DISSERTATION

ARITHMETIC PROPERTIES OF CURVES AND JACOBIANS

Submitted by

Dean M. Bisogno

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2020

Doctoral Committee:

Advisor: Rachel Pries

Jeffrey Achter
Renzo Cavalieri
Daniele Tavani

ABSTRACT

ARITHMETIC PROPERTIES OF CURVES AND JACOBIANS

This thesis is about algebraic curves and their Jacobians. The first chapter concerns Abhyankar's Inertia Conjecture which is about the existence of unramified covers of the affine line in positive characteristic with prescribed ramification behavior. The second chapter demonstrates the existence of a curve C for which a particular algebraic cycle, called the Ceresa cycle, is torsion in the Jacobian variety of C. The final chapter is a study of supersingular Hurwitz curves in positive characteristic.

ACKNOWLEDGEMENTS

Thank you to all of my collaborators and the community at CSU. In particular I would like to thank Dr. Jeff Achter, Dr. Renzo Cavalieri, and Dr. Alexander Hulpke. A special thanks to Dr. Rachel Pries for her patience throughout my time at CSU and guidance through mathematics. Lastly, thank you to my family at 1117 for all of their support.

DEDICATION

For equality.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

In this thesis I study three important topics in number theory. Each project provides evidence for open conjectures in number theory and arithmetic geometry. The first chapter concerns Abhyankar's Inertia Conjecture which predicts which inertia groups occur for unramified covers of the affine line in positive characteristic. The second studies algebraic constructions of certain cohomology classes which historically have been studied geometrically. This work has applications to finding points on algebraic curve via Grothendieck's Section Conjecture. The project discussed in the final chapter finds supersingular curves of specified genera. This is data towards open conjectures concerning the existence of supersingular curves of every genera in every non-zero characteristic.

1.1 Abhyankar's Inertia Conjecture for sporadic simple groups

Chapter 2 studies Abhyankar's Inertia Conjecture in the specific case of the sporadic groups. Abhyankar's Inertia Conjecture predicts which inertia groups occur for unramified covers of the affine line in positive characteristic. The sporadic groups are a family of 26 groups in the classification of finite simple groups. We define a (G, I)-Galois cover to be a G-cover of the projective line ramified only over infinity with inertia groups isomorphic to I. The set $\mathcal{I}_p(G)$ is the set of potential inertia groups which satisfy Abhyankar's Inertia Conjecture. The main results of Section 2.3 are the following.

Theorem 1.1.1. *Fix finite quasi-p groups $H \subset G$. Suppose the Sylow p-subgroups of G have order p and fix $I \in \mathcal{I}_p(H)$. If there exists an (H, I)-Galois cover, then there exists a (G, I)-Galois cover.*

Corollary 1.1.2. *Suppose $H \subset G$ are finite quasi-p groups, the index $[G : H]$ is coprime to p, and the Sylow p-subgroups of G have order p. Also suppose every $I \in \mathcal{I}_p(G)$ is a G-conjugate* *of some $I' \in \mathcal{I}_p(H)$. If Conjecture 2.1.2 is true for H in characteristic p, then it is true for G in characteristic p.*

Corollary 1.1.2 is applied to the 14 sporadic simple groups in Table 2.3 to verify Abhyankar's Inertia Conjecture in various characteristics. The final two sections of Chapter 2 study which ramification invariants can be shown to occur of the groups studies in the previous two chapters. The contents of Chapter 2 have been submitted for publication and can be found in [1].

1.2 Non-hyperelliptic Curves with torsion Ceresa classes

Chapter 3 is joint work with Wanlin Li, Daniel Litt, and Padmavathi Srinivasan and began at the MRC (math research community) on explicit methods in positive characteristic organized by the American Mathematical Society. Two questions were posed by Jordan Ellenberg. Could a Ceresa class be computed? If so, does there exist a non-hyperelliptic curve with a trivial or finite order Ceresa class? In Chapter 3 both questions are answered affirmatively.

The methods in Chapter 3 is unique as they apply to any pro-ℓ group with torsion-free abelianization. In particular the curve C need not be proper. The outcome is two Galois cohomology classes, MD(C, b) and J(C). We call MD(C, b) the modified diagonal class. The class MD(C, b) corresponds to the Ceresa class. We call J(C) the Johnson class and it corresponds to a basepoint-free Ceresa class. Both classes encode similar information to the classes studied in [2]. Several results are proven about these Galois-theoretic cohomology classes.

Proposition 1.2.1. *When C is a hyperelliptic curve, the class $J(C)$ is 2-torsion. Moreover, if b is a rational Weierstrass point, MD(C, b) is also 2-torsion.*

Proposition 1.2.1 verifies that the purely group-theoretic constructions studied elsewhere in the chapter are able to recover this important property of the Ceresa class.

The goal of finding a non-hyperelliptic curve with torsion Ceresa class is also accomplished. The example identified is the Fricke-Macbeath curve FM. The Fricke-Macbeath curve is the unique genus 7 Hurwitz curve over $\overline{\mathbb{Q}}$. The automorphism group of the Fricke-Macbeath curve is isomorphic to the simple group $\mathrm{PSL}_2(8)$. That is, FM is the unique genus 7 curve which admits 504 automorphisms [3, pg. 541].

Proposition 1.2.2. *Let C/K be a curve over a number field with $\overline{C} \cong FM$. The class $J(C)$ is torsion.*

The curve FM is a reasonable candidate due to several factors. By [4, Proposition 3.1], there are certain group cohomological restrictions which $\mathrm{Aut}(C)$ places on $\mathrm{J}(C)$. As a heuristic, studying curves with maximal automorphism groups increases the possibility that those restrictions force $\mathrm{J}(C)$ to have finite order. Chapter 3 has been submitted for publication under the title "Group-theoretic Johnson classes and Non-Hyperelliptic Curves with Torsion Ceresa Class" with coauthors Wanlin Li, Daniel Litt, and Padmavathi Srinivasan [4].

1.3 Supersingular Hurwitz curves

Chapter 4 is the outcome of an REU (research experience for undergraduates) run by the author and Rachel Pries during the summer of 2018 on the CSU campus. The REU spanned 6 weeks in which the group of Colorado State University undergraduates attended several weeks of lectures in number theory followed by several weeks working on a research problem and learning how to generate data using Sage and Magma. The problem posed to the REU students was to determine when Hurwitz curves are supersingular. In particular the we proved the following results.

Theorem 1.3.1. *Suppose n and l are relatively prime and $m = n^2 - nl + l^2$. The Hurwitz curve $H_{n,l}$ is supersingular over $\mathbb{F}_p$ if and only if $p^i \equiv -1 \bmod m$ for some positive integer i.*

Corollary 1.3.2. *If n and l are relatively prime and $H_{n,l}$ is supersingular over $\mathbb{F}_p$, then it is maximal over $\mathbb{F}_{p^{2i}}$ where i is the same as in Theorem 1.3.1.*

In Section 4.5 a table is provided detailing every supersingular Hurwitz curve of genus less than 5 over all fields with characteristic less than 37. The contents of Chapter 4 have been published under the title "The Supersingularity of Hurwitz Curves" with coauthors Erin Dawson, Henry Frauenhoff, Michael Lynch, Amethyst Price, Seamus Somerstep, Eric Work, and Rachel Pries [5].

Chapter 2

Abhyankar's Inertia Conjecture for Some Sporadic Groups

2.1 Background

Following the work of Serre, [6], Raynaud, and Harbater proved Abhyankar's Conjecture for Galois covers of affine curves in positive characteristic. Let k be an algebraically closed field of characteristic p. Let G be a finite group and $p(G)$ be the normal subgroup of G generated by elements of p-power order.

Theorem 2.1.1 (Abhyankar's Conjecture [7–9])**.** *Let X be a smooth projective curve of genus g defined over k. Let B be a finite non-empty set of points of X having cardinality r and let $U = X \setminus B$. A finite group G is the Galois group of an unramified cover of U if and only if $G/p(G)$ has a generating set of size at most $2g + r - 1$.*

Call G quasi-p if $G = p(G)$. A simple group is quasi-p for any prime dividing its order. When X is the projective line $\mathbb{P}^1_k$ and $B = \{\infty\}$, then Theorem 2.1.1 states that a finite group G is the Galois group of an unramified cover of $\mathbb{A}^1_k$ if and only if a generating set of $G/p(G)$ has size at most 0. Thus a finite group G is the Galois group of an unramified cover of the affine line over k if and only if G is quasi-p. Following the proof of Theorem 2.1.1, Abhyankar stated Conjecture 2.1.2.

Conjecture 2.1.2 (Abhyankar's Inertia Conjecture [10, Section 16])**.** *Let G be a finite quasi-p group. Let I be a subgroup of G which is an extension of a cyclic group of order prime-to-p by a p-group J. Then I occurs as an inertia group for a G-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ if and only if the conjugates of J generate G.*

The condition on J in Conjecture 2.1.2 is necessary. Suppose G and I are as in Conjecture 2.1.2 and that I is the inertia group of some G-Galois cover of $\mathbb{P}^1_k$ branched only at ∞. Let H be the normal subgroup of G generated by the conjugates of J. Then the G/H-Galois quotient cover is tamely ramified at ∞. Grothendieck showed that the tame fundamental group of the affine line is trivial [11, Corollary XIII.2.12]. Consequently, $H = G$ which proves the "only if" direction of Conjecture 2.1.2.

Fix $k = \overline{F}_p$ and a quasi-p group G.

Definition 2.1.3. Denote the set of potential inertia groups of G-Galois covers of $\mathbb{P}^1_k$ branched only at ∞ by $\mathcal{I}_p(G)$. Explicitly $\mathcal{I}_p(G)$ is defined in the following way

$$\mathcal{I}_p(G) = \{I \subset G \mid I \text{ satisfies the hypotheses of Conjecture 2.1.2}\}.$$

Throughout this chapter we specify a G-Galois cover of $\mathbb{P}^1_k$ branched only at ∞ with particular inertia group $I \in \mathcal{I}_p(G)$ at a ramified point. Such a cover is called a (G, I)-Galois cover. We say that Conjecture 2.1.2 is true (or verified) for G in characteristic p if for every $I \in \mathcal{I}_p(G)$ there exists a (G, I)-Galois cover.

This chapter verifies Conjecture 2.1.2 for certain sporadic groups in various characteristics. In order to do so we prove Lemma 2.3.5, a technical lemma which allows us to construct a well-defined thickening problem. Work of Habater and Stevenson [12] and Pries [13] determines the existence of solutions to these thickening problems. This allows us to prove the following theorem.

Theorem 2.1.4. *Suppose $H \subset G$ are finite quasi-p groups, the index $[G : H]$ is coprime to p, a Sylow p-subgroup of G has order p, and every $I \in \mathcal{I}_p(G)$ is a G-conjugate of some $I' \in \mathcal{I}_p(H)$. If Conjecture 2.1.2 is true for H in characteristic p, then it is true for G in characteristic p.*

As an application of the previous theorem we consider sporadic groups with stipulated properties.

- Sylow p-subgroups of G are isomorphic to $\mathbb{Z}/p$.
- The normalizer $\mathrm{N}_G(S)$ is isomorphic to $\mathbb{Z}/p \rtimes \mathbb{Z}/((p-1)/2)$.
- The group G contains a subgroup isomorphic to $\mathrm{PSL}_2(p)$.

These attributes are sufficient to verify Conjecture 2.1.2.

Corollary 2.1.5. *Abhyankar's Inertia Conjecture is true for the fourteen sporadic groups and characteristics in Table 2.3.*

The ramification invariant of a cover is an invariant of the filtration of higher ramification groups in the upper numbering. The ramification invariant is necessary though not sufficient to determine the genus of the covering curve associated to a (G, I)-Galois cover. More information can be found in Section 2.2.1.

In Section 2.4, we study the ramification invariants that can occur for G-Galois covers of $\mathbb{P}^1_k$ branched only at ∞ when G contains a subgroup $H \cong \mathrm{PSL}_2(p)$. In Section 2.5 we verify a refinement of Conjecture 2.1.2 for the Mathieu group M_{11}: all but eight of the possible ramification invariants occur for M_{11}-Galois covers of $\mathbb{P}^1_k$ branched only at ∞ in characteristic 11. We leave it as an open question whether these eight occur as well.

Theorem 2.1.6. *Conjecture 2.1.2 is true for M_{11} in characteristic $p = 11$. Further, all possible ramification invariants except $6/5$, $7/5$, $9/5$, $12/5$, $14/5$, $17/5$, $19/5$, and $27/5$ are verified to occur.*

We prove similar result for additional sporadic groups in Theorem 2.4.6.

Previous work has been successful when considering simple groups which are not sporadic. In [14, Section 4.1] and [15, Theorem 2], Harbater shows that the Sylow p-subgroups of the Galois group occur as inertia groups. Abhyankar's Inertia Conjecture (Conjecture 2.1.2) is true for the following groups:

a) $\mathrm{PSL}_2(p)$ for $p \geq 5$, [16, Corollary 3.3];

b) A_p for $p \geq 5$, [16, Corollary 3.5];

c) A_{p+2} when p is odd and $p \equiv 2 \bmod 3$ [17, Theorem 1.2].

In [18], Obus shows inertia groups isomorphic to $\mathbb{Z}/p^r$ and D_{p^r} are realizable for $\mathrm{PSL}_2(l)$ in characteristic p when p^m divides $|\mathrm{PSL}_2(l)|$, $l \neq p$ is an odd prime and $1 \leq r \leq m$. Das and Kumar show that certain inertia groups occur for covers whose Galois group is a product of alternating groups [19, Corollary 4.9]. Refined observations are made in both [16] and [17] beyond just the verification of Conjecture 2.1.2. Both papers are able to determine that all but finitely many of the possible ramification invariants occur. Further reading can be found in [17, Section 4].

2.2 Preliminaries

2.2.1 Ramification groups

Let $\phi\colon X \to Y$ be a G-Galois cover of curves with ξ a point of Y and η a point in the fiber over ξ. Let $\mathcal{O}_\eta$ denote the discrete valuation ring of $\mathcal{O}_Y$ given by the valuation ν_η at η. For $i \geq -1$, the i^{th} ramification group is given by

$$G_i = \{\delta \in G : \nu_\eta(\delta(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_\eta\}. \tag{2.1}$$

The higher ramification groups form a filtration

$$\{G_i\}_{i \geq -1} : G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots. \tag{2.2}$$

The subgroup G_{-1} is the decomposition group D_η at η. It is the subgroup of G of automorphisms that fix η. The inertia group I_η at η is G_0. In general, if π is a uniformizer of $\mathcal{O}_\eta$, then G_i is the kernel of the action of G_{-1} on $\mathcal{O}_\eta/\pi^{i+1}$. The subscript η on inertia and decomposition groups is suppressed unless relevent.

The ordering of the ramification groups in (2.2) is called the lower numbering while the renumbering introduced in Definition 2.2.1 is called the upper numbering.

Definition 2.2.1 (Upper Numbering [20, Section IV.iii])**.** Consider the function

$$t = \mathrm{H}(s) = \int_0^s \frac{dx}{[G_0 : G_x]},$$

called the Herbrand function and let $\psi(t)$ be the inverse map of $H(s)$. Then for any real $s \geq -1$, let $G_s = G_{\lceil s \rceil}$ and renumber the ramification groups by $G^t = G_s$.

Definition 2.2.2 (Jumps)**.** An index t such that $G^t \neq G^{t+\epsilon}$ for any $\epsilon > 0$ is called an upper jump.

a) The largest upper jump σ is called the ramification invariant.

b) Let $j = \psi(\sigma)$. This is called the inertia jump; it is the index of the last nontrivial ramification group in the lower numbering.

Let $\phi\colon X \to \mathbb{P}^1_k$ be a (G, I)-Galois cover for some $I \in \mathcal{I}_p(G)$ and η a ramified point with inertia group I. We denote the normalizer in G of a subgroup $I \subset G$ by $\mathrm{N}_G(I)$. The inertia groups at other ramification points are all the G-conjugates of I of which there are $[G : \mathrm{N}_G(I)]$. For every G-conjugate I' of I, the number of ramified points with inertia group I' is $[\mathrm{N}_G(I) : I]$. If a particular group structure is specified for I, it is meant that the inertia groups of ϕ are subgroups of G isomorphic to I.

If p strictly divides $|I|$, then I is a semi-direct product of the form $\mathbb{Z}/p \rtimes \mathbb{Z}/m_I$ where p and m_I are coprime by the Schur-Zassenhaus Theorem [21, pg. 132]. In this case, there is exactly one inertia jump j and $p \nmid j$. The ramification invariant is then related to the inertia jump by $\sigma = j/m_I$.

The following proposition provides some restrictions on the inertia jump and possible inertia groups.

Proposition 2.2.3 ([20, Proposition IV.ii.9])**.** *Suppose ϕ is a (G, I)-Galois cover with inertia jump j. By [20, Corollary IV.ii.4], I is an extension of a cyclic group C of order m by a p-group P via a group homomorphism $\psi\colon C \hookrightarrow \mathrm{Aut}(P)$. If $\tau \in I$ with order p and $\beta \in I$ with order m, then*

$$\psi(\beta)\tau\psi(\beta^{-1}) = \psi(\beta)^j\tau.$$

2.2.2 p-Properties of Galois groups

Recall from Theorem 2.1.1 that the existence of G-Galois covers of $\mathbb{P}^1$ branched only at ∞ in characteristic $p > 0$ is detected by the quasi-p condition on G.

Definition 2.2.4 (quasi-p)**.** Denote by $p(G)$ the subgroup of G generated by all p-power elements of G. If $p(G) = G$, then call G quasi-p.

All pairs G and p which we study in this chapter are chosen such that G is simple and p divides $|G|$.

Lemma 2.2.5. *If G is simple and p divides the order of G, then G is quasi-p.*

Proof. The subgroup $p(G)$ is normal and non-trivial in G. By the hypothesis, G is simple and thus satisfies $p(G) = G$. $\square$

The following condition, p-pure, on G was introduced by Raynaud. It is a geometric condition that guarantees that the reduction of a G-Galois cover of the affine line is connected over a terminal component. More techniques are available for p-pure groups see [8] and [22] for details.

Definition 2.2.6 (p-pure [8, pg. 426])**.** Let G be a finite quasi-p group and let S be a fixed Sylow p-subgroup of G. By $G(S)$ denote the subgroup of G generated by all proper, quasi-p subgroups $H \subset G$ having a Sylow p-subgroup contained in S. If $G(S) \neq G$ then G is p-pure.

Definition 2.2.7 (p-weight [13, Definition 3.1.2])**.** Fix G and S as in Definition 2.2.6. Consider all subgroups $G' \subset G$ such that G' is quasi-p and p-pure such that $G' \cap S$ is a Sylow p-subgroup of G'. The p-weight ω_G of G is the minimal number of such subgroups G' of G which are needed to generate G. Note that a group G is p-pure if $\omega_G = 1$.

2.2.3 Sporadic groups

The Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, and M_{24} are sporadic simple groups first described by Émile Mathieu in the 1870s [23, pg. 389]. The group M_{11} has order $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ and acts strictly 4-transitively on 11 objects. By [24, pg. 18], there are two 11-conjugacy classes labeled 11a and 11b. Conjugate maximal subgroups of M_{11} are the following [24, pg. 18].

Lemma 2.2.8. *The groups M_{11} and M_{22} are quasi-*11 *and* 11*-pure.*

Table 2.1: Maximal Subgroups of M_{11}

Subgroup	M_{10}	$PSL_2(11)$	$M_9 : 2$	S_5	$Q : S_3$
Order	720	660	144	120	48

Proof. For 11-purity, see Lemma 2.2.5.

To check 11-purity, pick $G \in \{M_{11}, M_{22}\}$. Fix a Sylow 11-subgroup S of G. The only quasi-11 subgroups containing S are its normalizer $N_G(S)$ and a unique subgroup T isomorphic to $PSL_2(11)$. But $N_G(S) \subset T$; thus G is 11-pure. □

Remark. The groups M_{12}, M_{23}, and M_{24} are not 11-pure. For $G \cong M_{12}$ every Sylow 11-subgroup of G is contained in both a maximal subgroup $H \cong PSL_2(11)$ of G and a maximal $K \cong M_{11}$ of G. The groups H and K are maximal subgroups, consequently $H \not\subset K$. Hence $G(S) = G$ and M_{12} is not 11-pure. This argument works similarly for M_{23} and M_{24}. Likewise, M_{22} is not 7-pure and M_{24} is not 23-pure.

Both the Higman-Sims group HS and McLaughlin group McL are stabilizers of certain planes in the Leech Lattice. The group HS stabilizes the plane given by the 3-3-2 triangle. The group McL stabilizes the plane given by the 3-2-2 triangle. The groups HS and McL have order strictly divisible by 11, have Sylow 11-subgroups isomorphic to $\mathbb{Z}/11$ with normalizers isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$, and contain a subgroup isomorphic to $PSL_2(11)$. Both HS and McL fail to be 11-pure.

Table 2.2: References for the groups HS, McL, and Ru.

Group	Order	Reference
HS	$2^9 3^2 5^3 \cdot 7 \cdot 11$	[25]
McL	$2^7 3^6 5^3 \cdot 7 \cdot 11$	[26]
Ru	$2^{14} 3^3 5^3 \cdot 7 \cdot 13 \cdot 29$	[27]

The group Ru has Sylow 29-subgroups isomorphic to $\mathbb{Z}/29$ with normalizers isomorphic to $\mathbb{Z}/29 \rtimes \mathbb{Z}/14$, and contains a maximal subgroup isomorphic to $PSL_2(29)$. Further, this is the only maximal subgroup of Ru with order divisible by 29. Consequently Ru is 29-pure.

2.3 Resolving Abhyankar's Inertia Conjecture from Subgroups

Few techniques are known to increase the size of inertia groups. A technique we demonstrate in this section constructs thickening problems which have solutions which are known to exist by results of Harbater and Stevenson [12, Theorem 4]. In [13] it is shown that inertia groups and ramification invariants behave predictably under this operation.

2.3.1 A Galois equivariant relation on ramification points

We begin by fixing some notation. Fix a (G, I)-Galois cover $\phi : X \to \mathbb{P}^1_k$. Pick a ramified point η on X and denote the inertia group at η by I_η. The group G acts transitively on ramification points, thus for each ramification point ϵ there exists a $g \in G$ such that $g \circ \eta = \epsilon$. Let I_g denote the inertia group at the ramified point $g \circ \eta$, consequently $I_g = gI_\eta g^{-1}$.

Note that $g_1 \circ \eta = g_2 \circ \eta$ if and only if $g_2^{-1} g_1 \in I_\eta$. This is because k is algebraically closed so the decomposition group at η and I_η coincide.

We define an equivalence relation on ramification points.

Definition 2.3.1. We say $g_1 \circ \eta \sim g_2 \circ \eta$ if and only if $g_2^{-1} g_1 \in \mathrm{N}_G(I_\eta)$. In particular this identifies η with the ramification points $z \circ \eta$ for all $z \in \mathrm{N}_G(I_\eta)$.

Lemma 2.3.2. *Suppose p divides the order of G and $I_\eta \in Syl_p(G)$. The groups*

$$N_G(I_{g_1}) = N_G(I_{g_2})$$

as subgroups of G if and only if $g_1 \circ \eta \sim g_2 \circ \eta$.

Proof. First we show that $\mathrm{N}_G(I_{g_1}) = \mathrm{N}_G(I_{g_2})$ if and only if $I_1 = I_2$. Assume $\mathrm{N}_G(I_{g_1}) = \mathrm{N}_G(I_{g_2})$. By the Sylow theorems, $\mathrm{N}_G(I_{g_i})$ contains a unique Sylow p-subgroup. Both I_{g_1} and I_{g_2} are the Sylow p-subgroup of $\mathrm{N}_G(I_{g_1})$. This shows that $I_{g_1} = I_{g_2}$ as subgroups of G. Alternatively if $I_{g_1} = I_{g_2}$ as subgroups of G, then the normalizers $\mathrm{N}_G(I_{g_1})$ and $\mathrm{N}_G(I_{g_2})$ must be equal as well.

Consequently, we must show that $g_2^{-1}g_1 \in \mathrm{N}_G(I_\eta)$ if and only if $I_1 = I_2$ as subgroups of G. We proceed by computing

$$\begin{aligned} g_2^{-1}g_1 \in \mathrm{N}_G(I_\eta) &\iff I_\eta = g_2^{-1}g_1 I_\eta g_1^{-1}g_2 \\ &\iff g_2 I_\eta g_2^{-1} = g_1 I_\eta g_1^{-1} \\ &\iff I_{g_2} = I_{g_1}. \end{aligned}$$

□

Corollary 2.3.3. *The relation $\sim$ collects the ramification points of ϕ into equivalence classes of cardinality $[N_G(I_\eta) : I_\eta]$ identified by subgroups of G isomorphic to $N_G(I_\eta)$.*

Proof. This follows immediately from Lemma 2.3.2. □

Suppose $\phi\colon X \to \mathbb{P}^1_k$ is a (G, I)-Galois cover. The set of ramification points of ϕ is denoted by R_ϕ and the cardinality of R_ϕ is $[G : I]$. The number of points in R_ϕ with inertia group precisely I is $[\mathrm{N}_G(I) : I]$. The set of equivalence classes of $R_\phi/\sim$ is denoted by $\overline{R}_\phi$ and the cardinality of $\overline{R}_\phi$ is $[G : \mathrm{N}_G(I)]$.

2.3.2 Induced covers, patching, and deformations

For the remainder of this section fix a finite quasi-p group G_1 and a quasi-p subgroup G_2 with index coprime to p. Let S be a Sylow p-subgroup of G_1 and choose I_i containing S. Assume that (G_i, I_i)-Galois covers $\phi_i\colon X_i \to \mathbb{P}^1_k$ exist.

Recall the proof of [13, Corollary 2.3.1]. A similar process is implemented here. We will induce a disconnected (G_1, I_2)-Galois cover φ_2 from a (G_2, I_2)-Galois cover. The induced cover φ_2 and a connected (G_1, I_1)-Galois cover are formally patched in neighborhoods of the ramification points. This operation yields a G_1-Galois thickening problem for which there is a solution $\mathbb{V}$ [12, Theorem 4]. Deformations of the special fiber of $\mathbb{V}$ yield a smooth, connected (G_1, I_2)-Galois cover.

We extend the notation of Section 2.3.1 to serve two covers. Fix a ramified point η_i of ϕ_i. By $I_{g,i}$ we denote the inertia group at the ramified point $g \circ \eta_i$.

Definition 2.3.4. Suppose $\phi_2 \colon X_2 \to \mathbb{P}^1_k$ is a G_2-Galois cover of curves. The induced curve $\mathcal{X}_2 := \mathrm{Ind}_{G_2}^{G_1}(X)$ is defined to be the disconnected curve consisting of $[G_1 : G_2]$ copies of X_2, indexed by left cosets of G_2 in G_1. There is an induced action of G_1 on $\mathcal{X}_2$. The induced cover is denoted $\varphi := \mathrm{Ind}_{G_2}^{G_1}(\phi_2) \colon \mathcal{X}_2 \to \mathbb{P}^1_k$.

Lemma 2.3.5. *For each $i \in \{1,2\}$ let $\phi_i \colon X_i \to \mathbb{P}^1_k$ be a (G_i, I_i)-Galois cover. Suppose $G_2 \subset G_1$ and let $\varphi_2 = \mathrm{Ind}_{G_2}^{G_1}(\phi_2)$ be the induced cover. If $N_{G_1}(I_1) \cong N_{G_1}(I_2)$, then there is a set bijection $b \colon \overline{R}_{\varphi_2} \to \overline{R}_{\phi_1}$. Further, there is a labeling of ramification points such that the bijection b is G_1-equivariant.*

Proof. First we check that the cardinalities of $\overline{R}_{\varphi_2}$ and $\overline{R}_{\phi_1}$ agree:

$$\begin{aligned} |\overline{R}_{\varphi_2}| &= [G_1 : G_2]|\overline{R}_{\phi_2}| = [G_1 : G_2][G_2 : \mathrm{N}_{G_2}(I_2)] \\ &= [G_1 : \mathrm{N}_{G_1}(I_1)] = |\overline{R}_{\phi_1}|. \end{aligned}$$

The equality of the first and second lines is justified by the hypothesis $\mathrm{N}_{G_1}(I_1) \cong \mathrm{N}_{G_1}(I_2)$.

Applying Corollary 2.3.3, define b to be the bijection sending the equivalence class of $\overline{R}_{\varphi_2}$ identified by N to the corresponding class of $\overline{R}_{\phi_1}$.

We now show that that b is G_1-equivariant. Let $b(\eta) \in \overline{R}_{\phi_1}$ be a ramification point with inertia group I_η and normalizer of inertia N. For any $g \in G_1$, $g \circ \eta$ has inertia group $gI_\eta g^{-1}$. We must show that $g \circ b(\eta)$ has inertia group $gI_\eta g^{-1}$. Recall that by definition $b(\eta)$ has normalizer of inertia N. Every ramification point with normalizer N has inertia group I_η. Consequently, $g \circ b(\eta)$ has inertia group $gI_\eta g^{-1}$. $\square$

Lemma 2.3.6. *Suppose p is prime and G is a finite quasi-p group with order strictly divisible by p. Fix a quasi-p subgroup $H \subset G$, and $I \in \mathcal{I}_p(H)$ with $I \cong \mathbb{Z}/p \rtimes \mathbb{Z}/m_I$. If there exists an (H, I)-Galois cover with inertia jump j, then there exists an (H, I)-Galois cover with inertia jump $j + im_I$ and a G-Galois cover with inertia jump $\gamma(j + im_I)$ for some positive integers i and γ.*

Proof. Let S be a Sylow p-subgroup of H and G. There exists a (G, S)-Galois cover ϕ by [15, Theorem 2]. Note that ϕ can be selected such that its inertia jump is $\gamma(j + im_I)$ for some pair of positive integers i and γ where $\gcd(\gamma, m_I) = 1$; this is a consequence of [13, Theorem 3.2.4].

By assumption, there exists an (H, I)-Galois cover ψ with inertia jump j. The inertia jump of ψ is increased to $j + im_I$ which finishes the proof [13, Theorem 2.2.2]. □

The proof of Theorem 2.3.7 uses formal patching to solve a particular thickening problem. The pattern of proof follows [13, Theorem 2.3.7] which uses [12, Theorem 4] to ensure a solution exists.

Theorem 2.3.7. *Consider finite quasi-p groups $G_2 \subset G_1$. Suppose the Sylow p-subgroups of G_1 have order p, fix $I \in \mathcal{I}_p(G_2)$. If there exists a (G_2, I)-Galois cover, then there exists a (G_1, I)-Galois cover.*

Proof. Fix a Sylow p-subgroup S of G_1 contained in I. Let $\phi_1 \colon X_1 \to \mathbb{P}^1_k$ be a (G_1, S)-Galois cover which exists by [15, Theorem 2]. Let ϕ_2 be a (G_2, I)-Galois cover, and $\varphi_2 \colon \mathcal{X}_2 \to \mathbb{P}^1_k$ denote the induced cover. Finally, let W be a curve isomorphic to two $\mathbb{P}^1_k$'s intersecting transversely at ∞. Construct $\vartheta : V \to W$ by patching X_1 and $\mathcal{X}_2$ at the ramification points identified by the bijection produced in Lemma 2.3.5.

We apply [13, Theorem 2.3.7] to ϕ_1 and ϕ_2. It is necessary that $|S| = p$ as well as certain numerical conditions are verified for the jumps of ϕ_1 and ϕ_2. These numerical conditions can be satisfied by Lemma 2.3.6. See [13, Notation 2.3.2, Notation 2.3.6] for additional details.

Let $R = k[[t]]$. The result of applying [13, Theorem 2.3.7] is the following. A family of covers over an R-curve P_R is constructed. The generic fiber of this family is a (G, I)-Galois cover, thus deformations of the special fiber yield the result. □

Corollary 2.3.8. *Suppose $G_2 \subset G_1$ are finite quasi-p groups, the index $[G_1 : G_2]$ is coprime to p, and the Sylow p-subgroups of G_1 have order p. Also suppose every $I \in \mathcal{I}_p(G_1)$ is a G_1-conjugate of some $I' \in \mathcal{I}_p(G_2)$. If Conjecture 2.1.2 is true for G_2 in characteristic p, then it is true for G_1 in characteristic p.*

Proof. Pick $I \in \mathcal{I}_p(G_1)$. By assumption, every element $I \in \mathcal{I}_p(G_1)$ is represented by a G_1-conjugate element $I' \in \mathcal{I}_p(G_2)$. Because Conjecture 2.1.2 is true for G_2, there exists a (G_2, I')-Galois cover. Applying Theorem 2.3.7 constructs a (G_1, I')-Galois cover ϕ. The group G_1 acts transitively on fibers of ϕ. For this reason all G_1-conjugates of I' occur as inertia groups at some point over ∞. This enables us to conclude that I is the inertia group at some ramified point of ϕ. □

As an application, Conjecture 2.1.2 is verified for several sporadic groups due to Conjecture 2.1.2 being known for $\mathrm{PSL}_2(p)$ in characteristic $p \geq 5$ [16, Corollary 3.3].

Corollary 2.3.9. *Abhyankar's Inertia Conjecture is true for the groups and characteristics in Table 2.3.*

Table 2.3: Groups and characteristics p for which Conjecture 2.1.2 is verified by Corollary 2.3.8.

p	Groups
5,7	M_{22}
11	M_{11}, M_{12}, M_{22}, M_{23}, HS, McL
13	F_{22}, Suz
17, 19	J_3
23	M_{24}
29	Ru
31	ON, B
59, 71	M

Proof. Fix G isomorphic to a group in Table 2.3, $p \neq 5$, and set $m_I = (p-1)/2$. Abhyankar's Inertia Conjecture is known for $\mathrm{PSL}_2(p)$ by [16, Corollary 3.3]. The group G contains a subgroup isomorphic to $\mathrm{PSL}_2(p)$. The normalizers of Sylow p-subgroups in G and $\mathrm{PSL}_2(p)$ are isomorphic to $\mathbb{Z}/p \rtimes \mathbb{Z}/m_I$. Consequently, the hypothesis of Corollary 2.3.8 are satisfied.

In the case $G \cong \mathrm{M}_{22}$ and $p = 5$, the proof is similar. The fundamental difference is that we consider a subgroup isomorphic to A_7, for which Abhyankar's Inertia Conjecture is known [17, Theorem 1.2]. □

Remark. This strategy of proof does not work for M_{24} with $p = 11$ because the normalizer of a Sylow 11-subgroup of M_{24} has order 110. There is no proper subgroup $H \subset \mathrm{M}_{24}$ for which it is known that there exists an H-Galois cover with inertia order 110. Consequently, this method does not verify Conjecture 2.1.2. In the next section we verify the existence of M_{24}-Galois covers of the affine line with all but finitely many potential inertia jumps.

2.3.3 Example: The Monster group M in characteristic 71

Consider the Monster group M which is the sporadic finite simple group with maximal order. The order of M is approximately 8×10^{53}. The prime 71 strictly divides the order of M, the group M contains a subgroup H isomorphic to $\mathrm{PSL}_2(71)$, and the normalizer of a Sylow 71-subgroup is isomorphic to $\mathbb{Z}/71 \rtimes \mathbb{Z}/35$ [28, Theorem 1]. To verify Conjecture 2.1.2 for M in characteristic 71 we must show for every subgroup I of M isomorphic to one of $\{\mathbb{Z}/71, \mathbb{Z}/71 \rtimes \mathbb{Z}/5, \mathbb{Z}/71 \rtimes \mathbb{Z}/7, \mathbb{Z}/71 \rtimes \mathbb{Z}/35\}$ there exists an (M, I)-Galois cover.

Pick $I \in \mathcal{I}_{71}(M)$ and denote the unique Sylow 71-subgroup of I by S. There exists a subgroup $H \cong \mathrm{PSL}_2(71)$ containing I. By [16, Corollary 2.4], there exists an (H, I)-Galois cover ϕ. There exists an (M, S)-Galois cover ψ [15, Theorem 2]. From ϕ and ψ Theorem 2.3.7 constructs an (M, I)-Galois cover.

2.4 Occurrence of all but Finitely Many Jumps

We now put aside the question of whether there exists a (G, I)-Galois cover for every $I \in \mathcal{I}_p(G)$ and instead consider which ramification invariants occur for unramified G-Galois covers of $\mathbb{A}^1_k$. Studying which ramification invariants occur loses information concerning the centralizers of the inertia groups which occur. This is not a strict loss, as we gain information regarding which inertia jumps occur. In particular, we realize all but finitely many of the potential ramification invariants for the sporadic groups in Table 2.3, Table 2.4, and Table 2.5.

Fix a prime p, finite quasi-p group G with order strictly divisible by p, and $k = \overline{\mathbb{F}}_p$. Recall from Section 2.2.1 that if p strictly divides G, then every $I \in \mathcal{I}_p(G)$ must be of the form $I \cong \mathbb{Z}/p \rtimes \mathbb{Z}/m_I$

for some m_I such that $\gcd(p, m_I) = 1$. For such a (G, I)-Galois cover, the ramification invariant σ is related to the inertia jump j by $\sigma = \frac{j}{m_I}$.

Definition 2.4.1. With the above notation, denote the set of potential ramification invariants for a (G, I)-Galois cover by

$$\sigma_p(I) = \left\{ \frac{j}{m_I} \in \mathbb{Q} \mid j > m_I, p \nmid j, \text{and } \gcd(j, m_I) = \frac{|\text{Cent}(I)|}{p} \right\}.$$

Now let I vary through all $\mathcal{I}_p(G)$ and denote the set of all possible ramification invariants of (G, I)-Galois covers in the following way

$$\sigma_p(G) = \bigcup_{I \in \mathcal{I}_p(G)} \sigma_p(I).$$

Definition 2.4.2. We say "all but finitely many ramification invariants occur for G in characteristic p" if for all but finitely many $\sigma \in \sigma_p(G)$ there exists a (G, I)-Galois cover with ramification invariants σ for some $I \in \mathcal{I}_p(G)$.

Lemma 2.4.3. *Suppose $I \in \mathcal{I}_p(G)$. If for every $\overline{j} \in \mathbb{Z}/m_I$ satisfying $\gcd(\overline{j}, m_I) = \frac{|Cent(I)|}{p}$ there exists a (G, I)-Galois cover with ramification invariant $\frac{j}{m_I}$ for some $j \equiv \overline{j} \bmod m_I$, then all but finitely many $\sigma \in \sigma_p(I)$ occur for (G, I)-Galois covers.*

Proof. In [13, Lemma 3.2.3] it is shown that if the inertia jump j occurs for a (G, I)-Galois cover, then any $j' > j$ such that $j' \equiv j \bmod m_I$ occurs for some (G, I)-Galois cover. Consequently, if there exists a (G, I)-Galois cover with inertia jump $j \equiv \overline{j} \bmod m_I$ for each equivalence class $\overline{j} \in \mathbb{Z}/m_I$ satisfying $\gcd(\overline{j}, m_I) = \frac{|\text{Cent}(I)|}{p}$, then all but possibly a few potential inertia jumps smaller than j occur for that equivalence class. Because I has order strictly divisible by p, the jump j' corresponds to the ramification invariant $\frac{j'}{m_I} \in \sigma_p(I)$. $\square$

Proposition 2.4.4. *Suppose p is prime, G is a finite quasi-p group with order strictly divisible by p, $S \in \text{Syl}_p(G)$, and H is a subgroup of G for which there exists an $(H, N_H(S))$-Galois cover. If* *for all $I \in \mathcal{I}_p(G)$ there exists a finite group D such that $I = I' \times D$ for some $I' \in \mathcal{I}_p(H)$, then all but finitely many ramification invariants $\sigma \in \sigma_p(G)$ occur.*

Proof. Let $I = \mathrm{N}_H(S)$ and note $I \cong \mathbb{Z}/p \rtimes \mathbb{Z}/m_I$ by the Schur-Zassenhaus Theorem [21, pg. 132]. Lemma 2.3.6 and the Different Inertia case of [13, Corollary 2.3.1] show that there exists a (G, I)-Galois cover with ramification invariant $\sigma = \frac{\gamma(j+im_I)}{m_I}$ where j and γ are coprime to m_I.

Pick an element $\bar{j} \in \mathbb{Z}/m_I$ where $\gcd(\bar{j}, p) = \frac{|\mathrm{Cent}(I)|}{p}$. There exists a positive integer $d \in \mathbb{N}$ such that $d\gamma j \equiv \bar{j} \bmod m_I$ and

$$\frac{d\gamma(j + im_I)}{\gcd(m_I, d)} \equiv \bar{j} \bmod m_I.$$

Let $I' \subset I$ be the subgroup with order $\frac{pm_I}{\gcd(m_I,d)}$. Applying [16, Proposition 3.1] yields a (G, I')-Galois cover with inertia jump $j' = \frac{d\gamma(j+im_I)}{\gcd(m_I,d)}$ and ramification invariant $\sigma = \frac{j'}{m_{I'}}$. $\square$

Remark. Assume the notation of Proposition 2.4.4. If D is trivial, then all but finitely many $\sigma \in \sigma_p(G)$ occuring is equivalent to Conjecture 2.1.2 being true for G in characteristic p.

Definition 2.4.5. By m_G we will denote the smallest integer such that $m_G \cdot \sigma_p(G) \subset \mathbb{Z}$.

Theorem 2.4.6. *As a result of Proposition 2.4.4, we can verify the occurrence of all but finitely many $\sigma \in \sigma_p(G)$ for the groups and characteristics in Table 2.3 as well as the groups and characterstics in Table 2.4 and $Table$ 2.5.*

Table 2.4: Groups in characteristics 5 and 7 for which all but finitely many jumps are verified along with structure of the normalizer of $S \in \mathrm{Syl}_p(G)$, the value of m_G, and the subgroup H for which Proposition 2.4.4 is applied.

$p = 5$					$p = 7$			
G	$N_G(S)$	m_G	H		G	$N_G(S)$	m_G	H
J_1	$D_5 \times S_3$	2	$\mathrm{PSL}_2(11)$		M_{23}	$(\mathbb{Z}/7 \rtimes \mathbb{Z}/3) \times \mathbb{Z}/2$	3	$\mathrm{PSL}_2(7)$
J_3	$D_5 \times S_3$	2	$\mathrm{PSL}_2(19)$		M_{24}	$(\mathbb{Z}/7 \rtimes \mathbb{Z}/3) \times \mathrm{S}_3$	3	$\mathrm{PSL}_2(7)$
					McL	$(\mathbb{Z}/7 \rtimes \mathbb{Z}/3) \times \mathbb{Z}/2$	3	$\mathrm{PSL}_2(7)$
					Ru	$D_7 \rtimes A_4$	6	$\mathrm{PSL}_2(13)$

Table 2.5: Groups in characteristic 11 for which all but finitely many jumps are verified along with structure of the normalizer of $S \in \mathrm{Syl}_p(G)$, the value of m_G, and the subgroup H for which Proposition 2.4.4 is applied.

$p = 11$			
G	$N_G(S)$	m_G	H
Co_3	$(\mathbb{Z}/11 \rtimes \mathbb{Z}/5) \times \mathbb{Z}/2$	5	$\mathrm{PSL}_2(11)$
F_{22}	$(\mathbb{Z}/11 \rtimes \mathbb{Z}/5) \times \mathbb{Z}/2$	5	$\mathrm{PSL}_2(11)$

Proof. All groups in Table 2.3, Table 2.4 and Table 2.5 satisfy the hypotheses of Proposition 2.4.4. In the cases $H \cong \mathrm{PSL}_2(p)$ see [16, Corollary 3.3]. For all other cases see [16, Theorem 3.6]. □

2.5 A Refinement for M_{11} in characteristic 11

We realize improved lower bounds on the ramification invariants for (M_{11}, I)-Galois covers in characteristic 11. Specifically all but eight of the possible ramification invariants are shown to occur. We prove Theorem 2.5.7 in the following way. Lemma 2.5.2 describes the possible minimal ramification invariants for an unramified M_{11}-Galois cover of $\mathbb{A}^1_k$. Lemma 2.5.4 determines the genera of a quotient cover given a ramification invariant. Then to show that $\sigma = 8/5$ occurs with inertia group isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$, Proposition 2.5.5 studies a cover in characteristic 11 provided by Serre in [29]. To show that $\sigma = 2$ occurs with inertia group isomorphic to $\mathbb{Z}/11$, Proposition 2.5.6 studies the semi-stable reduction of a characteristic 0 cover to characteristic 11. Finally, the larger ramification invariants are shown to occur via results of [30].

The techniques in this section depend on the p-purity of M_{11} and existence of a proper quasi-p subgroup of sufficiently small index relative to the size of p.

2.5.1 Intermediate genus formula

Let G be a finite simple group and let $C = (C_1, C_2, C_3)$ be a triple of conjugacy classes in G rational over a field L such that

$$\{(g_1, g_2, g_3) \in C : g_i \in C_i,\, g_i \neq 1, \text{ and } g_1 g_2 g_3 = 1\} \neq \emptyset.$$

Assume $\mathrm{char}(L) \nmid |C_i|$. For such a triple, there exists a tame G-Galois cover $Y \to \mathbb{P}^1_L$ branched at three points labeled P_1, P_2, P_3 over which an inertia group is generated by some $g_i \in C_i$.

Fix a subgroup $H \subset G$ and let $X = Y/H$. Consider the H-Galois subcover $Y \to X$ and degree $[G : H]$ cover $X \to \mathbb{P}^1$. Denote the normalizer of H in G by $N_G(H)$ and the inertia group at a point above P_i by I_i.

Lemma 2.5.1. *Consider G, H, X, and Y as above. The genus g of X can be computed as follows*

$$g = -[G : H] + 1 + \frac{[G : H]}{2} \sum_{i=1}^{3} \frac{|I_i| - 1}{|I_i|} - \frac{[N_G(H) : H]}{2} \sum_{i=1}^{3} \frac{|N_G(I_i)|}{|N_H(I_i)|} \frac{|H \cap I_i| - 1}{|H \cap I_i|}. \tag{2.3}$$

Proof. Write the Riemann-Hurwitz Formulas for the covers $Y \to \mathbb{P}^1_L$ and $Y \to X$:

$$2\,\mathrm{genus}(Y) - 2 = |G|(2\,\mathrm{genus}(\mathbb{P}^1_L) - 2) + |G| \sum_{i=1}^{3} \frac{1}{|I_i|}(|I_i| - 1); \tag{2.4}$$

$$2\,\mathrm{genus}(Y) - 2 = |H|(2g - 2) + |N_G(H)| \sum_{i=1}^{3} \frac{|N_G(I_i)|}{|N_H(I_i)|} \frac{|H \cap I_i| - 1}{|H \cap I_i|}. \tag{2.5}$$

Solving this system of equations for g yields (2.3). □

2.5.2 Vanishing cycles

Let $\phi\colon Y_0 \to (X_0 = \mathbb{P}^1_K)$ be a G-Galois cover defined over a complete discrete valuation field K branched at 0, 1, and ∞. Assume the characteristic of the residue field k is $p > 0$ and p strictly divides $|G|$. To force bad reduction, assume that p divides the order of the inertia group at some ramified point. Then ϕ has a stable reduction $\phi_s\colon Y_s \to Z_s$ with the following properties [31, Theorem 2].

- The base Z_s is a tree of projective lines.
- There is a unique original component, denoted Z, which each other component of Z_s intersects.

The components of Z_s other than Z are called tails. The restriction ϕ_α of ϕ_s to a tail X_α is a cover of $\mathbb{P}^1_k$. The point on a tail X_α where it intersects the original component is called ∞_α. A tail cover X_α is called a new tail if it is only ramified at ∞_α. Let P_i be the point of Z_s to which $i = 0, 1, \infty$ specializes. A tail X_α is called a primitive tail if one of the original branch points specializes to it. If G is p-pure then the cover is connected over one tail [32, Proposition 3.1.7].

Let $\mathbb{B}$ be the index set of tails. Each $\alpha \in \mathbb{B}$ uniquely identifies a tail cover ϕ_α and σ_α denotes the ramification invariant at ∞_α. Let $\mathbb{B}_{\text{new}}$ be the index set of new tails, and $\mathbb{B}_0$ the index set of primitive tails. When all inertia groups have order divisible by p, there are no primitive tails.

For $|\mathbb{B}_0| = 3$, the vanishing cycles formula in [32, Section 3.4.4] yields the following.

$$\sum_{\alpha \in \mathbb{B}_{\text{new}}} (\sigma_\alpha - 1) = 1. \tag{2.6}$$

2.5.3 Realizing small jumps for M_{11} in characteristic 11

Recall from Section 2.2.1 that the inertia group at Q is isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/m_I$ where $\gcd(11, m) = 1$. In M_{11} the normalizer of a subgroup isomorphic to $\mathbb{Z}/11$ is of the form $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$; thus $m_I = 5$ or $m_I = 1$.

Lemma 2.5.2. *There exists an M_{11}-Galois cover $Y \to \mathbb{P}^1_k$, only branched at ∞, with ramification invariant σ is in the set $\{\frac{6}{5}, \frac{7}{5}, \frac{8}{5}, \frac{9}{5}, 2\}$.*

Proof. Recall M_{11} is quasi-11, and M_{11} is 11-pure, applying [33, Theorem 3.5] proves that a minimal cover exists such that $\sigma \in \{\frac{6}{5}, \frac{7}{5}, \frac{8}{5}, \frac{9}{5}, 2\}$. □

Note that this does not solve the inertia conjecture because it does not show that all possible inertia groups occur. The first four ramification invariants are associated to inertia groups isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$ while $\sigma = 2$ is associated to inertia groups isomorpic to $\mathbb{Z}/11$.

To apply results of [34], it is important to know the possible degrees of non-Galois covers dominated by an M_{11}-Galois cover.

Lemma 2.5.3. *Let L be an algebraically closed field of any characteristic. Let $X \to \mathbb{P}^1_L$ be a degree d non-Galois cover with M_{11}-Galois closure $Y \to \mathbb{P}^1_L$. If $11 \leq d < 22$, then $d \in \{11, 12\}$.*

Proof. The possible degrees of $X \to \mathbb{P}^1_L$ correspond to indices of subgroups $H \subset \mathrm{M}_{11}$. The only maximal subgroups with an index in the given range are isomorphic to M_{10} and $\mathrm{PSL}_2(11)$. In particular $[\mathrm{M}_{11} : \mathrm{M}_{10}] = 11$ and $[\mathrm{M}_{11} : \mathrm{PSL}_2(11)] = 12$. Any other possible degrees must arise from subgroups of M_{10} or $\mathrm{PSL}_2(11)$. The only other candidate subgroup is $\mathrm{A}_6 \trianglelefteq \mathrm{M}_{10}$ which has index 22 in G. Consequently $d \in \{11, 12\}$. $\square$

Lemma 2.5.4. *Fix an (M_{11}, I)-Galois cover $Y \to \mathbb{P}^1_k$ with ramification invariant $\sigma = \frac{j}{5}$. Let $\varphi\colon X \to \mathbb{P}^1_k$ be a degree $11 \leq d < 22$ quotient cover of Y. Let $g =$ genus(X). If $d = 11$, then $g = j - 5$ and if $d = 12$, then $g = j - 6$.*

Proof. Pick $\theta \in I$ satisfying $|\theta| = 5$. The number of orbits of θ acting on $\{p+1, \ldots, d\}$ is denoted by t. By [34, Proposition 1.3], $t = \#\varphi^{-1}(\infty) - 1$ and

$$\text{genus}(X) = \frac{2j - t - d + 1}{2}. \tag{2.7}$$

By Lemma 2.5.3, the two possible degrees for $X \to \mathbb{P}^1_k$ are 11 and 12. If $d = 11$ then $t = 0$. Otherwise, $1 \leq t \leq d - p$. Thus when $d = 12$ then $t = 1$. $\square$

Proposition 2.5.5. *There exists an $(M_{11}, \mathbb{Z}/11 \rtimes \mathbb{Z}/5)$-Galois cover with ramification invariant $\sigma = 8/5$.*

Proof. The curve $C\colon X^{11} + 2X^9 + 3X^8 - T^8$ is an unramified cover of $\mathbb{A}^1_k$ mapping $(X, T) \mapsto T$. It is wildly ramified over ∞ with Galois closure M_{11} [29, pg. 43]. Note that this curve has non-ordinary singularities. The geometric genus 3 can be computed in a computer package such as Magma or Sage. Because C is a degree 11 cover of $\mathbb{P}^1_k$, wildly ramified above ∞, Lemma 2.5.4 implies $\sigma = \frac{8}{5}$. The inertia group for a wildly ramified point over ∞ with $\sigma = \frac{8}{5}$ is isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$. $\square$

Proposition 2.5.6. *There exists an $(M_{11}, \mathbb{Z}/11)$-Galois cover with ramification invariant $\sigma = 2$.*

Proof. Let $C = (C_1, C_2, C_3)$ where each C_i is an 11-conjugacy class of M_{11} and for some i and j, $C_i \neq C_j$. Each C_i is rational over $\mathbb{Q}(\sqrt{-11})$; let $L = \mathbb{Q}(\sqrt{-11})$. Consider an M_{11}-Galois cover $Y_0 \to \mathbb{P}^1_L$ branched at three points P_1, P_2, and P_3 with an inertia group over P_i generated by some element of C_i. Also consider the degree 12 quotient cover $X_0 \to \mathbb{P}^1_L$ dominated by the $\mathrm{PSL}_2(11)$-Galois cover $Y_0 \to X_0$. Applying (2.3) with C and $d = 12$ yields $\mathrm{genus}(X_0) = 4$.

Table 2.6: Possible genera for the reduction of $X \to \mathbb{P}^1$ of degree 11.

$\lvert\mathbb{B}_{\text{new}}\rvert$	$\{\sigma_\alpha : \alpha \in \mathbb{B}_{\text{new}}\}$	$\sum_{\alpha\in\mathbb{B}_{\text{new}}} \mathrm{genus}(X_\alpha)$
1	$\{\frac{10}{5}\}$	4
2	$\{\frac{6}{5}, \frac{9}{5}\}$ or $\{\frac{7}{5}, \frac{8}{5}\}$	3
3	$\{\frac{6}{5}, \frac{6}{5}, \frac{8}{5}\}$ or $\{\frac{6}{5}, \frac{7}{5}, \frac{7}{5}\}$	2
4	$\{\frac{6}{5}, \frac{6}{5}, \frac{6}{5}, \frac{7}{5}\}$	1
5	$\{\frac{6}{5}, \frac{6}{5}, \frac{6}{5}, \frac{6}{5}, \frac{6}{5}\}$	0

The vanishing cycles formula (2.6) gives a set of possibilities for $\{\sigma_\alpha : \alpha \in \mathbb{B}_{\text{new}}\}$. For the selected ramification type, $|\mathbb{B}_0| = 3$. Because all C_i are conjugacy classes of order 11, none of the tails indexed by $\mathbb{B}_0$ are primitive. Thus the vanishing cycles formula is

$$\sum_{\alpha\in\mathbb{B}_{\text{new}}} (j_\alpha/5 - 1) = 1. \tag{2.8}$$

From [32, Proposition 3.3.5], note that $5 < j_\alpha$. For each set of possible ramification invariants use (2.7) to compute the sum of the genera of the curves X_α.

Because Y_0 dominates a genus 4 cover, its reduction must as well. This only occurs in the first row of Table 2.6 for the single new tail with ramification invariant 2. The 11-purity of M_{11} ensures that the cover is connected over the tail component. Thus $\sigma = 2$ occurs with inertia group isomorphic to $\mathbb{Z}/11$. $\square$

Theorem 2.5.7. *Abhyankar's Inertia Conjecture is true for M_{11} in characteristic $p = 11$. More generally:*

a) If $j \in \{8 + i5, 16 + i5, 24 + i, 32 + i55 \mid i \in \mathbb{Z}_{\geq 0}\}$ *and* $p \nmid j$*, then* $\sigma = j/5$ *occurs as a ramification invariant for an* M_{11}*-Galois cover of* $\mathbb{P}^1_k$ *branched at a single point and with inertia groups isomorphic to* $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$*.*

b) If $\sigma \in \{2 + i \mid i \in \mathbb{Z}_{\geq 0}\}$ *and* $p \nmid \sigma$*, then* $\sigma = 2 + i$ *occurs as a ramification invariant for an* M_{11}*-Galois cover of* $\mathbb{P}^1_k$ *branched at a single point and with inertia groups isomorphic to* $\mathbb{Z}/11$*.*

Proof. Recall that the only possible inertia groups for an M_{11}-Galois cover of $\mathbb{A}^1_k$ are isomorphic to $\mathbb{Z}/11 \rtimes \mathbb{Z}/5$ and $\mathbb{Z}/11$. By Propositions 2.5.5 and 2.5.6, each of these occurs with ramification invariants $8/5$ and 2 respectively. The other inertia jumps can be produced with applications of [13, Corollary 2.3.1 Different Inertia Case] with $r = 1$. To see that $j = 16$ occurs, apply Theorem 2.3.7 with $G_1 \cong G_2 \cong \mathrm{M}_{11}$, $I_1 \cong I_2 \cong \mathbb{Z}/11 \rtimes \mathbb{Z}/5$, and $j_1 = j_2 = 8$. Theorem 2.3.7 can be reapplied with $j_1 = 16$ yielding $j = 24$. Likewise applying Theorem 2.3.7 a final time with $j_1 = 24$ produces $j = 32$.

Finally [30, Theorem 3.2] allows j to be increased by multiples of 5. $\square$

This method is not sufficient to determine whether these jumps j occur: 6, 7, 9, 12, 14, 17, 19, and 27.

Chapter 3

Group-theoretic Johnson classes and a non-hyperelliptic curve with torsion Ceresa class

3.1 Background

Let X be a smooth, projective, geometrically integral curve over a field K of genus ≥ 3, and let $x \in X(K)$ be a rational point. One can embed X in its Jacobian $\mathrm{Jac}(X)$ via the Abel-Jacobi map $P \mapsto [P - x]$ and let X^- denote the image of X under the negation map on the group $\mathrm{Jac}(X)$. The Ceresa cycle is the homologically trivial algebraic cycle $X - X^-$ in $\mathrm{Jac}(X)$. A classical result of Ceresa [35, Theorem 3.1] shows that when X is a very general curve over $\mathbb{C}$ of genus $g \geq 3$, the Ceresa cycle is not algebraically trivial.

Via the ℓ-adic cycle class map, the Ceresa cycle gives rise to a Galois cohomology class

$$\mu(X, x) \in H^1(\mathrm{Gal}(\bar{K}/K), H^{2g-3}_{\text{ét}}(\mathrm{Jac}(X) \otimes \bar{K}, \mathbb{Z}_\ell(g-1)))$$

which only depends on the rational equivalence class of the Ceresa cycle. Hain and Matsumoto [2] reinterpret this class in terms of the Galois action on the pro-ℓ étale fundamental group of X, and describe an analogous class $\nu(X)$ which is basepoint-independent.

We define two classes $\mathrm{MD}(X, x)$ and $J(X)$ in Galois cohomology (the latter of which is basepoint-independent), called the *modified diagonal* and *Johnson* classes, which capture aspects of the action of Galois on the pro-ℓ étale fundamental group of X. Under the assumption that X is smooth and projective, these classes are closely related to $\mu(X, x)$ and $\nu(X)$. The main novelty of our construction is that it proceeds via abstract group theory. In particular, it works for any pro-ℓ group with torsion-free abelianization — for example, we do not require our curves to be proper, and many of our results hold for general Demuskin groups. Even in the case of pro-ℓ surface groups, our analysis appears to refine existing results when $\ell = 2$; for example, the classes

$\mathrm{MD}(X, x)$ and $J(X)$ appear to give slightly more information than the classes $\mu(X, x), \nu(X)$ if $\ell = 2$ (if $\ell \neq 2$, one may recover our classes from those in [2] and vice versa).

The Ceresa class is well-known to be trivial if X is hyperelliptic and x is a rational Weierstrass point; likewise, the class $\nu(X)$ of [2] is trivial for any hyperelliptic curve. In Section 3.3.3 we use properties of the Johnson class to give what is, to our knowledge, the first known example of a non-hyperelliptic curve where $J(X)$ (and hence $\nu(X)$) is torsion. This curve is of genus 7.

Moreover, in Section 3.3.4, we show with Theorem 3.3.5 that any curve dominated by a curve with torsion Johnson class has torsion Johnson class as well. This can be viewed as a generalization of the fact that any curve dominated by a hyperelliptic curve is itself hyperelliptic. Use this property, we construct a non-hyperelliptic genus 3 curve with torsion Johnson class.

Theorem 3.1.1 (Proposition 3.3.3, the Fricke-Macbeath curve, and Corollary 3.3.6)**.** *Let C be a genus 7 curve over a field K of characteristic zero, such that $C_{\overline{K}}$ has automorphism group isomorphic to $\mathrm{PSL}_2(8)$. The Johnson class of C (that is, $J(C)$ and hence the basepoint-independent Ceresa class $\nu(C)$ defined in [2]) is torsion.*

If $\iota \in Aut(C)$ is any element of order 2, then the quotient C/ι is non-hyperelliptic of genus 3 with $J(C/\iota)$ and $\nu(C/\iota)$ torsion.

3.1.1 Outline of the chapter

In Section 3.2, we give a group-theoretic construction of the so-called modified diagonal and Johnson classes associated to a finitely generated pro-ℓ group with torsion-free abelianization. In Section 3.2.3, we specialize this construction to the pro-ℓ fundamental group of a curve and compare it to the classes $\mu(X, x), \nu(X)$ of Hain-Matsumoto [2]. In Section 3.3 we study properties of this construction and apply them to give a proof of the fact that hyperelliptic curves have 2-torsion Johnson class, and we show that any model of the the Fricke-Macbeath curve has torsion Johnson/Ceresa class. We also show that any curve dominated by a curve with torsion Johnson class has torsion Johnson class itself; hence a genus 3 non-hyperelliptic curve which is a quotient of the Fricke-Macbeath curve has torsion Johnson class as well.

3.2 Group-theoretic Ceresa classes

Let ℓ be a prime and G a finitely generated pro-ℓ group with torsion-free abelianization G^{ab}. Define the ℓ-adic group ring of G as

$$\mathbb{Z}_\ell[[G]] := \varprojlim_{G \twoheadrightarrow H} \mathbb{Z}_\ell[H].$$

Here the inverse limit is taken over all finite groups H which are continuous quotients of G. Let $\mathscr{I} \subset \mathbb{Z}_\ell[[G]]$ be the augmentation ideal.

Proposition 3.2.1. *The map $\phi : G \to \mathscr{I}/\mathscr{I}^2$ given by*

$$\phi : g \mapsto g - 1$$

is a continuous group homomorphism and induces an isomorphism

$$G^{ab} \xrightarrow{\sim} \mathscr{I}/\mathscr{I}^2.$$

Proof. This is [36, Lemma 6.8.6(b)]. □

Let $Z(G)$ denote the center of G. The action of G on itself by conjugation gives a short exact sequence

$$1 \to G/Z(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1$$

of continuous maps of profinite groups.

Definition 3.2.2. The modified diagonal class, denoted by

$$\mathrm{MD}_{\mathrm{univ}} \in H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$$

is the class associated to the extension of continuous Aut(G)-modules

$$0 \to \mathscr{I}^2/\mathscr{I}^3 \to \mathscr{I}/\mathscr{I}^3 \to \mathscr{I}/\mathscr{I}^2 \to 0. \tag{3.1}$$

The existence of $\mathrm{MD}_{\mathrm{univ}}$ follows from the fact that $\mathscr{I}/\mathscr{I}^2$ is a $\mathbb{Z}_\ell$-module (as G^{ab} is torsion-free by assumption). An explicit cocycle representing $\mathrm{MD}_{\mathrm{univ}}$ will be given in Section 3.2.1.

Remark. We call this class the modified diagonal class because we expect that when G is the pro-ℓ étale fundamental of a curve, the Galois-cohomological avatar of $\mathrm{MD}_{\mathrm{univ}}$ (Section 3.2.3) may be written rationally as a multiple of the image of the Gross-Kudla-Schoen [37,38] modified diagonal cycle under an étale Abel-Jacobi map. See e.g. [39] for a Hodge-theoretic analogue of this fact.

We now proceed to find an avatar of $\mathrm{MD}_{\mathrm{univ}}$ in the cohomology of the outer automorphism group of G, Out(G). Geometrically this will correspond to removing the basepoint-dependence of the class $\mathrm{MD}_{\mathrm{univ}}$ in the case G is the pro-ℓ étale fundamental group of a curve.

3.2.1 Descending to Out(G), and the Johnson class

We first analyze the pullback of $\mathrm{MD}_{\mathrm{univ}}$ along the canonical map $G \to$ Aut(G). We will use this analysis to construct a quotient $A(G)$ of $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$ such that $\mathrm{MD}_{\mathrm{univ}}|_G$ vanishes in $H^1(G, A(G))$; hence $\mathrm{MD}_{\mathrm{univ}}$ will induce a class in $H^1(\text{Out}(G), A(G))$, which we will term the Johnson class. The constructions here are closely related to work of Andreadakis, Bachmuth, and others (see e.g. [40–42]), but we include the details here as those papers deal with the discrete, rather than profinite, situation.

Note that $\mathscr{I}/\mathscr{I}^2$ is a free $\mathbb{Z}_\ell$-module by Proposition 3.2.1 and our assumption that G^{ab} is torsion-free. Tensoring the short exact sequence (3.1) by $(\mathscr{I}/\mathscr{I}^2)^\vee$ yields

$$0 \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}/\mathscr{I}^3) \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}/\mathscr{I}^2) \to 0.$$

The last term admits a natural map $\mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}/\mathscr{I}^2)$ (sending 1 to the identity map), and pulling back along this inclusion gives a G-module extension

$$0 \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \to X \to \mathbb{Z}_\ell \to 0, \tag{3.2}$$

where G acts trivially on $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$ and $\mathbb{Z}_\ell$ but non-trivially on X. The extension is characterized by a group homomorphism:

$$\begin{aligned} &G \to \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) \simeq \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \\ &g \mapsto (v \mapsto g(\tilde{v}) - \tilde{v}) \end{aligned}$$

where $\tilde{v}$ is any lift of $v \in \mathbb{Z}_\ell$ to X.

This map factors through $G^{ab} \cong \mathscr{I}/\mathscr{I}^2$ as $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$ is abelian.

Definition 3.2.3. For the rest of the chapter, let

$$m\colon G^{ab} \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$$

be the map coming from the extension class of (3.2) described in the paragraphs above.

We now give a more explicit description of the map m.

Lemma 3.2.4. *Consider the commutator map*

$$\begin{aligned} (\mathscr{I}/\mathscr{I}^2)^{\otimes 2} &\to \mathscr{I}^2/\mathscr{I}^3 \\ x \otimes y &\mapsto xy - yx. \end{aligned}$$

Then the map m in Definition 3.2.3 is the same as the map induced by adjunction:

$$m : \mathscr{I}/\mathscr{I}^2 \to \mathit{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) : x \mapsto (y \mapsto xy - yx)$$

under the identification between G^{ab} and $\mathscr{I}/\mathscr{I}^2$ from Proposition 3.2.1.

Proof. Let X be as in (3.2). Let $s \in X \subset \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}/\mathscr{I}^3)$ be an element reducing to the identity modulo $\mathscr{I}^2$. Then we define maps

$$m_1, m_2 \colon G \to \mathscr{I}/\mathscr{I}^2 \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$$

by

$$m_1(g) = (y \mapsto gs(y)g^{-1} - s(y)),$$

$$m_2(g) = (y \mapsto (g-1)s(y) - s(y)(g-1) = gs(y) - s(y)g).$$

The map m_1 is by definition the same as the map in Definition 3.2.3. The map m_2 is an explicit formula for the map in the statement of the lemma. Neither map depends on the choice of s. We wish to show they are the same.

For any $g \in G$, we have

$$g^{-1} = \frac{1}{1+(g-1)} = 1 - (g-1) + (g-1)^2 \bmod \mathscr{I}^3.$$

Hence for $g \in G, y \in \mathscr{I}/\mathscr{I}^2$ and $s(y) \in \mathscr{I}/\mathscr{I}^3$ being a lift of y, we have modulo $\mathscr{I}^3$:

$$\begin{aligned}
((m_1 - m_2)(g))(y) &\equiv gs(y)g^{-1} - s(y) - gs(y) + s(y)g \\
&\equiv gs(y)(g^{-1} - 1) - s(y)(1-g) \\
&\equiv gs(y)((1-g) + (g-1)^2) - s(y)(1-g) \\
&\equiv (g-1)s(y)(1-g) + gs(y)(g-1)^2 \\
&\equiv 0,
\end{aligned}$$

as $g - 1 \in \mathscr{I}$ and $s(y) \in \mathscr{I}/\mathscr{I}^3$ above. This shows that $m_1 = m_2$ as desired. $\square$

Definition 3.2.5. Let $A(G) := \operatorname{coker}(m : \mathscr{I}/\mathscr{I}^2 \to \operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$ be the cokernel of the commutator map defined above.

Using the quotient map $\operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \to A(G)$ and inclusion $G/Z(G) \to \text{Aut}(G)$, we get a map

$$H^1(\text{Aut}(G), \text{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) \to H^1(\text{Aut}(G), A(G)) \to H^1(G/Z(G), A(G)).$$

Proposition 3.2.6. *The image of* $\mathrm{MD}_{\mathrm{univ}}$ *under the composition above is zero.*

Proof. As G acts trivially by conjugation on $\mathscr{I}/\mathscr{I}^2$, $\mathscr{I}^2/\mathscr{I}^3$, and $\operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$. This means $H^1(G, \operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) = \operatorname{Hom}(G, \operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$. By Lemma 3.2.4, the pullback of class $\mathrm{MD}_{\mathrm{univ}}$ in $H^1(G, \operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$ maps to the homomorphism m under this identification. But by the definition of $A(G)$, its restriction to $G/Z(G)$, and hence to G, is trivial. $\square$

We now define the universal Johnson class.

Proposition 3.2.7. *There exists a unique element* J_{univ} *in* $H^1(\operatorname{Out}(G), A(G))$ *whose image in* $H^1(\operatorname{Aut}(G), A(G))$ *under the inflation map*

$$H^1(\operatorname{Out}(G), A(G)) \to H^1(\operatorname{Aut}(G), A(G))$$

is the same as the image of $\mathrm{MD}_{\mathrm{univ}}$ *under the map*

$$H^1(\mathit{Aut}(G), \operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) \to H^1(\operatorname{Aut}(G), A(G))$$

induced by the quotient map $\operatorname{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \to A(G)$.

Proof. The definition of $A(G)$ implies that the $G/Z(G)$-action on $A(G)$ is trivial. This means we have the following the inflation-restriction exact sequence in continuous group cohomology:

$$0 \to H^1(\text{Out}(G), A(G)) \to H^1(\text{Aut}(G), A(G)) \to H^1(G/Z(G), A(G))^{\text{Out}(G)}.$$

By Proposition 3.2.6, the image of $\mathrm{MD}_{\mathrm{univ}}$ in $H^1(G/Z(G), A(G))^{\mathrm{Out}(G)}$ is zero, and thus there exists a unique element J_{univ} in $H^1(\mathrm{Out}(G), A(G))$ whose image in $H^1(\mathrm{Aut}(G), A(G))$ is the same as the image of $\mathrm{MD}_{\mathrm{univ}}$. $\square$

Definition 3.2.8. We call the element $J_{\mathrm{univ}} \in H^1(\mathrm{Out}(G), A(G))$ constructed in Proposition 3.2.7 the universal Johnson class.

Remark. We call this class the Johnson class because in the case where G is a discrete surface group, our construction is closely related to the Johnson homomorphism studied in [43] and the cocycle constructed by Morita in [44].

3.2.2 The coefficient groups for the Modified Diagonal and Johnson classes

The goal of this section is to identify a natural $\mathrm{Aut}(G)$-submodule W of the group $\mathscr{I}^2/\mathscr{I}^3$ such that $\mathrm{MD}_{\mathrm{univ}}$ lives in the image of the natural map

$$H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, W)) \to H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)),$$

for $\ell \neq 2$. Similarly, we will find a natural submodule $A_W(G) \subset A(G)$ so that J_{univ} is in the image of the natural map

$$H^1(\mathrm{Out}(G), A_W(G)) \to H^1(\mathrm{Out}(G), A(G)).$$

For $\ell = 2$, we will prove similar results for $2^i \, \mathrm{MD}_{\mathrm{univ}}$ and $2^i J_{\mathrm{univ}}$, where $i = 1, 2$ depending on the group-theoretic properties of G.

Preliminaries on free pro-ℓ groups

Lemma 3.2.9. *Let G be a free pro-ℓ group, freely generated by $g_1, g_2, \ldots, g_r$, and let $\mathscr{I}$ be the augmentation ideal of the completed group ring $\mathbb{Z}_\ell[[G]]$.*

1. *For each of the generators g_i, let $x_i := g_i - 1 \in \mathbb{Z}_\ell[[G]]$. Then $\mathscr{I}/\mathscr{I}^2$ is a free $\mathbb{Z}_\ell$-module of rank r generated by the images of $x_1, x_2, \ldots, x_r$ and $\mathscr{I}^2/\mathscr{I}^3$ is free of rank r^2 with basis the images of $x_i x_j$.*

II. Let H be another finitely generated free pro-ℓ group, and let $f^{ab}\colon G^{ab} \to H^{\mathrm{ab}}$ be an isomorphism. Let $h_1, h_2, \ldots, h_r$ be any set of lifts of $f^{ab}(g_1), \ldots, f^{ab}(g_r)$ from H^{ab} to H. Then $f(g_i) = h_i$ defines an isomorphism $f\colon G \to H$.

III. Let $\tilde{G}$ be a finitely generated pro-ℓ group with torsion-free abelianization. Let $\pi\colon G \to \tilde{G}$ be a surjection such that the induced map $\pi^{ab}\colon G^{ab} \to \tilde{G}^{ab}$ is an isomorphism. Then any automorphism $\sigma_{\tilde{G}}\colon \tilde{G} \to \tilde{G}$ lifts to an automorphism $\sigma_G\colon G \to G$.

Proof.

I. Since G is free and $\mathbb{Z}_\ell[[G]]$ is complete with respect to the augmentation ideal, there is by [45, Proposition 7, pg. I-7] an isomorphism

$$\mathbb{Z}_\ell[[G]] \xrightarrow{\sim} \mathbb{Z}_\ell\langle\langle x_1, x_2, \ldots, x_r\rangle\rangle_{\mathrm{nc}}, \tag{3.3}$$

where $\mathbb{Z}_\ell\langle\langle x_1, x_2, \ldots, x_r\rangle\rangle_{\mathrm{nc}}$ is the non-commutative power series ring in r variables, such that g_i is sent to $x_i + 1$. The claim follows.

II. Since $h_1, h_2, \ldots, h_r$ are elements of H whose images topologically generate H^{ab}, by [46, Proposition 3.9.1] it follows that $h_1, h_2, \ldots, h_r$ also generate H. This shows that f is a surjection. We will now show that these elements in fact freely topologically generate H, which proves that f is an isomorphism.

Note that f^{ab} also induces an isomorphism

$$f^{\mathrm{ab}}\colon G^{\mathrm{ab}}/(G^{\mathrm{ab}})^\ell \to H^{\mathrm{ab}}/(H^{\mathrm{ab}})^\ell.$$

Combining this with [46, Proposition 3.9.1] applied to G and H, we get that the cardinalities of the minimal generating sets for these two groups are equal, since they are equal to $\dim_{\mathbb{F}_\ell} G^{\mathrm{ab}}/(G^{\mathrm{ab}})^\ell = \dim_{\mathbb{F}_\ell} H^{\mathrm{ab}}/(H^{\mathrm{ab}})^\ell$. Since $g_1, g_2, \ldots, g_r$ is a minimal generating set for G, it follows that $h_1, h_2, \ldots, h_r$ is a minimal generating set for H. By [46, Proposition 3.9.4], there are thus no relations between the h_i; hence f is injective as desired.

III. Choose any homomorphism $f : G \to G$ lifting $\sigma_{\tilde{G}}$. That it is an isomorphism follows from the previous part applied with $G = H$ and $f^{\mathrm{ab}} = (\pi^{\mathrm{ab}})^{-1} \circ \sigma_{\tilde{G}}^{\mathrm{ab}} \circ \pi^{\mathrm{ab}}$. □

Definition 3.2.10 (Alternating tensors)**.** Let G be a finitely generated pro-ℓ group with torsion-free abelianization, and let $V := \mathscr{I}/\mathscr{I}^2$. Let

$$\iota\colon V \otimes V \to V \otimes V$$

be the natural involution of the $\mathrm{Aut}(G)$-module $V \otimes V$ that acts on a simple tensor $v_1 \otimes v_2$ as $\iota(v_1 \otimes v_2) := v_2 \otimes v_1$. Let Alt^2 $V \subset V \otimes V$ be the $\mathrm{Aut}(G)$-submodule of alternating tensors, i.e., the maximal submodule where ι acts as multiplication by -1.

Let $W \subset \mathscr{I}^2/\mathscr{I}^3$ be the image of Alt^2 V under the natural surjective multiplication map $V \otimes V \to \mathscr{I}^2/\mathscr{I}^3$, and let $A_W(G) := \mathrm{coker}(m : \mathscr{I}/\mathscr{I}^2 \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, W))$ be the cokernel of the commutator map.

Proposition 3.2.11. *Let $W \subset \mathscr{I}^2/\mathscr{I}^3$ be as in Definition 3.2.10. Suppose that there exists an element $\sigma \in$ Aut(G) which acts on G^{ab} as multiplication by -1. Then the class $4\,\mathrm{MD}_{\mathrm{univ}}$ lies in the image of the natural map*

$$H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, W)) \to H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)).$$

If

$$H^0(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \otimes \mathbb{Z}_\ell/2) = 0,$$

then $2\,\mathrm{MD}_{\mathrm{univ}}$ has a unique preimage under this map.

We will prove this proposition at the end of this section. Note that if $\ell \neq 2$, the proposition implies that $\mathrm{MD}_{\mathrm{univ}}$ itself is in the image of the map in question with a unique preimage.

Note that by Lemma 3.2.4, since $x \otimes y - y \otimes x$ is skew-symmetric, the image of the map

$$m\colon \mathscr{I}/\mathscr{I}^2 \to \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$$
$$x \mapsto (y \mapsto xy - yx)$$

in Definition 3.2.3, is contained in $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, W)$. The next proposition follows immediately from this observation and Proposition 3.2.11.

Proposition 3.2.12. *Let $A_W(G)$ be the cokernel of the commutator map defined in Definition 3.2.10. Suppose that there exists an element $\sigma \in Aut(G)$ which acts on G^{ab} as multiplication by -1. Then the class $4J_{\mathrm{univ}}$ lies in the image of the natural map*

$$H^1(\mathrm{Out}(G), A_W(G)) \to H^1(\mathrm{Out}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, A(G))).$$

If $H^0(Out(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \otimes \mathbb{Z}_\ell/2) = 0$, then the class $2J_{\mathrm{univ}}$ has a unique preimage under this map.

Before proving Proposition 3.2.11, we first prove a lemma.

Lemma 3.2.13. *Let G be a finitely generated pro-ℓ group with torsion-free abelianization, let $V := \mathscr{I}/\mathscr{I}^2$, and let $W \subset \mathscr{I}^2/\mathscr{I}^3$ be as in Definition 3.2.10. Let S be the image of the natural map $\mathrm{Aut}(G) \to \mathrm{Aut}(V)$ and let $T := \ker(\mathrm{Aut}(G) \to S)$. Then*

I. Assume that $-id_V$ is in S. Then the group $H^i(S, \mathrm{Hom}(V, U))$ is 2-torsion for any $\mathrm{Aut}(G)$-submodule U of $V \otimes V$ and any $i \in \mathbb{Z}_{\geq 0}$.

II. Assume that $-id_V$ is in S. Then we have

$$H^1(S, \mathrm{Hom}(V, U)) \simeq H^0(S, \mathrm{Hom}(V, U) \otimes \mathbb{Z}_\ell/2)$$

for any $\mathrm{Aut}(G)$-submodule U of $V \otimes V$.

III. The image of the class $\mathrm{MD}_{\mathrm{univ}}$ *under the restriction map*

$$H^1(\mathrm{Aut}(G), \mathrm{Hom}(V, \mathscr{I}^2/\mathscr{I}^3)) \to H^1(T, \mathrm{Hom}(V, \mathscr{I}^2/\mathscr{I}^3))$$

lies in the image of the natural map

$$H^1(T, \mathrm{Hom}(V, W)) \to H^1(T, \mathrm{Hom}(V, \mathscr{I}^2/\mathscr{I}^3)).$$

Remark.

- The assumption in Lemma 3.2.13(I.) is satisfied by finitely generated free pro-ℓ groups and pro-ℓ surface groups (i.e. the pro-ℓ completion of the fundamental group of a genus g Riemann surface). Indeed, Lemma 3.2.9 (2) implies that $S = \mathrm{Aut}(V)$ in the first case and [47, Proposition 1] shows that $S \cong \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ in the second case.

- By the above remark and direct computation, the hypothesis that

$$H^0(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3) \otimes \mathbb{Z}_\ell/2) = 0$$

  in Propositions 3.2.11 and 3.2.12 are satisfied for finitely-generated free pro-ℓ groups and for pro-ℓ surface groups.

- Note that the statement of Lemma 3.2.13(III.) is a pro-ℓ version of Johnson's theorem [43] on the mapping class group of a Riemann surface with a marked point.

Proof of Lemma 3.2.13.

I. The proof is the same as [2, Lemma 5.4].

II. This is again similar to [2, Lemma 5.4]; it is immediate from the Bockstein sequence associated to the short exact sequence

$$0 \to \mathrm{Hom}(V, U) \xrightarrow{\cdot 2} \mathrm{Hom}(V, U) \to \mathrm{Hom}(V, U) \otimes \mathbb{Z}_\ell/2 \to 0.$$

III. We first prove the result in the case that G is a finitely-generated free pro-ℓ group. Then we will reduce to this case.

The case that G is a finitely-generated free pro-ℓ group, generated by $g_1, \cdots, g_r$.

Let

$$\Delta\colon \mathbb{Z}_\ell[[G]] \to \mathbb{Z}_\ell[[G]] \otimes \mathbb{Z}_\ell[[G]]$$

denote the comultiplication map of the group ring $\mathbb{Z}_\ell[[G]]$, i.e. the map defined by

$$\Delta : g \mapsto g \otimes g$$

for $g \in G$, and extended linearly. By Lemma 3.2.9(1), the set

$$\{x_1, \ldots, x_r, x_1^2, x_1x_2, \ldots, x_rx_{r-1}, x_r^2\}$$

is a $\mathbb{Z}_\ell$-basis for $\mathscr{I}/\mathscr{I}^3$. As any $\sigma \in T$ preserves $\mathscr{I}$ and fixes $\mathscr{I}/\mathscr{I}^2$, there exist unique elements $b_i^{kl}(\sigma) \in \mathbb{Z}_\ell$ such that

$$\sigma(x_i) = x_i + \sum_{kl} b_i^{kl}(\sigma)x_kx_l \mod \mathscr{I}^3. \tag{3.4}$$

From the following commutative diagram:

$$\begin{array}{ccc}
\mathbb{Z}_\ell[[G]] & \xrightarrow{\Delta} & \mathbb{Z}_\ell[[G]] \otimes \mathbb{Z}_\ell[[G]] \\
\big\downarrow{\scriptstyle \sigma} & & \big\downarrow{\scriptstyle \sigma\otimes\sigma} \\
\mathbb{Z}_\ell[[G]] & \xrightarrow{\Delta} & \mathbb{Z}_\ell[[G]] \otimes \mathbb{Z}_\ell[[G]],
\end{array}$$

for every i we have

$$\Delta(\sigma(x_i)) = (\sigma \otimes \sigma)(\Delta(x_i)). \tag{3.5}$$

We now compute both sides of this equality. Since $\Delta(g_i) = g_i \otimes g_i$ for all the generators g_i, we can compute that

$$\Delta(x_i) = \Delta(g_i - 1) = (x_i + 1) \otimes (x_i + 1) - 1 = x_i \otimes x_i + 1 \otimes x_i + x_i \otimes 1, \tag{3.6}$$

for the corresponding generators $x_i = g_i - 1$ of the augmentation ideal $\mathscr{I}$. Since Δ is a ring homomorphism, we also have

$$\Delta(x_k x_l) = \Delta(x_k)\Delta(x_l), \tag{3.7}$$

for every pair of indices k, l. Combining (3.4), (3.6), (3.7) with (3.5) and comparing coefficients of $x_k x_l$ on both sides gives

$$b_i^{kl}(\sigma) + b_i^{lk}(\sigma) = 0 \qquad \text{if } k \neq l \tag{3.8}$$

$$2b_i^{kk}(\sigma) = 0 \qquad \text{if } k = l \tag{3.9}$$

or equivalently by Definition 3.2.10 that

$$\sum_{kl} b_i^{kl}(\sigma) x_k x_l \in W \quad \text{for every } i. \tag{3.10}$$

Finally, explicit computation gives that

$$\mathrm{MD}_{\mathrm{univ}}|_T \in H^1(T, \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$$

is represented by the cocycle

$$\sigma \mapsto (x_i \mapsto \sum_{kl} b_i^{kl}(\sigma) x_k x_l) \mod \mathscr{I}^3. \tag{3.11}$$

Combining this with (3.10), we get that the explicit cocycle (3.11) representing $\mathrm{MD}_{\mathrm{univ}}$ restricted to T is visibly in the image of the map

$$H^1(T, \mathrm{Hom}(V, W)) \to H^1(T, \mathrm{Hom}(V, V \otimes V)). \qquad \square$$

Reduction to the case that G is free pro-ℓ. We now let $\tilde{G}$ be an arbitrary finitely-generated pro-ℓ group with torsion-free abelianization. Let G be a free pro-ℓ group and

$$\pi : G \to \tilde{G}$$

as a surjection inducing an isomorphism on abelianizations. Let $T_G \subset \mathrm{Aut}(G)$ be the subgroup consisting of automorphisms of G which descend to automorphisms of $\tilde{G}$ and act trivially on G^{ab}. Let $T_{\tilde{G}} \subset \mathrm{Aut}(\tilde{G})$ be the subgroup acting trivially on $\tilde{G}^{ab}$. By Lemma 3.2.9(3), the natural map $T_G \to T_{\tilde{G}}$ is surjective.

Since $T_{\tilde{G}}$ acts trivially on $\mathrm{Hom}(V, \mathscr{I}^2_{\tilde{G}}/\mathscr{I}^3_{\tilde{G}})$, we may rewrite

$$H^1(T_{\tilde{G}}, \mathrm{Hom}(V, \mathscr{I}^2_{\tilde{G}}/\mathscr{I}^3_{\tilde{G}})) = \mathrm{Hom}(T_{\tilde{G}}, \mathrm{Hom}(V, \mathscr{I}^2_{\tilde{G}}/\mathscr{I}^3_{\tilde{G}}));$$

we wish to show that the homomorphism in question factors through $\mathrm{Hom}(V, W_{\tilde{G}})$. But this is immediate for the analogous fact for G, combined with the fact that W_G surjects onto $W_{\tilde{G}}$, by definition.

Proof of Proposition 3.2.11. Let S, T be as in Lemma 3.2.13.

Apply the inflation-restriction sequence for the exact sequence of groups

$$0 \to T \to \mathrm{Aut}(G) \to S \to 0.$$

Lemma 3.2.13(I.) shows that $H^i(S, \mathrm{Hom}(V, W)^T)$ and $H^i(S, \mathrm{Hom}(V, V \otimes V)^T)$ are 2-torsion. Moreover, if $\mathrm{Hom}(V, U) \otimes \mathbb{Z}_\ell/2 = 0$, Lemma 3.2.13(II.) implies that

$$H^1(S, \mathrm{Hom}(V, W)^T) = H^1(S, \mathrm{Hom}(V, \mathscr{I}^2/\mathscr{I}^3)^T) = 0.$$

A diagram-chase finishes the proof. □

As a consequence of Remark 3.2.2 we have the following corollary.

Corollary 3.2.14. *Suppose G is a finitely-generated free pro-ℓ group or a pro-ℓ surface group. Then $2\,\mathrm{MD}_{\mathrm{univ}}$ (resp. $2J_{\mathrm{univ}}$) has a unique preimage $\widetilde{\mathrm{MD}}$ (resp. $\widetilde{J}$) under the natural map*

$$H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, W)) \to H^1(\mathrm{Aut}(G), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3))$$

(resp.

$$H^1(\mathrm{Out}(G), A_W(G)) \to H^1(\mathrm{Out}(G), A(G)).)$$

3.2.3 Ceresa classes of curves in ℓ-adic cohomology

Let X be a curve over K, and let ℓ be a prime different from the characteristic of K. For $\bar{x}$ a geometric point of X, let

$$o_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Out}(\pi_1^\ell(X_{\bar{K}}, \bar{x}))$$

be the map coming from the natural outer action of $\mathrm{Gal}(\bar{K}/K)$ on $\pi_1^{\text{ét}}(X_{\bar{K}}, \bar{x})$; here $\pi_1^\ell(X_{\bar{K}}, \bar{x})$ is the pro-ℓ completion of $\pi_1^{\text{ét}}(X_{\bar{K}}, \bar{x})$. Note that $\mathrm{Out}(\pi_1^\ell(X_{\bar{K}}, \bar{x}))$ is independent of $\bar{x}$. If $y \in X(K)$ is a rational point and $\bar{y}$ the geometric point obtained by some choice of algebraic closure $k \hookrightarrow \overline{k}$, we let

$$a_{\ell,y} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(\pi_1^\ell(X_{\bar{K}}, \bar{y}))$$

be the map induced by the canonical Galois action on $\pi_1^{\text{ét}}(X_{\overline{K}}, \bar{y})$.

Definition 3.2.15. The modified diagonal class $\mathrm{MD}(X, \bar{y})$ of the pointed curve $(X, \bar{y})$ is the pullback $a_{\ell,y}^* \mathrm{MD}_{\mathrm{univ}}$ of the group-theoretic modified diagonal class $\mathrm{MD}_{\mathrm{univ}}$ for the group $\pi_1^\ell(X_{\bar{K}}, \bar{y})$ defined in Definition 3.2.2; it depends on the choice of the rational base point y.

The Johnson class $J(X)$ of the curve X is the pullback $o_\ell^* J_{\mathrm{univ}}$ of the group-theoretic Johnson class J_{univ} for the group $\pi_1^\ell(X_{\bar{K}}, \bar{x})$ defined in Definition 3.2.8; it is by definition independent of the choice of geometric point $\bar{x}$.

Remark. Similarly, one may define classes $\widetilde{\mathrm{MD}}(X, b)$, and $\widetilde{J}(X)$ by pulling back the classes $\widetilde{\mathrm{MD}}$, and $\widetilde{J}$ of Corollary 3.2.14. Note that in general some 2-torsion information is lost when passing from MD to $\widetilde{\mathrm{MD}}$ (resp. J to $\widetilde{J}$).

Comparison to the Ceresa classes in [2]

For the rest of Section 3.2.3, we consider the case where X is a smooth, projective, and geometrically integral curve of genus g over a field K, with a rational point $b \in X(K)$. We let G be the pro-ℓ étale fundamental group $\pi_1^\ell(X \otimes \overline{K}, \bar{b})$ and let $\mathscr{I}$ be the augmentation ideal in $\mathbb{Z}_\ell[[G]]$, as in the previous section. The purpose of this section is to compare the classes $\mathrm{MD}(X, b)$ and $J(X)$ to the classes $\mu(X, b)$ and $\nu(X)$ defined in [2] arising from the Ceresa cycle. Explicitly, we show $\widetilde{\mathrm{MD}}(X, b) = \mu(X, b)$ and $\widetilde{J}(X) = \nu(X)$. For a comparison between the extension classes of mixed Hodge structures arising from the modified diagonal cycle and the Ceresa cycle, see [39, Section 1].

Lemma 3.2.16. *There are canonical isomorphisms of Galois-modules:*

$$\mathscr{I}/\mathscr{I}^2 \simeq G^{ab} \simeq H^1_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell)^\vee. \tag{3.12}$$

Proof. See Proposition 3.2.1 for the first isomorphism, [48, Example 11.3] for the second isomorphism. □

Lemma 3.2.17. *Let $H := \mathscr{I}/\mathscr{I}^2$, and let*

$$\omega : \mathbb{Z}_\ell(1) \to H^{\otimes 2}$$

be the map dual to the cup product

$$H^1(X_{\overline{K}}, \mathbb{Z}_\ell) \otimes H^1(X_{\overline{K}}, \mathbb{Z}_\ell) \to H^2(X_{\overline{K}}, \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell(-1)$$

under the identification from Lemma 3.2.16. Then we have an exact sequence

$$0 \to \mathbb{Z}_\ell(1) \xrightarrow{\omega} H^{\otimes 2} \to \mathscr{I}^2/\mathscr{I}^3 \to 0,$$

where the rightmost map is the natural multiplication map.

Proof. This is presumably well-known; we give a sketch of how to deduce it from existing literature. The analogous theorem for compact Riemann surfaces is immediate from [49, Corollary 8.2]. Now the result follows by taking pro-ℓ completions of the sequence in [49, Corollary 8.2] and comparing (1) the pro-ℓ completion of the group ring of a Riemann surface to $\mathbb{Z}_\ell[[G]]$, and (2) the singular cohomology of a compact Riemann surface to the ℓ-adic cohomology of $X_{\overline{K}}$. (Strictly speaking, the comparison above goes as follows: if necessary, lift X to characteristic zero. Then spread out, embed the ground ring in $\mathbb{C}$, and analytify. These arguments are lengthy and standard, so we omit them.) □

Recall from Definition 3.2.10 that $W \subset \mathscr{I}^2/\mathscr{I}^3$ is the image of $\mathrm{Alt}^2\ H \subset H^{\otimes 2}$ under the multiplication map $H^{\otimes 2} \to \mathscr{I}^2/\mathscr{I}^3$.

Lemma 3.2.18. *Restricting the multiplication map $H^{\otimes 2} \to \mathscr{I}^2/\mathscr{I}^3$ to $\mathrm{Alt}^2\ H$ induces an isomorphism*

$$(\mathrm{Alt}^2\ H)/\mathrm{Im}(\omega) \xrightarrow{\sim} W.$$

Proof. It suffices to show that the map ω of Lemma 3.2.17 factors through $\mathrm{Alt}^2 H$. But this is immediate from the fact that the cup product on $H^1(X_{\overline{K}}, \mathbb{Z}_\ell)$ is alternating. □

In [2, Section 5 and 10], Hain and Matsumoto define classes $m(X, b), n(X)$ in Galois cohomology, which control the action of the absolute Galois group of K on the quotient of $\pi_1^\ell(X_{\overline{K}}, b)$ by the second piece of the lower central series. In [2, Theorem 3 and 10.5] they compare these classes to classes $\mu(X,b), \nu(X)$ arising from the Ceresa cycle under the cycle class map. We briefly compare our classes to theirs, when X is smooth and proper.

Proposition 3.2.19. *Recall from Remark 3.2.3 the classes $\widetilde{\mathrm{MD}}(X,b)$, $\widetilde{J}(X)$ constructed from $2\,\mathrm{MD}(X,b)$, $2J(X)$. Let $\mu(X,b)$ and $\nu(X)$ be the classes in [2, Section 4] constructed from the image of the Ceresa cycle under a cycle class map, then $\widetilde{\mathrm{MD}}(X,b) = \mu(X,b)$ and $\widetilde{J}(X) = \nu(X)$.*

Proof. We give a sketch for $\widetilde{\mathrm{MD}}(X,b)$; the case of $\widetilde{J}(X)$ is identical. Let

$$G = L^1G \supset L^2G \supset \dots, \text{ where } L^{k+1}G = \overline{[G, L^kG]}$$

be the lower central series filtration of G. By [50, Corollary 4.2], we have the following commutative diagram of exact sequences, where all maps are compatible with the induced $\mathrm{Aut}(G)$ actions.

$$\begin{tikzcd}
0 \arrow[r] & L^2G/L^3G \arrow[r] \arrow[d, hook] & G/L^3G \arrow[r] \arrow[d, hook] & H \arrow[r] \arrow[d, "\simeq"] & 0 \\
0 \arrow[r] & \mathscr{I}^2/\mathscr{I}^3 \arrow[r] & \mathscr{I}/\mathscr{I}^3 \arrow[r] & \mathscr{I}/\mathscr{I}^2 \arrow[r] & 0.
\end{tikzcd}$$

Here all the vertical maps are induced by sending a group element g to $g-1$. Note that the middle vertical inclusion is only a set theoretic map, not a homomorphism.

Let

$$s : H \to G/L^3G, \text{ where } v \mapsto s(v)$$

be a set-theoretic section to the quotient map $G/L^3G \to H$, and let

$$s' : \mathscr{I}/\mathscr{I}^2 \to \mathscr{I}^2/\mathscr{I}^3, \text{ where } v-1 \mapsto s(v)-1$$

be the induced map. Let $T \subset \mathrm{Aut}(G)$ be the subgroup acting trivially on H. From the top sequence, following [2, Section 5.1], we get the Magnus homomorphism:

$$\tilde{\epsilon} \in \mathrm{Hom}(T, \mathrm{Hom}(H, L^2G/L^3G))^{\mathrm{GSp}\, H}$$
$$\tilde{\epsilon} \colon g \mapsto (v \mapsto g(s(v))s(v)^{-1} \bmod L^3G).$$

By [2, Proposition 5.5], there is a unique class $m \in H^1(\mathrm{Aut}\, G, \mathrm{Hom}(L^2G/L^3G))$ whose image under

$$H^1(\mathrm{Aut}\, G, \mathrm{Hom}(L^2G/L^3G)) \to H^0(\mathrm{GSp}\, H, H^1(T, \mathrm{Hom}(L^2G/L^3G)))$$

is $2\tilde{\epsilon}$ under the canonical identification

$$\mathrm{Hom}(T, \mathrm{Hom}(H, L^2G/L^3G))^{\mathrm{GSp}\, H} \simeq H^0(\mathrm{GSp}\, H, H^1(T, \mathrm{Hom}(L^2G/L^3G))).$$

By [2, Theorem 3], the pull-back of m by $G(\bar{K}/K) \to \mathrm{Aut}\, G$ induced by b agrees with the Ceresa class $\mu(X, b)$.

Now let us rewrite $g(s(v))s(v)^{-1} - 1$ modulo $\mathscr{I}^3$:

$$\begin{aligned}
g(s(v))s(v)^{-1} - 1 &= g(s(v))(s(v)^{-1} - 1) + g(s(v)) - 1 \\
&\equiv g(s(v))(1 - s(v) + (1 - s(v))^2) + g(s(v)) - 1 \\
&= g(s(v))(1 - s(v)) + (g(s(v)) - 1)(1 - s(v))^2 + (1 - s(v))^2 + g(s(v)) - 1 \\
&\equiv g(s(v))(1 - s(v)) + (1 - s(v))^2 + g(s(v)) - 1 \\
&= g(s(v)) - s(v) + (g(s(v)) - s(v))(1 - s(v)) \\
&\equiv g(s(v)) - s(v).
\end{aligned}$$

Here we use the substitution

$$s(v)^{-1} - 1 = 1 - s(v) + (1 - s(v))^2 \bmod \mathscr{I}^3$$

and the fact that

$$(g(s(v)) - 1)(1 - s(v))^2, (g(s(v)) - s(v))(1 - s(v)) \in \mathscr{I}^3$$

(because $g(s(v)) - s(v) \in \mathscr{I}^2$ by the definition of T).

But the cocycle representing the $\mathrm{MD}_{\mathrm{univ}} |_T$ is

$$g \mapsto (v - 1 \mapsto g(s(v) - 1) - (s(v) - 1) = g(s(v)) - s(v))$$

which proves that the two classes are the same under restriction to T. Now comparing the diagram chases in the proof of Proposition 3.2.11 and [2, Proposition 5.5] (using the identification from Lemma 3.2.18) completes the proof. $\square$

Stability under base change

We finally observe that the property of the Johnson or modified diagonal class being torsion is in fact a geometric property — that is, it descends through finite extensions of the ground field.

Proposition 3.2.20. *Let K be a field and X a smooth, geometrically connected curve over K. Let ℓ be a prime and $J(X)$ the associated Johnson class; if $b \in X(K)$ is a rational point we let $\mathrm{MD}(X, b)$ be the modified diagonal class. Let L/K be a finite extension. Then $J(X_L)$ (resp. $\mathrm{MD}(X_L, b_L)$) is torsion if and only if $J(X)$ (resp. $\mathrm{MD}(X, b)$) is torsion.*

Proof. Choose an algebraic closure $\overline{K}$ of K (and hence of L). Let $i_{L/K} : \mathrm{Gal}(\overline{K}/L) \to \mathrm{Gal}(\overline{K}/K)$ be the natural map; then it follows from the definition that $i^*_{L/K} J(X) = J(X_L)$ (respectively, $i^*_{L/K} \mathrm{MD}(X, b) = \mathrm{MD}(X_L, b_L)$). This proves the "if" direction.

To see the “only if" direction, suppose $J(X_L)$ (resp. $\mathrm{MD}(X_L, b_L)$) is torsion. It follows then that $i_{L/K*}i^*_{L/K}J(X)$ (resp. $i_{L/K*}i^*_{L/K}\,\mathrm{MD}(X, b)$) is torsion (where here $i_{L/K*}$ denotes the corestriction map). But $i_{L/K*}i^*_{L/K}$ is simply multiplication by the index of Gal$(\overline{K}/L)$ in Gal$(\overline{K}/K)$, which completes the proof. $\square$

3.3 Curves with torsion modified diagonal or Johnson class

3.3.1 $\mathrm{Aut}(X)$-invariance

Let X be a smooth geometrically connected curve over a field K, and ℓ a prime different from the characteristic of K. Choose a geometric point $\overline{x}$ of X and let $G = \pi_1^{\ell}(X_{\overline{K}}, \overline{x})$.

In this section, we show that $\mathrm{Aut}_K(X)$ places restrictions on the Johnson class $J(X)$; analogously, $\mathrm{Aut}_K(X, b)$ places restrictions on $\mathrm{MD}(X, b)$ for $b \in X(K)$.

Proposition 3.3.1. *Let $B \subset \mathrm{Aut}_K(X)$ be a finite subgroup such that $H^0(B, A(G)) = 0$. Then the Johnson class $J(X)$ is torsion with order $d \mid \#B$. Likewise, for $b \in X(K)$, if $B' \subset \mathrm{Aut}_K(X, b)$ is a finite subgroup with $H^0(B', \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) = 0$, then class $\mathrm{MD}(X, b)$ is torsion with order $d \mid \#B'$.*

Proof. We first prove the statement for $J(X)$.

We apply the inflation-restriction sequence to the group extension

$$1 \to B \to \mathrm{Gal}(\bar{K}/K) \times B \to \mathrm{Gal}(\bar{K}/K) \to 1,$$

which gives

$$\begin{aligned} 0 \to H^1(\mathrm{Gal}(\bar{K}/K), A(G)^B) &\to H^1(\mathrm{Gal}(\bar{K}/K) \times B, A(G)) \\ &\to H^1(B, A(G))^{\mathrm{Gal}(\bar{K}/K)}. \end{aligned}$$

Since B is a finite group, its cohomology $H^n(B, M)$ has exponent dividing $\#B$ for any finitely generated B-module M and any $n > 0$. The pullback of the Johnson class J_{univ} via

$$B \times \mathrm{Gal}(\bar{K}/K) \to \mathrm{Out}(\pi_1^{\ell}(X_{\bar{K}}))$$

is an element in $H^1(\mathrm{Gal}(\bar{K}/K)) \times B, A(G))$. Multiplying this class by $\#B$ gives a class in $H^1(\mathrm{Gal}(\bar{K}/K)), A(G)^B)$. But by assumption, $A(G)^B = 0$ which finishes the proof.

The proof is the same for the class $\mathrm{MD}(X, b)$ with the coefficients $A(G)$ replaced by the group $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)$ and B replaced by B'. $\square$

3.3.2 Hyperelliptic curves

Proposition 3.3.2. *When X is a hyperelliptic curve, class $J(X)$ is 2-torsion. Moreover, if X has a rational Weierstrass point x, class $\mathrm{MD}(X, x)$ is also 2-torsion.*

Proof. Let $\iota \in \mathrm{Aut}_K(X)$ denote the hyperelliptic involution on X. Then ι acts on $H_1(X, \mathbb{Z})$ (which is isomorphic to $\mathscr{I}/\mathscr{I}^2$) as multiplication by -1, and hence on $\mathscr{I}^2/\mathscr{I}^3$ as the identity. Thus $\mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)^{\iota} = 0$. Now the statements follow from Proposition 3.3.1, applied with $B = B' = \langle \iota \rangle$.

$\square$

Remark. The method used in Proposition 3.3.2 cannot yield similar results for superelliptic curves, using the cyclic group $\mathrm{Aut}(C/\mathbb{P}^1)$, as we now explain. For a degree n cyclic cover of the projective line, pick a prime $p \mid n$ so that we have $\mu_p \subset \mathrm{Aut}(C/\mathbb{P}^1)$ (here μ_p is the set of p-th roots of unity). Given a primitive root of unity $\zeta_p \in \mu_p$, its action on $H = H^1_{\text{sing}}(C, \mathbb{C})$ gives a decomposition $H = \oplus_{i=1}^{p-1} V_i$ where ζ_p acts on V_i as multiplication by ζ_p^i. Then we have $\dim V_i = \frac{2g}{p-1}$, which in particular does not depend on i [51]. Similarly, $H \otimes H$ also decomposes into eigenspaces for the ζ_p action, and all the V_i for $i = 1, \ldots, p-1$ appear with nonzero multiplicity in this decomposition. Therefore, we cannot rule out nontrivial $\mathrm{Aut}(C/\mathbb{P}^1)$-equivariant maps between H and $H \otimes H$ using this isotypic decomposition alone.

3.3.3 The Fricke-Macbeath curve

The Fricke-Macbeath curve C is the unique Hurwitz curve over $\overline{\mathbb{Q}}$ of genus 7. Its automorphism group is the simple group $\mathrm{PSL}_2(8)$ of order 504 [3, pg. 541]. Simplicity of $\mathrm{PSL}_2(8)$ implies that there is no central order 2 element in $\mathrm{Aut}_{\overline{\mathbb{Q}}}(C)$ and, in particular, C is not hyperelliptic. By analyzing the action of the automorphism group on the homology of curve, we show the following.

Proposition 3.3.3. *Let X/K be a curve over a number field with $X_{\overline{\mathbb{Q}}}$ isomorphic to the Fricke-Macbeath curve C above. The class $J(X)$ is torsion.*

Proof. By Proposition 3.2.20, we may without loss of generality assume $\mathrm{Aut}_K(X) \cong \mathrm{PSL}_2(8)$, by replacing K with a finite extension.

We now choose an embedding $K \hookrightarrow \mathbb{C}$ and analyze the induced representation ρ of $\mathrm{Aut}_K(X) \cong \mathrm{PSL}_2(8)$ on $H^1_{\text{sing}}(X(\mathbb{C})^{\text{an}}, \mathbb{Q})$. By standard comparison results the representation of $\mathrm{Aut}_K(X)$ on $H^1(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ will be isomorphic to the representation obtained from ρ by extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_\ell$.

Hodge theory tells us $H^1_{\text{sing}}(C, \mathbb{C})$ decomposes as the direct sum of two complex-conjugate 7-dimensional $\mathrm{PSL}_2(8)$-representations $\chi, \overline{\chi}$. As $\mathrm{PSL}_2(8)$ in fact acts on $H^1_{\text{sing}}(C, \mathbb{Q})$, it follows that the action of every element of $\mathrm{PSL}_2(8)$ on $H^1_{\text{sing}}(C, \mathbb{C})$ has trace in $\mathbb{Q}$. Furthermore, the action of $\mathrm{PSL}_2(8)$ on $H^1_{\text{sing}}(C, \mathbb{C})$ is faithful since the genus of X is greater than 1.

We now decompose $H^1_{\text{sing}}(C, \mathbb{C}) = \chi \oplus \overline{\chi}$ as an $\mathrm{Aut}_K(X) \cong \mathrm{PSL}_2(8)$ representation using character theory. In the following table, ζ_n is a choice of primitive n-th root of unity and $\bar{\zeta}_n$ its complex conjugate [24, pg. 6].

First note that if the 7-dimensional representation χ has a trivial subrepresentation, then this forces χ itself to be trivial (since the smallest nontrivial irreducible representation of $\mathrm{PSL}_2(8)$ has dimension 7). If this happens, then χ, and in turn $\overline{\chi}$ are trivial $\mathrm{PSL}_2(8)$-representations. This contradicts the faithfulness of $H^1_{\text{sing}}(C, \mathbb{C}) = \chi \oplus \overline{\chi}$ as a $\mathrm{PSL}_2(8)$-representation; hence χ is irreducible. So $H^1_{\text{sing}}(C, \mathbb{C})$ decomposes as a sum of an irreducible 7-dimensional representation and its complex conjugate.

Table 3.1: Character Table for $\mathrm{PSL}_2(8)$.

class	1	2	3	4	5	6	7	8	9
size	1	63	56	72	72	72	56	56	56
order	1	2	3	7	7	7	9	9	9
χ_1	1	1	1	1	1	1	1	1	1
χ_2	7	-1	-2	0	0	0	1	1	1
χ_3	7	-1	1	0	0	0	$-\zeta_9-\bar{\zeta}_9$	$\zeta_9^2+\bar{\zeta}_9^2$	$\zeta_9^4+\bar{\zeta}_9^4$
χ_4	7	-1	1	0	0	0	$\zeta_9^4+\bar{\zeta}_9^4$	$-\zeta_9-\bar{\zeta}_9$	$\zeta_9^2+\bar{\zeta}_9^2$
χ_5	7	-1	1	0	0	0	$\zeta_9^2+\bar{\zeta}_9^2$	$\zeta_9^4+\bar{\zeta}_9^4$	$-\zeta_9-\bar{\zeta}_9$
χ_6	8	0	-1	1	1	1	-1	-1	-1
χ_7	9	1	0	$\zeta_7+\bar{\zeta}_7$	$\zeta_7^2+\bar{\zeta}_7^2$	$\zeta_7^3+\bar{\zeta}_7^3$	0	0	0
χ_8	9	1	0	$\zeta_7^3+\bar{\zeta}_7^3$	$\zeta_7+\bar{\zeta}_7$	$\zeta_7^2+\bar{\zeta}_7^2$	0	0	0
χ_9	9	1	0	$\zeta_7^2+\bar{\zeta}_7^2$	$\zeta_7^3+\bar{\zeta}_7^3$	$\zeta_7+\bar{\zeta}_7$	0	0	0

Of the four 7-dimensional irreducible representations $\chi_i, i = 2, \cdots, 5$, of $\mathrm{PSL}_2(8)$ in the character table below, the only one that has the property that $\chi \oplus \overline{\chi}$ has all its traces in $\mathbb{Q}$ is χ_2. Hence

$$\rho \cong \chi_2 \oplus \overline{\chi_2} \cong \chi_2 \oplus \chi_2.$$

Now we compute the inner product

$$\langle \chi_2 \otimes \chi_2, \chi_2 \rangle = 7 \cdot 49 - 63 - 2 \cdot 4 \cdot 56 + 56 + 56 + 56 = 0.$$

Thus χ_2 does not appear in the decomposition of $\chi_2 \otimes \chi_2$ into irreducibles. Hence there can be no $\mathrm{PSL}_2(8)$-equivariant map from $\chi_2 \oplus \chi_2$ to $(\chi_2 \oplus \chi_2)^{\otimes 2}$, which means

$$H^0(\mathrm{PSL}_2(8), \mathrm{Hom}(\mathscr{I}/\mathscr{I}^2, \mathscr{I}^2/\mathscr{I}^3)) = 0.$$

Thus $H^0(\mathrm{PSL}_2(8), A(G)) = 0$, and by Proposition 3.3.1, the class $J(C)$ is torsion. Indeed, if $\mathrm{Aut}_K(C) = \mathrm{PSL}_2(8)$ then the class has order a divisor of 504. □

Corollary 3.3.4. *Let X be as in Proposition 3.3.3. Then the Ceresa class $\nu(X)$ as defined in [2] is torsion.*

Proof. This is immediate from Proposition 3.2.19. □

Remark. This is, to the authors' knowledge, the first known example of a non-hyperelliptic curve such that the image of the Ceresa cycle under the (ℓ-adic) Abel-Jacobi map is torsion. An analogous argument (with the mixed Hodge structure on the Betti fundamental group) shows that the Hodge-theoretic analogue is also torsion (that is, the image of the Ceresa cycle in the appropriate intermediate Jacobian is torsion). It is natural to ask if the Ceresa cycle itself is torsion in the Chow ring of the Jacobian of X modulo algebraic equivalence. Benedict Gross has explained to us that this is a prediction of the Beilinson conjectures.

It would be interesting to find (or prove the nonexistence of) a positive-dimensional family of non-hyperelliptic curves with torsion Ceresa class.

3.3.4 Curves dominated by a curve with torsion modified diagonal or Johnson class

In this last section we prove the following:

Theorem 3.3.5. *Let X be a curve over a finitely-generated field k of characteristic zero, and let $f : X \to Y$ be a dominant map of curves over k. Then:*

I. If $x \in X(k)$ is a rational point and $MD(X, x)$ is torsion, then $MD(Y, f(x))$ is torsion.

II. If $J(X)$ is torsion, then $J(Y)$ is torsion.

We view this as analogous to the fact that any curve dominated by a hyperelliptic curve is hyperelliptic.

As a corollary we have:

Corollary 3.3.6. *Let $\iota \in \mathrm{PSL}_2(8)$ be any element of order 2. If X/K is a curve of genus seven over a number field with $\mathrm{Aut}_K(X) \simeq \mathrm{PSL}_2(8)$, then $X/\langle\iota\rangle$ is a non-hyperelliptic curve of genus three with $J(X/\langle\iota\rangle)$ torsion.*

Remark. Note that curves X as above exist — for any model of the Fricke-Macbeath curve over a number field K, the base-change to a finite extension of K over which all the automorphisms are defined will suffice.

Proof of Corollary 3.3.6. The statement that $J(X/\langle\iota\rangle)$ is torsion is immediate from Theorem 3.3.5 and Proposition 3.3.3. So we need only verify that such curves are genus 3 and not hyperelliptic.

To see that $X/\langle\iota\rangle$ has genus 3, note that $\mathrm{PSL}_2(8)$ has a unique conjugacy class of order 2, whose trace (by the discussion in the proof of Proposition 3.3.3) on $H^1(X)$ is -2. Hence by the Lefschetz fixed point theorem, ι has 4 fixed points. Now Riemann-Hurwitz gives the claim.

To show that $X/\langle\iota\rangle$ is not hyperelliptic, first we note that $\mathrm{PSL}_2(8)$ has a unique conjugacy class of order 2. Hence for any two elements ι_1, ι_2 in this conjugacy class, the quotient curves $X/\langle\iota_1\rangle$ and $X/\langle\iota_2\rangle$ are isomorphic. Now in [52, Section 2], the authors give a model for one of the quotient curves — it is a smooth quartic curve in $\mathbb{P}^2$. Thus this isomorphism class of curves is non-hyperelliptic. □

We now give the proof of Theorem 3.3.5. We require the following lemmas.

Lemma 3.3.7. *Let G be a group and let*

$$0 \to U \to V \to W \to 0$$

be an extension of G-representations over an algebraically closed field of characteristic zero, with U, W semisimple. Then the extension splits if and only if the unipotent radical of the Zariski-closure of G in $GL(V)$ is trivial.

Proof. If the extension splits, then V is semisimple. Hence the Zariski-closure of the image of G is reductive, and we are done.

On the other hand, assume the sequence does not split. We may without loss of generality replace G with the Zariski-closure of its image in $GL(V)$; we now wish to argue that G is not reductive. Let $H \subset G$ be the kernel of the natural map $G \to GL(U \oplus W)$; H is evidently unipotent and normal, so it suffices to show that H is non-trivial. By semisimplicity of $U \oplus W$, it follows that G/H is reductive; hence applying inflation-restriction shows that $H^1(G, \mathrm{Hom}(W, U)) \to H^1(H, \mathrm{Hom}(W, U))$ is injective (using the assumption of characteristic zero). But $H^1(G, \mathrm{Hom}(W, U))$ is non-trivial by assumption. Hence the same is true for $H^1(H, \mathrm{Hom}(W, U))$ and thus H is non-trivial, as desired. $\square$

Lemma 3.3.8. *Let G be a group and let*

$$0 \to U \to V \to W \to 0$$

be an extension of G-representations over an algebraically closed field k of characteristic zero, with U, W semisimple. Let $S \subset G$ be a subgroup acting trivially on U, W, and let $m : S \to \mathrm{Hom}(W, U)$ be the induced map. Then the image of the extension class of this sequence under the natural map

$$H^1(G, \mathrm{Hom}(W, U)) \to H^1(G, \mathrm{Hom}(W, U)/\mathrm{im}(m))$$

vanishes if and only if the unipotent radical of the Zariski-closure of G in $GL(V)$ equals the Zariski-closure of the image of S in $GL(V)$.

Proof. Without loss of generality we may replace G with the Zariski-closure of its image in $GL(V)$ and S by the Zariski-closure of its image.

Let $N \subset G$ be the kernel of the natural representation $G \to GL(U \oplus W)$; this is a unipotent normal subgroup with reductive quotient (by the assumption that U, W are semisimple) and hence equals the unipotent radical of G. By definition we have $S \subset N$. We wish to show that the given vanishing holds in $H^1(G, \mathrm{Hom}(W, U)/\mathrm{im}(m))$ if and only if $S = N$.

Consider the short exact sequence

$$0 \to \mathrm{Hom}(W, U)/\mathrm{im}(m) \to V' \to k \to 0$$

induced by our element of $H^1(G, \mathrm{Hom}(W, U)/\mathrm{im}(m))$. Then by definition, the kernel of $N \to GL(V')$ is exactly S. Thus by Lemma 3.3.7 this extension splits if and only if $N \subset S$. This completes the proof. $\square$

Proof of Theorem 3.3.5. We first prove (1). Let $\mathscr{I}_X$ be the augmentation ideal in $\mathbb{Z}_\ell[[\pi_1^\ell(X_{\overline{k}}, \bar{x})]]$ and let $\mathscr{I}_Y$ be the augmentation ideal in $\mathbb{Z}_\ell[[\pi_1^\ell(Y_{\overline{k}}, f(\bar{x}))]]$.

Let $U_X = \mathscr{I}_X^2/\mathscr{I}_X^3 \otimes \mathbb{Q}_\ell, V_X = \mathscr{I}_X/\mathscr{I}_X^3 \otimes \mathbb{Q}_\ell, W_X = \mathscr{I}_X/\mathscr{I}_X^2 \otimes \mathbb{Q}_\ell$, and similarly let $U_Y = \mathscr{I}_Y^2/\mathscr{I}_Y^3 \otimes \mathbb{Q}_\ell, V_Y = \mathscr{I}_Y/\mathscr{I}_Y^3 \otimes \mathbb{Q}_\ell, W_Y = \mathscr{I}_Y/\mathscr{I}_Y^2 \otimes \mathbb{Q}_\ell$. Note that by Faltings's proof of the Tate conjecture for Abelian varieties [53, Satz 3], it follows that W_X, W_Y are semisimple Galois representations; as V_X, V_Y are quotients of $W_X^{\otimes 2}, W_Y^{\otimes 2}$, respectively, they are also semisimple.

By the observation on semisimplicity in the previous paragraph and Lemma 3.3.7, the Zariski closure of the image of Galois in $GL(V_X)$ is reductive. Hence the Zariski closure of Galois in $GL(V_Y)$ is reductive, as a quotient of a reductive group is reductive. Now we conclude by Lemma 3.3.7.

To prove (2), we proceed identically, using Lemma 3.3.8 in place of Lemma 3.3.7. Let G_X be the Zariski-closure of the image of $\pi_1^{\text{ét}}(X, \bar{x})$ in $GL(V_X)$, and similarly let G_Y be the Zariski-closure of the image of $\pi_1^{\text{ét}}(Y, f(\bar{x}))$ in $GL(V_Y)$ (note here that we are not taking geometric fundamental groups). Let S_X be the Zariski-closure of the image of $\pi_1^{\text{ét}}(X_{\overline{k}}, \bar{x})$ in $GL(V_X)$ and let S_Y be the Zariski-closure of the image of $\pi_1^{\text{ét}}(Y_{\overline{k}}, f(\bar{x}))$ in $GL(V_Y)$.

Unwinding the definition of $J(X)$, $J(Y)$ and applying Lemma 3.3.8, we conclude that $J(X)$ (resp. $J(Y)$) is torsion if and only if S_X (resp. S_Y) is the unipotent radical of G_X (resp. G_Y). By assumption this is true for G_X; now we conclude by the functoriality of G_X, S_X. That is, G_Y/S_Y is a quotient of G_X/S_X, hence reductive. $\square$

Chapter 4

The Supersingularity of Hurwitz Curves

4.1 Background

The first supersingular curves found were supersingular elliptic curves. Hasse noticed that some elliptic curves in positive characteristic had endomorphism rings of rank four. In 1941, Deuring defined the basic theory of supersingular elliptic curves. Supersingular curves are useful in error-correcting codes called Goppa codes. They also have potential applications to quantum resistant cryptosystems.

In this chapter we determine a condition for supersingularity of Hurwitz curves $H_{n,\ell}$ when n and ℓ are relatively prime. In particular we show that every supersingular Hurwitz curve $H_{n,\ell}$ is maximal over some finite field. We also provide a classification of supersingular Hurwitz curves with genus less than 5 over fields with characteristic less than 37 and some restrictions on the genera of Hurwitz curves.

We first define the Hurwitz curve and the Fermat curve. Next we define the zeta function of a curve. From the zeta function we compute the normalized Weil numbers which we use to study supersingularity. We must also state the Hasse-Weil bound in order to define maximality and minimality.

4.1.1 The Hurwitz Curve

Let n and ℓ be positive integers. The Hurwitz curve is given by the projective equation

$$H_{n,\ell} : X^n Y^\ell + Y^n Z^\ell + Z^n X^\ell = 0.$$

Throughout this chapter set $m = n^2 - n\ell + \ell^2$. The curve $H_{n,\ell}$ is smooth if $\gcd(m, p) = 1$ and has genus

$$g = \frac{m + 2 - 3\gcd(n, \ell)}{2}.$$

4.1.2 The Fermat Curve

The Fermat curve of degree d is given by the projective equation

$$\mathcal{F}_d : U^d + V^d + W^d = 0.$$

It has genus $\frac{(d-1)(d-2)}{2}$ and is smooth when the characteristic p of the field does not divide d. Note that the Hurwitz curve $H_{n,\ell}$ is covered by the Fermat curve of degree $m = n^2 - n\ell + \ell^2$; see Section 4.3.2 for more details.

4.1.3 Zeta Function

For a curve C defined over a field $\mathbb{F}_q$, denote the number of points on C by $\#C(\mathbb{F}_q)$. For extensions of $\mathbb{F}_q$ define $N_s = \#C(\mathbb{F}_{q^s})$. The zeta function of a curve is the series

$$Z(C/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right). \tag{4.1}$$

By the Weil conjectures,

$$Z(C/\mathbb{F}_q, T) = \frac{L(C/\mathbb{F}_q, T)}{(1-T)(1-qT)}. \tag{4.2}$$

The L-polynomial, $L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$, is of degree $2g$ [54, p152],

$$L(C/\mathbb{F}_q, T) = 1 + C_1 T + ... + C_{2g} T^{2g}. \tag{4.3}$$

The L-polynomial of a curve C over $\mathbb{F}_q$ with genus g factors in $\mathbb{C}[T]$ as

$$L(C/\mathbb{F}_q, T) = \prod_{i=1}^{2g} (1 - \alpha_i T).$$

Furthermore, $|\alpha_i| = \sqrt{q}$ for each $1 \leq i \leq 2g$ [54, pg. 155]. The coefficients of $L(C/\mathbb{F}_q, T)$ follow a pattern.

Lemma 4.1.1. *In Equation (4.3) for $0 \leq k \leq 2g$, the coefficient C_k has the form*

$$C_k = \sum_{\gamma \in \mathrm{par}(k)} \frac{\displaystyle\prod_{j \in \gamma} \frac{N_j}{j}}{\mathrm{len}(\gamma)!} - \sum_{i=0}^{k-1} (C_i \sum_{\mu=0}^{k-i} q^{\mu}).$$

Proof. Equation (4.1) can be expanded using the Taylor series of the exponential function

$$Z(C/\mathbb{F}_q, T) = \sum_{i=0}^{\infty} \frac{(N_1 T + \frac{N_2}{2} T^2 + \ldots + \frac{N_{2g}}{2g} T^{2g})^i}{i!}.$$

Collecting terms up through T^3 gives a pattern to follow:

$$Z(C/\mathbb{F}_q, T) = 1 + (N_1)T + \left(\frac{N_2}{2} + \frac{N_1^2}{2}\right) T^2 + \left(\frac{N_3}{3} + \frac{N_1 N_2}{2} + \frac{N_1^3}{6}\right) T^3 + \ldots . \tag{4.4}$$

The key step is to recognize the subscripts on the N_j are the partitions of k. Therefore, the coefficient on T^k can be written as

$$\sum_{\gamma \in \mathrm{par}(k)} \frac{\displaystyle\prod_{j \in \gamma} \frac{N_j}{j}}{\mathrm{len}(\gamma)!}.$$

Equation (4.2) gives a simplified version of $Z(C/\mathbb{F}_q, T)$. Using the Taylor series for each of the denominator terms as well as equation (4.3) results in the following expansion:

$$Z(C/\mathbb{F}_q, T) = (1 + C_1 T + ... + C_{2g} T^{2g})(1 + T + T^2 + \ldots)(1 + qT + q^2 T^2 + \ldots). \tag{4.5}$$

Expanding and collecting terms, the coefficients on T^k are given by $\sum_{i=0}^{k-1} (C_i \sum_{j=0}^{k-i} q^j) + C_k$. Setting equation (4.4) and equation (4.5) equal and comparing coefficients gives a linear system allowing one to solve for C_k in terms of the values of N_s. $\square$

4.1.4 The Newton Polygon and Supersingularity

Fix a curve $C/\mathbb{F}_q$ with associated L-polynomial $L(C/\mathbb{F}_q, T)$. We can verify whether $C/\mathbb{F}_q$ is supersingular by computing its Newton polygon. A couple definitions are required.

Definition 4.1.2 (Normalized Valuation on $\mathbb{F}_{p^r}$)**.** Let $n = p^l k$ be an integer with $p \nmid k$. We denote the normalized $\mathbb{F}_{p^r}$ valuation of n by $\text{val}_{p^r}(n) = \frac{l}{r}$. If $n = 0$ we say $\text{val}_{p^r}(0) = \infty$.

Definition 4.1.3 (Newton Polygon)**.** Fix a curve $C/\mathbb{F}_{p^r}$ with L-polynomial in the form of equation (4.3). The Newton polygon of $C/\mathbb{F}_{p^r}$ is the lower convex hull of the points $\{(i, \text{val}_{p^r}(C_i)) \mid 0 \leq i \leq 2g\}$.

Remark. Because $C_0 = 1$ for every curve $C/\mathbb{F}_{p^r}$, the Newton polygon will always have initial point $(0,0)$. Likewise the final coefficient of $L(C/\mathbb{F}_{p^r}, T)$ is always $C_{2g} = p^{rg}$. For this reason the Newton polygon always has terminal point $(2g, g)$.

From the above remark we can see that the Newton polygon of a curve C over $\mathbb{F}_{p^r}$ will always be a union of line segments on or below the line $y = \frac{1}{2}x$ with increasing slopes. A curve is supersingular when its Newton polygon is the line segment from $(0,0)$ to $(2g, g)$.

Definition 4.1.4 (Supersingularity)**.** A curve $C/\mathbb{F}_q$ is supersingular if its Newton polygon is a line segment with slope $\frac{1}{2}$.

4.1.5 Normalized Weil Numbers

The normalized Weil numbers (NWNs) are normalized reciprocal roots of the L-polynomial.

Definition 4.1.5 (Normalized Weil Numbers)**.** The Weil numbers of $C/\mathbb{F}_q$ are the reciprocal roots α_i of $L(C/\mathbb{F}_q, T)$ for $1 \leq i \leq 2g$. The normalized Weil numbers are the values $\alpha_i/\sqrt{q}$ for $1 \leq i \leq 2g$.

Remark. The curve C is supersingular if and only if all NWNs are roots of unity.

Remark. If $\{\alpha_1, \ldots, \alpha_{2g}\}$ are the NWNs over $\mathbb{F}_q$, then $\{\alpha_1^i, \ldots, \alpha_{2g}^i\}$ are the NWNs over $\mathbb{F}_{q^i}$.

4.1.6 Minimality and Maximality

Minimality or maximality of a curve $C/\mathbb{F}_q$ is determined by the Hasse-Weil bound

$$1 + q - 2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q}.$$

The curve is called minimal over $\mathbb{F}_q$ if its point count is equal to the lower bound and maximal if the point count is equal to the upper bound. If a curve is minimal or maximal over a field, it is also supersingular.

Remark. The curve C is maximal over $\mathbb{F}_q$ (resp. minimal over $\mathbb{F}_q$) if and only if all its NWNs are -1 (resp. 1) over $\mathbb{F}_q$.

In the following remark we use the notation that ζ_k is the primitive k^{th} root of unity $e^{\frac{2\pi i}{k}}$. Notice that there is a power s such that $\zeta_k^s = -1$ if and only if k is even.

Remark. Let C be a supersingular curve over $\mathbb{F}_q$. Suppose the NWNs of $C/\mathbb{F}_q$ are of the form $\zeta_{k_1}^{t_1}, \ldots, \zeta_{k_{2g}}^{t_{2g}}$. Assume $\gcd(k_i, t_i) = 1$. The curve C is maximal over $\mathbb{F}_{q^r}$ if and only if

- there exists $s \geq 1$ and b_i odd, such that $k_i = 2^s(b_i)$
- and r is an odd multiple of $2^{s-1}\text{lcm}(b_1, \ldots, b_n)$.

Proof. Assume C is maximal over $\mathbb{F}_{q^r}$. The curve C is maximal over $\mathbb{F}_{q^r}$ if and only if $\zeta_{k_i}^{rt_i} = -1$ for all i. Consequently, k_i is even for all i. Thus $k_i = 2^{s_i}b_i$ for some positive integer s_i and odd integer b_i. The condition $\zeta_{k_i}^{rt_i} = -1$ for all i implies that there exists an s such that $s = s_i$ for all i and r is an odd multiple of $2^{s-1}\text{lcm}(b_1, \ldots, b_n)$.

For the converse, the conditions imply that the NWNs of C over $\mathbb{F}_{q^r}$ are all -1. $\square$

4.2 Which Genera Occur

Recall that the genus of the Hurwitz curve $H_{n,\ell}$ has the following equation

$$g = \frac{n^2 - n\ell + \ell^2 - 3\gcd(n, \ell) + 2}{2}.$$

From this, it can be seen that the genus is determined by the quadratic form $q(x, y) = x^2 - xy + y^2$ and $\gcd(x, y)$. One might ask which genera can appear? Or, if we are given a genus of a supersingular Hurwitz curve, can we determine possibilities for x and y? In this section we will provide information about which genera can appear as a result of these equations.

Lemma 4.2.1. *Suppose we have two integers, m and n, representable by $q(x, y)$ over $\mathbb{Z}$, then mn is also representable by $q(x, y)$ over $\mathbb{Z}$.*

Proof. We can factor $x^2 - xy + y^2$ over $\mathbb{Q}(\sqrt{-3})$ in the following way

$$x^2 - xy + y^2 = (x - y\zeta_6)(x - y\zeta_6^5).$$

Note that $\zeta_6 = \frac{1+\sqrt{-3}}{2}$ and $\zeta_6 + \zeta_6^5 = 1$. Now, by the assumption that m and n are representable by $q(x, y)$, there exist $a, b, c, d \in \mathbb{Z}$ such that $q(a, b) = m$ and $q(c, d) = n$. This means that $m = (a - b\zeta_6)(a - b\zeta_6^5)$ and $n = (c - d\zeta_6)(c - d\zeta_6^5)$. Taking their product yields

$$mn = (a - b\zeta_6)(c - d\zeta_6)(a - b\zeta_6^5)(c - d\zeta_6^5).$$

Multiplying the terms with ζ_6 together, and the terms with ζ_6^5 together, we get

$$mn = (ac - (ad + bc)\zeta_6 + bd\zeta_6^2)(ac - (ad + bc)\zeta_6^5 + bd(\zeta_6^5)^2).$$

Using the identity $\zeta_6^2 = \zeta_6 - 1$, and that $\zeta_6^5 = \overline{\zeta_6}$, we can simplify the previous expression to

$$mn = ((ac - bd) - (ad + bc - bd)\zeta_6)((ac - bd) - (ad + bc - bd)\zeta_6^5).$$

This equation has the same form as the ones we started with, and so we can see that $(ac - bd, ad - bc + bd)$ is a solution to $q(x, y) = mn$, and since $a, b, c, d \in \mathbb{Z}$, we have $(ac - bd, ad + bc - bd) \in \mathbb{Z}^2$. $\square$

From this we can make an important statement about which numbers can be a result of this quadratic form. This ultimately relates back to our question about which genera can appear for a Hurwitz curve.

Theorem 4.2.2 ([55, Vol. II, pp. 310-314]). *The equation $m = x^2 - xy + y^2$ has solutions $x, y \in \mathbb{Z}$ if and only if for every prime p in the prime decomposition of m, either $p \equiv 0, 1 \mod 3$ or p is raised to an even power.*

Proof. This is the key idea of the proof. Let $p \neq 3$ be a prime. Then $p \equiv 1 \mod 3$ if and only if $\sqrt{-3}$ is a square in $\mathbb{F}_p$. This occurs if and only if p factors in $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_6)$ which is true if and only if $p = x^2 - xy + y^2$ has a solution for $(x, y) \in \mathbb{Z}^2$. $\square$

There is no restriction in Theorem 4.2.2 on what the values x and y are. However, for Hurwitz curves we require n and ℓ to be positive. The question remains as to when the equation $m = q(x, y)$ has solutions in the positive integers. To solve this we study the following automorphisms of $q(x, y) = m$.

$$\begin{cases} f: \mathbb{Z}^2 \to \mathbb{Z}^2 \mid f(x, y) \mapsto (y, x) \\ g: \mathbb{Z}^2 \to \mathbb{Z}^2 \mid g(x, y) \mapsto (-x, -y) \\ \varphi: \mathbb{Z}^2 \to \mathbb{Z}^2 \mid \varphi(x, y) \mapsto (x, x - y) \\ I: \mathbb{Z}^2 \to \mathbb{Z}^2 \mid I(x, y) \mapsto (x, y) \end{cases}$$

To see that $\varphi(x, y)$ is an automorphism, compute the following

$$\begin{aligned} q \circ \varphi(x, y) &= x^2 - x(x - y) + (x - y)^2 \\ &= x^2 - x^2 + xy + x^2 - 2xy + y^2 \\ &= x^2 - xy + y^2 \\ &= q(x, y). \end{aligned}$$

Corollary 4.2.3. *If the equation $m = q(x,y)$ has solution $(x,y) \in \mathbb{Z}^2$ then there is a solution with $(x',y') \in \mathbb{N}^2$.*

Proof. We separate into cases, depending on the values of x and y.

I. If both x and y are negative, then $g(x,y) = (-x,-y) \in \mathbb{N}^2$.

II. If y negative and x positive, then $\varphi(x,y) = (x, x-y) \in \mathbb{N}^2$.

III. If x negative and y positive, then $\varphi(f(x,y)) = (y, y-x) \in \mathbb{N}^2$.

IV. If x is 0, then $\varphi \circ f(0,y) = (y,y)$ and if y is 0, then $\varphi(y,0) = (y,y)$.

□

4.3 Curve maps and covers

4.3.1 Aoki's Curve

Let $\alpha = (a,b,c) \in \mathbb{N}^3$ with $a+b+c = m$. Note that S_3, the symmetric group on three letters, acts on α by permuting the coordinates. For $\sigma \in S_3$ we denote the action by α^σ. We say two triples $\alpha = (a_1,a_2,a_3)$ and $\beta = (b_1,b_2,b_3)$ are equivalent, denoted $\alpha \approx \beta$, if there exist elements $t \in (\mathbb{Z}/m)^*$ and $\sigma \in S_3$ such that

$$(a_1,a_2,a_3) \equiv (tb_{\sigma(1)}, tb_{\sigma(2)}, tb_{\sigma(3)}) \bmod m.$$

In [56] and [57], Aoki studies curves of the form

$$D_\alpha : v^m = (-1)^c u^a (1-u)^b.$$

He provides the following conditions for when D_α is supersingular.

Theorem 4.3.1 ([57, Theorem 1.1])**.** *The curve D_α is supersingular over $\mathbb{F}_{p^r}$ if and only if at least one of the following conditions holds:*

- $p^i \equiv -1 \bmod m$ *for some* i.

- $\alpha \approx (1, -p^i, p^i - 1)$ *for some integer* i *such that* $d = \gcd(p^i - 1, m) > 1$ *and* $p^j \equiv -1 \bmod \frac{m}{d}$ *for some integer* j.

4.3.2 Covers of $H_{n,\ell}$ by $\mathcal{F}_m$

In Section 4.1.2, we noted that the Hurwitz curve $H_{n,\ell}$ is covered by the Fermat curve $\mathcal{F}_m$ where $m = n^2 - n\ell + \ell^2$. On an affine patch the Fermat and Hurwitz curves are given by the following equations

$$\mathcal{F}_m : u^m + v^m + 1 = 0$$
$$H_{n,l} : x^n y^\ell + y^n + x^\ell = 0.$$

Then the following covering map is provided by [58, Lemma 4.1]

$$\begin{aligned} \phi : \mathcal{F}_m &\to H_{n,\ell} \\ (u, v) &\mapsto (u^n v^{-l}, u^l v^{n-l}). \end{aligned}$$

Furthermore, it is known that $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$ if and only if $p^i \equiv -1 \bmod m$ for some integer i [59, Prop. 3.10]. See also [60, Theorem 3.5]. In [61, Theorem 5] it is shown that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{p^{2i}}$ if and only if $p^i \equiv -1 \bmod m$.

Remark. If $X \to Y$ is a covering of curves defined over $\mathbb{F}_{p^r}$, then the NWNs of $Y/\mathbb{F}_{p^r}$ are a subset of the NWNs of $X/\mathbb{F}_{p^r}$, see [62].

Thus when a covering curve is supersingular (or maximal or minimal) the curve it covers will be as well.

4.3.3 A Birational Transformation

In [63], Bennama and Carbonne show that $H_{n,\ell}$ is isomorphic to a curve with affine equation

$$y'^m = x'^\lambda(x' - 1) \tag{4.6}$$

via the following variable change. Suppose $1 \leq \ell < n$ and $\gcd(n, \ell) = 1$. Then there exist integers θ and δ such that $1 \leq \theta \leq \ell$, $1 \leq \delta \leq n - 1$, and $n\theta - \delta\ell = 1$. Let $\lambda = \delta n - \theta(n - \ell)$ and $m = n^2 - n\ell + \ell^2$. The birational transformation is as follows

$$\begin{cases} x = (-x')^{-\delta}((-1)^\lambda y')^n \\ y = (-x')^{-\theta}((-1)^\lambda y')^\ell \end{cases}$$

and

$$\begin{cases} x' = -x^\ell y^{-n} \\ y' = (-1)^\lambda x^\theta y^{-\delta}. \end{cases}$$

Equation (4.6) is very similar to the equation for D_α that Aoki studies but there are small differences. The following argument shows that these can be reconciled. Consequently, this variable change can be used to apply Aoki's results to Hurwitz curves.

Notice that equation (4.6) is divisible by $(x' - 1)$ while Aoki studies curves whose equation contains a $(1 - x')$ factor. Aoki requires that $a + b + c = m$ so the exponent on the negative sign is important. Inspecting equation (4.6) we see that m will always be odd since $(n, \ell) = 1$. Consequently, this negative sign is not an issue. Since m is always odd we can replace v with $-v$. This choice allows us to pick $c = m - a - b$. Then $b = 1$ and $a = \lambda$.

4.4 Supersingular Hurwitz Curves

We arrive at explicit conditions on supersingularity for $H_{n,\ell}$ when n and ℓ are relatively prime. We use results from [63] and [56] to accomplish this. We will be using affine equations for the Hurwitz curve in this section.

Lemma 4.4.1. *If n and ℓ are relatively prime then $x^n y^\ell + y^n + x^\ell = 0$ is supersingular over $\mathbb{F}_p$ if and only if at least one of the following conditions holds.*

I. There exists $i \in \mathbb{Z}_{>0}$ such that $p^i \equiv -1 \bmod m$.

(In this case the Fermat curve covering the Hurwitz curve is maximal over $\mathbb{F}_{p^{2i}}$.)

II. There exists $i \in \mathbb{Z}_{>0}$ with $d = (p^i - 1, m) > 1$ such that

$$(\delta(n-\ell) + \ell\theta - 1, 1, -(\delta(n-\ell) + \ell\theta)) \approx (1, -p^i, p^i - 1)$$

and $p^j \equiv -1 \bmod (\frac{m}{d})$ for some integer j.

Proof. We use the variable substitution from [63] to apply Aoki's results to Hurwitz curves. We use the substitutions:

- $m = n^2 - n\ell + \ell^2$,
- $a = \lambda = \delta(n-\ell) + \ell\theta - 1$,
- $b = 1$,
- $c = m - (\delta(n-\ell) + \ell\theta)$.

Combining these with Aoki's results completes the proof. $\square$

Remark. If n and ℓ are relatively prime, then n and ℓ are relatively prime to $n^2 - n\ell + \ell^2$.

Theorem 4.4.2. *Suppose n and ℓ are relatively prime and $m = n^2 - n\ell + \ell^2$. Then $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$ if and only if $p^i \equiv -1 \bmod m$ for some positive integer i.*

Proof. If $p^i \equiv -1 \bmod m$ for some positive integer i, then $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$ by [59, Prop. 3.10]. Recall from section 4.3.2 that $\mathcal{F}_m$ covers $H_{n,\ell}$, thus $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$.

Suppose $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$. By Lemma 4.4.1 it is enough to show condition 2 in Lemma 4.4.1 can not happen. We begin by simplifying it using the substitution $\theta = \frac{1+\ell\delta}{n}$ and reducing modulo m to show that condition 2 is equivalent to $(\frac{\ell}{n} - 1, 1, -\frac{\ell}{n}) \approx (1, -p^i, p^i - 1)$ for some i such that $d = (p^i - 1, m) > 1$ and $p^j \equiv -1 \mod (\frac{m}{d})$ for some integer j. Recall that $\alpha \approx \alpha'$ if $\alpha = t\alpha'^{\sigma}$ for some $t \in (\mathbb{Z}/m)^*$ and $\sigma \in S_3$. We will show that $p^i - 1$ and m are relatively prime. We label the three coordinates of $(\frac{\ell}{n} - 1, 1, -\frac{\ell}{n})$ as (a, b, c) and the three coordinates of $(1, -p^i, p^i - 1)$ as (A, B, C).

The proof will address six cases accounting for the orbit of (A, B, C) under the action of S_3. In each case we will show that $\gcd(p^i - 1, m) = 1$. Specifically, we show $d = 1$ by taking these congruences modulo d. By Remark 4.4 we know that n^{-1} exists modulo m and modulo d. Finally, note that $\frac{\ell}{n}$ is relatively prime to d.

- $(a, b, c) \equiv t(A, B, C) \bmod m$: Comparing c and tC yields

$$-\frac{\ell}{n} \equiv t(p^i - 1) \bmod m.$$

  Consequently, $\frac{\ell}{n} \equiv 0 \bmod d$. Therefore, $d = 1$.

- $(a, b, c) \equiv t(B, A, C) \bmod m$: Comparing a with tB and b with tA yields

$$\frac{\ell}{n} - 1 \equiv -tp^i \bmod m$$
$$1 \equiv t \bmod m.$$

  Substituting we have $\frac{\ell}{n} \equiv p^i - 1 \bmod m$. Reducing modulo d produces $\frac{\ell}{n} \equiv 0 \bmod d$, thus $d = 1$.

- $(a,b,c) \equiv t(A,C,B) \bmod m$: Comparing b and tC yields

$$-\frac{\ell}{n} \equiv t(p^i - 1) \bmod m.$$

This is identical to the first case.

- $(a,b,c) \equiv t(C,B,A) \bmod m$: Comparing a and tC yields

$$\frac{\ell}{n} - 1 \equiv t(p^i - 1) \bmod m.$$

Thus $\frac{\ell}{n} - 1 \equiv 0 \bmod d$. Recall by the definition of m and selection of d, we have $d \mid n^2 - n\ell + \ell^2$. Hence, d divides $1 - \frac{\ell}{n} + (\frac{\ell}{n})^2$. We conclude $d|(\frac{\ell}{n})$, thus $d = 1$.

- $(a,b,c) \equiv t(C,A,B) \bmod m$: Comparing b with tA and c with tB yields

$$1 \equiv t \bmod m$$
$$\frac{\ell}{n} \equiv tp^i \bmod m.$$

This case is completed as in the previous case.

- $(a,b,c) \equiv t(B,C,A) \bmod m$: Comparing b with tC yields

$$1 \equiv t(p^i - 1) \bmod m.$$

Modulo d this reduces to $1 \equiv 0 \bmod d$. Therefore, $d = 1$.

$\square$

Corollary 4.4.3. *If n and ℓ are relatively prime and $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then it will be maximal over $\mathbb{F}_{p^{2i}}$ where i is the same as in Theorem 4.4.2.*

Proof. By Theorem 4.4.2, if $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then $p^i \equiv -1 \bmod m$ for some i. By the results of [61] we know that this implies $\mathcal{F}_m$ will be maximal over $\mathbb{F}_{p^{2i}}$. Since $\mathcal{F}_m$ covers $H_{n,\ell}$, this implies $H_{n,\ell}$ will also be maximal over $\mathbb{F}_{p^{2i}}$. □

Apriori, if $H_{n,\ell}$ is supersingular (or maximal or minimal) over $\mathbb{F}_p$ then $\mathcal{F}_m$ may not be because it has more NWNs.

Corollary 4.4.4. *If n and ℓ are relatively prime and $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$.*

Proof. If $H_{n,\ell}$ supersingular over $\mathbb{F}_p$ and $\gcd(n, \ell) = 1$, Theorem 4.4.2 shows the existence of positive integer i such that $p^i \equiv -1 \bmod m$. Then by [59, Prop. 3.10] $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$. □

Partial results are known for when a Hurwitz curve is maximal.

Theorem 4.4.5 ([58, Theorem 3.1])**.** *Let $\ell = 1$. The curve $H_{n,1}$ is maximal over $\mathbb{F}_{q^{2j}}$ if and only if $p^j \equiv -1 \bmod m$ for some positive integer j.*

Theorem 4.4.6 ([58, Theorem 4.5])**.** *Assume that $\gcd(n, \ell) = 1$ and m is prime. Then $H_{n,\ell}$ is maximal over $\mathbb{F}_{p^{2j}}$ if and only if $p^j \equiv -1 \bmod m$ for some positive integer j.*

Note that the key property used in [58] is the existence of some positive integer j such that

$$p^j \equiv -1 \bmod m. \tag{4.7}$$

Remark. Under the requirements $\ell = 1$, or $\gcd(n, \ell) = 1$ and m prime, the results in [58] and [61, Theorem 5] show that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{q^2}$ if and only if $H_{n,\ell}$ is maximal over $\mathbb{F}_{q^2}$.

We consider the case when $H_{n,\ell}$ and $\mathcal{F}_m$ are minimal.

Corollary 4.4.7. *If $\ell = 1$, or n and ℓ are relatively prime and m is prime, $H_{n,\ell}$ is minimal over $\mathbb{F}_{p^{4i}}$ if and only if $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4i}}$.*

Proof. First suppose $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4i}}$ with set N of NWNs. Then the NWNs of $H_{n,\ell}$ are a subset of N. Thus $H_{n,\ell}$ will also be minimal over $\mathbb{F}_{p^{4i}}$.

Now assume $H_{n,\ell}$ is minimal over $\mathbb{F}_{p^{4i}}$. Minimality implies supersingularity, thus $H_{n,\ell}$ must also be supersingular. By Theorem 4.4.2 supersingularity of $H_{n,\ell}$ over $\mathbb{F}_p$ implies $p^j \equiv -1 \bmod m$ for some positive integer j. Choose a minimal such j. Then Corollary 4.4.3 shows $H_{n,\ell}$ is maximal over $\mathbb{F}_{p^{2j}}$ thus minimal over $\mathbb{F}_{p^{4j}}$. Minimality of j implies that $\mathbb{F}_{p^{4j}}$ is a subfield of $\mathbb{F}_{p^{4i}}$. Consequently, $j \mid i$.

Now, by [58] $p^j \equiv -1 \bmod m$ implies that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{p^{2j}}$. Hence, $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4j}}$. Because $j \mid i$, $\mathcal{F}_m$ is minimal over $\mathcal{F}_{p^{4i}}$. $\square$

Remark. The curve $H_{3,3}$ is maximal over $\mathbb{F}_{5^2}$ but $\mathcal{F}_9$ is not. The above theorems show a supersingular Hurwitz curve and its covering Fermat curve will both be maximal over $\mathbb{F}_{p^{2i}}$. This does not imply that the Fermat curve will always be maximal over the same field extension that the Hurwitz curve is. The Hurwitz curve could also be maximal over $\mathbb{F}_{p^{2j}}$ where $j \mid i$ with i/j odd. In this case the Fermat curve may not be maximal over this field because it has a higher genus. Unfortunately our example of this does not have n and ℓ being relatively prime. It is difficult to find an example with n and ℓ relatively prime, as the genera of Hurwitz curves grow quickly causing the point counts to become computationally expensive.

Figure 4.1 illustrates how the current theory fits together. The straight, dotted arrows are under the conditions $\ell = 1$, or $\gcd(n, \ell) = 1$ and m prime. The notation max/$\mathbb{F}_{q^2}$ means, for some power q of p, the curve is maximal over $\mathbb{F}_{q^2}$. If a curve is maximal over $\mathbb{F}_{q^2}$ then it is minimal over $\mathbb{F}_{q^4}$. The curved arrows show that under appropriate conditions a Hurwitz or Fermat curve is supersingular if and only if it is minimal over some field extension. Corollary 4.4.3 and Corollary 4.4.4 are under the condition that $\gcd(n, \ell) = 1$, while [58] and Corollary 4.4.7 are under the condition that $\ell = 1$, or $\gcd(n, \ell) = 1$ and m is prime.

Figure 4.1: Current results regarding supersingularity, minimality, and maximality of Hurwitz and Fermat curves.

$$\begin{tikzcd}
\mathcal{F}_m \text{ s.s.}/\mathbb{F}_p \arrow[r, shift left, twoheadrightarrow, "{[61]}"] \arrow[d, shift right, "{[62]}"'] \arrow[rr, bend left, dotted, leftrightarrow] & \mathcal{F}_m \max/\mathbb{F}_{q^2} \arrow[l, shift left] \arrow[r] \arrow[d, shift right, "{[62]}"'] & \mathcal{F}_m \min/\mathbb{F}_{q^4} \arrow[d, shift right, "{[62]}"'] \\
H_{n,\ell} \text{ s.s.}/\mathbb{F}_p \arrow[u, shift right, "\text{Corollary 4.4.4}"'] \arrow[r, shift right, "\text{Corollary 4.4.3}"'] \arrow[rr, bend right, dotted, leftrightarrow] & H_{n,\ell} \max/\mathbb{F}_{q^2} \arrow[l, shift right] \arrow[r] \arrow[u, shift right, dotted, "{[58]}"'] & H_{n,\ell} \min/\mathbb{F}_{q^4} \arrow[u, shift right, dotted, "\text{Corollary 4.4.7}"']
\end{tikzcd}$$

4.5 Data

Here we provide a classification of supersingular Hurwitz curves over fields with characteristic $p < 37$ and with genus less than 5.

By counting points and using Lemma 4.1.1 we computed, using [64], the L-polynomials and NWNs of many supersingular Hurwitz curves over $\mathbb{F}_p$. When n and ℓ are not relatively prime it is possible that certain points of the equation for $H_{n,\ell}$ are singular. Resolving these singularities requires taking a field extension of $\mathbb{F}_p$. To adjust for this we see if $q \equiv 1 \mod \gcd(n, \ell)$ and count the multiplicities of singular points. This gives the correct point counts to compute the L-polynomial of the normalization of the equation. The table has all supersingular Hurwitz curves $H_{n,\ell}$ of genus less than 5 for primes less than 37. The table also includes some curves of genus 6.

Table 4.1: Supersingular Hurwitz curves in characteristic $p < 37$ with genus < 5.

n	l	p	g	L-Polynomial	NWNs (multiplicity)
2	1	5	1	$5T^2 + 1$	i, -i
2	1	11	1	$11T^2 + 1$	i, -i
2	1	17	1	$17T^2 + 1$	i, -i
2	1	23	1	$23T^2 + 1$	i, -i
2	1	29	1	$29T^2 + 1$	i, -i
3	3	5	1	$5T^2 + 1$	i, -i
3	3	11	1	$11T^2 + 1$	i, -i
3	3	17	1	$17T^2 + 1$	i, -i
3	3	23	1	$23T^2 + 1$	i, -i
3	3	29	1	$29T^2 + 1$	i, -i
3	1	3	3	$27T^6 + 1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	5	3	$125T^6 + 1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	13	3	$2197T^6 + 507T^4 + 39T^2 + 1$	i(3), -i(3)
3	1	17	3	$4913T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	19	3	$6859T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	31	3	$29791T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	3	3	$27T^6 + 1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	5	3	$125T^6 + 1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	13	3	$2197T^6 + 507T^4 + 39T^2 + 1$	i(3), -i(3)
3	2	17	3	$4913T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	19	3	$6859T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	31	3	$29791T^6 + 1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
4	2	5	4	$625T^8 + 500T^6 + 150T^4 + 20T^2 + 1$	i(4), -i(4)
4	2	17	4	$83521T^8 + 19652T^6 + 1734T^4 + 68T^2 + 1$	i(4), -i(4)
4	2	29	4	$707281T^8 + 97556T^6 + 5046T^4 + 116T^2 + 1$	i(4), -i(4)
4	1	5	6	$15625T^{12} + 1875T^8 + 75T^4 + 1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
4	3	5	6	$15625T^{12} + 1875T^8 + 75T^4 + 1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	3	6	$729T^{12} + 243T^8 + 27T^4 + 1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	7	6	$117649T^{12} + 7203T^8 + 147T^4 + 1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	13	6	$4826809T^{12} + 85683T^8 + 507T^4 + 1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$

Bibliography

[1] Dean Bisogno. Abhyankar's inertia conjecture for some sporadic groups, 2020. In Preparation.

[2] Richard Hain and Makoto Matsumoto. Galois actions on fundamental groups of curves and the cycle $C - C^{-}$. *J. Inst. Math. Jussieu*, 4(3):363–403, 2005.

[3] A. M. Macbeath. On a curve of genus 7. *Proc. London Math. Soc. (3)*, 15:527–542, 1965.

[4] Dean Bisogno, Wanlin Li, Daniel Litt, and Padmavathi Srinivasan. Group-theoretic johnson classes and a non-hyperelliptic curve with torsion ceresa class, 2020.

[5] Erin Dawson, Henry Frauenhoff, Michael Lynch, Amethyst Price, Seamus Somerstep, Eric Work, Dean Bisogno, and Rachel Pries. The supersingularity of Hurwitz curves. *Involve*, 12(8):1293–1306, 2019.

[6] Jean-Pierre Serre. Construction de revêtements étales de la droite affine en caractéristique p. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(6):341–346, 1990.

[7] Shreeram Abhyankar. Coverings of algebraic curves. *Amer. J. Math.*, 79:825–856, 1957.

[8] M. Raynaud. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. *Invent. Math.*, 116(1-3):425–462, 1994.

[9] David Harbater. Abhyankar's conjecture on Galois groups over curves. *Invent. Math.*, 117(1):1–25, 1994.

[10] Shreeram S. Abhyankar. Resolution of singularities and modular Galois theory. *Bull. Amer. Math. Soc. (N.S.)*, 38(2):131–169, 2001.

[11] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[12] David Harbater and Katherine F. Stevenson. Patching and thickening problems. *J. Algebra*, 212(1):272–304, 1999.

[13] Rachel J. Pries. Conductors of wildly ramified covers. III. *Pacific J. Math.*, 211(1):163–182, 2003.

[14] David Harbater. Fundamental groups of curves in characteristic p. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 656–666. Birkhäuser, Basel, 1995.

[15] David Harbater. Formal patching and adding branch points. *Amer. J. Math.*, 115(3):487–508, 1993.

[16] Irene I. Bouw and Rachel J. Pries. Rigidity, reduction, and ramification. *Math. Ann.*, 326(4):803–824, 2003.

[17] Jeremy Muskat and Rachel Pries. Alternating group covers of the affine line. *Israel J. Math.*, 187:117–139, 2012.

[18] Andrew Obus. Toward Abhyankar's inertia conjecture for $PSL_2(l)$. In *Geometric and differential Galois theories*, volume 27 of *Sémin. Congr.*, pages 195–206. Soc. Math. France, Paris, 2013.

[19] S. Das and M. Kumar. On Inertia Conjecture for Alternating group Covers. *ArXiv e-prints*, November 2017.

[20] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[21] Hans J. Zassenhaus. *The theory of groups*. 2nd ed. Chelsea Publishing Company, New York, 1958.

[22] Rachel J. Pries. Conductors of wildly ramified covers. II. *C. R. Math. Acad. Sci. Paris*, 335(5):485–487, 2002.

[23] Michio Suzuki. *Gun ron. Vol. 1*, volume 18 of *Gendai Sūgaku [Modern Mathematics]*. Iwanami Shoten, Tokyo, 1977.

[24] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[25] Donald G. Higman and Charles C. Sims. A simple group of order $44,352,000$. *Math. Z.*, 105:110–113, 1968.

[26] Jack McLaughlin. A simple group of order $898,128,000$. In *Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968)*, pages 109–111. Benjamin, New York, 1969.

[27] Arunas Rudvalis. A rank 3 simple group of order $2^{14}3^3 5^3 7 \cdot 13 \cdot 29$. I. *J. Algebra*, 86(1):181–218, 1984.

[28] Petra E. Holmes and Robert A. Wilson. On subgroups of the Monster containing A_5's. *J. Algebra*, 319(7):2653–2667, 2008.

[29] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

[30] Rachel J. Pries. Wildly ramified covers with large genus. *J. Number Theory*, 119(2):194–209, 2006.

[31] Stefan Wewers. Three point covers with bad reduction. *J. Amer. Math. Soc.*, 16(4):991–1032, 2003.

[32] Michel Raynaud. Spécialisation des revêtements en caractéristique $p > 0$. *Ann. Sci. École Norm. Sup. (4)*, 32(1):87–126, 1999.

[33] Rachel J. Pries. Conductors of wildly ramified covers. I. *C. R. Math. Acad. Sci. Paris*, 335(5):481–484, 2002.

[34] Irene I. Bouw. Covers of the affine line in positive characteristic with prescribed ramification. In *WIN—women in numbers*, volume 60 of *Fields Inst. Commun.*, pages 193–200. Amer. Math. Soc., Providence, RI, 2011.

[35] G. Ceresa. C is not algebraically equivalent to C^- in its Jacobian. *Ann. of Math. (2)*, 117(2):285–291, 1983.

[36] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.

[37] B. H. Gross and C. Schoen. The modified diagonal cycle on the triple product of a pointed curve. *Ann. Inst. Fourier (Grenoble)*, 45(3):649–679, 1995.

[38] Benedict H. Gross and Stephen S. Kudla. Heights and the central critical values of triple product L-functions. *Compositio Math.*, 81(2):143–209, 1992.

[39] Henri Darmon, Victor Rotger, and Ignacio Sols. Iterated integrals, diagonal cycles and rational points on elliptic curves. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2012/2*, volume 2012/ of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 19–46. Presses Univ. Franche-Comté, Besançon, 2012.

[40] S. Andreadakis. On the automorphisms of free groups and free nilpotent groups. *Proc. London Math. Soc. (3)*, 15:239–268, 1965.

[41] S. Bachmuth. Automorphisms of free metabelian groups. *Trans. Amer. Math. Soc.*, 118:93–104, 1965.

[42] S. Bachmuth. Induced automorphisms of free groups and free metabelian groups. *Trans. Amer. Math. Soc.*, 122:1–17, 1966.

[43] Dennis Johnson. An abelian quotient of the mapping class group $\mathcal{I}_g$. *Math. Ann.*, 249(3):225–242, 1980.

[44] Shigeyuki Morita. The extension of Johnson's homomorphism from the Torelli group to the mapping class group. *Invent. Math.*, 111(1):197–224, 1993.

[45] Jean-Pierre Serre. *Cohomologie Galoisienne*. Lecture Notes in Mathematics, Vol. 5. Springer-Verlag, Berlin-New York, 1973. Cours au Collège de France, Paris, 1962–1963, Avec des textes inédits de J. Tate et de Jean-Louis Verdier, Quatrième édition.

[46] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[47] Mamoru Asada and Masanobu Kaneko. On the automorphism group of some pro-l fundamental groups. In *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, volume 12 of *Adv. Stud. Pure Math.*, pages 137–159. North-Holland, Amsterdam, 1987.

[48] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[49] Richard Hain. Iterated integrals and algebraic cycles: examples and prospects. In *Contemporary trends in algebraic geometry and algebraic topology (Tianjin, 2000)*, volume 5 of *Nankai Tracts Math.*, pages 55–118. World Sci. Publ., River Edge, NJ, 2002.

[50] Daniel G. Quillen. On the associated graded ring of a group ring. *J. Algebra*, 10:411–418, 1968.

[51] Ben Moonen. Special subvarieties arising from families of cyclic covers of the projective line. *Doc. Math.*, 15:793–819, 2010.

[52] Jaap Top and Carlo Verschoor. Counting points on the Fricke-Macbeath curve over finite fields. *J. Théor. Nombres Bordeaux*, 30(1):117–129, 2018.

[53] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[54] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[55] Pierre Fermat. *Œuvres de Pierre Fermat. I.* Collection Sciences dans l'Histoire. [Science in History Collection]. Librairie Scientifique et Technique Albert Blanchard, Paris, 1999. La théorie des nombres. [Number theory], Translated by Paul Tannery, With an introduction and commentary by R. Rashed, Ch. Houzel and G. Christol.

[56] Noboru Aoki. On supersingular cyclic quotients of Fermat curves. *Comment. Math. Univ. St. Pauli*, 57(1):65–90, 2008.

[57] Noboru Aoki. On the zeta function of some cyclic quotients of Fermat curves. *Comment. Math. Univ. St. Pauli*, 57(2):163–185, 2008.

[58] Angela Aguglia, Gábor Korchmáros, and Fernando Torres. Plane maximal curves. *Acta Arith.*, 98(2):165–179, 2001.

[59] Tetsuji Shioda and Toshiyuki Katsura. On Fermat varieties. *Tôhoku Math. J. (2)*, 31(1):97–115, 1979.

[60] Noriko Yui. On the Jacobian variety of the Fermat curve. *J. Algebra*, 65(1):1–35, 1980.

[61] Saeed Tafazolian. A characterization of maximal and minimal Fermat curves. *Finite Fields Appl.*, 16(1):1–3, 2010.

[62] Jean Pierre Serre. Rational points on curves over finite fields. unpublished notes by F.Q. Gouvêa of lectures at Harvard Univ., 1985.

[63] H. Bennama and P. Carbonne. Courbes $X^mY^n + Y^mZ^n + Z^mX^n = 0$ et décomposition de la jacobienne. *J. Algebra*, 188(2):409–417, 1997.

[64] Inc. SageMath. *CoCalc Collaborative Computation Online*, 2016.