IMAGES OF METABELIAN GALOIS REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES

By

Rachel Davis

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

(MATHEMATICS)

at the

UNIVERSITY OF WISCONSIN – MADISON

2013

Date of final oral examination: July 25, 2013

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

Nigel Boston, Professor, Mathematics and ECE

Jordan Ellenberg, Professor, Mathematics

Melanie Matchett Wood, Assistant Professor, Mathematics

Richard Peabody Kent IV, Assistant Professor, Mathematics

Stephen Wainger, Emeritus Professor, Mathematics

Abstract

Let E be an elliptic curve over $\mathbb{Q}$. For ℓ-adic representations associated to E, much is understood about the sizes of the images and the conjugacy invariants of the images of Frobenius elements. On the other hand, much less is known about the outer Galois representations associated to E. These are representations from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to an outer automorphism group of a free pro-ℓ group.

The goal of this thesis is to take a first step in understanding more concretely more general Galois representations associated to E (to the automorphism group of a non-abelian group). In particular, I study the surjectivity of a Galois representation to a certain subgroup of the automorphism group of a metabelian group. I use the Frattini lifting theorem to turn the question of the surjectivity of this representation into a question about the surjectivity of a representation to the Frattini quotient of this group. Then, I compute some conjugacy invariants for the images of the Frobenius elements. This will give rise to new arithmetic information analogous to traces of Frobenius of the ℓ-adic representation.

Acknowledgements

I would like to thank my advisor, Nigel Boston, for his mathematical insight, patient teaching, and helpful encouragement during my time as his student. I am very glad to have had the opportunity to work with him. He has taught me about becoming a mathematician both through his suggestions and by his example. Thank you to Jordan Ellenberg and Melanie Wood for talking to me about my research. I would also like to thank Richard Kent, Stephen Wainger, Tonghai Yang, and Ken Ono for offering interesting classes and seminars.

There are many other people whom I view as mathematical and professional mentors and I am very grateful to all of them, especially Glenn Deans, Ruth Tancrede, William Rinaman, William Miller, Michael Miller, Murli Gupta, Joel Foisy, Sergei Tabachnikov, and Shirin Malekpour. Thank you to the other Wisconsin graduate students both for learning with me and for making the time enjoyable. Thank you Mom, Dad, Ryan, Nick, and Sam.

Notation and Symbols

- Let $G_{\mathbb{Q}}$ denote the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- Let E denote an elliptic curve.
- Let $E(K)$ denote the points of E defined over K
- ℓ a fixed prime
- $E[n]$ the n-torsion points of E defined over the algebraic closure of the number field of definition of E.
- For an abelian group A, $\mathrm{rk}_2 A = \dim_{\mathbb{F}_2} A/2A$.
- Let K denote a number field.
- Let $\mathcal{O}_K$ denote the maximal order of K.
- Let $\mu(K)$ denote the roots of unity in K.
- Let $\mathrm{Cl}(K)$ denote the class group of K.
- Let $\mathrm{U}(K)$ denote the unit group of K.
- Let $\mathrm{Cl}_{\mathbf{m}}(K)$ denote the ray class group of K with modulus $\mathbf{m}$.
- Let $(\mathcal{O}_K/\mathbf{m})^*$ denote the units mod $\mathbf{m}$ of K.
- Let $r_1(K)$ denote the number of real embeddings of K.
- Let $r_2(K)$ denote the number of pairs of complex conjugate embeddings of K.

Contents

Chapter 1

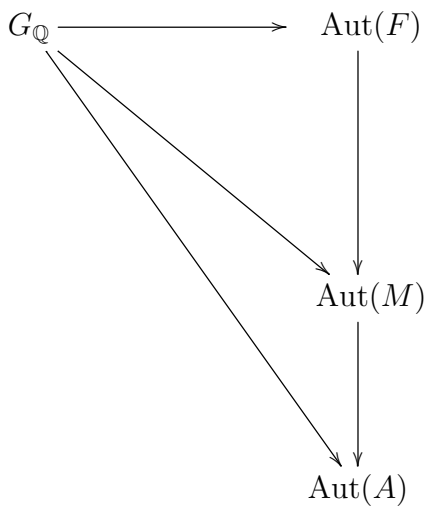
Introduction

1.1 Background and motivation

In the classical case of ℓ-adic Galois representations associated to elliptic curves, there are theorems concerning when these representations are surjective. Also, for these ℓ-adic representations, conjugacy invariants (such as the trace and determinant) of the images of Frobenius elements can be computed. Note that the ℓ-adic Galois representations are maps to the automorphism group of the abelian group $A = (\mathbb{Z}_\ell)^2$. In this thesis, all representations will be continuous homomorphisms.

More generally, Grothendieck ([13]) and others have a well-developed theoretical framework of outer Galois representations. These are representations to the outer automorphism group of a non-abelian free pro-ℓ group F. There is less concrete information known about the sizes of the images and the images of Frobenius in this case.

The goal of this research is to begin to understand more tangibly Galois representations to automorphism groups of non-abelian groups. Non-abelian free pro-ℓ groups, however, are very far from abelian groups, and so, as a first step, we work with a metabelian quotient M. Metabelian groups are precisely those groups with trivial second derived subgroup.



Each of the representations in the picture depends on an elliptic curve E defined over $\mathbb{Q}$ and a prime ℓ. In the picture, the top arrow is a lift (using the Weierstrass tangential section) of the outer Galois representation studied by Grothendieck and others. The bottom arrow is the ℓ-adic Galois representation. The maps are continuous homomorphisms. The vertical maps are the natural ones and the diagram commutes. I will study the images of the middle representation.

1.2 Our results

Let E be an elliptic curve defined over $\mathbb{Q}$. I discuss the relevant background for elliptic curves and ℓ-adic representations in Chapter 2. In Chapter 3, I give the background on the outer Galois representations. I define the metabelian group and the metabelian representation in Chapter 4. I also state the Frattini lifting theorem in this chapter, which turns the question

of surjectivity of the metabelian representation into a question about the surjectivity of the representation to the Frattini quotient (a finite group). In Chapters 5, 6, and 7 I look for a candidate field extension of $\mathbb{Q}$ cut out by this Frattini quotient. In Chapter 5, I use cohomology theory to look for certain S_4-extensions of $\mathbb{Q}$. In Chapter 6, I use class field theory to identify a field extension of $\mathbb{Q}$ with the Frattini quotient as a Galois group. In Chapter 7, I use Galois theory and my results from other sections to say that there exists a field extension of $\mathbb{Q}$ having all the desired properties (Galois group isomorphic to the Frattini quotient, the right ramification, etc.) if E has surjective 2-adic representation (Theorem 7), or if E is semistable with full 2-torsion (i.e. the Galois group of the 2-division field of E over $\mathbb{Q}$ is isomorphic to S_3), or if E is semistable with good supersingular reduction at 2. In Chapter 7, I conclude the existence of a Galois representation to the Frattini quotient of the image of the metabelian representation for certain families of elliptic curves. I relate this to Conjecture $\star$ that I will make below. In Chapter 8, I study the Frattini quotient in the case $\ell = 3$. In Chapter 9, I study conjugacy invariants for the images of Frobenius elements in a finite quotient of the metabelian representation. Eventually, I hope to find conjugacy invariants for the image of the metabelian representation.

The metabelian representation associated to E is a larger representation than the ℓ-adic representation. By considering the abelianization of the metabelian group M, the metabelian representation can recover the ℓ-adic representation. For this reason, it is useful for figuring out the size of the image of the metabelian representation associated to E to know the size of the ℓ-adic representation associated to E. For $\ell \geq 5$, if the ℓ-adic representation is surjective mod ℓ, then it is surjective.

In this thesis, I will focus on the case that $\ell = 2$. A result of Serre gives that if the representation to $\mathbb{Z}/8\mathbb{Z}$ is surjective, then the 2-adic representation is surjective. This can be shown using the Frattini lifting theorem (4.6). The Dokchitsers give a characterization of when the 2-adic representation is surjective mod 2, but not mod 4 and mod 4, but not mod 8 (see Chapter 2). In Chapter 2, I prove that if E is semistable and the 2-adic representation is surjective mod 2, then the 2-adic representation is surjective.

In Chapter 4, I show that the image of the outer Galois representation in $\mathrm{Out}(M)$ is isomorphic to $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Therefore, the outer representation does not contain more information than the ℓ-adic representation. There is a representation to a subgroup Γ of $\mathrm{Aut}(M)$ given by Grothendieck's theory. The group Γ has $\mathrm{GL}_2(\mathbb{Z}_\ell)$ as a quotient, but is a larger group. As in the ℓ-adic representation case, the metabelian representation is unramified outside of ℓ, primes dividing the conductor of E, and ∞. This motivates the following definition:

Definition 1.1. *Given an elliptic curve defined over a field F_1, we will say that a field extension F_2/F_1 has **the right ramification** if the extension is unramified outside 2, primes dividing the conductor N, and ∞ where N is the conductor of the associated elliptic curve defined over F_1.*

In chapter 4, I show that $\Gamma/\Phi(\Gamma) \cong \mathrm{SmallGroup}(384, 20163)$ (in Magma notation). We will define finite groups Γ_n for each n in Chapter 4. (The group Γ_n has a quotient to $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.) Using Frattini lifting and the result about the Frattini quotient of Γ gives the corollary that if the representation to Γ_3 is surjective, then the representation to Γ is surjective (which is meant to be analogous to the result in the case of 2-adic Galois representations, that

if the mod 8 representation is surjective then the 2-adic representation is surjective).

Because of the Frattini lifting theorem, in order to show that the representation to Γ is surjective, I am interested in showing that the representation to $\Gamma/\Phi(\Gamma)$ is surjective. In particular, in order for this to be true, there must exist a Galois extension L_1 of $\mathbb{Q}$ with the right ramification, whose Galois group over $\mathbb{Q}$ is isomorphic to $\Gamma/\Phi(\Gamma)$ and with L_1 containing $\mathbb{Q}(E[2])$ (the 2-division field of E). I first try to determine if such extensions are possible by studying S_4-extensions containing the 2-division field.

The group $\Gamma/\Phi(\Gamma)$ has 3 S_4-quotients. Assume that we are in the case that the mod 2 representation is surjective, so $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ where $K = \mathbb{Q}(E[2])$. Also, assume that E does not have an isogeny of degree 3. In Chapter 5, I show that in this case, there are at least 3 S_4-extensions of $\mathbb{Q}$ containing K with the right ramification.

In Chapter 6, I assume that E is an elliptic curve with conductor a prime p congruent to 3 mod 8, assume $\#\mathrm{Cl}(K)$ is odd, and that E has supersingular reduction at 2. I use class field theory to consider the ray class group of $K = \mathbb{Q}(E[2])$ with modulus $\mathbf{m} = 2^3 \cdot N \cdot \mathcal{O}_K$ if E has negative discriminant and modulus $\mathbf{m} = 2^3 \cdot N \cdot \infty\mathcal{O}_K$ if E has positive discriminant. Let L denote the subfield of this ray class field obtained by taking the fixed field of the elementary abelian 2-part of the ray class group. I first show that $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right) = 7$. Then, I show that

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{SmallGroup}(768, 1090187).$$

Thus, there exists an extension of $\mathbb{Q}$ containing K with Galois group $\Gamma/\Phi(\Gamma)$ with the right ramification.

If the metabelian representation for E is surjective, then there is an extension of $\mathbb{Q}$ corresponding to the Frattini quotient of the full image of the metabelian representation. In Chapter 7, I give a condition C that encompasses the necessary traits of such an extension. I prove that there exists an extension satisfying C in the case that E is as in Chapter 6. I also prove that there exists an extension satisfying C in the case that E has surjective 2-adic representation. One corollary of this result is that there is an extension satisfying C in the case that E is a semistable with full 2-torsion. Another corollary is that there is an extension satisfying C in the case that E is semistable with good supersingular reduction at 2.

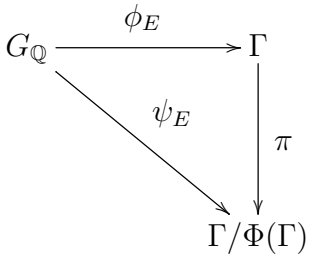
I get the following theorem as an immediate corollary of the fact that there exists an extension satisfying C in the case that E has surjective 2-adic representation.

Theorem 1.2. *Let E be an elliptic curve with $\rho_{E,2}$ surjective. This gives that there exists a map $\psi_E : G_{\mathbb{Q}} \to \Gamma/\Phi(\Gamma)$ satisfying condition C for E.*

Conjecture 1.3. *Conjecture $\star$*

We have seen that there is a map $\phi_E : G_{\mathbb{Q}} \to \Gamma$ (coming from Grothendieck's theory).

Consider the following diagram.



We conjecture that the composition $\pi \circ \phi_E$ is constructed by the previous theorem.

For example, in the special case that E is an elliptic curve with conductor a prime p congruent to 3 mod 8, $\#\mathrm{Cl}(K)$ is odd, and supersingular reduction at 2 (as in Chapter 6), $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{SmallGroup}(768, 1090187)$, which only has one $\Gamma/\Phi(\Gamma)$-quotient. Therefore, in this case, there is a unique ψ_E constructed. Therefore, the conjecture in this case is that this representation makes the above diagram commute. A corollary to the conjecture is that if ψ_E is surjective, then ϕ_E is surjective.

In Chapter 8, I define the metabelian representation in the case that $\ell = 3$. Using the Frattini lifting theorem, I get the result that if the representation to a finite group Γ_2 is surjective then the representation to Γ is surjective. (This result is analogous to the result for the 3-adic representation that says that if this representation is surjective mod 9, then the representation is surjective.)

In Chapter 9, we return to the case $\ell = 2$ to study conjugacy invariants of the images of Frobenius. In the case of ℓ-adic representations, natural conjugacy invariants to use are the trace and determinant of the image (a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$). We would like an invariant of Γ that generalizes trace and determinant. For now, we focus on the $H = \mathrm{SmallGroup}(768, 1090187)$-quotient of Γ and compute certain invariants for the images of the Frobenius elements in the field extensions of $\mathbb{Q}$ with Galois group H (see in Chapter 6). The type of invariant we use is a 7-tuple of elements in $(\mathbb{Z}/4\mathbb{Z})$ (see Chapter 9). For H itself, we get 17 different 7-tuples. Given the map m from elements of H to 7-tuples, we get a lemma that says if H_1 is a subgroup H with $|m(H_1)| = 17$, then $H_1 = H$.

In the case of ℓ-adic representations, we already know that the trace of the image Frob_p

is $a_p = p + 1 - \#E(\mathbb{F}_p) \bmod \ell^n$ and the determinant of the image is $p \bmod \ell^n$. Here we relate the elements of the 7-tuple to the number of points on a quartic elliptic curve that is a 2-covering of E. This enables us to compute the invariants of the images of Frobenius and hence the image itself for many elliptic curves.

Chapter 2

Elliptic Curves and ℓ-adic Representations

2.1 Elliptic curves background

An elliptic curve is a pair $(E, \mathbf{O})$, where E is a curve of genus 1 and $\mathbf{O} \in E$. The elliptic curve is defined over $\mathbb{Q}$, written $E/\mathbb{Q}$, if E is defined as a curve over $\mathbb{Q}$ and $\mathbf{O} \in E(\mathbb{Q})$.

Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exist functions $x, y \in \mathbb{Q}(E)$ such that the map $\phi : E \to \mathbb{P}^2$ with $\phi = [x, y, 1]$ gives an isomorphism of $E/\mathbb{Q}$ onto a curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

with coefficients a_1, a_2, a_3, a_4, $a_6 \in \mathbb{Q}$ such that $\phi(\mathbf{O}) = [0, 1, 0]$. We will define a quantity called the discriminant of the elliptic curve later in the section. The discriminant of this curve is required to be different from 0 because otherwise the respective curve has a singularity.

This equation is not uniquely determined with respect to the given elliptic curve E since any coordinate transformation $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ with $r, s, t \in \mathbb{Q}$ and $u \in \mathbb{Q}^*$ leads to another equation of the same shape. When applying this transformation, the discriminant is multiplied by the factor u^{12}.

By completing the square and then completing the cube on the right hand side, the equation can be written $y^2 = x^3 - 27c_4x - 54c_6$ or $y^2 = x^3 + Ax + B$, where $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ and $b_2 = a_1^2 + 4a + 2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Using these quantities, we can define the discriminant of the curve to be $\Delta = \frac{(c_4^3 - c_6^2)}{1728}$ or $-16(4A^3 + 27B^2)$.

Another important quantity attached to E is its j-invariant

$$j(E) = \frac{c_4^3}{\Delta}$$

2.1.1 Reduction of elliptic curves

Definition 2.1. *We say that E has **good reduction at** p if there is a Weierstrass equation for E with $a_i \in \mathbb{Z}_p$, that (when the coefficients are reduced modulo p) defines an elliptic curve over $\mathbb{F}_p$ (which happens if and only if the corresponding $\Delta \notin p\mathbb{Z}_p$).*

Definition 2.2. *Suppose p is a prime of bad reduction for E. The elliptic curve modulo p has a unique singular point. If that point is a node (respectively cusp), then we say E has multiplicative (respectively additive) reduction at p. A node (respectively cusp) means that two (respectively three) of the roots of the cubic are equal. Say E has **semistable reduction at** p if has good or multiplicative reduction at p. Call E semistable if its reduction at all primes is semistable.*

Multiplicative reduction occurs at p if and only if $v_p(c_4) = 0$, $v_p(\Delta) > 0$.

Let E be an elliptic curve defined over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + Ax + B$. An operation can be defined on the points on an elliptic curve which we can interpret as addition. Under this operation, the elliptic curve is endowed with the structure of an abelian group. The addition is performed subject to the rule that the sum of three points equals zero if and only if they lie on a line. We take the point at infinity as the **O** element. Let P, Q be two points different from the identity. The line through P and Q intersects the cubic in a third point $P * Q$. (If P=Q, take the line to be the line tangent to the curve at P.) Set $(x, y) * \mathbf{O} = (x, -y - a_1x - a_3)$, and define $P \oplus Q = (P * Q) * \mathbf{O}$. We have that $P \oplus \mathbf{O} = P$ and $[-1]P = P * \mathbf{O}$ is the additive inverse.

Let E be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(a) Let $P_0 = (x_0, y_0) \in E$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Now let

$$P_1 + P_2 = P_3 \text{ with } P_i = (x_i, y_i) \in E.$$

(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then

$$P_1 + P_2 = \mathbf{O}.$$

Otherwise, let $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$ if $x_1 \neq x_2$; $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$ if $x_1 = x_2$. (Then $y = \lambda x + v$ is the line through P_1 and P_2 or tangent to E if $P_1 = P_2$.

(c) $P_3 = P_1 + P_2$ is given by $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = -(\lambda + a_1)x_3 - v - a_3$.

(d) As special cases of (c), we have for $P_1 \neq \pm P_2$,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2;$$

and the duplication formula for $P = (x, y) \in E$

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 are the polynomials in the a_i's given earlier in the section.

2.1.2 Torsion points

Let E be an elliptic curve defined over a number field K. Fix a positive integer m. Define the m-division points of E:

$E[m] = \{P \in E(\overline{K}) : mP = \mathbf{O}\}$. Define the 2-division polynomial to be $\Lambda_2(x) = 4x^3 + b_2x^2 + 2b_4x + b_6 = (2y + a_1x + a_3)^2$. Note that this is the denominator of the duplication formula for a point given above.

Let K be an algebraic number field and let E be an elliptic curve defined over K, given by the equation $y^2 = x^3 + Ax + B$ with $\Delta = -16(4A^3 + 27B^2)$. We restrict ourselves to examine the decomposition behavior only for unramified prime ideals of $K(E[n])/K$. Doing this, we lose at most finitely many prime ideals. The Criterion of Néron, Ogg, Shafarevich determines exactly which prime ideals are excluded by this restriction.

Proposition 2.3 (Néron, Ogg, Shafarevich)**.** *Let E be an elliptic curve defined over K, and let $\mathfrak{p}$ be a prime ideal of K having norm q. Then the following assertions are equivalent:*

(a) E has good reduction modulo $\mathfrak{p}$

(b) $\mathfrak{p}$ *is unramified in* $K(E[n])/K$ *for all* $n \in \mathbb{N}$ *with* $(n, q) = 1$.

The Galois group of $K(E[n])/K$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For example, the possible Galois groups of $K(E[2])/K$ are given as follows:

Proposition 2.4. *Adelmann 5.4.2 ([1]*

$$\mathrm{Gal}(K(E[2])/K) \cong \begin{cases} \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), & if \Delta \notin K^{*2} \text{ and } E[2](K) = \{\mathbf{O}\}, \\ \mathbb{Z}/3\mathbb{Z}, & \Delta \in K^{*2} \text{ and } E[2](K) = \{\mathbf{O}\}, \\ \mathbb{Z}/2\mathbb{Z}, & \Delta \notin K^{*2} \text{ and } E[2](K) \neq \{\mathbf{O}\}, \\ \{1\}, & \Delta \in K^{*2} \text{ and } E[2](K) \neq \{\mathbf{O}\}. \end{cases}$$

Proof. $K(\sqrt{\Delta})$ is the subfield of $K(E[2]/K$ which is obtained by adjoining the discriminant of the defining polynomial $\Lambda_2(x) = (2y + a_1x + a_3)^2 = 4(x^3 + Ax + B)$. We have $[K(\sqrt{\Delta}) : K] = 2$ if and only if Δ is no square in K^*. Since the y-coordinate of any 2-torsion point equals $\mathbf{O}$, $\Lambda_2(x)$ is irreducible over $K[x]$ if and only if E has no K-rational 2-torsion point $\neq \mathbf{O}$. □

Proposition 2.5 ([1] 5.4.5)**.** *Decomposition Law for* 2*-Torsion Point Fields*

Assume that $\mathrm{Gal}(K(E[2])/K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. *Let* $\mathfrak{p}$ *be a prime ideal of* k *with norm* q *such that* $(q, 2) = 1$ *and* $v_p(\Delta) = 0$. *Let* $a_q = q + 1 - \#E(\mathbb{F}_q)$ *Then we have*

$$\mathfrak{f}_{K(E[2])/K}(\mathfrak{p}) = \begin{cases} 1, & if \left(\frac{\Delta}{p}\right)_2 = 1 \text{ and } a_q \equiv 0 \mod 2, \\ 3 & if \left(\frac{\Delta}{p}\right)_2 = 1 \text{ and } a_q \equiv 1 \mod 2, \\ 2, & if \left(\frac{\Delta}{p}\right)_2 = -1 \end{cases}$$

2.2 The ℓ-adic Galois representations

2.2.1 Definition

Let E be an elliptic curve defined over a number field K. For each positive integer m, we obtain a homomorphism

$$\overline{\rho}_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]).$$

The group $E[m]$ is isomorphic as an abstract abelian group to $(\mathbb{Z}/m\mathbb{Z})^2$. Combining the representations for the m-division points of E with $m = \ell^n$ for ℓ a prime and all positive integers n, we get that the absolute Galois group of K acts on the ℓ-adic Tate module

$$T_\ell(E) = \varprojlim_n E[\ell^n].$$

This yields a group representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E)).$$

After a choice of basis, $\mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. This is the ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ associated to E.

2.2.2 Sizes of images

This section recalls theorems about the sizes of the images of the ℓ-adic Tate representations.

Consider the case that E is an elliptic curve over $\mathbb{Q}$ without complex multiplication. In this case, a result of Serre asserts that (see [21], [22]) the image of $\rho_{E,\ell}$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ. Moreover, there is a bound ℓ_0 such that $\mathrm{im}\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell > \ell_0$. In other

words, the representation is surjective except for a finite set of primes.

Consider the representation

$$\overline{\rho}_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

A theorem of Serre says that for $\ell > 3$, the map $\rho_{E,\ell}$ is surjective if and only if $\overline{\rho}_{E,\ell}$ is surjective. Also, the map $\rho_{E,2}$ is surjective if and only if $\overline{\rho}_{E,8}$ is surjective and $\rho_{E,3}$ is surjective if and only if $\overline{\rho}_{E,9}$ is surjective. Noam Elkies wrote a paper that describes when the 3-adic representation associated to an elliptic curve is surjective mod 3 but not mod 9 [12]. Tim Dokchitser and Vladimir Dokchitser wrote a paper that describes when the 2-adic representation associated to an elliptic curve is surjective mod 2 but not mod 4, and mod 4 but not mod 8 [10].

2.2.3 Dokchitsers' result for $\ell = 2$

This section discusses a paper by Tim and Vladimir Dokchitser [10]. We have that if the representation $\overline{\rho}_{E,8}$ is surjective, then $\rho_{E,2}$ is surjective. The Dokchitsers studied the necessary and sufficient conditions for the representations $\overline{\rho}_{E,2}$ and $\overline{\rho}_{E,4}$ to be surjective.

Theorem 2.6 ([10] Dokchitser and Dokchitser)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ with discriminant $\Delta = -16(4A^3 + 27B^2)$ and j-invariant $j = -1728(4A)^3/\Delta$. Then*

- *(1) $\overline{\rho}_{E,2}$ is surjective if and only if $x^3 + Ax + B$ is irreducible and $\Delta \notin \mathbb{Q}^{\times 2}$.*
- *(2) $\overline{\rho}_{E,4}$ is surjective if and only if $\overline{\rho}_{E,2}$ is surjective, $\Delta \notin -1 \cdot \mathbb{Q}^{\times 2}$ and $j \neq -4t^3(t+8)$ for any $t \in \mathbb{Q}$.*
- *(3) $\overline{\rho}_{E,8}$ is surjective if and only if $\overline{\rho}_{E,4}$ is surjective and $\Delta \notin \pm 2 \cdot \mathbb{Q}^{\times 2}$*

We restate the proof here both because the arguments it contains will be useful and to clarify some points of the argument for our purposes.

Proof. We have already seen (1) in Proposition 2.5 and that $\mathbb{Q}(E[2])$ contains $\mathbb{Q}(\sqrt{\Delta})$.

Now recall that by the properties of the Weil pairing, $\mathbb{Q}(E[n]) \supset \mathbb{Q}(\zeta_n)$ and the corresponding map $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is simply the determinant. In particular,

$$\mathbb{Q}(E[4]) \supset \mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}) \text{ and } \mathbb{Q}(E[8]) \supset \mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2}).$$

Incidentally, as there are elliptic curves whose 2-torsion defines an S_3-extension of $\mathbb{Q}$ which is disjoint from $\mathbb{Q}(\zeta_8)$, e.g. $y^2 = x^3 - 2$, this shows that the canonical maps $(\mathrm{mod}2, \det)$

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to S_3 \times (\mathbb{Z}/4\mathbb{Z})^\times \text{ and } \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \to S_3 \times (\mathbb{Z}/8\mathbb{Z})^\times$$

are surjective (being already surjective on the subgroups $\mathrm{Im}\overline{\rho}_{E,4}$ and $\mathrm{Im}\overline{\rho}_{E,8}$). Hence, if $\overline{\rho}_{E,4}$ is surjective, then $\mathbb{Q}(E[2], \zeta_4)$ has degree 12 over $\mathbb{Q}$, so $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1})$ has degree 4 over $\mathbb{Q}$. Similarly, if $\overline{\rho}_{E,8}$ is surjective, then $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2})$ has degree 8 over $\mathbb{Q}$.

(3) If $\overline{\rho}_{E,8}$ is surjective, then so is $\overline{\rho}_{E,4}$, and as $\mathbb{Q}(\sqrt{\Delta}) \neq \mathbb{Q}(\sqrt{\pm 2})$, it follows that $\Delta \notin \pm 2 \cdot \mathbb{Q}^{\times 2}$. Conversely, if $\overline{\rho}_{E,4}$ is surjective and $\Delta \notin \pm 2 \cdot \mathbb{Q}^{\times 2}$, then $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-1}, \sqrt{2})$ is a $C_2 \times C_2 \times C_2$-extension of $\mathbb{Q}$. So $\mathrm{Im}\overline{\rho}_{E,8}$ surjects onto $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ (under the natural map that reduces each entry of the 2 by 2 matrix mod 4) and onto $(\mathbb{Z}/8\mathbb{Z})^\times$, and possesses a $C_2 \times C_2 \times C_2$-quotient. A computation shows that the only such subgroups of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ is the full group itself.

(2) We know that the splitting field of $x^4 - \Delta$ over $\mathbb{Q}$, $\mathbb{Q}_{\Delta,4}$, is contained in $\mathbb{Q}(E[4])$. Also, $[\mathbb{Q}_{\Delta,4} : \mathbb{Q}] = 8$; see [1, p.80-81]. Also, $\mathrm{Gal}(\mathbb{Q}_{\Delta,4}/\mathbb{Q})$ is equal to the dihedral group of order 8. Therefore, $\mathrm{Im}\overline{\rho}_{E,8}$ will have the dihedral group of order 8 as a quotient. After this point, the argument follows as in (3), except that in this case $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ does have a (unique up to conjugacy) proper subgroup which surjects onto the dihedral group of order 8, $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and onto $(\mathbb{Z}/4\mathbb{Z})^\times$, and has a $C_2 \times C_2$-quotient. This group has index 4, and is conjugate to $H_{24} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 3 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \rangle \cong C_3 \rtimes D_8$. The following lemma completes the proof. □

Lemma 2.7. *Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + Ax + B$ with $B \neq 0$. The following conditions are equivalent:*

1. $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ *is conjugate to a subgroup of H_{24}.*

2. *The polynomial*

$$f(x) = x^4 - 4Ax^3 + 6A^2x^2 + 4(7A^3 + 54B^2)x + (17A^4 + 108AB^2)$$

   has a rational root.

3. $j(E) = -4t^3(t+8)$ *for some $t \in \mathbb{Q}$.*

We omit the proof.

2.2.4 Elkies' result for $\ell = 3$

Elkies showed that there exist infinitely many $j \in \mathbb{Q}$ for which an elliptic curve of j-invariant j must have $\overline{\rho}_{E,3}$ surjective, but not $\overline{\rho}_{E,9}$ surjective. The simplest such examples are $j = 4374$, $j = 419904$ and $j = -44789760$. In general, j is the value of a rational function $f(x)$ of

degree 27 at all but finitely many $x \in \mathbb{P}^1(\mathbb{Q})$.

The group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is generated by

$$S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),$$

the images mod 3 of the standard generators of $\mathrm{SL}_2(\mathbb{Z})$. These generators of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ satisfy

$$S^2 = (ST)^3 = -I, T^3 = I$$

To lift $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ to a subgroup H of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, is enough to lift S, T to matrices mod 9 satisfying the same relations. A direct search finds 27 such lifts $\tilde{S}$, $\tilde{T}$, all equivalent under conjugation in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$.

2.2.5 Result for semistable elliptic curves and $\ell = 2$

The Dokchitsers' result characterizes in general, when the 2-adic representation is surjective mod 2, but not mod 4 and mod 4, but not mod 8. Here, I give a result that in the case of semistable elliptic curves, there are not the in-between cases.

Theorem 2.8. *Let E be a semistable elliptic curve over $\mathbb{Q}$. If $\overline{\rho}_{E,2}$ is surjective, then $\rho_{E,2}$ is surjective.*

Proof. Assume that $\overline{\rho}_{E,2}$ is surjective. We can write E in its Weierstrass form as $y^2 = x^3 + Ax + B$. The x-coordinates of the 2-torsion points of E are the roots of the polynomial $x^3 + Ax + B$. Since $\overline{\rho}_{E,2}$ is surjective, $x^3 + Ax + B$ is irreducible, so E has no rational

points of order 2. Then by a corollary of Brumer and Kramer ([6, Corollary 5.3(3)]), neither of $\pm\Delta$ is a perfect square.

There is a unique S_4-quotient of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. By a result of Adelmann ([1]), the S_4-extension of $\mathbb{Q}$ contained in $\mathbb{Q}(E[4])$ is given by $g = x^4 - 4\Delta x - 12A\Delta$. The unqiue S_3-extension inside of the splitting field of g is the splitting field of $f = x^3 + Ax + B$.

Lemma 2.9. *If $\overline{\rho}_{E,2}$ is surjective and $g = x^4 - 4\Delta x - 12A\Delta$ has a rational root, then E is not semistable.*

Proof. Assume $A = 0$. In this case, $g = x^4 - 4\Delta x$ does have a rational root $\beta = 0$. There exists p such that $v_p(\Delta) > 0$ and $v_p(A) > 0$. Therefore, E is not semistable in this case. Therefore, we can now assume that $A \neq 0$.

Let β be the rational root of g. We have $\beta^4 - 4\Delta\beta - 12A\Delta = 0$. At least two of the following three must be equal to the minimum of the three: $v_p(\beta^4)$, $v_p(4\Delta\beta)$, and $v_p(12A\Delta)$. Because neither of $\pm\Delta$ is a perfect square, there exists a prime p such that $v_p(\Delta)$ is odd.

Case 1: There is a prime p such that $v_p(\Delta)$ is odd with $p \neq 2, 3$. If $v_p(\beta) = 0$, then $v_p(\beta^4) = 0$, $v_p(12A\Delta) = v_p(A) + v_p(\Delta)$, and $v_p(4\Delta\beta) = v_p(\Delta) + v_p(\beta) = v_p(\Delta)$. But, $v_p(\Delta) > 0$, so neither of $v_p(A) + v_p(\Delta)$ nor $v_p(\Delta)$ is equal to 0. This contradicts the fact that at least 2 of the 3 valuations must be equal to the minimum of the 3 values. Therefore we can assume that $v_p(\beta) > 0$.

Case a: $v_p(\beta^4)$= $v_p(12A\Delta)$. Then $4v_p(\beta) = v_p(A)+v_p(\Delta)$. The left hand side is a nonzero multiple of 4. Also $v_p(\Delta)$ is odd. This implies that $v_p(A)$ is odd. Therefore, $v_p(A) > 0$.

Case b: $v_p(4\Delta\beta)$= $v_p(12A\Delta)$. Then $v_p(\Delta) + v_p(\beta) = v_p(A) + v_p(\Delta)$, so $v_p(\beta) = v_p(A)$. Since $v_p(\beta) > 0$, $v_p(A) > 0$.

Case c: $v_p(\beta^4)$= $v_p(4\Delta\beta)$. Then $4v_p(\beta) = v_p(\Delta) + v_p(\beta)$. If all 3 of the valuations are equal, we can use case a or b to show that $v_p(A) > 0$. Therefore, assume that $4v_p(\beta) = v_p(\Delta)+v_p(\beta) < v_p(12A\Delta) = v_p(A)+v_p(\Delta)$. Since this gives $v_p(\Delta)+v_p(\beta) < v_p(A)+v_p(\Delta)$, $v_p(\beta) < v_p(A)$, we get that $v_p(A) > 0$.

In all of the subcases, we have shown that $v_p(A) > 0$. Therefore, E is not semistable at p.

Case 2: $v_2(\Delta)$ is odd.

If $v_2(\beta) = 0$, then $v_2(\beta^4) = 0$, $v_2(12A\Delta) = 2 + v_2(A) + v_2(\Delta)$, and $v_2(4\Delta\beta) = 2 + v_2(\Delta) + v_2(\beta) = 2 + v_2(\Delta)$. Neither of $2 + v_2(A) + v_2(\Delta)$ nor $2 + v_2(\Delta)$ is equal to 0. This contradicts the fact that at least 2 of the 3 valuations must be equal to the minimum of the 3 values. Therefore we can assume that $v_2(\beta) > 0$.

Case a: $v_2(\beta^4)$= $v_2(12A\Delta)$. Then $4v_2(\beta) = 2 + v_2(A) + v_2(\Delta)$. The left hand side is a nonzero multiple of 4. Also $v_2(\Delta)$ is odd. This implies that $v_2(A)$ is odd. Therefore, $v_2(A) > 0$.

Case b: $v_2(4\Delta\beta)$= $v_2(12A\Delta)$. Then $2 + v_2(\Delta) + v_2(\beta) = 2 + v_2(A) + v_2(\Delta)$, so $v_2(\beta) = v_2(A)$. Since $v_2(\beta) > 0$, $v_2(A) > 0$.

Case c: $v_2(\beta^4)$= $v_2(4\Delta\beta)$. Then $4v_2(\beta) = 2 + v_2(\Delta) + v_2(\beta)$. If all 3 of the valuations are equal, we can use case a or b to show that $v_2(A) > 0$. Therefore, assume that $4v_2(\beta) = 2 + v_2(\Delta) + v_2(\beta) < v_2(12A\Delta) = 2 + v_2(A) + v_2(\Delta)$. Since this gives

$2 + v_2(\Delta) + v_2(\beta) < 2 + v_2(A) + v_2(\Delta)$, $v_2(\beta) < v_2(A)$, we get that $v_2(A) > 0$.

Case 3: $v_3(\Delta)$ is odd and $v_p(\Delta)$ is even for all other primes p dividing Δ. Then $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{3})$. If $v_2(A) > 0$, then E is not semistable. Therefore, we can assume in this case that E has good or multiplicative reduction at 2. Using Brumer and Kramer's Corollary 5.3(1) ([6]), if E has ordinary good reduction or multiplicative reduction modulo 2, then three divides the order of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ modulo the subgroup generated by the classes of ideals lying above 2. The order of the ideal class group of both $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ is 1.

□

Since g is irreducible, its Galois group is a transitive subgroup of S_4. Since $\mathbb{Q}(E[2])$ is contained in the splitting field of g, the Galois group has S_3 as a quotient. Therefore, the Galois group of g is all of S_4. Since Δ is not a square, $x^4 - \Delta$ is irreducible. The only subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ that surjects onto S_4 and surjects onto the dihedral group of order 8 is the whole group. Therefore, the image of $\overline{\rho}_{E,4}$ is all of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$.

We will now show that $\Delta \notin \pm 2\mathbb{Q}^{\times 2}$ by contradiction. Assume that Δ is equal to ± 2 times a square. Then, $v_2(\Delta)$ is odd. Proceeding as in case 2 in the lemma above, this implies that $v_2(A) > 0$. This contradicts the fact that E is semistable. Therefore, $\Delta \notin \pm 2\mathbb{Q}^{\times}$. Since $\overline{\rho}_{E,4}$ is surjective and $\Delta \notin \pm 2 \cdot \mathbb{Q}^{\times 2}$, we have that $\overline{\rho}_{E,8}$ is surjective. Then by the result of Serre, we get that $\rho_{E,2}$ is surjective. □

In the theorem above, I proved that if the representation to $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ is surjective, then the representation to $\mathrm{GL}_2(\mathbb{Z}_2)$ is surjective.

One question is whether a similar theorem holds for $\ell = 3$. Elkies gives a modular curve $\mathcal{X}_9$ of genus 0 parameterizing elliptic curves for which $\overline{\rho}_{E,3}$ (the representation to $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$) is surjective, but $\rho_{E,3}$ is not surjective. He gives an explicit rational function $f \in \mathbb{Q}(x)$ of degree 27 realizing the modular cover $\mathcal{X}_9 \to X(1)$. Elkies gives a list of examples and then explains that the list contains all nonzero integral j-invariants of elliptic curves parameterized by $\mathcal{X}_9$. His list has 7 elliptic curves, all of which have conductors that are not squarefree.

2.3 Results of Brumer and Kramer

Let E be an elliptic curve over $\mathbb{Q}$. Let $K = \mathbb{Q}(E[2])$. In order for the representation to Γ to be surjective, we need the Galos representation to $\Gamma/\Phi(\Gamma)$ to be surjective. We will look for candidate field extensions (i.e. extensions of $\mathbb{Q}$ containing K with Galois group isomorphic to $\Gamma/\Phi(\Gamma)$ and with the right ramification).

We introduce the work of Brumer and Kramer because we will use these results when we study the class field theory of K (see Chapter 6).

Proposition 2.10 ([6] Brumer-Kramer, 5.2)**.** *(1) If E has supersingular reduction at 2 then K is a cyclic cubic extension of $\mathbb{Q}(\sqrt{\Delta})$ unramified outside 2 and totally ramified at 2. Moreover, 2 remains prime in $\mathbb{Q}(\sqrt{\Delta})$.*

(2) If the formal group of E over $\mathbb{Q}_2$ has height one, then either E has a rational point of order two or else $\mathbb{Q}(E[2])$ is an unramified cyclic cubic extension of $\mathbb{Q}(\sqrt{\Delta})$ in which the primes dividing 2Δ split completely.

Proof. This is an immediate consequence of the ramification data given in a Proposition of Serre [22]pp. 273-277. Note that $\mathbb{Q}(\sqrt{\Delta})$ is the subfield of K cut out by the alternating group

A_3. □

Corollary 2.11. *Suppose that the curve E has no rational points of order two.*

(1) If E has ordinary good reduction or multiplicative reduction modulo 2, then three divides the order of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ modulo the subgroup generated by the classes of ideals lying above 2.

(2) If E is supersingular modulo 2, then: (a) $\Delta \equiv 5 \mod 8$ and (b) for every element in α in $\mathbb{Q}(\sqrt{\Delta})$ for which the ideal (α) is the cube of an ideal prime to 2, we have $\alpha \equiv 1 \mod 2$.

(3) Neither of $\pm\Delta$ is a perfect square.

Proof. (1) follows from Proposition (2) upon using the class field theoretic description of the extension $\mathbb{Q}(E[2])$ over $\mathbb{Q}(\sqrt{\Delta})$.

(2) Since $\mathbb{Q}_2(\sqrt{\Delta})$ is an unramified quadratic extension of $\mathbb{Q}_2$, we have $\Delta \equiv 5 \mod 8$. The assertion about α gives a necessary and sufficient condtion for the existence of a cyclic cubic extension of $K = \mathbb{Q}(\Delta)$ having the ramification properties in the Proposition of Serre ([22]pp. 273-277).

(3) is now clear using (1) and (2). □

Chapter 3

Grothendieck's Etale Fundamental Group

3.1 Outer Galois representations

In this section, we will describe in more detail a method of Grothendieck that given an elliptic curve defined over $\mathbb{Q}$ produces a representation of $G_{\mathbb{Q}}$ to the automorphism group of a free pro-ℓ group, F, on 2 generators. There is a natural map from $\mathrm{Aut}(F)$ to $\mathrm{Aut}((\mathbb{Z}_\ell)^2)$. The induced action on the abelianization of F is none other than the ℓ-adic representation associated to the elliptic curve.

Let E be an elliptic curve defined over $\mathbb{Q}$ with Identity $O \in E(\mathbb{Q})$. Denote by E_O or $E\backslash\{O\}$ the elliptic curve minus the identity. There is an exact sequence of arithmetic fundamental groups

$$1 \longrightarrow \pi_1(\overline{E}_O) \longrightarrow \pi_1(E_O) \xrightarrow{p_{E_O/\mathbb{Q}}} G_{\mathbb{Q}} \longrightarrow 1$$

where $\overline{E}_O = E_O \otimes \overline{\mathbb{Q}}$

The maps in the above sequence are explained in [18]. A brief summary of the definition of $p_{E_O/\mathbb{Q}}$ is given as follows:

- Given X an algebraic variety defined over $\mathbb{Q}$, we obtain the natural morphism $X \to \mathrm{Spec}(\mathbb{Q})$.

- Given a morphism of schemes $f : X_1 \to X_2$ and a geometric point $\overline{x}_1$ on X_1, then one obtains a homomorphism $\pi_1(X_1, \overline{x}_1) \to \pi_1(X_2, \overline{x}_2)$. (If one changes the base-point $\overline{x}_1$, the resulting homomorphism of fundamental groups is equivalent to the previous one and so omitted.)

- The fundamental group $\pi_1(\mathrm{Spec}(\mathbb{Q})$ may be identified with the absolute Galois group $G_{\mathbb{Q}}$.

We denote by $\pi_1(\overline{E}_O)(\ell)$ the maximal pro-ℓ quotient of $\pi_1(\overline{E}_O)$ and define the quotient group $\pi_1^{(\ell)}(E_O)$ of $\pi_1(E_O)$ to fit in the following exact sequence naturally

$$1 \longrightarrow \pi_1(\overline{E}_O)(\ell) \longrightarrow \pi_1^{(\ell)}(E_O) \xrightarrow{p_{E_O/\mathbb{Q}}} G_{\mathbb{Q}} \longrightarrow 1 \ .$$

From this we obtain the outer Galois representation

$$\phi_{E_O} : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}\left(\pi_1(\overline{E}_O)(\ell)\right) \ .$$

Here for each $\sigma \in G_{\mathbb{Q}}$, $\phi_{E_O}(\sigma)$ is the class of automorphisms of $\pi_1(\overline{E}_O)(\ell)$ induced by conjugation by elements of $p^{-1}_{E_O/\mathbb{Q}}(\sigma)$ so is well-defined up to inner automorphisms.

It is well-known that the Galois image $\phi_{E_O}(G_{\mathbb{Q}})$ is contained in the pro-ℓ mapping class group which is defined as the subgroup of all the braid-like outer automorphisms of $\pi_1(\overline{E}_O)(\ell)$. (See [16, Section 1.9].)

3.1.1 Weierstrass tangential section

We are able to lift ϕ_{E_O} to a representation to $\mathrm{Aut}\left(\pi_1(\overline{E}_O)(\ell)\right)$. There is a section $s : G_{\mathbb{Q}} \to \pi_1^{(\ell)}(E_O)$ called the Weierstrass tangential section. By conjugation through s, there arises a

monodromy representation

$$\phi_{E_O} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\left(\pi_1(\overline{E}_O)(\ell)\right) .$$

(See [17, Sections 2.4, 2.5]).

By the comparision theorem [13], the geometric fundamental group can be identified with the profinite completion of the topological fundamental group of $E_O(\mathbb{C})$. From this, we get that $\pi_1(\overline{E}_O)(\ell)$ may be identified with a free pro-ℓ group presented as

$$\Pi_{1,1} = \langle x_1, x_2, z | [x_1, x_2]z = 1 \rangle \tag{3.1}$$

so that z generates an inertia subgroup over O.

3.1.2 The Abelian quotient of the outer Galois representation

The monodromy representation on the maximal abelian quotient of $\Pi_{1,1}$ corresponds to the action on the first étale homology group of the elliptic curve. More concretely, the abelianization is $H_1(E, \mathbb{Z}_\ell) = (\mathbb{Z}_\ell)^2$ which is canonically identified with the ℓ-adic Tate module $\varprojlim_n E[\ell^n]$ as a $G_{\mathbb{Q}}$-module. Reduction of ϕ_{E_O} to this quotient gives the representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}\left((\mathbb{Z}_\ell)^2\right) \cong \mathbf{GL}_2(\mathbb{Z}_\ell).$$

3.2 Tsunogai's work

One relevant work in the literature is that of Tsunogai, who studied Ψ^*, a subgroup of the automorphism group of the free metabelian group F/F''([24]). He showed the conjugacy class in Ψ^* of some element of order 2 is not determined by the action induced on the abelian quotient

of F in the case $\ell = 2$.

Tsunogai defines $\Psi^* = \{\sigma \in \mathrm{Aut}(F/F'')|\sigma(z) = z^\alpha \text{ for some } \alpha \in \mathbb{Z}_\ell^\times\}$. We will also need the definition of $\Psi^*(1) = \{\sigma \in \Psi^*|\sigma(x) = fx, \sigma(y) = gy \quad (f, g \in F'/F'')\}$. These groups fit into the following exact sequence:

$$1 \longrightarrow \Psi^*(1) \longrightarrow \Psi^* \xrightarrow{\lambda} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow 1 \ .$$

Tsunogai studies the elements in the subset

$$S = \left\{ \sigma \in \Psi^* | \lambda(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma^2 = 1 \right\}$$

where λ is as above. Tsunogai was interested in understanding if there is a unique conjugacy class of elements of order 2 whose image under the ℓ-adic representation matches that of complex conjugation.

Tsunogai gets the following answer to the question about conjugacy above complex conjugation:

Theorem 3.1 (Tsunogai)**.** *1. If $\ell \neq 2$, any two elements of S are conjugate by an element in $\Psi^*(1)$*

2. If $\ell = 2$, there exist infinitely many elements of S which are mutually nonconjugate in Ψ^*

Chapter 4

Group Theory

This chapter defines a sequence of metabelian groups M_n for each ℓ and take the inverse limit of these groups. This is analogous to taking the groups $(\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})$ and taking the inverse limit to get $(\mathbb{Z}_\ell)^2$ in the abelian case. Then, a subgroup Γ of the automorphism group of the metabelian group (in the case $\ell = 2$) will be defined. In this section, we will also give a Frattini lifting theorem that will help prove results about surjectivity of the representation.

Let G be a profinite group. The Frattini subgroup of G is

$$\Phi(G) = \cap\{M | M \text{ is a maximal proper open subgroup of } G\}.$$

Consider F, a free pro-ℓ group on 2 generators (say, a, b). Let the maps $\pi_n : F \to (\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})$ be the canonical quotient maps. Let K_n be the kernel of π_n. Then define $M_n = F/\Phi(K_n)$.

Let $M_{2,\ell}(\ell)$ be the inverse limit of the groups M_n. This group is the free metabelian pro-ℓ group of rank 2 with commutator subgroup abelian of exponent ℓ. Roman′kov ([20]) considered the automorphism group of this group and showed that it is topologically finitely generated.

We define the quotient maps by the inner automorphism groups:

$$\mathrm{Aut}(M_{2,\ell}(\ell)) \xrightarrow{\quad q \quad} \mathrm{Out}(M_{2,\ell}(\ell)) \ ,$$

$$\mathrm{Aut}(M_n) \xrightarrow{\quad q_n \quad} \mathrm{Out}(M_n) \ .$$

4.1 Fox derivatives

This section will give an introduction to pro-ℓ Fox calculus. For a survey of this topic, see [15] and for a fuller treatment in the pro-ℓ case, see [14]. I will use this theory (for example in theorem 4.3 about the image of the outer Galois representation).

Let F be a free group of rank r. Let $F_1 \subset F$ be a normal subgroup of finite index. Then F_1 is again free with rank r_1, where $r_1 - 1 = (r-1)[F : F_1]$. Let N run over all normal subgroups of F contained in F_1 such that F_1/N is a finite ℓ-group and form the projective limit $\mathfrak{F} = \varprojlim(F/N)$. The profinite group $\mathfrak{F}$ constructed in this way will be called a free almost pro-ℓ group of rank r.

Theorem 4.1 (Ihara, see [14], Theorem 2.1, p.440-441)**.** *Let $\mathfrak{F}$ be a free almost pro-ℓ group of rank r generated by $x_1, \ldots x_r$. Let $\mathfrak{B} = \mathbb{Z}_\ell[[\mathfrak{F}]]$ be its completed group algebra over $\mathbb{Z}_\ell$. Let $\mathfrak{t} : \mathfrak{B} \to \mathbb{Z}_\ell$ be the trivializer (or augmentation homomorphism) defined by $t(\sum_{v\in F} a_v v) = \sum_{v\in F} a_v$. Then every element θ of $\mathfrak{B}$ can be expressed uniquely in the form*

$$\theta = \mathfrak{t}(\theta)\cdot 1 + \sum_{j=1}^{r} \theta_j(x_j - 1) \qquad (\theta_1, \ldots, \theta_r \in \mathfrak{B}),$$

where $1 = 1_{\mathfrak{F}}$ *is the identity element of* $\mathfrak{F}$*. Moreover, for each* j*,* $\theta \to \theta_j$ *gives a continuous* $\mathbb{Z}_\ell$*-linear map of* $\mathfrak{B}$ *onto itself.*

Proof. See [14]. □

Definition 4.2. $\frac{\partial \theta}{\partial x_j} = \theta_j \qquad (1 \leq j \leq r)$

The following are the basic rules for free differential calculus $\frac{\partial}{\partial x_j}$, each of which is an immediate consequence of the definition of $\frac{\partial}{\partial x_j}$ (see [14, p.440]):

- $\frac{\partial}{\partial x_j} : \mathfrak{B} \to \mathfrak{B}$ is continuous $(1 \leq j \leq r)$;
- $\frac{\partial x_i}{\partial x_j} = \delta_{ij}$ (Kronecker delta) $(1 \leq i, j \leq r)$;
- $\frac{\partial vw}{\partial x_j} = \frac{\partial v}{\partial x_j}\mathfrak{t}(w) + v\frac{\partial w}{\partial x_j} (v, w \in \mathfrak{B})$;
- $\frac{\partial {x_i}^{-1}}{\partial x_j} = -\delta_{ij} x_j^{-1} (f \in \mathfrak{F})$;
- if $\mathfrak{F}_1$ is any open subgroup of $\mathfrak{F}$, with free (almost pro-ℓ) generators $y_1, \cdots, y_{r_1}$, then

$$\frac{\partial \theta}{\partial x_j} = \sum_{i=1}^{r_1} \frac{\partial \theta}{\partial y_i}\frac{\partial y_i}{\partial x_j} \qquad (\theta \in \mathbb{Z}_\ell[[\mathfrak{F}_1]]),$$

  where we regard $\mathbb{Z}_\ell[[\mathfrak{F}_1]]$ as embedded in $\mathbb{Z}_\ell[[\mathfrak{F}]]$.

Now consider the case that F is a free pro-ℓ group on 2 generators. Given a map $\alpha \in \mathrm{Aut}(F)$, the Magnus representation is defined as follows:

$$J(\alpha) = \begin{pmatrix} \left(\frac{\partial \alpha(a_1)}{\partial a_1}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_1}\right)^{ab} \\ \left(\frac{\partial \alpha(a_1)}{\partial a_2}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_2}\right)^{ab} \end{pmatrix}$$

where ^{ab} means take the abelianization.

Since this matrix resembles a Jacobian, I will denote the matrix by $J(\phi)$ for an automorphism ϕ. Restricting to this representation to $\mathrm{IA}(M_{2,\ell}(\ell))$ gives a map from $\mathrm{IA}(M_{2,\ell}(\ell)) \longrightarrow \mathrm{GL}(2, \mathbb{Z}_\ell[[H]])$ where $H := H_1(F, \mathbb{Z}_\ell) \simeq (\mathbb{Z}_\ell)^2$.

4.2 Group theory results

We will use the notation G' to denote the derived subgroup of a group G. There is a structure of $M_{2,\ell}(\ell)'$ as a continuous $\mathcal{B}$-module such that

$$x - 1 \cdot c = [x, c], \qquad y - 1 \cdot c = [y, c], \qquad \alpha \cdot c = c^\alpha,$$

for any $c \in M_{2,\ell}(\ell)'$ and $\alpha \in \mathbb{Z}_\ell$. Then $M_{2,\ell}(\ell)'$ is a free $\mathcal{B}$-module of rank 1 generated by z, i.e.

$$\mathcal{B} \simeq M_{2,\ell}(\ell)'$$

$$F \leftrightarrow F \cdot z.$$

We will treat elements of $M_{2,\ell}(\ell)'$ in terms of $\mathcal{B}$ by this isomorphism (we will call F the exponent of z).

Theorem 4.3. *Let E be an elliptic curve defined over $\mathbb{Q}$. The image of the outer Galois representation in $\mathrm{Out}(M_{2,\ell}(\ell))$ is isomorphic to the image of the ℓ-adic representation associated to E.*

Proof. There is a map

$$\pi : \mathrm{Aut}(M_{2,\ell}(\ell)) \to \mathrm{Aut}(M_{2,\ell}(\ell)/M_{2,\ell}(\ell)') = \mathrm{GL}_2(\mathbb{Z}_\ell).$$

We will call the kernel of this map the IA-automorphism group and denote it by $\mathrm{IA}(M_{2,\ell}(\ell))$.

To prove the theorem, we need to show that every IA-automorphism is an inner automorphism. The proof is a combination of the proofs in ([2], p.99, Theorem 2) and ([20], Lemma 4.5). In order to do this, we will use Fox derivatives.

The commutator of two elements x,y of a group will be denoted $[x, y]$ and x^y will denote the conjugate of x by y, that is, $x^y = yxy^{-1}$.

Let $\phi \in \mathrm{IA}M_{2,\ell}(\ell) \cap \mathrm{im}G_{\mathbb{Q}}$.

Since $\phi \in \mathrm{IA}(M_{2,\ell}(\ell))$, Roman′kov shows that ϕ is in the form

$$\phi : \begin{array}{ll} a & \mapsto [b,a]^A a \\ b & \mapsto [b,a]^B b \end{array}$$

where $A, B \in \mathfrak{B}$. Then, the Magnus representation is the following:

$$J(\phi) = \begin{pmatrix} 1 + A(b-1) & (1-a)A \\ B(b-1) & 1 + B(1-a) \end{pmatrix}$$

Let $t_1 = a - 1$ and $t_2 = b - 1$. Then, $\det J(\phi) = 1 + A(b-1) + B(1-a) = 1 + At_2 - Bt_1$.

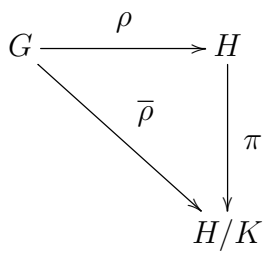
Since $\phi \in \mathrm{im}G_{\mathbb{Q}}$, by Equation 3.1, ϕ fixes the conjugacy class of z. In order for $z^{1+At_2-Bt_1}$ to be conjugate to z in $M_{2,\ell}(\ell)$, we must have that $1 + At_2 - Bt_1 = 1$. Since $\det J(\phi) = 1$, there exists an element C such that $A = Ct_1$ and $B = Ct_2$. As in ([20]), we get that, in this case, ϕ is the inner automorphism corresponding to $(a, b)^C$. □

The above theorem shows that there is no more information in the outer Galois representation than there is in the ℓ-adic representation. Instead, we will consider a representation to a subgroup of the automorphism group of $M_{2,\ell}(\ell)$ (and will focus on the case $\ell = 2$). Since $\mathrm{Out}(M_n) = \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$, we will consider the inverse image of $G_n = \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ under q_n.

Definition 4.4. *Define* $\Gamma_n = q_n^{-1}(\mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z}))$.

Definition 4.5. *Define* $\Gamma = \varprojlim_n \Gamma_n$.

Theorem 4.6. *(A Frattini Lifting Theorem) Let H, K be profinite groups and let ρ, $\overline{\rho}$ be continuous homomorphisms as below. Let $\pi : H \to H/K$ be the canonical quotient map. Suppose that π makes the following diagram commutative:*



Also, suppose that $\overline{\rho}$ is surjective and that $K \subseteq \Phi(H)$. Then, ρ is surjective.

Proof. Suppose that $\overline{\rho}$ is surjective. Suppose for the sake of contradiction that ρ is not surjective, so there is an open maximal subgroup M of H such that $\rho(G) \subseteq M$ then $H/K = \overline{\rho}(G) = \pi\rho(G) \subseteq \pi(M) = MK/K$, and so since $H/K \subseteq MK/K$, $H \subseteq MK$. Since $K \subseteq \Phi(H)$ and the Frattini subgroup is the intersection of all open maximal subgroups of H, then $K \subseteq M$, thus $H = MK \subseteq M$. This contradicts the assumption that M is a maximal subgroup of H. Therefore, ρ is surjective. □

For example, let $H = \mathrm{GL}_2(\mathbb{Z}_2)$. Then $H/\Phi(H) \cong \mathrm{SmallGroup}(96, 226)$ (in Magma notation). The group $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ has $H/\Phi(H)$ as a quotient. Therefore, using the Frattini lifting theorem, we recover the result that if the homomorphism $\overline{\rho}_{E,8}$ is surjective, then $\rho_{E,2}$ is surjective.

Theorem 4.7. *Let $H = \Gamma$. Then $H/\Phi(H) \cong \mathrm{SmallGroup}(384, 20163)$ (in Magma notation).*

Proof. Let $G = GL(2, \mathbb{Z}_2)$ and let $I = \mathrm{Inn}(M_{2,\ell}(\ell))$. Using Theorem 4.3, we get that the following sequence is exact:

$$1 \to I \to \Gamma \to G \to 1.$$

Let L be the kernel from Γ to Γ_1. Let K be the kernel from G to G_1. The Nine Lemma holds in the category of groups. It gives that since the columns of the following diagram are exact and the bottom two rows are exact that the top row is exact:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & L & \longrightarrow & K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & \Gamma & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & \Gamma_1 & \xrightarrow{\sim} & G_1 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

In the diagram, both Γ_1 and G_1 are isomorphic to S_3, the symmetric group on 3 letters. Since the top row is an exact sequence of pro-2 groups, it follows that

$$1 \longrightarrow I/(I \cap \Phi(L)) \longrightarrow L/\Phi(L) \longrightarrow K/\Phi(K) \longrightarrow 1$$

is an exact sequence.

Consider $t = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $u = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $v = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and $b = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then the following relations hold: $t^2, u^2, (tu)^4, (vu)^2, (tutv)^2,$
$(vtu)^3, (b,u), (b,(tu)^2), b^{-1}(tu)^{-1}b^{-1}(tu)^{-1}b(tu)b(tu), v^{-1}b^{-1}(tu)^{-1}b^{-1}v^{-1}b(tu)bv^{-1}(tu),$ $vbv^{-1}b^{-1}v^2$. Using this, we can compute that $K/\Phi(K)$ is an elementary abelian 2-group of rank 5.

In general, given a group G_0, $\mathrm{Inn}(G_0) \cong G_0/Z(G_0)$ where $Z(G_0)$ denotes the center of G_0. In this case, since $M_{2,\ell}(\ell)$ is generated by 2 elements, $M_{2,\ell}(\ell)/Z(M_{2,\ell}(\ell))$, and therefore, $\mathrm{Inn}(M_{2,\ell}(\ell))$ is generated by 2 elements. Therefore, $I/(I \cap \Phi(\Gamma)$ is an elementary abelian 2-group of rank 2 and therefore $L/\Phi(L)$ is an elementary abelian 2-group of rank 7. We get the following diagram:

$$\begin{array}{c} \Gamma \\ {\scriptstyle 6}\big| \\ L \\ {\scriptstyle 2^7}\big| \\ \Phi(L) \end{array}$$

Since $L \trianglelefteq \Gamma$, $\Phi(L) \leq \Phi(\Gamma)$ and therefore the order of $\Gamma/\Phi(\Gamma)$ divides 768.

Claim 4.8. $\Gamma/\Phi(L)$ *surjects onto* $\Gamma_3/\Phi(L_3)$

Proof. Let $N = \ker(\Gamma \to \Gamma_3)$. Then $N \leq L$ and $L_3 = L/N$. Consider the following diagram:

$$\Gamma \xrightarrow{q_1} \Gamma/N \xrightarrow{q_2} \frac{\Gamma/N}{\Phi(L/N)}, \quad \Gamma \xrightarrow{\phi} \frac{\Gamma/N}{\Phi(L/N)}$$

We need to show that $\ker(\phi) \geq \Phi(L)$. Under q_1, $\Phi(L)$ maps to $\Phi(L)N/N$. But, we have that $\Phi(L/N) \geq \Phi(L)N/N$. Therefore, this maps to the identity under q_2 and therefore, $\Phi(L) \leq \ker(\phi)$, so $\Gamma/\Phi(L)$ surjects onto $\Gamma_3/\Phi(L_3)$. □

We have that $\Gamma_3/\Phi(L_3) \cong \mathrm{SmallGroup}(768, 1090187)$ by a finite computation. Since $\Gamma/\Phi(L)$ is a group of order 768 surjecting onto this group, $\Gamma/\Phi(L) \cong \mathrm{SmallGroup}(768, 1090187)$. Taking the Frattini quotient of this group, we get that $\Gamma/\Phi(\Gamma) \cong \mathrm{SmallGroup}(384, 20163)$.

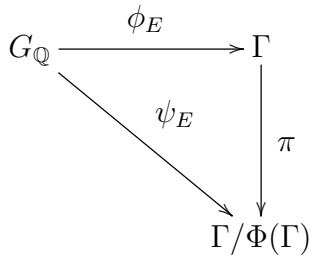
□

Corollary 4.9. *By using the Frattini lifting theorem and the above theorem, we get the result that if the representation to* Γ_3 *is surjective, then the representation to* Γ *is surjective.*

Chapter 5

Number Theory and Cohomology of Groups

In order to find a surjective representation ψ_E that makes the following diagram commute:



we need an extension of $\mathbb{Q}$ with Galois group isomorphic to $\Gamma/\Phi(\Gamma)$ with the right ramification. If there were such an extension, then since $\Gamma/\Phi(\Gamma)$ has 3 S_4-quotients, there must exist 3 S_4-extensions of $\mathbb{Q}$ with the right ramification. In this chapter, we consider if this is possible.

5.1 Work of Bayer and Frey

Proposition 5.1 ([3] Proposition 1.1)**.** *Let* $K = \mathbb{Q}(E[2])$*. There is a one-to-one correspondence between fields* $L \supset K$ *with* $\mathrm{Gal}(L/K) = S_4$ *and elements* $\phi \in H^1(G_{\mathbb{Q}}, E[2])\backslash\{0\}$*.*

Proof. By using the inf-res sequence one gets at once that $H^1(G_{\mathbb{Q}}, E[2]) =$

$\mathrm{Hom}_{\mathrm{Gal}(L/\mathbb{Q})}(\mathrm{Gal}(\overline{L}/L), E[2])$. Now take $\phi \in H^1(G_\mathbb{Q}, E[2])\backslash\{0\}$ and denote by $\tilde{\phi}$ the corresponding homomorphism. Let L_ϕ be the fixed field of its kernel. Then L_ϕ is a Galois extension over $\mathbb{Q}$ and $\mathrm{Gal}(L_\phi/K)$ is generated by two elements ϵ_1 and ϵ_2 of order dividing 2. Let σ be an element of order 3 in $\mathrm{Gal}(K/\mathbb{Q})$. Since for all $P \in E[2]\backslash\{0\}$ the element $\sigma P - P$ is nontrivial we get: If $\tilde{\phi}(\epsilon_1) \neq 0$ then $\sigma\epsilon_i\sigma^{-1} \neq \epsilon_i$ and hence $[L_\phi : K] = 4$. We conclude that $\mathrm{Gal}(L_\phi/\mathbb{Q}) = S_4$ and that ϕ is determined by $\tilde{\phi}(\epsilon_1)$. Now let τ be an element of order 2 in S_3 with $\tau\epsilon_1\tau = \epsilon_1$. Then $\tilde{\phi}(\epsilon_1)$ has to be the unique point of order 2 which is fixed by τ. Hence ϕ is uniquely determined by L_ϕ.

Conversely let $L/\mathbb{Q}$ be Galois with group S_4 containing $K = \mathbb{Q}(E[2])$ and $\mathrm{Gal}(L/K) =< \epsilon_1, \epsilon_2 >$ with $\tau\epsilon_1\tau = \epsilon_1$ and $\sigma\epsilon_1\sigma^{-1} = \epsilon_2$. Then $\tilde{\phi} : G_\mathbb{Q} \to E[2]$ determined by $\tilde{\phi}(\epsilon_1) = P_\tau$ and $\tilde{\phi}(\epsilon_2) = \sigma P_\tau$ is an element in $\mathrm{Hom}_{\mathrm{Gal}(L/\mathbb{Q})}(\mathrm{Gal}(\overline{L}/L), E[2])$ and hence corresponds to a nontrivial element in $H^1(G_\mathbb{Q}, E[2])$. □

5.2 Lower bound on the number of S_4-extensions

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Assume that $\overline{\rho}_{E,2}$ is surjective, so that $K = \mathbb{Q}(E[2])$ is an S_3-extension. We will show that there are at least 3 S_4-extensions of $\mathbb{Q}$ containing K unramified away from 2, N, and ∞ so long as E does not have complex multiplication by -3. In order to do this, we will use theorems about cohomology of groups.

First, define $E[2]^* = \mathrm{Hom}(E[2], \mu_2(\overline{\mathbb{Q}}))$ to be the Galois module where the action of $G_\mathbb{Q}$ is given by the formula

$$(\phi^g)(m) = g(\phi(g^{-1}m)).$$

Theorem 5.2. *Assume that $\mathbb{Q}(E[2])$ is an S_3-extension and that E does not have an isogeny of degree 3. Then, there are at least 3 S_4 extensions of $\mathbb{Q}$ with the right ramification.*

Proof. Let M be a $G_{\mathbb{Q}}$-module. In our case, $M = E[2]$. By local conditions, we mean a collection $\mathcal{L} = \{L_p\}$, where for each prime p (including infinity) we are given a subgroup $L_p \leq H^1(G_{\mathbb{Q}_p}, M)$ such that for all but finitely many p, $L_p = \ker(H^1(G_{\mathbb{Q}_p}, M) \to H^1(I_p, M))$. (These are called the unramified classes and will be denoted $H^1_{ur}(G_{\mathbb{Q}_p}, M)$.) The corresponding generalized Selmer group is

$$H^1_{\mathcal{L}}(G_{\mathbb{Q}}, M) = \{c \in H^1(G_{\mathbb{Q}}, M) : \mathrm{res}_p(c) \in L_p \text{ for all } p\},$$

where $\mathrm{res}_p : H^1(G_{\mathbb{Q}}, M) \to H^1(G_{\mathbb{Q}_p}, M)$ is the restriction homomorphism. Note that if $\mathcal{L}$ is a collection of local conditions for M then $\mathcal{L}^* = \{\mathcal{L}_v^\perp\}$ is a collection of local conditions for for the Pontryagin dual M^* of M.

We will take the local conditions to be such that the unramified classes are all but $2, p_1, \ldots p_n$, or ∞ where the p_i are the distinct odd prime divisors of N.

Using the Bayer/Frey correspondence (5.1), we get that the **nonzero** elements of $H^1_{\mathcal{L}}(\mathbb{Q}, E[2])$ correspond bijectively to the S_4-extensions M of $\mathbb{Q}$, containing $K = \mathbb{Q}(E[2])$ with M over K unramified away from $2, p_i, \infty$.

The Duality Theorem for Selmer groups ([9], Theorem 2.18) gives that

$$\frac{\#H^1_{\mathcal{L}}(\mathbb{Q}, E[2])}{\#H^1_{\mathcal{L}^*}(\mathbb{Q}, E[2]^*)} = \frac{\#H^0(\mathbb{Q}, E[2])}{\#H^0(\mathbb{Q}, E[2]^*)} \cdot \prod_{\nu} \frac{\#L_\nu}{\#H^0(\mathbb{Q}_\nu, E[2])}$$

Remarks: Note that $\#(E[2]^*) = \#(\mathrm{Hom}(E[2], \mu_2)) = 4$. Note that $\#H^0(G_\nu, E[2]) = \#H^1(G_\nu/I_\nu, E[2]^{I_\nu})$ for all but finitely many places, so we automatically get that almost all factors in the product are 1 (See [25], p. 111) (except for $\ell = 2, p_i, \infty$).

For $\ell = 2, p_i$, the following holds:

$$\frac{\#H^1(G_\ell, E[2])}{\#H^0(G_\ell, E[2])} = \#H^0(G_\ell, E[2]^*) \cdot \ell^{v_\ell(\#E[2])}.$$

For $\ell = \infty$, $G_{\mathbb{Q}_\infty}$ is the group of order 2 consisting of the identity and complex conjugation.

Let Δ be the discriminant of E. There are two cases:

Case 1: $\Delta < 0$. In this case, $E[2]$ consists of the point at ∞, 2 points not on the real axis, and 1 other point on the real axis. In this case, complex conjugation only fixes 2 of the points of $E[2]$, so $\#H^0(\mathbb{Q}_\infty, E[2]) = 2$. In this case, there are 4 cocycles and 2 of these are coboundaries, so $\#H^1(\mathbb{Q}_\infty, E[2]) = 2$. Therefore, the factor $\frac{\#L_\infty}{\#H^0(\mathbb{Q}_\infty, E[2])} = 1$ in this case.

Case 2: $\Delta > 0$. In this case, $E[2]$ consists of the point at ∞ and 3 other points on the real axis. In this case, complex conjugation fixes all of $E[2]$, so $\#H^0(\mathbb{Q}_\infty, E[2]) = 4$. Also, since the Galois action is trivial in this case, $\#H^1(\mathbb{Q}_\infty, E[2]) = \#\mathrm{Hom}(\mathbb{Q}_\infty, E[2]) = 4$. Therefore, the factor $\frac{\#L_\infty}{\#H^0(\mathbb{Q}_\infty, E[2])} = 1$ in this case.

So using the Duality theorem for Selmer groups above, we get

$$\frac{\#H^1_{\mathcal{L}}(\mathbb{Q}, E[2])}{\#H^1_{\mathcal{L}^*}(\mathbb{Q}, E[2]^*)} = \frac{\#H^0(\mathbb{Q}, E[2])}{\#H^0(\mathbb{Q}, E[2]^*)} \cdot 2^2 \cdot \#H^0(G_2, E[2]^*) \#H^0(G_{p_i}, E[2]^*).$$

We will first evaluate $\#H^0(\mathbb{Q}, E[2]) = \#\{m \in E[2] \quad | \quad \sigma(m) = m, \text{ for all } \sigma \in G_{\mathbb{Q}}\}$. Since E has no rational 2-torsion, only one point of $E[2]$ is fixed by every element of $G_{\mathbb{Q}}$. Therefore, $\#H^0(\mathbb{Q}, E[2]) = 1$.

Next, we will evaluate $\#H^0(\mathbb{Q}, E[2]^*)$. Suppose that $\phi \in E[2]^*$ such that $\phi^g = \phi$ for all $g \in G_{\mathbb{Q}}$. Then, $\phi(m) = (\phi^g)(m) = g(\phi(g^{-1}m))$. Note that $g(\phi(g^{-1}m)) = \phi(g^{-1}m)$ for all $g \in G_{\mathbb{Q}}$ for all $m \in E[2]$ since $\phi : E[2] \to \mu_2(\overline{\mathbb{Q}})$ and because $\mu_2(\overline{\mathbb{Q}}) \subseteq \mathbb{Q}$ so the Galois action on it is trivial. We now have that $\phi(m) = \phi(g^{-1}m)$ for all $g \in G_{\mathbb{Q}}$ and for all $m \in E[2]$. This implies that if $m \neq 0, \phi(m) = 1$. So, $\phi = 1$. Therefore, $\#H^0(\mathbb{Q}, E[2]^*) = 1$.

Applying that $\#H^0(\mathbb{Q}, E[2]) = \#H^0(\mathbb{Q}, E[2]^*) = 1$ to the Duality theorem for Selmer groups, we see that

$$\frac{\#H^1_{\mathcal{L}}(\mathbb{Q}, E[2])}{\#H^1_{\mathcal{L}^*}(\mathbb{Q}, E[2]^*)} = 4 \cdot \#H^0(G_2, E[2]^*)\#H^0(G_p, E[2]^*).$$

This shows that $\#H^1_{\mathcal{L}}(\mathbb{Q}, E[2]) \geq 4$.

Since $\#H^1_{\mathcal{L}}(\mathbb{Q}, E[2]) \geq 4$, the number of S_4-extensions of $\mathbb{Q}$, containing $K = \mathbb{Q}(E[2])$ that are unramified away from $2, p_i, \infty$ is at least $4 - 1 = 3$. $\square$

Chapter 6

An Example

This chapter uses some explicit class field theory in order to find extensions of the 2-division fields of elliptic curves. [We will use the elliptic curve with Cremona reference '11a1' as a running example. This elliptic curve is given by $y^2 + y = x^3 - x^2 - 10x - 20$. In this case, $\overline{\rho}_{E,8}$ is surjective. This can be checked using the criteria of [10]. Therefore, $\rho_{E,2}$ is surjective.]

6.1 Notation

Let E be an elliptic curve defined over $\mathbb{Q}$. Let N denote the conductor of E and let Δ denote the discriminant of E. Let $K = \mathbb{Q}(E[2])$ be the 2-division field of the elliptic curve. If E has negative discriminant, consider the ray class field of K corresponding to the modulus $\mathbf{m} = 2^3 \cdot N \cdot \mathcal{O}_K$. If E has positive discriminant, consider the ray class field of M corresponding to the modulus $\mathbf{m} = 2^3 \cdot N \cdot \infty\mathcal{O}_K$. Let L denote the subfield of this ray class field obtained by taking the fixed field of the elementary abelian 2-part of the ray class group.

For the following family of elliptic curves, $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right)$ is **exactly** 7. For a general semistable elliptic curve over $\mathbb{Q}$ with odd conductor and $\overline{\rho}_{E,2}$ is surjective, $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right) \geq 7$.

6.2 Examples

Theorem 6.1. *Assume that the conductor of E is a prime p congruent to 3 mod 8, assume $\#\mathrm{Cl}(K)$ is odd, and assume that E has supersingular reduction at 2. Then,* $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right) = 7$.

Proof. The criterion of Néron-Ogg-Shafarevich implies that K is unramified outside 2, p, and ∞ (see [19]). Using [6, Proposition 5.2], we find that K over $\mathbb{Q}$ is an S_3-extension. [For example, for the elliptic curve '11a1', the 2-division field is the splitting field of $x^3 - x^2 + x + 1$.]

The condition on p implies that $\Delta = \pm p^s$ for some odd integer s. Thus the quadratic subfield contained in K is either $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$. Since $p \equiv 3 \pmod 4$, $\mathbb{Q}(\sqrt{p})$ is ramified at 2. However, 2 must be inert in order for E to be supersingular at 2. Therefore, the quadratic subfield is $\mathbb{Q}(\sqrt{-p})$ and so the discriminant of K is negative and K is totally complex.

We have that $\mu(K) = \{1, -1\}$. (If there were more roots of unity than $\{1, -1\}$ in K, then K over $\mathbb{Q}$ would contain that cyclotomic subextension. Such an extension would have degree 2. The only possible cyclotomic fields with degree 2 over $\mathbb{Q}$ are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$. Since p is the conductor of an elliptic curve defined over $\mathbb{Q}$, $p \geq 11$).

Also, [6, Proposition 5.2] gives that for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ above p, we have that the ramification degree $e_{\mathfrak{P}}$ equals 2, the inertial degree $f_{\mathfrak{P}}$ equals 1, and the number of such primes is 3. There is exactly one prime ideal $\mathfrak{p}$ lying above 2. It has the ramification degree $e_{\mathfrak{P}} = 3$ and the inertial degree $f_{\mathfrak{P}} = 2$.

We will show that $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right) = 7$ for such E. It will then follow that $\mathrm{Gal}(L/K)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^7$. [Note that the elliptic curve '11a1' falls into this family of minimal examples, so the 2-rank of its ray class group will end up being precisely 7.]

The following is an exact sequence:

$$U(K) \xrightarrow{\rho} (\mathcal{O}_K/m)^* \xrightarrow{\psi} \mathrm{Cl}_m(K) \xrightarrow{\phi} \mathrm{Cl}(K) \ \to 1.$$

Dirichlet's Unit Theorem gives that $U(K) \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$. Since $\Delta < 0$, K is totally complex, so $r_1 = 0$ and $r_2 = 3$. Using this and that $\mu(K) = \{1, -1\}$, we get that $\mathrm{rk}_2\left(U(K)\right) = 3$.

If $\#\mathrm{Cl}(K)$ is odd, the 2-rank of this group is 0. Using the exact sequence, this gives that the 2-rank of $\mathrm{Cl}_m(K)$ equals the 2-rank of $(\mathcal{O}_K/m)^* - 3$. More generally, the 2-rank of $\mathrm{Cl}_m(K)$ equals the 2-rank of $(\mathcal{O}_K/m)^* - 3$ plus the 2-rank of $\mathrm{Cl}(K)$, so powers of 2 in the class number will only increase the overall 2-rank.

For ideals a, b, c of $\mathcal{O}_K$, if $b = a \cdot c$ where a and c are coprime, then $(\mathcal{O}_K/a)^* \times (\mathcal{O}_K/c)^* \cong (\mathcal{O}_K/b)^*$. Therefore, it suffices to compute the 2-rank of $(\mathcal{O}_K/\mathfrak{p}^k)^*$ for prime ideals $\mathfrak{p}$ lying above 2 or p.

Proposition 6.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $(p) = \mathfrak{p} \cap \mathcal{O}_K$ be such that $q = p^f$ is the cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$. Let $k \geq 1$ be an integer. Let*

$$W = \{x \in (\mathcal{O}_K/\mathfrak{p}^k) : x^{q-1} = 1\}$$

and

$$G_{\mathfrak{p}} = (1+\mathfrak{p})/(1+\mathfrak{p}^k).$$

Then $(\mathcal{O}_K/\mathfrak{p}^k)^* = W \times G_{\mathfrak{p}}$.

Proof. (See [11]). □

First, for $\mathfrak{p}$ a prime above the given odd prime p in $\mathcal{O}_K$, $G_{\mathfrak{p}}$ is a p-group, so $\mathrm{rk}_2 \quad G_{\mathfrak{p}} = 0$ and W is a cyclic group of even order. Each such prime therefore contributes 1 to the 2-rank. Therefore, together, the three primes above p in $\mathcal{O}_K$ contribute 3 to the 2-rank.

Second, consider $\mathfrak{p}$ a prime above 2 in $\mathcal{O}_K$. Let $K_{\mathfrak{p}}$ denote the completion of K at $\mathfrak{p}$. Since the only prime above 2 has ramification degree $e_{\mathfrak{p}}$ equal to 3 and inertial degree $f_{\mathfrak{p}}$ equal to 2,the local field $K_{\mathfrak{p}}$ is a degree $d = 6$ extension of $\mathbb{Q}_2$.

The structure of the multiplicative group of non-zero elements of a non-archimedean local field $K_{\mathfrak{p}}$ is isomorphic to

$$K_{\mathfrak{p}}^* \cong < \overline{\omega} > \times \mu_{q-1} \times U^{(1)}$$

where q is the order of the residue field (4 in our case), μ_{q-1} is the group of $(q-1)^{\text{st}}$ roots of unity (in $K_{\mathfrak{p}}^*$), $U^{(1)}$ is the group of principal units, and $\overline{\omega}$ is a uniformizer of $K_{\mathfrak{p}}$.

Since $K_{\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_2$ (of degree d), the structure as an abelian group is the following:

$$K_{\mathfrak{p}}^* \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$$

where $a \geq 0$ is defined so that the group of p-power roots of unity in $K_{\mathfrak{p}}$ is μ_{p^a}. In this case,

we have that $d = 6$. Altogether, the prime above 2 contributes 7 to the 2-rank.

Returning to the exact sequence, we get $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right) = 7$.

□

Theorem 6.3. *Assume that the conductor of E is a prime p congruent to $3 \bmod 8$, assume $\mathrm{Cl}(K)$ is odd, and assume that E has supersingular reduction at 2. Then*

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{SmallGroup}(768, 1090187).$$

Thus, there exists an extension of $\mathbb{Q}$ containing K with Galois group $\Gamma/\Phi(\Gamma)$ with the right ramification.

Proof. For each elliptic curve E satisfying the assumptions, we know that $\mathrm{Gal}(L/\mathbb{Q})$ is an extension of S_3 by the normal subgroup $(\mathbb{Z}/2\mathbb{Z})^7$ by Theorem 6.1. Magma ([5]) tells us that there are 20 such groups. Each of these groups has 0,1,3, or 7 S_4-quotients. Our goal is to identify which of these groups is $\mathrm{Gal}(L/\mathbb{Q})$.

We know that the splitting field of $X^4 - \Delta$ over $\mathbb{Q}$, $\mathbb{Q}_{\Delta,4}$, is contained in $\mathbb{Q}(E[4])$. Also, $[\mathbb{Q}_{\Delta,4} : \mathbb{Q}] = 8$; see [1, p.80-81]. This extension is contained in the abelian extension of K unramified outside 2 and Δ with $\mathrm{Gal}(\mathbb{Q}_{\Delta,4}/\mathbb{Q})$ equal to the dihedral group of order 8. Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ will have the dihedral group of order 8 as a quotient.

For elliptic curves with odd, squarefree conductors, we get that $\mathbb{Q}(\sqrt{2}, \sqrt{\Delta}, \sqrt{-1})$ is a degree 8 extension of $\mathbb{Q}$ and contained in the abelian extension of K unramified outside 2 and N. Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ will have the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient.

We know that there are at least 3 S_4 extensions contained in L that contain K by using the result from Chapter 5. Using that $\mathrm{Gal}(L/\mathbb{Q})$ has at least 3 S_4 quotients narrows the list of groups. Of the remaining possible groups, the only one with both a dihedral group of order 8 as a quotient, and the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient is the group $\mathrm{SmallGroup}(768, 1090187)$.

The group $\mathrm{SmallGroup}(768, 1090187)$ has a quotient isomorphic to $\Gamma/\Phi(\Gamma)$. The corresponding field extension is an extension of $\mathbb{Q}$ containing K with Galois group $\Gamma/\Phi(\Gamma)$ and with the right ramification. □

Note that the specific class of elliptic curves minimally achieve surjectivity to $\Gamma/\Phi(\Gamma)$ since $\mathrm{rk}_2\left(\mathrm{Cl}_{\mathbf{m}}(K)\right)$ must be one less than a power of 2. This is because the 2-rank of the ray class group measures the number of quadratic extensions of K only ramified at primes dividing $\mathfrak{m}$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals of K with $x^2 - \mathfrak{p}$ an extension of K contained in the ray class field of K, then all of the quadratic extensions can be obtained by multiplying together the primes in an element of the power set of the primes $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ except for the empty set.

Also, note that $\Gamma/\Phi(\Gamma)$ has $\mathrm{GL}_2(\mathbb{Z}_2)/\Phi(\mathrm{GL}_2(\mathbb{Z}_2))$ as a quotient, so if the conjecture holds, i.e. if the the field extension corresponding to $\Gamma/\Phi(\Gamma)$ comes from the metabelian representation, and the representation to $\Gamma/\Phi(\Gamma)$ is surjective, then each E in the family of elliptic curves has a surjective 2-adic representation.

Chapter 7

Main Theorem

We have seen in Chapter 6 that if E is an elliptic curve of prime conductor p congruent to 3 mod 8 with odd order $\mathrm{Cl}(K)$, $K = \mathbb{Q}(E[2])$, and supersingular reduction at 2, then there is an extension of $\mathbb{Q}$ containing K with Galois group $\Gamma/\Phi(\Gamma)$ and the right ramification. We will give various other conditions on E that guarantee this result.

First, we state a precise condition on the field extension that we are looking for. We will call this condition C for E.

Definition 7.1. *An extension $L_1/\mathbb{Q}$ satisfies condition C for an elliptic curve E if the following hold:*

1. *The field L_1 contains the field $K = \mathbb{Q}(E[2])$.*
2. *The Galois group $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \Gamma/\Phi(\Gamma)$*
3. *The extension $L_1/\mathbb{Q}$ has the right ramification*
4. *Let $G = \mathrm{GL}_2(\mathbb{Z}_2)$. There is a field K_1 with $L_1 \supset K_1 \supset K$ such that $\mathrm{Gal}(K_1/\mathbb{Q}) \cong G/\Phi(G)$. Also, $K_1 \subset \mathbb{Q}(E[8])$.*

Remark: Consider the last part of condition C. The group $\Gamma/\Phi(\Gamma)$ has 3 quotients isomorphic to $G/\Phi(G)$. We are interested in the corresponding field that is contained in the fields

$\mathbb{Q}(E[2^n])$ for $n \geq 3$. It suffices to find the K_1 contained in $\mathbb{Q}(E[8])$.

Definition 7.2. *Given a field extension L_1 over $\mathbb{Q}$ satisfying condition C for E, we get a representation $\psi_E : G_{\mathbb{Q}} \to \Gamma/\Phi(\Gamma)$. We will also say that ψ_E satisfies condition C.*

First, we will show that the elliptic curves in the example theorem 6.3 satisfy condition C.

Theorem 7.3. *Assume that the conductor of E is a prime p congruent to $3 \bmod 8$, assume $\mathrm{Cl}(K)$ is odd, and assume that E has supersingular reduction at 2.*

Proof. We have already seen in theorem 6.3 that there is an extension L of $\mathbb{Q}$ with Galois group $\mathrm{SmallGroup}(768, 1090187)$ and therefore a field L_1 contained in L with $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \Gamma/\Phi(\Gamma)$. Also, L_1 contains K since there is a unique S_3-quotient of $\mathrm{SmallGroup}(768, 1090187)$ and an S_3-quotient of $\Gamma/\Phi(\Gamma)$. We have that L_1 is contained in L, which is contained in the ray class field of K with modulus $\mathbf{m}$. This modulus is not divisible by primes other than 2, primes dividing N, and ∞. Therefore, $L_1/\mathbb{Q}$ is unramified outside of 2, primes dividing N, and ∞, so $L_1/\mathbb{Q}$ has the right ramification. Therefore, $L_1/\mathbb{Q}$ satisfies the first 3 parts of condition C for the elliptic curve E.

We have seen that in this case, $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$, so $\overline{\rho}_{E,2}$ is surjective. We also have that E is semistable. Using theorem 2.2.5, we get that $\rho_{E,2}$ is surjective. Therefore, the image of the 2-adic representation of E in G is all of G. Therefore, for the last part of condition C, we are looking for $K_1/\mathbb{Q}$ with K_1 contained in L_1 and with $\mathrm{Gal}(K_1/K) \cong G/\Phi(G)$.

The groups $\mathrm{SmallGroup}(768, 1090187)$ and $\Gamma/\Phi(\Gamma)$ each have 3 quotients isomorphic to $G/\Phi(G)$ and 3 S_4-quotients. Exactly one of the 3 S_4-quotients is contained in $\mathbb{Q}(E[4])/\mathbb{Q}$.

By taking the compositum of this S_4-extension of $\mathbb{Q}$ with the $\mathbb{Q}(\sqrt{2}, \sqrt{\Delta}, \sqrt{-1})$ extension of $\mathbb{Q}$, we get the $G/\Phi(G)$ extension of $\mathbb{Q}$ contained in $\mathbb{Q}(E[8])$. □

Theorem 7.4. *Let E be an elliptic curve defined over $\mathbb{Q}$. Assume that E has surjective 2-adic representation. Then there is an extension of $\mathbb{Q}$ satisfying condition C for E.*

Proof. Let E have conductor N. Consider L to be the 2-quotient of a certain ray class group as in Chapter 6. Since E has surjective 2-adic representation, there is a field K_1 contained in L with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$ over $\mathbb{Q}$. This is the field extension of $\mathbb{Q}(\sqrt{2}, \sqrt{N}, \sqrt{-1})$ over $\mathbb{Q}$. Also, since the 2-adic representation is surjective, we know that E does not have CM, so by the result in Chapter 5, we know that there are at least 3 S_4 extensions K_2, K_3, K_4 that contain K and are contained in L. Taking the compositum of the fields K_i for $1 \leq i \leq 4$, we get a Galois extension of $\mathbb{Q}$ with Galois group $\Gamma/\Phi(\Gamma)$. This field is contained in L, so it has the right ramification.The proof that there is a $G/\Phi(G)$ extension of $\mathbb{Q}$ coming from the 2-adic representation of E follows as in 6.3.

□

Corollary 7.5. *Assume that E is a semistable elliptic curve defined over $\mathbb{Q}$. Assume that $\overline{\rho}_{E,2}$ is surjective. Then, there is an extension of $\mathbb{Q}$ satisfying condition C for E.*

Proof. Using theorem 2.2.5, we have that since E is a semistable elliptic curve over $\mathbb{Q}$ with $\overline{\rho}_{E,2}$ surjective, $\rho_{E,2}$ is surjective. Then, applying theorem 7 gives the result. □

Corollary 7.6. *Let E be an elliptic curve defined over $\mathbb{Q}$. Assume that E is semistable. Assume that E has good supersingular reduction at 2. Then, there is an extension of $\mathbb{Q}$ satisfying condition C for E.*

Proof. Using [6][Proposition 5.2], we find that K over $\mathbb{Q}$ is an S_3-extension. Therefore, corollary 7.5 applies. □

In particular, these assumptions imply that if the extension corresponding to $\Gamma/\Phi(\Gamma)$ is cut out by the metabelian representation, then the 2-adic representation is surjective. Below are some examples of what happens when one of the assumptions from Theorem 7.6 is dropped.

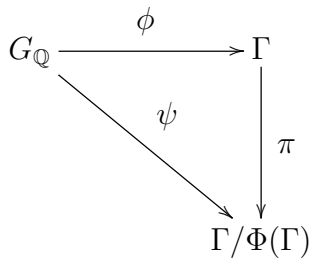
1. A counterexample that is not semistable and has good supersingular reduction at 2 is '27a1'. This elliptic curve has CM and does not surject onto $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$. In this case, $\mathrm{Gal}(L/\mathbb{Q})$ only has 1 S_4 quotient.

2. A counterexample that is semistable and does not have good supersingular reduction at 2 is '17a1'. This elliptic curve does not surject onto $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) \simeq S_3$.

We showed that for certain families of elliptic curves, there is a number field L containing the 2-division field of E with $\mathrm{Gal}(L/\mathbb{Q})$ having a quotient isomorphic to $\Gamma/\Phi(\Gamma)$. Also, the corresponding extension of $\mathbb{Q}$ has the correct ramification.

Theorem 7.7. *Let E be an elliptic curve with $\rho_{E,2}$ surjective. This gives that there exists a map $\psi_E : G_{\mathbb{Q}} \to \Gamma/\Phi(\Gamma)$ satisfying condition C.*

Corollary 7.8. *Assume that Conjecture $\star$ holds (1.3), i.e. that in the following diagram*



the composition $\pi \circ \phi_E$ is constructed by the previous theorem and therefore, the diagram commutes. Then the metabelian representation associated to E, $\phi : G_{\mathbb{Q}} \to \Gamma$ is surjective.

Chapter 8

Prime $\ell = 3$

We will define Γ_n and Γ in this case.

Consider F, a free pro-ℓ group on 2 generators (say, a, b). Let the maps $\pi_n : F \to (\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})$ be the canonical quotient maps. Let K_n be the kernel of π_n. Then define $M_n = F/\Phi(K_n)$.

Let $M_{2,\ell}(\ell)$ be the inverse limit of the groups M_n. This group is the free metabelian pro-ℓ group of rank 2 with commutator subgroup abelian of exponent ℓ.

We define the quotient maps q and q_n by the inner automorphism groups as before:

$$\mathrm{Aut}(M_{2,\ell}(\ell)) \xrightarrow{\quad q \quad} \mathrm{Out}(M_{2,\ell}(\ell)) \ ,$$

$$\mathrm{Aut}(M_n) \xrightarrow{\quad q_n \quad} \mathrm{Out}(M_n) \ .$$

Definition 8.1. *Define* $\Gamma_n = q_n^{-1}(\mathrm{GL}_2(\mathbb{Z}/3^n\mathbb{Z}))$.

Definition 8.2. *Define* $\Gamma = \varprojlim_n \Gamma_n$.

Theorem 8.3. *The order of* $\Gamma/\Phi(\Gamma)$ *is* 34992 *and* Γ_2 *is isomorphic to* $\Gamma/\Phi(\Gamma)$.

Proof. Let $G = GL(2, \mathbb{Z}_3)$ and let $I = \mathrm{Inn}(M_{2,\ell}(\ell))$. Using Theorem 4.3, we get that the following sequence is exact:

$$1 \to I \to \Gamma \to G \to 1.$$

Let L be the kernel from Γ to Γ_1. Let K be the kernel from G to G_1. The Nine Lemma holds in the category of groups. It gives that since the columns of the following diagram are exact and the bottom two rows are exact that the top row is exact:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & L & \longrightarrow & K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & \Gamma & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & \Gamma_1 & \xrightarrow{\sim} & G_1 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

In the diagram, both Γ_1 and G_1 are isomorphic to $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$ of order 48. Since the top row is an exact sequence of pro-3 groups, it follows that

$$1 \longrightarrow I/(I \cap \Phi(L)) \longrightarrow L/\Phi(L) \longrightarrow K/\Phi(K) \longrightarrow 1$$

is an exact sequence.

Consider $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $v = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $b = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Then the following relations hold: $w^4, bv^{-1}b^{-1}v^2, w^2b^{-1}w^2b,$

$w^2v^{-1}w^2v, wv^{-1}wv^{-1}w^{-1}v^{-1}, b^{-1}wb^{-1}wbwbw, w^{-1}v^{-2}w^{-1}b^{-1}w^{-1}vw^{-1}b, v^{-3}b^{-3}vb^2v^{-1}b$. Using this, we can compute that $K/\Phi(K)$ is an elementary abelian 3-group of rank 4.

In general, given a group G_0, $\mathrm{Inn}(G_0) \cong G_0/Z(G_0)$ where $Z(G_0)$ denotes the center of G_0. In this case, since $M_{2,\ell}(\ell)$ is generated by 2 elements, $M_{2,\ell}(\ell)/Z(M_{2,\ell}(\ell))$, and therefore, $\mathrm{Inn}(M_{2,\ell}(\ell))$ is generated by 2 elements. Therefore, $I/(I \cap \Phi(\Gamma)$ is an elementary abelian

3-group of rank 2 and therefore $L/\Phi(L)$ is an elementary abelian 3-group of rank 6. We get the following diagram:

$$\begin{array}{c} \Gamma \\ {\scriptstyle 48}\,\big| \\ L \\ {\scriptstyle 3^6}\,\big| \\ \Phi(L) \end{array}$$

Since $L \trianglelefteq \Gamma$, $\Phi(L) \leq \Phi(\Gamma)$ and therefore the order of $\Gamma/\Phi(\Gamma)$ divides 34992.

On the other hand, we have that $\Gamma/\Phi(\Gamma)$ surjects onto $\Gamma_2/\Phi(\Gamma_2)$, which is a group of order 34992. Therefore, the order or $\Gamma/\Phi(\Gamma)$ is 34992 and $\Gamma/\Phi(\Gamma) \simeq \Gamma_2/\Phi(\Gamma_2)$. Also, we note that $\Gamma_2/\Phi(\Gamma_2) \simeq \Gamma_2$ by computation. □

By using the Frattini lifting theorem and the above theorem, we will get a result that if the representation to Γ_2 is surjective, then the representation to Γ is surjective.

Chapter 9

Conjugacy Invariants for Γ

We would like an invariant of Γ that generalizes trace and determinant. For now, we focus on the quotient of $\Gamma \cong \mathrm{SmallGroup}(768, 1090187)$ and compute these invariants for the images of the Frobenius elements in the field extensions of $\mathbb{Q}$ with Galois group isomorphic to the same group (see in Chapter 6).

The group $\mathrm{SmallGroup}(768, 1090187)$ has 6 $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$-quotients. We can consider the traces of Frobenius coming from each of these representations.

Using class field theory as in Chapter 6, we get a field extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathrm{SmallGroup}(768, 1090187)$. We can compute the images of Frob_p in this group for $p \notin 2, p_i$ with p_i equal to the primes dividing the conductor of E.

For example, the chart below (9) shows the traces of Frobenius and 6 sets of traces mod 4 coming from the 6 $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$-quotients for the elliptic curve curve with Cremona reference '11a1'. The 2nd column has the usual traces of Frobenius for each prime p. The coefficients in the third column are these traces taken mod 4.

We consider the following 7-tuple associated to an element of $H = \mathrm{SmallGroup}(768, 1090187)$:

$[a_{1,p}, a_{2,p}, a_{3,p}, a_{4,p}, a_{5,p}, a_{6,p}, d_p]$ where the $a_{i,p}$ are the traces are the 6 quotient maps from H to $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. For each of these maps, the determinant is the same. Let d_p denote this quantity. We have that $d_p \equiv p \bmod 4$.

All of the traces are the same mod 2 since all of the $\mathrm{SmallGroup}(768, 1090187)$-quotients contain the same $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ quotient.

Chart for Frobenius Invariants for '11a1'

p	$p+1-\#E(\mathbb{F}_p)$						
3	-1	3	3	3	3	3	3
5	1	1	1	1	3	3	3
7	-2	2	0	2	2	0	2
13	4	0	2	2	0	2	2
17	-2	2	0	2	2	0	2
19	0	0	2	2	0	2	2
23	-1	3	3	3	1	1	1
29	0	0	0	0	0	0	0
31	7	3	3	3	1	1	1
37	3	3	3	3	1	1	1
41	-8	0	2	2	0	2	2
43	-6	2	2	0	2	2	0
47	8	0	0	0	0	0	0
53	-6	2	2	2	2	2	2
59	5	1	1	1	1	1	1
61	12	0	0	0	0	0	0
67	-7	1	1	1	1	1	1
71	-3	1	1	1	3	3	3
73	4	0	2	2	0	2	2
79	-10	2	2	0	2	2	0
83	-6	2	2	0	2	2	0
89	15	3	3	3	3	3	3
97	-7	1	1	1	1	1	1

9.1 7-tuples

Let $m : H \to [a_{1,p}, a_{2,p}, a_{3,p}, a_{4,p}, a_{5,p}, a_{6,p}, d_p]$ be the map from elements of H to 7-tuples.

Running over the whole group H gives the following set of 17 7-tuples:

$S = \{[2,2,2,2,2,2,1],[1,1,1,3,3,3,3],[2,0,2,2,0,2,3],[1,1,1,1,1,1,3],[3,3,3,1,1,1,1],$
$[2,0,2,2,0,2,1],[1,1,1,1,1,1,1],[3,3,3,1,1,1,3],[0,2,2,0,2,2,3],[0,2,2,0,2,2,1],$
$[2,2,0,2,2,0,3],[0,0,0,0,0,0,3],[2,2,0,2,2,0,1],[0,0,0,0,0,0,1],[3,3,3,3,3,3,3],$
$[3,3,3,3,3,3,1],[1,1,1,3,3,3,1]\}$.

The converse also holds in that if all 17 7-tuples are in the image, then the group is H.

Lemma 9.1. *Let H_1 is a subgroup of H such that $m(H_1)$ hits all 17 7-tuples. Then $H_1 = H$*

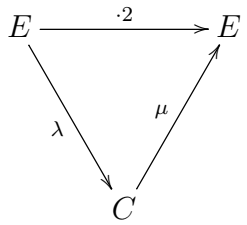
Proof. Consider the subset $S_1 = \{\}$. If $m(H_1)$ contains the set S, then $H_1 = H$. (proof by iteration). There are many subsets S_i of S such that if $m(H_1)$ contains S_i then $H_1 = H$. $\square$

9.2 Two-coverings of elliptic cruves

In Chapter 5, we presented the following result of Bayer and Frey.

Proposition 9.2 ([3] Proposition 1.1)**.** *Let $K = \mathbb{Q}(E[2])$. There is a one-to-one correspondence between fields $L \supset K$ with $\mathrm{Gal}(L/K) = S_4$ and elements $\phi \in H^1(G_{\mathbb{Q}}, E[2])\backslash\{0\}$.*

Bayer and Frey also recall the geometric interpretation of elements in $H^1(G_{\mathbb{Q}}, E[2])$ as 2-coverings of E over $\mathbb{Q}$ as in [7]: ϕ corresponds to a commutative triangle



with λ $\overline{\mathbb{Q}}$-birational and μ $\mathbb{Q}$-rational. Then C is a curve of genus 1 over $\mathbb{Q}$ with Jacobian E.

Let S be the set of primes ℓ, p_i, ∞ where p_i are the primes dividing the conductor of E. We denote by $H^1(G_{\mathbb{Q}}, E[2]; S)$ the subgroup of $H^1(G_{\mathbb{Q}}, E[2])$ consisting of cocycles that are unramified away from S. Let δ be the coboudnary map from $E(\mathbb{Q})$ to $H^1(G_{\mathbb{Q}}, E[2])$. Then we get that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \overset{\delta}{\hookrightarrow} H^1(G_{\mathbb{Q}}, E[2]; S) \ .$$

In the setting of 2-descent on an elliptic curve, we are only interested in the image of δ in $H^1(G_{\mathbb{Q}}, E[2]; S)$.

In the case that ϕ is an element of the Selmer group of E, a result of Birch and Swinnerton-Dyer [4] gives that the curve C is the corresponding two-covering which can be given by an equation $U^2 = f_4(V)$ where f_4 is a polynomial of degree 4 over $\mathbb{Q}$ and L_ϕ is the splitting field of f_4.

9.2.1 Positive rank

If the rank of $E(\mathbb{Q})$ is positive, we can take $P \in E(\mathbb{Q}) \backslash 2E(\mathbb{Q})$ and $\phi = \delta(P)$. Then Bayer and Frey say that it is easy to determine a polynomial $f_4(V)$ determining L_ϕ by dividing P by two. The addition formulas (for instance [23]) imply:

If E is given by

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

and

$$P = (x, y)$$

then

$$f_4(V) = V^4 - 4xV^3 - (2a_4 + a_1a_3 + a_1^2x + 4a_2x)V^2 - 2(a_3^2 + 4a_6 + 2a_4x + a_1a_3x)V -$$

$$(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_1a_3a_4 + a_2a_3^2 - a_4^2 + a_3^2x + 4a_6x).$$

Let C be the elliptic curve associated to $y^2 = f_4$. Note that C depends on E and on P.

To each prime p, we associate the 7-tuple, $[a_{1,p}, a_{2,p}, a_{3,p}, a_{4,p}, a_{5,p}, a_{6,p}, d_p]$ in the following way:

Let $a_{C,p}$ be the trace of Frobenius of C at p.

- $a_{1,p} = a_p = p + 1 - \#E(\mathbb{F}_p) \bmod 4$ (the usual trace of Frobenius)
- $d_p = p \bmod 4$ (the usual determinant of Frobenius)
- if $\left(\frac{\Delta}{p}\right) = 1$, then $a_{2,p} = a_{1,p}$, if $\left(\frac{\Delta}{p}\right) = -1$, then $a_{2,p} = a_{C,p} \bmod 4$
- if $\left(\frac{\Delta}{p}\right) = 1$ then $a_{3,p} := a_{1,p}$, if $\left(\frac{\Delta}{p}\right) = -1$, then $a_{3,p} = a_{1,p} + a_{2,p} \bmod 4$
- If $\left(\frac{-2}{p}\right) = 1$, then $a_{4,p} = a_{1,p}$, $a_{5,p} = a_{2,p}$, and $a_{6,p} = a_{3,p}$. If $\left(\frac{-2}{p}\right) = -1$, then $a_{4,p} = -a_{1,p} \bmod 4$, $a_{5,p} = -a_{2,p} \bmod 4$, and $-a_{6,p} = a_{3,p} \bmod 4$

Example 1: $E : Y^2 + Y = X^3 + X$

This is the curve $'43a1'$ in the Cremona database. Its discriminant is -43 and we can take $P = (0, 0)$ as a $\mathbb{Q}$-rational point not divisible by 2. The polynomial $f_4(V) = V^4 - 2V - 1$.

The discriminant of this polynomial is $-2^4 43^1$. Let g be the defining polynomial of the unique S_4-extension of $\mathbb{Q}$ contained inside $\mathbb{Q}(E[4])$. The discriminant of g is $-2^4 43^3$. Therefore, we see that f_4 and g generate distinct S_4-extensions of $\mathbb{Q}$.

Applying the formula for 7-tuples as above, we get

Chart for '43a1'

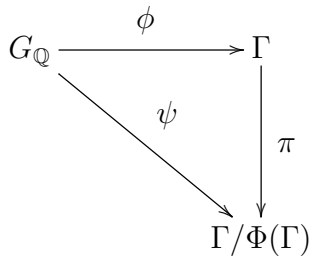
p	$p+1-\#E(\mathbb{F}_p)$							
3	-2	2	0	2	2	0	2	3
5	-4	0	2	2	0	2	2	1
7	0	0	2	2	0	2	2	3
11	3	3	3	3	3	3	3	3
13	-5	3	3	3	1	1	1	1
17	-3	1	1	1	1	1	1	1
19	-2	2	2	0	2	2	0	3
23	-1	3	3	3	1	1	1	3
29	-6	2	0	2	2	0	2	1
31	-1	3	3	3	1	1	1	3
37	0	0	0	0	0	0	0	1
41	5	1	1	1	1	1	1	1
47	4	0	0	0	0	0	0	3
53	-5	3	3	3	1	1	1	1
59	-12	0	0	0	0	0	0	3
61	2	2	0	2	2	0	2	1
67	-3	1	1	1	1	1	1	3
71	2	2	0	2	2	0	2	3
73	2	2	0	2	2	0	2	1
79	-8	0	0	0	0	0	0	3
83	15	3	3	3	3	3	3	3
89	-4	0	2	2	0	2	2	1
97	7	3	3	3	3	3	3	1

Using the formula, we get all 17 7-tuples. Also, we get the same chart here that we would get if we used the class field theory approach as we did for the elliptic curve '11a1' in the first part of this chapter. Using Lemma 9.1, we get that the representation $\psi_E : G_{\mathbb{Q}} \to \Gamma/\Phi(\Gamma)$ is surjective. Since the conductor of E is a prime p congruent to 3 mod 8, $\#\mathrm{Cl}(K)$ is odd, and

E has supersingular reduction at 2,

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{SmallGroup}(768, 1090187).$$

Therefore, there is only one such ψ_E coming from class field theory as in Chapter 6. If this ψ_E is the representation that makes the diagram commute



then the representation ϕ_E to Γ is surjective.

Example 2: $E : Y^2 + Y = X^3 - 3X + 4$

This is the curve $'135a1'$ in the Cremona database. Its discriminant is $-3^3 5^2$ and we can take $P = (4, -8)$ as a $\mathbb{Q}$-rational point not divisible by 2. The polynomial $f_4(V) = V^4 - 16V^3 + 6V^2 + 14V - 59$. The discriminant of this polynomial is $-2^4 43^3 5^2$. Let g be the defining polynomial of the unique S_4-extension of $\mathbb{Q}$ contained inside $\mathbb{Q}(E[4])$. The discriminant of g is $-2^4 43^3 5^2$. We have that f_4 and g have the same splitting field.

Applying the formula for 7-tuples as above, we only get the following 13 of the 17-tuples:

$S = \{[2,2,2,2,2,2,1], [1,1,1,3,3,3,3], [2,0,2,2,0,2,3], [1,1,1,1,1,1,3], [3,3,3,1,1,1,1],$
$[2,0,2,2,0,2,1], [1,1,1,1,1,1,1], [3,3,3,1,1,1,3], [0,0,0,0,0,0,3], [0,0,0,0,0,0,1],$
$[3,3,3,3,3,3,3], [3,3,3,3,3,3,1], [1,1,1,3,3,3,1]\}$.

Data: We computed the number of 7-tuples for all of the elliptic curves in the Cremona database of elliptic curve with conductor $N \leq 240000$ ([8]) that are surjective 2-adically and

that have rank 1.

We get that there are 415226 such elliptic curves. All except 2107 of these curves have 17 7-tuples in the image. Among the 2107 elliptic curves, there are no semistable elliptic curves. Also, in each case f_4 is an irreducible quartic. The image of all of these is the set of 13 7-tuples given in example 2. The examples that are not surjective and have conductor under 500 are the folllowing: '135a1', '225e1', '225e2', '297a1', '441f1', '441f2', '459b1', '484a1', '484a2'.

9.2.2 Rank zero

In this case, we can no longer use the formula to divide a points $P \in E(\mathbb{Q})\backslash 2E(\mathbb{Q})$ by 2 as above. Here we will just consider the numerator of multiplying a point 2. We get the polynomial

$$f = x^4 - b_4x^2 - 2b_6x - b_8.$$

Unlike in the case, where ϕ was coming from a rational point, we no longer are guaranteed that this polynomial will be unramified outside of S.

Example 1: Consider the elliptic curve '11a1'. For this curve,

$$f = x^4 + 20x^2 + 158x + 21.$$

The discriminant of this polynomial is $-2^2 11^1 79^2$.

The polynomial $x^4 - 4\Delta x - 12A\Delta$ has discriminant $-2^4 11^3$ in this case. Using f in the formula above gives 17 7-tuples. However, the corresponding representation is ramified at 2,

11, and 17, so is not contained in the metabelian representation.

The curve $y^2 = f$ is a quartic elliptic curve. There are formulas to write this quartic elliptic curve in Weierstrass form (e.g. see **??**). Doing this, we get that this is the elliptic curve $E1 =$ '6952a1'. Its Mordell-Weil group has rank 2. If we now use $E1$ as a starting place, and take the numerator of the formula for multiplying a point by 2, and use the polynomial f_4 as in the last subsection, we get

$$x^4 + 72x^3 - 3512x^2 - 176960x + 5891504$$

with discriminant $-2^8 11^1$. Using this polynomial, we get 17 7-tuples and the corresponding representation is unramified outside S.

Example 2: Consider the elliptic curve '139a1'. Here $f = x^4 + 6x^2 + 32x + 29$ of discriminant $-2^6 139$. In this case, we get 17 7-tuples using the formula with C as $y^2 = f$. The corresponding representation is unramified outside S. There are 295570 elliptic curves in the Cremona database of elliptic curve with conductor $N \leq 240000$ ([8]) that are surjective 2-adically and that have rank 0. Of these, only 11950 of these the primes dividing the conductor of $E1$ contained in the set S.

Appendix A

The Magnus Representation

Recall the definition of the Magnus representation. Let F be a free pro-ℓ group on 2 generators. Given a map $\alpha \in \text{Aut}(F)$, the Magnus representation is defined as follows:

$$J(\alpha) = \begin{pmatrix} \left(\frac{\partial \alpha(a_1)}{\partial a_1}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_1}\right)^{ab} \\ \left(\frac{\partial \alpha(a_1)}{\partial a_2}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_2}\right)^{ab} \end{pmatrix}$$

where ^{ab} means take the abelianization.

Since this matrix resembles a Jacobian, I will denote the matrix by $J(\phi)$ for an automorphism ϕ. Restricting to this representation to $\text{IA}(M_{2,\ell}(\ell))$ gives a map from $\text{IA}(M_{2,\ell}(\ell)) \longrightarrow \text{GL}(2, \mathbb{Z}_\ell[[H]])$ where $H := H_1(F, \mathbb{Z}_\ell) \simeq (\mathbb{Z}_\ell)^2$.

By using the chain rule, we will see that the Magnus representation is a crossed homomorphism for $\alpha, \beta \in \text{Aut}(F_2)$.

$$J(\alpha) = \begin{pmatrix} \left(\frac{\partial \alpha(a_1)}{\partial a_1}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_1}\right)^{ab} \\ \left(\frac{\partial \alpha(a_1)}{\partial a_2}\right)^{ab} & \left(\frac{\partial \alpha(a_2)}{\partial a_2}\right)^{ab} \end{pmatrix}$$

$$\alpha(J(\beta)) = \begin{pmatrix} \left(\alpha(\frac{\partial \beta(a_1)}{\partial a_1})\right)^{ab} & \left(\alpha(\frac{\partial \beta(a_2)}{\partial a_1})\right)^{ab} \\ \left(\alpha(\frac{\partial \beta(a_1)}{\partial a_2})\right)^{ab} & \left(\alpha(\frac{\partial \beta(a_2)}{\partial a_2})\right)^{ab} \end{pmatrix}$$

$$J(\alpha \circ \beta) = \begin{pmatrix} \left(\frac{\partial \alpha(\beta((a_1))}{\partial a_1}\right)^{ab} & \left(\frac{\partial \alpha(\beta(a_2))}{\partial a_1}\right)^{ab} \\ \left(\frac{\partial \alpha(\beta(a_1))}{\partial a_2}\right)^{ab} & \left(\frac{\partial \alpha(\beta(a_2))}{\partial a_2}\right)^{ab} \end{pmatrix}$$

For example,

$$\left(\frac{\partial\alpha(\beta((a_1))}{\partial a_1}\right) = \left(\alpha\left(\frac{\partial\beta(a_1)}{\partial a_1}\right)\right)\left(\frac{\partial\alpha(a_1)}{\partial a_1}+\alpha\left(\frac{\partial\beta(a_1)}{\partial a_2}\right)\right)\left(\frac{\partial\alpha(a_2)}{\partial a_1}\right)$$

and matching this up with the matrices $J(\alpha)$ and $\alpha(J(\beta))$, we see that the Magnus representation is a crossed homomorphism because it satisfies the relation:

$$J(\alpha\circ\beta) = J(\alpha)\alpha(J(\beta)).$$

Bibliography

[1] C. ADELMANN, *The decomposition of primes in torsion point fields*, vol. 1761 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 2001.

[2] S. BACHMUTH, *Automorphisms of free metabelian groups*, Trans. Amer. Math. Soc., 118 (1965), pp. 93–104.

[3] P. BAYER AND G. FREY, *Galois representations of octahedral type and 2-coverings of elliptic curves*, Math. Z., 207 (1991), pp. 395–408.

[4] B. J. BIRCH AND H. P. F. SWINNERTON-DYER, *Notes on elliptic curves. I*, J. Reine Angew. Math., 212 (1963), pp. 7–25.

[5] W. BOSMA, J. CANNON, AND C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. Computational algebra and number theory (London, 1993).

[6] A. BRUMER AND K. KRAMER, *The rank of elliptic curves*, Duke Math. J., 44 (1977), pp. 715–743.

[7] J. W. S. CASSELS, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc., 41 (1966), pp. 193–291.

[8] J. CREMONA, *The elliptic curve database for conductors to 130000*, in Algorithmic number theory, vol. 4076 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 11–29.

[9] H. DARMON, F. DIAMOND, AND R. TAYLOR, *Fermat's last theorem*, in Current Developments in Mathematics 1, International Press, 2000, pp. 1–154.

[10] T. DOKCHITSER AND V. DOKCHITSER, *Surjectivity of mod 2^n representations of elliptic curves*, 2011. Available as `http://arxiv.org/abs/1104.5031`.

[11] K. EISENTRÄGER AND S. HALLGREN, *Algorithms for ray class groups and Hilbert class fields*, in Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, Philadelphia, PA, 2010, SIAM, pp. 471–483.

[12] N. ELKIES, *Elliptic curves with 3-adic galois representation surjective mod 3 but not mod 9*, 2006. Available as `http://arxiv.org/abs/math/0612734`.

[13] A. GROTHENDIECK AND M. RAYNAUD, *Revêtements étales et groupe fondamental*, Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.

[14] Y. IHARA, *On Galois representations arising from towers of coverings of* $\mathbf{P}^1\backslash\{0, 1, \infty\}$, Invent. Math., 86 (1986), pp. 427–459.

[15] M. MORISHITA, *Knots and primes*, Universitext, Springer, London, 2012.

[16] H. NAKAMURA, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci. Univ. Tokyo, 2 (1995), pp. 197–231.

[17] ——, *On arithmetic monodromy representations of Eisenstein type in fundamental groups of once punctured elliptic curves*, Research Institute for Mathematical Sciences, (2010), pp. 1–58.

[18] H. NAKAMURA, A. TAMAGAWA, AND S. MOCHIZUKI, *The Grothendieck conjecture on the fundamental groups of algebraic curves [translation of Sūgaku* **50** *(1998), no. 2, 113–129; MR1648427 (2000e:14038)]*, Sugaku Expositions, 14 (2001), pp. 31–53. Sugaku Expositions.

[19] A. P. OGG, *Elliptic curves and wild ramification*, Amer. J. Math., 89 (1967), pp. 1–21.

[20] V. A. ROMAN′KOV, *Generating elements of groups of automorphisms of free metabelian pro-p-groups*, Sibirsk. Mat. Zh., 33 (1992), pp. 145–158, 223.

[21] J.-P. SERRE, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[22] ——, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15 (1972), pp. 259–331.

[23] J. H. SILVERMAN, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer, Dordrecht, second ed., 2009.

[24] H. TSUNOGAI, *On the automorphism group of a free pro-l meta-abelian group and an application to Galois representations*, Math. Nachr., 171 (1995), pp. 315–324.

[25] L. C. WASHINGTON, *Galois cohomology*, in Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 101–120.