Cohen-Lenstra heuristics and vanishing of zeta functions for superelliptic curves over finite fields

by
Hyun Jong Kim

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)

at the
University of Wisconsin-Madison
2024

Date of Final Oral Exam: 04/16/2024
The dissertation is approved by the following members of the Final Oral Committee:
Jordan S. Ellenberg, Professor, Mathematics
Tonghai Yang, Professor, Mathematics
Brian Lawrence, Assistant Professor, Mathematics
Marissa Kawehi Loving, Assistant Professor, Mathematics

Cohen-Lenstra heuristics and vanishing of zeta functions for superelliptic curves over finite fields

Hyun Jong Kim

Abstract

We prove a Cohen-Lenstra type result commenting on the distribution of class group structures amongst function fields of superelliptic curves over finite fields. We also prove a result commenting on the sparsity of such superelliptic curves whose zeta functions vanish at a fixed complex number. These results are proven via point-counting techniques on certain Hurwitz schemes generalizing techniques of Ellenberg-Venkatesh-Westerland and Ellenberg-Li-Shusterman. To obtain these point counts, We prove a unitary big monodromy theorem generalizing big monodromy theorems of Yu and Achter-Pries by appealing to an arithmeticity theorem of Venkataramana.

Dedication

To my family, without whom my dreams would not be possible.
To my friends, who believe in me and enrich my life.

Acknowledgements

I would like to thank my advisor, Professor Jordan S. Ellenberg for proposing this thesis project, and for his steadfast support throughout my PhD. I hope to someday be a prolific and eclectic mathematician as he is in my own right.

I dedicate this thesis to my mother, Yui Jeong, my father, Jou An, and my elder sisters, Hye Sun and Hye Jin, who have all wholeheartedly believed in me and supported my dreams of becoming a mathematician for almost twenty years. They have ensured that I am well conditioned to tackle everyday challenges. I also dedicate this thesis to my many friends, who have similarly believed in me and who give me the strength to believe in myself. A few among my friends whom I would especially like to acknowledge include (in alphabetical order by family name) Tejasi Bhatnagar, Kaiyi Huang, Mihaela Ifrim, Sun Woo Park, Taylor Tan, and John Yin — they have supported me emotionally as I faced especially arduous challenges over the past year.

I would additionally like to thank Jeff Achter, Tejasi Bhatnagar, Jordan S. Ellenberg, Chris Hall, Aaron Landesmann, Wanlin Li, Sun Woo Park, Rachel Pries, and Will Sawin for helpful discussions concerning this project.

Contents

List of Tables

Chapter 1

Introduction

Given a global field K, write $\mathrm{Cl}(K)$ for its ideal class group. Given an abelian group A, write A_ℓ for the Sylow ℓ-subgroup of A for a prime number ℓ, and write A_o for the odd part of A, i.e. the subgroup of A of elements of odd order. The original Cohen-Lenstra heuristics [17] are conjectures for the distribution of the odd parts of class groups of imaginary and real quadratic fields. One can state these conjectures as follows, cf [6, Conjecture 5.10.1, Conjecture 5.10.2]:

Conjecture 1.0.1. *For $X > 0$, let S_X be the set of discriminants D of imaginary quadratic number fields such that $|D| < X$. For any odd prime ℓ and any finite abelian ℓ-group A,*

$$\lim_{X\to\infty} \frac{\#\{D \in S_X : \mathrm{Cl}(\mathbb{Q}(\sqrt{D}))_p \cong A\}}{\#S_X} = \frac{\prod_{i=1}^{\infty}(1-p^{-i})}{|\operatorname{Aut}(A)|}.$$

Conjecture 1.0.2. *For $X > 0$, let S_X be the set of discriminants D of real quadratic number fields such that $|D| < X$. For any finite abelian group A of odd order,*

$$\lim_{X\to\infty} \frac{\#\{D \in S_X : \mathrm{Cl}(\mathbb{Q}(\sqrt{D}))_o \cong A\}}{\#S_X} = \frac{1}{2|A| \cdot (\prod_{i=1}^{\infty}(1-2^{-i})) \cdot \left(\prod_{k>2}\zeta(k)\right) \cdot |\operatorname{Aut}(A)|}$$

where $\zeta(k)$ is the Riemann zeta function.

There have been various conjectures and results about analogous distributions for both number fields and functions fields since the inception of these conjectures. See [47], [25],

and [44] for some relevant works in the literature. One of the main results of this thesis is a generalization Ellenberg, Venkatesh, and Westerland's [15] result for function fields resembling Cohen and Lenstra's original conjecture for imaginary quadratic fields:

Theorem 1.0.3 ([15, 1.2 Theorem])**.** *Let $\ell > 2$ be prime and A a finite abelian ℓ-group. Write δ^+ (resp. δ^-) for the upper density (resp. lower density) of imaginary*[1] *quadratic extensions of $\mathbb{F}_q(t)$ for which the ℓ-part of the class group is isomorphic to A. Then $\delta^+(q)$ and $\delta^-(q)$ converge, as $q \to \infty$ with $q \neq 1 \pmod{\ell}$ to $\frac{\prod_{i>1}(1-\ell^{-i})}{|\operatorname{Aut}(A)|}$.*

Theorem 7.0.1 generalizes the above result to Kummer extensions of $\mathbb{F}_q(t)$ of the form $y^d = f(t)$. In particular, our main results assume that $\mathbb{F}_q$ contain a primitive dth-root of unity or equivalently that $q \equiv 1 \pmod{d}$. Note that both Theorem 1.0.3 and Theorem 7.0.1 concern limits which first let $\deg f(t) \to \infty$ and then let $q \to \infty$. In contrast, [25] concerns limits of distributions for function fields which first let $q \to \infty$ and then let the branch locus degree approach infinity.

Our method for proving this generalization mimics the method that [15] used to prove Theorem 1.0.3 above — one asymptotically counts $\mathbb{F}_q$-points on certain Hurwitz schemes which we denote by $\mathbf{X}_n/\mathbb{F}_q$ in Chapter 6. Letting

- $d \geq 2$ be an integer,
- ℓ be a prime number relatively prime to d,
- A be a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(\sum_{i=0}^{d-1} X^i)$,
- G be the semidirect product $A \rtimes \mathbb{Z}/d\mathbb{Z}$ where $1 \in \mathbb{Z}/d\mathbb{Z}$ acts on A by multiplication by ζ_d, and
- c is the conjugacy class of G consisting of elements of the form (a, ζ_d) for $a \in A$,

the Hurwitz scheme $\mathbf{X}_n$ parameterizes tamely ramified G-covers $f : C \to \mathbb{P}^1$ with monodromy type (see Chapter 3) c away from ∞ such that the quotient $C \to C/A$ is unramified

[1] i.e. ramified at ∞, cf. Definition 3.3.1

above the points in C/A above $\infty \in \mathbb{P}^1$. By the Grothendieck-Lefschetz fixed point formula,

$$|\mathbf{X}_n(\mathbb{F}_q)| = \sum_{j=1}^{2n} (-1)^j \operatorname{Tr}(\operatorname{Frob}_q | H_c^j(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda)). \tag{1.0.1}$$

Ellenberg, Venkatesh, and Westerland's homological stability results [15, Theorem 6.1] asymptotically bound the $j < 2n$ terms, which are $o(q^n)$. We then show that the $j = 2n$ term is q^n whenever n is sufficiently large. In turn, we show this via Corollary 4.3.8, which is a statement about Hermitian spaces, and via Theorem 6.2.6 and Proposition 6.2.8, which give desirable "big monodromy results", i.e. that certain monodromy representations have sufficiently large image.

The main difference between the case of $d = 2$ proved by [15] and the case of more general d is the action of ζ_d on $\operatorname{Jac}(C)$, where C is the curve corresponding to the function field — when $d = 2$, the action is simply negation and when $d > 2$, the action is be more complicated. Moreover, the Weil pairing on $\operatorname{Jac}(C)$ yields a non-trivial Hermitian pairing when $d > 2$. Hence, Corollary 4.3.8 is a statement about Hermitian spaces unlike is predecessor [15, Lemma 8.9], which is about symplectic spaces, and the monodromy representations of interest are unitary representations and not merely symplectic representations.

Furthermore, Ellenberg, Li, and Shusterman [13] used the machinery in Ellenberg, Venkatesh, and Westerland's paper [15] to prove a statement about the vanishing of zeta functions for hyperelliptic curves over $\mathbb{F}_q$.

Theorem 1.0.4 ([13, Theorem 1.2/3.2])**.** *Fix a prime p, and a complex number $s = \frac{1}{2} + it$. Write $\mathcal{H}_g(\mathbb{F}_q)$ for the family of genus g hyperellipic curves over $\mathbb{F}_q$ and write $Z_C(s)$ for the zeta function of a curve. As $k \to \infty$, we have*

$$\sup_g \frac{|\{C \in \mathcal{H}_g(\mathbb{F}_q) : Z_C(s) = 0\}|}{|\mathcal{H}_g(\mathbb{F}_q)} \ll p^{-k/276}$$

Theorem 9.0.9 similarly generalizes this result for superelliptic curves corresponding to the above Kummer extensions of $\mathbb{P}^1$. Once again, that the monodromy representations

of interest are unitary representations when $d > 2$ present difficulties not present in the $d = 2$ case. More specifically, Lemma 10.4.2, which generalizes [15, Lemma 3.5], is more cumbersome to prove when $d > 2$ compared to when $d = 2$.

Chapter 2 discusses aspects of the structure of groups of the form $A \rtimes \mathbb{Z}/d\mathbb{Z}$ where A is a finite ℓ-group for a prime $\ell \nmid d$. Lemma 2.0.5 and Lemma 2.0.6 show that the homological stability results of [15] are applicable to the Hurwitz scheme $\mathbf{X}_n$. Chapter 3 discusses monodromy types for covers of $\mathbb{P}^1$. Proposition 3.2.2 provides a convenient way to understand the monodromy types for curves given by $y^d = \prod_i (t - t_i)^{e_i}$ — the monodromy type of $t = t_i$ can be regarded as $e_i \in \mathbb{Z}/d\mathbb{Z}$. Chapter 4 discusses the Hermitian space theory leading up to Corollary 4.3.8 needed in later parts of this thesis.

Chapter 5 discusses the unreduced and reduced Burau representations, which are representations of the Artin braid group B_n. The chapter presents Venkataramana's result [43] that the reduced Burau representations evaluated at roots of unity are arithmetic, i.e. their images are of finite index in the largest possible "trivial" codomain. Section 6.1 introduces notations for the aforementioned Hurwitz schemes of interest, Section 6.2 proves relevant big monodromy results. There, Venkataramana's arithmeticity results establish base cases and Achter and Pries' clutching methods [2] demonstrate the inductive step of an induction argument. Section 6.3 puts together the details from the previous chapters and sections to prove Theorem 6.3.1, which asymptotically counts the $\mathbb{F}_q$-points of $\mathbf{X}_n$ as described above. Chapter 7 then uses Theorem 6.3.1 to finish proving Theorem 7.0.1. The details presented in this chapter are basically identical to those in [15, 8.1 to 8.4 Lemma] except for the fact that the abelian group surjections involved all must be equivariant for the ζ_d-action as well. We nevertheless include these details for completeness.

Chapter 8 and Chapter 9 generalize and ideas in [15, Section 2, Section 3]. Chapter 8 counts points on twists of $\mathbf{X}_n$ and Chapter 9 bounds the number of superelliptic curves whose zeta functions vanish at a fix complex number. Finally, Chapter 10 proves details, culminating in Lemma 10.4.2, about the orbits of the Burau representations evaluated at roots of unity and reduced modulo ℓ ultimately needed to conclude Theorem 9.0.9.

Chapter 2

Conjugacy structure of $A \rtimes \mathbb{Z}/d\mathbb{Z}$

In this section, we prove some lemmas concerning the group structure of $A \rtimes \mathbb{Z}/d\mathbb{Z}$ where d is a positive integer and A is a $\mathbb{Z}_\ell$-module with a $\mathbb{Z}/d\mathbb{Z}$-action for a prime ℓ that does not divide d. We often, but not always, write $\mathbb{Z}/d\mathbb{Z}$ as $\langle \zeta_d \rangle$ where ζ_d is a fixed generator of $\mathbb{Z}/d\mathbb{Z}$ and write the group structure of ζ_d multiplicatively and with an identity element of 1. Write $A^{\zeta_d} = A^{\langle \zeta_d \rangle}$ for the $\langle \zeta_d \rangle$-invariant subgroup of A.

Lemma 2.0.1. *Let $d \geq 2$ be an integer, and let A be a $\mathbb{Z}_\ell$-moodule with a $\langle \zeta_d \rangle \cong \mathbb{Z}/d\mathbb{Z}$-action where ℓ is a prime that does not divide d. The following hold for all $k, k_1, k_2 \in \mathbb{Z}$*

1. $(a_1, \zeta_d^{k_1}) \cdot (a_2, \zeta_d^{k_2}) = (a_1 + \zeta_d^{k_1} a_2, \zeta_d^{k_1+k_2})$
2. $(a, \zeta_d^k)^{-1} = (-\zeta_d^{-k} a, \zeta_d^{-k})$
3. $(a_1, \zeta_d^{k_1}) \cdot (a_2, \zeta_d^{k_2}) \cdot (a_1, \zeta_d^{k_1})^{-1} = (a_1 + \zeta_d^{k_1} a_2 - \zeta_d^{k_2} a_1, \zeta_d^{k_2})$
4. $(a_1, \zeta_d^k) \cdot (a_2, \zeta_d^k)^{-1} = (a_1 - a_2, 1)$
5. $(a_1, \zeta_d^k) \cdot (a_2, 1) \cdot (a_1, \zeta_d^k)^{-1} = (\zeta_d^k a_2, 1)$
6. $(a_1, 1) \cdot (a_2, \zeta_d^k) \cdot (a_1, 1)^{-1} = ((1 - \zeta_d^k) a_1 + a_2, \zeta_d^k)$

Proof. All of these are immediate calculations. □

We are further concerned with the case in which A^{ζ_d} is trivial. Corollary 2.0.3 lists equivalent conditions. To prove Corollary 2.0.3, we discuss

Since $\ell \nmid d$, $X^d - 1$ is square free over $\mathbb{Z}_\ell$. Letting $X^d - 1 = \prod_i f_i(X)$ be the prime factorization of $X^d - 1$ over $\mathbb{Z}_\ell$, we have an isomorphism $\mathbb{Z}_\ell[X]/(X^d - 1) \cong \prod_i \mathbb{Z}_\ell[X]/f_i(X)$, and the $\mathbb{Z}_\ell[X]/f_i(X)$ are the rings of integers of the unramified extensions $\mathbb{Q}_\ell[X]/(f_i(X))$ of $\mathbb{Q}_\ell$. Let $B_i = \mathbb{Z}_\ell[X]/f_i(X)$. In particular, a $\mathbb{Z}_\ell$-module with a $\langle \zeta_d \rangle$ action, i.e. a $(\mathbb{Z}_\ell[X]/(X^d - 1))$-module after identifying X with ζ_d, is the product of its B_i-components A_i. Given an element $a \in A$, write $a_i \in A_i$ for its B_i-component. Moreover, the B_i are discrete valuation rings with uniformizer ℓ, so the structure theorem for finitely generated modules over PID's applies. To summarize, we can decompose A via isomorphisms

$$A \cong \prod_i A_i \tag{2.0.1}$$

$$A_i \cong \bigoplus_{j=1}^{k_i} B_i/(\ell^{d_{i,j}}) \tag{2.0.2}$$

for finitely many integers $d_{i,j} \geq 0$. For convenience, let $f_0(X) = X - 1$ so that $B_0 \cong \mathbb{Z}_\ell$ and $\zeta_d = 1$ in B_0.

Lemma 2.0.2. *Let $d \geq 2$ be an integer, let ℓ be a prime not dividing d, and let A be a finitely generated $\mathbb{Z}_\ell$-module with a $\langle \zeta_d \rangle$-action. With notations as above, $A_0 = A^{\zeta_d}$.*

Proof. By construction, the elements of A_0 are clearly ζ_d-invariant. To show that the $A^{\zeta_d} \subseteq A_0$, it is equivalent to show that $\prod_{i \neq 0} A_i$ has only trivial ζ_d-invariants. Since ζ_d respects each multiplication A_i in $\prod_{i \neq 0} A_i$ and respects each direct summand of the decomposition $A_i \cong \bigoplus_{j=1}^{k_i} B_i/(\ell^{d_{i,j}})$, showing that $\prod_{i \neq 0} A_i$ has only trivial ζ_d-invariants is equivalent to showing that each $B_i/(\ell^{d_{i,j}})$ has only trivial ζ_d-invariants.

To show this, first note that the action of ζ_d on $B_i/\ell B_i$ does not have $1 \in \mathbb{F}_\ell$ as an eigenvalue whenever $i \neq 0$ because the characteristic polynomial of the multiplication-by-ζ_d-map on B_i is $f_i(X) \in \mathbb{Z}_\ell[X]$, which does not have a root of 1 when reduced modulo ℓ. Suppose for contradiction that there is some nonzero $b \in B_i/(\ell^{d_{i,j}})$ such that $\zeta_d b = b$. Note that this cannot happen when $d_{i,j} = 0$ because then $\frac{b}{\ell^{\mathrm{ord}_\ell(b)}}$ would be an element of $B_i^\times$ fixed by ζ_d, and reducing this element modulo ℓ would produce a eigenvector of $B_i/\ell B_i$ of

eigenvalue 1. Now assume that $d_{i,j} \geq 1$. In particular, $\operatorname{ord}_\ell b \leq d_{i,j} - 1$. Since the action of ζ_d on $B_i/\ell B_i$ has only trivial invariants, b must be in ℓB_i. Say that $b_1 \in B_i$ such that $b = b_1\ell$. In particular, $\zeta_d b_1 \ell = b_1 \ell$, so there is some $c_1 \in B_i$ such that $\zeta_d b_1 = b_1 + c_1 \ell^{d_{i,j}-1}$. Reducing modulo ℓ once again shows that $b_1 = b_2\ell$ for some $b_2 \in B_i$, so there is some $c_2 \in B_i$ such that $\zeta_d b_2 \ell = b_2 + c_2 \ell^{d_{i,j}-2}$. Continuing in this manner eventually yields elements $b_{d_{i,j}-1}, c_{d_{i,j}-1} \in B_i$ such that $b = b_{d_{i,j}-1}\ell^{d_{i,j}-1}$ and $\zeta_d b_{d_{i,j}-1} = b_{d_{i,j}-1} + c_{d_{i,j}-1}\ell$. The ℓ-adic order of $b_{d_{i,j}-1}$ is at most zero and hence must be exactly zero but the reduced equation $\zeta_d \bar{b}_{d_{i,j}-1} = \bar{b}_{d_{i,j}-1}$ modulo ℓ shows that $\bar{b}_{d_{i,j}-1}$ is an eigenvector of ζ_d of eigenvalue 1, which is a contradiction. Hence, $B_i/(\ell^{d_{i,j}})$ has trivial ζ_d-invariants as desired. □

Corollary 2.0.3. *Let $d \geq 2$ be an integer, let ℓ be a prime not dividing d, and let A be a finitely generated $\mathbb{Z}_\ell$-module with a $\langle \zeta_d \rangle$-action. The following are equivalent:*

1. *The induced action of ζ_d on $A/\ell A$ does not have $1 \in \mathbb{F}_\ell$ as an eigenvalue.*
2. *A^{ζ_d} is trivial.*
3. *A is a module over $\mathbb{Z}_\ell[\zeta_d] := \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.*

Proof. The equivalence of (2) and (3) follows immediately from Lemma 2.0.2. Moreover, (3) implies (1) because the action of ζ_d respects the direct summands $B_i/(\ell^{d_{i,j}})$ in the decomposition (2.0.2) and because the action of ζ_d on $B_i/\ell B_i$ does not have $1 \in \mathbb{F}_\ell$ as an eigenvalue for all $i \neq 0$ as shown in the proof of Lemma 2.0.2. Moreover, if (3) is not true, then the B_0-component A_0 of A must be nontrivial, so the action of ζ_d on $A_0/\ell A_0$ must have an eigenvalue of 1 and hence (1) would not be true. Therefore, (3) and (1) are equivalent.

□

Under the equivalent conditions of Corollary 2.0.3, some of the conjugacy classes of $A \rtimes \langle \zeta_d \rangle$ are simple.

Lemma 2.0.4. *Let $d \geq 2$ be an integer, and let A be a $\mathbb{Z}_\ell$-moodule with a $\langle \zeta_d \rangle \cong \mathbb{Z}/d\mathbb{Z}$-action where ℓ is a prime that does not divide d. Suppose that A^{ζ_d} is trivial. For any fixed*

integer k that is relatively prime to d, the set

$$c = \{(a, \zeta_d^k) \in A \rtimes \langle \zeta_d \rangle : a \in A\}$$

is a conjugacy class of $A \rtimes \langle \zeta_d^k \rangle$. In fact, any two elements of c are conjugate via an element of c and are conjugate via an element of A.

Proof. On the one hand, c is indeed closed under conjugation. On the other hand, note that $1-\zeta_d^k$ is invertible as a map $A \to A$ because k is assumed to be relatively prime to d and because the action of ζ_d on $A/\ell A$ does not have an eigenvalue of $1 \in \mathbb{F}_\ell$. Lemma 2.0.1(3) above then shows that

$$(a_1, \zeta_d^k)(a_2, \zeta_d^k)(a_1, \zeta_d^k)^{-1} = (a_3, \zeta_d^k)$$

if $a_1 = \frac{-\zeta_d^k a_2 + a_3}{1-\zeta_d^k}$. Moreover, Lemma 2.0.1(6) shows that

$$(a_1, 1)(a_2, \zeta_d^k)(a_1, 1)^{-1} = (a_3, \zeta_d^k)$$

if $a_1 = \frac{a_3 - a_2}{1-\zeta_d^k}$. □

Ellenberg, Venkatesh, and Westerland's homological stability result [15, Theorem 6.1] as well as its consequences in loc. cit. depend on having a non-splitting conjugacy class — we say that a conjugacy class c of a group G is *non-splitting* if for any subgroup $H \leq G$, the intersection $c \cap H$ is either empty or a conjugacy class in H. We show that the conjugacy classes of Lemma 2.0.4 are nonsplitting.

Lemma 2.0.5. *Let $d \geq 2$ be an integer, and let A be a $\mathbb{Z}_\ell$-moodule with a $\langle \zeta_d \rangle \cong \mathbb{Z}/d\mathbb{Z}$-action where ℓ is a prime that does not divide d. Suppose that A^{ζ_d} is trivial. For any fixed integer k that is relatively prime to d, the conjugacy class c of elements $A \rtimes \langle \zeta_d \rangle$ of the form (a, ζ_d^k) is non-splitting.*

Proof. Say that H is a subgroup of $A \rtimes \langle \zeta_d \rangle$ such that $c \cap H \neq \emptyset$. We want to show that $c \cap H$ is a conjugacy class of H. Suppose that $(a_2, \zeta_d^k), (a_3, \zeta_d^k) \in H$. We will

show that these two elements are related by some $(a,1) \in H$. In particular, H has $(a_2,\zeta_d^k)(a_3,\zeta_d^k)^{-1} = (a_2-a_3,1)$. Moreover, write $\sum_{i=0}^{d-1} b_i\zeta_d^i$ for the multiplicative inverse of $1-\zeta_d$ in $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1}+\cdots+1)$. Since k is relatively prime to d, H has an element of the form (α_i,ζ_d^i) for every i. Therefore, H has elements

$$(\alpha_i,\zeta_d^i)\cdot(a_2-a_3,1)\cdot(\alpha_i,\zeta_d^i)^{-1} = (\zeta_d^i(a_2-a_3),1)$$

and hence H has the b_i-th power of these elements, namely $(b_i\zeta_d^i(a_2-a_3),1)$. Let $a = \sum_{i=0}^{d-1} b_i\zeta_d^i(a_2-a_3)$ so that $(a,1)\in H$ and so that

$$(a,1)(a_2,\zeta_d^k)(a,1)^{-1} = (a(1-\zeta_d^k)+a_2,\zeta_d^k) = ((a_2-a_3)+a_2,1) = (a_3,1)$$

as desired. □

Lemma 2.0.6. *Let $d \geq 2$ be an integer, and let A be a nontrivial $\mathbb{Z}_\ell$-module with a $\langle\zeta_d\rangle \cong \mathbb{Z}/d\mathbb{Z}$-action where ℓ is a prime that does not divide d. Suppose that the induced action of ζ_d on $A/\ell A$ does not have an eigenvalue of 1 and has a primitive dth root of unity in $\overline{\mathbb{F}}_\ell$ as an eigenvalue. The group $A \rtimes \langle\zeta_d\rangle$ is center free.*

Proof. By Lemma 2.0.1(3), we have

$$(a_1,\zeta_d^{k_1})\cdot(a_2,\zeta_d^{k_2})\cdot(a_1,\zeta_d^{k_1})^{-1} = (a_1+\zeta_d^{k_1}a_2-\zeta_d^{k_2}a_1,\zeta_d^{k_2}).$$

Given $(a_1,\zeta_d^{k_1}) \in A\rtimes\langle\zeta_d\rangle$ that is not the identity element $(0,1)$, it suffices to show that there is some $(a_2,\zeta_d^{k_2}) \in A\rtimes\langle\zeta_d\rangle$ such that $a_2 \neq a_1+\zeta_d^{k_1}a_2-\zeta_d^{k_2}a_1$, i.e. that $a_2(1-\zeta_d^{k_1}) \neq a_1(1-\zeta_d^{k_2})$.

If $k_1 = 0$, then this non-equality is equivalent to $0 \neq a_1(1-\zeta_d^{k_2})$. Note that $a_1(1-\zeta_d) = 0$ would imply that $a_1 = 0$ by Corollary 2.0.3 which is not the case because $(a_1,\zeta_d^{k_1})$ is assumed to not be the identity element. Therefore, letting $k_2 = 1$ suffices.

If $k_1 \neq 0$, then choose $a_2 \in A$ to be a lift of an element of $A/\ell A$ belonging to the sum of the eigenspaces (over $\overline{\mathbb{F}}_\ell$ whose eigenvalues are the primitive dth roots of unity. In

particular, $a_2(1-\zeta_d^{k_1}) \neq 0$. It now suffices to let $k_2 = 0$. $\square$

Remark 2.0.7. Let d and ℓ be distinct prime numbers. Any nontrivial $\mathbb{Z}_\ell$-module A with a $\langle \zeta_d \rangle$-action whose ζ_d-invariant subgroup is trivial must have a primitive dth root of unity on $\overline{\mathbb{F}}_\ell$ as an eigenvalue, thereby satisfying the hypotheses in Lemma 2.0.6.

Chapter 3

Monodromy types of G-covers of stable genus 0-curves

In this section, we relate various ways to define monodromy of G-covers of stable genus 0-curves for finite groups G.

3.1 Definitions

Definition 3.1.1 (cf. [15, Section 7.1, 7.3], [13, Proof of Proposition 2.1], [25, Section 11.1])**.** A *curve over a scheme* S is a proper morphism $C \to S$ whose geometric fibers are connected and 1-dimensional. A *cover of a curve* $C \to S$ is a finite, flat, and surjective morphism $Y \to C$ of S-schemes from a curve $Y \to S$. Such a cover is *tame* if the ramification index at every point is prime to the characteristic of the residue field at the point. For a cover $f : Y \to C$, let $\mathrm{Aut}(f)$ be the automorphism group of $f : Y \to C$. Such a cover f is *Galois* if f is separable and if $\mathrm{Aut}\, f$ acts transitively on fibers of geometric points of C. Given a tame Galois cover $f : Y \to C$, its *branch locus* D is the reduced divisor of C such that $D \to S$ is étale, and f is étale over $C - D$, and $C - D$ is the maximal with these properties. If there is some constant n such that the geometric fibers of $D \to S$ are all of degree n, then f is said to have n *branch points*. Such a constant exists whenever S is connected.

In the case that $S = \operatorname{Spec} k$, given a finite group G and a conjugacy closed subset c of $G \setminus \{e\}$, a *tame G-cover of $\mathbb{P}^1$ consists of*

- *a tamely ramified finite Galois cover $f : C \to \mathbb{P}^1$ where C/k is a smooth proper geometrically connected curve, and*
- *an isomorphism $\phi : G \to \operatorname{Aut}(f)$.*

We will often only write $f : C \to \mathbb{P}^1$ when referring to the tame G-cover of $\mathbb{P}^1$ whilst leaving ϕ implicit.

More generally, we can consider labeled admissible stable G-covers of curves. We generalize the definitions in [2, Section 2.1], which considers the case where the group G is a cyclic group of prime order.

Definition 3.1.2 (cf. [2, Section 2.1], [11, Definition 1.2])**.** Let $G = \mathbb{Z}/d\mathbb{Z}$ and let S be an irreducible scheme over $\operatorname{Spec} \mathbb{Z}[1/d, \zeta_d]$. Let k be an algebraically closed field equipped with a ring morphism $\mathbb{Z}[1/d, \zeta_d] \to k$.

A *semi-stable curve* $\psi : C \to S$ is a flat and proper morphism whose geometric fibers are connected, reduced curves whose only singularities are ordinary double points. Given a point s of S, let C_s denote the fiber of C over s. Let $\operatorname{Sing}_S(C)$ denote the set of $z \in C$ such that z is a singular point on the fiber $C_{\psi(z)}$.

A *mark* Ξ on C/S is a closed subscheme of $C - \operatorname{Sing}_S(C)$ which is finite and étale over S. The *degree* of Ξ is the number of points in any geometric fiber of $\Xi \to S$. Given a semi-stable curve $\psi : C \to S$ and a mark Ξ on C/S, the pair $(C/S, \Xi)$ is called a *marked semi-stable curve*. Furthermore, $(C/S, \Xi)$ is a *stably marked semi-stable curve* if every irreducible component in every geometric fiber of C has at least three points which are either in $\operatorname{Sing}_S(C)$ or in Ξ. We say that a mark Ξ has a labeling if Ξ is an ordered disjoint union of sections $S \to C$. In this case, a *labeling* of the mark Ξ is denoted by $\eta : \{1, \ldots, r\} \to \Xi$ where r is the degree of Ξ.

Let G be a finite group. Given a G-action $\iota_0 : G \hookrightarrow \operatorname{Aut}_S(C)$ on C/S, let R denote the ramification locus of the cover $C \to C/\iota_0(G)$, and let $R_{\mathrm{sm}} = R - (R \cap \operatorname{Sing}_S(C))$ be the

smooth ramification locus. The pair $(C/S, \iota_0)$ is a *stable G-curve* if C/S is a semi-stable curve, R_{sm} is a mark on C/S, and $(C/S, R_{\mathrm{sm}})$ is stably marked.

Given a stable G-curve $(C/S, \iota_0)$, and a geometric point z of $R \cap \mathrm{Sing}_S(C)$, let $C_{z,1}$ and $C_{z,2}$ be the two components of the formal completion of $C_{\psi(z)}$. We say that $(C/S, \iota_0)$ is *admissible* if, for every geometric point $z \in R \cap \mathrm{Sing}_S(C)$, $\iota_0(1)$ stabilizes each branch $C_{z,i}$ and the characters of the action of ι_0 on the tangent spaces of $C_{z,1}$ and $C_{z,2}$ at z are inverses. A *labeling* of an admissible stable G-curve $(C/S, \iota_0)$ is a labeling η of R_{sm}. Note that a labeling η of an admissible stable G-curve $(C/S, \iota_0)$ induces a labeling $\eta_0 : \{1, \ldots, r\} \to B_{\mathrm{sm}}$ on the quotient $C/\iota_0(G)$ where B_{sm} is the smooth branch locus of the covering $C \to C/\iota_0(G)$.

Let s be a geometric point of S with residue field k, and let a be a point of the fiber $R_{\mathrm{sm},s}$. In particular, G acts on the tangent space of C_s at a via a character $\chi_a : G \to k^\times$. In the case that $G = \mathbb{Z}/d\mathbb{Z}$ where $d \geq 2$ is an integer, there is a unique choice of $\gamma_a \in G \backslash \{0\}$ so that $\chi_a(1) = \zeta_d^{\gamma_a}$. This value of γ_a is called the *canonical generator of inertia at a*. Given a labeled admissible stable G-curve $(C/S, \iota_0, \eta)$, where $G = \mathbb{Z}/d\mathbb{Z}$, its *class vector* is the set map $\gamma : \{1, \ldots, r\} \to G \backslash \{0\}$ given by $\gamma(i) = \gamma_{\eta(i)}$. We often write $\gamma = (\gamma(1), \ldots, \gamma(r))$.

We are mostly concerned with admissible stable G-curves $(C/S, \iota_0)$ such that $G = \mathbb{Z}/d\mathbb{Z}$ the quotient $C/\iota_0(G)$ has (arithmetic) genus 0. In this case, $C/\iota_0(G)$ is a stably marked curve by [11, Proposition 1.4].

Using conventions in [46, Sections 5.1, 5.2], we define monodromy types of tame G-covers of $\mathbb{P}^1$.

Definition 3.1.3. Let k be a field. Given an indeterminate z, the *Puiseaux series field* $k((z^{1/\infty}))$ is the field extension of the Laurent series field $k((z))$ generated by $z^{1/m}$ for m relatively prime to $\mathrm{char}\, k$.

When $k = \bar{k}$, $k((z^{1/\infty}))$ is the maximal prime-to-$(\mathrm{char}\, k)$ extension of $k((z))$. In this case, there is an isomorphism

$$\mathrm{Gal}(k((z^{1/\infty}))/k((z))) \simeq \hat{\mathbb{Z}}(1)_k \tag{3.1.1}$$

given by $\sigma \mapsto \{\sigma_m\}$ where $\hat{\mathbb{Z}}(1)_k = \varprojlim_m \mu_m(k)$ and $\sigma_m = \frac{\sigma(z^{1/m})}{z^{1/m}}$.

Let k be an algebraically closed field. For $t_0 \in k$, write $z = t - t_0$. Given any Galois prime-to-(char k) extension L of $k(t) = k(z)$, there is a $\mathrm{Gal}(L/k(t))$-conjugacy class of homomorphisms $\mathrm{Gal}(k((z^{1/\infty}))/k((z))) \to \mathrm{Gal}(L/k(t))$ which correspond to the $k(t)$-field injections $L \to k((z^{1/\infty}))$. Composing such a homomorphism with the isomorphism (3.1.1) yields the homomorphism

$$r_{t_0,Q} : \hat{\mathbb{Z}}(1)_k \to \mathrm{Gal}(L/k(t))$$

whose image is an inertia group $I(Q|P) \subseteq \mathrm{Gal}(L/k(t))$ for a place (more precisely, a system of places of finite Galois prime-to-(char k)-extensions of $k(t)$) Q of L above the place P of $k(t)$ corresponding to t_0. In particular, the $\mathrm{Gal}(L/k(t))$-conjugacy class of $r_{t_0,Q}$ is independent of the choice of $k(t)$-embedding $L \to k((z^{1/\infty}))$. Let r_{t_0} denote this conjugacy class.

Moreover, choosing some base point $*$ for $\mathbb{P}^1_k$ and letting $U \subseteq \mathbb{P}^1_k$ be an open subset containing $*$[1], Let $\pi_1^t(U,*)$ be the tamely ramified fundamental group of U (see [16, Exposé XIII, 2.1.3] for a more detailed discussion). Let $L = L^{\max}$ be the maximal prime-to-(char k)-extension of $k(t)$ unramified at points of U so that $\pi_1^t(U,*) \cong \mathrm{Gal}(L^{\max}/k(t))$. Let $t_1, \ldots, t_n$ be the k-points of $\mathbb{P}^1 - U$. By Grothendieck's comparison of étale and topological fundamental groups [16, Exposé XIII, Corollaire 2.12], there exist elements $\gamma_1, \ldots, \gamma_n \in \pi_1^t(U, \infty)$ such that

- $\gamma_1 \cdots \gamma_n = 1$,
- γ_i topologically generates an inertia group at t_i, i.e. $\gamma_i = r_{t_i,Q}(\zeta_i)$ for some topological generators $\zeta_i \in \hat{\mathbb{Z}}(1)_k$ and some Q above t_i, and
- $\gamma_1, \ldots, \gamma_{n-1}$ freely generate $\pi_1^t(U,*)$ as a profinite group.

[1] [46, Section 5.2] specified ∞ to be the base point of $\mathbb{P}^1$, but we do not make the same specification here as we study covers of $\mathbb{P}^1$ that are possibly branched at ∞

In fact, the condition $\gamma_1 \cdots \gamma_n = 1$ applied to the extension

$$k\left(t,\ \sqrt[m]{(t-t_1)/(t-t_2)},\ \sqrt[m]{(t-t_2)/(t-t_3)},\cdots,\ \sqrt[m]{(t-t_n)/(t-t_1)}\right)$$

of $k(t)$ shows that the ζ_i are all equal, say to some $\zeta \in \hat{\mathbb{Z}}(1)_k$. We refer to $\gamma_1, \ldots, \gamma_n$ and ζ as *generator data for* U.

Definition 3.1.4 (cf. [15, Section 7.3], [13, Proof of Proposition 2.1])**.** Let k be a field, let G be a finite group with $\operatorname{char} k \nmid |G|$, and let $f : C \to \mathbb{P}^1$ be a tamely ramified G-cover over k equipped with an isomorphism $\phi : G \to \operatorname{Aut}(f) \cong \operatorname{Gal}(L/k(t))$ where L is the G-extension of $k(t)$ corresponding to C. Let $U \in \mathbb{P}^1_{\bar{k}}$ be the unbranched locus of f and let $t_1, \ldots, t_n$ be the points of $\mathbb{P}^1_{\bar{k}} \backslash U$. Choose generator data $\gamma_1, \ldots, \gamma_n \in \pi_1^t(U, \infty)$ and $\zeta \in \hat{\mathbb{Z}}(1)_{\bar{k}}$ for U as above.

Let $c \subseteq G$ be closed under conjugation. We say that *the monodromy type (with respect to the choice of generator data) of f at/above t_i is c* if the image of γ_i under the surjection $\pi_1^t(U, *) \twoheadrightarrow \operatorname{Aut}(f) \xrightarrow{\phi^{-1}} G$ given by the covering $f : C_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ is an element of c. If $P \in \mathbb{P}^1_{\bar{k}}$ is not a branched point of f, then we say that *the monodromy type of f at/above P is trivial or is* $1 \in G$. Furthermore, we say that f has *monodromy type c (with respect to the choice of generator data)* if all finite branch points P of f have monodromy type c.

Remark 3.1.5. The notion of f having monodromy of type c does not specify whether ∞ is a branch point of f and what the monodromy type above $\infty \in \mathbb{P}^1$ is. We use this convention to later consider in Chapter 6 moduli of G-covers of $\mathbb{P}^1$ with monodromy of a fixed type (away from ∞).

Remark 3.1.6. Monodromy types as defined above generally depend on the choice of the generator data $\gamma_1, \ldots, \gamma_n \in \pi_1^t(U, \infty)$ and $\zeta \in \hat{\mathbb{Z}}(1)_{\bar{k}}$. A different choice of generator data replaces c with $c^\alpha := \{g^\alpha : g \in c\}$ for some α. By symmetry, there must be some β such that $c = (c^\alpha)^\beta$. When discussing monodromy types, we leave the choice of generator data implicit. In the case of interest, we let G be $A \rtimes \langle \zeta_d \rangle$ where A is a finite ℓ-group such that $A^{\langle \zeta_d \rangle} \neq 1$, we let $c = c_k$ be $\{(a, \zeta_d^k) : a \in A\}$, which is a non-splitting conjugacy class

by Lemma 2.0.5, where k is a fixed integer that is relatively prime to d, and we consider G-covers of $\mathbb{P}^1$ with monodromy type c. Changing the choice of generator data in this case changes the monodromy type from c_k to some $c_{k'}$ for some k' that is also relatively prime to d. In fact, there is a choice of monodromy data, obtained by replacing ζ if necessary, that makes the monodromy types of the covers into c_1.

Proposition 3.1.7 establishes that monodromy types respect subcovers when G is a semi-direct product.

Proposition 3.1.7. *Let k be a field. Let Γ, H be finite groups with Γ acting on H and such that $\operatorname{char} k \nmid |\Gamma|, |H|$ and let $H \rtimes \Gamma$ be the semidirect product with respect to this action. Let $f : C \to \mathbb{P}^1_k$ be a tame $(H \rtimes \Gamma)$-cover of smooth curves over a field k. In particular, f factors as tame Galois covers $C \to C/H$ and $g : C/H \to \mathbb{P}^1_k$ of smooth curves over k; the former cover is an H-cover and the latter is a Γ-cover. Fix some generator data $\gamma_1, \ldots, \gamma_n \in \pi_1^t(U_f, \infty)$ and $\zeta \in \hat{\mathbb{Z}}(1)_{\bar{k}}$ for the unbranched locus U_f of f in $\mathbb{P}^1_{\bar{k}}$.*

1. *If $t_{i_1}, \ldots, t_{i_m}$ are the branched points of g, then the images of $\gamma_{i_1}, \ldots, \gamma_{i_m}$ under the natural surjection $\pi : \pi_1^t(U_f, *) \to \pi_1^t(U_g, *)$ and ζ form generator data for the unbranched locus U_g of g in $\mathbb{P}^1_{\bar{k}}$.*

2. *Write $i_f(P)$ and $i_g(P)$ for the monodromy types of f and g above $P \in \mathbb{P}^1_{\bar{k}}$ with respect to the above generator data; these are conjugacy classes in $H \rtimes \Gamma$ and Γ respectively. The image of $i_f(P)$ in Γ is $i_g(P)$.*

Proof. 1. $\pi(\gamma_i)$ is trivial whenever $i \notin \{i_1, \ldots, i_m\}$, so $\gamma_{i_1} \cdots \gamma_{i_m} = 1$. Moreover, γ_{i_j} is a topological generator of an inertia subgroup of $\pi_1^t(U_f, *)$ at t_{i_j}, so its image under the natural surjection is a topological generator of an inertia subgroup of $\pi_1^t(U_g, *)$ at t_{i_j}. Lastly, under the comparison of étale and topological fundamental groups [16, Exposé XIII, Corollaire 2.12] (see also [16, Exposé XII, Corollarie 5.2]), one sees that $\gamma_{i_1}, \ldots, \gamma_{i_m}$ freely generate $\pi_1^t(U_g, *)$ as a profinite group.

2. If P is unbranched for f, then $i_f(P)$ and $i_g(P)$ are both trivial. Otherwise, $i_f(P)$ is the $(H \rtimes \Gamma)$-conjugacy class of the image of γ_i under the surjection $\pi_1^t(U_f, *) \to$

$H \rtimes \Gamma$ given by f, where P is identified with $t = t_i$. If P is branched for g in this case, then $i_g(P)$ is the H-conjugacy class of the image of $\pi(\gamma_i)$ under the surjection $\pi_1^t(U_g, *) \to H$ given by g. This coincides with the image of γ_i under the composition $\pi_1^t(U_f, *) \to H \rtimes \Gamma \to H$. If P is unbranched for g instead, then $i_g(P)$ is trivial by definition. Moreover, $\pi(i_f(P))$ is the image of γ_i under the composition $\pi_1^t(U_f, *) \to H \rtimes \Gamma \to H$, which equals the composition $\pi_1^t(U_f, *) \xrightarrow{\pi} \pi_1^t(U_g, *) \to H$. Thus, $\pi(i_f(P))$ is trivial. In any case, the image of $i_f(P)$ in Γ is $i_g(P)$.

□

The ramification behavior above points can be calculated from the monodromy types.

Proposition 3.1.8. *Let $f : C \to \mathbb{P}^1_k$ be a tame G-cover of smooth curves over a field k where* $\operatorname{char} k \nmid |G|$. *Given a closed point $P \in \mathbb{P}^1_k$ and a point $Q \in C$ such that $f(P) = Q$, the ramification index of Q over P equals the order of the monodromy type of f at Q.*

Proof. It suffices to prove this when k is algebraically closed. The ramification index of Q over P equals $\#I(Q|P) \cdot [\kappa(Q) : \kappa(P)]_i$ where $I(Q|P)$ is the inertia group of Q over P and $[\kappa(Q) : \kappa(P)]_i$ is the inseparable degree of the residue field at Q over the residue field at P (see, for example, [39, Corollary 7.10]). Since $\operatorname{char} k \nmid |G|$, the inseparable degree is 1. Moreover, $I(Q|P)$ is generated by the monodromy type of f at Q (with respect to a chosen generator of $\hat{\mathbb{Z}}(1)_k$ and isomorphism $\operatorname{Aut} f \cong G$). Therefore, the ramification index of Q over P equals the order of this monodromy type. □

The moduli of G-covers of $\mathbb{P}^1$ parameterizing monodromy types in c discussed later in Chapter 6 will be rational over the base finite field $\mathbb{F}_q$ as long as c is rational as below:

Definition 3.1.9. Let G be a finite group and c be a union of conjugacy classes in G. We say that c is *rational* if c is closed under the assignment $x \mapsto x^N$ for all N relatively prime to G. Similarly, given a prime power q, we say that c is $\mathbb{F}_q$*-rational* if c is closed under the assignment $x \mapsto x^q$.

3.2 Monodromy for Kummer extensions of $\mathbb{P}^1$

Let $G = \mathbb{Z}/d\mathbb{Z}$ for an integer $d \geq 2$, and suppose that k is a field with primitive dth-roots of unity. By Kummer theory, $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{F}_q(t)$ are of the form $\mathbb{F}_q(t)[y]/(y^d - f(t))$ where $f(t) \in \mathbb{F}_q(t)$. Equivalently, the $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1_{\mathbb{F}_q}$ are smooth completions of the curve given by $y^d = f(t)$ and in fact these covers are tame. We can take $f(t) \in \mathbb{F}_q[t]$ to be a polynomial without any dth or higher power factors. In this subsection, we describe monodromy types for such $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1$.

Lemma 3.2.1. *Let k be a field, let $d \geq 2$ be an integer not divisible by* $\operatorname{char} k$*, and let $f : C \to \mathbb{P}^1_k$ be the covering map from the smooth completion C of the affine plane curve C_A given by $y^d = f(t)$ where $f(t) \in k(t)$. Assume that C is geometrically connected. Without loss of generality, say that $f(t)$ is a polynomial without any dth or higher power factors. Write $f(t) = a\prod_{i=1}^n f_i(t)^{e_i}$ where $a \in k^\times$ and $f_i(t)$ are monic irreducible polynomials. For each i, C has exactly* $\gcd(d, e_i)$ *distinct points over the vanishing locus of $f_i(t)$ in $\mathbb{P}^1_k$. Moreover, C has exactly* $\gcd(d, \deg f)$ *distinct points over ∞. Furthermore, the rational function y on C*

1. *has vanishing order $\frac{e_i}{\gcd(d,e_i)}$ at each of the points above the vanishing point of $f_i(t)$ in $\mathbb{P}^1_k$,*
2. *has poles of order $\frac{\deg f}{\gcd(d,\deg f)}$ at the normalizations at the points above ∞, and*
3. *does not vanish and does not have a pole at other points on C.*

Moreover, f is branched above ∞ if and only if $\deg f \not\equiv 0 \pmod d$.

Proof. It suffices to demonstrate these results in the case that k is algebraically closed. In this case, $f_i(t)$ can be written as $t - t_i$ where $t_i \in k$. For each j, let f_j be a positive integer such that $e_j f_j \equiv \gcd(d, e_j) \pmod d$; write $e_j f_j = \gcd(d, e_j) + dk_j$. For each j, the equality $y^d = f(t) = a(t - t_j)^{e_j}\prod_{i\neq j}(t - t_i)^{e_i}$ of rational functions of C is equivalent to

$$y_{j,1}^d = a^{f_j}(t - t_j)^{\gcd(d,e_j)}\prod_{i\neq j}(t - t_i)^{e_i}$$

where $y_{j,1} = \frac{y^{f_j}}{(t-t_j)^{k_j}}$. In turn, this equation is equivalent to

$$y_{j,2}^{\gcd(d,e_j)} = a^{f_j} \prod_{i \neq j} (t - t_i)^{e_i} \tag{3.2.1}$$

where $y_{j,2} = \frac{y_{j,1}^{d/\gcd(d,e_j)}}{t-t_j}$. The affine curve given by the equation (3.2.1) has $\gcd(d, e_j)$ smooth points above $t = t_j$. At each of these smooth points Q, the rational function $t - t_j$ vanishes, so $y_{j,1}$ also vanishes because $y_{j,2} = \frac{y_{j,1}^{d/\gcd(d,e_j)}}{t-t_j}$. In particular, the vanishing order of $t - t_j$ at Q is a multiple of $\frac{d}{\gcd(d,e_j)}$. This vanishing order equals the ramification index of Q, and the sum of the ramification indices of the smooth points above $t = t_j$ must be exactly d, so in fact these smooth points Q are exactly the points of C above $t = t_j$, the function $y_{j,1}$ is a uniformizer at each Q, and $t - t_j$ vanishes with order exactly $\frac{d}{\gcd(d,e_j)}$.

Since $y_{j,1} = \frac{y^{f_j}}{(t-t_j)^{k_j}}$, the vanishing order of y^{f_j} at each of these Q is exactly $1 + \frac{dk_j}{\gcd(d,e_j)} = \frac{e_j f_j}{\gcd(d,e_j)}$. Thus, the vanishing order of y at these Q is $\frac{e_j}{\gcd(d,e_j)}$.

Note that the affine curve given by $y^d = f(t)$ is smooth at the points that are not above $t = t_i$ and not above ∞. Therefore, such points are points of C. Moreover, y does not vanish and does not have poles at such points because $f(t)$ does not vanish and does not have poles away from $t = t_i$ and $t = \infty$.

To prove (3), write $s = \frac{1}{t}$ so that $t = \infty$ corresponds to $s = 0$. The equation $y^d = f(t)$ is equivalent to

$$\begin{aligned} y^d &= f\left(\frac{1}{s}\right) \\ (s^{\lceil \frac{\deg f}{d} \rceil} y)^d &= s^{d\lceil \frac{\deg f}{d} \rceil} f\left(\frac{1}{s}\right). \end{aligned} \tag{3.2.2}$$

Note that $s^{d\lceil \frac{\deg f}{d} \rceil} f\left(\frac{1}{s}\right)$ is a polynomial in s of degree $d\lceil \frac{\deg f}{d} \rceil$, and has exactly $d\lceil \frac{\deg f}{d} \rceil - \deg f$ factors of s. Part (1) shows that C has exactly $\gcd(d, d\lceil \frac{\deg f}{d} \rceil - \deg f) = \gcd(d, \deg f)$ distinct points over $t = \infty$. Moreover, the rational function $s^{\lceil \frac{\deg f}{d} \rceil} y$ vanishes with order exactly $\frac{d\lceil \frac{\deg f}{d} \rceil - \deg f}{\gcd(d, \deg f)}$ above each point over $s = 0$. As a rational function of C, the proof of part (1) above establishes that s vanishes at each point over $s = 0$ with order $\frac{d}{\gcd(d, \deg f)}$.

Therefore, the vanishing order of y at each of these points is $-\frac{\deg f}{\gcd(d,\deg f)}$. In other words, y has a pole of order $\frac{\deg f}{\gcd(d,\deg f)}$ at each of these points.

□

Proposition 3.2.2. *Let $d \geq 2$ be an integer. Let k be a field such that $\operatorname{char} k \nmid d$ and let $\varphi : C \to \mathbb{P}^1_k$ be a tame $\mathbb{Z}/d\mathbb{Z}$-cover over k. Let $\zeta = (\zeta_m)_m \in \hat{\mathbb{Z}}(1)_{\bar{k}}$ and $\gamma_1, \ldots, \gamma_n \in \pi_1^t(U, *)$ be a choice of generator data for U, where $U \subseteq \mathbb{P}^1_{\bar{k}}$ is the complement of the branch locus of $\varphi \times_k \bar{k}$. After base changing to an extension k_d of k with a primitive dth-root of unity, say that C is given by the smooth completion of the affine plane curve given by $y^d = f(t)$ where $f(t) \in k_d[t]$ is a polynomial without any dth or higher power factors. After this base change, further say that $\phi : \mathbb{Z}/d\mathbb{Z} \to \operatorname{Aut}(\varphi)$ is chosen to send $1 \in \mathbb{Z}/d\mathbb{Z}$ to the automorphism of C given by $(x, y) \mapsto (x, \zeta_d y)$. Write $f(t) = a\prod_{i=1}^n f_i(t)^{e_i}$ where $a \in k_d^\times$, $f_i(t)$ are monic irreducible polynomials, and $1 \leq e_i \leq d-1$. The monodromy type of C above the vanishing point of $f_i(t)$ in $\mathbb{P}^1_k$ is $e_i \in \mathbb{Z}/d\mathbb{Z}$, and the monodromy type of C above $\infty \in \mathbb{P}^1_k$ is $-\deg f$.*

Proof. It suffices to demonstrate the desired results in the case that k is algebraically closed. In this case, write $z_i = f_i(t) = t - t_{0,i}$ for $t_{0,i} \in k$ and let $P \in \mathbb{P}^1_k$ be the (finite) point corresponding to $t_{0,i}$. Writing $L = k(t)[y]/(y^d - f(t))$ for the function field of C, consider any $k(t)$-embedding $\iota : k(t)[y]/(y^d - f(t)) \hookrightarrow k((z_i^{1/\infty}))$ — such an embedding is given by sending y to $a^{1/m}(t-t_{0,i})^{\frac{e_i}{d}} \cdot w$ where $a^{1/m}$ is any choice of dth root of a in $k = \bar{k}$, and w is any choice of dth root of $\prod_{j\neq i}(t-t_{0,j})^{e_j}$ in $k((z))$. Under the isomorphism (3.1.1), ζ corresponds to the element of $\sigma : \operatorname{Gal}(k((z_i^{1/\infty}))/k((z_i)))$ given by $z_i^{1/m} \mapsto \zeta_m z_i^{1/m}$. In turn, σ sends $a^{1/m}(t-t_{0,i})^{\frac{e_i}{d}} \cdot w$ to $a^{1/m}(\zeta_d)^{e_i}(t-t_{0,i})^{\frac{e_i}{d}} \cdot w = \zeta_d^{e_i}(t-t_{0,i})^{\frac{e_i}{d}} \cdot w$. In other words, the homomorphism $\operatorname{Gal}(k((z_i^{1/\infty}))/k((z_i))) \to \operatorname{Gal}(L/k(t)) \cong \operatorname{Aut} f$ corresponding to ι is given by sending σ to the $k(t)$ automorphism given by sending y to $\zeta_d^{e_i} y$. Under ϕ, this automorphism corresponds to $e_i \in \mathbb{Z}/d\mathbb{Z}$. Therefore, the composition

$$\hat{\mathbb{Z}}(1)_k \xrightarrow{\cong} \mathrm{Gal}(k((z^{1/\infty}))/k((z))) \longrightarrow \mathrm{Gal}(L^{\max}/k(t)) \xrightarrow{\cong} \pi_1^t(U,*)$$

$$\twoheadrightarrow \mathrm{Gal}(L/k(t)) \xrightarrow{\cong} \mathrm{Aut}(f) \xrightarrow{\phi^{-1}} \mathbb{Z}/d\mathbb{Z}$$

sends ζ to $e_i \in \mathbb{Z}/d\mathbb{Z}$. Within the above series of maps, ζ is sent to γ_i in $\pi_1^t(U,*)$, so the monodromy type of f above $t = t_i$ is $e_i \in \mathbb{Z}/d\mathbb{Z}$.

Let $s = \frac{1}{t}$ to see, as in equation (3.2.2) to see that the monodromy type of f above $s = 0$ is $d\lceil \frac{\deg f}{\deg d} \rceil - \deg f$, which is congruent to $-\deg f$ modulo d. Thus, the monodromy type of f above ∞ is $-\deg f$. □

Remark 3.2.3. The sum of the monodromy types above the branch points (counted with multiplicity) is 0 modulo d. This is a consequence of the relations on generators γ_i of the inertia groups at the branch points as discussed in Section 3.1.

Remark 3.2.4. In the situation of Proposition 3.2.2, changing the generator data and the choice of ϕ scales the monodromy types uniformly across the branch points. More precisely, if $(e_1, \ldots, e_n)$ is the n-tuple of monodromy types of f at the finite points $t = t_1, \ldots, t_n$, then the tuple becomes $(\alpha \cdot e_1, \ldots, \alpha \cdot e_n)$ after changing the generator data and/or ϕ for some $\alpha \in (\mathbb{Z}/d\mathbb{Z})^\times$. In other words, the tuple $(e_1, \ldots, e_n)$ is a well defined element of $\mathbb{P}^{n-1}(\mathbb{Z}/d\mathbb{Z})$ independent of the generator data and the choice of ϕ. This element of $\mathbb{P}^{n-1}(\mathbb{Z}/d\mathbb{Z})$ also coincides with the tuple $(e'_1, \ldots, e'_n)$ of canonical generators of inertia at $Q_1, \ldots, Q_n$ where Q_i is a choice of ramification point in C above $t = t_i$.

3.3 Imaginary cyclic extensions of $\mathbb{F}_q(t)$

Definition 3.3.1. We say that a finite extension of $k(t)$ is *imaginary* (resp. *totally imaginary*) if it is ramified (resp. totally ramified) above ∞.

We will focus on $\mathbb{Z}/d\mathbb{Z}$-extensions of $\mathbb{F}_q(t)$ in later chapters, particularly ones which are totally imaginary or not imaginary. The below proposition shows that totally imaginary

$\mathbb{Z}/d\mathbb{Z}$ extensions exist only when $q \equiv 1 \pmod{d}$ which is the case exactly when $\mathbb{F}_q$ has primitive dth roots of unity.

Proposition 3.3.2. *Let q be a prime power. Let $d \geq 2$ be an integer that is coprime to q. Suppose that L is a cyclic dth-power extension of $K = \mathbb{F}_q(t)$. Let $\mathfrak{q}$ be a place of L that lies over a place $\mathfrak{p}$ of K with ramification degree e. If the residue field of $\mathfrak{p}$ is isomorphic to $\mathbb{F}_{q^a}$, then $q^a \equiv 1 \pmod{e}$. In particular, if L is totally imaginary, then $q \equiv 1 \pmod{d}$, or equivalently, $\mathbb{F}_q$ has primitive dth roots of unity.*

Proof. Let $\hat{K}_\mathfrak{p}$ and $\hat{L}_\mathfrak{q}$ denote the completions of K and L with respect to $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Let $K_\mathfrak{p}^{\mathrm{unr}}$ be the maximal abelian unramified extension of $\hat{K}_\mathfrak{p}$, and let $K_\mathfrak{p}^{\mathrm{tr}}$ be the maximal tamely ramified extension of $\hat{K}_\mathfrak{p}$. The Galois group of $K_\mathfrak{p}^{\mathrm{tr}}$ over $K_\mathfrak{p}^{\mathrm{unr}}$ is isomorphic to $\Pi := \prod_{\substack{\ell \text{ prime} \\ \ell \nmid q}} \mathbb{Z}_\ell$ and the Galois group of $K_\mathfrak{p}^{\mathrm{unr}}$ over $\hat{K}_\mathfrak{p}$ is the cyclic group generated by $\mathrm{Frob}_\mathfrak{p}$. Therefore, the Galois group of $K_\mathfrak{p}^{\mathrm{tr}}$ over $K_\mathfrak{p}$ is the semidirect product $\Pi \rtimes \langle \mathrm{Frob}_\mathfrak{p} \rangle$, where $\mathrm{Frob}_\mathfrak{p}$ acts on Π by q^a.

Since d and q are coprime, $\mathfrak{q}$ is tamely ramified over $\mathfrak{p}$, so $\hat{L}_\mathfrak{q} \subseteq K_\mathfrak{p}^{\mathrm{tr}}$. Moreover, $\mathrm{Gal}(\hat{L}_\mathfrak{q}/\hat{K}_\mathfrak{p})$ is identified with the decomposition group $D(\mathfrak{q}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K) \cong \mathbb{Z}/d\mathbb{Z}$, and this decomposition group is of order ef, where f is the degree of $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$. Write $g = \frac{d}{ef}$ so that the natural restriction $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{tr}}/\hat{K}_\mathfrak{p}) \twoheadrightarrow \mathrm{Gal}(\hat{L}_\mathfrak{q}/\hat{K}_\mathfrak{p})$ is identified with a surjection

$$\tau : \Pi \rtimes \langle \mathrm{Frob}_\mathfrak{p} \rangle \twoheadrightarrow g\mathbb{Z}/d\mathbb{Z},$$

factoring through a composition $\Pi \cong \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{unr}}/\hat{K}_\mathfrak{p}) \twoheadrightarrow \mathrm{Gal}(\hat{L}_\mathfrak{q}/\hat{L}_\mathfrak{q} \cap K_\mathfrak{p}^{\mathrm{unr}}) \hookrightarrow \mathrm{Gal}(\hat{L}_\mathfrak{q}/\hat{K}_\mathfrak{p}) \cong g\mathbb{Z}/d\mathbb{Z}$. Note that $[\hat{L}_\mathfrak{q} \cap K_\mathfrak{p}^{\mathrm{unr}} : \hat{K}_\mathfrak{p}] = f$, so the image of Π in $\mathrm{Gal}(\hat{L}_\mathfrak{q}/\hat{K}_\mathfrak{p})$ is identified with $fg \in \mathbb{Z}/d\mathbb{Z}$.

Let $\gamma \in \Pi$ be an element such that $\tau(\gamma) = fg \in \mathbb{Z}/d\mathbb{Z}$. On the one hand, $\gamma^{\mathrm{Frob}_\mathfrak{p}} = q^a\gamma$, so $\tau(\gamma^{\mathrm{Frob}_\mathfrak{p}}) = q^a \cdot \tau(\gamma) = q^a \cdot fg \in \mathbb{Z}/d\mathbb{Z}$. On the other hand, $\tau(\gamma^{\mathrm{Frob}_\mathfrak{p}}) = \tau(\mathrm{Frob}_\mathfrak{p}) + \tau(\gamma) - \tau(\mathrm{Frob}_\mathfrak{p}) = \tau(\gamma) = fg$. Therefore, $q^a \cdot fg = fg$ in $\mathbb{Z}/d\mathbb{Z}$. Since the order of fg as an element of $\mathbb{Z}/d\mathbb{Z}$ is e, $q^a \equiv 1 \pmod{e}$.

□

Chapter 4

Hermitian Spaces over $\mathbb{Z}_\ell[\zeta_d]$

For an integer $d \geq 1$, let $\Phi_d(X) \in \mathbb{Z}[X]$ denote the dth-cyclotomic polynomial.

Notation 4.0.1. Given a commutative ring A and an integer $d \geq 2$, denote by $A[\zeta_d]_{\text{all}}$, $A[\zeta_d]_{\zeta_d \neq 1}$, $A[\zeta_d]_{\text{prim}}$ the A-algebras $A[X]/(X^d - 1)$, $A[X]/(\sum_{i=0}^{d-1} X^i)$, and $A[X]/(\Phi_d(X))$ respectively. Further let

$$A[\zeta_d]_{\zeta_d \neq -1} = \begin{cases} A[\zeta_d]_{\text{all}} & \text{if } 2 \nmid d \\ A[X]/\left(\frac{X^d-1}{X+1}\right) & \text{if } 2 \mid d \end{cases}$$

$$A[\zeta_d]_{\zeta_d \neq \pm 1} = \begin{cases} A[\zeta_d]_{\zeta_d \neq 1} & \text{if } 2 \nmid d \\ A[X]/\left(\frac{\sum_{i=0}^{d-1} X^i}{X+1}\right) & \text{if } 2 \mid d. \end{cases}$$

In particular, $A[\zeta_d]_{\zeta_d \neq -1}$ and $A[\zeta_d]_{\zeta_d \neq \pm 1}$ are quotients of $A[\zeta_d]_{\text{all}}$ and $A[\zeta_d]_{\zeta_d \neq 1}$ respectively. If in fact $A[\zeta_d] = A[\zeta_d]_{\text{all}}$ (resp. $A[\zeta_d] = A[\zeta_d]_{\zeta_d \neq 1}$) factorizes as $A[\zeta_d]_{\zeta_d \neq -1} \times A[X]/(X+1)$ (resp. $A[\zeta_d]_{\zeta_d \neq \pm 1} \times A[X]/(X+1)$), then let $\varepsilon_{A[\zeta_d]} \in A[\zeta_d]$ be the element corresponding to the pair $(1, -1)$ under the factorization.

When often simply refer to each of these algebras as $A[\zeta_d]$ and indicate which we are referring to, if distinctions are necessary, before we use this simplified notation in context. Note that Chapter 7 and Chapter 8 both let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq -1}$.

For any of these algebras $A[\zeta_d]$, note that $\zeta_d^d = 1$ and that $A[\zeta_d]$ has an involution

sending ζ_d to ζ_d^{-1}.

In this section, For prime numbers ℓ and integers $d \geq 2$ not divisible by ℓ, Proposition 4.1.1 induces Hermitian forms over $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ from the ℓ-adic Weil pairings on Jacobians of $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1$. We also prove Corollary 4.3.8, which concerns the theory of such Hermitian forms. Since d is not divisible by ℓ, $\mathbb{Z}_\ell[\zeta_d]_{\mathrm{all}}$ does not ramify over $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell[\zeta_d]_{\mathrm{all}} \cong \prod_{d'|d} \mathbb{Z}_\ell[\zeta_{d'}]_{\mathrm{prim}}$.

For a discussion of the theory of Hermitian forms over general involution rings, see [24].

Definition 4.0.2. Let R be a (not necessarily commutative) ring with an involution $\bar{\cdot} : R \to R$. The *opposite module* $\overline{M}$ of the left R-module M is the additive group M with the right R-module structure

$$mr = \overline{r}m$$

for all $r \in R$ and $m \in M$. The *dual module* $M^\vee$ of the right R-module M is the abelian group $\mathrm{Hom}_R(M, R)$ that is a left R-module under the action

$$(rf)(m) = rf(m)$$

for all $r \in R$ and $m \in M$. The *transpose module* M^* of an (right) R-module M is defined to be $\overline{M^\vee}$.

Definition 4.0.3 (cf. [24, Chapter I, 2.2, 3.1, 3.2])**.** Let R be a ring with an involution $\bar{\cdot} : R \to R$. Let ε be an element of the center of R such that $\varepsilon \cdot \overline{\varepsilon} = 1$. Let V be an R-module. A *Hermitian form* (or more precisely, an *ε-Hermitian form*) on V is a biadditive pairing $H : V \times V \to R$ such that

1. $H(av, bw) = \overline{a}H(v, w)b$ for all $v, w \in V$ and $a, b \in R$, and
2. $H(v, w) = \varepsilon\overline{H(w, v)}$ for all $v, w \in V$.

When V is a projective R-module, we say that (V, H) is a *Hermitian module*. When (V, H)

is a Hermitian module, H is said to be *nonsingular* if the adjoint map $V \to V^*, v \mapsto H(v,-)$ is an R-module isomorphism. In this case, (V,H) is said to be a *Hermitian space*.

A morphism $(V_1,H_1) \to (V_2,H_2)$ of Hermitian modules is an R-linear morphism $\varphi : V_1 \to V_2$ such that $H_2(\varphi(v),\varphi(w)) = H_1(v,w)$ for all $v,w \in V_1$.

Remark 4.0.4. It is common to use the opposite convention for sesquilinearity, i.e. it is common to define a Hermitian form H to satisfy $H(av,bw) = aH(v,w)\overline{b}$.

Remark 4.0.5. We mostly need the theory of $\varepsilon_{\mathbb{Z}_\ell[\zeta_d]}$-Hermitian forms where $\ell \nmid d$. As Lemma 4.0.8 shows, such Hermitian forms correspond to 1-Hermitian forms over factors D_i as in (4.1.10) where $\zeta_d \neq -1$ and to (-1)-Hermitian forms over $\mathbb{Z}_\ell[X]/(X+1)$ (occuring only when d is even). Since the involution on $\mathbb{Z}_\ell[X]/(X+1)$ is trivial, (-1)-Hermitian forms over it are skew-symmetric bilinear forms.

We will use some facts about orthogonality for Hermitian modules.

Definition 4.0.6 (cf. [24, Chapter I, 3.4, 3.6])**.** Let R be a ring with involution and let $\varepsilon \in R$ satisfy $\varepsilon \cdot \overline{\varepsilon} = 1$.

1. If (V_i,H_i) are ε-Hermitian-modules for $i = 1,2$, the *orthogonal sum* $(M_1,h_1) \perp (M_2,h_2)$ is defined as the Hermitian module

$$(M_1 \oplus M_2, H_1 \perp H_2)$$

where $H_1 \perp H_2$ is the Hermitian form uniquely characterized by

$$H(v,w) = \begin{cases} H_i(v,w) & \text{if } v,w \in V_i \\ 0 & \text{if } v \in V_1, w \in V_2 \end{cases}.$$

In particular,

$$H(v_1+v_2, w_1+w_1) = H_1(v_1,w_1) + H_2(v_2,w_2)$$

for all $v_1,w_1 \in V_1$ and $v_2,w_2 \in V_2$.

2. Two subsets $X \subset V$ and $Y \subset V$ of a Hermitian module (V, H) are *orthogonal* if $H(x, y) = 0$ for all $x \in X$ and $y \in Y$.

3. Given a submodule $U \subset V$ of a ε-Hermitian module (V, H), we define the *orthogonal complement* $U^{\perp}$ by

$$U^{\perp} = \{x \in V : H(x, u) = 0 \text{ for all } u \in U\}.$$

4. A ε-Hermitian module (V, H) over R is said to be *diagonalizable* if there exists a basis $v_1, \ldots, v_n$ of V such that the matrix of H with respect to $v_1, \ldots, v_n$ is diagonal, i.e. $H(v_i, v_j) = 0$ for all $i \neq j$. Such a basis is called an *orthogonal basis*. If $H(v_i, v_i) = 1$ for all i, then the orthogonal basis is called an *orthonormal basis*.

Lemma 4.0.7 ([24, Chapter I, Lemma 3.6.2])**.** *Let (V, H) be a Hermitian module.*

1. *Let U be a submodule of V which is finitely generated and projective. If $(U, H|_U)$ is nonsingular, then $(V, H) = (U, H|_U) \perp (U^{\perp}, H|_{U^{\perp}})$.*

2. *If $(V, H) \simeq (V_1, H_1) \perp (V_2, H_2)$ for some Hermitian modules (V_i, H_i) for $i = 1, 2$, then the H_i are nonsingular if and only if H is nonsingular.*

In the case of interest, $R = A[\zeta_d] = A[x]/(1+x+\cdots+x^{d-1})$, for a ring A and $\bar{\cdot} : R \to R$ is the A-algebra involution homomorphism given by $\zeta_d \mapsto \zeta_d^{-1}$. More specifically, we will apply the theory of Hermitian forms of $A[\zeta_d]$ in the case that $A = \mathbb{Z}_\ell$ — Corollary 4.3.8 is concerned with a $\mathbb{Z}_\ell[\zeta_d]$-module with a perfect symplectic pairing $\omega : V \times V \to \mathbb{Z}_\ell$ that is preserved by ζ_d, i.e. $\omega(\zeta_d v, \zeta_d w) = \omega(v, w)$ for all $v, w \in V$. We show that ω yields a nonsingular Hermitian form $H : V \times V \to \mathbb{Z}_\ell[\zeta_d]$ in Proposition 4.1.1. Before doing so, we first prove Lemma 4.0.8, which is convenient for understanding Hermitian forms over finite products of involution rings.

Lemma 4.0.8. *Let R be a ring with involution. Write $R \cong \prod_i D_i$ where the product is a finite product of involution rings, and the isomorphism is of involution rings. Hermitian modules over R correspond to tuples of Hermitian modules over D_i. More precisely, letting*

V be any R-module, writing V_i for the D_i-component of V, letting $\varepsilon_i \in D_i$ satisfy $\varepsilon_i\overline{\varepsilon_i} = 1$, and letting ϵ be the element of R whose D_i-component is ε_i, there is a bijection

$$\left\{ \begin{array}{l} \textit{Tuples } (H_i)_i \textit{ where} \\ H_i : V_i \times V_i \to D_i \\ \textit{are } \varepsilon_i\textit{-Hermitian forms} \end{array} \right\} \to \left\{ \begin{array}{l} \varepsilon\textit{-Hermitian forms} \\ H : V \times V \to R \end{array} \right\}$$

$$(H_i)_i \mapsto \perp_i H_i.$$

To discuss $\perp_i H_i$, note that we regard $H_i : V_i \times V_i \to D_i$ as a ε-Hermitian form over R via the injection $D_i \hookrightarrow \prod_i D_i \cong R$ sending an element $d_i \in D_i$ to the element of $\prod_i D_i$ whose ith component is d_i and whose other components are 0.

Furthermore, given that each V_i is a finitely generated and projective D_i-module (equivalently V is a finitely generated and projective R-module), the H_i are all nonsingular if and only if $\perp_i H_i$ is nonsingular.

Proof. It suffices to prove this in the case that $R \cong D_1 \times D_2$. We show that claimed bijection has an inverse map that is the map sending a Hermitian form $H : V \times V \to R$ to the pair $(H|_{V_1}, H|_{V_2})$.

Given a ε-Hermitian form $H : V \times V \to R$, note that $H|_{V_1} : V_1 \times V_1 \to R$ are respectively valued in D_1 respectively because

$$\begin{aligned} H|_{V_1}(v, w) &= H((1,0)v, (1,0)w) \\ &= \overline{(1,0)} \cdot (1,0)H(v,w) \\ &= (1,0) \cdot (1,0)H(v,w) \\ &= (1,0)H|_{V_1}(v,w) \end{aligned}$$

where $(1,0) \in D_1 \times D_2 \cong R$. In fact, $H|_{V_1}$ is a $(\varepsilon_1, 0)$-Hermitian form over R because

$$\begin{aligned} H|_{V_1}(v,w) &= H((1,0)v, (1,0)w) \\ &= (1,0)H((1,0)v,(1,0)w) \\ &= (1,0)\varepsilon\overline{H((1,0)w,(1,0)v)} \\ &= \varepsilon_1\overline{H|_{v_1}(w,v)}. \end{aligned}$$

Similarly, $H|_{V_2} : V_2 \times V_2 \to R$ is valued in D_2 and is a $(0, \varepsilon_2)$-Hermitian form over R. Moreover, $V \cong V_1 \oplus V_2$ as R-modules, and for any $v_1 \in V_1$ and $v_2 \in V_2$,

$$\begin{aligned} H(v_1,v_2) &= H((1,0)v_1,(0,1)v_2) \\ &= \overline{(1,0)} \cdot (0,1)H(v_1,v_2) \\ &= (1,0)\cdot(0,1)H(v_1,v_2) \\ &= 0, \end{aligned}$$

so $H = H|_{V_1} \perp H|_{V_2}$.

On the other hand, given $H_i : V_i \times V_i \to D_i$ we show that $H_i : V_i \times V_i \to D_i \hookrightarrow D_1 \times D_2 \cong R$ is a ε-Hermitian form over R. Given $a \in R$, let $a_i \in D_i$ be the D_i-component of a. For all $v, w \in V_i$,

$$\begin{aligned} H(v,w) &= \varepsilon_i\overline{H(w,v)} \\ &= \varepsilon\overline{H(w,v)}. \end{aligned}$$

For any $v, w \in V_i$ and $a, b \in R$, we then have

$$\begin{aligned} H_i(av,bw) &= H_i(a_iv, b_iw) \\ &= \overline{a_i}H_i(v,w)b_i \\ &= \overline{a}H_i(v,w)b, \end{aligned}$$

so H_i is indeed a Hermitian form over R. Note that $(H_1 \perp H_2)_{V_i} = H_i$, so the claimed inverse map is indeed the inverse map to the claimed bijection as desired. By Lemma 4.0.7, the H_i are all nonsingular if and only if $\perp_i H_i$ is nonsingular. □

4.1 Hermitian forms induced from the Weil pairing of a superelliptic curve

Proposition 4.1.1. *Let A be a commutative ring, let $d \geq 2$ be an integer, let $A[\zeta_d]$ be $A[\zeta_d]_{\zeta_d \neq 1}$ equipped with the A-algebra involution $\bar{\cdot} : \zeta_d \mapsto \zeta_d^{-1}$, and let V be an $A[\zeta_d]$-module. If d is even, then additionally assume that $d/2$ is a nonzerodivisor of A, that $A \cong A[\zeta_d]_{\zeta_d \neq \pm 1} \times A[X]/(X+1)$, and that $1 + \zeta_d$ is invertible in $A[\zeta_d]_{\zeta_d \neq \pm 1}$. Symplectic pairings over $A[\zeta_d]$ on V which are preserved by ζ_d functorially induce $\varepsilon_{A[\zeta_d]}$-Hermitian forms over $A[\zeta_d]$. More specifically, there exist natural maps*

$$\left\{ \begin{array}{c} \textit{Sympletic pairings} \\ \omega : V \times V \to A \\ \textit{preserved by } \zeta_d \end{array} \right\} \to \left\{ \begin{array}{c} \varepsilon_{A[\zeta_d]}\textit{-Hermitian forms} \\ H : V \times V \to A[\zeta_d] \end{array} \right\}$$

which are functorial in symplectic modules (V, ω) over A preserved by ζ_d and Hermitian forms (V, H) over $A[\zeta_d]$.

Moreover, there exist such natural maps that assign perfect symplectic pairings over A which are preserved by ζ_d to nonsingular Hermitian forms over $A[\zeta_d]$.

Proof. Let A' be $A[\zeta_d]$ if d is odd and $A[\zeta_d]_{\zeta_d \neq \pm 1}$ if d is even. Let V' be the A'-component of A and let $\omega' = \omega|_{V'}$. When d is even, let $V|_{\zeta_d = -1}$ be the $A[X]/(1+X)$-component of V and let $\omega|_{\zeta_d=-1}$ be the restriction of ω to $V|_{\zeta_d=-1}$.

We show that there exist $a_i \in \mathbb{Z}[\zeta_d]$ such that

$$H'(v, w) := \sum_{i=1}^{d-1} a_i \omega'(v, \zeta_d^i w)$$

is a 1-Hermitian form over A' for any symplectic module (V, ω) over A. Afterwards, let H be H' if d is odd, and let d be the $\varepsilon_{A[\zeta_d]}$-Hermitian form corresponding to H' on V' and to $\omega|_{\zeta_d=-1}$ on $V|_{\zeta_d=-1}$ via Lemma 4.0.8. Assigning (V, ω) to (V, H) then induces a functor from the category of symplectic modules over A that are preserved by ζ_d to the category of Hermitian forms.

On the one hand,

$$\begin{aligned} H'(v, \zeta_d w) &= \sum_{i=1}^{d-1} a_i \omega'(v, \zeta_d^{i+1} w) \\ &= \sum_{i=2}^{d-1} a_{i-1} \omega'(v, \zeta_d^{i} w) \\ &= -a_{d-2}\omega'(v, \zeta_d w) + \sum_{i=2}^{d-1} (a_{i-1} - a_{d-2})\omega'(v, \zeta_d^i w), \end{aligned}$$

and on the other hand,

$$H'(v, w)\zeta_d = \sum_{i=1}^{d-1} a_i \zeta_d \omega'(v, \zeta_d^i w),$$

so $H'(v, \zeta_d w) = H'(v, w)\zeta_d$ is equivalent to

$$a_1 \zeta_d = -a_{d-1} \tag{4.1.1}$$

$$a_i \zeta_d = a_{i-1} - a_{d-1} \qquad \text{for } 2 \le i \le d-1, \tag{4.1.2}$$

Also equivalently,

$$(a_1 : \cdots : a_{d-1}) = (1 : \zeta_d^{-1} + 1 : \zeta_d^{-2} + \zeta_d^{-1} + 1 : \cdots : \zeta_d^3 + \zeta_d^4 + \cdots + \zeta_d^{-1} + 1 : -\zeta_d). \tag{4.1.3}$$

Moreover,

$$\begin{aligned} H'(w,v) &= \sum_{i=1}^{d-1} a_i \omega'(w, \zeta_d^i v) \\ &= \sum_{i=1}^{d-1} -a_i \omega'(\zeta_d^i v, w) \\ &= \sum_{i=1}^{d-1} -a_i \omega'(v, \zeta_d^{d-i} w) \\ &= \sum_{i=1}^{d-1} -a_{d-i} \omega'(v, \zeta_d^i w) \end{aligned}$$

and

$$\overline{H'(v,w)} = \sum_{i=1}^{d-1} \overline{a_i} \omega'(v, \zeta_d^i w).$$

These are equal if and only if

$$a_{d-i} = -\overline{a_i} \text{ for all } 1 \leq i \leq d-1. \tag{4.1.4}$$

Letting $a = a_1$, the condition (4.1.3) is equivalent to

$$a_i = (\zeta_d^{-i+1} + \zeta_d^{-i+2} + \cdots + 1)a \quad \text{for all } 1 \leq i \leq d-1$$

and under this condition, the condition (4.1.4) is equivalent to

$$(\zeta_d^{-d+i+1} + \zeta_d^{-d+i+2} + \cdots + 1)a = a_{d-i} = -\overline{a_i} = -(\zeta_d^{i-1} + \zeta_d^{i-2} + \cdots + 1)\overline{a}$$

for all $1 \leq i \leq d-1$. In turn, this condition is equivalent to the single condition when $i = d-1$, i.e. to

$$a = a_1 = -\overline{a}_{d-1} = -(-\zeta_d^{-1})\overline{a} = \zeta_d^{-1}\overline{a}.$$

To see this, assuming that $a = \zeta_d^{-1}\overline{a}$, note that

$$\begin{aligned}
-(\zeta_d^{i-1} + \zeta_d^{i-2} + \cdots + 1)\overline{a} &= -(\zeta_d^{i-1} + \zeta_d^{i-2} + \cdots + 1)\zeta_d a \\
&= -(\zeta_d^{i} + \zeta_d^{i-1} + \cdots + \zeta_d)a \\
&= (\zeta_d^{i+1} + \zeta_d^{i+2} + \cdots + 1)a \\
&= (\zeta_d^{-d+i+1} + \zeta_d^{-d+i+2} + \cdots + 1)a
\end{aligned}$$

Therefore, finding solutions for $a_1, \ldots, a_{d-1}$ is equivalent to finding solutions for a to the equation $a = \zeta_d^{-1}\overline{a}$. One such solution for odd d is $a = \zeta_d^{\frac{d-1}{2}}$. Similarly, one such solution for even d is $a = \zeta^{\frac{d}{2}} + \zeta_d^{\frac{d}{2}+1}$.

Note that $a_1, \ldots, a_{d-1}$ generate A' over A for these aforementioned values of a; in fact, a_1 (and in fact form a basis when d is odd). We now show that perfect symplectic pairings over A which are preserved by ζ_d are assigned to nonsingular Hermitian forms over $A[\zeta_d]$. Now suppose that ω is a perfect symplectic pairing. By Lemma 4.0.8 It suffices to show that the adjoint map $V' \to (V')^*, \quad v \mapsto (w \mapsto H'(v, w))$ of H' is an isomorphism and, when d is even, that $\omega|_{\zeta_d=-1}$ is perfect. Since ω is perfect, so are ω' and $\omega|_{\zeta_d=-1}$.

We first show that the adjoint map of H' is surjective. Let $f \in (V')^*$, i.e. f is an A'-linear map $f : (V')^{\mathrm{op}} \to A'$. Since the a_i form an A-basis of A', there exist unique maps $f_i : V' \to A$ such that $f(w) = \sum_{i=1}^{d-1} a_i f_i(w)$. Note that the f_i are all A-linear. Moreover, since $f(\zeta_d w) = \zeta_d f(w)$, we have

$$\sum_{i=1}^{d-1} a_i f_i(\zeta_d w) = \sum_{i=1}^{d-1} a_i f_i(w)\zeta_d. \tag{4.1.5}$$

Recalling that we have (4.1.1), the RHS of (4.1.5) equals

$$\begin{aligned} a_1 f_1(w)\zeta_d + \sum_{i=2}^{d-1} a_i f_i(w)\zeta_d &= -a_{d-1} f_1(w) + \sum_{i=2}^{d-1} (a_{i-1} - a_{d-1}) f_i(w) \\ &= -a_{d-1} f_1(w) + \sum_{i=1}^{d-2} (a_i - a_{d-1}) f_{i+1}(w) \\ &= \left(\sum_{i=1}^{d-2} a_i f_{i+1}(w) \right) + a_{d-1}(-f_1(w) - \cdots - f_{d-1}(w)). \end{aligned}$$

Comparing the a_i-components in (4.1.5) then yields

$$\begin{aligned} f_{i+1}(w) &= f_i(\zeta_d w) \quad \text{for } 1 \leq i \leq d-2 \\ -f_1(w) - \cdots - f_{d-1}(w) &= f_{d-1}(\zeta_d w). \end{aligned} \tag{4.1.6}$$

Since $f_1 : V' \to A$ is an A-linear map and since ω' is a perfect symplectic form, there exists some $v \in V$ such that $f_1(-) = \omega'(v, -)$. By (4.1.6), it follows that $f_i(w) = \omega'(v, \zeta_d^i w)$ for all $1 \leq i \leq d-1$, so $f(w) = \sum_{i=1}^{d-1} a_i f_i(w) = \sum_{i=1}^{d-1} a_i \omega'(v, \zeta^i w)$. Therefore, the adjoint map of H' is indeed surjective.

We now show that the adjoint map of H' is injective. Suppose that $v \in V$ satisfies $\sum_{i=1}^{d-1} a_i \omega'(v, \zeta_d^i w) = 0$ for all $w \in V$. If d is odd, then we must have that $\omega'(v, w) = 0$ for all $w \in V$ because the a_i form an A-basis of $A' = A[\zeta_d]$. If d is even, then since $1 + \zeta_d^2 + \cdots + \zeta_d^{d-2} = 0$ in A' and since (4.1.3) holds, we have

$$a_{d-1} = \sum_{i=1}^{d-2} (-1)^i a_i.$$

The equality $\sum_{i=1}^{d-1} a_i \omega'(v, \zeta_d^i w) = 0$ is thus equivalent to

$$\sum_{i=1}^{d-2} a_i \omega'(v, \zeta_d^i w) = -a_{d-1} \omega'(v, \zeta_d^{d-1} w) = \sum_{i=1}^{d-2} (-1)^{i+1} a_i \omega'(v, \zeta_d^{d-1} w).$$

Moreover, under the choice of a, $a_1, \ldots, a_{d-2}$ form an A-basis of A', so $\omega'(v, \zeta_d^i w) =$

$(-1)^{i+1}\omega'(v, \zeta_d^{d-1}w)$ for each $i = 1, \ldots, d-2$. In particular

$$\omega'(v, \zeta_d w) + \omega'(v, \zeta_d^3 w) + \cdots + \omega'(v, \zeta_d^{d-1} w) = \frac{d}{2} \cdot \omega'(v, \zeta_d w).$$

On the other hand, the LHS above equals

$$\omega'(v, \zeta_d w + \zeta_d^3 w + \cdots \zeta_d^{d-1} w) = \omega'(v, 0) = 0,$$

so under the assumption that $\frac{d}{2}$ is a nonzerodivisor of A, we have that $\omega'(v, \zeta_d w) = 0$ for all $w \in V$. Therefore, $\omega'(v, w) = 0$ for all $w \in V$ whether d is even or odd. Since ω' is perfect, $v = 0$ in either case. Hence, the adjoint map of H' is indeed injective and is thus indeed an isomorphism as desired. □

We will factor involution rings R into division rings with involution and double division rings and decompose Hermitian forms as Hermitian forms over these factor rings. We will also show in Proposition 4.1.6 that Hermitian spaces over nice enough division or double division rings have orthogonal bases. We introduce the definition of double division rings below.

Definition 4.1.2. Let A be a (not necessarily commutative) ring. The *opposite ring of* A is the ring A^{op} with the same underlying set, the same additive group, and reverse multiplication, i.e.

$$a^{\mathrm{op}} \cdot b^{\mathrm{op}} = (b \cdot a)^{\mathrm{op}}$$

where a^{op} stands for a as an element of A^{op}. We often omit the superscript $^{\mathrm{op}}$.

Definition 4.1.3. [24, Chapter I, 6.7] Let A be a ring. The *hyperbolic ring of* A is the product $H(A) = A \times A^{\mathrm{op}}$ with involution

$$(a, b) \mapsto (b, a).$$

A *double division ring* is a ring of the form $H(A)$ where A is a division ring.

Let $d \geq 2$ be an integer and let ℓ be a prime number not dividing d. There are isomorphisms

$$\mathbb{Q}_\ell[\zeta_d]_{\zeta_d \neq 1} \cong \prod_{\substack{d'|d \\ d' \neq 1}} \mathbb{Q}_\ell[\zeta_{d'}]_{\text{prim}} \tag{4.1.7}$$

$$\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1} \cong \prod_{\substack{d'|d \\ d' \neq 1}} \mathbb{Z}_\ell[\zeta_{d'}]_{\text{prim}}.$$

which are in fact isomorphisms of rings with involutions. For each d', $\mathbb{Q}_\ell[\zeta_{d'}]_{\text{prim}}$ is a Galois algebra over $\mathbb{Q}_\ell$. There is also an isomorphism

$$(\mathbb{Z}/d'\mathbb{Z})^\times \cong \text{Aut}_{\mathbb{Q}_\ell\text{-alg}}(\mathbb{Q}_\ell[\zeta_{d'}]_{\text{prim}}), \quad a \mapsto (X \mapsto X^a).$$

Moreover, $\mathbb{Q}_\ell[\zeta_{d'}]_{\text{prim}}$ splits as a finite product $\prod_i L_{d',i}$ of finite unramified extensions of $\mathbb{Q}_\ell$ and $\text{Aut}_{\mathbb{Q}_\ell\text{-alg}}(\mathbb{Q}_\ell[\zeta_{d'}]_{\text{prim}})$ acts transitively on $L_{d',i}$ and yields isomorphisms amongst the $L_{d',i}$. Let $B_{d',i}$ be the valuation ring of $L_{d',i}$. In particular,

$$\mathbb{Z}_\ell[\zeta_{d'}]_{\text{prim}} \cong \prod_i B_{d',i}. \tag{4.1.8}$$

From (4.1.7) and (4.1.8), we also write

$$\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1} \cong \prod_i B_i. \tag{4.1.9}$$

For each i, the involution $\bar{\cdot} : \zeta_d \to \zeta_d^{-1}$ on $\mathbb{Z}_\ell[\zeta_d]$ either restricts to an automorphism of B_i or restricts to an isomorphism $B_i \to B_{\sigma(i)}$ where $i \neq \sigma(i)$ and $\sigma(\sigma(i)) = i$. In the latter case, $B_i \times B_{\sigma(i)}$ is isomorphic (as a ring with involution) to the double division ring $B_i \times B_i^{\text{op}} = B_i \times B_i$ via the map $\varphi : B_i \times B_i \to B_i \times B_{\sigma(i)}, \quad (a, b) \mapsto (a, \bar{b})$; note that φ respects the involutions on $B_i \times B_i$ and on $B_i \times B_{\sigma(i)}$, i.e. $\overline{\varphi(a,b)} = \varphi(\overline{(a,b)})$ because

$$\overline{\varphi(a,b)} = \overline{(a,\bar{b})} = (\bar{\bar{b}}, \bar{a}) = (b, \bar{a}) = \varphi(b,a) = \varphi(\overline{(a,b)}).$$

There is thus an isomorphism

$$\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1} \cong \prod_i D_i \tag{4.1.10}$$

of involution rings where the D_i are division rings (i.e. integral domains since all of the rings here are commutative) or double division rings. Moreover, if d is prime, then all of the D_i are isomorphic. Factorizations similar to (4.1.7), (4.1.8), (4.1.10) hold over other rings $\mathbb{Z}_\ell[\zeta_d]$ in the notation of Notation 4.0.1.

Notation 4.1.4. Given a ring R with involution $\bar{\cdot}$, let $R^{\bar{\cdot}}$ denote the subring of elements fixed by $\bar{\cdot}$.

Lemma 4.1.5. *Let $d \geq 3$ be a positive integer, let ℓ be a prime number not dividing d, and let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq \pm 1}$. Factorize $\mathbb{Z}_\ell[\zeta_d]$ as $\prod_i D_i$ as in* (4.1.10)*. In particular, each of the D_i is either an integral domain or a double division ring.*

1. *Every invertible element of the subring $D_i^{\bar{\cdot}}$ of D_i is the norm of some element of D_i.*
2. *Every invertible element of the subring $\mathbb{Z}_\ell[\zeta_d]^{\bar{\cdot}}$ of $\mathbb{Z}_\ell[\zeta_d]$ is the norm of some element of $\mathbb{Z}_\ell[\zeta_d]$.*

Proof. The norm map $\mathbb{Z}_\ell[\zeta_d] \to \mathbb{Z}_\ell[\zeta_d]^{\bar{\cdot}}$ is given by $a \mapsto a \cdot \bar{a}$. When D_i is an integral domain, recall that D_i is in fact the valuation rings of a finite field extension L_i of $\mathbb{Q}_\ell$. The involution $\bar{\cdot}$ on D_i is induced by an involution on L_i. This involution $\bar{\cdot}$ on L_i respects the valuation on L_i, so $D_i^{\bar{\cdot}}$ is the valuation ring of the subfield $L_i^{\bar{\cdot}}$ of L_i. Moreover, since the L_i are unramified over $\mathbb{Q}_\ell$, each L_i is unramified over $L_i^{\bar{\cdot}}$. Therefore, the norm map on $D_i^\times$ surjects onto $(D_i^{\bar{\cdot}})^\times$ (see [27, Corollary V.1.2] or [39, Theorem 10.22] for example).

When D_i is a double division ring, say $D_i = B_i \times B_i^{\mathrm{op}} = B_i \times B_i$ with involution $\bar{\cdot} : B_i \times B_i, (a, b) \mapsto (b, a)$, then note that $D_i^{\bar{\cdot}}$ consists exactly of the elements corresponding to the elements of $B_i \times B_i$ of the form (a, a). The norm map on $B_i \times B_i$ also sends $(a, 1)$ to (a, a). Therefore, the norm map on $(B_i \times B_i)^\times$ maps onto $((B_i \times B_i)^{\bar{\cdot}})^\times$.

Either way, the norm map on $D_i^\times$ maps onto $(D_i^{\bar{\cdot}})^\times$, so the norm map on $\mathbb{Z}_\ell[\zeta_d]^\times$ maps onto $(\mathbb{Z}_\ell[\zeta_d]^{\bar{\cdot}})^\times$. □

The following proposition establishes that a Hermitian space over a division ring or a double division ring has an orthogonal basis under nice circumstances:

Proposition 4.1.6. *An ε-Hermitian space (V, H) over a ring D with involution has an orthogonal basis if one of the following hold:*

1. *D is a division ring and the involution of D is not trivial.*
2. *D is a division ring, the involution of D is trivial, $\varepsilon = 1$, and $\operatorname{char} D \neq 2$.*
3. *D is a double division ring and 2 is a unit in D.*

Proof. The first two parts restate [24, Chapter I, Proposition 6.2.4] in the case $\varepsilon = 1$. When 2 is a unit in D, any Hermitian module (V, H) over D is even [24, Chapter I, 3.1][1]. Any even Hermitian space over a double division ring has an orthogonal basis [24, Chapter I, 6.7]. □

Proposition 4.1.7. *Let $d \geq 3$ be a positive integer, let $\ell \neq 2$ be a prime number not dividing d, and let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq \pm 1}$. As in (4.1.10), write*

$$\mathbb{Z}_\ell[\zeta_d] \cong \prod_{i \in I} D_i$$

where the product and isomorphism are of involution rings, and each of the D_i is either a division ring or a double division ring.

1. *For any $\varepsilon \in D_i$ such that $\varepsilon \cdot \overline{\varepsilon} = 1$, any Hermitian space over any of the D_i has an orthonormal basis.*
2. *Let $D = \prod_{i \in J} D_i$ with $J \subseteq I$. Any free 1-Hermitian space over D has an orthonormal basis.*

Proof. 1. By Proposition 4.1.6, any ε-Hermitian space over any of the D_i has an orthogonal basis because the involution on each D_i is not trivial and because $\ell \neq 2$ and hence 2 is invertible in $\mathbb{Z}_\ell$.

[1] That (V, H) is even means that $H(v, w) = k(v, w) + \overline{k(w, v)}$ for some sesquilinear form k on V. We do not use this definition in this thesis.

Let (V, H) be a Hermitian space over D_i and let $v_1, \ldots, v_n$ be an orthogonal basis of V. In particular, H is nonsingular and (V, H) is the orthogonal sum of the submodules V_i generated by v_i and hence the $H|_{V_i}$ are all nonsingular by Lemma 4.0.7. Therefore, $H(v_i, v_i)$ must be a unit of D_i.

By Lemma 4.1.5, there exist $a_i \in D_i^\times$ such that $H(v_i, v_i)$ is the norm of a_i in $(D_i^-)^\times$. We have $H(a_i^{-1}v_i, a_i^{-1}v_i) = 1$. Replacing v_i with $a_i^{-1}v_i$ yields an orthonormal basis of V.

2. Let (V, H) be such a Hermitian space over D. Let V_i be the D_i-component of V, and let $H_i = H|_{V_i}$. By Lemma 4.0.8, the H_i are nonsingular 1-Hermitian forms over D_i. By the above, H_i has an orthonormal basis over D_i, say $v_{i,1}, \ldots, v_{i,n_i}$. In particular, the orthogonal decomposition $V \cong \perp_i V_i$ further decomposes into $V \cong \perp_{i,1\le j\le n_i} \langle v_{i,j}\rangle$ and this decomposition is in fact a decomposition of Hermitian spaces over D. Since V is assumed to be a free D-module, all of the n_i are equal. Let n be n_i. For each $1 \le j \le n$, choose $a_{i,j} \in D_i^\times$ such that $a_{i,j} \cdot \overline{a_{i,j}} = H(v_{i,j}, v_{i,j})^{-1}$ in D_i. Let $v_j := \sum_i a_{i,j} v_{i,j}$ and note that $H(v_j, v_j) = \sum_i a_{i,j} \cdot \overline{a_{i,j}} H(v_{i,j}, v_{i,j}) = 1$ in D. Moreover, $H(v_j, v_{j'}) = 0$ whenever $j \ne j'$ because $H(v_{i,j}, v_{i',j'}) = 0$ for all i, i'. In particular, one can show that the v_j are linearly independent over $\mathbb{Z}_\ell[\zeta_d]$. Letting $e_i \in D$ correspond to 1 in D_i and to 0 in $D_{i'}$ for all $i' \ne i$, note that $e_i v_j = e_i a_{i,j} v_{i,j}$. Furthermore, $e_i a_{i,j}$ is invertible as an element of D_i, so $v_{i,j}$ is in the D-span of v_j. Therefore, the v_j form an orthonormal basis of (V, H).

□

We now show that the ℓ-adic Tate module of a prime-order cyclic cover of $\mathbb{P}^1_{\mathbb{F}_q}$ is a projective module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \ne -1}$ to establish in Corollary 4.1.11 that the Tate module decomposes as orthonormalizable Hermitian spaces over the division ring and double division ring factors of $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \ne \pm 1}$ and that the Tate module itself is almost an orthonormalizable Hermitian space when it is a free $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \ne \pm 1}$-module.

Lemma 4.1.8. *Let k be a field. Let $d \ge 2$ be an integer not divisible by* $\operatorname{char} k$. *Let C*

be a $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1_k$, and let ζ_d be a generator of $\mathrm{Aut}(C/\mathbb{P}^1) \cong \mathbb{Z}/d\mathbb{Z}$. Let ℓ be a prime number not dividing d and not divisible by $\mathrm{char}\, k$. The ℓ-adic Tate module $T_\ell(\mathrm{Jac}(C))$ (over $\bar{k}$) is a projective $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module by letting $\zeta_d \in \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ act on $T_\ell(\mathrm{Jac}(C))$ by the automorphism induced by $\zeta_d \in \mathrm{Aut}(C/\mathbb{P}^1)$, by abuse of notation.

Proof. Let $\varphi : C \to \mathbb{P}^1$ denote the covering map, and fix an $\bar{k}$-point P_0 of C. For any $\bar{k}$-point P of C, the divisor $\left(\sum_{i=0}^{d-1} [\zeta_d P] - [\zeta_d Q_0]\right)$ of C is a principal divisor given by the function $\varphi^*(x(\varphi(P)))$ where $\varphi : C \to \mathbb{P}^1$ is the covering map and $x(\varphi(P))$ is the function of $\mathbb{P}^1$ of divisor $\varphi(P) - \varphi(P_0)$. Therefore, $\Phi_d(\zeta_d) = \sum_{i=0}^{d-1} \zeta_d$ acts as 0 on $\mathrm{Jac}(C)$, so $T_\ell(\mathrm{Jac}(C))$ is indeed a $\mathbb{Z}_\ell[X]/(1 + X + \cdots + X^{d-1})$-module where X acts by ζ_d.

Factoring $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1} \cong \prod_i B_i$ as in (4.1.9), each B_i is a PID. The $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module $T_\ell(\mathrm{Jac}(C))$ corresponds to a tuple $(M_i)_i$ of B_i-modules by $T_\ell(\mathrm{Jac}(C)) \cong \prod_i M_i$. Moreover, $T_\ell(\mathrm{Jac}(C))$ is free (of rank $2g$ where g is the genus of C) as a $\mathbb{Z}_\ell$-module, so each M_i must be a free B_i-module because otherwise, M_i would have a finite direct summand by the structure theorem for PID's. Therefore, $T_\ell(\mathrm{Jac}(C))$ is a projective $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module. □

Let k, d, ℓ, and C be as in Lemma 4.1.8. We use the character theory of the representation χ_C of $\langle \zeta_d \rangle$ on $H^1(C_{\bar{k}}, \mathbb{Q}_\ell) \cong (T_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^\vee$. Suppose that the cover $C \to \mathbb{P}^1$ has branch points $P_1, \ldots, P_n \in \mathbb{P}^1(\bar{k})$ of monodromy $g_1, \ldots, g_r \in \mathbb{Z}/d\mathbb{Z} \cong \langle \zeta_d \rangle$ respectively. By [12, Proposition 1.3], which expresses a Riemann-Hurwitz theorem for characters, the character χ_C of the representation of $\langle \zeta_d \rangle$ on $H^1(C_{\bar{k}}, \mathbb{Q}_\ell) \cong (T_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^\vee$ satisfies

$$\begin{aligned} \chi_C &= 2\chi_{\mathrm{triv}} + 2(g(\mathbb{P}^1) - 1)\chi_{\langle 1 \rangle} + \sum_i (\chi_{\langle 1 \rangle} - \chi_{\langle g_i \rangle}) \\ &= 2\chi_{\mathrm{triv}} - 2\chi_{\langle 1 \rangle} + \sum_{i=1}^{n} (\chi_{\langle 1 \rangle} - \chi_{\langle g_i \rangle}) \end{aligned} \tag{4.1.11}$$

where χ_{triv} is the trivial character of $\langle \zeta_d \rangle$ and $\chi_{\langle g \rangle}$ is the character of $\langle \zeta_d \rangle$ induced from the trivial character $\chi_{\mathrm{triv}, \langle g \rangle}$ on $\langle g \rangle$ where $g \in \langle \zeta_d \rangle$. Moreover, the irreducible representations $\langle \zeta_d \rangle$ over an algebraically closed field of characteristic 0 are the dimension 1 representations ψ_a for $a \in \mathbb{Z}/d\mathbb{Z}$ given by $\psi_a(\zeta_d^j) = \zeta_d^{ja}$. In particular, $\chi_{\mathrm{triv}} = \psi_0$.

Lemma 4.1.9. *Let k, d, ℓ, and C be as above. With the above notation for k, d, ℓ, and C,*

1. *For $g \in \langle \zeta_d \rangle$,*

$$\chi_{\langle g \rangle} = \sum_{\substack{a \in \mathbb{Z}/d\mathbb{Z} \\ \operatorname{ord} g \mid a}} \psi_a$$

as characters of representations on $\overline{\mathbb{Q}}_\ell$-vector spaces, where by $\operatorname{ord} g \mid a$ we mean that $a \equiv \alpha \cdot \operatorname{ord} g \pmod{d}$ for some integer α. In particular,

$$\chi_{\langle g \rangle}(\zeta_d^i) = \begin{cases} \frac{d}{\operatorname{ord} g} & \text{if } \zeta_d^i \in \langle g \rangle \\ 0 & \text{otherwise} \end{cases}$$

so $\chi_{\langle g \rangle}$ is valued in $\mathbb{Q}_\ell$.

2. *Fix r_d to be a primitive dth root of unity in $\overline{\mathbb{Q}}_\ell$. Then, $\chi_{\langle g \rangle}$ is the character of $\overline{\mathbb{Q}}_\ell[X] / \prod_{\substack{a \in \mathbb{Z}/d\mathbb{Z} \\ \operatorname{ord} g \mid a}} (X - r_d^a)$ as a $\langle \zeta_d \rangle$ representation where ζ_d acts as X.*

Proof. 1. The formula [37, The start of Section 7.2 and Chapter 7, Proposition 20] that computes the induced character of a character on a subgroup of a group yields

$$\begin{aligned} \chi_{\langle g \rangle}(\zeta_d^i) &= \frac{1}{\operatorname{ord} g} \sum_{\substack{t \in \langle \zeta_d \rangle \\ t^{-1}\zeta_d^i t \in \langle g \rangle}} \chi_{\mathrm{triv}, \langle g \rangle}(t^{-1}\zeta_d^i t) \\ &= \begin{cases} \frac{d}{\operatorname{ord} g} & \text{if } \zeta_d^i \in \langle g \rangle \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

from which the claimed result follows.

2. By (1),

$$\begin{aligned} \chi_{\langle g \rangle}(\zeta_d^i) &= \sum_{\substack{a \in \mathbb{Z}/d\mathbb{Z} \\ \operatorname{ord} g \mid a}} \psi_a(\zeta_d^i) \\ &= \sum_{\substack{a \in \mathbb{Z}/d\mathbb{Z} \\ \operatorname{ord} g \mid a}} \zeta_d^{a \cdot i}. \end{aligned}$$

As an element of $\mathbb{Q}_\ell$, this equals $\sum_{\substack{a\in\mathbb{Z}/d\mathbb{Z}\\ \text{ord}\, g|a}} r_d^{a\cdot i}$, which coincides with the trace of ζ_d^i acting on $\overline{\mathbb{Q}}_\ell[X]/\prod_{\substack{a\in\mathbb{Z}/d\mathbb{Z}\\ \text{ord}\, g|a}}(X-r_d^a)$, so the claimed result holds.

□

Proposition 4.1.10. *Let k, d, ℓ, and C be as above. If the cover $C \to \mathbb{P}^1$ has r_1 branch points $P_1, \ldots, P_{r_1} \in \mathbb{P}^1(\bar{k})$ whose monodromies, which are elements of $\mathbb{Z}/d\mathbb{Z}$, each have order exactly d, then the ℓ-adic Tate module $T_\ell(\mathrm{Jac}(C))$ has a free $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module of rank at least $r_1 - 2$ as a direct summand.*

Moreover, if all of the monodromies of the branch points have order exactly d (including the point $\infty \in \mathbb{P}^1$ assuming that it is a branch point), which happens when d is prime for example, then $T_\ell(\mathrm{Jac}(C))$ is a free $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module of rank $r-2$ where r is the branch locus degree of the cover $C \to \mathbb{P}^1$.

Proof. Recall Equation (4.1.11). Fixing r_d to be a primitive dth root of unity in $\overline{\mathbb{Q}_\ell}$, Lemma 4.1.9(2) shows that $\prod_{\substack{a\in\mathbb{Z}/d\mathbb{Z}\\ \text{ord}\, g|a}}(X-r_d^a)$ is a polynomial over $\mathbb{Q}_\ell$ and $\chi_{\langle g\rangle}$ is the character of $\overline{\mathbb{Q}}_\ell[X]/\prod_{\substack{a\in\mathbb{Z}/d\mathbb{Z}\\ \text{ord}\, g|a}}(X-r_d^a)$ as a $\langle\zeta_d\rangle$ representation where ζ_d acts as X. Thus, $\chi_{\langle 1\rangle} - \chi_{\langle g\rangle}$ is the character of $\overline{\mathbb{Q}}_\ell[X]/\prod_{\substack{a\in\mathbb{Z}/d\mathbb{Z}\\ \text{ord}\, g\nmid a}}(X-r_d^a)$, which is $\overline{\mathbb{Q}}_\ell[\zeta_d]_{\zeta_d\neq 1}$ if g has order exactly d. Likewise, $\chi_{\langle 1\rangle} - \chi_{\text{triv}}$ is also the character of $\overline{\mathbb{Q}}_\ell[\zeta_d]_{\zeta_d\neq 1}$. Representation of finite groups over algebraically closed fields of characteristic 0 are determined by their characters [37, Chapter 2, Corollary 2], so given that the cover $C \to \mathbb{P}^1$ has r_1 branch points whose monodromies each have order exactly d, χ_C is the character of a representation over $\overline{\mathbb{Q}}_\ell$ that has a free $\overline{\mathbb{Q}}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module of rank at least $r_1 - 2$ as a direct summand. Since field extensions are faithfully flat, $H^1(C_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ in fact has a free $\mathbb{Q}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module of rank at least $r_1 - 2$ as a direct summand, so this is also true of $T_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

By Lemma 4.1.8, $T_\ell(\mathrm{Jac}(C))$ is a $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module. Say that the prime factorization of $\Phi_d(X)$ over $\mathbb{Z}_\ell$ is $\prod_i h_i(X)$; all of the $h_i(X)$ are distinct because $\mathbb{Q}(\zeta_d)$ is unramified above the prime ℓ of $\mathbb{Q}$ since $\ell \nmid d$. In particular, $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d\neq 1} \cong \prod_i B_i$, where $B_i = \mathbb{Z}_\ell[X]/h_i(X)$. Since $T_\ell(\mathrm{Jac}(C))$ is a projective $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d\neq 1}$ and hence has free B_i-components, and since $T_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ to has a free $\mathbb{Q}_\ell[\zeta_d]_{\zeta_d\neq 1}$-module of rank at least $r_1 - 2$ as a direct

summand, $T_\ell(\mathrm{Jac}(C))$ must have a free $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module of rank at least $r_1 - 2$ as a direct summand.

If all of the monodromies of the branch points have order exactly d, then $T_\ell(\mathrm{Jac}(C)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a free $\mathbb{Q}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module of rank $r-2$ and $T_\ell(\mathrm{Jac}(C))$ must be a free $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module of rank $r - 2$. □

We now prove Corollary 4.1.11, which summarizes many of the ideas of the current subsection.

Corollary 4.1.11. *Let k be a field. Let $d \geq 3$ be an integer not divisible by* $\mathrm{char}\, k$. *Let C be a $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1_k$, and identify $\mathrm{Aut}(C/\mathbb{P}^1) \cong \mathbb{Z}/d\mathbb{Z}$ with $\langle \zeta_d \rangle$. Let ℓ be a prime number not dividing $2d$ and not divisible by* $\mathrm{char}\, k$. *Write $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ as the product $\prod_i D_i$ of division rings and double division rings as in* (4.1.10).

1. *The ℓ-adic Weil pairing $\omega : T_\ell(\mathrm{Jac}(C)) \times T_\ell(\mathrm{Jac}(C)) \to \mathbb{Z}_\ell$ induces a nonsingular $\varepsilon_{\mathbb{Z}_\ell[\zeta_d]}$-Hermitian form $H : T_\ell(\mathrm{Jac}(C)) \times T_\ell(\mathrm{Jac}(C)) \to \mathbb{Z}_\ell[\zeta_d]$.*

2. *Writing V_i as the D_i-component of $T_\ell(\mathrm{Jac}(C))$, and H_i as the restriction of H to V_i, the Hermitian form (V_i, H_i) is nonsingular and has an orthonormal basis whenever ζ_d is not -1 in D_i.*

3. *If $T_\ell(\mathrm{Jac}(C))$ is a free $\mathbb{Z}_\ell[\zeta_d]$-module, then the $\mathbb{Z}[\zeta_d]_{\zeta_d \neq \pm 1}$-component of $(T_\ell(\mathrm{Jac}(C)), H)$ has an orthonormal basis. In particular, if d is odd, then $(T_\ell(\mathrm{Jac}(C)), H)$ has an orthonormal basis.*

Proof. Since ω is a nondegenerate symplectic form preserved by ζ_d, Proposition 4.1.1 shows that ω induces a nonsingular Hermitian form on $T_\ell(\mathrm{Jac}(C))$ over $\mathbb{Z}_\ell[\zeta_d]$. By Lemma 4.0.8, (V_i, H_i) are all nonsingular. Since $\ell \neq 2$ and hence 2 is a unit in each D_i, Proposition 4.1.7 shows that (V_i, H_i) has an orthonormal basis.

Furthermore, if $T_\ell(\mathrm{Jac}(C))$ is a free $\mathbb{Z}_\ell[\zeta_d]$-module, its $\mathbb{Z}[\zeta_d]_{\zeta_d \neq \pm 1}$-component is a free 1-Hermitian space, in which case it also has an orthonormal basis by Proposition 4.1.7. □

Remark 4.1.12. Note that the notions of norms and hence orthonormal bases of a (-1)-Hermitian space over a ring with trivial involution, such as $\mathbb{Z}_\ell[X]/(X+1)$, are not fruitful — since the Hermitian form of such a space is actually a symplectic space, norms on such a space are zero. In particular, there is no orthonormal basis of a $\varepsilon_{\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}}$-Hermitian space over $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ when d is even.

4.2 Unitary groups

Let (V, H) be an ε-Hermitian module over a ring R with involution $\bar{\cdot}$. For $m \in R^\times$, let $\mathrm{GU}_m(V)$ be the set of R-linear automorphisms α of V satisfying $H(\alpha(v_1), \alpha(v_2)) = mH(v_1, v_2)$ for all $v_1, v_2 \in V$. Write $\mathrm{U}(V) = \mathrm{GU}_1(V)$, $\mathrm{GU}(V) = \bigcup_m \mathrm{GU}_m(V)$. When (V, H) is a free Hermitian space, note that $\alpha \in \mathrm{GU}_m(V)$ satisfies $\det \alpha \cdot \overline{\det \alpha} = m$. If R is a product $\prod_i D_i$ of finitely many involution rings and (V, H) corresponds to the tuple $(V_i, H_i)_i$ of Hermitian modules over D_i via Lemma 4.0.8, then $\mathrm{GU}_m(V) \cong \prod_i \mathrm{GU}_m(V_i)$.

For a free Hermitian space (V, H), write $\mathrm{SU}(V) = \{\alpha \in \mathrm{U}(V) : \det \alpha = 1\}$. More generally, if R is a product $\prod_i D_i$ of finitely many involution rings and (V, H) is a Hermitian space such that the component (V_i, H_i) of (V, H) over D_i is free for every i, then write $\mathrm{SU}(V) = \{\alpha \in \mathrm{U}(V) : \alpha|_{V_i} \in \mathrm{SU}(V_i)\}$. By construction, $\mathrm{SU}_m(V) \cong \prod_i \mathrm{SU}_m(V_i)$.

4.3 Counting the number of $\mathbb{F}_q$-rational connected components of Hurwitz schemes

In this subsection, we prove Proposition 4.3.1, whose statement and purpose are both analogous to those of [15, Lemma 8.9]. Namely, both Corollary 4.3.8 and [15, Lemma 8.9] are used to show that certain Hurwitz schemes over $\mathbb{F}_q$ have exactly one $\mathbb{F}_q$-rational connected component assuming such big monodromy results discussed further in Section 6.2. However, the ζ_d-action introduces subtle differences that prevent the ideas of the proof of [15, Lemma 8.9] from applying directly. In particular, elements $f : V \to A$ of the set O defined in [15] require a stabilizer $h : V \to V$ to only satisfy $\omega(h(v), h(w)) = q\omega(v, w)$ for

all $v, w \in V$, where ω is the given symplectic pairing on V. In contrast, an element f of the set O defined in Proposition 4.3.1 requires a stabilizer $h : V \to V$ that is equivariant for the ζ_d-action as well. The proof of Proposition 4.3.1 generalize the symplectic theoretic ideas from [15, Lemma 8.9] via the theory of Hermitian forms.

Proposition 4.3.1. *Let $d \geq 3$ be an integer, let ℓ be a prime number not dividing $2dr$, let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$. Let A be a fixed $\mathbb{Z}_\ell[\zeta_d]$-module of finite cardinality and say that A is a quotient module of $\mathbb{Z}_\ell[\zeta_d]^{\oplus r}$.*

Let V be a projective $\mathbb{Z}_\ell[\zeta_d]$-module equipped with a perfect symplectic pairing $\omega : V \times V \to \mathbb{Z}_\ell$ preserved by ζ_d. Recall from Proposition 4.1.1 that ω induces a nonsingular $\varepsilon_{\mathbb{Z}_\ell[\zeta_d]}$-Hermitian form $H : V \times V \to \mathbb{Z}_\ell[\zeta_d]$. Let $q \in \mathbb{Z}_\ell^\times$ be such that $q - 1$ is invertible in $\mathbb{Z}_\ell$. Define O as the set of all $\mathbb{Z}_\ell[\zeta_d]$-equivariant surjections $V \to A$ whose stabilizer, inside $\mathrm{GU}(V)$, intersects $\mathrm{GU}_q(V)$ nontrivially, i.e.

$$O = \{f : V \to A \text{ surjective, equivariant for } \zeta_d, \text{ and there exists } h \in \mathrm{GU}_q(V) \text{ with } f \circ h = f\}.$$

If V has a free $\mathbb{Z}_\ell[\zeta_d]$-module of rank at least $2r$ as a direct summand, then O is nonempty and $\mathrm{U}(V)$ acts transitively on O. In fact, $\mathrm{SU}(V)$ acts transitively on O if V has a free $\mathbb{Z}_\ell[\zeta_d]$-module of rank more than $2r$ as a direct summand.

We prove Proposition 4.3.1 via Proposition 4.3.3 and Proposition 4.3.7.

Lemma 4.3.2. *Let D be a principal ideal ring that is a product of integral domains. A finitely generated D-module M decomposes in the form $\bigoplus_j^r M_j$ where the M_j are quotients of D and $r < \infty$.*

Proof. Say that $D = \prod_k B_k$ where B_k are integral domains. Since D is a principal ideal ring and the B_k are quotients of D, the B_k are PID's. Moreover, M corresponds to a tuple $(M_k)_k$ of B_k-modules; M_k is the B_k-component of M and $M = \prod_k M_k$. For each k, the structure theorem for finitely generated modules over PID's yields a decomposition $M_k \cong \bigoplus_j^{r_k} M_{k,j}$ where each $M_{k,j}$ is a B_k-module that is a quotient of B_k and $r_k < \infty$.

Letting $r = \max_k r_k$, letting $M_{k,j} = 0$ whenever $j > r_k$, and letting $M_j = \prod_k M_{k,j}$, M_j is a quotient of D and M decomposes in the form $\bigoplus_j^r M_j$. □

Proposition 4.3.3. *Let $d \geq 3$ be an integer, let ℓ be a prime number not dividing $2d$. Let D be a division ring or a double division ring quotient of $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq \pm 1}$. Fix a D-module A of finite cardinality. Let (V, H) be a free Hermitian space over D. Let $q \in \mathbb{Z}_\ell^\times$. Decompose A as $\oplus_{i=1}^r A_i$ as in Lemma 4.3.2. If the rank s of V as a D-module is at least $2r$, then the set*

$$O = \{f : V \to A \text{ surjective, } D\text{-linear, and there exists } h \in \mathrm{GU_q}(V) \text{ with } f \circ h = f\}$$

is nonempty.

Proof. Let $v_1, \ldots, v_s$ be an orthogonal basis of V with respect to D such that $H(v_{2i-1}, v_{2i-1}) = 1$ and $H(v_{2i}, v_{2i}) = -1$ for $1 \leq i \leq r$ and such that $H(v_i, v_i) = 1$ for $2r + 1 \leq i \leq s$. Recall that V has an orthonormal basis by Proposition 4.1.7 and such an orthonormal basis can be normalized in this proposed manner because all elements of $(D^{\bar{}})^\times$ are norms of elements of $D^\times$ by Lemma 4.1.5.

Let $f : V \to A$ be given by

$$\begin{aligned} v_{2i-1}, v_{2i} &\mapsto \frac{1}{2} \in A_i \subset A \quad 1 \leq i \leq r \\ v_i &\mapsto 0 \in A \quad 2r + 1 \leq i \leq s \end{aligned}$$

and extended D-linearly; here $1 \in A_i$ is a D-module generator of A_i, which exists because A_i is a quotient of D, and $\frac{1}{2} \in A_i$ is the element such that $\frac{1}{2} + \frac{1}{2} = 1$.

Let $h : V \to V$ be the D-linear automorphism given by

$$\begin{aligned} v_{2i-1} &\mapsto \frac{1+q}{2} v_{2i-1} + \frac{1-q}{2} v_{2i} \\ v_{2i} &\mapsto \frac{1-q}{2} v_{2i-1} + \frac{1+q}{2} v_{2i} \quad \text{for } 1 \leq i \leq r \\ v_i &\mapsto \alpha v_i \quad \text{for } 2r + 1 \leq i \leq s \end{aligned}$$

where $\alpha \in D$ is some element whose norm $\alpha \cdot \overline{\alpha}$ is q. Note that $h \in \mathrm{GU}_q(V)$ because

$$\begin{aligned}
H(hv_{2i-1}, hv_{2i-1}) &= H\left(\frac{1+q}{2}v_{2i-1} + \frac{1-q}{2}v_{2i}, \frac{1+q}{2}v_{2i-1} + \frac{1-q}{2}v_{2i}\right) \\
&= \left(\frac{1+q}{2}\right)^2 - \left(\frac{1-q}{2}\right)^2 = q \\
H(hv_{2i}, hv_{2i}) &= H\left(\frac{1-q}{2}v_{2i-1} + \frac{1+q}{2}v_{2i}, \frac{1-q}{2}v_{2i-1} + \frac{1+q}{2}v_{2i}\right) \\
&= \left(\frac{1-q}{2}\right)^2 - \left(\frac{1+q}{2}\right)^2 = -q \quad \text{for } 1 \le i \le r \\
H(hv_i, hv_i) &= H(\alpha v_i, \alpha v_i) \\
&= N(\alpha) \cdot H(v_i, v_i) = q \quad \text{for } 2r+1 \le i \le s.
\end{aligned}$$

Moreover, $f \circ h : V \to A$ is the D-linear map such that

$$\begin{aligned}
v_{2i-1} &\mapsto \left(\frac{1+q}{2}\right)\frac{1}{2} + \left(\frac{1-q}{2}\right)\frac{1}{2} = \frac{1}{2}, \\
v_{2i} &\mapsto \left(\frac{1-q}{2}\right)\frac{1}{2} + \left(\frac{1+q}{2}\right)\frac{1}{2} = \frac{1}{2}, \quad 1 \le i \le r \\
v_i &\mapsto \alpha \cdot 0 = 0 \quad 2r+1 \le i \le s
\end{aligned}$$

respectively, so $f \circ h = f$. Therefore, O is nonempty as desired. □

We continue with the notation in the above lemma to give a decomposition of V. The decomposition that we will arrive at is similar to the decomposition of V as presented in the proof of [15, Lemma 8.9] Given $f \in O$, let $h \in \mathrm{GU}_q(V)$ be so that $f \circ h = f$ and thus $\mathrm{im}(h-1) \subseteq \ker f$. Given $\lambda \in \bar{\mathbb{F}}_\ell^\times$, let V_λ be the sum of the generalized eigenspaces of h on V as a $\mathbb{Z}_\ell$-module for all eigenvalues that reduce to λ in $\bar{\mathbb{F}}_\ell$. More precisely, let $\overline{V} = V \otimes \overline{\mathbb{Q}}_\ell$, and then set

$$V_\lambda = V \cap \bigoplus_{|\nu - \lambda| < 1} \overline{V}_\nu$$

where $\overline{V}_\nu$ is the generalized ν-eigenspace of h in $\overline{V}$. Equivalently, V_λ consists of all $v \in V$ for which $g_\lambda(h)^n v \to 0$ as $n \to \infty$ where $g_\lambda(x) \in \mathbb{Z}_\ell$ is a polynomial which reduces to the

minimal polynomial of λ over $\mathbb{F}_\ell$.

Let W_λ be the sum of all other generalized eigenspaces of h on V_i other than λ and $\frac{q}{\lambda}$, i.e. of all eigenvalues ν that satisfy $|g_\lambda(\nu)g_{\frac{q}{\lambda}(\nu)}| = 1$; in other words,

$$W_\lambda = \bigcap_{n=1}^{\infty} g_\lambda(v)g_{\frac{q}{\lambda}}(\nu)^n = 1.$$

Note that V_λ and W_λ depend on h.

Lemma 4.3.4. *Given $h \in \mathrm{GU}_q(V)$,*

1. *there is a decomposition*

$$V = \begin{cases} V_\lambda \oplus V_{\frac{q}{\lambda}} \oplus W_\lambda & \text{if } \lambda \text{ is not a square root of } q \text{ in } \overline{\mathbb{F}}_\ell \\ V_\lambda \oplus W_\lambda & \text{if } \lambda \text{ is a square root of } q \text{ in } \overline{\mathbb{F}}_\ell. \end{cases}$$

   as D-modules.

2. *V_λ and $V_{\frac{q}{\lambda}}$ are both isotropic and both orthogonal to W_λ with respect to H, i.e. $H|_{V_\lambda \times V_\lambda}$, $H|_{V_{\frac{q}{\lambda}} \times V_{\frac{q}{\lambda}}}$, $H|_{V_\lambda \times W_\lambda}$, $H|_{V_{\frac{q}{\lambda}} \times W_\lambda}$ are all 0. In particular, $W_\lambda^\perp = V_\lambda + V_{\frac{q}{\lambda}}$ whether or not λ is a square root of q.*

3. *$W_\lambda^\perp$ and W_λ have orthonormal bases.*

Proof. We show that V decomposes as $V_\lambda \oplus V_{\frac{q}{\lambda}} \oplus W_\lambda$ in the case that λ is not a square root of q in $\overline{\mathbb{F}}_\ell$. For $v \in V$, write v uniquely as $v = v_\lambda + v_{\frac{q}{\lambda}} + w$ where $v_\lambda, v_{\frac{q}{\lambda}}, w$ respectively lie in the $\overline{\mathbb{Q}}_\ell$-spans of $V_\lambda, V_{\frac{q}{\lambda}}, W_\lambda$. In particular,

$$\begin{aligned} g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n v &= g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n v_\lambda + g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n v_{\frac{q}{\lambda}} + g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n w \\ &= g_{\frac{q}{\lambda}}(h)^n g_\lambda(h)^n v_\lambda + g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n v_{\frac{q}{\lambda}} + g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n w. \end{aligned}$$

Since $g_\lambda(h)^n v_\lambda \to 0$ and $g_{\frac{q}{\lambda}}(h)^n v_{\frac{q}{\lambda}}$ converge to 0 as $n \to \infty$, they are in V for sufficiently large n, so $g_\lambda(h)^n g_{\frac{q}{\lambda}}(h)^n w \in W_\lambda$ for sufficiently large n. Moreover, $g_\lambda(h)$ and $g_{\frac{q}{\lambda}}(h)$ are invertible on W_λ, so in fact $w \in W_\lambda$. Thus, $v_\lambda + v_{\frac{q}{\lambda}} \in V$, and proceeding similarly, we

have that $v_\lambda \in V_\lambda$ and $v_{\frac{q}{\lambda}} \in V_{\frac{q}{\lambda}}$. Therefore, $V = V_\lambda \oplus V_{\frac{q}{\lambda}} \oplus W_\lambda$. Similarly, $V = V_\lambda \oplus W_\lambda$ if λ is a square root of q in $\bar{\mathbb{F}}_\ell$.

We show that V_λ and $V_{\frac{q}{\lambda}}$ are both isotropic and both orthogonal to W_λ with respect to H. Showing that V_λ is isotropic and orthogonal to W_λ is tantamount to showing that $H(x,y) = 0$ whenever $x \in V_\lambda$ and $y \in V_\lambda \oplus W_\lambda$. Note that $g_\lambda(h)^n x \to 0$ as $n \to \infty$ and for all n there exists some $z_n \in V$ such that $y = g_{\frac{q}{\lambda}}(h)^n z_n$ because $g_{\frac{q}{\lambda}}$ is invertible on both V_λ and W_λ. Write $g_\lambda(x) = x^k + a_{k-1}x^{k-1} + \cdots a_0$; note that $a_0 \in \mathbb{Z}_\ell^\times$ because $\lambda \in \overline{\mathbb{F}}_\ell^\times$. In particular, $g_{\frac{q}{\lambda}}(x) = x^k + \frac{a_1}{a_0}qx^{k-1} + \cdots + \frac{a_{k-1}}{a_0}q^{k-1} + \frac{q^k}{a_0}$, and

$$\begin{aligned} H(x,y) &= H(x, g_{\frac{q}{\lambda}}(h)^n z_n) \\ &= H(x, h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n) + H\left(x, \frac{a_1}{a_0} q h^{k-1} g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) + \cdots + H\left(x, \frac{q^k}{a_0} g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right). \end{aligned}$$

Since H is is bilinear over $\mathbb{Z}_\ell$, since the coefficients of g_λ are in $\mathbb{Z}_\ell$, and since h scales H by q, the above equals

$$\begin{aligned} &H\left(x, h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) + H\left(hx, \frac{a_1}{a_0} h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) + \cdots + H\left(h^k x, \frac{1}{a_0} h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) \\ =&H\left(x, h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) + H\left(\frac{a_1}{a_0} hx, h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) + \cdots + H\left(\frac{h^k}{a_0} x, h^k g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right) \\ =&H\left(\frac{g_\lambda(h)}{a_0} x, g_{\frac{q}{\lambda}}(h)^{n-1} z_n\right). \end{aligned}$$

Iterating, we have that $H(x,y) = H\left(\left(\frac{g_\lambda(h)}{a_0}\right)^n x, z_n\right)$ and hence that $H(x,y)$ lies in $H(g_\lambda(h)^n x, V)$ for all n. Therefore, $H(x,y) = 0$ as desired, so V_λ is isotropic and orthogonal to W_λ. By symmetry, $V_{\frac{q}{\lambda}}$ is isotropic and orthogonal to W_λ.

Since V is a free D-module, $W_\lambda^\perp$ and W_λ are projective D-modules. Moreover, H is nonsingular and hence restricts to nonsingular Hermitian forms on $W_\lambda^\perp$ and W_λ by Lemma 4.0.7. Therefore, $W_\lambda^\perp$ and W_1 are Hermitian spaces with respect to H and have orthonormal bases by Proposition 4.1.7 and in particular are free D-modules. □

We introduce some language to consolidate the Hermitian theories over division rings and over double division rings in the proof of Proposition 4.3.7 below.

Definition 4.3.5. Let D be either a division ring with involution or a double division ring, let M be a D-module, and let $m \in M$. In the case that D is a double division ring, identify D with $H(A) = A \times A^{\mathrm{op}}$ where A is a division ring. Recall that the involution $\bar{\cdot}$ on $A \times A^{\mathrm{op}}$ is given by $(a, b) \mapsto (b, a)$

1. The *type of m is well defined* if one of the following hold:
   (a) D is a double division ring, $m \neq 0$, and $m \in (1,0)M \cup (0,1)M$, or
   (b) D is a division ring.
2. Assuming that the type of m is well defined, we define the *type of m* to be the element $\iota(m) \in D$ given by the following:
   (a) If D is a double division ring and $m \in (1,0)M$, then $\iota(m) = (1,0)$
   (b) If D is a double division ring and $m \in (0,1)M$, then $\iota(m) = (0,1)$.
   (c) If D is a division ring, then $\iota(m) = 1$.

   In any case, $\iota(m)$ is idempotent and $\iota(m)m = m$.

Lemma 4.3.6. *Suppose that D is a double division ring. Let M be a D-double and let $H : M \times M \to D$ be a Hermitian form on M.*

1. *If $m_1, m_2 \in M$ and m_2 has well defined type, then $H(m_1, m_2) = 0$, or $H(m_1, m_2)$ has well defined type that equals $\iota(m_2)$. If $m_1, m_2 \in M$ and m_1 has well defind type, then $H(m_1, m_2) = 0$*
2. *If $m_1, m_2 \in M$ have well defined and equal type, then $H(m_1, m_2) = 0$.*

Proof. 1. Note that

$$H(m_1, m_2) = H(m_1, \iota(m_2)m_2) = H(m_1, m_2)\iota(m_2)$$

so either $H(m_1, m_2)$ is 0 or of type $\iota(m_2)$.

2. Similarly,

$$H(m_1, m_2) = H(\iota(m_1)m_1, \iota(m_2)m_2) = \overline{\iota(m_1)}H(m_1, m_2)\iota(m_2) = 0$$

□

Proposition 4.3.7. *With notation as in Proposition 4.3.3 and assuming that* $q \not\equiv 1 \pmod{\ell}$*, if* O *is nonempty, then* $\mathrm{U}(V)$ *acts transitively on* O*. If* O *is nonempty and the rank* s *of* V *as a* D*-module is greater than* $2r$*, then* $\mathrm{SU}(V)$ *acts transitively on* O*.*

Proof. Given $f \in O$ and $h \in \mathrm{GU}_q(V)$ such that $f \circ h = f$, let $V = (V_1 \oplus V_q) \perp W_1$ be the decomposition of Lemma 4.3.4 and write $W = W_1$. Note that $V_q \oplus W$ lies in the image of $h - 1$ and hence in the kernel of f. In particular, f can only be nonzero on V_1.

Decompose A in the form $A \cong \prod_{i=1}^{r} A_i$ such that A_i is a nonzero quotient of D if D is an integral domain or such that A_i is a nonzero quotient of either $B \times 0$ or $0 \times B$ if $D \cong B \times B$ is a double division ring; note that this is not the same kind of decomposition presented in Lemma 4.3.2 if D is a double division ring. Let $1 \in A_i$ for each $i = 1, \ldots, r$ denote an D-module generator. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ be elements of A which reduce to a D-module generator 1 in A_i and to 0 in A_j when $j \neq i$. Note that e_i is of well defined type.

For each $1 \leq s \leq r$, we recursively obtain elements $v_1, \ldots, v_s \in V_1$ and $w_1, \ldots, w_s \in V_q$ to satisfy the following:

1. $f(v_i) = e_i$.

2. If D is a double division ring, then v_i and w_i are of well defined type, and $\iota(v_i) = \iota(e_i)$, and $\overline{\iota(v_i)} = \iota(w_i)$.

3. $H(v_i, w_j) = \delta_{ij}\iota(w_j)$.

    - In particular, if D is a double division ring, then $H(v_i + w_i, v_j + w_j) = \delta_{ij}$. This

is because

$$H(v_i + w_i, v_j + w_j) = H(v_i, w_j) + H(w_i, v_j) = \delta_{ij}\iota(w_j) + \delta_{ji}\overline{\iota(w_j)} = \delta_{ij}.$$

4. The D submodule U_s of $V_1 \oplus V_q$ generated by $v_1, \ldots, v_s, w_1, \ldots, w_s$ is free and $H|_{U_s}$ is nonsingular. In particular, $V_1 \oplus V_q = U_s \perp U_s^\perp$ by Lemma 4.0.7

   - If D is an integral domain, then $v_1, \ldots, v_s, w_1, \ldots, w_s$ form a D-basis of U_s.
   - If D is a double division ring, then $v_1 + w_1, \ldots, v_s + w_s$ form a D-basis of U_s.

5. $f(U_s^\perp) \subseteq A_{s+1} \times \cdots \times A_r$, i.e. the images of elements of $U_s^\perp$ under f have no $e_1, \ldots, e_s$ components.

We show that the first three properties imply the fourth, i.e. that $v_1, \ldots, v_s, w_1, \ldots, w_s$ generate a free D-module and that the presented bases are indeed bases. More specifically, in the case that D is an integral domain, $v_1, \ldots, v_s, w_1, \ldots, w_s$ are linearly independent — if $\sum_{i=1}^s (\alpha_i v_i + \beta_i w_i) = 0$ for some $\alpha_i, \beta_i \in D$, then $0 = H\left(v_j, \sum_{i=1}^s (\alpha_i v_i + \beta_i w_i)\right) = \beta_j$ and similarly $0 = H\left(w_j, \sum_{i=1}^s (\alpha_i v_i + \beta_i w_i)\right) = \alpha_j$. Similarly, if D is a double division ring instead, then $v_1 + w_1, \ldots, v_s + w_s$ are linearly independent over D. Also note that $v_1 + w_1, \ldots, v_s + w_s$ generate the same D-module as $v_1, \ldots, v_s, w_1, \ldots, w_s$ because $v_i = \iota(v_i) \cdot (v_i + w_i)$ and $w_i = \iota(w_i) \cdot (v_i + w_i)$, so $v_1 + w_1, \ldots, v_s + w_s$ indeed form a D-basis of U_s.

We proceed with the base case of the recursive construction. To obtain $v_1 \in V_1$ and $w_1 \in V_q$ satisfying these properties, first choose $v \in V_1$ such that $f(v) = e_1$. Replace v with $\iota(e_1)v$ so that v has the same type as e_1 as well. Whether or not D is an integral domain, there is some $w \in V_1 \oplus V_q$ such that $H(v, w)$ is nonzero because H is nonsingular. By Lemma 4.3.6, $H(v, w)$ is an element of D of type $\overline{\iota(v)}$. Replace w with its projection in V_q and replace w with an appropriate scalar multiple so that $H(v, w) = \overline{\iota(v)}$. Note that this is possible even when D is a double division ring because $H(v, w)$ is a nonzero element of $\overline{\iota(v)} \cdot D$ and hence the scalar multiplication can be accomplished with an element of $B^\times$.

Further replace w with $\overline{\iota(v)} \cdot w$ so that $\iota(w) = \overline{\iota(v)}$. Let X_1 be the free D submodule of $V_1 \oplus V_q$ generated by v and w. Recall that v and w form a basis of X_1 if D is an integral domain and that $v + w$ forms a basis of X_1 otherwise.

We show that $H|_{X_1}$ is nonsingular. In other words, we show that the adjoint map $X_1 \to X_1^*, \quad v \mapsto H(v, -)$ is a D-isomorphism. If D is a double division ring, then the adjoint map sends $a(v + w)$, where $a \in D$ to $H(a(v + w), -)$, which in turn is the map $X_1 \to D$ that sends $v + w$ to $\overline{a}$. Thus, the adjoint map a bijection and hence an R-module isomorphism. If D is an integral domain, then the adjoint map sends $av + bw$, where $a, b \in D$ to $H(av + bw, -)$, which in turn is the map $X_1 \to D$ sending v to $\overline{b}$ and w to $\overline{a}$. The adjoint map is therefore also a bijection and hence an R-module isomorphism in this case as desired. Thus, $V_1 \oplus V_q = X_1 \perp X_1^{\perp}$ by Lemma 4.0.7.

Proposition 4.1.7 shows that $X_1^{\perp}$ is a free D-module because it is a nonsingular projective Hermitian module over D. Choose a basis $x_1, \ldots, x_k$ of $X_1^{\perp}$, and let $a_1, \ldots, a_k \in D$ be so that the element $f(x_i - a_i v_1)$ of A has image 0 in A_1. Note that $x_1 - a_1 v_1, x_2 - a_2 v_1, \ldots, x_k - a_k v_1$ are linearly independent over D. Let X_1' be the free module that they generate. In particular, $f(X_1') \subseteq A_2 \times \cdots A_r$. Since f maps V_1 surjectively onto A, there is some element of ${X'}_1^{\perp}$ which maps to e_1 under f. Let v_1 be $\iota(e_1)$ times the V_1 component of this element, so in particular, $v_1 \in V_1 \cap {X_1'}^{\perp}$, $f(v_1) = e_1$, and $\iota(v_1) = \iota(e_1)$. Just as w was chosen based on v, there exists some $w_1 \in V_q$ such that $H(v_1, w_1) = \iota(w_1)$ and such that $\iota(w_1) = \overline{\iota(v_1)}$. Replacing w_1 with its ${X_1'}^{\perp}$ component preserves the equality $H(v_1, w_1) = \iota(w_1)$ because $v_1 \in {X_1'}^{\perp}$, preserves that $\iota(w_1) = \overline{\iota(v_1)}$, and additionally specifies w_1 to be an element of $V_1 \cap {X_1'}^{\perp}$. Moreover, the D-module U_1 generated by v_1, w_1 is free and $H|_{U_1}$ is nonsingular. The D-ranks of X_1 and $X_1^{\perp}$ are 2 and k respectively and the rank of X_1' is k, so the rank of ${X_1'}^{\perp}$ is 2. Moreover, if the rank 2 submodule U_s of ${X_1'}^{\perp}$ were to be a proper submodule, then $H|_{U_s}$ would be singular, so in fact U_s is precisely ${X_1'}^{\perp}$. Thus, $f(U_s^{\perp}) = f(X_1') \subseteq A_2 \times \cdots A_r$ as well, so v_1 and w_1 indeed satisfy the desired properties.

Suppose inductively that $v_1, \ldots, v_s \in V_1$ and $w_1, \ldots, w_s \in V_q$ satisfy the properties

where $1 \leq s < r$. We proceed similarly as in the base case to obtain $v_{s+1} \in V_1$ and $w_{s+1} \in V_q$. By the inductive hypothesis, $V_1 \oplus V_q = U_s \perp U_s^{\perp}$. Let $v \in V_1$ such that $f(v) = e_{s+1}$. Replace v with $\iota(e_{s+1})v$ so that $\iota(v) = \iota(e_{s+1})$ as well. The U_s-component v' of v has no components in $v_1, \ldots, v_s$ because $f(v_i) = e_i$. Therefore, v' only has components in $w_1, \ldots, w_s$. Let v'_{s+1} be the $U_s^{\perp}$ component of v, i.e. $v'_{s+1} = v - v'$. In particular, $f(v'_{s+1}) = e_{s+1}$, the type of v'_{s+1} equals that of v, and $H(v'_{s+1}, w_j) = 0$ for $1 \leq j \leq s$ because $w_j \in U_s$. Let $w \in V_1 \oplus V_q$ such that $H(v'_{s+1}, w) \neq 0$ and replace w with its projection in V_q so that $w \in V_q$ as well. Further replace w with $\overline{\iota(v)}w$ and then by a scalar multiple so that $\iota(w) = \overline{\iota(v)}$ and $H(v'_{s+1}, w) = 1$ as well. Let

$$w'_{s+1} = w - \sum_{i=1}^{s} H(v_i, w) w_i. \tag{4.3.1}$$

Note that w'_{s+1} is of type $\iota(w)$; for each i, either $\iota(v_i) = \overline{\iota(w)}$, in which case $\iota(H(v_i, w)) = \iota(w)$ so $H(v_i, w)w_i$ is of the same type as w, or $\iota(v_i) = \iota w$, in which case $H(v_i, w) = 0$. For $1 \leq i' \leq s$,

$$\begin{aligned}
H(v_{i'}, w'_{s+1}) &= H\left(v_{i'}, w - \sum_{i=1}^{s} H(v_i, w) w_i\right) \\
&= H(v_{i'}, w) - \sum_{i=1}^{s} H(v_{i'}, H(v_i, w) w_i) \\
&= H(v_{i'}, w) - H(v_{i'}, H(v_{i'}, w) w_{i'}) \\
&= H(v_{i'}, w) - H(v_{i'}, w) H(v_{i'}, w_{i'}) \\
&= H(v_{i'}, w) - H(v_{i'}, w) \iota(w_{i'}).
\end{aligned}$$

We show that the RHS expression above equals 0. If D is an integral domain, then $\iota(w_{i'}) = 1$, so the RHS expression indeed equals 0. Otherwise, either $\text{type}(v_{i'}) = \text{type}(w)$ in which case $H(v_{i'}, w) = 0$, or $\text{type}(v_{i'}) = \overline{\text{type}(w)}$, in which case $H(v_{i'}, w) = H(v_{i'}, w)\overline{\iota(v_{i'})} = H(v_{i'}, w)\iota(w_{i'})$. Thus, in any case, the RHS expression equals 0 as claimed. Moreover,

$$\begin{aligned} H(v'_{s+1}, w'_{s+1}) &= H\left(v'_{s+1}, w - \sum_{i=1}^{s} H(v_i, w) w_i\right) \\ &= H(v'_{s+1}, w) - \sum_{i=1}^{s} H(v'_{s+1}, H(v_i, w) w_i) \\ &= H(v'_{s+1}, w) = 1. \end{aligned}$$

Let X_{s+1} be the free D-module generated by $v_1, \ldots, v_s, v'_{s+1}, w_1, \ldots, w_s, w'_{s+1}$. In particular, $X_{s+1} = U_s \perp \langle v'_{s+1}, w'_{s+1} \rangle$, so X_{s+1} is nonsingular and hence $V_1 \oplus V_q = X_{s+1} \perp X_{s+1}^{\perp}$. Since $U_s \subset X_{s+1}$, $X_{s+1}^{\perp} \subset U_s^{\perp}$ and hence $f(X_{s+1}^{\perp}) \subseteq A_{s+1} \times \cdots \times A_r$ by the inductive hypothesis. Choose a basis $x_1, \ldots, x_k$ of $X_{s+1}^{\perp}$, let $a_1, \ldots, a_k \in D$ (note that k is different from the k used in the base case of the recursive argument) be so that the element $f(x_i - a_i v'_{s+1})$ of A has image 0 when projected to A_{s+1}. Note that $x_1 - a_1 v'_{s+1}, \ldots, x_k - a_k v'_{s+1}$ are linearly independent over D. Let X'_{s+1} be the free module that they generate. In particular, $f(X'_{s+1}) \subseteq A_{s+2} \times \cdots \times A_r$, and X'_{s+1} is orthogonal to U_s, i.e. $U_s \subseteq (X'_{s+1})^{\perp}$. Since f maps V_1 surjectively onto A, but $f(U_s) \subseteq A_1 \times \cdots \times A_s$ and $f(X'_{s+1}) \subseteq A_{s+2} \times \cdots \times A_r$, there must be some element of $U_s^{\perp} \cap (X'_{s+1})^{\perp}$ that maps to e_{s+1} under f. Let v_{s+1} be $\iota(e_{s+1})$ times the V_1-component of this element so $v_{s+1} \in V_1 \cap U_s^{\perp} \cap (X'_{s+1})^{\perp}$, $\mathrm{type}(v_{s+1}) = \mathrm{type}(e_{s+1})$, and $f(v_{s+1}) = e_{s+1}$. Furthermore, $H(v_{s+1}, w_j) = 0$ for $1 \leq j \leq s$ because $w_j \in U_s$. Once again, there exists some element $w \in V_q$ such that $H(v, w) \in D^{\times}$. Replace w with its projection in $(X'_{s+1})^{\perp}$, then with $\overline{\iota(v_{s+1})} \cdot w$, and then with an appropriate scalar multiple so that $w \in V_q \cap (X'_{s+1})^{\perp}$, $\mathrm{type}(w) = \overline{\mathrm{type}(v_{s+1})}$, and $H(v_{s+1}, w) = 1$. With this new choice of w, define w_{s+1} as we defined w'_{s+1} in (4.3.1) so that w_{s+1} is of the same type as w and $H(v_i, w_j) = \delta_{ij}$ for all $1 \leq i, j \leq s+1$. Let U_{s+1} be the free module generated by $v_1, \ldots, v_{s+1}, w_1, \ldots, w_{s+1}$. In particular, $H|_{U_{s+1}}$ is nonsingular. Moreover, the ranks of X_{s+1} and $X_{s+1}^{\perp}$ are $2(s+1)$ and k respectively and the rank of X'_{s+1} is k, so the rank of $(X'_{s+1})^{\perp}$ is $2(s+1)$. Moreover, the rank $2(s+1)$ submodule U_{s+1} of $(X'_{s+1})^{\perp}$ is a nonsingular Hermitian module for H, so in fact U_{s+1} is precisely $(X'_{s+1})^{\perp}$. Thus, $f(U_{s+1}^{\perp}) = f(X'_{s+1}) \subseteq A_{s+2} \times \cdots \times A_r$, so we

can indeed recursively obtain the elements of V_1 and V_q with the desired properties.

Now given $f' \in O$ as well, we show that there is an element $\varphi \in \mathrm{U}(V)$ such that $f = f' \circ \varphi$. Letting $h' \in \mathrm{GU}_q(V)$ be so that $f' \circ h' = f'$, decompose V as $(V_1' \oplus V_q') \perp W'$ with respect to h' via Lemma 4.3.4 and choose elements $v_1', \ldots, v_r' \in V_1'$ and $w_1', \ldots, w_r' \in V_q$ similarly. Applying Lemma 4.0.7 again shows that $V_1 \oplus V_q = U_r \perp U_r^\perp$ and $V_1' \oplus V_q' = U_r' \perp U'^\perp_r$ where U_r and U_r' are respectively the D-modules generated by $v_1, \ldots, v_r, w_1, \ldots, w_r$ and $v_1', \ldots, v_r', w_1', \ldots, w_r'$. In particular, we have the orthogonal decompositions $U_r \perp U_r^\perp \perp W = V = U_r' \perp U'^\perp_r \perp W'$, and by the inductive construction, f vanishes on $U_r^\perp$ and $U'^\perp_r$. Let $\varphi : V \to V$ be any D-linear automorphism which takes v_i to v_i', takes w_i to w_i', and transforms $U_r^\perp \perp W$ to $U'^\perp_r \perp W'$ such that $H(\varphi(v), \varphi(w)) = H(v, w)$ for all $v, w \in U_r^\perp \perp W$. The latter is possible because $U_r^\perp \perp W$ and $U'^\perp_r \perp W'$ are nonsingular Hermitian modules over D and hence have orthonormal bases by Proposition 4.1.7. In the case that D is a double division ring, the former can be accomplished by letting φ send $v_i + w_i$ to $v_i' + w_i'$ and extending D-linearly. Note that $H(\varphi(v), \varphi(w)) = H(v, w)$ for all $v, w \in U_r$. Moreover, $f(v_i) = e_i = f'(v_i')$ and f vanishes on w_i, w_i', $U_r^\perp$, $U'^\perp_r$, W, and W'. Therefore, φ is indeed an element of $\mathrm{U}(V)$ such that $f = f' \circ \varphi$. The action of $\mathrm{U}(V)$ on O is thus transitive as desired.

We now show that the action of $\mathrm{SU}(V)$ on O is transitive when $s > 2r$. As above, given $f, f' \in O$, let $\varphi \in \mathrm{U}(V)$ such that $f \circ \varphi = f'$ and decompose V as $(V_1' \oplus V_q') \perp W'$ with respect to f'. In this case, W' is a free D-modules of positive rank. Moreover, $\det \varphi \cdot \overline{\det \varphi} = 1$, so in particular $\det \varphi$ is an invertible element of D. Choose an orthonormal basis of W' via Proposition 4.1.7. Let $\alpha : V \to V$ be the D-linear automorphism acting as the identity on $V_1' \oplus V_q'$ and as the matrix

$$\begin{pmatrix} \frac{1}{\det \varphi} & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

on W' with respect to the orthonormal basis. Note that $f = f' \circ (\alpha \circ \varphi)$ because f and f' are nonzero on W and W' respectively and that $\det(\alpha \circ \varphi) = 1$, so the action of $\mathrm{SU}(V)$ on O is transitive as claimed. □

Proof of Proposition 4.3.1. Decompose $\mathbb{Z}_\ell[\zeta_d]$ as $\prod_i D_i$ as in (4.1.10) and say that (V, H) corresponds to the tuple $(V_i, H_i)_i$ of Hermitian forms over D_i via Lemma 4.0.8. Since H is nonsingular, all the H_i are nonsingular, so the V_i are free D_i-modules. Moreover, let A_i be the D_i-component of A, so $A \cong \prod_i A_i$.

Let O_i be the set

$$O_i = \{f_i : V_i \to A_i \text{ surjective, } D_i\text{-linear, and there exists } h_i \in \mathrm{GU}_q(V_i) \text{ with } f_i \circ h = f_i\}.$$

The correspondences of (V, H) with the tuple $(V_i, H_i)_i$ and of A with $\prod_i A_i$ induces a bijection $O \xrightarrow{\sim} \prod_i O_i$ equivariant for the actions of $\mathrm{U}(V) \cong \prod_i \mathrm{U}_i(V)$. If V has a free $\mathbb{Z}_\ell[\zeta_d]$-module of rank at least $2r$ as a direct summand, then each V_i is a free D_i-module of at least that rank. By Proposition 4.3.3 and Proposition 4.3.7, O_i is nonempty and $\mathrm{U}(V_i)$ acts transitively on O_i whenever $\zeta_d \neq -1$ in D_i. In fact, $\mathrm{SU}(V_i)$ acts transitively on O_i as well if V has a free $\mathbb{Z}_\ell[\zeta_d]$-module of rank at least $2r + 1$ as a direct summand. If $\zeta_d = -1$ in D_i, then H_i is in fact a symplectic form, so the unitary group $\mathrm{U}(V_i)$ is the symplectic group $\mathrm{Sp}(V_i)$; note that V_i is of even rank over D_i because H_i is nonsingular. By [15, Lemma 8.9], O_i is nonempty and $\mathrm{U}(V_i) \cong \mathrm{Sp}(V_i)$ acts transitively on O_i because $2r > \dim_{\mathbb{F}_\ell} A_i/\ell A_i$. In fact, one can argue similarly as in the last paragraph of the proof of Proposition 4.3.7 applied to the context of the last paragraph of the proof of [15, Lemma 8.9] to show that $\mathrm{SU}(V_i) = \{\varphi \in \mathrm{U}(V_i) : \det(\varphi) = 1\}$ acts transitively on O_i. Therefore, O is nonempty and $\mathrm{U}(V)$ (or $\mathrm{SU}(V)$) acts transitively on O. □

Corollary 4.3.8. *Let k be a field. Let $d \geq 3$ be a prime power not divisible by the characteristic of k. Let ℓ be a prime number not dividing $2d$ and not divisible by* $\operatorname{char} k$. *Let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$. Let $q \geq 2$ be an integer such that $q \not\equiv 1 \pmod{\ell}$. Fix a $\mathbb{Z}_\ell[\zeta_d]$-module A of finite cardinality and say that A is a quotient of $\mathbb{Z}_\ell[\zeta_d]^{\oplus r}$.*

Let C be a $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1_k$, and identify $\mathrm{Aut}(C/\mathbb{P}^1) \cong \mathbb{Z}/d\mathbb{Z}$ with $\langle \zeta_d \rangle$. Write $V = T_\ell \operatorname{Jac}(C)$. Whenever there at least $2r+3$ branch points of the cover $C \to \mathbb{P}^1$ of whose monodromies are elements of $(\mathbb{Z}/d\mathbb{Z})^\times$, the set

$$O = \{f : V \to A \text{ surjective and } \mathbb{Z}_\ell[\zeta_d]\text{-linear, and there exists } h \in \mathrm{GU}_q(V) \text{ with } f \circ h = f\}$$

is nonempty and $\mathrm{SU}(V)$ acts transitively on O.

Proof. This follows from Proposition 4.1.10 and Proposition 4.3.1. □

Remark 4.3.9. To apply [15, Lemma 8.9] in the proof of Proposition 4.3.1, we needed to know that V_i is of even rank in case $\zeta_d = -1$ in D_i. We alternatively show this via (4.1.11). For $\zeta_d = -1$ to hold in D_i, d must be even. Moreover, the monodromies of the branch points of the cover $C \to \mathbb{P}^1$ are elements of $\mathbb{Z}/d\mathbb{Z}$ whose sum is 0 by Proposition 3.2.2. In particular, the number of branch points with monodromy congruent to 1 mod 2 must be even. Consequently, in expressing χ_C as a sum of the irreducible characters ψ_a by applying (4.1.11) and Lemma 4.1.9(1), the character $\psi_{\frac{d}{2}}$ appears even many times. Thus, the $\mathbb{Z}_\ell[X]/(X+1)$-rank in $T_\ell(\operatorname{Jac}(C))$ is even.

Chapter 5

The Burau representations

This section presents the unreduced and reduced Burau representations, which will be used in Section 6.2 to establish a big monodromy result. Moreover, Chapter 10 studies orbits of the actions of the braid group on vectors given by these Burau representations and the results there are applied to Chapter 8 and Chapter 9.

Definition 5.0.1. Let $n \geq 2$ be an integer. The *Artin braid group* B_n is the group with $n-1$ generators $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ under the braid relations

- $\sigma_i \sigma_j = \sigma_j \sigma_i$ for all $i, j = 1, 2, \ldots, n-1$ with $|i-j| \geq 2$, and
- $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $i = 1, 2, \ldots, n-2$.

Definition 5.0.2. For $n \geq 2$, the *unreduced Burau representation of* B_n is the the representation $\psi_n : B_n \to \mathrm{GL}_n(\mathbb{Z}[t, t^{-1}])$ sending the standard braid σ_i to the block matrix

$$\left(\begin{array}{c|ccc} I_{i-1} & 0 & 0 & 0 \\ \hline 0 & 1-t & t & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & I_{n-i-1} \end{array}\right)$$

Given some invertible element ζ in a ring R, we call the composition

$$B_n \overset{\psi_n}{\hookrightarrow} \mathrm{GL}_n(\mathbb{Z}[t,t^{-1}]) \xrightarrow{t=\zeta} \mathrm{GL}_n(R)$$

the *unreduced Burau representation of B_n evaluated at $t=\zeta$*.

Given a prime number ℓ, we call the composition

$$B_n \overset{\psi_n}{\hookrightarrow} \mathrm{GL}_n(\mathbb{Z}[t,t^{-1}]) \xrightarrow{\text{modulo } \ell} \mathrm{GL}_n(\mathbb{Z}/\ell\mathbb{Z}[t,t^{-1}])$$

the *unreduced Burau representation of B_n modulo ℓ*.

In the case that $R = \mathbb{Z}/\ell\mathbb{Z}[\zeta]$, where ζ is invertible, we also refer the unreduced Burau representation of B_n evaluated at $t=\zeta$ as the *unreduced Burau representation of B_n modulo ℓ evaluated at $t=\zeta$*.

Definition 5.0.3. For $n \geq 2$, the *reduced Burau representation of B_n* is the representation $\psi_n^r : B_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[t,t^{-1}])$ defined as follows: for $n \geq 3$, ψ_n^r is the homomorphism given by

$$\sigma_1 \mapsto \left(\begin{array}{cc|c} -t & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & I_{n-3} \end{array}\right)$$

$$\sigma_i \mapsto \left(\begin{array}{c|ccc|c} I_{i-2} & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & t & -t & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & I_{n-i-2} \end{array}\right), \quad 2 \leq i \leq n-2,$$

$$\sigma_{n-1} \mapsto \left(\begin{array}{c|cc} I_{n-3} & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & t & -t \end{array}\right).$$

For $n = 2$, $\psi_2^r(\sigma_1) = (-t)$.

We define the *reduced Burau representation of B_n evaluated at $t = \zeta$* (for an invertible element ζ in a ring R, the *reduced Burau representation of B_n modulo ℓ* (for a prime number ℓ), and the *unreduced Burau representation of B_n modulo ℓ evaluated at $t = \zeta$* similarly as in Definition 5.0.2.

Remark 5.0.4. There are competing conventions for the unreduced and reduced Burau representations that differ by transposes and/or by involutions on $\mathbb{Z}[t, t^{-1}]$, i.e. by an exchange of t and t^{-1}. In particular, the convention for the unreduced Burau representation in Definition 5.0.2 coincides with that of [21, Definition 3.1.1] and is transpose to that of [35, Definition 2.1]. The convention for the reduced Burau representation in Definition 5.0.3 coincides with those of [38, Section 2, Page 200] and [43, Section 1.1.2] and is transpose to that of [21, Between Theorem 3.9 and Lemma 3.10].

See [21, Chapter 3] for a discussion on the Burau representations. When discussing the action of B_n on a $A^{\oplus n}$ (resp. $A^{\oplus(n-1)}$) for an $\mathbb{Z}[t, t^{-1}]$-module A via ψ_n (resp. ψ_n^r), we mean the action of the square matrices that are images of ψ_n (resp. ψ_n^r) acting on the left of column vectors.

5.1 The Burau representations are unitary

The ring $\mathbb{Z}[t, t^{-1}]$ of Laurent polynomials has a natural involution $a \mapsto \overline{a}$ given by $t \mapsto \bar{t} = t^{-1}$. In particular, one can discuss Hermitian forms over $\mathbb{Z}[t, t^{-1}]$ with respect to this involution. Squier [38] showed that the reduced Burau representation is unitary, i.e. preserves a Hermitian form on $\mathbb{Z}[t, t^{-1}]^{\oplus n}$. In fact, the unreduced Burau representation is unitary as well - Salter [35, Definition 2.3, Lemma 2.4] presented an explicit Hermitian matrix whose Hermitian form is preserved by the unreduced Burau representation.

One can verify that the $n \times n$ matrices H_n over an $\mathbb{Z}[t, t^{-1}]$-involution algebra R such

that $H_n^* = H_n$ and $\psi_n(\sigma_i)^* H_n \psi_n(\sigma) = H_n$ for every $\sigma \in B_n$ are exactly those given by

$$(H_n)_{ij} = \begin{cases} a & \text{if } i = j \\ bt^{j-i-1} & \text{if } j > i \\ \overline{b}t^{1-i+j} & \text{if } i > j \end{cases},$$

where $a = \frac{b - t\overline{b}}{t-1}$. where $b \in R$ and $a \in R^{-}$ (recall Notation 4.1.4). More visually,

$$H_n = \begin{pmatrix} a & b & bt & bt^2 & \cdots \\ \overline{b} & a & b & bt & \cdots \\ \overline{b}t^{-1} & \overline{b} & a & b & \\ \overline{b}t^{-2} & \overline{b}t^{-1} & \overline{b} & a & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{5.1.1}$$

We will also write $H_{n,a,b}$ when we need to construct such a matrix with specific values a and b.

Remark 5.1.1. Note that such matrices H_n are different, even after conjugation and/or transpose, to the matrix J given in [35, Definition 2.3]. There is no immediate reason for H_n and J to be conjugate and/or transpose to each other even though the unreduced Burau representation presented in Definition 5.0.2 is transpose to that in [35, Definition 2.1].

Let $h : R^{\oplus n} \times R^{\oplus n} \to E$ be the Hermitian form given by

$$h(v, w) = c_v^* H_n c_w, \tag{5.1.2}$$

where c_v, c_w respectively denote the column vectors corresponding to $v, w \in R^{\oplus n}$ (with respect to the elementary basis vectors $e_1, \ldots, e_n$), the operator $\cdot^*$ denotes conjugate transpose of vectors/matrices, and E is the subring of $\mathbb{Z}[t, t^{-1}]$ fixed under the involution. Note that the ψ_n, with matrices acting on the left of (column vectors in) $R^{\oplus n}$ preserves h. In

particular, ψ_n preserves the norm

$$v \in R^{\oplus n} \mapsto h(v, v).$$

Now let H_n^r be the $(n-1) \times (n-1)$ matrix

$$H_n^r = \begin{pmatrix} \frac{(t+1)^2}{t} & -(\frac{1}{t}+1) & 0 & 0 & \cdots & 0 \\ -(t+1) & \frac{(t+1)^2}{t} & -(\frac{1}{t}+1) & 0 & \cdots & 0 \\ 0 & -(t+1) & \frac{(t+1)^2}{t} & -(\frac{1}{t}+1) & \cdots & 0 \\ 0 & 0 & -(t+1) & \frac{(t+1)^2}{t} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \frac{(t+1)^2}{t} \end{pmatrix}.$$

One can verify that $\psi_n^r(\sigma_i)^* H_n^r \psi_n(\sigma_i) = H_n^r$ for every $i = 1, \ldots, n-1$, i.e. H_n^r induces a Hermitian form preserved by the reduced Burau representation ψ_n^r. This matrix is essentially derived from the description of the Hermitian form in [43, Section 1.1.3]. Furthermore, $\det H_n^r = \left(\frac{t+1}{t}\right)^{n-1} \left(\frac{t^n-1}{t-1}\right)$ by [43, Lemma 13].

Remark 5.1.2. H_n^r above is conjugate/transpose to the matrix in [43, Section 4.1] as the sesquilinearity conditions in the definitions of Hermitian forms of Definition 4.0.3 and of [43, Section 1.1.3] are opposite to each other.

Since all of the entries of H_n^r has a factor of $t+1$, the matrix becomes zero upon evaluating at $t = -1$. However, dividing all of the entries of H_n^r by $t+1$ and then

evaluating at $t=-1$ yields the $(n-1)\times(n-1)$ skew-symmetric matrix

$$\tilde{H}_n^r = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ -1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 0 & 1 & \cdots & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{5.1.3}$$

that the $\psi_n^r(\sigma_i)$ preserve; note that the involution on $\mathbb{Z}[t,t^{-1}]|_{t=-1}$ is trivial. In particular, the Hermitian form arising from $\tilde{H}_n^r$ is a symplectic form. Thus, the image of ψ_n^r evaluated at $t=-1$ lies in a symplectic group and norms of any vector with respect to this Hermitian form are all zero. Moreover,

$$\det \tilde{H}_n^r = \frac{1}{t^{n-1}} \sum_{i=0}^{n-1} t^i = \begin{cases} 0 & \text{if } 2 \mid n \\ 1 & \text{otherwise.} \end{cases} \tag{5.1.4}$$

Assuming that R factorizes as $R=\prod_i R_i$, where the R_i are division or double division rings with involution, let $\tilde{h}_n^r$ be the Hermitian form on $T^{\oplus(n-1)}$ given (via Lemma 4.0.8) on $R_i^{\oplus(n-1)}$ by H_n^r if R_i is a division ring where $t\neq -1$ and by $\tilde{H}_n^r$ otherwise. In particular, when $R=A[\zeta_d]_{\text{all}}$ factorizes as $A[\zeta_d]_{\zeta_d\neq -1}\times A[X]/(X+1)$, $\tilde{h}_n^r$ is a $\varepsilon_{A[\zeta_d]_{\text{all}}}$-Hermitian form.

5.2 The reduced Burau representation at d-th roots of unity is an arithmetic group

Venkataramana [43] showed that the images of ψ_n^r evaluated at d-th roots ζ_d of unity is an arithmetic group for all large enough n (with respect to d). The following is a restatement of the main theorem of [43] fit to the above notations:

Theorem 5.2.1 ([43, Theorem 2])**.** *Let $d\geq 3$ be an integer, and let $\mathbb{Z}[\zeta_d]=\mathbb{Z}[\zeta_d]_{prim}$. Equip $\mathbb{Z}[\zeta_d]_{prim}^{\oplus(n-1)}$ with the 1-Hermitian form $\tilde{h}_n^r$. In particular, $\psi_n^r|_{t=\zeta_d}: B_n\to \mathrm{GL}_{n-1}(\mathbb{Z}[\zeta_d])$*

maps into $U(\mathbb{Z}[\zeta_d]^{\oplus(n-1)})$. *If* $n \geq 2d+1$, *then the image of* $\psi_n^r|_{t=\zeta_d}$ *is a finite index subgroup of* $U(\mathbb{Z}[\zeta_d]^{\oplus(n-1)})$.

In fact, when $d = 3, 4, 6$, [43, Theorem 3] shows that $\psi_n^r|_{t=\zeta_d}$ is an arithmetic group for all n. Furthermore, [43] combines a theorem of [1] and Theorem 5.2.1 to obtain the following:

Theorem 5.2.2 ([43, Theorem 2])**.** *Let* $d \geq 2$ *be an integer, and write* $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$. *Equip* $\mathbb{Z}[\zeta_d]^{\oplus(n-1)}$ *with the* $\varepsilon_{\mathbb{Z}[\zeta_d]}$*-Hermitian form* $\tilde{h}_n^r$. *In particular,* $\psi_n^r|_{t=\zeta_d} : B_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[\zeta_d])$ *maps into* $U(\mathbb{Z}[\zeta_d]^{\oplus(n-1)})$. *If* $n \geq 2d+1$, *then the image of* $\psi_n^r|_{t=\zeta_d}$ *is a finite index subgroup of* $U(\mathbb{Z}[\zeta_d]^{\oplus(n-1)})$.

Remark 5.2.3. Recall that $\tilde{h}_n^r$ restricted to the factor $\mathbb{Z}[X]/(X+1)$ of $\mathbb{Z}[\zeta_d]_{\mathrm{all}}$ is a symplectic form — $U(\mathbb{Z}[X]/(X+1)^{\oplus(n-1)})$ here thus is the symplectic group $\mathrm{Sp}(\mathbb{Z}[X]/(X+1)^{\oplus(n-1)})$.

5.3 Arithmetic groups have large adic images

Let L a field with an involution $\bar{\cdot}$. Let $K = L^{\bar{\cdot}}$ be the fixed field of L under this involution. Given a (± 1)- Hermitian form h on $L^{\oplus n}$, there is an algebraic group $\mathrm{U}_n(L, f)$ over K such that $\mathrm{U}_n(L, f)(K) = \mathrm{U}(L^{\oplus n})$ (where $L^{\oplus n}$ is equipped with h); if $\bar{\cdot}$ is nontrivial, then $\mathrm{U}_n(L, h)$ is a subalgebraic group of $\mathrm{GL}_{2n}(K)$. Similarly, there is an algebraic group $\mathrm{SU}_n(L, h)$ over K such that $\mathrm{SU}_n(L, h)(K) = \mathrm{SU}(L^{\oplus n})$. In the case that L is a number field, $\mathrm{U}_n(L, h)(\mathcal{O}_K) = \mathrm{U}(\mathcal{O}_L^{\oplus n})$ and $\mathrm{SU}_n(L, h)(\mathcal{O}_K) = \mathrm{SU}(\mathcal{O}_L^{\oplus n})$. See [29, Section 2.3.3] and [43, Section 3] for relevant discussions about these algebraic groups.

Proposition 5.3.1. *Let* L *be a number field with an involution* $\bar{\cdot}$, *let* $K = L^{\bar{\cdot}}$, *let* h *be a nondegenerate* (± 1)*-Hermitian form on* $L^{\oplus n}$, *and let* $\Gamma \subseteq \mathrm{U}(L^{\oplus n})$ *be a finite index subgroup. For a (finite) place* v *of* K, *let* $\mathcal{O}_{L,v} = \mathcal{O}_{K,v} \otimes_{\mathcal{O}_K} \mathcal{O}_L$, *which has a* v*-adic topology. Assume that the set of* $\alpha \in \mathcal{O}_L^\times$ *such that* $\alpha \cdot \overline{\alpha} = 1$ *is finite. For all but finitely many finite places* v *of* K, *the closure of the image of* Γ *in* $\mathrm{U}(\mathcal{O}_{L,v}^{\oplus n})$ *contains* $\mathrm{SU}(\mathcal{O}_{L,v}^{\oplus n})$.

Proof. If an an L-automorphism φ of $L^{\oplus n}$ preserves h, then $\det\varphi^* \cdot \det\varphi = 1$. Note that $\Gamma \cap \mathrm{SU}(\mathcal{O}_L^{\oplus n})$ is the kernel of the map $\Gamma \to \{\alpha \in \mathcal{O}_L^\times : \alpha \cdot \overline{\alpha} = 1\}$ sending φ to $\det\varphi$, so $\Gamma \cap \mathrm{SU}(\mathcal{O}_L^{\oplus n})$ has finite index in Γ, which has finite index in $\mathrm{U}(L^{\oplus n})$. Therefore, $\Gamma' := \Gamma \cap \mathrm{SU}(\mathcal{O}_L^{\oplus n})$ has finite index in $\mathrm{SU}(\mathcal{O}_L^{\oplus n})$.

The algebraic group $\mathrm{SU}_n(L,h)$ over K is geometrically connected [29, Proposition 2.15] and hence connected, so it is the identity component of $\mathrm{U}_n(L,h)$. By [29, Proposition 7.4], $\mathrm{SU}_n(L,h)$ has the weak approximation property (see [29, Section 7.1]). In particular, the map $\prod_{v\in MKK} \mathrm{SU}_n(L,h)(\mathcal{O}_K) \to \mathrm{SU}_n(L,h)(\mathcal{O}_{K,v})$, which is identifiable with $\mathrm{SU}(\mathcal{O}_L^{\oplus n}) \to \prod_{v\in M_K} \mathrm{SU}(\mathcal{O}_{L,v}^{\oplus n})$, has dense image, where M_K denotes the set of inequivalent valuations on K. Suppose that $v_1,\ldots,v_m$ are finite places of K such that the image of Γ' under the maps $\mathrm{SU}(\mathcal{O}_L^{\oplus n}) \to \mathrm{SU}(\mathcal{O}_{L,v_i}^{\oplus n})$ are not dense. Identifying the v_i with their corresponding primes of K, there exist integers $k_1,\ldots,k_m$ such that the image of Γ' under $f_i : \mathrm{SU}(\mathcal{O}_L^{\oplus n}) \to \mathrm{SU}((\mathcal{O}_L/v_i^{k_i})^{\oplus n})$ is not surjective. Note that $f : \mathrm{SU}(\mathcal{O}_L^{\oplus n}) \to \prod_{i=1}^m \mathrm{SU}((\mathcal{O}_L/v_i^{k_i})^{\oplus n})$ is surjective and that $f(\Gamma')$ is contained in $\prod_i f_i(\Gamma')$. Since $[\mathrm{SU}((\mathcal{O}_L/v_i^{k_i})^{\oplus n}) : f_i(\Gamma')] \geq 2$, we have $[\mathrm{SU}(\mathcal{O}_L^{\oplus n}) : \Gamma'] \geq 2^m$, so m must be finite. Therefore, there are at most finitely many places v of K such that the image of Γ' under $\mathrm{SU}(\mathcal{O}_L^{\oplus n}) \to \mathrm{SU}(\mathcal{O}_{L,v}^{\oplus n})$ is not dense, i.e. the closure of the image of Γ in $\mathrm{U}(\mathcal{O}_{L,v}^{\oplus n})$ contains $\mathrm{SU}(\mathcal{O}_{L,v}^{\oplus n})$. □

In the case of interest, L is a cyclotomic field. We show that the set of elements of $\alpha \in \mathcal{O}_L^\times$ such that $\alpha \cdot \overline{\alpha} = 1$ is finite.

Lemma 5.3.2. *1. An algebraic integer α whose Galois conjugates all have absolute value 1 is a root of unity.*

2. Let L be a finite abelian field over $\mathbb{Q}$. There are only finitely many $\alpha \in \mathcal{O}_L$ such that $\alpha \cdot \overline{\alpha} = 1$.

Proof. 1. This is proved, for instance, in expository notes by Wang-Erickson [45, Claim in Proposition 13].

2. Given an embedding $L \to \mathbb{C}$, let $\bar{\cdot}$ be complex conjugation. For any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$,

we have

$$\sigma(\alpha)\overline{\sigma(\alpha)} = \sigma(\alpha)\sigma(\overline{\alpha}) = \sigma(\alpha\overline{\alpha}) = \sigma(1) = 1.$$

Therefore, there are only finitely many such α by (1).

□

Corollary 5.3.3. *Let $d \geq 2$ be an integer, and write $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$. Equip $\mathbb{Z}[\zeta_d]^{\oplus(n-1)}$ with the $\varepsilon_{\mathbb{Z}[\zeta_d]}$-Hermitian form $\tilde{h}^r_n$. In particular, $\psi^r_n|_{t=\zeta_d} : B_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[\zeta_d])$ maps into $U(\mathbb{Z}[\zeta_d]^{\oplus(n-1)})$. If $n \geq 2d+1$, then the closure of the image of the composition*

$$B_n \xrightarrow{\psi^r_n|_{t=\zeta_d}} \mathrm{U}(\mathbb{Z}[\zeta_d]^{\oplus(n-1)}) \to U(\mathbb{Z}_\ell[\zeta_d]^{\oplus(n-1)})$$

contains $\mathrm{SU}(\mathbb{Z}_\ell[\zeta_d]^{\oplus(n-1)})$ for all but finitely many prime numbers ℓ.

Proof. This follows by applying Lemma 5.3.2 and Proposition 5.3.1 to the involution ring factors $\mathbb{Z}[\zeta_e]_{\mathrm{prim}}$ for $e \mid d$.

□

Chapter 6

Counting Rational Points on Hurwitz schemes over $\mathbb{F}_q$

6.1 Hurwitz schemes

Let $\mathsf{Conf}'_n/\operatorname{Spec}\mathbb{Z}$ denote the configuration space of squarefree degree n-divisors on $\mathbb{P}^1$. Letting $\mathbb{P}^n_{\mathbb{Z}}$ be the projective n-space $\mathbb{P}^n_{\mathbb{Z}}$ with coordinates $a_0 : a_1 : \cdots : a_n$, which alternatively parameterize binary forms $a_0X^n + a_1X^{n-1}W + \cdots + a_nW^n$ up to scaling, one more concretely constructs Conf'_n as the open subscheme of $\mathbb{P}^n_{\mathbb{Z}}$ where the discriminant $(\Delta \sum_{i=0}^n a_iX^{n-i}W^i)$ does not vanish.

For finite groups G, Romagny and Wewers [32, Theorem 4.11] constructed a scheme $\mathcal{H}_{G,n}$ of finite type over $\mathbb{Z}$ with an étale cover $\pi : \mathcal{H}_{n,G,\mathbb{Z}} \to \mathsf{Conf}'_n$. For any algebraically closed field k, there is an $\mathrm{Aut}(k)$-equivariant bijection between $\mathcal{H}_{G,n}(k)$ and the set of isomorphism classes of tame G-covers of $\mathbb{P}^1_k$ with n branch points. Moreover, If $x \in \mathcal{H}_{G,n}(k)$ corresponds to a G-cover $f : C \to \mathbb{P}^1_k$, then $\pi(x) \in \mathsf{Conf}'_n(k)$ is the point parameterizing the branch locus of f in $\mathbb{P}^1$. [32, Corollary 4.12] further establishes that, when G is center free, $\mathcal{H}_{G,n}(k)$ is in natural bijection with the set of isomorphism classes of G-covers with degree-n branch locus defined over k.

We discuss Hurwitz schemes introduced in [15, Section 7.3] and [13, Proof of Proposi-

tion 2.1] to generalize point counts over finite fields on these Hurwitz schemes carried out in these papers to the case that $G = A \rtimes \mathbb{Z}/d\mathbb{Z}$ where A is a finite ℓ-group; note that these papers mainly discuss the case when $d = 2$.

[15, Section 7.3] constructs a Hurwitz scheme $\mathsf{Hn}_{G,n}$ parameterizing tame G-covers of $\mathbb{P}^1$ whose branch divisor in $\mathbb{A}^1$ is of degree n — the branched covers may be either ramified at ∞ or not. To construct such a Hurwitz scheme, let Conf_n be the configuration space of configuration space of squarefree degree n-divisors on $\mathbb{A}^1$. Concretely, one can construct Conf_n as the closed subscheme of Conf'_{n+1} cut out by $a_0 = 0$, i.e. as the configuration space of squarefree degree $(n+1)$-divisors on $\mathbb{P}^1$ that contain ∞. Alternatively, one can construct Conf_n as the open subscheme of Conf_n where a_0 does not vanish, i.e. as the configuration of squarefree degree n-divisors on $\mathbb{P}^1$ that do not contain ∞. Given a finite group G, take $\mathsf{Hn}_{G,n}$ to be the disjoint union of $\mathcal{H}_{G,n+1} \times_{\mathsf{Conf}'_{n+1}} \mathsf{Conf}_n$ and $\mathcal{H}_{G,n} \times_{\mathsf{Conf}'_n} \mathsf{Conf}_n$.

If c is a rational conjugacy closed subset of G, then there is a closed and open subscheme $\mathrm{Hur}^c_{G,n} \subseteq \mathsf{Hn}_{G,n}$ parameterizing tame G-covers with monodromy of type c. In fact, if c is $\mathbb{F}_q$-rational and $\gcd(q, |G|) = 1$, then $\mathrm{Hur}^c_{G,n}$ can be constructed over $\mathbb{F}_q$, cf. [14, the discussion between Defintion 8.3 and Proposition 8.4]. In either case, note that $\mathrm{Hur}^c_{G,n}$ parameterizes tame G-covers of $\mathbb{P}^1$ branched at n points away from ∞ with monodromy of type c — whether these covers are branched at ∞ and the monodromy types these covers have at ∞ are not specified.

Remark 6.1.1. [15, Proposition 7.8] is stated when c is a rational conjugacy class. This proposition also holds when the phrase "rational conjugacy class" is replaced with the phrase "$\mathbb{F}_q$-rational conjugacy class" — either rationality condition is only needed to ensure that $\mathsf{Hn}^c_{G,n}$ can be defined over $\mathbb{F}_q$.

We further define Hurwitz schemes of interest. In the case of interest, $d \geq 2$ is an integer, $q \equiv 1 \pmod{d}$, ℓ is a prime that does not divide q, $G = A \rtimes (\mathbb{Z}/d\mathbb{Z})$ where A is a nontrivial $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ module of finite cardinality, where $1 \in \mathbb{Z}/d\mathbb{Z}$ acts on A by ζ_d, and where c is the conjugacy class of elements of the form $(a, 1) \in G$. Note that c is indeed a conjugacy class by Lemma 2.0.4. A tame G-cover $f : C \to \mathbb{P}^1_k$ over a field k

factors as $C \xrightarrow{g} C/A \xrightarrow{h} \mathbb{P}^1_k$ where g is a tame A-cover and h is a tame $\mathbb{Z}/d\mathbb{Z}$-cover. If f is also branched at n points of $\mathbb{A}^1_k$ with monodromy type c, then Proposition 3.1.8 shows that the ramification indices of f and h above these branch points are the orders of $(a,1) \in G$ and of $1 \in \mathbb{Z}/d\mathbb{Z}$ respectively. These orders are d since $(1-\zeta_d)$ is invertible on A. Thus, g must be unramified above $\mathbb{A}^1_k$.

Moreover, the monodromy type of ∞ is of the form $(a, -n \pmod d)$ where $a \in A$ by Proposition 3.2.2 and Proposition 3.1.7. Proposition 3.1.8 shows that the ramification indices of $h \circ g$ and h over ∞ are the orders of $(a,-n) \in A \rtimes \mathbb{Z}/d\mathbb{Z}$ and of $-n \in \mathbb{Z}/d\mathbb{Z}$ respectively. If $\gcd(n,d) = 1$, then these orders are both d. In this case, h is totally ramified above ∞ and g is unramified the point in C/A above ∞. Note that such a tame G-cover f over $\mathbb{F}_q$ exists only if $q \equiv 1 \pmod d$ by Proposition 3.3.2. If $d \mid n$ instead, h must be unramified above ∞, but g might be ramified above ∞. In this case, we restrict our attention to a Hurwitz scheme parameterizing exactly the covers f such that g is unramified above ∞.

Definition 6.1.2. Let $d \geq 2$ be an integer, let ℓ be a prime number not dividing d, let $G = A \rtimes (\mathbb{Z}/d\mathbb{Z})$ where A is a nontrivial $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ module of finite cardinality and where $1 \in \mathbb{Z}/d\mathbb{Z}$ acts on A by ζ_d. Note that G is center-free by Lemma 2.0.6. Let $c = \{(a,1) \in G : a \in A\}$, which is a conjugacy class by Lemma 2.0.4.

For integers $n \geq 1$ that are either divisible by d or relatively prime to d and a prime power q coprime to $d\ell$ such that $q \equiv 1 \pmod d$, define the scheme $\mathbf{X}_n/\mathbb{F}_q$ as follows:

- If $(n,d) = 1$, then let $\mathbf{X}_n = \mathsf{Hn}^c_{G,n}$.
- If $d \mid n$, then let $\mathbf{X}_n$ be the intersection of $\mathsf{Hn}^c_{G,n}$ with the open and closed subscheme $\mathcal{H}_{G,n} \times_{\mathsf{Conf}'_n} \mathsf{Conf}_n$ of $\mathsf{Hn}_{G,n}$. In particular, $\mathbf{X}_n$ is the disjoint union of connected components of $\mathsf{Hn}^c_{G,n}$.

In either case, $\mathbf{X}_n$ parameterizes the covers f for which g is unramified above ∞. We will later apply class field theory and Kummer theory to such g as appropriate. The fact that G is center free and [32, Theorem 2.1] imply that $\mathsf{Hn}^c_{G,n}$ is a fine moduli space.

Proposition 6.1.3 below generalizes [15, Proposition 8.7]; the latter is a special case of the former when $d = 2$ and $\gcd(d, n) = 1$, and the proof of the former that we present below is very similar to the proof of the latter.

Let k be a field. Given a finite field extension L of $k(t)$, write Cl_L for the class group of $\mathcal{O}_L$, the integral closure of $k[t]$ inside L. Assuming that k is algebraically closed in L and assuming that L has a k-rational point, this class group is isomorphic to $\mathrm{Jac}(C_L)(k)$ where C_L is the smooth curve over k corresponding to L — see [33, Theorem C(ii)] for more details. This happens, for instance, over the base field $k = \mathbb{F}_q$ if $L = \mathbb{F}_q(t)[y]/(y^d - f(t))$ for a nonconstant dth-power free polynomial $f(t)$ with $(\deg f(t), d) = 1$ since L is a totally imaginary extension of $\mathbb{F}_q(t)$ by Lemma 3.2.1. Suppose further that C_L is a tame $(\mathbb{Z}/d\mathbb{Z})$-cover of $\mathbb{P}^1$ over k. Identifying ζ_d with $1 \in \mathbb{Z}/d\mathbb{Z} \cong \mathrm{Aut}(C_L/\mathbb{P}^1)$, there are actions of ζ_d on $\mathrm{Jac}(C_L)$ and Cl_L in this case.

Proposition 6.1.3. *Let $d \geq 2$ be an integer, let ℓ be a prime number not dividing d, and let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$. Fix A to be a $\mathbb{Z}_\ell[\zeta_d]$-module of finite cardinality. Let $G = A \rtimes (\mathbb{Z}/d\mathbb{Z})$ where $1 \in \mathbb{Z}/d\mathbb{Z}$ acts on A by ζ_d and let c be the conjugacy class in G of the elements of the form $(a, 1)$. Let q be a power of a prime not dividing $d\ell$ such that $q \equiv 1 \pmod{d}$. In particular, $\mathbb{F}_q$ contains a primitive dth root of unity and $\mathbf{X}_n$ is defined over $\mathbb{F}_q$.*

For each integer $n \geq 1$ coprime to d, there is a bijection between $\mathbf{X}_n(\mathbb{F}_q)$ and the set of isomorphism classes of pairs (L, α), where L is a $\mathbb{Z}/d\mathbb{Z}$-extension of $\mathbb{F}_q(t)$ of discriminant degree n of the form $L = \mathbb{F}_q(t)(\sqrt[d]{f(t)})$ for some squarefree $f(t) \in \mathbb{F}_q[t]$, and where α is a surjective homomorphism

$$\alpha : \mathrm{Cl}_L \to A$$

equivariant for the ζ_d-actions. Here, two pairs (L, α) and (L', α') are isomorphic if there exists an $\mathbb{F}_q(t)$-isomorphism $f : L \to L'$ with $f^*\alpha' = \alpha$.

Remark 6.1.4. The squarefree condition on $f(t)$ ensures that the $\mathbb{Z}/d\mathbb{Z}$-cover C_L of $\mathbb{P}^1$ has consistent monodromy type over all branch points in $\mathbb{A}^1$. Moreover, the base field is geometrically closed inside $L = k(t)(\sqrt[d]{f(t)})$ for such an $f(t)$ because the points of C_L

above the branch points in $\mathbb{A}^1$ are all totally (tamely) ramified by Proposition 3.2.2 and Proposition 3.1.8.

Proof. For L a $\mathbb{Z}/d\mathbb{Z}$ extension of $K := \mathbb{F}_q(t)$, let ζ_d be the automorphism of L over K that corresponds to 1 under the identification $\mathrm{Aut}(L/K) \cong \mathbb{Z}/d\mathbb{Z}$. Let J_L be the Galois group of the maximal abelian everywhere unramified extension E/L with pro-ℓ Galois group. In particular, E/K is Galois and $\mathrm{Gal}(E/K)$ has J_L as a normal subgroup. We show that the subgroup $N := \left\langle \sum_{i=0}^{d-1} \zeta_d^i(x) : x \in J_L \right\rangle$ is a normal subgroup of $\mathrm{Gal}(E/K)$.

There is a short exact sequence

$$1 \to (J_L = \mathrm{Gal}(E/L)) \to \mathrm{Gal}(E/K) \to (\mathrm{Gal}(L/K) \cong \langle \zeta_d \rangle) \to 1,$$

and $\mathrm{Gal}(E/K)$ is isomorphic to $J_L \rtimes \mathrm{Gal}(L/K)$. For elements $(y, \zeta_3) \in J_L \rtimes \mathrm{Gal}(L/K)$, calculate

$$\begin{aligned}(y, \zeta_3^k) \cdot \left(\sum_{i=0}^{d-1} \zeta_d^i(x), 0 \right) \cdot (y, \zeta_3^k)^{-1} &= \left(y + \zeta_3 \left(\sum_{i=0}^{d-1} \zeta_d^{i+k}(x) \right) - y, 0 \right) \\ &= \left(\sum_{i=0}^{d-1} \zeta_d^i(x), 0 \right).\end{aligned}$$

Thus, N is normal in $\mathrm{Gal}(E/K)$ as desired.

Now let F_L be the fixed field of E by N. In particular, F_L/K is also a Galois extension and there is a short exact sequence

$$1 \to J_L' \to \mathrm{Gal}(F_L/K) \to \mathrm{Gal}(L/K) \to 1. \tag{6.1.1}$$

where $J_L' := \mathrm{Gal}(F_L/L)$. There is also a short exact sequence

$$1 \to \mathrm{Gal}(E/F_L) \to \mathrm{Gal}(E/L) \to \mathrm{Gal}(F_L/L) \to 1$$

of abelian groups. This short exact sequence is identifiable with

$$1 \to N \to J_L \to J'_L \to 1$$

and hence J'_L is the quotient of $\mathrm{Gal}(E/F_L)$ by N. Since J_L is a pro ℓ-group by definition, J'_L is also a pro ℓ-group. Furthermore, the sequence (6.1.1) yields an isomorphism

$$\mathrm{Gal}(F_L/K) \cong J'_L \rtimes \langle \tau_d \rangle. \tag{6.1.2}$$

where τ_d is any element of $\mathrm{Gal}(F_L/K)$ that reduces to ζ_d in $\mathrm{Gal}(L/K)$.

Class field theory (see e.g. [41, Theorem 1.1.4] for a statement) yields a short exact sequence:

$$(\mathrm{Cl}_L)_\ell \hookrightarrow J_L \twoheadrightarrow \hat{\mathbb{Z}}_\ell \tag{6.1.3}$$

where $(\mathrm{Cl}_L)_\ell$ denotes the Sylow-ℓ subgroup of Cl_L and $\hat{\mathbb{Z}}_\ell$ is the pro-ℓ part of $\hat{\mathbb{Z}} \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Moreover, the surjection $J_L \twoheadrightarrow \hat{\mathbb{Z}}_\ell$ is identified with the homomorphism $(\pi_1^{\text{ét}}(C_L))^{\mathrm{ab}} \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_q)$ induced by the structure morphism $C_L \to \mathbb{F}_q$. Note that ζ_d acts compatibly on all groups in the above short exact sequence.

Note that ζ_d acts trivially on $\hat{\mathbb{Z}}_\ell$, so $\sum_{i=0}^{d-1} \zeta_d^i$ acts as d on $\hat{\mathbb{Z}}_\ell$ and in particular acts as an automorphism. Apply the snake lemma to

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathrm{Cl}_L)_\ell & \longrightarrow & J_L & \longrightarrow & \hat{\mathbb{Z}}_\ell & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \sum_{i=0}^{d-1} \zeta_d^i} & & \downarrow{\scriptstyle \sum_{i=0}^{d-1} \zeta_d^i} & & \downarrow{\scriptstyle \sum_{i=0}^{d-1} \zeta_d^i} & & \\
0 & \longrightarrow & (\mathrm{Cl}_L)_\ell & \longrightarrow & J_L & \longrightarrow & \hat{\mathbb{Z}}_\ell & \longrightarrow & 0
\end{array}$$

to conclude that the cokernels of $\sum_{i=0}^{d-1} \zeta_d^i$ acting on $(\mathrm{Cl})_\ell$ and J_L are isomorphic, i.e. $J_L / \left(\sum_{i=0}^{d-1} \zeta_d^i \right) J_L \cong (\mathrm{Cl}_L)_\ell / \left(\sum_{i=0}^{d-1} \zeta_d^i \right) (\mathrm{Cl}_L)_\ell$. The former of these groups is J'_L. Moreover, for any fractional ideal I on $\mathcal{O}_L$, the product $\prod_{i=0}^{d-1} \zeta_d(I)$ is an extension of a fractional ideal from K and hence is principal, i.e. is trivial as an element of Cl_L. Therefore,

$(\mathrm{Cl}_L)_\ell / \left(\sum_{i=0}^{d-1} \zeta_d^i\right) (\mathrm{Cl}_L)_\ell = (\mathrm{Cl}_L)_\ell$, so we have a ζ_d-equivariant isomorphism

$$J'_L \xrightarrow{\sim} (\mathrm{Cl}_L)_\ell. \tag{6.1.4}$$

Thus, given a pair (L, α) where L is an imaginary $\mathbb{Z}/d\mathbb{Z}$-extension of $\mathbb{F}_q(t)$ of discriminant degree n, and $\alpha : \mathrm{Cl}_L \to A$ is a ζ_d-equivariant surjection, composing α with (6.1.4) above yields a ζ_d-equivariant surjection $f_\alpha : J'_L \to A$. This map f_α extends to a surjection $J'_L \rtimes \langle \tau_d \rangle \to A \rtimes \langle \zeta_d \rangle$ by sending (id, τ_d) to any element of the form (a, ζ_d). Such a surjection is identifiable with a map $g_\alpha : \mathrm{Gal}(F_L/K) \to G$ by (6.1.2). Moreover, since all elements of $A \rtimes \langle \zeta_d \rangle$ of the form (a, ζ_d) are conjugate under A by Lemma 2.0.4, the choice of g_α is unique up to A-conjguacy.

Now let F_α be the fixed field of $\ker(g_\alpha)$. It is a Galois extension of K with an isomorphism $\mathrm{Gal}(F_\alpha/K) \cong G$ defined up to A-conjugacy. Moreover, $\mathbb{F}_q$ is algebraically closed inside F_α. In other words, given the pair (L, α), there is an associated geometrically connected curve Y_α whose function field is F_α together with a cover $Y_\alpha \to \mathbb{P}^1$ and an isomorphism $g_\alpha : \mathrm{Aut}(Y_\alpha/\mathbb{P}^1) \to G$.

Note that F_α/L is everywhere unramified because F_α is a subfield of E, which is by definition everywhere unramified above L. Thus, the ramified places of F_α/K are the same as those of L/K and the ramification degrees of F_α/K are the same as those of L/K. In fact, the condition that L is of the form $\mathbb{F}_q(t)(\sqrt[d]{f(t)})$ for some squarefree $f(t) \in \mathbb{F}_q[t]$ and Proposition 3.2.2 imply (with an appropriate choice of topological generator of $\hat{\mathbb{Z}}(1)$) that the monodromy types above the branch points of $C_L \to \mathbb{P}^1$ in $\mathbb{A}^1$ are all $1 \in \mathbb{Z}/d\mathbb{Z}$ and that the monodromy type above ∞ is $-n \in \mathbb{Z}/d\mathbb{Z}$. By Proposition 3.1.7, the monodromy types above the branch points of $Y_\alpha \to \mathbb{P}^1$ in $\mathbb{A}^1$ are all in c and the monodromy type above ∞ is of the form $(a, -n) \in G$.

The isomorphism class of the G-cover of $\mathbb{P}^1$ defined by (Y_α, g_α) does not depend on conjugating g_α by elements of A. To see this, let (Y'_α, g'_α) be another pair obtained via such a conjugation, say by $(x, 0) \in A \rtimes \mathbb{Z}/d\mathbb{Z} = G$. In other words, starting from the

surjection $f_\alpha : J'_L \to A$, if $g_\alpha : \mathrm{Gal}(F_L/K) \to G$ sends τ to $(y, 1)$, then g'_α sends τ to

$$(x, 0)(y, 1)(x, 0)^{-1}$$

where $i \mapsto \varphi_i : \mathbb{Z}/d\mathbb{Z} \to \mathrm{Aut}(A)$ denotes the action of $\mathbb{Z}/d\mathbb{Z}$ on A determining G. Letting F_α and F'_α respectively be the fixed fields of $\ker(g_\alpha)$ and $\ker(g'_\alpha)$, we obtain isomorphisms $\mathrm{Gal}(F_\alpha/K) \simeq G$ and $\mathrm{Gal}(F'_\alpha/K) \simeq G$. These isomorphisms are naturally identified with isomorphisms $g_\alpha : \mathrm{Aut}(Y_\alpha/\mathbb{P}^1) \to G$ and $g'_\alpha : \mathrm{Aut}(Y'_\alpha/\mathbb{P}^1) \to G$ where Y_α and Y'_α respectively are the curves associated to F_α and F'_α.

To summarize, given an isomorphism class of a pair (L, α), we have produced a tame G-cover $F_\alpha \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ branched at n points in $\mathbb{A}^1$ above which the monodroy types are c. In turn, such a cover corresponds to a point of $\mathbf{X}_n(\mathbb{F}_q)$, so we have a map

$$\{(L, \alpha)\}/(\text{isomorphism}) \to \mathbf{X}_n(\mathbb{F}_q). \tag{6.1.5}$$

Now we produce an inverse of this map. Given a point of $\mathbf{X}_n(\mathbb{F}_q)$, write $X \to \mathbb{P}^1$ for the corresponding tame G-cover branched at n points of $\mathbb{A}^1$ with monodromy of type c. By the discussion leading up to Definition 6.1.2 and by the construction of $\mathbf{X}_n$, the quotient map $X \to X/A$ is étale.

Let L be the function field of X/A. By Proposition 3.2.2, L must be of the form $\mathbb{F}_q(t)[y]/(y^d - f(t))$ for some squarefree $f(t) \in \mathbb{F}_q[t]$. Applying class field theory to the étale cover $X \to X/A$ yields a ζ_d-equivariant homomorphism $\alpha : \mathrm{Cl}_L \to A$ and this construction yields the inverse map to (6.1.5) as desired. Thus, there is indeed a bijection as claimed. □

Remark 6.1.5. When d is coprime to n, the points of $\mathbf{X}_n$ parameterize totally imaginary $\mathbb{Z}/d\mathbb{Z}$-extensions L of $\mathbb{F}_q(t)$.

6.2 Big monodromy hypotheses

We begin this subsection by motivating big monodromy results which imply the conclusion of Theorem 6.3.1 when they hold. Fix a positive integer d and a fixed prime power $q \equiv 1 \pmod{d}$. Given a positive integer n, let $\mathfrak{S}_n$ be the set of isomorphism classes of extensions L of $\mathbb{F}_q(t)$ of the form $\mathbb{F}_q(t)[y]/(y^d - f(t))$ where $f(t) \in \mathbb{F}_q[t]$ is squarefree and of degree n. Moreover, for an abelian ℓ-group A with a $\langle \zeta_d \rangle$-action and a $\mathbb{Z}/d\mathbb{Z} \cong \langle \zeta_d \rangle$-extension L of $\mathbb{F}_q(t)$, write $m_A(L)$ for $|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]_{\mathrm{all}}}(\mathrm{Cl}(\mathcal{O}_L), A)|$. If A is in fact a $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module, then note that $m_A(L) = |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}}(\mathrm{Cl}(\mathcal{O}_L), A)|$.

Theorem 6.3.1 below, like its predecessor [15, Theorem 8.8], asymptotically counts $\mathbb{F}_q$-rational points of $\mathbf{X}_n$ to relate $\sum_{L \in \mathfrak{S}_n} m_A(L)$ and $|\mathfrak{S}_n|$. The proof of the theorem achieves this point count by using the Lefschetz trace formula and by considering the traces of Frob_q on $H_c^j(\mathbf{X}_n \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathbb{Q}_r)$ for the cases $j < 2n$ and $j = 2n$ separately. Ellenberg, Venkatesh, and Westerland's cohomological stability results for Hurwitz spaces and schemes ([15, Theorem 6.1, Corollary 6.2, Proposition 7.8]) bound the terms given by $j < 2n$. On the other hand, the trace of Frobenius for the $j = 2n$ term is precisely identified by showing that $\mathbf{X}_n \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ has precisely one $\mathbb{F}_q$-rational connected component, assuming an appropriate big monodromy result.

In general, one can discuss the mod-ℓ or ℓ-adic monodromy representations of abelian schemes generalizing notions of Galois representations. See [2, Section 3.1] for a more expansive discussion of such representations. Let X/S be an abelian scheme of relative dimension g over an irreducible base S. For any rational prime ℓ invertible on S and $k \geq 1$, the ℓ^k-torsion subgroup $X[\ell^k]$ is a finite étale cover of S and hence $\pi_1^{\text{ét}}(S, s)$ acts on $X[\ell^k]$ for any geometric point s of S. In fact, this action respects the additive structure on $X[\ell^k]$, so there is an induced *monodromy representation*

$$\rho_{X \to S, s, \mathbb{Z}/\ell^k\mathbb{Z}} : \pi_1^{\text{ét}}(S, s) \to \mathrm{Aut}(X[\ell^k]_s) \cong \mathrm{GL}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}). \tag{6.2.1}$$

The isomorphism class of the image of $\rho_{X \to S, s, \ell^k}$ is independent of the choice of base point

s. Taking the inverse limit over k yields a continuous representation of the ℓ-adic Tate module of X:

$$\rho_{X\to S,s,\mathbb{Z}_\ell} : \pi_1^{\text{ét}}(S,s) \to \varprojlim_k \operatorname{Aut}(X[\ell^k]_s) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Let $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(X \to S, s)$ and $M_{\mathbb{Z}_\ell}(X \to S, s)$ respectively be the images of $\rho_{X\to S,s,\mathbb{Z}/\ell^k\mathbb{Z}}$ and $\rho_{X\to S,s,\mathbb{Z}_\ell}$ and call them the mod-ℓ^k and ℓ-adic monodromy groups of $X \to S$. If the abelian scheme X over S is clear in context, then denote the monodromy representations by $\rho_{S,s,\mathbb{Z}/\ell^k\mathbb{Z}}$ and $\rho_{S,s,\mathbb{Z}_\ell}$ and the monodromy groups by $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(S,s)$ and $M_{\mathbb{Z}_\ell}(S,s)$ respectively. Note that the isomorphism classes of the monodromy groups do not depend on the base point s, and we sometimes omit s when notating these groups.

If more conditions are specified, then the image of the monodromy representations may be contained in smaller linear groups. For example, if X is principally polarized, then in fact the image of $\rho_{X\to S,s,\mathbb{Z}_\ell}$ is contained in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, the group of similitudes of $((T_\ell X)_s, \omega)$, where $\omega : T_\ell X \times T_\ell X^\vee \to \mu_{\ell,S}$ is the ℓ-adic Weil pairing. Moreover, if a primitive ℓth root of unity exists globally on S, then $\pi_1(S,s)$ acts trivially on $\mu_{\ell,S}$, so the image of $\rho_{X\to S,s,\mathbb{Z}_\ell}$ is contained in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$.

Given a relative proper semi-stable curve $\psi : C \to S$, the identity component $\mathrm{Pic}^0(C) := \mathrm{Pic}^0_{C/S}$ of the relative Picard functor of ψ is a semiabelian scheme [9, Proposition 4.3] (cf. [4, Theorem 9.4.1]). For a geometric point s of S such that $\mathrm{Pic}^0(C_s)$ is an abelian variety, there is a nonempty open neighborhood S^* of s such that $\mathrm{Pic}^0(C|_{S^*})$ is an abelian scheme over S^*. By [4, Example 9.2.8], s is such a point whenever C_s is a tree of smooth curves. Define the mod-ℓ^k and $\mathbb{Z}_\ell$ monodromy representations of C (with respect to S^*) to be those of $\mathrm{Pic}^0(C|_{S^*}) \to S^*$, and define the monodromy groups $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(C \to S, s)$ and $M_{\mathbb{Z}_\ell}(C \to S, s)$ to be the images of these representations. We omit C in these notations when the curve C is clear in context. The monodromy groups do not depend on the choice of S^* by Lemma 6.2.1(2) below — in general, if $X \hookrightarrow Y$ is an open dense embedding, then the induced map of étale fundamental groups is a surjection by [Stacks, 0BN6].

One can generalize such notions of monodromy representations and monodromy groups to families of abelian varieties over algebraic stacks $\mathcal{S}$ by generalizing the formalism of

étale covers over to stacks; note that [28] studies fundamental groups of algebraic stacks by establishing that the category of Galois étale covers of an algebraic stack is a Galois category.

Informally speaking, a "big monodromy theorem" would state that the image of a monodromy representation is "not much smaller" than the linear group that is the codomain of the representation. Some big monodromy results in the literature include those in [43], [48], [2], [18], [20].

In cases of interest, X will be the identity component $\mathrm{Pic}^0_{C/S}$ of the relative Picard group of a proper family of smooth curves over a base scheme S. Given $n \geq 1$, recall from Section 6.1 the construction of Conf_n as the closed subscheme of Conf'_{n+1} with $a_0 = 0$ and as the open subscheme of Conf'_n with $a_0 \neq 0$. Here, let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{\mathrm{prim}}$. Let C_n be the smooth proper curve over $\mathsf{Conf}_n \times_{\mathbb{Z}} \mathbb{Z}[1/d, \zeta_d]$ birational to the plane curve

$$\begin{cases} Y^d = a_1X^n + a_2X^{n-1}W + \cdots + a_{n+1}W^n & \text{if } d \nmid n;\ \text{embed } \mathsf{Conf}_n \text{ into } \mathsf{Conf}'_{n+1} \\ Y^d = a_0X^n + a_1X^{n-1}W + \cdots + a_nW^n & \text{if } d \mid n;\ \text{embed } \mathsf{Conf}_n \text{ into } \mathsf{Conf}'_n. \end{cases} \tag{6.2.2}$$

In either case, the branch locus of C_n as a cover of $\mathbb{P}^1_{[X:W]}$ is of degree n away from $\infty = [1 : 0]$. Moreover, C_n has a $\mathbb{Z}/d\mathbb{Z}$-action where $1 \in \mathbb{Z}/d\mathbb{Z}$ sends $([X : W], Y)$ to $([X : W], \zeta_d Y)$. For any prime ℓ, any $\mathbb{Z}[1/(d\ell), \zeta_d]$-algebra R, and any geometric point s of $\mathsf{Conf}_n \times_{\mathbb{Z}} R$, we have a monodromy representation

$$\pi_1^{\text{ét}}(\mathsf{Conf}_n \times_{\mathbb{Z}} R, s) \to \varprojlim_k \mathrm{Aut}(\mathrm{Pic}^0_{C_n/\mathsf{Conf}_n \times_{\mathbb{Z}} R}[\ell^k]_s) \subseteq \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \tag{6.2.3}$$

where g is the genus of C_n. In fact, the image of the above monodromy representation lies in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ and further lies in $U(V)$ (see Section 4.2 for notation) where V is the $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$-module $T_\ell \mathrm{Pic}^0(C_n|_s)$ equipped with a Hermitian form induced by Proposition 4.1.1 from the Weil pairing ω on V and the $\mathbb{Z}/d\mathbb{Z}$-action on C_n.

We will compare monodromy groups with one another to deduce that the largeness of one implies that of another. We do so by recognizing that monodromy representations

factor one another or, in other words, that monodromy representations respect natural maps of fundamental groups.

Lemma 6.2.1. *Let $T \to S$ be a morphism of irreducible schemes. Let X/S be an abelian scheme. For any geometric point t of T, let s be the induced geometric point of S. For any rational prime ℓ invertible on S, the diagram*

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(T,t) & \longrightarrow & \mathrm{Aut}((X \times_S T)[\ell^k]_t) \\ \downarrow & & \downarrow \cong \\ \pi_1^{\acute{e}t}(S,s) & \longrightarrow & \mathrm{Aut}(X[\ell^k]_s) \end{array}$$

commutes, where the horizontal maps are the mod ℓ^k monodromy representations. Moreover, under the identification $\mathrm{Aut}((X \times_S T)[\ell^k]_t) \cong \mathrm{Aut}(X[\ell^k]_s)$,

1. *The monodromy group of X/S contains the monodromy group of $(X \times_S T)/T$*
2. *If $\pi_1^{\acute{e}t}(T,t) \to \pi_1^{\acute{e}t}(S,s)$ is surjective, then the monodromy group of X/S coincides with the monodromy group of $(X \times_S T)/T$.*

Proof. The action of $\pi_1^{\text{ét}}(S,s)$ on the finite étale cover $X[\ell^k]$ of S naturally induces an action of $\pi_1^{\text{ét}}(T,t)$ on the finite étale cover $X[\ell^k] \times_S T \cong (X \times_S T)[\ell^k]$ of T, so the diagram commutes. In particular, the image of the composed homomorphism

$$\pi_1^{\text{ét}}(T,t) \to \pi_1^{\text{ét}}(S,s) \to \mathrm{Aut}(X[\ell^k]_s)$$

is contained in the image of its factor

$$\pi_1^{\text{ét}}(S,s) \to \mathrm{Aut}(X[\ell^k]_s).$$

If $\pi_1^{\text{ét}}(T,t) \to \pi_1^{\text{ét}}(S,s)$ is surjective, then the images in fact coincide. □

Corollary 6.2.2. *Let S be a normal integral scheme and let $X \to S$ be an abelian scheme. Let η be the generic point of S and let $\bar{\eta}$ be the spectrum of an algebraically closed extension of $K := \kappa(\eta)$. For any rational prime ℓ invertible on S, the monodromy group of the*

representation $\rho_{\eta\to X\times_S\eta,\bar\eta,\mathbb{Z}/\ell^k\mathbb{Z}} : \mathrm{Gal}(\bar K/K) \cong \pi_1^{\acute et}(\eta,\bar\eta) \to \mathrm{Aut}(X[\ell^k]_{\bar\eta})$ *coincides with the monodromy group of* $\rho_{X\to S,\bar\eta,\mathbb{Z}/\ell^k\mathbb{Z}} : \pi_1^{\acute et}(X,\bar\eta) \to \mathrm{Aut}(X[\ell^k]_{\bar\eta})$.

Proof. By Lemma 6.2.1 it suffices to show that the homomorphism $\mathrm{Gal}(\bar K/K) \cong \pi_1^{\text{ét}}(\eta,\bar\eta) \to \pi_1^{\text{ét}}(X,\eta)$ is surjective, which is true by [Stacks, Tag 0BQM]. □

Now let $R = \mathbb{F}_q$ for a prime power q coprime to ℓd. Let η be the generic point of $\mathsf{Conf}_n \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathbb{F}_q$, and write K_n for the function field of η. The embedding $\eta \hookrightarrow \mathsf{Conf}_n \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathbb{F}_q$ induces from (6.2.3) a monodromy representation

$$\pi_1^{\text{ét}}(\eta,\bar\eta) \to \pi_1^{\text{ét}}(\mathsf{Conf}_n \times_{\mathbb{Z}} \mathbb{F}_q,\bar\eta) \to \varprojlim_k \mathrm{Aut}(\mathrm{Pic}^0_{C_n/\mathsf{Conf_n}\times_{\mathbb{Z}}\mathbb{F}_q}[\ell^k]_{\bar\eta})$$

which we identify with the Galois representation

$$\mu : \mathrm{Gal}(\overline{K}_n/K_n) \cong \pi_1^{\text{ét}}(\eta,\bar\eta) \to \varprojlim_k \mathrm{Aut}(\mathrm{Pic}^0_{C_n/K_n}[\ell^k]_{\bar\eta}) \tag{6.2.4}$$

via Lemma 6.2.1. We will need big monodromy results for such Galois representations in the proof of Theorem 6.3.1. Corollary 6.2.2 shows that the monodromy groups of the representations (6.2.3) (after choosing $s = \bar\eta$) and (6.2.4) coincide, so big monodromy results for (6.2.3) are equivalent to those of (6.2.4)

Write V_n for the codomain $\varprojlim_k \mathrm{Aut}(\mathrm{Pic}^0_{C_n/K_n}[\ell^k]_{\bar\eta})$ of the above Galois representation. Note that there is a short exact sequence

$$\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_qK_n) \to \mathrm{Gal}(\overline{K}_n/K_n) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q).$$

The actions of $\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_qK_n)$ and $\mathrm{Aut}(C_n/\mathbb{P}^1_{K_n}) \cong \langle\zeta_d\rangle$ on V_n both preserve the Weil pairing $\omega : V_n \times V_n \to \mathbb{Z}_\ell(1)$. In particular, the Weil pairing induces a Hermitian form via Proposition 4.1.1 on V_n that $\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_qK_n)$ preserves. Recalling notation from Section 4.2, we thus have

$$\mu\left(\mathrm{Gal}\left(\overline{K}_n/\overline{\mathbb{F}}_qK_n\right)\right) \subseteq \mathrm{U}(V_n).$$

Moreover, if F is an element of $\mathrm{Gal}(\overline{K}_n/K_n)$ lying over Frobenius in $\mathrm{Gal}\left(\overline{\mathbb{F}}_q/\mathbb{F}_q\right)$, then $\mu(F)$ lies in $\mathrm{GU}_q(V_n)$. In particular, $\mu(\mathrm{Gal}(\overline{K}_n/K_n)) \subset \mathrm{GU}(V_n)$. Due to Proposition 4.3.7 and its consequences Corollary 4.3.8 and Proposition 4.3.1, big monodromy results that state that the image μ contains $\mathrm{SU}(V_n)$ will suffice for our purposes.

To obtain this desired big monodromy result in the above characteristic p setting, we first use [43] to show that the complex analytic ℓ-adic monodromy representation has large image. The base change of the family C_n defined in (6.2.2) to $\mathbb{C}$ is an algebraic family $f : C_n \otimes \mathbb{C} \to \mathsf{Conf}_n \otimes \mathbb{C}$ of algebraic manifolds, which is a fibration. In general, given a fibration $f : X \to S$ let $f^{-1}(s)$ be a typical fiber of this family. The topological fundamental group $\pi_1(S(\mathbb{C}), s)$ acts on the cohomology group $H^m(f^{-1}(s), \mathbb{Z})$, and this action is called the *monodromy representation on* $H^m(f^{-1}(s), \mathbb{Z})$. In the case that $f : X \to S$ is a family of smooth projective complex algebraic curves and $\ell \neq p$ is a prime, the monodromy representation on $H^1(f^{-1}(s), \mathbb{Z})$ induces an action of $H^1(f^{-1}(s), \mathbb{Z}/\ell^k\mathbb{Z}) \cong H^1(f^{-1}(s), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^k\mathbb{Z}$ compatible with the monodromy representation $\rho_{\mathrm{Pic}^0 X \to S, s, \mathbb{Z}/\ell^k\mathbb{Z}} : \pi_1^{\text{ét}}(S, s) \to \mathrm{Aut}(\mathrm{Pic}^0 X_s[\ell^k])$ defined in (6.2.1) under the identifications $\pi_1^{\text{ét}}(S, s) \cong \pi_1(\widehat{S(\mathbb{C})}, s)$ [16, Exposé XII, Corollaire 5.2] and $\mathrm{Pic}^0 X_s[\ell^k] \cong H^1_{\text{ét}}(X_s, \mathbb{Z}/\ell^k\mathbb{Z}) \cong H^1(X_s(\mathbb{C}), \mathbb{Z}/\ell^k\mathbb{Z})$[1]. Note that $\pi_1(\mathsf{Conf}_n(\mathbb{C}), s) \cong B_n$.

Let $\mathsf{PConf}_n^{\mathbb{A}^1}/\mathbb{Z}$ and $\mathsf{PConf}_n^{\mathbb{P}^1}/\mathbb{Z}$ respectively be the *ordered configuration schemes* of labeled n-tuples of distinct sections of $\mathbb{A}^1$ and $\mathbb{P}^1$. We write PConf_n for $\mathsf{PConf}_n^{\mathbb{A}^1}$. More concretely, these schemes can be constructed as open subschemes of $(\mathbb{A}^1)^n$ and $(\mathbb{P}^1)^n$ described by n-tuples $(p_1, \ldots, p_n)$ where $p_i \neq p_j$ for any $i \neq j$. Note that there is a Galois, étale S_n-cover $\mathsf{PConf}_n^{\mathbb{A}^1} \to \mathsf{Conf}_n$ sending $(p_1, \ldots, p_n)$ to $(X - p_1) \cdots (X - p_n)$. This cover induces a normal injection $\pi_1^{\text{ét}}(\mathsf{PConf}_n, s) \to \pi_1^{\text{ét}}(\mathsf{Conf}_n, s)$ with cokernel S_n. The topological fundamental group $\pi_1(\mathsf{PConf}_n(\mathbb{C}), s)$ is the *pure braid group* P_n. Hence, pulling back the family $f : C_n \otimes \mathbb{C} \to \mathsf{Conf}_n \otimes \mathbb{C}$ of curves over to $\mathsf{PConf}_n \otimes \mathbb{C}$, the monodromy representation of $\pi_1(\mathsf{PConf}_n(\mathbb{C}), s) \cong P_n$ is the restriction of that of $\pi_1(\mathsf{Conf}_n(\mathbb{C}), s) \cong B_n$

[1] To see the identification $\mathrm{Pic}^0 X_s[\ell^k] \cong H^1_{\text{ét}}(X_s, \mathbb{Z}/\ell^k\mathbb{Z})$, note that $H^1_{\text{ét}}(X_s, \mathbb{G}_m) \cong \mathrm{Pic}(X_s)$ [26, Theorem 13.7] and use the long exact sequence in étale cohomology for the Kummer exact sequence $0 \to \mu_\ell \to \mathbb{G}_m \to \mathbb{G}_m \to 0$. The identification $H^1_{\text{ét}}(X_s, \mathbb{Z}/\ell^k\mathbb{Z}) \cong H^1(X_s(\mathbb{C}), \mathbb{Z}/\ell^k\mathbb{Z})$ is by [10, Exposé XVI, Lemme 4.4], cf. [26, Theorem 21.1]

under the injection $P_n \hookrightarrow B_n$.

Note that $\mathsf{PConf}_n^{\mathbb{A}^1}$ is identifiable as the closed subscheme of $\mathsf{PConf}_{n+1}^{\mathbb{P}^1}$ in which the last section is ∞. The induced embedding of complex points is the fiber of $\infty \in \mathbb{P}^1(\mathbb{C})$ of the fibration $\mathsf{PConf}_{n+1}^{\mathbb{P}^1}(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ sending $(p_1, \ldots, p_{n+1})$ to p_{n+1}. This fibration induces an exact sequence $\pi_1(\mathsf{PConf}_n^{\mathbb{A}^1}(\mathbb{C}), s) \to \pi_1(\mathsf{PConf}_{n+1}^{\mathbb{P}^1}(\mathbb{C}), s) \to \pi_1(\mathbb{P}^1(\mathbb{C})) = 1$. Therefore,

Lemma 6.2.3. *The embedding of* $\mathsf{PConf}_n^{\mathbb{A}^1}(\mathbb{C})$ *into* $\mathsf{PConf}_{n+1}^{\mathbb{P}^1}(\mathbb{C})$ *induces a surjection of fundamental groups. By the comparison of topological and étale fundamental groups [16, Exposé XII, Corollaire 5.2], the embedding of* $\mathsf{PConf}_n^{\mathbb{A}^1} \times \mathbb{C} \to \mathsf{PConf}_{n+1}^{\mathbb{P}^1}$ *induces a surjection of étale fundamental groups.*

The following is due to [43, Theorem 1], which follows from [43, Proposition 24] after applying Poincaré duality.

Proposition 6.2.4. *If* $n \geq 2d+1$*, then the image of the monodromy representation of* $\pi_1(\mathsf{Conf}_n(\mathbb{C}), s) \cong B_n$ *on* $H^1(C_n)$ *is a subgroup of finite index in* $U(H^1(C_n))$*.*

Corollary 6.2.5. *For all* $d \geq 2$*, for all* $n \geq 2d+1$*, there exist finitely many prime numbers* $\ell \nmid d$ *such that the closure of the image of* $\pi_1(\mathsf{Conf}_n(\mathbb{C}), s)$ *under the* ℓ*-adic monodromy representation on* $H^1(C_n, \mathbb{Z}_\ell)$ *contains* $\mathrm{SU}(H^1(C_n, \mathbb{Z}_\ell))$*. The same holds with* $\mathsf{PConf}_n^{\mathbb{A}^1}$ *replacing* Conf_n*.*

Proof. Combine Proposition 6.2.4, Proposition 5.3.1, and Lemma 5.3.2. □

In the above statement, the prime numbers ℓ a priori depend on d and n. To prove Theorem 7.0.1 and Theorem 9.0.9 we will need a stronger statement, in which ℓ does not depend on n:

Theorem 6.2.6. *Let* $d \geq 2$ *be an integer. For all but finitely many prime numbers* ℓ*, and for all* $n \geq 2d+1$*, the closure of the image of* $\pi_1(\mathsf{Conf}_n(\mathbb{C}), s)$ *under the* ℓ*-adic monodromy representation on* $H^1(C_n|_s, \mathbb{Z}_\ell)$ *contains* $\mathrm{SU}(H^1(C_n, \mathbb{Z}_\ell))$*. Equivalently,* $M_{\mathbb{Z}_\ell}(\mathsf{Conf}_n \times \mathbb{C}, s) \supseteq \mathrm{SU}(H^1(C_n|_s, \mathbb{Z}_\ell))$*. The same holds with* $\mathsf{PConf}_n^{\mathbb{A}^1}$ *replacing* Conf_n*.*

[2] studies (among other moduli) the moduli $\widetilde{\mathcal{M}}_G$, where $G = \mathbb{Z}/d\mathbb{Z}$ for prime numbers d, parameterizing labeled admissible stable G-curves $(C/S, \iota_0, \eta)$. We are additionally interested in the possibility that $d \geq 2$ is not necessarily a prime number. [2, Lemma 2.2] establishes that $\widetilde{\mathcal{M}}_G$ is a smooth, proper Deligne-Mumford stack over $\operatorname{Spec} \mathbb{Z}[1/d, \zeta_d]$ and the subspace $\widetilde{\mathcal{M}}_G^\circ$ parameterizing smooth curves is open and dense; the lemma in fact holds for any $d \geq 2$. Given a class vector $\gamma : \{1, \ldots, r\} \to \mathbb{Z}/d\mathbb{Z} - \{0\}$ of length r, the substack $\widetilde{\mathcal{M}}_G^\gamma$ of $\widetilde{\mathcal{M}}_G$ for which $(C/S, \iota_0, \eta)$ has class vector γ is an irreducible connected component [2, Lemma 2.3]. In the case that $d \geq 2$ is not necessarily prime, the proof of the lemma generalizes immediately by replacing $\widetilde{\mathcal{M}}_G^{\gamma,\circ}$ with its open and dense subspace of smooth curves C whose r branch points have distinct images in $C/\iota_0(G)$.

Further write $\widetilde{\mathcal{M}}_{g,r}$ for the moduli of triples $(C/S, \Xi, \eta)$ where C/S is a semi-stable curve of genus g, Ξ is a mark of degree r on C such that $(C/S, \Xi)$ is stably marked, and η is a labeling of Ξ. There is a clutching map [23, Definition 3.8]

$$\widetilde{\mathcal{M}}_{g_1,r_1} \times \widetilde{\mathcal{M}}_{g_2,r_2} \to \widetilde{\mathcal{M}}_{g_1+g_2,r_1+r_2-2}$$

which glues curves C_1 and C_2 over S together at the last section of C_1 and the first section of C_2. The composition of $\widetilde{\mathcal{M}}_G^{\gamma_1} \times \widetilde{\mathcal{M}}_G^{\gamma_2} \to \widetilde{\mathcal{M}}_{g_1,r_1} \times \widetilde{\mathcal{M}}_{g_2,r_2}$ with the above clutching map glues two labeled admissible stable G-curves $(C_i/S, \iota_{0,i}, \eta_i)$ to obtain a labeled G-curve C/S with class vector $\gamma = (\gamma_1(1), \ldots, \gamma_1(r_1 - 1), \gamma_2(2), \ldots, \gamma_2(r_2))$. By [11, Proposition 2.2], C/S is equivariantly smoothable if and only if $\gamma_1(r) \equiv -\gamma_2(1) \pmod{d}$, in which case one says that (γ_1, γ_2) *deforms to* γ or that γ *degenerates to* (γ_1, γ_2). Assuming that $\gamma_1(r)$ (and equivalently $\gamma_2(1)$) is relatively prime to d, the covers $C_1 \to C/\iota_{0,1}(G)$ and $C_2 \to C/\iota_{0,2}(G)$ are totally ramified above the branch points corresponding to $\gamma_1(r_1)$ and $\gamma_2(1)$ respectively. In particular, there is exactly one point above each of these branch points, so the clutching map induces a well-defined map

$$\kappa : \widetilde{\mathcal{M}}_G^{\gamma_1} \times \widetilde{\mathcal{M}}_G^{\gamma_2} \to \widetilde{\mathcal{M}}_G^{\gamma}. \tag{6.2.5}$$

[2, Theorem 3.4, Theorem 3.8] use the above clutching map (6.2.5) to prove big monodromy statements for $d = 2, 3$ by inducting on the length of γ. We use these same inductive ideas to prove Theorem 6.2.6, using the results [43] to establish base cases.

Before doing so, let γ_n be the class vector

$$\gamma_n = \begin{cases} (\underbrace{1, \ldots, 1}_{n \text{ times}}, -n \pmod d) & \text{if } n \not\equiv 0 \pmod d \\ (\underbrace{1, \ldots, 1}_{n \text{ times}}) & \text{if } n \equiv 0 \pmod d. \end{cases}$$

Write $(\widetilde{\mathcal{M}}_G^\gamma)^\circ$ for $\widetilde{\mathcal{M}}_G^\gamma \cap \widetilde{\mathcal{M}}_G^\circ$, which is the open and dense subspace of $\widetilde{\mathcal{M}}_G^\gamma$ of smooth curves, and write $(\widetilde{\mathcal{M}}_G^\gamma)^{\max}$ for the open and dense subspace of $\widetilde{\mathcal{M}}_G^\gamma$ of curves whose relative Picard scheme is a family of abelian varieties. By definition, $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\widetilde{\mathcal{M}}_G^\gamma, s)$ is $M_{\mathbb{Z}/\ell^k\mathbb{Z}}((\widetilde{\mathcal{M}}_G^\gamma)^{\max}, s)$. Note that $(\widetilde{\mathcal{M}}_G^\gamma)^{\max}$ includes trees of smooth curves by [4, Example 9.2.8].

There is an embedding $\iota_n : \mathsf{PConf}_n \hookrightarrow (\widetilde{\mathcal{M}}_G^{\gamma_n})^\circ$ sending $(p_1, \ldots, p_n) \in (\mathbb{A}^1)^n$ to the projective curve given by the affine equation $y^d = (x - p_1) \cdots (x - p_n)$; such a curve indeed has class vector γ_n by Proposition 3.2.2. Moreover, the tautological curve over $(\widetilde{\mathcal{M}}_G^{\gamma_n})^\circ$ pulls back to n under ι_n.

Lemma 6.2.7 shows that the embedding $\iota_n \otimes \mathbb{C}$ induces a surjection on étale fundamental groups. Since the embedding $(\widetilde{\mathcal{M}}_G)^\circ \times \mathbb{C} \hookrightarrow (\widetilde{\mathcal{M}}_G^\gamma)^{\max} \times \mathbb{C}$ is open and dense and hence induces a surjection on étale fundamental groups as well, the composed embedding $\mathsf{PConf}_n \otimes \mathbb{C} \hookrightarrow (\widetilde{\mathcal{M}}_G^\gamma)^{\max} \times \mathbb{C}$ also induces a surjection on étale fundamental groups. By Lemma 6.2.1(2), this in turn shows that $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\mathsf{PConf}_n \times \mathbb{C}, s) = M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\widetilde{\mathcal{M}}_G^\gamma \times \mathbb{C}, s)$.

Lemma 6.2.7. *Let $d \geq 2$, and $n \geq 2$ be integers. For any geometric point $s \in \mathsf{PConf}_n \times \mathbb{C}$, the map ι_n induces a surjection on étale fundamental groups.*

Proof. If $n \equiv 0 \pmod d$, then ι_n is an open dense embedding, as the points of PConf_n and correspond exactly with the points of $(\widetilde{\mathcal{M}}_G^{\gamma_n})^\circ$ parameterizing $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1$ unramified above ∞. Therefore, $\iota_n \otimes \mathbb{C}$ induces a surjection on étale fundamental groups [Stacks,

0BN6].

If $n \not\equiv 0 \pmod{d}$, then ι_n is identifiable with the closed embedding $\mathsf{PConf}_n \hookrightarrow \mathsf{PConf}_{n+1}^{\mathbb{P}^1}$ mentioned before Lemma 6.2.3. Note that $\mathsf{PConf}_{n+1}^{\mathbb{P}^1}$ can be identified with $(\widetilde{\mathcal{M}}_G^{\gamma_n})^\circ$ by sending $(p_1, \ldots, p_n, p_{n+1}) \in (\mathbb{P}^1)^n$ to the $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1$ ramified at each p_i with monodromy type $\gamma_n(i)$; the affine equations for such a cover can again be obtained via Proposition 3.2.2. □

Proof of Theorem 6.2.6. By Lemma 6.2.1, it suffices to prove the theorem for PConf_n. For all but finitely many primes ℓ and for all $2d+1 \le n \le 3d+1$, the closure of the image of $\pi_1(\mathsf{PConf}_n(\mathbb{C}), s)$ under the ℓ-adic monodromy representation on $H^1(C_n|_s, \mathbb{Z}_\ell) \cong \mathrm{Pic}^0(C_n|_s)[\ell]$ contains $\mathrm{SU}(H^1(C_n|_s, \mathbb{Z}_\ell))$ by Corollary 6.2.5. Let $\mathcal{L}$ denote this set of all but finitely many primes ℓ. Equivalently, by Lemma 6.2.1(2) and Lemma 6.2.7,

$$M_{\mathbb{Z}_\ell}(\widetilde{\mathcal{M}}_G^{\gamma_n} \times \mathbb{C}, s) \supseteq \mathrm{SU}(T_\ell \,\mathrm{Pic}^0(C_n|_s) \tag{6.2.6}$$

for all $2d+1 \le n \le 3d+1$ and $\ell \in \mathcal{L}$.

Inductively suppose that the containment (6.2.6) holds for all $2d+1 \le n \le m-1$ for some $m \ge 3d+2$. Given class vectors γ_a, γ_b deforming to γ and points $s_i \in \widetilde{\mathcal{M}}_G^{\gamma_i}(\mathbb{C})$ for $i = a, b$, write $s = \kappa(s_a, s_b)$ where κ is the clutching map (6.2.5). [2, Lemma 3.1] (generalized to the case where d is not necessarily prime) shows that $(\kappa \otimes \mathbb{C})^* \,\mathrm{Pic}^0(C^\gamma)[\ell] \cong \mathrm{Pic}^0(\mathcal{C}^{\gamma_1})[\ell] \times \mathrm{Pic}^0(\mathcal{C}^{\gamma_2})[\ell]$ and that $M_{\mathbb{Z}/\ell\mathbb{Z}}(\kappa(\widetilde{\mathcal{M}}_G^{\gamma_a} \times \widetilde{\mathcal{M}}_G^{\gamma_b}), s)$ is a subgroup of $M_{\mathbb{Z}/\ell\mathbb{Z}}(\widetilde{\mathcal{M}}_G^{\gamma}, s)$.

We have a commuting diagram of clutching maps:

$$\begin{array}{ccc} \widetilde{\mathcal{M}}_G^{\gamma_{d+1}} \times \widetilde{\mathcal{M}}_G^{\gamma_{d+1}} \times \widetilde{\mathcal{M}}_G^{\gamma_{m-2d-2}} & \xrightarrow{\kappa_R} & \widetilde{\mathcal{M}}_G^{\gamma_{d+1}} \times \widetilde{\mathcal{M}}_G^{\gamma_{m-d-1}} \\ \downarrow{\scriptstyle \kappa_L} & & \downarrow \\ \widetilde{\mathcal{M}}_G^{\gamma_{2d+2}} \times \widetilde{\mathcal{M}}_G^{\gamma_{m-2d-2}} & \longrightarrow & \widetilde{\mathcal{M}}_G^{\gamma_m}. \end{array}$$

Write $(s_1, s_2, s_3) \in (\widetilde{\mathcal{M}}_G^{\gamma_{d+1}} \times \widetilde{\mathcal{M}}_G^{\gamma_{d+1}} \times \widetilde{\mathcal{M}}_G^{\gamma_{m-2d-2}})(\mathbb{C})$, write $s \in \widetilde{\mathcal{M}}_G^{\gamma_m}$ for the image of (s_1, s_2, s_3), and write V_1, V_2, V_3, V be $\mathrm{Pic}^0(C)[\ell]$ for the curves C parameterized by s_1, s_2, s_3, s respectively. We then have the decomposition $V \cong V_1 \perp V_2 \perp V_3$ as Hermitian spaces. By the inductive hypothesis, $M_{\mathbb{Z}/\ell\mathbb{Z}}(\widetilde{\mathcal{M}}_G^{\gamma_{2d+2}})$ and $M_{\mathbb{Z}/\ell\mathbb{Z}}(\widetilde{\mathcal{M}}_G^{\gamma_{m-d-1}})$ respectively

contain the $\mathrm{SU}(V_1 \perp V_2)$ and $\mathrm{SU}(V_2 \perp V_3)$. By [2, Lemma 3.2(b)(ii)], $M_{\mathbb{Z}/\ell\mathbb{Z}}(\widetilde{\mathcal{M}}_G^{\gamma_m}) \supseteq \mathrm{SU}(V)$. A subgroup of $\mathrm{SU}(\mathbb{Z}_\ell)$ surjecting onto $\mathrm{SU}(\mathbb{Z}/\ell)$ is $\mathrm{SU}(\mathbb{Z}_\ell)$ itself (see the proofs of [2, Corollary 3.5, Corollary 3.10]), so in fact $M_{\mathbb{Z}_\ell}(\widetilde{\mathcal{M}}_G^{\gamma_m}) \supseteq \mathrm{SU}(T_\ell \operatorname{Pic}^0(C_n|_s))$. □

Now we convert the big monodromy result of Theorem 6.2.6 into characteristic p by appealing to the theory of tamely ramified fundamental groups.

Proposition 6.2.8. *Let $d \geq 2$, and $n \geq 2$ be integers. Given a prime number $\ell \nmid d$ and a prime number $p \nmid d\ell$, we have $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\mathsf{PConf}_n \times \mathbb{C}) \subseteq M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p)$.*

Proof. A Künneth formula [36, Lemma 16.1.2] shows that $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \mathbb{C}, s) \cong \pi_1^{\text{ét}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}, s) \cong \pi_1^{\text{ét}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, s)$, where s is a $\overline{\mathbb{Q}}$-point of PConf_n.

Moreover, [15, Lemma 7.6] constructs a smooth and proper compactification X_n[2] of PConf_n over $\mathbb{Z}$ such that $X_n \setminus \mathsf{PConf}_n$ is a relative normal crossings divisor. As per [16, Exposé XIII, 2.1.0, 2.1.3], one defines from the open embeddding $\mathsf{PConf}_n \hookrightarrow X_n$ the tamely ramified fundamental groups π_1^{tr} of PConf_n over base schemes S. In particular, $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, s) \cong \pi_1^{\text{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, s)$ as all ramifications are tame in characteristic 0.

Write $\mathbb{Z}_p^{\text{unr}}$ for the valuation ring of $\mathbb{Q}_p^{\text{unr}}$. Given a specialization $\bar{s}_1 \to \bar{s}_2$ of geometric points of $\mathbb{Z}_p^{\text{unr}}$, we have a specialization morphism [16, Exposé XIII, 2.10]

$$\pi_1^{\text{tr}}(\mathsf{PConf}_{n,\bar{s}_1}, a_1) \to \pi_1^{\text{tr}}(\mathsf{PConf}_n \times \mathbb{Z}_p^{\text{unr}}, a_1) \xrightarrow{\cong} \pi_1^{\text{tr}}(\mathsf{PConf}_n \times \mathbb{Z}_p^{\text{unr}}, a_2) \xleftarrow{\cong} \pi_1^{\text{tr}}(\mathsf{PConf}_{n,\bar{s}_2}, a_2).$$

where a_i is a geometric point of $\mathsf{PConf}_{n,\bar{s}_i} = \mathsf{PConf}_n \times \bar{s}_i$ for $i = 1, 2$. Letting $\overline{s}_1 = \operatorname{Spec} \overline{\mathbb{Q}_p^{\text{unr}}} = \operatorname{Spec} \overline{\mathbb{Q}}_p$ and $\overline{s}_2 = \operatorname{Spec} \overline{\mathbb{F}}_p$, this specialization morphism is a morphism $\pi_1^{\text{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, a_1) \to \pi_1^{\text{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p, a_2)$.

We show that the mod ℓ^k-monodromy representations of PConf_n (over a base scheme S of characteristic not ℓ such that $\mathsf{PConf}_n \times S$ is a normal integral scheme) factor through the natural surjections $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times S, s) \to \pi_1^{\text{tr}}(\mathsf{PConf}_n \times S, s)$, i.e. that these representations are tamely ramified in X_n. Since $\operatorname{Pic}^0(C_n/\mathsf{PConf}_n \times S)$ is an abelian scheme, $J[\ell] :=$

[2] Not to be confused with the Hurwitz scheme which we have been denoting as $\mathbf{X}_n$.

$\mathrm{Pic}^0(C_n/\mathsf{PConf}_n \times S)[\ell]$ is finite étale over $\mathsf{PConf}_n \times S$. For $J[\ell]$ to be tamely ramified along $X_n \setminus \mathsf{PConf}_n$ would mean the following [40, Definition 5.7.1.5]: for each divisor D of X not in PConf_n and for each connected component Y of $J[\ell]$, the closed points of the normalization of $\mathrm{Spec}(\mathcal{O}_{X_n,D})$ in the function field $K(Y)$ has ramification indices prime to the characteristic of $\kappa(D)$. Take $T \to \mathsf{PConf}_n \times S$ to be the normalization of the compositum extension of the function fields of the connected components of $J[\ell]$. In particular, $J[\ell] \times_S T \cong \mathbb{Z}/\ell\mathbb{Z}^{2g}$ as abelian schemes over T where g is the genus of C_n. Thus, the ramification index of $\mathrm{Spec}(\mathcal{O}_{X_n,D})$ in $K(T)$ must divide ℓ^{2g} and hence the same must be true of any ramification index of $\mathrm{Spec}(\mathcal{O}_{X_n,D})$ in any $K(Y)$. Since S is assumed to be of characteristic not ℓ, $J[\ell]$ is tamely ramified along$X_n \setminus \mathsf{PConf}_n$. We apply this to $S = \mathbb{Q}_p^{\mathrm{unr}}, \mathbb{Z}_p^{\mathrm{unr}}, \overline{\mathbb{F}}_p$.

To summarize, we have the following sequence of group homomorphisms all of which have compatible mod ℓ^k-monodromy representations:

$$\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \mathbb{C}, s) \xrightarrow{\cong} \pi_1^{\text{ét}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, s) \to \pi_1^{\mathrm{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{Q}}_p, s) \to \pi_1^{\mathrm{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p, s').$$

The image of $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \mathbb{C}, s)$ under its monodromy representation is thus contained in the image of $\pi_1^{\mathrm{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p, s')$ under its monodromy representation. The former image is $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\mathsf{PConf}_n \times \mathbb{C})$. Since $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p, s')$ naturally surjects onto $\pi_1^{\mathrm{tr}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_p, s')$, the latter image equals $M_{\mathbb{Z}/\ell^k\mathbb{Z}}(\mathsf{PConf}_n \times \overline{\mathbb{F}}_q)$. □

Corollary 6.2.9. *Let $d \geq 2$. For all but finitely many primes $\ell \nmid d$, for all $n \geq 2d+1$, and for any prime power q coprime to ℓd, we have*

$$\mu(\mathrm{Gal}(\overline{K}_n/\bar{\mathbb{F}}_q K_n)) \supseteq \mathrm{SU}(V_n),$$

where K_n and μ are as in (6.2.4).

Proof. By Corollary 6.2.2, the image of μ coincides with the monodromy group $M_{\mathbb{Z}_\ell}(\mathsf{Conf}_n \times \bar{\mathbb{F}}_q)$. By Theorem 6.2.6 and Proposition 6.2.8, $M_{\mathbb{Z}_\ell}(\mathsf{PConf}_n \times \bar{\mathbb{F}}_q)$ contains $\mathrm{SU}(V_n)$. The morphism $\mathsf{PConf}_n \to \mathsf{Conf}_n$, which forgets the ordering of each configuration, induces a ho-

momorphism $\pi_1^{\text{ét}}(\mathsf{PConf}_n \times \bar{\mathbb{F}}_q, \bar{s}) \to \pi_1^{\text{ét}}(\mathsf{Conf}_n \times \bar{\mathbb{F}}_q, \bar{s})$ and hence an inclusion $M_{\mathbb{Z}_\ell}(\mathsf{PConf}_n \times \bar{\mathbb{F}}_q) \subseteq M_{\mathbb{Z}_\ell}(\mathsf{Conf}_n \times \bar{\mathbb{F}}_q)$. Therefore, $M_{\mathbb{Z}_\ell}(\mathsf{Conf}_n \times \bar{\mathbb{F}}_q)$ contains $\mathrm{SU}(V_n)$.

□

6.3 Counting surjections from class groups

Recall some notation at the start of Section 6.2. We first state Theorem 6.3.1 by including a big monodromy condition as an assumption in the hypothesis. We then state Corollary 6.3.2, which applies Corollary 6.2.9 to Theorem 6.3.1 to remove the big monodromy condition in the hypothesis at the cost of restrictions on d, ℓ, and n. If future works should strengthen the big monodromy results of Section 6.2 by allowing for more general combinations of d, ℓ, and n, then Corollary 6.3.2 can be strengthened as well.

Theorem 6.3.1. *Let $d \geq 3$ be an integer, let ℓ be a prime number not dividing d, and let $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$. Fix A to be a $\mathbb{Z}_\ell[\zeta_d]$-module of finite cardinality. There are constants $B_{d,\ell,A}$, $C_{d,\ell,A}$, and $N_{d,\ell,A}$ such that*

$$\left| \frac{\sum_{L \in \mathfrak{S}_n} m_A(L)}{|\mathfrak{S}_n|} - 1 \right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}}$$

for all n,q such that

- *n is relatively prime to d,*
- *$q \equiv 1 \pmod{d}$ is a prime power,*
- *$\sqrt{q} > 2B_{d,\ell,A}$, $n \geq N_{d,\ell,A}$,*
- *ℓ does not divide $2dq(q-1)$, and*
- *$\mathrm{SU}(V_n) \subseteq \mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n))$.*

In fact, it suffices for $N_{d,\ell,A} = 2r + 3$ if A is a quotient of $\mathbb{Z}_\ell[\zeta_d]^{\oplus r}$.

Corollary 6.3.2. *Let $d \geq 3$ be an integer. For all but finitely many prime numbers $\ell \nmid d$, for any module A of finite cardinality for the ring $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$, there are constants $B_{d,\ell,A}$, $C_{d,\ell,A}$, and $N_{d,\ell,A}$ such that*

$$\left| \frac{\sum_{L \in \mathfrak{S}_n} m_A(L)}{|\mathfrak{S}_n|} - 1 \right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}}$$

for all n,q such that

- *n is relatively prime to or divisible by d,*
- *$q \equiv 1 \pmod{d}$ is a prime power,*
- *$\sqrt{q} > 2B_{d,\ell,A}$, $n \geq N_{d,\ell,A}$, and*
- *ℓ does not divide $2dq(q-1)$.*

In fact, it suffices for $N_{d,\ell,A} = \max(2d+1, 2r+3)$ if A is a quotient of $\mathbb{Z}_\ell[\zeta_d]^{\oplus r}$.

Remark 6.3.3. In the proof of Theorem 6.3.1 below, note that the condition $n \geq 2r+3$ is used to apply Corollary 4.3.8.

Remark 6.3.4. The below proof of Theorem 6.3.1 is based on the that of [15, Theorem 8.8]. The main difference between the two proofs is that the former proof needs to account for ζ_d-actions in general whereas the latter proof only needs to do so for $d = 2$, i.e. when $\zeta_d = -1$. In particular, the latter proof counts surjections between $\mathbb{Z}_\ell$-modules and the former proof counts surjections between modules over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq -1}$. Moreover, the ℓ-adic Weil pairing on $\mathrm{Jac}(C_L)$, where C_L is the $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1$ corresponding to a imaginary $\mathbb{Z}/d\mathbb{Z}$-extension L of $\mathbb{F}_q(t)$, is a symplectic pairing $\omega : T_\ell \mathrm{Jac}(C_L) \times T_\ell \mathrm{Jac}(C_L) \to \mathbb{Z}_\ell(1)$ that is also preserved by the ζ_d action, i.e. $\omega(\zeta_d v, \zeta_d w) = \omega(v, w)$. Such a symplectic pairing gives rise to a Hermitian pairing by Proposition 4.1.1 since $T_\ell \mathrm{Jac}(C_L)$ is a $\mathbb{Z}_\ell[\zeta_d]$-module by Lemma 4.1.8. In contrast, the ℓ-adic Weil pairing for the Jacobian of a hyperelliptic curve is merely a symplectic pairing.

Proof of Theorem 6.3.1. Let H^i denote ith étale cohomology group and let H^i_c denote the the ith compactly supported étale cohomology group.

Note that if A is the trivial group, then the LHS of the desired inequality is 0. Now assume that A is nontrivial.

Let G and c be as in Proposition 6.1.3. In particular, there is a bijection between $\mathbf{X}_n(\mathbb{F}_q)$ and the set of isomorphism classes of pairs (L, α) as stated in the proposition. Each isomorphism class of (L, α) has d elements; the automorphisms of $L/\mathbb{F}_q(t)$ act simply transitively on such an isomorphism class, so

$$\sum_{L \in \mathfrak{S}_n} m_A(L) = d|\mathbf{X}_n(\mathbb{F}_q)|.$$

We count $\mathfrak{S}_n$. To exhaust $\mathfrak{S}_n$, it is sufficient to let f range through a set of representatives for squarefree polynomials of degree n up to the multiplication action of $(\mathbb{F}_q^*)^d$. The number of monic squarefree polynomials of degree n with coefficients in $\mathbb{F}_q$ is equal to $q^n - q^{n-1}$ [5, 4, equation (vi)]. Since $q \equiv 1 \pmod{d}$, the cubic elements form an index d subgroup of $\mathbb{F}_q^*$. Therefore,

$$|\mathfrak{S}_n| = d(q^n - q^{n-1})$$

and hence the LHS of the desired inequality equals

$$\left| \frac{|\mathbf{X}_n(\mathbb{F}_q)|}{q^n - q^{n-1}} - 1 \right|.$$

It thus suffices to show that

$$\left| \frac{|\mathbf{X}_n(\mathbb{F}_q)|}{q^n} - 1 \right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}} \tag{6.3.1}$$

when n and q are sufficiently large relative to A.

Let $\overline{\mathbf{X}}_n := \mathbf{X}_n \times \bar{\mathbb{F}}_q$. Recall that G is center-free by Lemma 4.1.8. Moreover, c is a q-rational conjugacy class of G because $q \equiv 1 \pmod{d}$, and it is non-splitting by Lemma 2.0.5. As per Remark 6.1.1, an appropriate generalization of [15, Proposition 7.8] applies to $\mathbf{X}_n$ and additionally applying Poincaré's duality for the smooth n-dimensional

variety $\overline{\mathbf{X}}_n$, there are constants $K(A)$ and $B_{d,\ell,A}$ such that [3]

$$\dim H_c^{2n-i}\left(\overline{\mathbf{X}}_n, \mathbb{Q}_\lambda\right) = \dim H^i\left(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda\right) \leq K(A) \cdot B_{d,\ell,A}^i \tag{6.3.2}$$

for all $i > 0$ as long as λ is a prime greater than $\max(|G|, q, n)$ — for example, it suffices to take $K(A), B_{d,\ell,A} = C(G, c)$ in the notation of [15, Section 7.8.1].

Deligne [8] proved that the absolute value of every eigenvalue of the geometric Frobenius Frob_q on compactly supported H_c^j of a smooth variety is bounded above by $q^{j/2}$. Consequently,

$$\begin{aligned}
\left| q^{-n} \sum_{j<2n} (-1)^j \operatorname{Tr}(\mathrm{Frob}_q \,|H_c^j(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda)) \right| &\leq q^{-n} \sum_{j=0}^{2n-1} q^{j/2} \dim H_c^j(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda) \\
&\leq q^{-n} K(A) \sum_{j=0}^{2n-1} B_{d,\ell,A}^{2n-j} q^{j/2} \\
&\leq K(A) \sum_{k=1}^{\infty} \left(\frac{B_{d,\ell,A}}{\sqrt{q}}\right)^k \\
&= K(A) \cdot \frac{\frac{B_{d,\ell,A}}{\sqrt{q}}}{1 - \frac{B_{d,\ell,A}}{\sqrt{q}}}.
\end{aligned}$$

The last quantity is at most $2\frac{K(A)B_{d,\ell,A}}{\sqrt{q}}$ when $\frac{B_{d,\ell,A}}{\sqrt{q}} \leq \frac{1}{2}$. Let $C_{d,\ell,A} = 2K(A)B_{d,\ell,A}$ so that

$$\left| q^{-n} \sum_{j<2n} (-1)^j \operatorname{Tr}(\mathrm{Frob}_q \,|H_c^j(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda)) \right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}} \tag{6.3.3}$$

whenever $\sqrt{q} \geq 2B_{d,\ell,A}$.

We now show, assuming that $n \geq 2r + 3$, that

$$\operatorname{Tr}(\mathrm{Frob}_q \,|H_c^{2n}(\overline{\mathbf{X}}_n; \mathbb{Q}_\lambda)) = q^n.$$

By Poincaré duality, this is equivalent to the statement that there is exactly one $\mathbb{F}_q$-

[3] Even though $\mathbf{X}_n$ is not the same as $\mathsf{Hn}_{G,n}^c$ when $d \mid n$, the inequality still applies since $\mathbf{X}_n$ is the union of some connected components of $\mathsf{Hn}_{G,n}^c$ in this case.

rational connected component of $\overline{\mathbf{X}}_n$. This, together with the Lefschetz trace formula and the bound (6.3.3) will imply (6.3.1).

Let η be the generic point of $\mathsf{Conf}_n \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{F}_q$ and let K_n be its function field. The étale cover $\mathbf{X}_n \to \mathsf{Conf}_n \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{F}_q$ is determined by a geometric generic fiber Σ of η together with the action of $\operatorname{Gal}(\bar{K}_n/K_n)$ on that fiber. Associated to the Galois group is a short exact sequence

$$1 \to \operatorname{Gal}(\bar{K}_n/\overline{\mathbb{F}}_q K_n) \to \operatorname{Gal}(\bar{K}_n/K_n) \to \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to 1.$$

Thus, there is exactly one $\mathbb{F}_q$-rational connected component of $\mathbf{X}_n$ if and only if only one $\operatorname{Gal}(\bar{K}_n/\overline{\mathbb{F}}_q K_n)$-orbit of Σ is preserved by the action of $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, which we prove by expressing Σ in a different way. Recall the construction of Conf_n as the subscheme of Conf'_{n+1} with $a_0 = 0$.

By abuse of notation, let C_n denote the base change of the curve notated as C_n in Section 6.2 over K_n. Choose k sufficiently large so that $\ell^k A = 0$. Let $V_{n,k}$ be the ℓ^k-torsion points of the Jacobian $\operatorname{Jac}(C_n)$ over $\bar{K}_n$. Then $V_{n,k} \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^{2g}$ as a $\mathbb{Z}/\ell^k\mathbb{Z}$-module, where g is the genus of C_n. Note that $g = \frac{(m-2)(d-1)}{2}$ by the Riemann-Hurwitz formula where m is the branch locus degree of $C_n \to \mathbb{P}^1$, i.e. $m = \begin{cases} n+1 & \text{if } d \nmid n \\ n & \text{if } d \mid n \end{cases}$. Moreover, we have a mod-ℓ^k monodromy representation

$$\mu_{\ell^k} : \operatorname{Gal}(\bar{K}_n/K_n) \to \operatorname{Aut}(V_{n,k})$$

which factors the Galois/monodromy representation μ from (6.2.4). Letting L be the function field of C_n, there is also an action of $\operatorname{Aut}(C_n/\mathbb{P}^1) \cong \operatorname{Gal}(L/K_n(t))$ on $V_{n,k}$ induced by the action on C_n. Identify the automorphism/Galois group with $\langle\zeta_d\rangle \cong \mathbb{Z}/d\mathbb{Z}$ so that $V_{n,k}$ is a $(\mathbb{Z}/\ell^k\mathbb{Z})[\zeta_d]$-module (and in fact a $\mathbb{Z}_\ell[\zeta_d]$-module) by Lemma 4.1.8.

Now consider the set $\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(V_{n,k}, A)$ of surjective homomorphisms from $V_{n,k}$ to A as $\mathbb{Z}_\ell[\zeta_d]$-modules. This set carries a natural action of $\operatorname{Gal}(\bar{K}_n/K_n)$ derived from μ_{ℓ^k}.

Since Conf_n is a moduli scheme for degree-n squarefree divisors on $\mathbb{A}^1$, there is a universal such divisor on $\mathbb{A}^1/\mathsf{Conf}_n$, which restricts to a canonical degree-n squarefree (i.e. reduced) divisor D on $\mathbb{A}^1/\bar{K}_n$. The set $\mathbf{X}_n(\bar{K}_n)$ of tame G-covers of $\mathbb{A}^1/\bar{K}_n$ branched at D (which is to say Σ) is naturally identified with $\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(V_{n,k}, A)$ by the argument of Proposition 6.1.3, equivariantly for the action of $\mathrm{Gal}(\bar{K}_n/K_n)$ on both sides (The statement of class field theory of Equation (6.1.3) needs to be replaced with the fact that the abelian étale covers of $C_n/\overline{K}$ with Galois group A are classified by surjections $\mathrm{Jac}(C_n)[\ell^k](\overline{K}) \twoheadrightarrow A$, see e.g. [22, (2.4)]).

To summarize, the geometric components of $\overline{X}_n/\overline{\mathbb{F}}_q$ are in bijection with the $\mathrm{Gal}\left(\overline{K}_n/\overline{\mathbb{F}}_q K_n\right)$-orbits on $\mathrm{Sur}(V_{n,k}, A)$. It thus suffices to show that exactly one $\mathrm{Gal}\left(\overline{K}_n/\overline{\mathbb{F}}_q K_n\right)$-orbit on $\mathrm{Sur}(V_{n,k}, A)$ is preserved by the action of $\mathrm{Gal}\left(\overline{\mathbb{F}}_q/\mathbb{F}_q\right)$ (again, for n large enough). Moreover, an orbit O is defined over $\mathbb{F}_q$ if and only if the stabilizer in $\mathrm{GU}(V_{n,k})$ of some, equivalently every, $x \in O$ has nontrivial intersection with $\mathrm{GU}_q(V_{n,k})$.

By assumption, $\mathrm{SU}(V_{n,k}) \subseteq \mu_{\ell^k}(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n))$. Moreover, since $\ell^k A = 0$, the pullback via $V_n \to V_{n,k}$ identifies $\mathrm{Sur}(V_{n,k}, A)$ with $\mathrm{Sur}(V_n, A)$. It thus suffices to show that there is a unique $\mathrm{SU}(V_n)$-orbit on $\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(V_n, A)$ defined over $\mathbb{F}_q$ when n is sufficiently large. This follows from Corollary 4.3.8 for $n \geq 2r + 3$. □

We also identify sufficient values for the constants $B_{d,\ell,A}$ and $C_{d,\ell,A}$ afforded by Corollary 6.2.9. While we do not use these values for Chapter 7, we will need them for Chapter 9.

Proposition 6.3.5 (cf. [13, Proposition 2.7])**.** *Corollary 6.3.2 holds for the constants* $B_{d,\ell,A} = (2d|A|)^{39d+18}$ *and* $C_{d,\ell,A} = 2 \cdot (2d|A|)^{69d+31}$.

Proof. Recall that the proof of Theorem 6.3.1 uses constants $K(A)$ and $B_{d,\ell,A}$ such that the bound (6.3.2) holds.

In turn, this bound comes from a stability theorem [15, Theorem 6.2] and an absolute cohomological bound [15, Proposition 2.5]. The stability theorem implies that there exist constants α, β, δ dependent on d and ℓ such that

$$\dim H^i_{\text{ét}}(X^a_n \times \overline{\mathbb{F}}_q; \mathbb{Q}_\lambda) = \dim H^i_{\text{ét}}(X^a_{n+\delta} \times \overline{\mathbb{F}}_q; \mathbb{Q}_\lambda)$$

whenever $n > \alpha i + \beta$. Furthermore, the absolute bound (along with some comparison results between the cohomologies of Hurwitz schemes over $\mathbb{C}$ and $\overline{\mathbb{F}}_q$ explained more in detail in the proof of [15, Proposition 7.8]) tells us that

$$\dim H^i_{\text{ét}}(X^a_n \times \overline{\mathbb{F}}_q; \mathbb{Q}_\lambda) \leq (2|A \rtimes \mathbb{Z}/d\mathbb{Z}|)^n = (2d|A|)^n.$$

These imply that

$$\dim H^i_{\text{ét}}(X^a_n \times \overline{\mathbb{F}}_q; \mathbb{Q}_\lambda) \leq (2d|A|)^{\alpha i + \beta + \delta}$$

for every n.

We now obtain more concrete values of α, β, and δ using the ideas presented in the proof of [13, Proposition 2.7] and details which we prove in Section 10.4. The proof shows that $\alpha = 3A_0$, $\beta = 2A_0 + A_2$, and $\delta = \deg U_D$ suffice with the following assignments and lower bounds:

- U_D is defined in (10.4.1); $D = 1$ suffices by Lemma 10.4.2, in which case $\deg U_D = d$.
- $A(R) = \max(\deg \ker U_D, \deg \operatorname{coker} U_D)$, which is at most $2d + 1$ by Lemma 10.4.2.
- $A_0 = 6A(R) + \deg U_D \leq 13d + 6$.
- $A_2 = A(R) + \deg U_D \leq 3d + 1$.

In particular, it suffices for α, β, and δ to be $39d + 18$, $29d + 13$, and d respectively.

Thus, $B_{d,\ell,A} = (2d|A|)^\alpha = (2d|A|)^{39d+18}$ and $K(A) = (2d|A|)^{\beta+\delta} = (2d|A|)^{30d+13}$ suffice. Recall that we let $C_{d,\ell,A} = 2K(A)B_{d,\ell,A}$ in the proof of Theorem 6.3.1, so $C_{d,\ell,A} = 2 \cdot (2d|A|)^{69d+31}$ suffices. □

Chapter 7

Cohen-Lenstra distribution for imaginary $\mathbb{Z}/d\mathbb{Z}$-extensions of $\mathbb{F}_q(t)$

Using Theorem 6.3.1, we can prove Theorem 7.0.1. Just as how [15, Main Theorem, Theorem 1.2] uses [15, Theorem 8.8] and Proposition [15, Proposition 8.3], we will require Proposition 7.0.5, which is a statement about probability measures similar to [15, Proposition 8.3]. The module-theoretic ideas used to prove [15, Proposition 8.3] readily generalize to prove Proposition 7.0.5. We nevertheless record the details for completeness. Compare this relative ease of generalization against the difficulties towards proving Proposition 4.3.1 and Corollary 4.3.8 — where the theory of Hermitian forms was used to generalize the ideas using the theory of symplectic forms in [15, Lemma 8.9] — cf. the discussion at the start of Section 4.3.

Throughout this section, write $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ when $d \geq 2$ is an integer and $\ell \nmid d$ is a prime number. Further write $\mathcal{L}_{d,\ell}$ for the set of isomorphism classes of $\mathbb{Z}_\ell[\zeta_d]$-modules with finite cardinality. In particular, such a module has an action of $\langle \zeta_d \rangle$ and its ζ_d-invariant submodule is trivial by Corollary 2.0.3. Write $C_{d,\ell} = \left(\sum_{[A] \in \mathcal{L}} \frac{1}{\mathrm{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(A)} \right)^{-1}$, which converges (see [7, Théorème 3.6] and cf. [44, Remark 3.4 and the discussion between Definition 6.1 and Theorem 6.2]). The *Cohen-Lenstra distribution* $\mu_{d,\ell}$ in the case of interest is the probability distribution on $\mathcal{L}$ such that the $\mu_{d,\ell}$-mass on the isomorphism

class of A equals $\frac{C_{d,\ell}}{|\operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(A)|}$.

As with Theorem 6.3.1, we first state Theorem 7.0.1 to include a big monodromy condition in the hypothesis and then apply Corollary 6.2.9 to state Corollary 7.0.2. Again, if Corollary 6.2.9 can be strengthened to include more combinations of d, ℓ, and n, then Corollary 7.0.2 can be strengthened as well.

Theorem 7.0.1. *Let $d \geq 3$ be an integer, and let ℓ be a prime number not dividing $2d$. Fix $[A] \in \mathcal{L}_{d,\ell}$. Assuming that $\mathrm{SU}(V_n) \subseteq \mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n)$ for all sufficiently large n, write δ^+ and δ^- respectively for the following upper and lower densities of totally imaginary $\mathbb{Z}/d\mathbb{Z}$ extensions L of $\mathbb{F}_q(t)$ for which the ℓ-part of the class group is isomorphic to A under an isomorphism equivariant for the $\langle\zeta_d\rangle \cong \mathrm{Gal}(L/\mathbb{F}_q(t))$ actions on A and $(\mathrm{Cl}_L)_\ell$:*

$$\delta^+(q) = \limsup_{\substack{n\to\infty \\ \gcd(n,d)=1 \\ \mathrm{SU}(V_n)\subseteq\mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n)}} \frac{\sum_{L\in\mathfrak{S}_n} \iota(L)}{|\mathfrak{S}_n|}$$

$$\delta^-(q) = \liminf_{\substack{n\to\infty \\ \gcd(n,d)=1 \\ \mathrm{SU}(V_n)\subseteq\mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n)}} \frac{\sum_{L\in\mathfrak{S}_n} \iota(L)}{|\mathfrak{S}_n|}.$$

Here, $\iota(L)$ is 1 if $(\mathrm{Cl}_L)_\ell$ is isomorphic to A as a $\mathbb{Z}_\ell[\zeta_d]$-module and is 0 otherwise.

Then, $\delta^+(q)$ and $\delta^-(q)$ converge, as $q \to \infty$ with $\ell \nmid 2dq(q-1)$ and $q \equiv 1 \pmod{d}$, to $\mu_{d,\ell}([A]) = \frac{C_{d,\ell}}{|\operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(A)|}$.

Corollary 7.0.2. *Let $d \geq 3$ be an integer. For all but finitely many primes ℓ not dividing $2d$, for any $[A] \in \mathcal{L}_{d,\ell}$, write δ^+ and δ^- as in Theorem 7.0.1. Then $\delta^+(q)$ and $\delta^-(q)$ converge, as $q \to \infty$ with $\ell \nmid 2dq(q-1)$ and $q \equiv 1 \pmod{d}$, to $\mu_{d,\ell}([A]) = \frac{C_{d,\ell}}{|\operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(A)|}$.*

Theorem 7.0.3 asserts that $\mu_{d,\ell}$ is characterized as the probability measure μ on $\mathcal{L}_{d,\ell}$ for which the expected number of surjections from a μ-random module onto a fixed module A_0 equals 1, cf. [15, Lemma 8.2] for a similar statement for finite abelian ℓ-groups.

Theorem 7.0.3. *Let $d \geq 2$ be an integer, let ℓ be a prime number, and let μ be a probability*

distribution on $\mathcal{L}_{d,\ell}$. Then, $\mu = \mu_{d,\ell}$ if and only if

$$\mathbb{E}(|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(A, A_0)|) = 1 \tag{7.0.1}$$

for every $[A_0] \in \mathcal{L}_{d,\ell}$ where $[A]$ is the random variable valued in $\mathcal{L}_{d,\ell}$ with probability distribution μ.

Proof. [44, Theorem 6.2], applied to the case where $A = \mathbb{Q}[\zeta_d]_{\zeta_d \neq 1}$, $S = \{\ell\}$, $\mathfrak{O} = \mathbb{Z}_{(\ell)}[\zeta_d]$ (here, $\mathbb{Z}_{(\ell)}$ is the localization of $\mathbb{Z}$ at the prime ideal (ℓ)), $\underline{u} = (0, \ldots, 0)$ according to the notations in loc. cit. , establishes that (7.0.1) holds when $\mu = \mu_{d,\ell}$. Additionally letting $X_n = [A]$ in [44, Theorem 6.11] shows that (7.0.1) implies $\mu = \mu_{d,\ell}$. □

Lemma 7.0.4 (cf. [15, Lemma 8.4])**.** *Let $d \geq 2$ be an integer and let ℓ be a prime number not dividing d. Given $\epsilon > 0$ and $[A] \in \mathcal{L}_{d,\ell}$, there exists a constant $c(A)$ and a finite subset $M \subset \mathcal{L}$ so that, whenever $|X| > c(A)$*

$$|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A)| \leq \epsilon \frac{\sum_{A' \in M} |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')|}{|M|}.$$

Proof. Define a *basic enlargement* of A to be an A' for $[A'] \in \mathcal{L}_{\ell,d}$ that admits a $\mathbb{Z}_\ell[\zeta_d]$-surjection $A' \twoheadrightarrow A$ with kernel isomorphic to the residue field $\kappa(B_i)$ of a factor B_i of $\mathbb{Z}_\ell[\zeta_d]$ as in (4.1.9). We show for any $[X] \in \mathcal{L}_{d,\ell}$ with a $\mathbb{Z}_\ell[\zeta_d]$-surjection onto A such that $|X| > |A|$ and for any quotient A' of X that is a basic enlargement of A that

$$|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')| \geq (\ell^s - 1)|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A)|$$

where $\ell^s = \frac{|A'|}{|A|} = |\kappa(B_i)|$; in particular, $s \leq d - 1$. Given such an X and an A', fix surjections $\pi : A' \twoheadrightarrow A$ and $f : X \twoheadrightarrow A'$. We show that there are at least $\ell^s - 1$ surjective lifts $\tilde{f} : X \twoheadrightarrow A'$ of f with respect to π.

1. If A' is not isomorphic to $A \times \kappa(B_i)$ for any factor B_i of $\mathbb{Z}_\ell[\zeta_d]$ as in (4.1.9), then any lift $\tilde{f} : X \to A'$ is surjective, and the set of lifts is a principal homogeneous space of $\operatorname{Hom}_{\mathbb{Z}_\ell[\zeta_d]}(X, A'/A)$. The set of lifts is also nonempty by the choice of A'

and $A'/A \simeq \kappa(B_i)$, so there are at least $|\operatorname{Hom}_{\mathbb{Z}_\ell[\zeta_d]}(X, A'/A)|$ lifts and hence at least $|\kappa(B_i)| = \ell^s$ lifts.

2. If A' is isomorphic to $A \times \kappa(B_i)$ for some B_i, then the B_i-component of $\ker(f)$ cannot be contained in $\lambda_i X_i$ where λ_i is a uniformizer of B_i and where X_i is the B_i-component of X; otherwise f would induce a surjection $X_i/\lambda_i X_i \to A_i/\lambda_i A_i$ where A_i is the B_i-component of A, but then the $\kappa(B_i)$-ranks of X_i and A_i would coincide, so $\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')$ would be empty, contradicting the choice of A'.

   Thus, there exist homomorphisms $\varphi : X \to \kappa(B_i)$ that are nontrivial on $\ker(f)$ and each such φ induces a surjection $\tilde{f} = (f, \varphi) : X \to A'$ that lifts f. There are at least $(\ell^s - 1)$ choices for φ, there are at least $\ell^s - 1$ surjective lifts $\tilde{f}$ of f.

Now let an s-enlargement of A refer to any A' with $[A'] \in \mathcal{L}_{d,\ell}$ that admits a $\mathbb{Z}_\ell[\zeta_d]$-surjection $A' \twoheadrightarrow A$ with kernel of size ℓ^s. Given $\epsilon > 0$ and $[A] \in \mathcal{L}_{d,\ell}$, let $c(A) = k(d-1)$ and let $M \subset \mathcal{L}_{\ell,d}$ be the set of isomorphism classes of s-enlargements of A for $k(d-1) < s \leq (k+1)(d-1)$ where k is chosen large enough so that

$$\frac{\sum_{s=k(d-1)+1}^{(k+1)(d-1)} p(s + \log_\ell |A| + o(1))^{d-1}}{(\ell - 1)^k} < \epsilon$$

where $p(n)$ is the partition function and $o(1)$ is dependent only on d and ℓ — obtaining such a k is possible because d and A are fixed and $p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$, which was first obtained by Hardy and Ramanujan [19, Section 1.41] and independently obtained by Uspensky [42] (see [3, Section 5.1.2] for yet another discussion on this asymptotic formula).

Note that the number of isomorphism classes of s-enlargements of A is bounded above by the number of $\mathbb{Z}_\ell[\zeta_d]$-modules of cardinality $\ell^{s+o(1)} \cdot |A|$. In turn, this number of isomorphism classes is bounded above by $\prod_i \#\{B_i\text{-modules with cardinality } \ell^{s+o(1)} \cdot |A|\}$. For each i, the number of B_i-modules with cardinality $\ell^{s+o(1)} \cdot |A|$ is bounded above by $p(\log(\ell^{s+o(1)} \cdot |A|)) = p(s + \log_\ell |A| + o(1))$ because B_i-modules of finite cardinality are of the form $\bigoplus_{j=1}^{k_i} B_i/(\ell^{d_{i,j}})$ and the isomorphism class of such a direct sum is determined by

the multiset $\{d_{i,j}\}_j$. Since there are at most $(d-1)$ many i's, we have

$$|M| = \sum_{s=k(d-1)+1}^{(k+1)(d-1)} \#\{s\text{-enlargements of } A\} \leq \sum_{s=k(d-1)+1}^{(k+1)(d-1)} p(s + \log_\ell |A| + o(1))^{d-1}$$

so the choice of k yields

$$\frac{|M|}{(\ell-1)^k} < \epsilon.$$

For any $[X] \in \mathcal{L}_{d,\ell}$ such that $|X| > c(A)$, one can iteratively obtain basic enlargements to obtain some s-enlargement A' of A with $k(d-1) \leq s < (k+1)(d-1)$ such that

$$|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')| \geq (\ell-1)^s |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A)| \geq (\ell-1)^k |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A)|.$$

Equivalently,

$$|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A)| \leq \frac{|\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')|}{(\ell-1)^k}.$$

In turn, the RHS above is bounded above by

$$\begin{aligned}\frac{\sum_{A' \in M} |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')|}{(\ell-1)^k} &= \frac{|M|}{(\ell-1)^k} \cdot \frac{\sum_{A' \in M} |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')|}{|M|} \cdot \\ &< \epsilon \cdot \frac{\sum_{A' \in M} |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(X, A')|}{|M|}.\end{aligned}$$

□

Given $[A] \in \mathcal{L}_{d,\ell}$ and a probability measure ν on A, write $\langle \operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A) \rangle_\nu$ for the expected number of surjections from a ν-random group to A.

Given Theorem 7.0.3 and Lemma 7.0.4, the proof of Proposition 7.0.5 is virtually identical to that of [15, Proposition 8.3].

Proposition 7.0.5 (cf [15, Proposition 8.3])**.** *Let $d \geq 2$ and let ℓ be a prime number not dividing d. Let $\varepsilon_0 > 0$ and $L \subset \mathcal{L}_{d,\ell}$ be a finite subset. There exists $\delta > 0$ and a finite subset $L' \subset \mathcal{L}_{d,\ell}$ such that, if ν is any probability measure on $\mathcal{L}_{d,\ell}$ for which $\langle \operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A) \rangle_\nu \in [1-\delta, 1+\delta]$ for any $A \in L'$, then also $|\nu(A) - \mu_{d,\ell}(A)| \leq \epsilon_0$ for any*

$A \in L$.

Proof. Let $L'_k := \{A \in \mathcal{L}_{d,\ell} : |A| \leq k\}$. Suppose for contradiction that the assertion is false. In particular, for each integer $k \geq 1$, there is some measure ν_k on $\mathcal{L}_{d,\ell}$ that "does not work" for $L' = L'_k$ and $\delta = \frac{1}{k}$, i.e.

1. $|\langle \mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A)\rangle_{\nu_k} - 1| \leq \frac{1}{k}$ for all $A \in L'_k$, and
2. $|\nu_k(A) - \mu_{d,\ell}(A)| > \epsilon_0$ for some $A \in L$.

Passing to a weakly convergent subsequence, we obtain measures ν_k such that

$$\lim_{k\to\infty} \langle \mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A)\rangle_{\nu_k} = 1$$

for every fixed $A \in \mathcal{L}_{d,\ell}$ and such that the ν_k weakly converge to a measure ν_∞ which does not equal $\mu_{d,\ell}$.

Fix an arbitrary $\epsilon > 0$, which is not related to ϵ_0. We show that $\langle \mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A)\rangle_{\nu_\infty} = 1$. On the one hand, this expected value is at most 1 by Fatou's lemma. On the other hand, with $c = c(A)$ and $M \subset \mathcal{L}_{d,\ell}$ as in Lemma 7.0.4,

$$\begin{aligned}
\langle \mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A)\rangle_{\nu_\infty} &= \sum_{|B|\leq c} \nu_\infty(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)| + \sum_{|B|>c} \nu_\infty(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)| \\
&\geq \sum_{|B|\leq c} \nu_\infty(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)| \\
&= \lim_k \sum_{|B|\leq c} \nu_k(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)| \\
&= 1 - \lim_k \sum_{|B|>c} \nu_k(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)|. \qquad (7.0.2)
\end{aligned}$$

By Lemma 7.0.4,

$$\sum_{|B|>c} \nu_k(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A)| \leq \epsilon |M|^{-1} \sum_{|B|>c, A'\in M} \nu_k(B) |\mathrm{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A')| \qquad (7.0.3)$$

Now, by assumption, for any $A' \in M$ and any $k > |A'|$,

$$\sum_{|B|>c} \nu_k(B) |\operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(B, A')| \leq \langle \operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A') \rangle_{\nu_k} \leq 1 + 1/k$$

and using (7.0.3) and passing to the limit, we get

$$\limsup_k \sum_{|B|>c} \nu_k(B) |\operatorname{Sur}(B, A)| \leq \varepsilon.$$

Thus by (7.0.2) and the above inequality, we get $\langle \operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A) \rangle_{\nu_\infty} \in [1 - \varepsilon, 1]$. Since ε is arbitrary,

$$\langle \operatorname{Sur}_{\mathbb{Z}_\ell[\zeta_d]}(-, A) \rangle_{\nu_\infty} = 1.$$

Applying this conclusion with A trivial, we see that ν_∞ is a probability measure. Theorem 7.0.3 shows that $\nu_\infty = \mu_{d,\ell}$, which is a contradiction. □

Moreover, given Proposition 7.0.5, the proof of Theorem 7.0.1 is virtually identical to the proof of [15, Theorem 1.2] written between the statement and proof of [15, Theorem 8.8];

Proof of Theorem 7.0.1. Let $[A_0]$ be any fixed element of $\mathcal{L}_{\ell,d}$ and let $\epsilon > 0$. Given n, let ν_n be the probability measure on $\mathcal{L}_{\ell,d}$ with $\nu_n(A) = \frac{\#\{L \in \mathfrak{S}_n : \mathrm{Cl}(\mathcal{O}_L) \cong_{\mathbb{Z}_\ell[\zeta_d]} A\}}{|\mathfrak{S}_n|}$.

Apply Proposition 7.0.5 to $\epsilon_0 = \epsilon$, $L = \{A_0\}$, and $\nu = \nu_n$ to obtain a finite subset $L' \subset \mathcal{L}_{d,\ell}$ and $\delta > 0$ such that

$$\left| \frac{\sum_{L \in \mathcal{S}_n} m_A(L)}{|\mathfrak{S}_n|} - 1 \right| < \delta \text{ for all } A \in L' \Rightarrow |\nu_n(A_0) - \mu(A_0)| < \epsilon.$$

Now let $B_{d,\ell,A}$, $C_{d,\ell,A}$, and $N_{d,\ell,A}$ be as in Theorem 6.3.1, and let Q be so that $Q > 4B_{d,\ell,A}^2$ and $C_{d,\ell,A}/\sqrt{Q} < \delta$ for every $A \in L'$ where $B_{d,\ell,A}$ is as in Theorem 6.3.1. If $q > Q$ and $n \geq N_{d,\ell,A}$, then $\left| \frac{\sum_{L \in \mathcal{S}_n} m_A(L)}{|\mathfrak{S}_n|} - 1 \right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}} < \frac{C_{d,\ell,A}}{\sqrt{Q}} < \delta$ and hence $|\nu_n(A_0) - \mu(A_0)| < \epsilon$. Thus, for any $q > Q$, $\delta^+(q)$ and $\delta^-(q)$ are both bounded between $\mu_{d,\ell}([A_0]) - \epsilon$ and $\mu_{d,\ell}([A_0]) + \epsilon$. The result follows because ϵ is arbitrary. □

Chapter 8

Counting Rational Points on twists of Hurwitz schemes over $\mathbb{F}_q$

Throughout this section, continue writing $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ when $d \geq 2$ is an integer and $\ell \nmid d$ is a prime number. Similarly write $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$.

In this section, we tweak the ideas from [13, Section 2] to once again accommodate for the ζ_d-action as in Chapter 6 and Chapter 7 to prove Corollary 8.0.4. In turn, we use Corollary 8.0.4 to prove Theorem 9.0.9.

Let $d \geq 2$ and let $q \equiv 1 \pmod{d}$ be a prime power. Let $Q_{n,q}$ denote the set of squarefree polynomials over $\mathbb{F}_q$ of degree n. For each $f \in Q_{n,q}$, let C_f be the (smooth completion of the) curve given by $y^d = f(t)$. Note that C_f is a (tamely ramified) $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1_{\mathbb{F}_q}$ curve because $\mathbb{F}_q$ has a primitive dth root of unity. Let J_f be the Jacobian of C_f. In particular, the action of ζ_d on C_f induces an action on J_f. Let Frob_q denote the geometric Frobenius map on C_f as well as the induced action on J_f. Note that the actions of ζ_d and J_f on C_f commute and hence the induced actions on J_f commute as well. Given a prime number ℓ such that $\ell \nmid dq$, and for $a \in \mathbb{Z}/\ell\mathbb{Z}$ and $i \in \mathbb{Z}/d\mathbb{Z}$, the elements R of $J_f[\ell](\bar{\mathbb{F}}_q)$ which satisfy

$$\mathrm{Frob}_q \cdot R = a\zeta_d^i R \tag{8.0.1}$$

form a finite rank $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$-module. Let $m_{a,i}(f)$ denote the number of nonzero elements of

this module. Additionally, let $Q_{n,q}^{a,i}$ denote the set of $f \in Q_{n,q}$ such that $m_{a,i}(f)$ is greater than 0.

For the rest of this section, we let A be a quotient ring, often one which is an involution ring, of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$, let $G = A \rtimes \langle \zeta_d \rangle$ (where $\langle \zeta_d \rangle$ is a way to multiplicatively write the cyclic group $\mathbb{Z}/d\mathbb{Z}$), and let c be the set of elements of the form (a, ζ_d). By Lemma 2.0.5, c is a non-splitting conjugacy class of G. Given an integer $n \geq 1$ divisible by d or relatively prime to d, we let $\mathbf{X}_n$ be as in Definition 6.1.2 with respect to G and c.

Let k be an extension field of $\mathbb{F}_q$. As discussed in Chapter 6, k-points of $\mathbf{X}_n$ correspond to certain isomorphism classes of tame G-covers $f : C \to \mathbb{P}^1_k$. In turn, these isomorphism classes correspond to isomorphism classes of triples (g, ϕ, h), where $g : C \to D$ is an étale A-cover, $h : D \to \mathbb{P}^1_k$ is a tame $(\mathbb{Z}/d\mathbb{Z})$-cover, $f = h \circ g$, and $\phi : A \to \mathrm{Aut}(g)$ is an isomorphism. Given $a \in A^\times$, let $\langle a \rangle$ denote the automorphism of X_n sending (g, ϕ, h) to $(g, a\phi, h)$. Note that the (arithmetic) frobenius Frob_q on $X_n/\bar{\mathbb{F}}_q$ commutes with $\langle a \rangle$. Thus, the homomorphism $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{Aut}(X_n/\bar{\mathbb{F}}_q)$ sending Frob_q to $\langle a \rangle$ is a 1-cocycle from $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ to $\mathrm{Aut}(X_n/\bar{\mathbb{F}}_q)$ and hence determines a twist X_n^a of X_n defined over $\mathbb{F}_q$ (see, for example, [31, Theorem 4.5.2] for a statement).

Lemma 8.0.1 (cf. [13, Lemma 2.3])**.** *With notation as above and for any $i_0 \in \mathbb{Z}/d\mathbb{Z}$ and $a \in \mathbb{Z}/\ell\mathbb{Z}^\times$,*

$$\sum_{f \in Q_{n,q}} m_{a,i_0}(f) = \frac{1}{d} \sum_{f \in Q_{n,q}} \sum_{i=0}^{d-1} m_{a,i}(f) = (q-1)|\mathbf{X}_n^a(\mathbb{F}_q)|.$$

Proof. A point of $\mathbf{X}_n^a(\mathbb{F}_q)$ is a point x of $\mathbf{X}_n(\bar{\mathbb{F}}_q)$ such that $\mathrm{Frob}_q \cdot x = \langle a \rangle \cdot x$. Such a point x correspond to a triple $(g, \phi, h)/\bar{\mathbb{F}}_q$ such that $\mathrm{Frob}_q \cdot (g, \phi, h)$ is isomorphic to $a(g, \phi, h) = (g, a\phi, h)$. In particular, the isomorphism class of h is fixed by Frobenius and hence the branch locus of h is an $\mathbb{F}_q$-rational divisor. Let $F(t) \in \mathbb{F}_q[t]$ be the unique monic squarefree polynomial whose vanishing locus is the branch locus of t. By Proposition 3.2.2, the source of h is isomorphic to C_F over $\bar{\mathbb{F}}_q$ because the monodromy type of the G-cover $t \circ g : X \to \mathbb{P}^1$ is c.

Fixing such an $h : C_F \to \mathbb{P}^1$ over $\bar{\mathbb{F}}_q$, we count the number of points of $X_n^a(\mathbb{F}_q)$ lying

over h. Choices of (g,ϕ) such that $(g,\phi,h) \in X_n^a(\overline{\mathbb{F}}_q) = X_n(\overline{\mathbb{F}}_q)$ for the fixed h are in bijection with the ζ_d-equivariant surjections $J(C_F)[\ell](\overline{\mathbb{F}}_q) \to A$ up to isomorphism — two such surjections s and s' are isomorphic if and only if $s = \zeta_d^i s'$ for some i. The action of Frobenius on X_n^a on the set of surjections sends s to $a^{-1}\operatorname{Frob}_q s$, so s descends to a point of $X_n^a(\mathbb{F}_q)$ if and only if $\operatorname{Frob}_q \cdot s = \zeta_d^i a s$ for some i. Therefore, the number of points of $X_n^a(\mathbb{F}_q)$ lying over h is $\frac{1}{d}\sum_{i=0}^{d-1} m_{a,i}(F)$.

Now say that $\epsilon \in \mathbb{F}_q^*$ and $f \in Q_{n,q}$. By abuse of notation, say that ζ_d acts on C_f (and on $C_{\epsilon f}$) by $(x,y) \mapsto (x, \zeta_d y)$ for some fixed primitive dth root ζ_d in $\mathbb{F}_q$, which exists as $q \equiv 1 \pmod{d}$. For any $\delta \in \overline{\mathbb{F}}_q$ such that $\delta^d = \epsilon$, say that j is such that $\zeta_d^j = \frac{\delta^q}{\delta}$. Note that the curves C_f and $C_{\epsilon f}$ are isomorphic over $\overline{\mathbb{F}}_q$ via $\varphi : C_f \to C_{\epsilon f}, \quad (x,y) \mapsto (x, \delta y)$. Moreover, $\zeta_d^j \circ \varphi \circ \operatorname{Frob}_q = \operatorname{Frob}_q \circ \varphi$. Given $R \in J_f[\ell](\overline{\mathbb{F}}_q)$ such that (8.0.1) holds, we have

$$\operatorname{Frob}_q \varphi(R) = \zeta_d^j \varphi \operatorname{Frob}_q R = \zeta_d^j \varphi a \zeta_d^i R = a\zeta_d^{i+j}(\varphi R),$$

so $m_{a,i}(f) = m_{a,i+j}(\epsilon f)$. In particular,

$$\sum_{i=0}^{d-1} m_{a,i}(f) = \sum_{i=0}^{d-1} m_{a,i}(\epsilon f), \tag{8.0.2}$$

so

$$\frac{1}{d} \sum_{f \in Q_{n,q}} \sum_{i=0}^{d-1} m_{a,i}(f) = \sum_{\substack{F \in Q_{n,q} \\ \text{monic}}} \sum_{\epsilon \in \mathbb{F}_q^*} \left(\frac{1}{d} \sum_{i=0}^{d-1} m_{a,i}(\epsilon F) \right),$$

where f is expressed as ϵF for a monic F. Since, for each monic F, the sum $\sum_{i=0}^{d-1} m_{a,i}(\epsilon F)$ is independent of ϵ by (8.0.2), the above equals

$$(q-1) \sum_{\substack{F \in Q_{n,q} \\ \text{monic}}} \frac{1}{d} \sum_{i=0}^{d-1} m_{a,i}(F).$$

Since the number of points of $X_n^a(\mathbb{F}_q)$ lying over $h : C_F \to \mathbb{P}^1$ (over $\bar{\mathbb{F}}_q$) equals $\frac{1}{d}\sum_{i=0}^{d-1} m_{a,i}(F)$,

the above equals $(q-1)|X_n^a(\mathbb{F}_q)|$. Thus,

$$\frac{1}{d}\sum_{f\in Q_{n,q}}\sum_{i=0}^{d-1} m_{a,i}(f) = (q-1)|X_n^a(\mathbb{F}_q)|.$$

Now let $\delta \in \overline{\mathbb{F}}_q$ be so that $\zeta_d = \delta^{q-1}$. Note that $\delta^d \in \mathbb{F}_q$ because $\delta^{(q-1)d} = \zeta_d^d = 1$. Therefore, for any $i_0 \in \mathbb{Z}/d\mathbb{Z}$,

$$\sum_{f\in Q_{n,q}} m_{a,i_0}(f) = \sum_{f\in Q_{n,q}} m_{a,i_0}(\delta^d f) = \sum_{f\in Q_{n,q}} m_{a,i_0+1}(f),$$

so

$$\frac{1}{d}\sum_{f\in Q_{n,q}}\sum_{i=0}^{d-1} m_{a,i}(f) = \frac{1}{d}\sum_{f\in Q_{n,q}}\sum_{i=0}^{d-1} m_{a,i_0}(f) = \sum_{f\in Q_{n,q}} m_{a,i_0}(f).$$

□

Proposition 8.0.2 (cf. [13, Proposition 2.1, Proposition 2.7])**.** *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, and let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$. The constants $B_{d,\ell,A}$, $C_{d,\ell,A}$, and $N_{d,\ell,A}$ of Theorem 6.3.1 satisfy*

$$\left|\frac{\sum_{f\in Q_{n,q}} m_{a,i_0}(f)}{|Q_{n,q}|} - 1\right| \leq \frac{C_{d,\ell,A}}{\sqrt{q}}$$

for all a, n, q, i_0 such that

- $a \in A^\times$
- *n is relatively prime to or divisible by d,*
- $q \equiv 1 \pmod{d}$ *is a prime power,*
- $\sqrt{q} > 2B_{d,\ell,A}$, $n \geq N_{d,\ell,A}$,
- *ℓ does not divide $2dq(q-1)$,*
- $\mathrm{SU}(V_n) \subseteq \mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n))$,
- $i_0 \in \mathbb{Z}/d\mathbb{Z}$.

Remark 8.0.3. Although the proof of [13, Proposition 2.1] uses many of the same ideas from the proof of [15, Theorem 8.8], which requires $\ell \nmid (q-1)$, [13, Proposition 2.1] ultimately does not require the condition $\ell \nmid (q-1)$. This condition is originally used in [15, Theorem 8.8] to show that the Hurwitz scheme denoted by $\mathbf{X}_n$ has exactly one geometrically irreducible component defined over $\mathbb{F}_q$. In contrast, [13] is concerned with Hurwitz schemes arising in the case $d = 2$ and $A = \mathbb{Z}/\ell\mathbb{Z}$; it turns out that such Hurwitz schemes are geometrically irreducible even without the condition $\ell \nmid (q-1)$ and hence these Hurwitz schemes have exactly one geometrically irreducible component defined over $\mathbb{F}_q$. However, this argument does not apply to the context of Proposition 8.0.2, which is concerned with the case where $d \geq 3$ and A is a quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$.

Proof. By Lemma 8.0.1 and since $|Q_{n,q}| = (q-1)(q^n - q^{n-1})$ by [5, 4, equation (vi)], it suffices to show that there exist $B_{d,\ell,A}$ and $N_{d,\ell,A}$ such that

$$\left| \frac{|X_n^a(\mathbb{F}_q)|}{q^n} - 1 \right| \leq B_{d,\ell,A} q^{-1/2}$$

for all n, q, i_0 as specified in the statement of the theorem. This follows by the same ideas as in the proof of Theorem 6.3.1[1] — by the Grothendieck-Lefschetz trace formula, we have

$$|X_n^a(\mathbb{F}_q)| = \sum_i (-1)^i \operatorname{Tr}(\operatorname{Frob}_q | H_c^i(\mathbf{X}_n^a \times \overline{\mathbb{F}}_q, \mathbb{Q}_\lambda))$$

for primes λ not dividing q. Further taking λ to be a prime greater than $\max(|G|, q, n)$ in fact yields the dimension bound (6.3.2) applicable to $\mathbf{X}_n \times \overline{\mathbb{F}}_q \cong \mathbf{X}_n^a \times \overline{\mathbb{F}}_q$. Recall that the the inequality (6.3.3) holds as long as $\sqrt{q} > 2B_{d,\ell,A}$. It now suffices to show that there exists an $N_{d,\ell,A}$ such that

$$\operatorname{Tr}(\operatorname{Frob}_q | H_c^{2n}(\mathbf{X}_n^a \times \overline{\mathbb{F}}_q, \mathbb{Q}_\lambda)) = q^n \tag{8.0.3}$$

[1] One difference to note between Theorem 6.3.1 and Proposition 8.0.2 is that the latter allows n to be divisible by d. The requirement in Theorem 6.3.1 for n to not be divisible by d and instead for $(d, n) = 1$ comes from Proposition 6.1.3 and the discussion above this proposition. There, the requirement guarantees that fields $L = \mathbb{F}_q(t)[y]/(y^d - f(t))$ in consideration are totally imaginary and hence that the corresponding smooth projective curves C_L possess $\mathbb{F}_q$-rational points. In turn, this identifies $\operatorname{Jac}(C_L)(\mathbb{F}_q)$ with Cl_L. For Proposition 8.0.2 however, no such identification is needed.

holds for all $n > N_{d,\ell,A}$ such that $\gcd(d,n) = 1$ or $d \mid n$ and such that $\mathrm{SU}(V_n) \subseteq \mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n))$. The equality (8.0.3) is equivalent to the statement that there is exactly one $\mathbb{F}_q$-rational connected component of $\mathbf{X}_n^a \times \overline{\mathbb{F}}_q$ — the proof of Theorem 6.3.1 shows this to be the case. □

Given an integer $d \geq 2$, a prime ℓ, a prime power q such that $\ell \nmid dq$ and $q \equiv 1 \pmod{d}$, $a \in \mathbb{Z}_\ell[\zeta_d]$, and $i \in \mathbb{Z}/d\mathbb{Z}$,

Corollary 8.0.4 (cf. [13, Corollary 2.6])**.** *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, and let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$. The constants $B_{d,\ell,A}$, $C_{d,\ell,A}$, and $N_{d,\ell,A}$ of Theorem 6.3.1 satisfy*

$$\frac{|Q_{n,q}^{a,i}|}{|Q_{n,q}|} \leq \frac{1}{\ell - 1} + \frac{C_{d,\ell,A}}{(\ell-1)\sqrt{q}}$$

for all n, q, ℓ, a, i such that

- *n is relatively prime to or divisible by d,*
- *$q \equiv 1 \pmod{d}$ is a prime power,*
- *$\sqrt{q} > 2B_{d,\ell,A}$, $n \geq N_{d,\ell,A}$*
- *ℓ does not divide $2dq(q-1)$,*
- *$\mathrm{SU}(V_n) \subseteq \mu(\mathrm{Gal}(\overline{K}_n/\overline{\mathbb{F}}_q K_n))$,*
- *$a \in \mathbb{Z}/\ell\mathbb{Z}^\times$,*
- *$i \in \mathbb{Z}/d\mathbb{Z}$.*

Proof. Let δ denote the quantity $\frac{|Q_{n,q}^{a,i}|}{|Q_{n,q}|}$ to be bounded. Since $m_{a,i}(f)$ is the number of nonzero elements of a $\mathbb{Z}/\ell\mathbb{Z}$-vector space, it is at least $\ell - 1$ if it is greater than 0. In particular,

$$\frac{\sum_{f \in Q_{n,q}} m_{a,i}(f)}{|Q_{n,q}|} \geq (\ell-1)\frac{|Q_{n,q}^{a,i}|}{|Q_{n,q}|} = (\ell-1)\delta.$$

By Proposition 8.0.2, the LHS above is bounded above by $1 + \frac{C_{d,\ell,A}}{\sqrt{q}}$ for all n, q, ℓ, a, i specified by the statement of the corollary. $\square$

Chapter 9

Vanishing of zeta functions and L-functions for trielliptic curves

The ideas of this section generalize those in [13, Section 3] to prove Theorem 9.0.9, which in turn generalizes [13, Theorem 3.2, Theorem 1.2]. These theorems provide explicit upper bounds on the proportion of superelliptic function fields whose zeta functions vanish at a fixed complex number s.

Given a variety $X/\mathbb{F}_q$, there is a function $Z_X(T)$ defined as

$$Z_X(T) := \prod_{\text{closed points } P \in X} \left(1 - T^{\deg P}\right)^{-1}$$

and which converges for $|T| < q^{-\dim X}$. We then define the zeta function $\zeta_X(s) := Z_X(q^{-s})$ which converges for $\mathrm{Re}(s) > \dim X$. See [30, Chapter 3] or [34, Chapter 5], for instance, for discussions on this zeta function and on the Weil conjectures.

In the case that C is a nice curve, i.e. a smooth, projective, geometrically integral variety of dimension 1, over $\mathbb{F}_q$, the Weil conjectures show that there is a polynomial $P_C(T) \in \mathbb{Z}[T]$ such that

$$Z_C(T) = \frac{P_C(T)}{(1-T)(1-qT)}.$$

In fact, the constant and leading coefficients of $P_C(T)$ are respectively 1 and g where g is

the genus of C. Let $\mathrm{Jac}(C)$ denote the Jacobian of C and let $T_\ell \mathrm{Jac}(C)$ denote the ℓ-adic Tate module of this Jacobian. The polynomial $P_C(T)$ is then the reverse polynomial of the characteristic polynomial of the geometric Frobenius map Frob_q acting on $T_\ell \mathrm{Jac}(C)$ for any prime ℓ not equal to $\mathrm{char}\, \mathbb{F}_q$.

To prove Lemma 9.0.8, which establishes the vanishing of Artin L-functions as an equivalent condition to the vanishing of $P_C(q^{-s})$ when C is a $\mathbb{Z}/d\mathbb{Z}$-cover of $\mathbb{P}^1_{\mathbb{F}_q}$ and $q \equiv 1 \pmod{d}$, we will need some facts relating the Artin L-functions and the Dirichlet L-functions for C. In turn, we need the following definitions and notations.

Definition 9.0.1 (cf. [34, Chapter 3, the Definition before Proposition 3.1 and the Definition before Proposition 3.4])**.** Let q be a prime power and let d be a divisor of $q-1$. For an irreducible polynomial $P \in \mathbb{F}_q[t]$ and a polynomial $a \in \mathbb{F}_q[t]$, define $\left(\frac{a}{P}\right)_d$ to be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{q^{\deg P}-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}$$

if P does not divide a and to be 0 otherwise.

Given $a, b \in \mathbb{F}_q[t]$ with $b \neq 0$, define $\left(\frac{a}{b}\right)_d$ to be $\prod_{j=1}^{s} \left(\frac{a}{Q_j}\right)_d^{f_j}$ where $b = \beta Q_1^{f_1} \cdots Q_s^{f_s}$ is the prime decomposition of b.

Definition 9.0.2. Let $d \geq 2$ be an integer and let $q \equiv 1 \pmod{d}$ be a prime power. For a polynomial $f(t) \in \mathbb{F}_q[t]$, let $\chi_f : \mathbb{F}_q[t] \to \mathbb{F}_q$ denote the Dirichlet character given by $\chi_f(g) = \left(\frac{f}{g}\right)_d$. In particular, χ_f can be well defined as a function on the set of finite primes of $\mathbb{P}^1_{\mathbb{F}_q}$ — let $\chi_f(P) = \left(\frac{f}{g_P}\right)_d$ where $g_P \in \mathbb{F}_q[t]$ is the monic irreducible polynomial corresponding to P. Note that $\chi_f^j = \chi_{f^j}$ for any $j \in \mathbb{Z}/d\mathbb{Z}$.

Given a fixed primitive dth root r of unity in $\mathbb{F}_q$, we will also identify χ_f as a $\mathbb{C}$-valued character by sending r to $e^{2\pi i/d}$.

We now define L-series of Dirichlet characters.

Definition 9.0.3 (cf. [34, Chapter 17, before Proposition 17.7] for a discussion in the

case of $d = 2$). With notation as in Definition 9.0.2, define the L-series $L(s, \chi_f)$ as follows:

$$L(s, \chi_f) = \sum_{g \in \mathbb{F}_q[t] \text{ monic}} \frac{\chi_f(g)}{q^{s \cdot \deg g}} = \prod_{P \text{ finite prime of } \mathbb{F}_q(t)} \left(1 - \frac{\chi_f(P)}{q^{s \cdot \deg P}}\right)^{-1}.$$

Given $j \in \mathbb{Z}/d\mathbb{Z}$, also let $L(s, \chi_f^j) = L(s, \chi_{f^j})$.

If $f = f_0 f_1^d$, then note that

$$L(s, \chi_f) = L(s, \chi_{f_0}) \cdot \prod_{P | f_1} \left(1 - \frac{\chi_{f_0}(P)}{q^{s \cdot \deg P}}\right).$$

In particular, away from $\operatorname{Re} s = 0$, $L(s, \chi_f)$ vanishes if and only if $L(s, \chi_{f_0})$ vanishes.

Definition 9.0.4. Let $d \geq 2$ be an integer and let $q \equiv 1 \pmod{d}$ be a prime power. Given $f(t) \in \mathbb{F}_q[t]$ and a fixed primitive dth root r of unity in $\mathbb{F}_q$, write χ to be the complex-valued character on $G = \mathrm{Gal}(\mathbb{F}_q(t)[y]/(y^d - f(t))/\mathbb{F}_q(t))$ determined by $\chi(\sigma) = e^{2\pi i/d}$ where σ is the element of G that sends y to ry.

Definition 9.0.5 (cf. [34, Chapter 5])**.** Let K be a global function field with constant field (i.e. the algebraic closure of the prime field) $\mathbb{F}_q$. Let P be a prime of K, i.e. the maximal ideal of a discrete valuation ring R whose quotient field is K. Let the degree $\deg P$ of P be the dimension of the residue field R/P over the constant field $\mathbb{F}_q$. Moreover, the norm $N(P)$ is $q^{\deg P}$.

Definition 9.0.6 (cf. [34, Chapter 14, before Proposition 14.9])**.** Let L/K be an abelian Galois extension of global function fields with galois group G and say that the constant field of K is $\mathbb{F}_q$. Given a prime Q of L lying over and unramified above the prime P of K, the *Artin automorphism* $(P, L/K)$ is a generator of the decomposition group $D(P)$ characterized by the congruence

$$(P, L/K)\omega = \omega^{N(P)} \pmod{Q}$$

for any element ω of L integral at Q.

Let $\chi : G \to \mathbb{C}$ be a Dirichlet character. Given a prime P of K, let $I(P)$ be the inertia group of P and define $\chi(P)$ by the following:

- if P is unramified in L, then $\chi(P) = \chi((P, L/K))$
- if P is ramified in L and χ is ramified at P, i.e. $\chi(I(P)) \neq 1$, then $\chi(P) = 0$.
- if P is ramified in L and χ is unramified at P, then $\chi(P) = \chi((P, L^{I(P)}/K))$; this is well defined because χ factors as a character $\mathrm{Gal}(L^{I(P)}/K) \cong G/I(P)$.

The Artin L-series of χ is defined by

$$L(s, \chi) = \prod_{P \text{ prime of } K} \left(1 - \frac{\chi(P)}{N(P)^s}\right)^{-1}.$$

Lemma 9.0.7 shows that the L-series of the Dirichlet character χ_f, regarded as a complex valued character, roughly coincides with the Artin L-series of χ. In fact, these two characters coincide on finite primes of $\mathbb{P}^1_{\mathbb{F}_q}$, so their respective L-functions coincide after making appropriate adjustments at ∞. See [34, Proposition 17.7] for a discussion in the case of $d = 2$.

Lemma 9.0.7. *Let $d \geq 2$ be an integer. Let q be a prime power such that $q \equiv 1 \pmod{d}$. Let f be a monic polynomial in $\mathbb{F}_q[t]$ and fix a primitive dth root r of unity in $\mathbb{F}_q$. Identify χ_f as a $\mathbb{C}$-valued character with respect to this choice of r as discussed in Definition 9.0.2. Also let χ be the complex-valued character on the Galois group G of $L = \mathbb{F}_q(t)[y]/(y^d - f(t))$ over $\mathbb{F}_q(t)$ as defined in Definition 9.0.4 with respect to this choice of r.*

1. *$\chi_f(P) = \chi(P)$ for all finite primes P of $\mathbb{P}^1_{\mathbb{F}_q}$.*
2. *$L(s, \chi^j) = L_\infty(s, \chi_f^j) L(s, \chi_f^j)$ for any $j \in \mathbb{Z}/d\mathbb{Z}$ where*

$$L_\infty(s, \chi_f^j) = \left(1 - \frac{\chi^j(\infty)}{q^s}\right)^{-1}.$$

Proof. 1. Recall that $\chi(P)$ is defined as

$$\chi(P) = \begin{cases} \chi((P, L/\mathbb{F}_q(t)) & \text{if } P \text{ is unramified in } L \\ 0 & \text{if } P \text{ is ramified and } \chi(I(P)) \neq 1 \cdot \\ \chi((P, L^{I(P)}/\mathbb{F}_q(t)) & \text{if } P \text{ is ramified and } \chi(I(P)) = 1 \end{cases}$$

where $(P, K/\mathbb{F}_q(t))$ denotes the Artin automorphism of the abelian extension $K/\mathbb{F}_q(t)$.

Let P be a finite prime unramified in L. The Artin automorphism satisfies $(P, L/\mathbb{F}_q(t))\omega = \omega^{q^{\deg P}} \pmod{Q}$ for any $\omega \in L$ integral at Q where Q is any prime lying over P. Note that $(P, L/\mathbb{F}_q(t))$ is a generator of the decomposition group of G at P; in this case, the decomposition group equals G itself. On the other hand, $\chi_f(P)$ is the element r_P of $\mathbb{F}_q$ such that $r_P \equiv f^{\frac{q^{\deg P}-1}{d}} \pmod{P}$. In particular, r_P needs to be a dth root of unity in $\mathbb{F}_q$. Note that $f^{\frac{q^{\deg P}-1}{d}} = y^{q^{\deg P}-1}$. If $r_P \equiv y^{q^{\deg P}-1} \pmod{P}$, then $r_P \equiv y^{q^{\deg P}-1} \pmod{Q}$ as well, in which case $r_P y \equiv y^{q^{\deg P}} \pmod{Q}$. Thus, $(P, L/\mathbb{F}_q(t))y = r_P y$.

Say that $j \in \mathbb{Z}/d\mathbb{Z}$ is so that $r_P = r^j$, in which case $\chi((P, L/\mathbb{F}_q(t))) = e^{2\pi ij/d}$. Moreover,

$$\begin{aligned} \chi_f(P) &= \left(\frac{f}{g_P}\right) \\ &\equiv f^{\frac{q^{\deg g_P}-1}{d}} \\ &\equiv y^{q^{\deg P}-1} \\ &\equiv r_P \pmod{P} \end{aligned}$$

where $g_P \in \mathbb{F}_q[t]$ is the monic irreducible polynomial corresponding to P. Therefore, $\chi_f(P) = e^{2\pi ij/d}$ as a complex number, so $\chi(P) = \chi_f(P)$.

If P is instead ramified, in fact P is totally ramified and the inertia group $I(P)$ of P is G itself. If $\chi(I(P)) \neq 1$, then $\chi(P) = 0$ by definition and if $\chi(I(P)) = 1$ instead, then $\chi(P) = \chi((P, L^{I(P)}/\mathbb{F}_q(t))$, but the Artin symbol $(P, L^{I(P)}/\mathbb{F}_q(t))$ is trivial, so

$\chi(P) = 0$. Either way, $\chi(P) = 1$. Moreover, since P is a finite ramified prime, P divides $f(t)$, so $\chi_f(P) = 0$. Therefore, $\chi(P) = \chi_f(P)$.

2. By part (1), the multiplicands for finite primes of $\mathbb{F}_q(t)$ in the Euler products for $L(s, \chi^j)$ and $L(s, \chi_f^j)$ coincide. Moreover, $L_\infty(s, \chi_f^j)$ equals the multiplicand for ∞ in the Euler product for $L(s, \chi^j)$, so $L(s, \chi^j) = L_\infty(s, \chi_f^j)L(s, \chi_f^j)$ as desired.

□

Lemma 9.0.8. *Let $d \geq 3$ be an integer. Let q be a prime power such that $q \equiv 1 \pmod{d}$, and let f be a monic polynomial in $\mathbb{F}_q[t]$. Let C_f be the smooth completion of the curve defined by $y^d = f(t)$ and let $P_f \in \mathbb{Z}[x]$ be the reverse characteristic polynomial of geometric Frobenius acting on the Jacobian of C_f.*

For any $s \neq 0, 1$, the following are equivalent:

1. *$P_f(q^{-s}) = 0$,*
2. *$Z_{C_f}(q^{-s}) = 0$,*
3. *the Artin L-function $L(s, \chi)$ vanishes for some nontrivial complex-valued character χ on the Galois group G of $\mathbb{F}_q(t)(\sqrt[d]{f(t)})$ over $\mathbb{F}_q(t)$,*
4. *$L(s, \chi_f^j)$ vanishes for some $j \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}$.*

Proof. We have

$$\zeta_{C_f}(s) = \zeta_{\mathbb{P}^1}(s) \prod_{\chi \neq \chi_0} L(s, \chi)$$

where the product is over the nontrivial characters χ of the Galois group G of $C_f/\mathbb{P}^1$ [34, Proposition 14.9]. Moreover,

$$Z_{\mathbb{P}^1}(T) = \frac{1}{1 - qT},$$

so

$$\zeta_{\mathbb{P}^1}(s) = \frac{1}{1 - q^{1-s}}.$$

Thus, $\zeta_{\mathbb{P}^1}(s)$ has no zeroes and has no poles away from $s = 1$. Therefore, $\zeta_{C_f}(s)$ vanishes exactly when some $L(s, \chi)$ vanishes. Additionally,

$$Z_{C_f}(T) = \frac{P_f(T)}{(1-T)(1-qT)}$$

and hence

$$\zeta_{C_f}(s) = Z_{C_f}(q^{-s}) = \frac{P_f(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Therefore, $\zeta_{C_f}(s)$ vanishes exactly when $P_f(q^{-s})$ vanishes, so $\zeta_{C_f}(s)$ indeed vanishes exactly when some $L(s, \chi)$ vanishes. By Lemma 9.0.7, these conditions are in turn equivalent to the vanishing of some $L(s, \chi_f^j)$. □

We now prove the main result of this section. Unlike Theorem 6.3.1 and Theorem 7.0.1, however, we state this theorem immediately in terms of what Corollary 6.2.9 affords instead of "black-boxing" a big monodromy condition as an assumption in the hypothesis. Nevertheless, the exponent C_d in the theorem would be improved should the big monodromy result of Corollary 6.2.9 be generalized to more combinations of d, ℓ, and n.

Theorem 9.0.9. *Let $d \geq 3$. There exists a constant $C_d > 0$ only depending on d such that, for any $s \neq 0, 1$,*

$$\limsup_{\substack{n\to\infty \\ \gcd(d,n)=1 \text{ or } d|n}} \frac{|\{f \in Q_{n,q} | Z_{C_f}(q^{-s}) = 0\}|}{|Q_{n,q}|} \ll q^{-C_d}.$$

or equivalently by Lemma 9.0.8

$$\limsup_{\substack{n\to\infty \\ \gcd(d,n)=1 \text{ or } d|n}} \frac{|\{f \in Q_{n,q} | L(s, \chi_f^j) = 0 \text{ for some } j \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}\}|}{|Q_{n,q}|} \ll q^{-C_d}.$$

where the asymptotic bound is with respect to the limit taken over powers q of a fixed prime power $q_0 \equiv 1 \pmod{d}$. In fact, $C_d = \frac{1}{(138d+62)\cdot(d-1)}$ suffices.

Proof. By Lemma 9.0.8, the set $\{f \in Q_{n,q} | L(s, \chi_f^j) = 0 \text{ for some } j \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}\}$ equals

$$Q_{n,q}^{q^{-s}} := \{f \in Q_{n,q} | P_f(q^{-s}) = 0\}.$$

where $P_f(x) \in \mathbb{Z}[x]$ is the reverse characteristic polynomial of geometric Frobenius acting on the Jacobian of C_f. Note that roots of $P_f(x)$ are reciprocals of algebraic integers.

Let $q_0 \equiv 1 \pmod{d}$ be a fixed prime power and let $g_{q_0^s} \in \mathbb{Z}[x]$ be the minimal polynomial of q_0^s. For all sufficiently large powers q of q_0, Chebotarev's density theorem yields a prime $\ell = \ell_q = \left(\frac{1}{4d}\right)^{\frac{1}{d-1}} \left(\frac{q}{4}\right)^{\frac{1}{(138d+62)\cdot(d-1)}} \cdot (1 + o(1))$ that is unramified in the splitting field L of $g_{q_0^s}$ of Φ_d over $\mathbb{Q}$ and such that Frob_{ℓ_q} is the (conjugacy class of the) identity element of $\mathrm{Gal}(L/\mathbb{Q})$. In fact, ℓ_q can be chosen to not divide $q - 1$. Whenever q is large enough, $\ell_q > [\mathcal{O}_L : \mathbb{Z}[q_0^s]]$ and hence $\ell_q \nmid [\mathcal{O}_L : \mathbb{Z}[q_0^s]]$. By the Dedekind-Kummer theorem (see e.g. [27, Proposition 8.3] for a statement), $g_{q_0^s}$ splits completely modulo ℓ_q. Let $A = \mathbb{Z}/\ell_q\mathbb{Z}[\zeta_d]_{\mathrm{prim}} = (\mathbb{Z}/\ell_q\mathbb{Z}[X])/(\Phi_d(X))$. Further note that, when q is large enough, ℓ_q is large enough so that the big monodromy result condition of Corollary 6.2.9 and its consequences, including Proposition 6.3.5, hold.

Let $a \in \mathbb{Z}/\ell_q\mathbb{Z}^\times$ be so that $g_{q_0^s}(a) \equiv 0 \pmod{\ell_q}$. If $q = q_0^k$, then define $P_{f,k}(x)$ as the polynomial $P_f(x^k)$. Given a polynomial h, let h^{rev} denote its reverse polynomial. In particular,

$$P_{f,k}^{\mathrm{rev}}(q_0^s) = P_f^{\mathrm{rev}}(q^s) = (q^s)^{\deg P_f} P_f(q^{-s}),$$

so if $P_f(q^{-s}) = 0$, then $g_{q_0^s}(x)$ divides $P_{f,k}^{\mathrm{rev}}(x)$. Thus, $P_{f,k}^{\mathrm{rev}}(a) \equiv 0 \pmod{\ell_q}$ and hence $P_f(a^{-k}) \equiv 0 \pmod{\ell_q}$. Equivalently, there is some nonzero $R \in J_f[\ell_q](\overline{\mathbb{F}}_q)$ such that $\mathrm{Frob}_q R = a^k R$, so $m_{a^k,0}(f) > 0$. Therefore,

$$\frac{|Q_{n,q}^{q^{-s}}|}{|Q_{n,q}|} \leq \frac{|Q_{n,q}^{a^k,0}|}{|Q_{n,q}|}$$

By Corollary 8.0.4,

$$\limsup_{\substack{n\to\infty \\ \gcd(d,n)=1 \text{ or } d|n}} \frac{|\{f \in Q_{n,q} | L(s,\chi_f^j) = 0 \text{ for some } j \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}\}|}{|Q_{n,q}|} \leq \frac{1}{\ell_q - 1} + \frac{C_{d,\ell_q,A}}{(\ell_q - 1)\sqrt{q}}$$

for all sufficiently large q. By Proposition 6.3.5, this bound holds for $C_{d,\ell_q,A} = 2 \cdot (2d|A|)^{69d+31} \leq 2 \cdot (2d\ell_q^{d-1})^{69d+31}$. The asymptotic size of ℓ_q is chosen so that $\frac{C_{d,\ell_q,A}}{\sqrt{q}}$ is bounded above by a constant. Therefore, the desired asymptotic bound holds. $\square$

Chapter 10

Orbits of the Burau representation evaluated at roots of unity modulo ℓ

This section proves Lemma 10.4.2, which is used in Proposition 6.3.5 to obtain constants $B_{d,\ell,A}$ and $C_{d,\ell,A}$, just as how [13, Proposition 2.7] obtains constants for $d = 2$. We study the structure of the graded ring R of (10.1.1) below, obtaining upper bounds for the degrees of $\ker U_D$ and $\operatorname{coker} U_D$ where U_D is a central element of R presented in (10.4.1). In turn, the degree n component of R is a k-vector space with basis corresponding to the orbits of a braiding action on tuples over $G = A \rtimes \mathbb{Z}/d\mathbb{Z}$ of length n and, as Theorem 10.3.7 demonstrates, the orbits of this action are precisely deterined by three invariants. Understanding these orbits is much easier for $d = 2$ as only two invariants suffice. The $d = 2$ case is also much easier to work with because $\zeta_2 = -1$.

Convention 10.0.1. Let $d \geq 2$ be an integer, let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{\text{all}}$, let A be a $\mathbb{Z}[\zeta_d]$-module, let $G = A \rtimes \langle \zeta_d \rangle$, and let c be the set $\{(a, \zeta_d) : a \in A\}$. Given an n-tuple $((a_1, \zeta_d), \ldots, (a_n, \zeta_d))$ of elements of c, identify this list with the vector $(a_1, \ldots, a_n) \in A^{\oplus n}$. We often write this vector as the column vector $\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T$ with matrices acting on the left.

10.1 Braiding on the conjugacy class of $A \rtimes \mathbb{Z}/d\mathbb{Z}$ and the unreduced Burau representation

We identify the (Artin) braiding action of $A \rtimes \mathbb{Z}/d\mathbb{Z}$ with the unreduced Burau representation evaluated at $t = \zeta_d$.

Definition 10.1.1. Let G be a group. The *braiding action of B_n on G^n* is given as follows — the standard generator $\sigma_j \in B_n$ acts by

$$\sigma_j : (g_1, \ldots, g_n) \mapsto \left(g_1, \ldots, g_{j-2}, g_{j-1}, g_j g_{j+1} g_j^{-1}, g_j, g_{j+2} \ldots, g_n\right).$$

Note that only the j-th and $(j+1)$-st entries are possibly modified.

For a finite group G, a conjugacy class c, and a field k of characteristic not dividing $|G|$, [15, Section 3] defines the graded ring

$$R = \sum_n H_0(\mathrm{Hur}^c_{G,n}, k) \tag{10.1.1}$$

where $\mathrm{Hur}^c_{G,n}$ is the complex Hurwitz space with of tamely ramified G-covers of $\mathbb{P}^1_{\mathbb{C}}$ with n branch points with monodromy of type c. If c is nonsplitting as well, then, for each p, $\dim H_p(\mathrm{Hur}^c_{G,n}, k)$ stabilizes with respect to n [15, Theorem 6.1, Corollary 6.2]. The braiding action restricted to c^n for a conjugacy closed subset c of G induces the relations on R. More explicitly, R is generated over k by degree 1 elements $\{r_g\}_{g \in c}$ and has relations

$$r_g r_h = r_{ghg^{-1}} r_g.$$

Lemma 10.1.2. *Let $d \geq 2$, let A be a $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$-module, and let G and c be as in Convention 10.0.1. Under Convention 10.0.1, the braiding action of B_n on c^n corresponds to the action induced by the unreduced Burau representation ψ_n evaluated at $t = \zeta_d$. More precisely, the standard generators $\sigma_1, \ldots, \sigma_{n-1}$ of B_n act on $A^{\oplus n}$ as elements of $\mathrm{GL}_n(\mathrm{End}_{\mathbb{Z}[\zeta_d]}(A))$ and these elements can be represented by $n \times n$ matrices*

over $\mathrm{End}_{\mathbb{Z}[\zeta_d]}(A)$ *acting on column vectors on the left. These matrices in fact are the images of* $\sigma_1, \ldots, \sigma_n$ *under the composition of group homomorphisms*

$$B_n \xrightarrow{\psi_n} \mathrm{GL}_n(\mathbb{Z}[t, t^{-1}]) \xrightarrow{t=\zeta_d} \mathrm{GL}_n(\mathbb{Z}[\zeta_d]) \xrightarrow{\textit{base change}} \mathrm{GL}_n(\mathrm{End}_{\mathbb{Z}[\zeta_d]}(A)).$$

Proof. The σ_j act via the braiding action on c^n by

$$(g_1, \ldots, g_n) \mapsto \left(g_1, \ldots, g_{j-2}, g_{j-1}, g_j g_{j+1} g_j^{-1}, g_j, g_{j+2}, \ldots, g_n\right).$$

By Lemma 2.0.1,

$$(a_j, \zeta_d) \cdot (a_{j+1}\zeta_d) \cdot (a_j, \zeta_d)^{-1} = (a_j + \zeta_d a_{j+1} - \zeta_d a_j, \zeta_d) = ((1-\zeta_d)a_j + \zeta_d a_{j+1}, \zeta_d).$$

The action of σ_j on corresponding column vectors is thus

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_{j-2} \\ a_{j-1} \\ (1-\zeta_d)a_j + \zeta_d a_{j+1} \\ a_j \\ a_{j+2} \\ \vdots \\ a_n \end{pmatrix}. \tag{10.1.2}$$

The image of σ_j under the unreduced Burau representation evaluated at $t = \zeta_3$ is the

block matrix

$$\begin{pmatrix} I_{j-1} & 0 & 0 & 0 \\ 0 & 1-\zeta_d & \zeta_d & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & I_{n-j-1} \end{pmatrix}.$$

Regarding the entries of this matrix as endomorphisms of A as a $\mathbb{Z}[\zeta_d]$-module, this matrix acts on the column vectors in the same way as (10.1.2) above. □

Convention 10.1.3. In view of Lemma 10.1.2, given a ring R, we will regard $R[\zeta_d]_{\text{all}}$ or quotients thereof (such as $R[\zeta_d]_{\zeta_d \neq 1}$, see Notation 4.0.1) as $R[t, t^{-1}]$-algebras by evaluating $t = \zeta_d$.

We introduce invariants preserved under the braiding action.

Definition 10.1.4 (cf. [15, Section 2.4])**.** Let $v = (g_1, \ldots, g_n)$ be an n-tuple of elements of a group G. The *global monodromy* $M_G(v)$ of this n-tuple is the subgroup $\langle g_1, \ldots, g_n \rangle$ of G. The *boundary monodromy* $M_B(v)$ of this n-tuple is the element $g_1 \cdots g_n$ of G.

Proposition 10.1.5. *Let G be a group. For any n-tuple of elements of G, the braiding action of B_n preserves the global and boundary monodromy of the n-tuple.*

Proof. The global monodromy of $\sigma_j(g_1, \ldots, g_n)$ is the subgroup of G generated by $g_1, \ldots, g_{j-2}$, $g_{j-1}, g_j g_{j+1} g_j^{-1}, g_j, g_{j+2}, \ldots, g_n$; note that the group generated by $g_j g_{j+1} g_j^{-1}$ and g_j is the same as the group generated by g_j, g_{j+1}. Thus, the global monodromy of $\sigma_j(g_1, \ldots, g_n)$ equals the subgroup of G generated by $g_1, \ldots, g_n$ and this subgroup is the global monodromy of $(g_1, \ldots, g_n)$.

The boundary monodromy of $\sigma_j(g_1, \ldots, g_n)$ is $g_1 \cdots g_{j-1} \cdot (g_j g_{j+1} g_j^{-1} \cdot g_j) g_{j+2} \cdots g_n$, which equals $g_1 \cdots g_{j-1} \cdot g_j \cdot g_{j+1} \cdot g_{j+2} \cdots g_n$, which is the boundary monodromy of $(g_1, \ldots, g_n)$. □

For the rest of this section, A is either $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$ or some $D_i/\ell D_i$ where D_i is a factor of $\mathbb{Z}_\ell[\zeta_d]$ as in (4.1.10) with involution. We note that subgroups of a group $A \rtimes \langle \zeta_d \rangle$ are determined by a submodule A' of A and an element of A/A'.

Proposition 10.1.6. *Let $d \geq 2$ be an integer, let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$, let A be a $\mathbb{Z}[\zeta_d]$-module, let $G = A \rtimes \langle \zeta_d \rangle$, and let $c \subseteq G$ be the set of elements of the form (a, ζ_d). Subgroups H of G containing at least one element of c bijectively correspond to pairs $(A', [a_0])$ where $A' \subseteq A$ is a $\mathbb{Z}[\zeta_d]$-submodule, and $[a_0] \in A/A'$. More precisely,*

1. *Given $H \leq G$, A' is the image of $H \cap (A \rtimes \langle 1 \rangle)$ under projection to the first coordinate (i.e. $A' \rtimes \langle 1 \rangle = H \cap (A \rtimes \langle 1 \rangle)$) and a_0 is any element of A such that $(a_0, \zeta_d) \in H \cap c$.*

2. *Given $(A', [a_0])$, H is the subgroup of G generated by (a_0, ζ_d) and elements of the form $(a', 1)$ where $a' \in A'$.*

We refer to H as the subset of G determined by A' and a_0.

Proof. Note that the assignment described in (1) is well defined, i.e. the class $[a_0] \in A/A'$ is independent of the choice of a_0 — if $(a_0, \zeta_d), (b_0, \zeta_d) \in H \cap c$, then $(a_0, \zeta_d)(b_0, \zeta_d)^{-1} = (a_0 - b_0, 1)$ by Lemma 2.0.1 and hence $a_0 - b_0 \in A'$.

We show that (1) and (2) describe inverse assignments. Starting with $H \leq G$, let A', a_0 be as described in (1). Further let H' be described in (2) arising from $(A', [a_0])$. Clearly $H' \subseteq H$. Moreover, for any $(a, \zeta_d^k) \in H$, note that $(\sum_{i=0}^{k-1} \zeta_d^i a_0, \zeta_d^k) = (a_0, \zeta_d)^k \in H' \subseteq H$. Therefore, $(a, \zeta_d^k) \cdot (a_0, \zeta_d)^{-k} = (a - \sum_{i=0}^{k-1} \zeta_d^i a_0, 1) \in H$ and hence $a - \sum_{i=0}^{k-1} \zeta_d^i a_0 \in A'$. Thus, $(a - \sum_{i=0}^{k-1} \zeta_d^i a_0, 1) \in H'$ and since $(\sum_{i=0}^{k-1} \zeta_d^i a_0, \zeta_d^k) \in H'$, the group H' has the element

$$\left(a - \sum_{i=0}^{k-1} \zeta_d^i a_0, 1\right) \cdot \left(\sum_{i=0}^{k-1} \zeta_d^i a_0, \zeta_d^k\right) = (a, \zeta_d^k),$$

so $H \subseteq H'$.

Conversely, starting with $(A', [a_0])$, let H be as described in (2). Let $(B', [b_0])$ be as described in (1) arising from H. Clearly $A' \subseteq B'$. Suppose for contradiction that there is some $a \in B' \setminus A'$. in particular, $(a, 1) \in H$. Choose a so that $(a, 1)$ can be written as a product of the form

$$(a_0, \zeta_d)^{k_1} \cdot (\alpha_1, 1) \cdot (a_0, \zeta_d)^{k_2} \cdot (\alpha_2, 1) \cdots$$

of shortest possible length. This product must be of the form

$$(a_0, \zeta_d)^{k_1} \cdot (\alpha_1, 1) \cdot (a_0, \zeta_d)^{k_2} \cdot (\alpha_2, 1) \cdots (a_0, \zeta_d)^{k_n}$$

and $k_1 = -k_n$, so

$$(\alpha_1, 1) \cdot (a_0, \zeta_d)^{k_2} \cdot (\alpha_2, 1) \cdots = (a_0, \zeta_d)^{-k_1} \cdot (a, 1) \cdot (a_0, \zeta_d)^{-k_n} = (\zeta_d^{-k_1} a, 1).$$

Since the product is as short as possible, $\zeta_d^{-k_1} a \in A'$, but since A' is a $\mathbb{Z}[\zeta_d]$-module, this means that $a \in A'$, which is a contradiction. Hence, $A' = B'$. Moreover, b_0 could have been chosen to be a_0 in the first place, so $[a_0] = [b_0]$. □

In view of Proposition 10.1.6, we describe how the global monodromy of

$$v_c = ((a_1, \zeta_d), \ldots, (a_n, \zeta_d))$$

is determined.

Notation 10.1.7. Given an n-tuple (or an n-row or column vector) $v = (a_1, \ldots, a_n) \in A$ where A is a $\mathbb{Z}[t, t^{-1}]$-module, write $M_{G,1}(v)$ for the $\mathbb{Z}[t, t^{-1}]$-module generated by $\{a_i - a_{i_0} : i = 1, \ldots, n\}$ for any $i_0 \in \{1, \ldots, n\}$. Note that $M_{G,1}(v)$ does not depend on the choice of i_0. Equivalently, $M_{G,1}(v)$ is generated by $\{a_i - a_j : i, j = 1, \ldots, n\}$. Further note that, under Convention 10.1.3, $M_{G,1}(v)$ is defined when A is a $\mathbb{Z}[X]/(X^d - 1)$-module.

The following proposition establishes that the global monodromy of v_c is determined exactly by $M_{G,1}(v_A)$ and the congruence class of a_{i_0} modulo $M_{G,1}(v_A)$ for any i_0 where $v_A = (a_1, \ldots, a_n)$.

Proposition 10.1.8. *Let $d \geq 2$ be an integer, let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$, let A be a $\mathbb{Z}[\zeta_d]$-module, let $G = A \rtimes \langle \zeta_d \rangle$, and let $c = \{(a, \zeta_d) \in G : a \in A\}$. Given $v_c = (g_1, \ldots, g_n) \in c^n$, write $g_i = (a_i, \zeta_d)$ and $v_A = (a_1, \ldots, a_n)$. The following hold:*

1. *$M_G(v_c) \cap c = \{(a_{i_0} + \alpha, \zeta_d) : \alpha \in M_{G,1}(v_A)\}$ for any $i_0 \in \{1, \ldots, n\}$.*

2. $M_G(v_c) \cap (A \rtimes \langle 1 \rangle) = M_{G,1}(v_A) \rtimes \langle 1 \rangle \cong M_{G,1}(v_A)$.

3. $M_G(v_c) = \langle g_{i_0}, M_{G,1}(v_A) \rtimes \langle 1 \rangle \rangle$ *for any* $i_0 \in \{1, \ldots, n\}$.

In other words, the global monodromy $M_G(v_c)$ *of* $v_c \in c^n$ *is determined (in the sense of Proposition 10.1.6) exactly by* $M_{G,1}(v_A)$ *and the equivalence class of* a_{i_0} *modulo* $M_{G,1}(V_A)$ *where* v_A *is the element of* $A^{\oplus n}$ *corresponding to* $v_c \in c^n$. *In particular, writing* $v_c, w_c \in c^n$ *by*

$$v_c = ((a_1, \zeta_d), \ldots, (a_n, \zeta_d))$$
$$w_c = ((b_1, \zeta_d), \ldots, (b_n, \zeta_d)),$$

v_c *and* w_c *have the same global monodromy if and only if* $M_{G,1}(v_A)$ *and* $M_{G,1}(w_A)$ *are equal and* a_i *and* b_j *are equivalent modulo this submodule of* A.

Proof. By Lemma 2.0.1, $(a_i, \zeta_d) \cdot (a_1, \zeta_d)^{-1} = (a_i - a_1, 1)$. In particular, $M_G(v_c)$, which is by definition generated by $g_1, \ldots, g_n$, is also generated by $g_{i_0}, (a_1 - a_{i_0}, 1), (a_2 - a_{i_0}, 1) \ldots, (a_n - a_{i_0}, 1)$ for any i_0. Furthermore, the elements $a \in A$ such that $(a, 1) \in M_G(v_c)$ form a $\mathbb{Z}[\zeta_d]$-module — if $(a, 1)$ is in $M_G(v_c)$, then $(a_{i_0}, \zeta_d) \cdot (a, 1) \cdot (a_{i_0}, \zeta_d)^{-1} = (\zeta_d a, 1)$. Therefore, $M_G(v_c) \cap (A \rtimes \langle 1 \rangle)$ contains $M_{G,1}(v_A) \rtimes \langle 1 \rangle$, and hence $M_G(v_c) \cap c$ contains all the elements of the form $(\alpha, 1) \cdot (a_{i_0}, \zeta_d) = (a_{i_0} + \alpha, \zeta_d)$ where $\alpha \in M_{G,1}(v_A)$. This containment is strict because g_i, for $i = 2, \ldots, n$, is recovered by letting $\alpha = a_1 - a_{i_0}$. In particular, $M_G(v_c) \cap (A \rtimes \langle 1 \rangle)$ equals $M_{G,1}(v_A) \rtimes \langle 1 \rangle$ as well. We have thus shown (1), (2), and (3). □

Corollary 10.1.9. *Let* $d \geq 2$ *be an integer and let* $\ell \nmid d$ *be a prime number. Let* $G = A \rtimes \langle \zeta_d \rangle$ *where* A *is a quotient of* $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{all}$. *Factorize* $\mathbb{Z}_\ell[\zeta_d]$ *as the product* $\prod_{i \in I} B_i$ *of DVR's similarly to* (4.1.9). *In particular,* A *factorizes as a product* $\prod_{i \in I'} B_i/(\ell)$ *of fields, where* I' *is a subset of* I. *Let* c *be the subset of* G *consisting of the elements of the form* (a, ζ_d) *for* $a \in A$. *Let* $v_c = (g_1, \ldots, g_n) \in c^n$, *write* $g_j = (a_j, \zeta_d)$, *and write* $v_A = (a_1, \ldots, a_n)$. *Further write* $v_{A,i}$ *for the* $B_i/(\ell)$*-component* $(a_{1,i}, \ldots, a_{n,i})$ *of* v_A.

Then, $M_G(v_c)$ is determined exactly by the $B_i/(\ell)$-modules $M_{G,1}(v_{A,i})$ and the $M_{G,1}(v_{A,i})$-equivalence class of $a_{j_0,i}$, which does not depend on the choice of j_0. More precisely, $M_{G,1}(v_A) = \prod_i M_{G,1}(v_{A,i})$ and the $M_{G,1}(v_A)$-equivalence class of a_{j_0} (which corresponds to the $M_{G,1}(v_{A,i})$-equivalence classes of $a_{j_0,i}$) determine (in the sense of Proposition 10.1.6) $M_G(v_c)$. Furthermore,

$$M_{G,1}(v_{A,i}) = \begin{cases} B_i/(\ell) & \text{if at least two of } a_{1,i}, \ldots, a_{n,i} \text{ are different} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Proposition 10.1.8, $M_G(v_c)$ is determined exactly by $M_{G,1}(v_A)$, which is generated the A-module generated by $a_2 - a_1, \ldots, a_n - a_1$, and the $M_{G,1}(v_A)$-equivalence class of a_1. The A-module $M_{G,1}(v_A)$ corresponds to the tuple of its $B_i/(\ell)$-components, which are generated by $a_{2,i} - a_{1,i}, \ldots, a_{n,i} - a_{1,i}$ and hence are $M_{G,1}(v_{A,i})$. Moreover, the $M_{G,1}(v_A)$-equivalence class of a_{j_0} corresponds to the tuple of the $M_{G,1}(v_{A,i})$-equivalence classes of $a_{j_0,i}$. Lastly, since $B_i/(\ell)$ is a field, $M_{G,1}(v_{A,i})$ is $B_i/(\ell)$ itself if and only if any of the $a_{2,i} - a_{1,i}, \ldots, a_{n,i} - a_{1,i}$ is nonzero. □

Proposition 10.1.10. *Let $d \geq 2$ be an integer, let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{all}$, let A be a $\mathbb{Z}[\zeta_d]$-module, let $G = A \rtimes \langle \zeta_d \rangle$, and let c be the set $\{(a, \zeta_d) : a \in A\}$. Given $v_A = (a_1, \ldots, a_n) \in A^{\oplus n}$, identify v_A with $v_c \in c^n$ under Convention 10.0.1. The boundary monodromy $M_B(v_c)$ equals $(\sum_{i=1}^n \zeta_d^{i-1} a_i, \zeta_d^n)$. Therefore, with n fixed, the boundary monodromy of an element of c^n is determined exactly by the linear invariant $\sum_{i=1}^n \zeta_d^i a_i$.*

Proof. The boundary monodromy of c_n is

$$(a_1, \zeta_d) \cdots (a_n, \zeta_d),$$

and calculating this as $(\sum_{i=1}^n \zeta_d^{i-1} a_i, \zeta_d^n)$ is immediate. □

In view of Corollary 10.1.9 and Proposition 10.1.10, we introduce the following terminology to more easily discuss the boundary and global monodromy invariants when using

Convention 10.0.1.

Definition 10.1.11. Let $d \geq 2$ be an integer, and let $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{\text{all}}$. Given a $\mathbb{Z}[\zeta_d]$-module A, and $v_A = (a_1, \ldots, a_n) \in A^{\oplus n}$, we define $M_B(v) := \sum_{i=1}^n a_i \zeta_d^i$ to be the *boundary monodromy* of v_A. In view of Proposition 10.1.10, $M_B(v_c) = (\zeta_d^{-1} M_B(v_A), \zeta_d^n)$ where v_c corresponds to v_A under Convention 10.0.1.

By the *global monodromy* $M_G(v_A)$ of v_A, we mean the global monodromy $M_G(v_c)$ of $v_c = ((a_1, \zeta_d), \ldots, (a_n, \zeta_d)) \in c^n$. Proposition 10.1.8 shows that $M_G(v_A)$ is determined exactly by $M_{G,1}(v_A)$ and the $M_{G,1}(v_A)$-equivalence class of $a_1, \ldots, a_n$. In the case that A is a quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$ with $\ell \nmid d$ a prime number, Corollary 10.1.9 in fact shows that $M_G(v_A)$ is determined exactly by whether $a_{1,i}, \ldots, a_{n,i} \in B_i$ are the same and, if so, what this value is across the i's indexing the factorization $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \prod_i B_i$.

10.2 A nice change of basis

Let $\mathcal{C}$ be the $n \times n$ matrix over $\mathbb{Z}[t, t^{-1}]$ given by

$$\mathcal{C} = \begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & -\frac{1}{t} & \frac{1}{t} & 0 & \cdots & 0 & 0 \\ 1 & 0 & -\frac{1}{t^2} & \frac{1}{t^2} & \cdots & 0 & 0 \\ 1 & 0 & 0 & -\frac{1}{t^3} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & -\frac{1}{t^{n-2}} & \frac{1}{t^{n-2}} \\ 1 & 0 & 0 & 0 & \cdots & 0 & -\frac{1}{t^{n-1}} \end{pmatrix}. \tag{10.2.1}$$

We describe how the change of basis by $\mathcal{C}$ changes the presentations of the unreduced Burau matrices $\psi_n(\sigma_i)$, the unitary matrix H_n, and the boundary monodromy function — the presentations are essentially given by the matrices and vectors computed in Lemma 10.2.1. In particular, B_n acts on the vectors under the change of basis by $\mathcal{C}$ by the *reduced* Burau representation ψ_n^r on all but the first coordinate.

Let A be a $\mathbb{Z}[t,t^{-1},\det(\mathcal{C})]$-module. Given a vector $v \in A^{\oplus n}$, write v_{ψ_n} for the column vector of v with respect to the elementary basis elements $e_1,\dots,e_n \in A^{\oplus n}$ and $v_{\mathcal{C}}$ for the column vector of v with respect to the basis elements $\sum_{i=1}^n e_i, e_1 - \frac{1}{t}e_2, \frac{1}{t}e_2 - \frac{1}{t^2}e_3, \dots, \frac{1}{t^{n-2}}e_{n-1} - \frac{1}{t^{n-1}}e_n$. In particular, $v_{\psi_n} = \mathcal{C}v_{\mathcal{C}}$ for every v. The action of $\sigma_i \in B_n$ via the unreduced Burau representation ψ_n acting on $A^{\oplus n}$ sends a column vector v_{ψ_n} to $\psi_n(\sigma_i)v_{\psi_n}$. Correspondingly, the action of σ_i sends a column vector $v_{\mathcal{C}}$ to $(\mathcal{C}^{-1}\psi_n(\sigma_i)\mathcal{C})v_{\mathcal{C}}$. Moreover, letting h be the Hermitian form (5.1.2) given by H_n, we have $h(v,w) = v_{\psi_n}^* H_n w_{\psi_n} = v_{\mathcal{C}}^*(\mathcal{C}^* H_n \mathcal{C})w_{\mathcal{C}}$, so h is given by the matrix $\mathcal{C}^* H_n \mathcal{C}$ with respect to the change of basis. Lastly, the boundary monodromy function is given by the row vector $\begin{pmatrix} t & t^2 & \dots & t^n \end{pmatrix}$ multiplied to the left of v_{ψ_n} (and evaluated at $t = \zeta_d$), so the function is given by the multiplication by $\begin{pmatrix} t & t^2 & \dots & t^n \end{pmatrix}\mathcal{C}^{-1}$ to the left of $v_{\mathcal{C}}$.

Lemma 10.2.1 calculates the matrices $\mathcal{C}^{-1}\psi_n(\sigma_i)\mathcal{C}$, $\mathcal{C}^* H_{n,-1,1}\mathcal{C}$, and $\begin{pmatrix} t & t^2 & \dots & t^n \end{pmatrix}\mathcal{C}^{-1}$; recall the notation $H_{n,a,b}$ introduced after (5.1.1).

Lemma 10.2.1. *1.* $\det(\mathcal{C}) = \frac{(-1)^{n+1}\sum_{i=0}^{n-1} t^i}{t^{n(n-1)/2}}$

2. Over $\mathbb{Z}[t,t^{-1},\det(\mathcal{C})]$,

$$\mathcal{C}^{-1}\psi_n(\sigma_i)\mathcal{C} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \psi_n^r(\sigma_i) \end{array}\right)$$

for every $i = 1,\dots,n-1$.

3.

$$\mathcal{C}^* H_{n,-1,1}\mathcal{C} = \left(\begin{array}{c|c} S & 0 \\ \hline 0 & H_n^r \end{array}\right)$$

where

$$S = -\left(\sum_{i=1}^{n-2}(n-i-1)t^i + (n-2) + \sum_{i=-n+2}^{-1}(n+i-1)t^i\right). \tag{10.2.2}$$

Note that $S = \overline{S}$.

4. $\begin{pmatrix} \zeta_d & \zeta_d^2 & \dots & \zeta_d^n \end{pmatrix}\mathcal{C} = \begin{pmatrix} \sum_{i=1}^n \zeta_d^i & 0 & \dots & 0 \end{pmatrix}$.

Proof. One can verify (1) by applying elementary column operators to $\mathcal{C}$ to transform $\mathcal{C}$ into an upper triangular matrix. One can also arithmetically verify (2), (3), and (4). $\square$

Therefore, writing $v_{\mathcal{C}} = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}^T$, the action of B_n via ψ_n fixes the first coordinate α_1 and is given by ψ_n^r on the other coordinates, the boundary monodromy of v is a multiple of α_1 by an invertible element, and the norm of v with respect to H_n is $\alpha_1 \cdot \overline{\alpha}_1 \cdot S$, where S is as in Lemma 10.2.1(3), plus the norm of $\begin{pmatrix} \alpha_2 & \cdots & \alpha_n \end{pmatrix}^T$ with respect to H_n^r.

We also prove Lemma 10.2.2 and Lemma 10.2.3 to later establish the invertibility of $\mathcal{C}$ and $H_{n,-1,1}$ over $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$ in certain circumstances.

Lemma 10.2.2. *Let $d \geq 2$ be an integer. Let μ_d be a primitive dth root of unity in $\overline{\mathbb{Q}}$ and suppose that $d \nmid n$. Then $1 - \mu_d$ and $\sum_{i=0}^{n-1} \mu_d^i$ respectively divide d and $\frac{d}{\gcd(d,n)}$ as elements of the ring $\mathbb{Z}[\mu_d]$.*

Proof. Given a primitive eth root of unity μ, we have $X^{e-1} + \cdots + 1 = \prod_{i=1}^{e-1}(X - \mu^i)$. Evaluating at $X = 1$ yields $e = \prod_{i=1}^{e-1}(1 - \mu^i)$. Letting $e = d$ proves that $1 - \mu_d$ divides d. Letting $\mu = \mu_d^n$ so that $e = \frac{d}{\gcd(d,n)}$ yields $e = \prod_{i=1}^{e-1}(1 - \mu^i)$. Since $(1 - \mu) = (1 - \mu_d) \cdot \sum_{i=0}^{n-1} \mu_d^i$, we thus have that $\sum_{i=1}^{n-1} \mu_d^i$ divides e. $\square$

Lemma 10.2.3. *The expression S in* (10.2.2) *equals $\frac{t(1-t^{-n})}{(1-t^{-1})} \cdot \frac{1-t^{n-2}}{1-t}$.*

Proof. This holds because

$$\begin{aligned}
S - t^{-1}S &= \left(\sum_{i=1}^{n-2}(n-i-1)t^i + (n-2) + \sum_{i=-n+2}^{-1}(n+i-1)t^i\right) \\
&\quad - \left(\sum_{i=0}^{n-3}(n-i-2)t^i + (n-2)t^{-1} + \sum_{i=-n+1}^{-2}(n+i)t^i\right) \\
&= \left(t^{n-2} + \sum_{i=1}^{n-3}(n-i-1)t^i + (n-2) + (n-2)t^{-1} + \sum_{i=-n+2}^{-2}(n+i-1)t^i\right) \\
&\quad - \left(\sum_{i=1}^{n-3}(n-i-2)t^i + (n-2) + (n-2)t^{-1} + \sum_{i=-n+2}^{-2}(n+i)t^i + t^{-n+1}\right) \\
&= t^{n-2} + \sum_{i=1}^{n-3}t^i - \sum_{i=-n+2}^{-2}t^i - t^{-n+1} \\
&= \sum_{i=1}^{n-2}t^i - \sum_{i=-n+1}^{2}t^i \\
&= (t - t^{-n+1}) \cdot \sum_{i=0}^{n-3}t^i.
\end{aligned}$$

□

Lemma 10.2.4 below translates Proposition 10.1.8 and Corollary 10.1.9 to describe the global monodromy of a vector in $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]^{\oplus n}$ with respect to the base change by $\mathcal{C}$.

Lemma 10.2.4. *Let $D \geq 2$ be an integer and let $\ell \nmid d$ be a prime number. Let $G = A \rtimes \langle \zeta_d \rangle$ where A is a quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$. Factorize $\mathbb{Z}_\ell[\zeta_d]$ as the product $\prod_i B_i$ of DVR's similarly to* (4.1.9)*. Let n be an integer such that* $\gcd(d, n) = 1$*. In particular, $\sum_{i=0}^{n-1}\zeta_d^i$ and $\mathcal{C}$ are invertible over $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]$ by Lemma 10.2.1 and Lemma 10.2.2. Given $v_A = v_{A,\psi_n} = (a_1, \ldots, a_n)^T \in A^{\oplus n}$ written with respect to the standard basis of $A^{\oplus n}$, write $v_{A,\mathcal{C}} = (a'_1, \ldots, a'_n)^T$ for its base change under $\mathcal{C}$, i.e. $v_{A,\psi_n} = \mathcal{C}v_{A,\mathcal{C}}$. Write additional subscripts of i on vectors over A or elements of A to indicate $B_i/(\ell)$-components; for instance $v_{A,i}$ is the $B_i/(\ell)$-component of v_A and $a_{1,i}$ is the $B_i/(\ell)$-component of a_1.*

The following hold:

1. *$M_{G,1}(v_{A,i}) \subseteq B_i/(\ell)$ is $B_i/(\ell)$ if and only if at least one of $a'_{2,i}, \ldots, a'_{n,i}$ is nonzero*

and is 0 *otherwise.*

2. *$M_G(v_A)$ is determined (as per Proposition 10.1.6) by $M_{G,1}(v_A)$ and*

$$a'_1 = \left(\sum_{i=1}^{n} \zeta_d^i\right)^{-1} M_B(v_A).$$

In particular, with d, ℓ, n fixed, $M_G(v_A)$ is determined exactly by a'_1 and by which among the $B_i/(\ell)$-components of $(a'_2, \ldots, a'_n)^T$ are zero. In fact, $M_{G,1}(v_A)$ is the A-module generated by $a'_2, \ldots, a'_n$.

Proof. We show (1). By Corollary 10.1.9, $M_{G,1}(v_{A,\psi_n,i})$ is 0 if and only if the $B_i/(\ell)$-component of v_{A,ψ_n} has all of the same coordinates. Since $v_{A,\psi_n} = \mathcal{C}v_{A,\mathcal{C}}$, this is turn happens exactly when $(a'_{2,i}, \ldots, a'_{n,i})^T$ is zero. Otherwise, $M_{G,1}(v_{A,\psi_n,i})$ is $B_i/(\ell)$.

We now show (2). By Corollary 10.1.9, $M_G(v_A)$ is determined by $M_{G,1}(v_A)$ and a_1, which equals $a'_1 + a'_2$. If $(a'_{2,i}, \ldots, a'_{n,i})^T$ is nonzero, then $M_{G,1}(v_{A,i}) = B_i/(\ell)$. Otherwise, $a_{1,i} = a'_{1,i}$. In either case, $a_{1,i}$ and $a'_{1,i}$ are in the same $M_{G,1}(v_{A,i})$-equivalence class, so a'_1 and a_1 are in the same $M_{G,1}(v_A)$-equivalence class. Therefore, $M_G(v_A)$ is determined by $M_{G,1}(v_A)$ and a'_1 as desired. Also recall from Lemma 10.2.1 and the discussion preceding it that $M_B(v_A) = \sum_{i=1}^{n} \zeta_d^i a'_1$. □

10.3 The Orbits of the unreduced Burau representation evaluated at $t = \zeta_d$ modulo ℓ are determined by three invariants

In Theorem 10.3.7, we show that the orbits of the unreduced Burau representations evaluated at $t = \zeta_d$ modulo ℓ for sufficiently large n are determined by the three invariants — the global monodromy, the boundary monodromy, and the norm — of their elements.

Via Lemma 10.3.1, we first establish orbits of the action of SU to later use the fact (Section 10.2) that the unreduced Burau representation is essentially almost given by the

reduced Burau representation and to use Venkataramana's [43] results showing that the reduced Burau representation is an arithmetic subgroup of the appropriate unitary group.

Lemma 10.3.1. *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, and let $n \geq 4$ be an integer. Let $A = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$ or an involution ring quotient thereof. In particular, A factors in the form $\prod_i D_i/(\ell)$ where the indices i here run over a subset of the indices i appearing in the factorization $\mathbb{Z}_\ell[\zeta_d] = \prod_i D_i$ recorded in* (4.1.10) *where the D_i are division or double division rings with involution. Equip $A^{\oplus n}$ with a nonsingular ε_A-Hermitian form H (see Notation 4.0.1). Write H_i for the $D_i/(\ell)$-component of H as in Lemma 4.0.8; the H_i are nonsingular. Whenever D_i is a double division ring, write $D_i = B_i \times B_i'$ where $B_i' = B_i$ is an integral domain and the involution on D_i is given by $(a, b) \mapsto (b, a)$. Let $v_1, v_2 \in A^{\oplus n}$ and write $v_{1,i}, v_{2,i}$ for the D_i-component of v_1 and v_2.*

Then, v_1 and v_2 are in the same orbit under the action of $\mathrm{SU}(A^{\oplus n})$ if and only if the exactly one of the following hold for each i:

1. *$v_{1,i}$ and $v_{2,i}$ are both 0,*
2. *The norms $H_i(v_{1,i}, v_{1,i})$ and $H_i(v_{2,i}, v_{2,i})$ are equal and invertible elements of D_i.*
3. *D_i is an integral domain, $v_{1,i}$ and $v_{2,i}$ are both nonzero, and have zero norm.*
4. *D_i is a double division ring, and $v_{1,i}$ and $v_{2,i}$ either both have zero $B_i/(\ell)$-component and nonzero $B_i'/(\ell)$-component, or vice versa.*
5. *D_i is a double division ring, $v_{1,i}$ and $v_{2,i}$ both have nonzero $B_i/(\ell)$ and $B_i'/(\ell)$-components, and $v_{1,i}$ and $v_{2,i}$ both have zero norm.*

Proof. Since $\mathrm{SU}(A) \cong \prod_i \mathrm{SU}(D_i/(\ell)^{\oplus n})$, it suffices to prove that the properties described in (1)-(5) determine orbits of the action of $\mathrm{SU}(D_i/(\ell)^{\oplus n})$ on $D_i/(\ell)^{\oplus n}$. Moreover, note that the properties (of being 0, having a specific norm, having zero $B_i/(\ell)$ and $B_i'(\ell)$ components) are all preserved under $\mathrm{SU}(D_i/(\ell)^{\oplus n})$, so the "only if" direction holds. We now prove the "if" direction.

First suppose that $\zeta_d = -1$ in D_i, which can only occur when d is even. In this case, only (1) or (3) can occur. Clearly, 0 forms its own orbit. If $v_{1,i}$ and $v_{2,i}$ are both nonzero, then they are in the same orbit under $\mathrm{SU}(D_i/(\ell)^{\oplus n}) \cong \mathrm{Sp}(D_i/(\ell)^{\oplus n})$.

Now suppose that $\zeta_d \neq -1$ in D_i instead. Again, 0 forms its own orbit. To establish that (2) describes an orbit, suppose that the norms of $v_1, v_2 \in D_i/(\ell)^{\oplus n}$ are equal and invertible as elements of $D_i/(\ell)$ (in fact of $D_i/(\ell)^{\cdot}$). By Lemma 4.0.7, $(D_i/(\ell)^{\oplus n}, H_i) = (\langle v_j \rangle, H_i|_{\langle v_j \rangle}) \perp (\langle v_j \rangle^{\perp}, H_i|_{\langle v_j \rangle^{\perp}})$ for $j = 1, 2$. In particular, $(\langle v_j \rangle^{\perp}, H_i|_{\langle v_j \rangle^{\perp}})$ is nonsingular, so it has an orthornomal basis by Proposition 4.1.7. Any automorphism φ on $D_i/(\ell)^{\oplus n}$ sending v_1 and v_2 and an orthonormal basis of $(\langle v_1 \rangle^{\perp}, H_i|_{\langle v_1 \rangle^{\perp}})$ to an orthonormal basis of $(\langle v_2 \rangle^{\perp}, H_i|_{\langle v_2 \rangle^{\perp}})$ is an element of $\mathrm{U}(D_i^{\oplus n})$. Scaling one of the basis elements of $(\langle v_2 \rangle^{\perp}, H_i|_{\langle v_2 \rangle^{\perp}})$ by $\frac{1}{\det \varphi}$ and replacing φ accordingly thus makes φ an element of $\mathrm{SU}(D_i/(\ell)^{\oplus n})$ sending v_1 to v_2.

To establish that (3) and (5) describe orbits, now suppose that the conditions specified in (3) or (5) hold. Via Proposition 4.1.7, identify an orthonormal basis of H_i and write

$$v_{1,i} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \quad v_{2,i} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

with respect to the orthornormal basis. In the case that D_i is a double division ring, replace $v_{1,i}$ and $v_{2,i}$ if necessary with some vectors in the same SU-orbit so that at least one coordinate in each is in $D_i/(\ell)^{\times}$. Without loss of generality, say that $a_1, b_1 \in D_i/(\ell)^{\times}$. Letting $w = \begin{pmatrix} -a_1 & 0 & \cdots & 0 \end{pmatrix}^T$, note that $w \perp (v + w)$ and that the norms of w and $v + w$ are nonzero and additive inverses of each other. By Lemma 4.1.5, there is some $u \in D_i/(\ell)^{\times}$ such that $u \cdot \overline{u} = -1$. Letting $y_w := \begin{pmatrix} -a_1 & 0 & 0 & \cdots & 0 \end{pmatrix}^T$ and $y_{v+w} := \begin{pmatrix} 0 & ua_1 & 0 & \cdots & 0 \end{pmatrix}^T$, note that $y_w \perp y_{v+w}$, that w and y_w have the same norms and that $v + w$ and y_{v+w} have the same norms. Using Lemma 4.0.7 and Proposition 4.1.7 similarly as before, we can add orthonormal bases of $\langle w, v + w \rangle^{\perp}$ and $\langle y_w, y_{v+w} \rangle^{\perp}$ to the

lists $(w, v+w)$ and (y_w, y_{v+w}) respectively to obtain orthogonal bases of $D_i/(\ell)^{\oplus n}$, then let φ be the automorphism of $D_i/(\ell)^{\oplus n}$ sending the former orthogonal basis to the latter. By replacing u with an appropriate scalar multiple (alternatively, by scaling one of the added orthonormal basis vectors), φ in fact becomes an element of $\mathrm{SU}(D_i/(\ell)^{\oplus n})$. Thus, $v_{1,i}$ is in the same orbit as $y_{v+w} - y_w = \begin{pmatrix} a_1 & ua_1 & 0 & \cdots & 0 \end{pmatrix}^T$. Similarly, $v_{2,i}$ is in the same orbit as $\begin{pmatrix} b_1 & u'b_1 & 0 & \cdots & 0 \end{pmatrix}$ for some $u' \in D_i/(\ell)^\times$ assuming, without loss of generality, that $b_1 \neq 0$. In fact, just as argued before, $\begin{pmatrix} a_1 & ua_1 & 0 & \cdots & 0 \end{pmatrix}^T$ is in the same orbit as $\begin{pmatrix} a_1 & ua_1 & b_1 & u'b_1 & \cdots & 0 \end{pmatrix}^T$, which is also in the same orbit as $\begin{pmatrix} b_1 & u'b_1 & 0 & \cdots & 0 \end{pmatrix}$. Thus, $v_{1,i}$ and $v_{2,i}$ are in the same orbit as desired.

To establish that (4) describes an orbit, suppose that D_i is a double division ring, without loss of generality, that $v_{1,i}$ and $v_{2,i}$ both have nonzero $B_i/(\ell)$-component and zero $B_i'/(\ell)$-component. Note that $\mathrm{SU}(D_i/(\ell)^{\oplus n}) \subset \mathrm{SL}(B_i/(\ell)^{\oplus n}) \times \mathrm{SL}(B_i'/(\ell)^{\oplus n})$ is the image of $\mathrm{SL}(B_i/(\ell)^{\oplus n})$ under the embedding $\tau \mapsto \tau \times (\tau^T)^{-1}$. In particular, there is some element of $\mathrm{SL}(B_i/(\ell)^{\oplus n})$ taking the $B_i/(\ell)$-component of $v_{1,i}$ to that of $v_{2,i}$ and hence there is an element of $\mathrm{SU}(D_i/(\ell)^{\oplus n})$ taking $v_{1,i}$ to $v_{2,i}$. □

We induct on n to prove that the orbits of the unreduced Burau representation on $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d]^{\oplus n}$ are determined by the three invariants. Proposition 10.3.2 serves as the base case to this induction.

Proposition 10.3.2. *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, and let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$. Suppose that $n \geq 4$ is an integer such that $\gcd(d, n(n-2)) = 1$ and the image of ψ_n^r evaluated at $\zeta_d \in A$ modulo ℓ contains $\mathrm{SU}(A^{\oplus(n-1)})$ where $A^{\oplus(n-1)}$ is equipped with the Hermitian form $\tilde{h}_n^r$ (see Section 5.1).*

The orbit of any element $v_A \in A^{\oplus n}$ under the action of B_n via ψ_n evaluated at ζ_d modulo ℓ is determined precisely by the global monodromy $M_G(v_A)$, the boundary monodromy $M_B(v_A)$ (Definition 10.1.11), and norm under h base changed to A as described in Section 5.1, where h is given by the unitary matrix $H_{n,-1,1}$.

Remark 10.3.3. Suppose that $A = \mathbb{Z}/\ell\mathbb{Z}[X]/(X+1)$. For $n \geq 4$, the orbits of $v_A \in A^{\oplus n}$

under the action of B_n via ψ_n evaluated at ζ_d modulo ℓ are determined precisely by the global monodromy $M_G(v_A)$ and the boundary monodromy $M_B(v_A)$, cf. [13, Proof of Proposition 2.7]. Indeed, since $\zeta_d = -1$ and since the involution on A is trivial, one can compute

$$v_A^* H_{n,-1,1} v_A = -M_B(v_A)^2.$$

so the boundary monodromy determines the norm of v_A under the Hermitian form given by $H_{n,-1,1}$.

Proof. Factorize $A = \prod_i D_i/(\ell)$ as in Lemma 10.3.1 and write $D_i = B_i$ if D_i is an integral domain and $D_i = B_i \times B_i'$ if D_i is a double division ring.

Proposition 10.1.5 and Proposition 10.1.10 show that any two elements in the same orbit have the same global and boundary monodromies. The discussion in Section 5.1 describes that the action of B_n preserves the norm under h. Conversely, we show that any two elements of $A^{\oplus n}$ with the same monodromies and norm are in the same orbit.

Since $\ell \nmid d$ and since $\gcd(d, n) = 1$, $\sum_{i=1}^n \zeta_d^i$ is invertible in A by Lemma 10.2.1. In particular, the matrix $\mathcal{C}$, evaluated at $t = \zeta_d$, specified in (10.2.1) is invertible by Lemma 10.2.2. Writing v_{ψ_n} and $v_{\mathcal{C}}$ for the column vectors of $v \in A^{\oplus n}$ with respect to the elementary bases $e_1, \ldots, e_n$ and $\sum_{i=1}^n e_i, e_1 - \frac{1}{t}e_2, \frac{1}{t}e_2 - \frac{1}{t^2}e_3, \ldots, \frac{1}{t^{n-2}}e_{n-1} - \frac{1}{t^{n-1}}e_n$ respectively, recall from Section 10.2 that the action of $\sigma_i \in B_n$ on $v_{\mathcal{C}}$ is given by $\mathcal{C}^{-1}\psi_n(\sigma_i)\mathcal{C} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \psi_n^r(\sigma_i) \end{array}\right)$, that the boundary monodromy function is given by the multiplication by $\begin{pmatrix} \zeta_d & \zeta_d^2 & \cdots & \zeta_d^n \end{pmatrix} \mathcal{C}^{-1} = \begin{pmatrix} \sum_{i=1}^n \zeta_d^i & 0 & \cdots & 0 \end{pmatrix}$ to the left of $v_{\mathcal{C}}$, and that $\mathcal{C}^* H_{n,-1,1} \mathcal{C} = \left(\begin{array}{c|c} S & 0 \\ \hline 0 & H_n^r \end{array}\right)$ is the matrix of h under the base change by $\mathcal{C}$. By Lemma 10.2.3 and Lemma 10.2.2 and since $\gcd(d, n(n-2)) = 1$, S is invertible in A. For the rest of this proof, let $H_n = H_{n,-1,1}$.

Writing $v_{\mathcal{C}} = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}^T$, further recall that the action of B_n via ψ_n fixes the first coordinate α_1 and is given by ψ_n^r on the other coordinates, the boundary monodromy of v is a multiple of α_1 by an invertible element, and the norm of v with respect to H_n is

$S \cdot \alpha_1 \cdot \overline{\alpha}_1$ plus the norm of $\begin{pmatrix} \alpha_2 & \cdots & \alpha_n \end{pmatrix}^T$ with respect to H_n^r.

Now say that $v, w \in A^{\oplus n}$ have the same monodromies and norm and write $v_{\mathcal{C}} = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}^T, w_{\mathcal{C}} = \begin{pmatrix} \beta_1 & \cdots & \beta_n \end{pmatrix}^T$. It suffices to show that $v_{\mathcal{C}}$ and $w_{\mathcal{C}}$ are in the same orbit under the action of the group of matrices of the form

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \psi_n^r(\sigma) \end{array}\right),$$

with $\sigma \in B_n$. Since v and w have the same boundary monodromy, $\alpha_1 = \beta_1$. Moreover, $v'_{\mathcal{C}} := \begin{pmatrix} \alpha_2 & \cdots & \alpha_n \end{pmatrix}^T$ and $w'_{\mathcal{C}} := \begin{pmatrix} \beta_2 & \cdots & \beta_n \end{pmatrix}^T$ have the same norm given by H_n^r since $v_{\mathcal{C}}$ and $w_{\mathcal{C}}$ have the same norm given by $\mathcal{C}^* H_n \mathcal{C}$. Equivalently, $v'_{\mathcal{C}}$ and $w'_{\mathcal{C}}$ have the same $\tilde{h}_n^r$-norm because $\tilde{h}_n^r$ is given by H_n^r over factors D_i where $\zeta_d \neq -1$ and $\tilde{h}_n^r$ is a symplectic form over factors D_i where $\zeta_d = -1$ and H_n^r evaluates to 0 at $t = \zeta_d = -1$.

By [43, Lemma 13], $\det H_n^r$, before evaluating t, is $\left(\frac{t+1}{t}\right)^{n-1} \left(\frac{t^n-1}{t-1}\right)$. Thus, the Hermitian form given by H_n^r is nonsingular exactly when $t+1$ and $\frac{t^n-1}{t-1} = \sum_{i=0}^{n-1} t^i$ evaluate to be invertible values. The only D_i on which $t+1$ is not invertible is $D_i = \mathbb{Z}_\ell[X]/(X+1)$, which is a factor of $\mathbb{Z}_\ell[\zeta_d]$ only when d is even. In this case, n must be odd since $\gcd(d, n(n-2))$ is assumed to be 1. In particular, $\det \tilde{H}_n^r = 1$ by (5.1.4), so $\tilde{h}_n^r$ is nonsingular.

By Lemma 10.2.4, when a vector v has fixed boundary monodromy, its global monodromy is determined exactly by the sets

$$\{B_i : \text{ the } B_i/(\ell)\text{-component of } v'_{\mathcal{C}} \text{ is nonzero}\}$$
$$\{B'_i : D_i = B_i \cup B'_i \text{ and the } B'_i/(\ell)\text{-component of } v'_{\mathcal{C}} \text{ is nonzero}\}.$$

For each factor D_i, write $v'_{\mathcal{C},i}$ and $w'_{\mathcal{C},i}$ for the D_i-components of $v'_{\mathcal{C}}$ and $w'_{\mathcal{C}}$. In particular, $v'_{\mathcal{C},i} = 0$ if and only if $w'_{\mathcal{C},i} = 0$. Similarly, when $D_i = B_i \times B'_i$, the $B_i/(\ell)$-component (resp. $B'_i/(\ell)$-component) of $v'_{\mathcal{C},i}$ is 0 if and only if the corresponding component of $w'_{\mathcal{C},i}$ is zero. Lemma 10.3.1 hence shows that $v'_{\mathcal{C}}$ and $w'_{\mathcal{C}}$ are in the same orbit under the action of $\mathrm{SU}(A^{\oplus(n-1)})$. $\square$

Lemma 10.3.4 is the main idea driving the inductive step of the aforementioned induction. It establishes that each orbit of the unreduced Burau representation has a vector with a specified, "nice" first coordinate and that truncating this first coordinate preserves the global monodromy. If two vectors have the same monodromies, norm, and first coordinate, then Lemma 10.3.6 then shows that truncating the first coordinates from the two vectors results in vectors with the same boundary monodromy and norm.

Lemma 10.3.4. *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$, and let $n \geq 6$ be an integer such that $\gcd(d, n) = 1$. Say that $v = v_{\psi_n} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}^T \in A^{\oplus n}$ is a column vector. Write D_i and B_i, B_i' as in the proof of Proposition 10.3.2. Write $M_{G,i} = M_{G,1}(v_{\psi_n,i}) \subseteq D_i$ for each i.*

There is some column vector $w = w_{\psi_n} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix}^T \in A^{\oplus n}$ such that, writing $w_{\psi_n}^{trun} = \begin{pmatrix} b_2 & b_3 & \cdots & b_n \end{pmatrix}^T$,

- $M_G(v_{\psi_n}) = M_G(w_{\psi_n}) = M_G(w_{\psi_n}^{trun})$,
- $M_B(v_{\psi_n}) = M_B(w_{\psi_n})$,
- $N(v_{\psi_n}) = N(w_{\psi_n})$, *where N is the norm with respect to $H_{n,-1,1}$, and*
- $b_{1,i}$ *is*

$$b_i := \begin{cases} 0 & \text{if } M_{G,i} = D_i \\ (0, \beta') & \text{if } D_i = B_i \times B_i' \text{ and } M_{G,i} = B_i/(\ell) \times 0 \\ (\beta, 0) & \text{if } D_i = B_i \times B_i' \text{ and } M_{G,i} = 0 \times B_i'/(\ell), \\ \gamma & \text{if } M_{G,i} = 0 \end{cases} \tag{10.3.1}$$

for every i; here, we let $\gamma \in D_i$ be any $M_{G,i}$-congruence class representative such that $M_G(v_{\psi_n,i})$ is determined (in the sense of Proposition 10.1.6) by $M_{G,i}$ and γ and we write $\gamma = (\beta, \beta')$ if $D_i = B_i \times B_i'$.

Remark 10.3.5. Like Proposition 10.3.2, Lemma 10.3.4 requires d and n to be relatively prime because both facts require the change of basis by $\mathcal{C}$. However, unlike Proposition 10.3.2, Lemma 10.3.4 does not require d and $n-2$ to be relatively prime — whereas the former requires the expression S introduced in Lemma 10.2.1 to be invertible, the latter does not.

Proof. Let $w_{\psi_n} \in A^{\oplus n}$. Write $v_{\psi_n,i}$ for the $D_i/(\ell)$-component of $v = v_{\psi_n}$. Write $N(v_{\psi_n,i}) = v_{\psi_n,i}^* H_{n,-1,1} v_{\psi_n,i} \in D_i^-$ norm of $v_{\psi_n,i}$. Write $M_{B,i} \in D_i$ for $\left(\sum_{i=0}^{n-1} \zeta_d^i\right)^{-1} \cdot M_B(v_{\psi_n,i})$, which is well defined by Lemma 10.2.2. If $v_{\psi_n,i}$ has all the same coordinates, then $M_G(v_{\psi_n,i}) \cap (D_i/(\ell) \rtimes \langle 1 \rangle) = 0 \rtimes \langle 1 \rangle$ by Corollary 10.1.9. In this case, $M_G(v_{\psi_n,i}) = M_G(w_{\psi_n,i})$ if and only if $v_{\psi_n,i} = w_{\psi_n,i}$.

Now suppose that $v_{\psi_n,i}$ has at least two distinct coordinates. If $D_i = B_i \times B_i'$ and $M_{G,i} = B_i/(\ell) \times 0$, then β' in the definition (10.3.1) equals the $B_i'/(\ell)$-components of all of $a_{1,i}, \ldots, a_{n,i}$. In this case, $M_G(v_{\psi_{n,i}}) = M_G(w_{\psi_n,i})$ if and only if the $B_i'/(\ell)$-components of $v_{\psi_{n,i}}$ and $w_{\psi_{n,i}}$ coincide. By symmetry, analogous facts are true when $M_{G,i} = 0 \times B_i'/(\ell)$.

$M_{B,i}$	$N(v_{\psi_n,i})$	$M_{G,i}$	$w_{\mathcal{C},i}$	$w_{\psi_n,i}$
Invertible	Any	D_i	$\begin{pmatrix} M_{B,i} \\ -M_{B,i} \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1-\zeta_d^{-1})M_{B,i} \\ M_{B,i} + \alpha\zeta_d^{-2} \\ M_{B,i} - \alpha\zeta_d^{-3} \end{pmatrix}$
0	$\neq 0$	D_i	$\begin{pmatrix} 0 \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ \alpha\zeta_d^{-1} \\ -\alpha\zeta_d^{-2} \end{pmatrix}$
0	0	D_i	$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ \zeta_d^{-1} \\ -\zeta_d^{-2} \\ \alpha\zeta_d^{-3} \\ -\alpha\zeta_d^{-4} \end{pmatrix}$

Table 10.1: Descriptions of the first several coordinates of $w_{\mathcal{C},i}$ such that the first coordinate of $w_{\psi_n,i}$ is $b_i = 0$ when D_i is an integral domain. The unwritten trailing coordinates of $w_{\mathcal{C},i}$ are all 0. Since $w_{\psi_n,i} = \mathcal{C} w_{\mathcal{C},i}$, the unwritten trailing coordinates of $w_{\psi_n,i}$ must be all $M_{B,i}$. Where appropriate, $\alpha \in D_i$ is chosen via Lemma 4.1.5 to ensure that the norm of $w_{\mathcal{C},i}$ equals $N(v_{\psi_n,i})$.

Tables 10.1, 10.2, and 10.3 list (the first several coordinates of the) column vectors $w_{\mathcal{C},i}$ corresponding to desired $w_{\psi_n,i}$ under the base change by $\mathcal{C}$, i.e. $w_{\psi_n,i}$ has the same

$M_{B,i}$	$N(v_{\psi_n,i})$	$M_{G,i}$	$w_{\mathcal{C},i}$	$w_{\psi_n,i}$
Invertible	Any	D_i	$\begin{pmatrix} M_{B,i} \\ -M_{B,i} \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1-\zeta_d^{-1})M_{B,i} \\ M_{B,i}+\alpha\zeta_d^{-2} \\ M_{B,i}-\alpha\zeta_d^{-3} \end{pmatrix}$
(β,β') Invertible	$S\cdot M_{B,i}\cdot\overline{M_{B,i}}$	$B_i/(\ell)\times 0$	$\begin{pmatrix} M_{B,i} \\ (-\beta,0) \end{pmatrix}$	$\begin{pmatrix} (0,\beta') \\ (\beta,\beta')+\zeta_d^{-1}(\beta,0) \end{pmatrix}$
Invertible	$\neq S\cdot M_{B,i}\cdot\overline{M_{B,i}}$	$B_i/(\ell)\times 0$	N/A	N/A
0	$\neq 0$ (i.e. invertible)	D_i	$\begin{pmatrix} 0 \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ \alpha\zeta_d^{-1} \\ -\alpha\zeta_d^{-2} \end{pmatrix}$
0	$\neq 0$	$B_i/(\ell)\times 0$	N/A	N/A
0	0	D_i	$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ \zeta_d^{-1} \\ -\zeta_d^{-2} \\ \alpha\zeta_d^{-3} \\ -\alpha\zeta_d^{-4} \end{pmatrix}$
0	0	$B_i/(\ell)\times 0$	$\begin{pmatrix} 0 \\ 0 \\ (1,0) \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1,0)\zeta_d^{-1} \\ -(1,0)\zeta_d^{-2} \end{pmatrix}$

Table 10.2: Descriptions of the first several coordinates of $w_{\mathcal{C},i}$ such that the first coordinate of $w_{\psi_n,i}$ is b_i when $D_i = B_i \times B_i'$ is a double division ring and $M_{B,i}$ is either invertible or 0. The unwritten trailing coordinates of $w_{\mathcal{C},i}$ are all 0. Since $w_{\psi_n,i} = \mathcal{C}w_{\mathcal{C},i}$, the unwritten trailing coordinates of $w_{\psi_n,i}$ must be all $M_{B,i}$. Where appropriate, $\alpha \in D_i$ is chosen via Lemma 4.1.5 to ensure that the norm of $w_{\mathcal{C},i}$ equals $N(v_{\psi_n,i})$.

monodromies and norm as $v_{\psi_n,i}$ and $w_{\mathcal{C},i} = \mathcal{C}^{-1}w_{\psi_n,i}$. Recall from Section 10.2 that the first coordinate of $w_{\mathcal{C},i}$ is exactly $M_{B,i}$. Furthermore, the first coordinate of $w_{\psi_n,i} = \mathcal{C}w_{\mathcal{C},i}$ is 0 whenever the second coordinate in $w_{\mathcal{C},i}$ is $-M_{B,i}$. In the other cases, the first coordinate of $w_{\psi_n,i}$ is b_i as specified in Equation (10.3.1):

- In the second row of Table 10.2, i.e. when $M_{B,i} = (\beta,\beta')$ is invertible, $N(v_{\psi_n,i}) = S\cdot M_{B,i}\cdot\overline{M_{B,i}}$, and $M_{G,i} = B_i/(\ell)\times 0$, we have $w_{\mathcal{C},i} = \begin{pmatrix} M_{B,i} & (-\beta,0) & 0 & \cdots & 0 \end{pmatrix}^T$, so the first coordinate of $w_{\psi_n,i}$ is $(0,\beta')$.

- In the fifth row of Table 10.3, i.e. when $M_{B,i} = (\beta,0)$, $N(v_{n,i}) = 0$, and $M_{G,i} = 0\times B_i'/(\ell)$, we have $w_{\psi_n,\mathcal{C}} = \begin{pmatrix} M_{B,i} & 0 & (0,1) & 0 & \cdots & 0 \end{pmatrix}^T$, so the first coordinate of $w_{\psi_n,i}$ is $(\beta,0)$.

We describe why the choices of $w_{\mathcal{C},i}$ (can be made to) have norm $N(v_{\psi_n,i})$. Note that

$M_{B,i}$	$N(v_{\psi_n,i})$	$M_{G,i}$	$w_{\mathcal{C},i}$	$w_{\psi_n,i}$
$(\beta,0)$	$\neq 0$	D_i	$\begin{pmatrix} M_{B,i} \\ -M_{B,i} \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1-\zeta_d^{-1})M_{B,i} \\ M_{B,i}+\alpha\zeta_d^{-2} \\ M_{B,i}-\alpha\zeta_d^{-3} \end{pmatrix}$
$(\beta,0)$	$\neq 0$	$B_i/(\ell)\times 0$ or $0\times B_i'/(\ell)$	N/A	N/A
$(\beta,0)$	0	D_i	$\begin{pmatrix} M_{B,i} \\ -M_{B,i} \\ 0 \\ 1 \\ 0 \\ \alpha \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1+\zeta_d^{-1})M_{B,i} \\ M_{B,i}+\zeta_d^{-2} \\ M_{B,i}-\zeta_d^{-3} \\ M_{B,i}+\alpha\zeta_d^{-4} \\ M_{B,i}-\alpha\zeta_d^{-5} \end{pmatrix}$
$(\beta,0)$	0	$B_i/(\ell)\times 0$	$\begin{pmatrix} M_{B,i} \\ -M_{B,i} \end{pmatrix}$	$\begin{pmatrix} 0 \\ (1-\zeta_d^{-1})M_{B,i} \end{pmatrix}$
$(\beta,0)$	0	$0\times B_i'/(\ell)$	$\begin{pmatrix} M_{B,i} \\ 0 \\ (0,1) \end{pmatrix}$	$\begin{pmatrix} (\beta,0) \\ (\beta,0)+(0,1)\zeta_d^{-1} \\ (\beta,0)-(0,1)\zeta_d^{-2} \end{pmatrix}$

Table 10.3: Descriptions of the first several coordinates of $w_{\mathcal{C},i}$ such that the first coordinate of $w_{\psi_n,i}$ is b_i when $D_i = B_i \times B_i'$ is a double division ring and $M_{B,i}$ is neither invertible nor 0; without loss of generality, say that $M_{B,i}$ is of the form $(b,0) \in B_i/(\ell) \times B_i'/(\ell)$. The unwritten trailing coordinates of $w_{\mathcal{C},i}$ are all 0. Since $w_{\psi_n,i} = \mathcal{C}w_{\mathcal{C},i}$, the unwritten trailing coordinates of $w_{\psi_n,i}$ must be all $M_{B,i}$. Where appropriate, $\alpha \in D_i$ is chosen via Lemma 4.1.5 to ensure that the norm of $w_{\mathcal{C},i}$ equals $N(v_{\psi_n,i})$.

the norm of $w_{\mathcal{C},i}$ is $w_{\mathcal{C},i}^* \cdot (\mathcal{C}^* H_{n,-1,1}\mathcal{C}) w_{\mathcal{C},i} = w_{\mathcal{C},i}^* \left(\begin{array}{c|c} S & 0 \\ \hline 0 & H_n^r \end{array}\right) w_{\mathcal{C},i}$. It is also convenient to recall that a vector over $B_i/(\ell) \times B_i'/(\ell)$ with zero $B_i/(\ell)$ or $B_i'/(\ell)$-component has zero norm by Lemma 4.3.6. Moreover, note the use of the symbols α in the choices of $w_{\mathcal{C},i}$ in multiple cases listed in the tables — in each of these cases, α is meant to be an element of D_i such that the norm of $w_{\mathcal{C},i}$ is $N(v_{\psi_n,i})$. If $D_i = \mathbb{Z}_\ell[X]/(X+1)$, then $H_n^r = 0$, so the norm is $S \cdot M_{B,i} \cdot \overline{M_{B,i}}$. In this case, the norm is determined by $M_{B,i}$, which is the first coordinate of $w_{\mathcal{C},i}$; choose $\alpha = 0$ for instance. Otherwise, α chosen either to be 0 or to be an invertible element of D_i via Lemma 4.1.5. For example, $w_{\mathcal{C},i}$ is set to be of the form $w_{\mathcal{C},i} = \begin{pmatrix} M_{B,i} & -M_{B,i} & 0 & \alpha & 0 & 0 & \cdots & 0 \end{pmatrix}^T$ in the first row of each table. The norm

of such a $w_{\mathcal{C},i}$ is

$$w^*_{\mathcal{C},i}\left(\begin{array}{c|c} S & 0 \\ \hline 0 & H^r_n \end{array}\right) w_{\mathcal{C},i} = S \cdot M_{B,i} \cdot \overline{M_{B,i}} + (-M_{B,i}) \cdot (-\overline{M_{B,i}}) \cdot \frac{(\zeta_d+1)^2}{\zeta_d} + \alpha \cdot \overline{\alpha} \cdot \frac{(\zeta_d+1)^2}{\zeta_d}.$$

Since norms in this context are elements of D_i^- and hence are either 0 or invertible, and since (ζ_d+1) is invertible by Lemma 10.2.2, an $\alpha \in D_i$ making the above expression equal to $N(v_{n,i})$ exists.

The tables contain some rows that correspond to impossible combinations of $M_{B,i}$, $N(v_{\psi_n,i})$, and $M_{G,i}$. We remark on why these combinations are impossible. The combination specified by the third row of Table 10.2 cannot occur because if $M_{G,i}$ is $B_i/(\ell) \times 0$ (or $0 \times B_i'/(\ell)$), then the norm of $w_{\mathcal{C},i}$ must be $S \cdot M_B \cdot \overline{M_B} + 0 = S \cdot M_B \cdot \overline{M_B}$. Similarly, combinations specified by the fifth row of Table 10.2 and by the second row of Table 10.3 cannot similarly cannot occur because the norm of $w_{\mathcal{C},i}$ must be 0 in these cases.

Recall from Lemma 10.2.4 that the global monodromy of w_{ψ_n} is determined exactly by $M_{G,1}(w_{\psi_n})$ and $(\sum_{i=1}^n \zeta_d^i)^{-1} M_B(w_{\psi_n}) = (M_{B,i})_i$. The former is the $D_i/(\ell)$-module generated by the coordinates of $w_{\mathcal{C},i}$ except for the first one. In each case as listed in the tables, this D_i-module is equal to $M_{G,i}$.

Finally, we describe why $w^{\mathrm{trun}}_{\psi_n}$ has the same global monodromy as w_{ψ_n}. By Corollary 10.1.9, $M_{G,i}$ is the $D_i/(\ell)$-module generated by the differences between the coordinates of $w_{\psi_n,i}$. Similarly, $M_{G,1}(w^{\mathrm{trun}}_{\psi_n,i})$ is the $D_i/(\ell)$-module generated by the differences between the coordinates of $w^{\mathrm{trun}}_{\psi_n,i}$. In each case as listed in the tables, $M_{G,i}$ coincides with $M_{G,1}(w^{\mathrm{trun}}_{\psi_n,i})$. The following are justifications to this claim, divided amongst similar cases described in the tables:

- In the first rows of each table,

$$w_{\psi_n,i} = \begin{pmatrix} 0 & (1-\zeta_d^{-1})M_{B,i} & M_{B,i} + \alpha\zeta_d^{-2} & M_{B,i} - \alpha\zeta_d^{-3} & M_{B,i} & \cdots & M_{B,i} \end{pmatrix}^T.$$

  Since n is assumed to be at least 6, $w_{\psi_n,i}$ has some trailing coordinates of $M_{B,i}$.

In particular, the difference between the coordinates $(1-\zeta_d^{-1})M_{B,i}$ and $M_{B,i}$ is the invertible element $-\zeta_d^{-1}M_{B,i}$ and hence $M_{G,1}(w_{\psi_n,i}^{\text{trun}}) = D_i$.

- In the second and third row of Table 10.1, the fourth, sixth, and seventh rows of Table 10.2, and the fifth row of Table 10.3, $M_{B,i}$ equals the first coordinate of $w_{\psi_n,i}$ and since $n \geq 6$, $w_{\psi_n,i}$ has some trailing coordinates of $M_{B,i}$. In particular, truncating the first coordinate does not change the set of values of D_i that are coordinates of $w_{\psi_n,i}$ and $M_{G,1}(w_{\psi_n,i}^{\text{trun}} = M_{G,i}$.

- In the second row of Table 10.2, $w_{\psi_n,i}$ has some trailing coordinates of $M_{B,i} = (\beta, \beta')$. The difference between the coordinates $(\beta, \beta') + \zeta_d^{-1}(\beta, 0)$ and (β, β') is the element $\zeta_d^{-1}(\beta, 0)$, which generates $M_{G,i}$. Hence, $M_{G,1}(w_{\psi_n,i}^{\text{trun}} = M_{G,i}$

- In the fourth row of Table 10.3, one can argue $M_{G,1}(w_{\psi_n,i}^{\text{trun}} = M_{G,i}$ as in the previous case.

- In the third row of Table 10.3, if $\alpha = 0$, then the difference between the coordinates $M_{B,i} + \zeta_d^{-2}$ and $M_{B,i} - \zeta_d^{-3}$ is $\zeta_d^{-2} + \zeta_d^{-3}$. Since D_i is assumed to be of the form $B_i \times B_i'$ in this case, ζ_d is not a square root of -1 in B_i and in B_i'. Thus, $\zeta_d^{-2} + \zeta_d^{-3} = \zeta_d^{-3}(1 + \zeta_d)$ is invertible in D_i and hence generates $M_{G,i}$.

□

We now relate the boundary monodromies and norms of vectors obtained by adding coordinates to shorter vectors. Note that the Lemma 10.3.6 below appends coordinates to the end of a vector, but analogous statements that append coordinates to the front of a vector also hold.

Lemma 10.3.6. *Let $d \geq 2$ be an integer, and let A be a $\mathbb{Z}[t, t^{-1}]$-module. Write N_n for the norm on $A^{\oplus n}$ given by $H_{n,-1,1}$.*

1. *If* $v_n = \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T \in A^{\oplus n}$ *and* $v_{n+1} = \begin{pmatrix} a_1 & \cdots & a_n & a_{n+1} \end{pmatrix}^T \in A^{\oplus(n+1)}$,

then

$$N_{n+1}(v_{n+1}) = N_n(v_n) + M_B(v_n) \cdot t^{-n} \cdot \overline{a_{n+1}} + \overline{M_B(v_n)} \cdot t^n \cdot a_{n+1} - a_{n+1}\overline{a_{n+1}}.$$

In particular, if $w_n = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}^T$ *and* $w_n = \begin{pmatrix} b_1 & \cdots & b_n & a_{n+1} \end{pmatrix}^T$ *and if* $M_B(v_n) = M_B(w_n)$*, then* $N_n(v_n) = N_n(w_n)$ *holds if and only if* $N_{n+1}(v_{n+1}) = N_{n+1}(w_{n+1})$.

2. *Now suppose that* A *is a module over* $\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$*. If* $v_n = \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T \in A^{\oplus n}$ *and* $v_{n+d} = \begin{pmatrix} a_1 & \cdots & a_n & \alpha & \cdots & \alpha \end{pmatrix}^T \in A^{\oplus(n+d)}$*, then*

$$N_{n+d}(v_{n+d}) = N_n(v_n)$$

Proof. 1. Calculate

$$\begin{aligned}
N_{n+1}(v_{n+1}) &= v_{n+1}^* H_{n+1,-1,1} v_{n+1} \\
&= \left(\begin{array}{c|c} v_n^* & \overline{a_{n+1}} \end{array} \right) \left(\begin{array}{ccc|c} & H_{n,-1,1} & & \begin{matrix} t^{n-1} \\ \vdots \\ 1 \end{matrix} \\ \hline t^{-n+1} & \cdots & 1 & -1 \end{array} \right) \left(\begin{array}{c} v_n \\ \hline a_{n+1} \end{array} \right) \\
&= \left(\begin{array}{c|c} v_n^* & \overline{a_{n+1}} \end{array} \right) \left(\begin{array}{c} H_n v_n + \begin{pmatrix} t^{n-1} \\ \vdots \\ 1 \end{pmatrix} a_{n+1} \\ \hline a_1 t^{-n+1} + \cdots + a_n - a_{n+1} \end{array} \right) \\
&= v_n^* H_n v_n + v_n^* \begin{pmatrix} t^{n-1} \\ \vdots \\ 1 \end{pmatrix} a_{n+1} + \overline{a_{n+1}}(a_1 t^{-n+1} + \cdots + a_n - a_{n+1}) \\
&= N_n(v_n) + (\overline{a_1} t^{n-1} + \cdots \overline{a_n}) a_{n+1} + (a_1 t^{-n+1} + \cdots + a_n)\overline{a_{n+1}} + a_{n+1} \cdot \overline{a_{n+1}} \\
&= N_n(v_n) + M_B(v_n) \cdot t^{-n} \cdot \overline{a_{n+1}} + \overline{M_B(v_n)} \cdot t^n \cdot a_{n+1} - a_{n+1}\overline{a_{n+1}}.
\end{aligned}$$

2. Writing $M = \begin{pmatrix} \zeta_d^{n-1} & \cdots & \zeta_d^{n+d-2} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & \zeta_d^{d-1} \end{pmatrix}$, and noting that $M \begin{pmatrix} \alpha & \cdots & \alpha \end{pmatrix}^T = 0$, we similarly have

$$\begin{aligned} N_{n+d}(v_{n+d}) &= v_{n+d}^* H_{n+d,-1,1} v_{n+d} \\ &= \left(\begin{array}{ccc|ccc} \overline{v_1} & \cdots & \overline{v_n} & \overline{\alpha} & \cdots & \overline{\alpha} \end{array} \right) \left(\begin{array}{c|c} H_{n,-1,1} & M \\ \hline M^* & H_{d,-1,1} \end{array} \right) \left(\begin{array}{c} v_1 \\ \vdots \\ v_n \\ \hline \alpha \\ \vdots \\ \alpha \end{array} \right) \\ &= v_n^* H_{n,-1,1} v_n + \begin{pmatrix} \overline{\alpha} & \cdots & \overline{\alpha} \end{pmatrix} H_{d,-1,1} \begin{pmatrix} \alpha \\ \vdots \\ \alpha \end{pmatrix}. \\ &= N_n(v_n) + \Sigma \alpha \cdot \overline{\alpha}, \end{aligned}$$

where Σ is the sum of the entries of $H_{d,-1,1}$. The sum of the entries of $H_{d,-1,1}$ that are strictly above the diagonal is

$$\begin{aligned} \sum_{i=0}^{d-2} \sum_{j=0}^{i} \zeta_d^j &= \sum_{i=0}^{d-2} \frac{1 - \zeta_d^{i+1}}{1 - \zeta_d} \\ &= \frac{(d-1) - \sum_{i=0}^{d-2} \zeta_d^{i+1}}{1 - \zeta_d} \\ &= \frac{(d-1) - (-1)}{1 - \zeta_d} \\ &= \frac{d}{1 - \zeta_d}. \end{aligned}$$

Since $H_{d,-1,1} = H^*_{d,-1,1}$ and since the diagonal entries of $H_{d,-1,1}$ are all -1,

$$\Sigma = \frac{d}{1-\zeta_d} + \overline{\frac{d}{1-\zeta_d}} - d = 0.$$

Therefore, $N_{n+d}(v_{n+d}) = N_n(v_n)$.

□

We now demonstrate the inductive step of the aforementioned induction argument.

Theorem 10.3.7. *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, and let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$. Suppose that $n \geq \max(6, d)$ is an integer such that $\gcd(d, n(n-2)) = 1$ and the image of ψ^r_n evaluated at $\zeta_d \in A$ contains $\mathrm{SU}(A^{\oplus(n-1)})$ where $A^{\oplus(n-1)}$ is equipped with the ε_A-Hermitian form $\tilde{h}^r_n$ — for every $d \geq 3$ and all but finitely many ℓ (depending on d), this holds for $n = 2d+1$ by Corollary 5.3.3.*

For all $m \geq n$, orbits of the elements of $A^{\oplus m}$ under the action of B_m via ψ_m evaluated at ζ_d modulo ℓ are determined precisely by the global monodromy, boundary monodromy (Definition 10.1.11), and norm under h base changed to A as described in Section 5.1, where h is given by the unitary matrix $H_{m,-1,1}$.

Proof. Proposition 10.3.2 demonstrates the case $m = n$. Inductively suppose that the claim holds for every $m \in \{n, n+1, \ldots, k-1\}$ and suppose that $v = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}^T$ and $w = \begin{pmatrix} b_1 & b_2 & \cdots & b_k \end{pmatrix}^T$ are two column vectors in $A^{\oplus k}$ with the same global monodromy, boundary monodromy, and norm. We show that v and w are in the same orbit. Since the factorization $\mathbb{Z}_\ell[\zeta_d] \cong \prod_i B_i$ has at most $d-1$ factors and since $M_{G,1}(v_A) = \prod_i M_{G,1}(v_{A,i})$, there are some (at most) d coordinates $a_{j_1}, \ldots, a_{j_d}$ such that $M_{G,1}(a_{j,1}, \ldots, a_{j,d}) = M_{G,1}(v_A)$. Moreover, the actions by $\psi_k(\sigma_i)^{\pm 1}$ allow us to swap positions of any specified coordinate of v with a neighboring coordinate at the cost of possible changing the swapped coordinate. In this manner, move the coordinates $a_{j_1}, \ldots, a_{j_d}$ to be the first d coordinates to obtain a vector $v' \in A^{\oplus k}$ and similarly obtain a vector $w' \in A^{\oplus k}$ for w. Replace v and w with v' and W' respectively.

It now suffices to show that the new v and w are in the same orbit. For an integer $r \leq k$ and a vector $u \in A^{\oplus k}$, let v_r be the subvector of u of the first r-coordinates. Via Lemma 10.3.4, produce vectors $u_v, u_w \in A^{\oplus n}$ that have the same monodromies and norms as v_n and w_n, whose first coordinates are the elements of A whose $D_i/(\ell)$-components are given by Equation (10.3.1), and such that removing these first coordinates preserves the global monodromy. We show that these first coordinates are equal. Recall that v was arranged so that $M_G(v_d) = M_G(v)$. In particular, $M_G(v_d) = M_G(v_n)$ and similarly, $M_G(w_d) = M_G(w_n)$. Since $M_G(v) = M_G(w)$, we have $M_G(v_n) = M_G(w_n)$ and hence $M_{G,1}(v_{n,i}) = M_{G,1}(w_{n,i})$ for every i, so the first coordinates are indeed equal. By the base case of the induction, i.e. Proposition 10.3.2, v_n and w_n are in the same orbits (under the action of B_n via ψ_n) as vectors u_v and u_w respectively, so v and w are respectively in the same orbits as vectors v' and w' such that $v'_n = u_v$ and $w'_n = u_w$. Let v'_{trail} and w'_{trail} respectively be the vectors obtained by removing the first coordinates of v' and w'. In particular, $M_B(v'_{\text{trail}}) = M_B(w'_{\text{trail}})$. By Lemma 10.3.6, their norms (given by $H_{k-1,-1,1}$) are equal. Moreover, since removing the first coordinates of u_v and u_w preserves their global monodromy, $M_G(v'_{\text{trail}}) = M_G(w'_{\text{trail}})$. Thus, v'_{trail} and w'_{trail} are in the same orbit (under the action of B_{k-1} via ψ_{k-1}) by the inductive hypothesis and hence v' and w' are in the same orbit. □

10.4 The Ring of Connected Components of Hurwitz Schemes

Degree n-elements $r_{g_1} \cdots r_{g_n}$ of the ring R of (10.1.1) are determined exactly by the orbit of $v_g = (g_1, \ldots, g_n)$ under the braiding action. In the case of interest, by which we mean the case $A = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$, $G = A \rtimes \langle \zeta_d \rangle$, and $c = \{(a, \zeta_d) : a \in A\}$, Theorem 10.3.7 shows that this orbit is determined exactly by the global monodromy, boundary monodromy, and norm of (the A-vector corresponding under Convention 10.0.1 to) v_g.

Moreover, R has central elements

$$U_D = \sum_{g \in c} r_g^{D|g|} \tag{10.4.1}$$

for integers D. If c is non-splitting, then there is some integer D such that the kernel and cokernel of multiplication by U_D are both of finite degree [15, Lemma 3.5]. In the case of interest, any integer D fulfills this property.

Before showing this, we identify the complete set of orbits of $A^{\oplus n}$ under ψ_n. Lemma 10.4.1 establishes that there exist vectors $v_A = (a_1, \ldots, a_n)^T \in A^{\oplus n}$ of every possible combination of global monodromy, boundary monodromy, and norm, with some restrictions, for every sufficiently large n.

For each division or double division ring quotient D_i of $\mathbb{Z}_\ell[\zeta_d]_{\zeta_d \neq 1}$, let $a_{j,i}$ be the $D_i/(\ell)$-component of a_j and let $v_{A,i} = (a_{1,i}, \ldots, a_{n,i})^T$. Write $D_i = B_i \times B_i'$ if D_i is a double division ring and $D_i = B_i$ otherwise. By Corollary 10.1.9, $M_{G,1}(v_A) = \prod_i M_{G,1}(v_{A,i})$ and each factor $M_{G,1}(v_{A,i})$ is a quotient ring of $D_i/(\ell)$. More specifically, $M_{G,1}(v_{A,i}) = 0$ if and only if $a_{1,i}, \ldots, a_{n,i}$ are all equal, and $M_{G,1}(v_{A,i}) = B_i/(\ell) \times 0$ (resp. $0 \times B_i'/(\ell)$) if and only if the $B_i'/(\ell)$-components (resp. $B_i/(\ell)$-components) of $a_{1,i}, \ldots, a_{n,i}$ are all equal.

Since $M_B(v_{A,i}) = \sum_{j=1}^n a_{j,i}\zeta_d^j$, the $B_i/(\ell)$-components (resp. $B_i'/(\ell)$-components) of the $M_B(v_{A,i})$ are determined by the $B_i/(\ell)$-components (resp. $B_i'/(\ell)$-components) of the $M_B(v_{A,i})$. Moreover, $N(v_{A,i}) = v_{A,i}^* H_{n,-1,1} v_{A,i}$, so if the $D_i/(\ell)$-components of the $a_{1,i}, \ldots, a_{n,i}$ are all equal, then $N(v_{A,i})$ is determined. If instead the $B_i/(\ell)$-components or $B_i'/(\ell)$-components of the $a_{1,i}, \ldots, a_{n,i}$ are all 0, then $N(v_{A,i}) = 0$. Lemma 10.4.1 shows that these are the only restrictions for large enough n.

Lemma 10.4.1. *Let $d \geq 3$ be an integer, let $\ell \nmid d$ be a prime number, let A be an involution ring quotient of $\mathbb{Z}/\ell\mathbb{Z}[\zeta_d] = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}$, and let $G = A \rtimes \langle \zeta_d \rangle$. Write D_i, B_i, and B_i' as above. Given $M_G \leq G$, say that M_G is determined by A' and $[a_0] \in A/A'$ (in the sense of Proposition 10.1.6), and write A_i' for the $D_i/(\ell)$-component of A'. Suppose that $n \geq 4$ is an integer such that $\gcd(d, n(n-2)) = 1$. For all $m \geq n$, every $M_G \leq G$, every $M_B \in A$, and every $N \in A^-$, there exists some $v_A \in A^{\oplus m}$ such that $M_G = M_G(v_A)$, $M_B = M_B(v_A)$, and $N = N(v_A)$ if and only if the following hold:*

- *If $A_i' = 0$ then*
  - *$M_B(v_{A,i}) = M_B((a_{0,i}, a_{0,i}, \ldots, a_{0,i})^T)$, and*

  - $N(v_{A,i}) = N((a_{0,i}, a_{0,i}, \ldots, a_{0,i})^T)$.

- *If* $A'_i = B_i/(\ell) \times 0$ *(resp.* $0 \times B'_i/(\ell)$*), then*

  - *if the* $B'_i/(\ell)$*-component (resp.* $B_i/(\ell)$*-component) of* $a_{0,i}$ *is* 0*, then* $N(v_{A,i}) = 0$.

Proof. The "only if" direction follows from the discussion above. For the "if" direction, it suffices to show this in the case that $A = D_i/(\ell)$ is a division ring or double division ring. We proceed inductively, first demonstrating the case $m = n$.

Given a vector $v_{\mathcal{C}} = (a'_1, \ldots a'_n) \in A^{\oplus n}$ corresponding to a vector $v_A \in A^{\oplus n}$ under base change by $\mathcal{C}$, i.e. $v_A = \mathcal{C}v_{\mathcal{C}}$, recall as in the proof of Proposition 10.3.2 that $M_B(v_A) = \sum_{i=1}^n \zeta_d^i a'_1$ and that $N(v_A) = v_{\mathcal{C}}^* \cdot (\mathcal{C}^* H_{n,-1,1} \mathcal{C}) v_{\mathcal{C}} = v_{\mathcal{C}}^* \left(\begin{array}{c|c} S & 0 \\ \hline 0 & H_n^r \end{array}\right) v_{\mathcal{C}}$. Furthermore, $M_G(v_A)$ is determined (in the sense of Proposition 10.1.6) exactly by a'_1 and by which among the $B_i/(\ell)$-components (and $B'_i/(\ell)$-components of $(a'_2, \ldots, a'_n)^T$ are zero by Lemma 10.2.4. Given M_G, M_B, and N, set the coordinates $a'_1, \ldots, a'_n$ of $v_{\mathcal{C}}$ in the following manner so that $M_G = M_G(v_A), M_B = M_B(v_A)$, and $N = N(v_A)$:

- Let $a'_1 = \left(\sum_{i=1}^n \zeta_d^i\right)^{-1} M_B$; this ensures that $M_B(v_A) = M_B$.

- If $A' = D_i/(\ell)$, then let $(a'_2, \ldots, a'_n)^T$ be some nonzero vector (in both the $B_i/(\ell)$ and $B'_i/(\ell)$-components if applicable) such that $N = v_{\mathcal{C}}^* \left(\begin{array}{c|c} S & 0 \\ \hline 0 & H_n^r \end{array}\right) v_{\mathcal{C}}$ — there is a way to do so in which $a'_5, \ldots, a'_n$ are all 0 and (a'_2, a'_3, a'_4) is either of the form $(a'_2, 0, 0)$ or of the form $(a'_2, 0, a'_4)$, depending on whether $N - S \cdot a'_1 \overline{a'_1}$ is invertible, by applying Lemma 4.1.5 similarly as in the proof of Lemma 10.3.4.

- If $A' = B_i/(\ell) \times 0$, then let the $B'_i/(\ell)$ and $B_i/(\ell)$-components of $(a'_2, \ldots, a'_n)^T$ be 0 and any nonzero vector respectively. Make similar choices when $A' = 0 \times B'_i/(\ell)$ instead.

- If $A' = 0$, then let $(a'_2, \ldots, a'_n)^T = 0$.

For each of these choices, we have $M_G(v_A) = M_G$ and $N(v_A) = N$, so this proves the $m = n$ case.

Now suppose inductively that the $m = k-1$ case holds for some $k-1 \geq n$, and suppose that we are given M_G, M_B, and N. If $A' = D_i/(\ell)$, then let $v_{A,k-1} = (a_1, \ldots, a_{k-1})^T \in A^{\oplus(k-1)}$ be any vector such that $M_G = M_G(v_{A,k-1}), M_B = M_B(v_{A,k-1})$, and $N = N(v_{A,k-1})$. Letting $v_A = (a_1, \ldots, a_{k-1}, 0)^T$, we have that $M_G = M_G(v_A)$, $M_B = M_B(v_A)$, and $N = N(v_A)$. If $A' = 0$, then let $v_A = (a_0, \ldots, a_0)^T \in A^{\oplus k}$.

If $A' = B_i/(\ell) \times 0$, then we identify some appropriate $v_{A,k-1} = (a_1, \ldots, a_{k-1})^T \in A^{\oplus(k-1)}$ and $a_k \in A$ to construct $v_A = (a_1, \ldots, a_{k-1}, a_k)^T$. By Corollary 10.1.9, the $B_i'/(\ell)$-components of $a_1, \ldots, a_k$ must all equal that of a_0. In particular, the $B_i'/(\ell)$-components of $M_B(v_{A,k-1})$ and a_k are determined. The construction of v_A requires

$$N = N(v_A) = N(v_{A,k-1}) + M_B(v_{A,k-1}) \cdot \zeta_d^{-(k-1)} \cdot \overline{a_k} + \overline{M_B(v_{A,k-1})} \cdot \zeta_d^{k-1} \cdot a_k - a_k \overline{a_k} \quad (10.4.2)$$

by Lemma 10.3.6. Letting a_k be any element of A with the same $B_i'/(\ell)$-component as a_0, we need

$$M_B(v_{A,k-1}) = M_B - \zeta_d^k a_k. \quad (10.4.3)$$

Whether or not the $B_i'/(\ell)$-component of a_0 is 0, the inductive hypothesis produces some $v_{A,k-1} \in A^{\oplus(k-1)}$ such that (10.4.3) and (10.4.2) hold. This concludes the proof of the lemma. □

Lemma 10.4.2. *Let $d \geq 3$ be an integer. For a prime number $\ell \nmid d$, let $G = \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1} \rtimes \langle \zeta_d \rangle$, and let $c = \{(a, \zeta_d) : a \in \mathbb{Z}/\ell\mathbb{Z}[\zeta_d]_{\zeta_d \neq 1}\}$. For all but finitely many prime numbers $\ell \nmid d$, [15, Lemma 3.5] holds for $D = 1$, i.e. the kernel and cokernel of $R \xrightarrow{U_D} R, \quad r \mapsto U_D r$ are of finite degree. More specifically,* $\deg \ker U_D, \deg \operatorname{coker} U_D \leq 2d + 1$.

Proof. Note that c is a non-splitting conjugacy class by Lemma 2.0.5. Given a subgroup H of G, let $S_n(H)$ denote the set of degree n elements $r_{g_1} \cdots r_{g_n}$, with $g_i \in c \cap H$ such that $g_1, \ldots, g_n$ generate H just as in [15, Lemma 3.5]. For any $g \in c \cap H$, note that $|g| = d$. The proof of loc. cit. shows that the map $S_n(H) \to S_{n+|g|}(H), \quad s \mapsto r_g^{|g|} s$ is bijective for all $H \leq G$, all $g \in c \cap H$, and all sufficiently large n. To show that [15, Lemma 3.5] holds for $D = 1$, the proof of loc. cit. shows that it suffices to show that different choices of

$g \in c \cap H$ induce the same bijection.

Given $r_{g_1} \cdots r_{g_n} \in S_n(H)$ and $g_a, g_b \in c \cap H$, let $v_G = (g_1, \ldots, g_n)$, and let $v_{G,a}$ and $v_{G,b}$ respectively be the length $(n + \ell)$-tuples $(g_1, \ldots, g_n, g_a, \ldots, g_a)$ and $(g_1, \ldots, g_n, g_b, \ldots, g_b)$ respectively. Since $g_a, g_b \in H$ and the global monodromy of v_G is H, the global monodromies of $v_{G,a}$ and $v_{G,b}$ are also H. Furthermore, (the A-vectors corresponding under Convention 10.0.1 to) $v_{G,a}$ and $v_{G,b}$ have equal norm by Lemma 10.3.6. It is also immediate to check that $v_{G,a}$ and $v_{G,b}$ have equal boundary monodromies. Thus, for $n \geq 2d + 1$, Theorem 10.3.7 and Corollary 6.2.9 show that $v_{G,a}$ and $v_{G,b}$ have the same braiding orbit, $r_{g_a}^d$ and $r_{g_a}^d$ indeed are the same bijection. Lemma 10.4.1 also shows that there are n-tuples of elements of c of every possible combination of global monodromy, boundary monodromy, and norm (satisfying certain restrictions) whenever $n \geq 2d + 1$. Therefore, $\deg \ker U_D, \deg \operatorname{coker} U_D \leq 2d + 1$. □

Remark 10.4.3. In the case of $d = 2$, the analogous statement holds with $\deg \ker U_D$, $\deg \operatorname{coker} U_D = 4$, cf. [13, The Proof of Proposition 2.7].

Bibliography

[1] Norbert A'Campo. "Tresses, monodromie et le groupe symplectique". In: *Commentarii mathematici Helvetici* 54 (1979), pp. 318–327.

[2] Jeffrey D. Achter and Rachel Pries. "The integral monodromy of hyperelliptic and trielliptic curves". In: *Mathematische Annalen* 338.1 (2007), pp. 187–206. DOI: https://doi.org/10.1007/s00208-006-0072-0.

[3] George E. Andrews. *The theory of partitions*. Encyclopedia of Mathematics and its Applications 2. Cambridge university press, 1998.

[4] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Berlin Heidelberg, 2012. ISBN: 9783642514388.

[5] Leonard Carlitz. "The Arithmetic of Polynomials in a Galois Field". In: *Proceedings of the National Academy of Sciences of the United States of America* 17.2 (1931), pp. 120–122.

[6] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Vol. 138. Graduate Texts in Mathematics. Springer Berlin, Heidelberg, 1993.

[7] Henri Cohen and Jacques Martinet. "Étude heuristique des groupes de classes des corps de nombres." fre. In: *Journal für die reine und angewandte Mathematik* 404 (1990), pp. 39–76. URL: http://eudml.org/doc/153196.

[8] Pierre Deligne. "La conjecture de Weil : I". fr. In: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307. URL: http://www.numdam.org/item/PMIHES_1974__43__273_0/.

[9] Pierre Deligne. "Le lemme de Gabber". In: *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*. Vol. 127. Astérisque, 1985, pp. 131–150.

[10] Pierre Deligne and Michael Artin. *Théorie des Topos et Cohomologies Étale des Schémas. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4). Tome 3*. Lecture Notes in Mathematics. Heidelberg: Springer Berlin, 1973. DOI: https://doi.org/10.1007/BFb0070714.

[11] Torsten Ekedahl. "Boundary behaviour of Hurwitz schemes". In: *The Moduli Space of Curves*. Ed. by Robbert H. Dijkgraaf, Carel F. Faber, and Gerard B. M. van der Geer. Boston, MA: Birkhäuser Boston, 1995, pp. 173–198. ISBN: 978-1-4612-4264-2.

[12] Jordan S. Ellenberg. "Endomorphism Algebras of Jacobians". In: *Algebra & Number Theory* 162 (2001), pp. 243–271. DOI: 10.1006/aima.2001.1994.

[13] Jordan S. Ellenberg, Wanlin Li, and Mark Shusterman. "Nonvanishing of hyperelliptic zeta functions over finite fields". In: *Algebra & Number Theory* 14.7 (Aug. 2020), pp. 1895–1909. DOI: 10.2140/ant.2020.14.1895. URL: https://doi.org/10.2140%5C%2Fant.2020.14.1895.

[14] Jordan S. Ellenberg, TriThang Tran, and Craig Westerland. *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields*. 2023. arXiv: 1701.04541 [math.NT].

[15] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. "Homology stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields". In: *Annals of Mathematics* 183 (2016), pp. 729–786. DOI: https://doi.org/10.4007/annals.2016.183.3.1.

[16] Alexander Grothendieck and Michèle Raynaud. *Revêtements Étales et Groupe Fondamental*. Lecture Notes in Mathematics. Heidelberg: Springer Berlin, 1971. DOI: https://doi.org/10.1007/BFb0058656.

[17] Henri H. Cohen and Hendrik W. Lenstra Jr. Lenstra. "Heuristics on class groups of number fields". In: *Number Theory Noordwijkerhout 1983*. Ed. by Hendrik Jager. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 33–62. ISBN: 978-3-540-38906-4.

[18] Chris Hall. "Big symplctic or orthogonal monodromy modulo ℓ". In: *Duke Mathematical Journal* 141.1 (2008), pp. 179–203.

[19] Godfrey H. Hardy and Srinivasa Ramanujan. "Asymptotic formulæ in combinatory analysis". In: *Proceedings of the London Mathematical Society* 2.1 (1918), pp. 75–115.

[20] Lalit Jain. "Big mod ℓ monodromy for families of G covers". PhD thesis. University of Wisconsin-Madison, 2016.

[21] Christian Kassel and Vladimir Turaev. *Braid Groups*. Vol. 247. Graduate Texts in Mathematics. New York: Springer Verlag, 2008.

[22] Nicholas M. Katz and Serge Lang. "Finiteness theorems in geometric classfield theory". In: *Enseign. Math.(2)* 27.3-4 (1981), pp. 285–319.

[23] Finn F. Knudsen. "THE PROJECTIVITY OF THE MODULI SPACE OF STABLE CURVES, II: THE STACKS M g,n". In: *Mathematica Scandinavica* 52.2 (1983), pp. 161–199. ISSN: 00255521, 19031807. URL: http://www.jstor.org/stable/24491475 (visited on 08/25/2023).

[24] Max-Albert Knus. *Quadratic and Hermitian Forms over Rings*. Vol. 294. Grundlehren der mathematischen Wissenschaften. Heidelberg: Springer Berlin, 1991.

[25] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown. *A predicted distribution for Galois groups of maximal unramified extensions*. 2022. arXiv: 1907.05002 [math.NT].

[26] James S. Milne. *Lectures on Étale Cohomology*. 2013.

[27] Jürgen Neukirch. *Algebraic Number Theory*. Heidelberg: Springer Berlin, 1999.

[28] Behrang Noohi. "FUNDAMENTAL GROUPS OF ALGEBRAIC STACKS". In: *Journal of the Institute of Mathematics of Jussieu* 3.1 (2004), pp. 69–103. DOI: 10.1017/S1474748004000039.

[29] Vladimir Platonov and Andrei Rapinchuk. *Algebraic Groups and Number Theory*. Trans. by Rachel Rowen. Translated by Rachel Rowen. Elsevier Science, 1993. ISBN: 9780080874593.

[30] Bjorn Poonen. *Lectures on rational points on curves*. 2006. URL: https://math.mit.edu/~poonen/papers/curves.pdf.

[31] Bjorn Poonen. *Rational Points on Varieties*. Graduate Studies in Mathematics. American Mathematical Society, 2017. ISBN: 9781470437732. URL: https://books.google.com/books?id=bQVDDwAAQBAJ.

[32] Matthieu Romagny and Stefan Wewars. "Hurwitz Spaces". In: *Séminaries & Congrès* 13 (2006), pp. 313–341.

[33] Michael Rosen. "S-Units and S-Class Group in Algebraic Function Fields". In: *Journal of Algebra* 26 (1973), pp. 98–108.

[34] Michael Rosen. *Number Theory in Function Fields*. Vol. 210. Graduate Texts in Mathematics. New York: Springer, 2002.

[35] Nick Salter. "Linear-central filtrations and the image of the Burau representation". In: *Geometriae Dedicata* 211 (2021), pp. 145–163.

[36] Peter Scholze and Jared Weinstein. *Berkeley Lectures on p-adic Geometry*. Vol. 207. Annals of Mathematics Studies. Princeton University Press, 2020. ISBN: 9780691202150. URL: https://books.google.com/books?id=Rb7iDwAAQBAJ.

[37] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Vol. 42. Graduate Texts in Mathematics. New York: Springer, 1977.

[38] Craig C. Squier. "The Burau Representation is Unitary". In: *Proceedings of the American Mathematical Society* 90.2 (1984), pp. 199–202.

[Stacks] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018.

[39] Andrew V. Sutherland. *MIT 18.785 Fall 2017 Lecture Notes*. 2017. URL: https://math.mit.edu/classes/18.785/2017fa/lectures.html.

[40] Tamás Szamuley. *Galois Group and Fundamental Groups*. Vol. 117. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009. DOI: https://doi.org/10.1017/CBO9780511627064.

[41] Péter Tóth. "Geometric Abelian Class Field Theory". MA thesis. Universiteit Utrecht, 2011.

[42] James V. Uspensky. "Asymptotic formulae for numerical functions which occur in the theory of partitions". In: *Bulletin of the Russian Academy of Sciences* 14.6 (1920), pp. 199–218.

[43] Tyakal Nanjundiah Venkataramana. "Image of the Burau representation at d-th roots of unity". In: *Annals of Mathematics* 179.3 (2014), pp. 1041–1083. ISSN: 0003486X. URL: http://www.jstor.org/stable/24522784 (visited on 07/31/2023).

[44] Weiton Wang and Melanie Matchett Wood. "Moments and interpretations of the Cohen-Lenstra-Martinet heuristics". In: *Commentarii Mathematici Helvetici* 96 (2021), pp. 339–387.

[45] Carl Wang-Erickson. *Cyclotomic Fields*. https://sites.pitt.edu/~caw203/pdfs/cyclotomic_fields_part_iii.pdf. 2008.

[46] Melanie Matchett Wood. "An algebraic lifting invariant of Ellenberg, Venkatesh, and Westerland". In: *Res Math Sci* 8.21 (2021).

[47] Melanie Matchett Wood. "Cohen-Lenstra Heuristics and Local Conditions". In: *Research in Number Theory* 4.41 (2018).

[48] Jiu-Kang Yu. "Toward a proof of the Cohen-Lenstra conjecture in the function field case". preprint. 1997.