G) \subset \text{Sp}(H^1(C, \mathbb{Z}/\ell\mathbb{Z}))$. In addition, since the monodromy representation arises from lifts of homeomorphisms of $\mathbb{P}^1(\mathbb{C})$ preserving f , $M_{\ell}(G)$ must

commute with the action of G on $H_1(C, \mathbb{Z}/\ell\mathbb{Z})$ and so

$$M_\ell(G) \subset C_{\mathrm{Sp}(V_\ell)}(G),$$

where $C_{\mathrm{Sp}(V_\ell)}(G)$, the *symplectic centralizer* of G is the subgroup of $\mathrm{Sp}(V_\ell)$ commuting with the action of G .

The goal of the rest of this chapter is to prove the following *big* monodromy result.

Theorem (Theorem 5.4.2). *For $\ell \nmid 2|G|$ and $\min_i m_i$ sufficiently large,*

$$[C_{\mathrm{Sp}(V_\ell)}(G), C_{\mathrm{Sp}(V_\ell)}(G)] \subset M_\ell(G)$$

Here is a rough sketch of the proof. First we describe how V_ℓ decomposes in terms of irreducible representations for G . Using results from Section 3.1, we will be able to explicitly compute $C_{\mathrm{Sp}(V_\ell)}(G)$. This decomposition along with the Equivariant Witt's Lemma allows us to explicitly compute the number of orbits of $C_{\mathrm{Sp}(V_\ell)}(G)$ on the set of G -equivariant injections from a fixed G -module W to V_ℓ . This set of injections will naturally arise as a fiber of a cover of $\mathrm{CHur}_{G, \mathbf{m}}^c$ and the number of orbits of $M_\ell(G)$ on it will correspond to the connected components of a Hurwitz space. We can then apply Theorem 2.4.1 to count the precise number of orbits. Finally we will conclude the proof by using the transitivity results and characterization of subgroups of products of groups given in Section 3.2.

Throughout the rest of the chapter assume that $\ell \nmid 2|G|$.

5.2 Galois Action on Homology

We begin the proof of this theorem by understanding the representation theory of V_ℓ as a G -module. Let $\mathrm{Irr}_\ell(G)$ denote the set of irreducible representations of G over $\mathbb{F}_\ell$. For

$\rho \in \text{Irr}_\ell(G)$ we let the associated G -module be W_ρ .

Since $\ell \nmid |G|$ we can decompose V_ℓ into isotypic G -representations,

$$V_\ell = \bigoplus_{\rho \in \text{Irr}_\ell(G)} V_\rho$$

where each V_ρ is the isotypic component for ρ , $V_\rho \cong W_\rho^{k_\rho}$ for some k_ρ . By the following theorem this decomposition is independent of C and just depends on its type $(G, \mathcal{C}, m)$.

Theorem 5.2.1 ([7]). *Let χ be the character of G acting on V_ℓ . Then*

$$\chi = 2\chi_{\text{triv}} + (|E| - 2)\chi_{\text{reg}} - \sum_{p \in \mathbf{E}} \chi_p$$

where

- χ_{triv} is the character of the trivial G -representation, ρ_{triv}
- χ_{reg} is the character of the regular G -representation, ρ_{reg}
- χ_p is the character of the representation induced from the trivial representation of the subgroup $\langle g_p \rangle$ where g_p is the monodromy of a loop around the branch point p

When applying connectedness results like 2.4.1, we will need to be able to choose $\mathbf{m}$ to be sufficiently large and be guaranteed that the multiplicity of ρ in V_ℓ also increases. The following lemma guarantees this.

Lemma 5.2.2. *If $\min_i m_i$ is sufficiently large, then each nontrivial k_ρ can be made arbitrarily large. In addition the trivial representation will never occur.*

Proof. Let the multiplicity of an irreducible representation ρ in a representation ψ be denoted by $m(\psi, \rho)$. First we show that $m(\rho_{\text{reg}}, \rho)$ is greater than or equal to

the $m(\text{Ind}_{\langle g \rangle}^G \rho_{\text{triv}}, \rho)$ for g arbitrary. Treating W_ρ as a module for D_ρ , by the Artin-Wedderburn theorem, the former multiplicity is $\dim_{D_\rho} W_\rho$. Schur's lemma implies that the latter multiplicity is

$$m(\text{Ind}_{\langle g \rangle}^G \rho_{\text{triv}}, \rho) = \dim \text{Hom}_G(W_\rho, \text{Ind}_{\langle g \rangle}^G \rho_{\text{triv}}) / \dim_{\mathbb{F}_\ell} D_\rho.$$

Applying Frobenius Reciprocity,

$$\begin{aligned} \dim \text{Hom}_G(W_\rho, \text{Ind}_{\langle g \rangle}^G \rho_{\text{triv}}) &= \dim \text{Hom}_G(\text{Res}_{\langle g \rangle}^G \rho, \rho_{\text{triv}}) \\ &= \dim \text{Hom}(\rho_{\text{triv}}, \text{Res}_{\langle g \rangle}^G \rho) \\ &= \dim_{\mathbb{F}_\ell} W_\rho^{\langle g \rangle} \end{aligned}$$

By definition $d\rho(g) = \rho(g)d$ for all $d \in D_\rho$ so $W_\rho^{\langle g \rangle}$ is a D_ρ submodule of W_ρ and furthermore $\dim_{\mathbb{F}_\ell} W_\rho^{\langle g \rangle} / \dim_{\mathbb{F}_\ell} D_\rho = \dim_{D_\rho} W_\rho^{\langle g \rangle}$. Hence the statement on multiplicities follows since $\dim_{D_\rho} W_\rho^{\langle g \rangle} \leq \dim_{D_\rho} W_\rho$.

Now by Theorem 5.2.1 we know for $\rho \neq \rho_{\text{triv}}$

$$(|E| - 2)m(\rho_{\text{reg}}, \rho) \geq \sum_{p \in \mathbf{E}} m(\text{Ind}_{\langle g_p \rangle}^G \rho_{\text{triv}}, \rho)$$

and using the above computation, we can rewrite this as

$$\sum_{p \in \mathbf{E}} (\dim_{D_\rho} W_\rho - \dim_{D_\rho} W_\rho^{\langle g_p \rangle}) - 2(\dim_{D_\rho} W_\rho) \geq 0.$$

To show that k_ρ grows with $\min m_i$, it suffices to show that at least one of the $\dim_{D_\rho} W_\rho - \dim_{D_\rho} W_\rho^{\langle g_p \rangle} > 0$. This is clear since G is generated by the g_ρ and ρ is a non-trivial irreducible representation.

Finally, the G -invariants V_ℓ^G , correspond to those homology classes that descend to $\mathbb{P}^1(\mathbb{C})$. Since $H_1(\mathbb{P}^1(\mathbb{C}), \mathbb{Z}/\ell\mathbb{Z})$ is trivial, $V_\ell^G = 0$. $\square$

Let

$$V = \bigoplus_{\rho \in \mathcal{D}} V_\rho \oplus \bigoplus_{\rho \in \text{Irr}_\ell(G) - \mathcal{D}} M_\rho$$

be a decomposition of V_ℓ into irreducible G representations, where as in the notation of 3.1.3, $\mathcal{D}$ represents the set of self-dual irreducible representations of V_ℓ .

We have an induced decomposition of the symplectic centralizer.

$$C_{\text{Sp}(V_\ell)}(G) = \prod_{\rho \in \mathcal{D}} C_{\text{Sp}(V_\rho)}(G) \times \prod_{\rho \in \text{Irr}(G) - \mathcal{D}} C_{\text{Sp}(M_\rho)}(G) \quad (5.1)$$

Theorem 3.1.10 implies that each $C_{\text{Sp}(V_\rho)}(G), C_{\text{Sp}(M_\rho)}(G)$ is isomorphic to $\Gamma(k_\rho, D_\rho)$ where Γ is one of GL, Sp, U, or O. Each $C_{\text{Sp}(V_\rho)}(G), C_{\text{Sp}(M_\rho)}(G)$ can also naturally be viewed as a group of isometries of a G -invariant form on $\text{Inj}_G(W_\rho^{k_\rho}, V_\rho)$.

5.3 Covers Corresponding to Subspaces

Let W be a fixed $\mathbb{F}_\ell[G]$ module. Specifying an unramified cover $C' \rightarrow C$ with Galois group W is equivalent to giving a surjection $V_\ell \twoheadrightarrow W$. Dualizing, such surjections are in bijection with injections $W^\vee \hookrightarrow V_\ell^\vee$. Furthermore requiring the composition $C' \rightarrow C \rightarrow \mathbb{P}^1(\mathbb{C})$ to be Galois is the same as requiring that the action of G preserves this injection, or alternatively the surjection. Hence, if W is a $\mathbb{F}_\ell[G]$ module, the set of covers of C with Galois group W , which are Galois over $\mathbb{P}^1(\mathbb{C})$ with Galois group $G \ltimes W$, are in bijection with $\text{Inj}_G(W^\vee, V_\ell)$, where we have composed with the isomorphism $V_\ell^\vee \rightarrow V_\ell$ arising from the symplectic form.

We are interested in understanding the space of all such covers. Since $C' \rightarrow C$ is unramified, the branch points of the cover $C' \rightarrow \mathbb{P}^1(\mathbb{C})$ are the same as that of $C \rightarrow \mathbb{P}^1(\mathbb{C})$. Let the associated surjection, $f' : \pi_1(\mathbb{P}^1(\mathbb{C}) - \mathbf{E}, \infty) \rightarrow G \ltimes W$. Hence in

the notation of section 2.2.3, C' is a cover of type $(G \ltimes W, C', m)$ where C' is a tuple of conjugacy classes. We now determine C' explicitly.

Lemma 5.3.1. *Fix a conjugacy class $C \subset G$. Let k be the order of an element of $c \in C$ and let $p_k(x) = x^{k-1} + x^{k-2} + \cdots + 1$. Then the set of elements*

$$\{(c, w) : c \in C, w \in \ker p(c)\}$$

forms a conjugacy class of $G \ltimes W$ and is precisely the set of elements lying over C that have order k .

Proof. Take $g \in G, c \in C, w, v \in W$ with $p(c)w = 0$. Then

$$(g, v)(c, w)(g, v)^{-1} = (g c g^{-1}, v + g w - g c g^{-1} v).$$

By assumption

$$p(g c g^{-1})(1 - g c g^{-1})v = 0 \text{ and } p(g c g^{-1})g w = g p(c)w = 0.$$

Now take d with $g c g^{-1} = d$ and assume $p(d)w' = 0$. We need to find (g, v) such that $(g, v)(c, w)(g, v)^{-1} = (d, w')$, so by the computation above, it suffices to solve the equation

$$(1 - g c g^{-1})v + g w = w'$$

for some v . Now this implies that $(1 - d)v = w' + g w \in \ker p(d)$. Since the order of d is k which is coprime to the characteristic of $\mathbb{F}_\ell$ we see that $(1 - d)$ is invertible on $\ker p(d)$. Hence we can find such a v . $\square$

Denote such a conjugacy class corresponding to C by C_W .

Lemma 5.3.2. $C' = (C'_1, \dots, C'_k)$ where $C'_i = (C_i)_W$.

Proof. Let $e \in E_i$ be a branch point and let $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}), \infty)$ be a small loop around e . Assume that $f(\gamma) = c \in \mathcal{C}_i$. The composition of f' with the natural projection $G \ltimes W \rightarrow G$ gives f . Hence $f'(\gamma) = (c, w)$ for some $w \in W$. Since $C' \rightarrow C$ is unramified, the order of the inertia subgroup at e for C and C' must be the same. This implies that the order of c and the order of (c, w) agree. This is equivalent to the condition that $p(c)w = 0$. $\square$

The space of all such $G \ltimes W$ covers with monodromy in $\mathcal{C}'$, is just $\text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'}$. There is a natural map $\tau : \text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'} \rightarrow \text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}$ mapping the point representing C' , $[C']$ to the point representing C , $[C]$. Since $\text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'}$ and $\text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}$ both admit étale maps to $\text{Conf}_{|\mathbf{m}|}(\mathbb{C})$, we see that τ is étale by the cancellation property of étale morphisms.

$$\begin{array}{ccc} \text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'} & \xrightarrow{\tau} & \text{CHur}_{G, \mathbf{m}}^{\mathcal{C}} \\ \downarrow & \swarrow & \\ \text{Conf}_{\mathbf{m}}(\mathbb{C}) & & \end{array}$$

By the discussion above, the fiber $\tau^{-1}([C])$ is identified with $\text{Inj}_G(W^\vee, V_\ell)$. Since τ is étale, the associated monodromy action of $\pi_1(\text{CHur}_{G, \mathbf{m}}^{\mathcal{C}}, [C])$ on $\tau^{-1}([C])$ agrees with the action of $M_\ell(G)$ on $\text{Inj}_G(W^\vee, V_\ell)$. Hence the number of orbits of $M_\ell(G)$ on $\text{Inj}_G(W^\vee, V_\ell)$ will agree with the number of orbits of $M_\ell(G)$ on the fiber $\tau^{-1}([C])$. This latter quantity is just $|\pi_0(\text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'})|$, the number of connected components of $\text{CHur}_{G \ltimes W, \mathbf{m}}^{\mathcal{C}'}$.

Lemma 5.3.3. *Let W be a vector space over $\mathbb{F}_\ell$ with an action of G . Then*

$$H_2(G \ltimes W) = (\text{Alt}^2 W)^G.$$

Proof. Let $H_2 = H_2(G \ltimes W)$. We will use the Hochschild-Serre Spectral sequence. The

terms on the second page are $E_{r,s}^2 = H_r(G, H_s W)$. We also have the filtration

$$0 \subset F_0 H_2 \subset F_1 H_2 \subset F_2 H_2 = H_2$$

with successive quotients $G_i H_2 = F_i H_2 / F_{i-1} H_2 = E_{r,2-r}^\infty$.

Now

$$G_2 H_2 = E_{2,0}^\infty = E_{2,0}^2 = H_2(G) = 0$$

so $G_2 H_2 = 0$ and $F_2 H_2 = F_1 H_2$. For $r, s > 0$, by Theorem A.1.18 in [28], $E_{r,s}^\infty = E_{r,s}^2 = H_r(G, H_s(W)) = 0$, since $H_s(W)$ is a $\mathbb{F}_\ell$ vector space and $(\ell, |G|) = 1$. In particular we see that $G_1 H_2 = E_{1,1}^\infty = 0$ implying that $F_2 H_2 = F_1 H_2 = F_0 H_2$. Hence $H_2 = F_0 H_2 = E_{0,2}^\infty$.

Now $E_{0,2}^2 = H_0(G, H_2(W)) = H_2(W)_G$. From the definition of the differential

$$E_{0,2}^3 = E_{0,2}^2 / \text{im} (E_{2,1}^2 \rightarrow E_{0,2}^2) = E_{0,2}^2.$$

Furthermore after the third page, the images of all differentials are 0, so, $E_{0,2}^\infty = E_{0,2}^3 / \text{im} (E_{3,0}^3 \rightarrow E_{0,2}^3)$. Clearly $E_{3,0}^3$ is divisible by primes dividing $|G|$, and $E_{0,2}^2$ has exponent ℓ , so $E_{3,0}^3 \rightarrow E_{0,2}^3$ has image 0.

Concluding we see that

$$H_2(G \ltimes W) \cong E_{0,2}^\infty = H_2(W)_G.$$

Now Theorem 6.4.c of [8] identifies $H_2(W)$ with $\text{Alt}^2 W$. Since invariants and co-invariants are isomorphic for $\mathbb{F}_\ell$ representations of G ,

$$H_2(G \ltimes W) \cong (\text{Alt}^2 W)^G.$$

□

The final theorem of this section gives an explicit way to count the orbits of $M_\ell(G)$ on $\text{Inj}_G(W^\vee, V_\ell)$.

Theorem 5.3.4. *Let W be a $\mathbb{F}_\ell[G]$ module vector such that $\text{Inj}_G(W, V_\ell)$ is nonempty. If $\min_i m_i$ is sufficiently large, then the number of orbits of $M_\ell(G)$ on $\text{Inj}_G(W, V_\ell)$ is $|(\text{Alt}^2 W)^G|$.*

Proof. By the above discussion the number of orbits of $M_\ell(G)$ on $\text{Inj}_G(W, V_\ell)$ is given by $|\pi_0(\text{CHur}_{G \times W, \mathbf{m}}^{\mathcal{C}'})|$. We can combine Theorem 2.4.1 and Lemma 5.3.3 to see that

$$|\pi_0(\text{CHur}_{G \times W, \mathbf{m}}^{\mathcal{C}'})| = (\text{Alt}^2 W)^G / Q_{\mathcal{C}'} \quad (5.2)$$

Hence we need to just show that $Q_{\mathcal{C}'}$, the image of the induced map

$$H_2(\mathbb{Z}^2) \rightarrow H_2(\langle x, y \rangle) \hookrightarrow (\text{Alt}^2 W)^G$$

is trivial for every $x \in \mathcal{C}'$ and y commuting with x .

By lemma 5.3.1, x is necessarily of the form (g, w) with $g \in G$ and $w \in \ker p(g)$. The order of (g, w) is just the order of g . Hence the subgroup $\langle x, y \rangle$ is annihilated by $|G|$ and so is $H_2(\langle x, y \rangle)$. Since $(\text{Alt}^2 W)^G$ is an ℓ -group, $H_2(\langle x, y \rangle)$ is also annihilated by ℓ . This implies that $Q_{\mathcal{C}'}$ is trivial since ℓ is coprime to $|G|$.

□

5.4 Proof of the Main Monodromy Theorem

We are finally in a position to give a proof of the main theorem. In the decomposition, 5.1, let $M_\ell(G)_\rho$ denote the image of the monodromy group $M_\ell(G)$ projected onto $C_{\text{Sp}(V_\rho)}(G)$.

Lemma 5.4.1. *Assume $\min_i m_i$ is large enough. Then $C_{\mathrm{Sp}(V_\rho)}(G)' \subset M_\ell(G)_\rho$.*

Proof. First consider the case when $\rho \in \mathcal{D}$, the set of self-dual irreducible representations of G . By Theorem 5.3.4, the number of orbits of $M_\ell(G)_\rho$ on $\mathrm{Inj}_G(W_\rho^k, V_\rho)$ is just $|(\mathrm{Alt}^2 W_\rho^k)^G|$. By lemma 3.1.9 the latter is just the number of orbits of $C_{\mathrm{Sp}(V_\rho)}(G)$ on $\mathrm{Inj}_G(W_\rho^k, V)$. The result then follows in this case by Theorem 3.2.4. If $\rho \in \mathrm{Irr}(G) - \mathcal{D}$ then $C_{\mathrm{Sp}(V_\rho)}(G)$ is a general linear group. By Theorem 5.3.4 the number of orbits of $M_\ell(G)$ on $\mathrm{Inj}_G(W_\rho^3, V_\rho)$ is $|(\mathrm{Alt}^2 W_\rho^3)^G|$. When W_ρ is not self dual, this quantity is 1. Hence $M_\ell(G)_\rho$ acts transitively on the three dimensional subspaces of V_ρ and so by Theorem 3.2.2 the result follows. $\square$

Using the group theoretic tools from section 3.3 we can now prove the main theorem. Let $\phi : C_{\mathrm{Sp}(V_\ell)}(G) \rightarrow \mathbb{P}C_{\mathrm{Sp}(V_\ell)}(G)$ be the quotient by the center described in 3.2.

Theorem 5.4.2. *Let G be a group with trivial Schur multiplier and ℓ a prime such that $\ell \nmid 2|G|$. For $\min_i m_i$ large enough, $(G, \mathcal{C}, \mathbf{m})$ has big monodromy, i.e.*

$$C_{\mathrm{Sp}(V_\ell)}(G)' = \prod_{\rho \in \mathcal{D}} C_{\mathrm{Sp}(V_\rho)}(G)' \times \prod_{\rho \in \mathrm{Irr}(G) - \mathcal{D}} C_{\mathrm{Sp}(M_\rho)}(G)' \subset M_\ell(G)$$

Proof. Since $\min_i m_i$ is being chosen large enough, the previous lemma implies that $C_{\mathrm{Sp}(V_\rho)}(G)' \subset M_\ell(G)_\rho$. Also, by Lemma 5.2.2 by choosing $\min_i m_i$ large enough, we can guarantee that each $k_p \geq 5$.

Now choose two non-isomorphic representations $\rho, \rho' \in \mathrm{Irr}_\ell(G)$. Let $M_\ell(G)_{\rho, \rho'}$ be the image of the projection

$$M_\ell(G) \rightarrow C_{\mathrm{Sp}(V_\rho)}(G) \times C_{\mathrm{Sp}(V_{\rho'})}(G).$$

and let $\phi(M_\ell(G))_{\rho, \rho'}$ be the image of the projection,

$$\phi(M_\ell(G)) \rightarrow \mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G) \times \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G).$$

I claim that $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G)' \times \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)' \subset \phi(M_\ell(G))_{\rho, \rho'}$. By Lemma 3.2.1, $\Gamma_1 = C_{\mathrm{Sp}(V_\rho)}(G)$ and $\Gamma_2 = C_{\mathrm{Sp}(V_{\rho'})}(G)$ satisfy the assumptions of Theorem 3.3.3 applied to the subgroup $\phi(M_\ell(G))$.

Thus there are two possible cases.

- **Case 1** $C_{\mathrm{Sp}(V_\rho)}(G) \not\cong C_{\mathrm{Sp}(V_{\rho'})}(G)$ and $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G)' \not\cong \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)'$: In this case $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G)' \times \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)' \subset \phi(M_\ell(G))_{\rho, \rho'}$.
- **Case 2** $C_{\mathrm{Sp}(V_\rho)}(G) \cong C_{\mathrm{Sp}(V_{\rho'})}(G)$ and $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G)' \cong \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)'$: For this case, we have to rule out $\phi(M_\ell(G))_{\rho, \rho'}$ being a diagonally embedded subgroup of $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G) \times \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)$. Since $\rho \not\cong \rho'$, Theorem 5.3.4 implies that the number of orbits of $M_\ell(G)_{\rho, \rho'}$ on $\mathrm{Inj}_G(W_\rho \oplus W_{\rho'}, H^1(C, \mathbb{F}_\ell))$ is given by

$$|(\mathrm{Alt}^2 W_\rho \oplus W_{\rho'})^G| = |(\mathrm{Alt}^2 W_\rho)^G| |(\mathrm{Alt}^2 W_{\rho'})^G|.$$

By Corollary 3.1.9 this also counts the number of orbits of $C_{\mathrm{Sp}(V_\rho)}(G) \oplus C_{\mathrm{Sp}(V_{\rho'})}(G)$ on $\mathrm{Inj}_G(W_\rho \oplus W_{\rho'}, V_\ell)$.

If $\phi(M_\ell(G))_{\rho, \rho'}$ were diagonally embedded in $\mathbb{P}C_{\mathrm{Sp}(V_\rho)}(G) \times \mathbb{P}C_{\mathrm{Sp}(V_{\rho'})}(G)$, it would necessarily have more orbits on the lines of the vector space

$$\mathrm{Inj}_G(W_\rho \oplus W_{\rho'}, V_\ell).$$

We elaborate on this now. Since $C_{\mathrm{Sp}(V_\rho)}(G) \cong C_{\mathrm{Sp}(V_{\rho'})}(G)$, and since $k_\rho, k_{\rho'} \geq 5$, we can set $k := k_\rho = k_{\rho'}$, $\mathbb{F} := \mathbb{F}_\rho = \mathbb{F}_{\rho'}$ and $G := C_{\mathrm{Sp}(V_\rho)}(G) \cong C_{\mathrm{Sp}(V_{\rho'})}(G)$. Abstractly as $\mathbb{F}^k$ vector spaces, $\mathrm{Inj}_G(W_\rho, V_\rho) \cong \mathrm{Inj}_G(W_{\rho'}, V_{\rho'})$ and we set V to be this common vector space. Let H be the image of $\phi(M_\ell(G))$ in $G \times G$ identified with $C_{\mathrm{Sp}(V_\rho)}(G) \times C_{\mathrm{Sp}(V_{\rho'})}(G)$.

Since $\mathbb{P}G/\mathbb{P}G' \cong \mathbb{P}C_{\text{Sp}(V_\rho)}(G)/\mathbb{P}C_{\text{Sp}(V_\rho)}(G)'$ is cyclic the projection of H onto each component of $\mathbb{P}G \times \mathbb{P}G$, denoted H_1 and H_2 respectively, are identical subgroups of $\mathbb{P}G$ containing $\mathbb{P}G'$. So in particular, choosing an isomorphism $\psi : H_1 \rightarrow H_2$, the elements of H are all of the form $(\gamma, \psi(\gamma))$ with $\gamma \in H_1$.

Now consider the line $\mathbf{v}$ spanned by some $(v, v) \in V \times V$. The orbit of $\mathbf{v}$ under H is forced to be lines spanned by elements of the form $(\gamma v, \psi(\gamma)v)$. In particular, no line spanned by a vector of the form (v, w) with $w \neq v$ can be in the orbit of $\mathbf{v}$. The full orbit of $G \times G$ certainly has such an element.

We can now use Theorem 3.3.2 to establish that:

$$\prod_{\rho \in D} \mathbb{P}C_{\text{Sp}(V_\rho)}(G)' \times \prod_{\rho \in \text{Irr}(G) - D} \mathbb{P}C_{\text{Sp}(M_\rho)}(G)' \subset \phi(M_\ell(G))$$

Finally we can conclude the result using Lemma 3.3.4. □

Bibliography

- [1] S. S. ABHYANKAR, *Three ways of measuring distance, three orbits, three subdegrees, or the great theorems of Cameron and Kantor*, Notices Amer. Math. Soc., 49 (2002), pp. 759–769.
- [2] N. A'CAMPO, *Tresses, monodromie et le groupe symplectique*, Comment. Math. Helv., 54 (1979), pp. 318–327.
- [3] J. D. ACHTER, *The distribution of class groups of function fields*, J. Pure Appl. Algebra, 204 (2006), pp. 316–333.
- [4] J. D. ACHTER AND R. PRIES, *The integral monodromy of hyperelliptic and trielliptic curves*, Math. Ann., 338 (2007), pp. 187–206.
- [5] D. ALLCOCK AND C. HALL, *Monodromy groups of Hurwitz-type problems*, Adv. Math., 225 (2010), pp. 69–80.
- [6] M. ASCHBACHER, *Finite group theory*, vol. 10 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, second ed., 2000.
- [7] S. A. BROUGHTON, *The homology and higher representations of the automorphism group of a Riemann surface*, Trans. Amer. Math. Soc., 300 (1987), pp. 153–158.
- [8] K. S. BROWN, *Cohomology of groups*, vol. 87 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

- [9] P. J. CAMERON, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc., 13 (1981), pp. 1–22.
- [10] P. J. CAMERON AND W. M. KANTOR, *2-transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra, 60 (1979), pp. 384–422.
- [11] H. COHEN AND H. W. LENSTRA, JR., *Heuristics on class groups*, in Number theory (New York, 1982), vol. 1052 of Lecture Notes in Math., Springer, Berlin, 1984, pp. 26–36.
- [12] H. DAVENPORT AND H. HEILBRONN, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A, 322 (1971), pp. 405–420.
- [13] T. S. DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version x.y.z)*, YYYY. <http://www.sagemath.org>.
- [14] N. M. DUNFIELD AND W. P. THURSTON, *Finite covers of random 3-manifolds*, Invent. Math., 166 (2006), pp. 457–521.
- [15] J. ELLENBERG, *Geometric analytic number theory*, Lecture Notes for 2014 Arizona Winter School.
- [16] J. S. ELLENBERG, A. VENKATESH, AND C. WESTERLAND, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, (2009).
- [17] J. S. ELLENBERG, A. VENKATESH, AND C. WESTERLAND, *Homological stability for hurwitz spaces and the cohen-lenstra conjecture over function fields, ii*, 2012.
- [18] B. FARB AND D. MARGALIT, *A primer on mapping class groups*, vol. 49 of Princeton Mathematical Series, Princeton University Press, Princeton, NJ, 2012.

- [19] M. D. FRIED AND H. VLKLEIN, *The inverse galois problem and rational points on moduli spaces*, MATH. ANNALEN, 290 (1991), pp. 771–800.
- [20] E. FRIEDMAN AND L. C. WASHINGTON, *On the distribution of divisor class groups of curves over a finite field*, in Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239.
- [21] W. FULTON, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Mathematics, 90 (1969), pp. 542–575.
- [22] L. C. GROVE, *Classical groups and geometric algebra*, vol. 39 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2002.
- [23] C. HALL, *Big symplectic or orthogonal monodromy modulo l* , Duke Math. J., 141 (2008), pp. 179–203.
- [24] A. HATCHER, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.
- [25] C. HERING, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geometriae Dedicata, 2 (1974), pp. 425–460.
- [26] A. HURWITZ, *Ueber riemann'sche flächen mit gegebenen verzweigungspunkten*, Mathematische Annalen, 39 (1891), pp. 1–60.
- [27] W. M. KANTOR AND R. A. LIEBLER, *The rank 3 permutation representations of the finite classical groups*, Trans. Amer. Math. Soc., 271 (1982), pp. 1–71.
- [28] K. P. KNUDSON, *Homology of linear groups*, vol. 193 of Progress in Mathematics, Birkhäuser Verlag, Basel, 2001.

- [29] M. W. LIEBECK, C. E. PRAEGER, AND J. SAXL, *Regular subgroups of primitive permutation groups*, Mem. Amer. Math. Soc., 203 (2010), pp. vi+74.
- [30] E. LOOIJENGA, *Prym representations of mapping class groups*, Geom. Dedicata, 64 (1997), pp. 69–83.
- [31] C. R. MATTHEWS, L. N. VASERSTEIN, AND B. WEISFEILER, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3), 48 (1984), pp. 514–532.
- [32] C. T. MCMULLEN, *Braid groups and Hodge theory*, Math. Ann., 355 (2013), pp. 893–946.
- [33] D. PERIN, *On collineation groups of finite projective spaces*, Math. Z., 126 (1972), pp. 135–142.
- [34] K. A. RIBET, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math., 98 (1976), pp. 751–804.
- [35] D. P. ROBERTS AND A. VENKATESH, *Hurwitz monodromy and full number fields*, Algebra Number Theory, 9 (2015), pp. 511–545.
- [36] M. ROMAGNY AND S. WEWERS, *Hurwitz spaces*, in Groupes de Galois arithmétiques et différentiels, vol. 13 of Sémin. Congr., Soc. Math. France, Paris, 2006, pp. 313–341.
- [37] T. N. VENKATARAMANA, *Image of the Burau representation at d -th roots of unity*, Ann. of Math. (2), 179 (2014), pp. 1041–1083.

- [38] —, *Monodromy of cyclic coverings of the projective line*, Invent. Math., 197 (2014), pp. 1–45.
- [39] H. VÖLKLEIN, *Groups as Galois groups*, vol. 53 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1996. An introduction.
- [40] D. B. WRIGHT DAVID J., *Density of discriminants of cubic extensions.*, Journal für die reine und angewandte Mathematik, 386 (1988), pp. 116–138.
- [41] J.-K. YU, *Toward a proof of the cohen-lenstra conjecture in the function field case.*