Isogenies and Selmer Groups of Abelian Varieties

James Bell

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Mathematics

University College London

September 22, 2025

I, James Bell, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.

Abstract

The rank of an abelian variety is its most important invariant, determining the structure of its rational points, however there is no known algorithm to compute it. A procedure to find it, which works for some abelian varieties, is by descent, which involves computing a Selmer group. The Selmer groups of the variety give an upper bound, and the difference from the correct rank can be explained by the Tate–Shafarevich group, which measures the failure of a local-to-global principle.

This thesis deduces results about Selmer and Tate–Shafarevich groups from the existence of certain isogenies. We give results about the size of the Tate–Shafarevich group in the cases of abelian varieties with complex multiplication, and elliptic curves over dihedral extensions. We also show that the Selmer groups and certain other invariants do not determine the isomorphism class of an abelian variety.

Impact Statement

Understanding the rational points on curves is a key question in number theory. Apart from conic sections, which are well-understood, the simplest case is elliptic curves, which are a type of cubic equation. The points on an elliptic curve have a structure, and there is a finite set of points which can be used to generate all of them. Finding the structure of these points is a remarkably difficult question, and the subject of the Birch–Swinnerton-Dyer conjecture, which is one of the Millenium Prize problems.

A consequence of this conjecture is the p-parity conjecture. This gives a prediction for the size of Selmer groups, which are a tool to give an upper bound on the number of generators necessary to give all of the points on an elliptic curve. Some cases of p-parity are known, and have been used by Bhargava and Shankar to show that a positive proportion of elliptic curves over the rationals satisfy the Birch–Swinnerton-Dyer conjecture. This work on Selmer groups earned Bhargava a Fields Medal in 2014. One result of this thesis is a proof of the p-parity conjecture for a class of abelian varieties, which are a generalisation of elliptic curves.

The Selmer groups give an upper bound for the number of generators needed, but sometimes this is more than the true number. Another result of this thesis controls the difference between these in certain settings, and in some cases this allows us to compute the structure of the points faster than standard algorithms.

Outside of mathematics, number theory has had many applications in cryptography. In particular, elliptic curves, abelian varieties and isogenies are used in some of the most modern encryption methods. These applications are not the main motivation for this thesis, and we do not discuss any consequences of the results, but they may be of interest to researchers in cryptography.

Acknowledgements

My most sincere thanks must go to my supervisor, Vladimir Dokchitser. The topics and questions covered in this thesis were his suggestions, and he patiently devoted many hours to explaining concepts to me, and suggested techniques, references or people to talk to at all the (many) times I was stuck.

I would like to thank the rest of 'Vlad's minions' – Jordan, Holly, Alex, Lilybelle, David and Harry – for the interesting and informative discussions I had with them, mathematical and otherwise, as well as the weekly supply of cake.

I would also like to thank Dominik Bullach and Alex Bartel for their helpful suggestions when I was struggling with integral representation theory, and the reviewer of my paper on complex multiplication, who helped clarify my work significantly.

I am grateful to Antonia, Ciara, friends in the KLB and all my running companions, who have made these four years much more enjoyable than they would otherwise have been, and my mum, dad and brother Tom, for their constant support.

Finally, I'm not sure how I would have got through this without Frances, who has been with me and believed in me through all the highs and lows. I am eternally grateful for her support.

This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1]. The EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London.

UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s)

(i) **1. For a research manuscript that has already been published** (if not yet published, please skip to section 2)**:**

(a) **What is the title of the manuscript?** p^{∞}-Selmer ranks of CM abelian varieties

(b) **Please include a link to or doi for the work:** `https://doi.org/10.1112/blms.13094`

(c) **Where was the work published?** Bulletin of the London Mathematical Society

(d) **Who published the work?** Wiley

(e) **When was the work published?** 6th June 2024

(f) **List the manuscript's authors in the order they appear on the publication:** James Bell

(g) **Was the work peer reviewed?** Yes

(h) **Have you retained the copyright?** No

(i) **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** Yes. `https://doi.org/10.48550/arXiv.2208.14563`

If 'No', please seek permission from the relevant publisher and check the box next to the below statement:

☐ *I acknowledge permission of the publisher named under 1d to include in this thesis portions of the publication named as included in 1c.*

(ii) **For a research manuscript prepared for publication but that has not yet been published** (if already published, please skip to section 3)**:**

(a) **What is the current title of the manuscript?**

(b) **Has the manuscript been uploaded to a preprint server 'e.g. medRxiv'?**

If 'Yes', please give a link or doi:

(c) **Where is the work intended to be published?**

(d) **List the manuscript's authors in the intended authorship order:**

(e) **Stage of publication:**

(iii) **For multi-authored work, please give a statement of contribution covering all authors** (if single-author, please skip to section 4)**:**

(iv) **In which chapter(s) of your thesis can this material be found?** Chapter 3

e-Signatures confirming that the information above is accurate (this form should be co-signed by the supervisor/ senior author unless this is not appropriate, e.g. if the paper was a single-author work)**:**

Candidate: James Bell

Date: 16th February 2025

Supervisor/Senior Author signature (where appropriate)**:**

Date:

UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s)

(i) **1. For a research manuscript that has already been published** (if not yet published, please skip to section 2)**:**

(a) **What is the title of the manuscript?** A Note on the Growth of Sha in Dihedral Extensions

(b) **Please include a link to or doi for the work:** `https://doi.org/10.7169/facm/250311-7-4`

(c) **Where was the work published?** Functiones et Approximatio, Commentarii Mathematici

(d) **Who published the work?** Adam Mickiewicz University

(e) **When was the work published?** 2025

(f) **List the manuscript's authors in the order they appear on the publication:** James Bell

(g) **Was the work peer reviewed?** Yes

(h) **Have you retained the copyright?** No

(i) **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** Yes. `https://doi.org/10.48550/arXiv.2411.15663`

If 'No', please seek permission from the relevant publisher and check the box next to the below statement:

☐ *I acknowledge permission of the publisher named under 1d to include in this thesis portions of the publication named as included in 1c.*

(ii) **For a research manuscript prepared for publication but that has not yet been published** (if already published, please skip to section 3)**:**

(a) **What is the current title of the manuscript?**

(b) **Has the manuscript been uploaded to a preprint server 'e.g. medRxiv'?**

If 'Yes', please give a link or doi:

(c) **Where is the work intended to be published?**

(d) **List the manuscript's authors in the intended authorship order:**

(e) **Stage of publication:**

(iii) **For multi-authored work, please give a statement of contribution covering all authors** (if single-author, please skip to section 4)**:**

(iv) **In which chapter(s) of your thesis can this material be found?** Chapter 4

e-Signatures confirming that the information above is accurate (this form should be co-signed by the supervisor/ senior author unless this is not appropriate, e.g. if the paper was a single-author work)**:**

Candidate: James Bell

Date: 3rd July 2025

Supervisor/Senior Author signature (where appropriate)**:**

Date:

UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s)

(i) **1. For a research manuscript that has already been published** (if not yet published, please skip to section 2)**:**

(a) **What is the title of the manuscript?**

(b) **Please include a link to or doi for the work:**

(c) **Where was the work published?**

(d) **Who published the work?**

(e) **When was the work published?**

(f) **List the manuscript's authors in the order they appear on the publication:**

(g) **Was the work peer reviewed?**

(h) **Have you retained the copyright?**

(i) **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi**
If 'No', please seek permission from the relevant publisher and check the box next to the below statement:

☐ *I acknowledge permission of the publisher named under 1d to include in this thesis portions of the publication named as included in 1c.*

(ii) **For a research manuscript prepared for publication but that has not yet been published** (if already published, please skip to section 3)**:**

(a) **What is the current title of the manuscript?** Non-Isomorphic Abelian Varieties with the Same Arithmetic

(b) **Has the manuscript been uploaded to a preprint server 'e.g. medRxiv'?** Yes
If 'Yes', please give a link or doi: `https://doi.org/10.48550/arXiv.2502.02254`

(c) **Where is the work intended to be published?** Royal Society Open Science

(d) **List the manuscript's authors in the intended authorship order:** James Bell

(e) **Stage of publication:** Accepted

(iii) **For multi-authored work, please give a statement of contribution covering all authors** (if single-author, please skip to section 4)**:**

(iv) **In which chapter(s) of your thesis can this material be found?** Chapter 5

e-Signatures confirming that the information above is accurate (this form should be co-signed by the supervisor/ senior author unless this is not appropriate, e.g. if the paper was a single-author work)**:**

Candidate: James Bell
Date: 14th September 2025

Supervisor/Senior Author signature (where appropriate)**:**
Date:

Contents

Chapter 1

Introduction

The study of Diophantine equations, or equations to be solved in rational numbers, goes back to the Ancient Greeks. In modern terms, number theorists study the points on an algebraic variety. Quadratic equations in two variables give rise to conic sections, and their points have long been well-understood. The next step is elliptic curves. The idea of adding two points on a cubic curve by the chord and tangent process had been known since the seventeenth century, and turns the rational points on the curve into a group. Answering a question of Poincaré, in the 1920s Mordell and Weil proved the following:

Theorem 1.0.1 (Mordell–Weil)**.** *The group of points of an elliptic curve E over a number field K form a finitely-generated abelian group. In particular,*

$$E(K) \cong \mathbb{Z}^{\mathrm{rk}(E/K)} \times E(K)_{\mathrm{tors}},$$

where $\mathrm{rk}(E/K) \in \mathbb{Z}_{\geq 0}$ *is the rank of the curve, and* $E(K)_{\mathrm{tors}}$ *is a finite group.*

The rank of the elliptic curve is a crucial property, telling us whether or not the curve has infinitely many points, and if so what their structure is. Computing ranks is one of the biggest open problems in number theory. While the torsion can be computed practically, the rank is less well-understood, and there is no known algorithm to find ranks which is guaranteed to terminate, or even to tell us whether or not the rank is 0 and hence $E(K)$ is finite. Whether the rank of curves over $\mathbb{Q}$ is bounded or can be arbitrarily large is also an open problem. The aim of this thesis is

to better understand ranks and related invariants.

Example 1.0.2 (The congruent number problem)**.** As an example, consider the following problem, which was first considered over a thousand years ago and remains open.

Given an integer n, is there a right-angled triangle with rational side lengths and area n?

Equivalently, can we solve $a^2 + b^2 = c^2$ and $ab = 2n$ in rational numbers? If so, we call n congruent. It turns out that this can be transformed into a question about elliptic curves, and n is congruent if and only if the elliptic curve $y^2 = x^3 - n^2x$ has positive rank.

Elliptic curves are the simplest case of abelian varieties, which are a type of higher-dimensional varieties with an abelian group structure. Much of the theory of elliptic curves carries across to abelian varieties, principally the fact that they also satisfy the Mordell–Weil theorem. Therefore understanding their ranks is also an important problem in number theory, and the ultimate motivation for the work presented in this thesis.

The next part of this chapter deals with classical material about abelian varieties, and the current state of our knowledge. Specifically, Section 1.1 deals with the Birch–Swinnerton-Dyer conjecture, and Section 1.2 with the Selmer and Tate–Shafarevich groups and the parity conjecture. Section 1.3 gives the statements of our main results. These are divided in to three areas: Selmer groups of abelian varieties with complex multiplication; the growth of the Tate–Shafarevich group under dihedral field extensions; and the extent to which arithmetic properties determine the isomorphism class of an abelian variety. These correspond to Chapters 3, 4 and 5 of the thesis respectively. Section 1.4 details the structure of the remainder of the thesis, and finally Section 1.5 lists the notation used.

1.1 The Birch–Swinnerton-Dyer Conjecture

Based on computational evidence, in the 1960s Birch and Swinnerton-Dyer developed a conjecture which linked the rank of an elliptic curve E to the number of

points on the reduction of E modulo primes. This was refined by Tate, and extended to abelian varieties. Proving this just for elliptic curves over $\mathbb{Q}$ is now a Millennium Prize problem, one of the most significant open problems in all of mathematics, and it has been a key part of research on elliptic curves ever since it was conjectured. It tells us that an analytic object, the L-function, encodes the rank of the abelian variety as well as other important properties.

Conjecture 1.1.1 (Birch–Swinnerton-Dyer [10], Tate [94])**.** *Let A be an abelian variety over a number field K. Then*

(i) The L-function $L(A,s)$ has a meromorphic continuation to $\mathbb{C}$, and has a zero of order $\mathrm{rk}(A/K)$ at $s=1$.

(ii) The Tate–Shafarevich group of A/K is finite.

(iii) The residue is given by a formula

$$\lim_{s\to 1}\frac{L(A,s)}{(s-1)^{\mathrm{rk}(A/K)}} = \mathrm{BSD}(A/K),$$

where $\mathrm{BSD}(A/K)$ is defined in terms of arithmetic invariants of A including $|Ш(A/K)|$.

Here the L-function of an abelian variety is a meromorphic function, which is defined as an infinite product of terms at primes and converges on a right half-plane. The analytic continuation of L was shown by Deuring [37] to hold for elliptic curves with complex multiplication, and is also known for abelian varieties with complex multiplication. It took until 2001 for analytic continuation to be proven for all elliptic curves over $\mathbb{Q}$, as a result of the modularity theorem of Breuil, Conrad, Diamond, Taylor and Wiles [16].

Progress has been made on some cases of the conjecture. For instance, Kolyvagin, Gross–Zagier and others proved, assuming modularity, that when A is an elliptic curve over $\mathbb{Q}$ and the L-function is non-zero or has a trivial zero at 1, parts (i) and (ii) hold ([51, 56] – see [34] for a complete proof). Bhargava and Shankar have shown that a positive proportion of curves over $\mathbb{Q}$ have rank 0, for which

Bhargava won a Fields Medal. Combining their work with that of Skinner and Urban relating to L-functions [90], they showed that a positive proportion of elliptic curves over $\mathbb{Q}$ have analytic rank 0, and so by Kolyvagin's result satisfy part (i) of the Birch–Swinnerton-Dyer conjecture. Evidence for part (i) modulo 2 also exists in the form of parity results, which will be discussed in Section 1.2. Further evidence for this conjecture is the analogous conjecture for abelian varieties over function fields. In this setting the full conjecture follows from finiteness of the ℓ-primary part of Ш, for any prime ℓ. This is known for both elliptic curves [70, 94], and abelian varieties [53].

There is extensive numerical evidence for this conjecture, at least in the case of elliptic curves over $\mathbb{Q}$ with low rank. Part (i) has been verified for all elliptic curves over $\mathbb{Q}$ with conductor less than 140000 (this is 614308 isogeny classes, all with rank at most 3) [29], and the full theorem has been verified for all curves with conductor at most 5000 and analytic rank at most 1 [30, 67]. Keller and Stoll have also been able to verify this for some modular abelian surfaces [54].

Beyond these known cases and the numerical evidence, a key reason to believe the conjecture is a theorem of Cassels [20]. He observed that if A and B are isogenous elliptic curves, then they must have the same rank and the same L-function. He then proved that, while the individual invariants are not preserved by isogenies, the conjectured formula for $\lim_{s\to 1} L(A,s)/(s-1)^{\mathrm{rk}(A/K)}$ will give the same result, i.e. if the conjecture holds for A, it must hold for B. Tate generalised this to abelian varieties [94]. This relationship between the invariants of isogenous varieties has had further applications, as it combines information about the rank with local data, which is easier to compute. One of its most significant applications is towards the proof of the parity conjectures described below. This relation between invariants is one of the main tools we use in Chapter 3 of this thesis.

1.2 Finding the Rank

To find the rank of an abelian variety, one often computes a Selmer group, which gives an upper bound. This upper bound may not be tight, and the difference is

explained by the mysterious Tate–Shafarevich group. Alternatively, we may ask for the parity of the rank (whether it is odd or even), and there is a conjectural result which makes this much easier to compute. These three related objects are the main focus of this thesis.

Selmer Groups

Given an isogeny $f : A \to B$ of abelian varieties, we can define the f-Selmer group of A, $\mathrm{Sel}_f(A/K)$. Formally, this is defined as the kernel of a map

$$H^1(G_K, A[\phi]) \to \prod_{\text{places } v} H^1(G_{K_v}, A)[\phi]$$

(see Section 2.3). It also has an interpretation in terms of coverings of A which are everywhere locally soluble. This was introduced by Cassels in 1962 [17], and named in honour of earlier work by Selmer on the problem of finding the rank of an elliptic curve. Knowing the size of a Selmer group allows us to give an upper bound on the rank. Fortunately, the Selmer group is finite and can be computed, at least in theory and often in practice.

Remark 1.2.1. This finiteness result is part of one proof of the Mordell–Weil theorem. Indeed if we let $A = B$ and f be the multiplication by n isogeny, it shows that $\frac{A(K)}{nA(K)}$ is finite.

Computing the rank of an elliptic curve is usually done by a descent method. This uses Selmer groups to give an upper bound, and a search for points to find a lower bound. The difficulty comes from the fact that the upper bound will not always equal the rank; the difference between them is explained by the Tate–Shafarevich group of A. More precisely, for the isogeny $[n]$, the Selmer group of A has a subgroup isomorphic to $\frac{A(K)}{nA(K)}$, with a quotient isomorphic to the n-torsion in the Tate–Shafarevich group. Working out which part of a Selmer group represents points on the curve, and which part tells us about the Tate–Shafarevich group, is a key problem which would quantify the disparity between this upper bound and the rank. No algorithm to do this in general is known. Computing multiple Selmer groups for different isogenies can give us some more information, but this is still not

guaranteed to give the correct bound, and becomes difficult in practice, especially for higher-dimensional abelian varieties.

In this thesis we will focus on the n-Selmer group of an abelian variety, i.e. the Selmer group corresponding to the multiplication by n isogeny.

Tate–Shafarevich Groups

The Tate–Shafarevich group of an abelian variety A/K is a difficult object to study. It represents a 'gap' in the arithmetic of an abelian variety over a number field compared to the arithmetic of the variety over all the completions of that field. The non-trivial elements can be viewed as homogeneous spaces for the variety, up to isomorphism over K, which have no points over K but have points over the completion K_v at all places v. It therefore measures the failure of a local-to-global principle, since it is trivial when this principle holds for all homogeneous spaces for A. It can also be defined as the kernel of the map

$$H^1(G_K, A) \to \prod_{\text{places } v} H^1(G_{K_v}, A)$$

(see Section 2.2). If we knew the size of the p-part of Ш, then computing the p-Selmer group would tell us the rank. If at least the p-primary part is finite, then by finding the p^n-Selmer groups for large n, we could eventually get the correct bound.

In 1940, Lind [62] was the first to give an example of a homogeneous space representing a non-trivial element of this group, and Selmer [83] gave several more in the 1950s. The group was introduced in its modern sense by Lang–Tate [60] and Shafarevich [82] in the late 1950s. Since at least the 1960s it has been widely believed to be finite (though it is unclear who first conjectured this), and a number of results have been proven conditional on this, including the parity conjecture for elliptic curves [42].

Parity Conjectures

Rather than compute the rank exactly, we can instead look at its parity. There is a conjectural expression for this, which can be seen as the rank part of the Birch–Swinnerton-Dyer conjecture modulo 2. While the Birch–Swinnerton-Dyer conjecture

gives a formula for the rank, it still requires us to understand the L-function, a difficult analytic object which may not even be defined at $s = 1$. One way mathematicians have tried to avoid the L-function issue is to combine it with another conjecture, which predicts that the L-function satsifies a functional equation.

Conjecture 1.2.2 (Hasse–Weil (see [85]))**.** *Let A/K be an abelian variety of dimension n, and let $d = [K : \mathbb{Q}]$. The L-function of A has a meromorphic continuation to $\mathbb{C}$, and satisfies*

$$L^*(A,s) = w(A/K)L^*(A,2-s).$$

Here $w(A/K) \in \{\pm 1\}$ is called the global root number and

$$L^*(A,s) = N_A^{s/2}|\Delta_K|^{ns}(2\pi)^{-nds}\Gamma(s)^{nd}L(A,s),$$

where N_A is the conductor of A and Δ_K the discriminant of K.

As the extra terms linking L and L^* are easily controlled around $s = 1$, we can combine this with the first part of the Birch–Swinnerton-Dyer conjecture to give a result which does not include L-functions. This is a conjecture involving purely arithmetic data, so it may be more approachable both in terms of attempting to prove it, and in terms of using it to predict the parity of the rank.

Conjecture 1.2.3 (Parity)**.** *Let A/K be an abelian variety. Then*

$$(-1)^{\mathrm{rk}(A/K)} = w(A/K).$$

The advantage of this conjecture is that $w(A/K)$ can be calculated in terms of local data, which is often much simpler to understand and calculate than global data. The global root number is a product of local root numbers, which are defined in a non-constructive way in terms of a certain Weil representation. Details can be found in Section 2 of [11]. We will not need the full definition as they have been classified for elliptic curves and most abelian varieties [11, 80], and so can be easily computed from a Weierstrass model of an elliptic curve. This conjecture has many applications, which often come from the fact that when the root number is -1, the

parity conjecture implies that the rank is positive. One such example is a partial solution to the congruent number problem mentioned in Example 1.0.2. Assuming the parity conjecture, one can show that n is a congruent number whenever $n \equiv 5$, 6 or 7 $\pmod 8$. Cowland Kellock and Dokchitser [28] detail this and many more applications.

While there is much numerical evidence for the parity conjecture in the case of elliptic curves, and it is known for the complex multiplication case as both sides have been shown to equal 1, not many general results are known unconditionally. A more approachable equivalent, which is known in a number of cases, is the p-parity conjecture, which replaces the rank of an elliptic curve with information about its p^n-Selmer groups. Given a prime p, we will define a new invariant $\mathrm{rk}_p(A/K)$, the p^∞-Selmer rank, which is equal to $\mathrm{rk}(A/K)$ if $Ш(A/K)$ is finite (more precisiely, they are equal exactly when $Ш(A/K)[p^\infty]$ is finite). For a full definition, see Definition 2.3.3.

Conjecture 1.2.4 (p-Parity)**.** *Let A/K be an abelian variety. Then*

$$(-1)^{\mathrm{rk}_p(A/K)} = w(A/K).$$

It appears that Selmer [84] was the first to consider parities of ranks. He studied 2-descent on certain families of elliptic curves, and conjectured that "The number of generators indicated by a first descent differs from the true number of generators by an even number." This is equivalent to saying that $\mathrm{rk}_2(E/K) \equiv \mathrm{rk}(E/K) \pmod 2$. Birch and Stephens considered p-parity, and proved 2-parity for elliptic curves of the form $y^2 = x^3 - Dx$ in 1966 [9].

In summary, to compute ranks by descent we must compute a Selmer group. This gives an upper bound, which exceeds the rank by an amount determined by $Ш(A/K)$. $Ш(A/K)$ is widely believed to be finite, and if it is then the parity conjecture is true for elliptic curves. In general, all we can prove unconditionally are cases of p-parity, which tell us about the p^n-Selmer groups of abelian varieties instead of their ranks.

Known results

A number of cases of the p-parity conjecture are now known. For elliptic curves, it has been proven in the cases of curves over $\mathbb{Q}$ [41] and other totally real fields [42, 50, 75], and curves over number fields which admit a p-isogeny [22]. For an elliptic curve over a number field K, 2-parity is known over quadratic extensions of K [42, 58, 59], and a similar result is now known for Jacobians of hyperelliptic curves satisfying some local conditions [73].

In the case of elliptic curves E with complex multiplication, we have $\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ equal to an imaginary quadratic field. It follows that the rank is even (see Proposition 3.0.2). In this case, one can also show that the root number $w(E/K)$ is always 1, so the parity conjecture holds. To prove p-parity, we must show that the p^∞-Selmer rank is even. For primes which are inert or ramified in this field, we can view the Selmer groups as modules over the endomorphism ring, and deduce p-parity. The split case is harder; Česnavičius proved it by reducing the problem to a case where he could show that the elliptic curve must admit a p-isogeny, and used his p-parity result for this situation [22].

Less is known for general abelian varieties. For odd primes p, the p-parity conjecture is known for abelian varieties A admitting an isogeny of degree $p^{\dim(A)}$, with some restrictions [27]. For $p = 2$, it is known for principally polarised abelian surfaces with some conditions on the 2-torsion and reduction at 2 [45].

The weaker result that finiteness of Ш implies the parity conjecture is known more generally, including for elliptic curves over all number fields [42], and semistable principally polarised abelian surfaces satisfying local conditions [45].

The known cases of p-parity have had important applications. For instance, Bhargava and Shankar used the case of elliptic curves over $\mathbb{Q}$ (in an alternative form, which states that $\dim_{\mathbb{F}_p}\mathrm{Sel}_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p}E(\mathbb{Q})[p]$ is even if and only if $w(E/\mathbb{Q}) = 1$) to show that a positive proportion of elliptic curves satisfy the Birch–Swinnerton-Dyer conjecture [8].

While we still know little about the Tate–Shafarevich group, there has been some progress. At the time Birch and Swinnerton-Dyer made their conjecture, there

was no known example where Ш was provably finite. The first examples where this could be proven were given by Rubin [81] in 1987, and more are now known due to Kolyvagin. It is however simpler to show that $Ш[p^\infty]$ is finite using descent methods, and this has been done for many elliptic curves ([88] X.5).

In 1962, Cassels discovered a bilinear pairing on Ш for elliptic curves, and proved that it was alternating [18]. From this he could deduce that if Ш is finite, it must have square order, and the same is true of $Ш[p^\infty]$. This has applications, including towards parity results, and will be used in the results of Chapter 4. Tate generalised the pairing to abelian varieties [93]. While it was widely believed that Ш would also have square order in this case, this need not be true, as the pairing may not be alternating. For principally polarised abelian varieties, Flach showed in 1990 that it is skew-symmetric [48]. In 1999, Poonen and Stoll showed that for a principally polarised abelian variety A/K, $Ш(A/K)$ is a square or twice a square (and explained when each occurs) [79]. In 2024 Konstantinou proved that, in general, the order could be n times a square for any square-free n [57].

While the exact size of Ш is hard to determine, a number of results showing that Ш can become arbitrarily large are also known. Cassels showed that there are elliptic curves E over $\mathbb{Q}$ with $Ш(E/\mathbb{Q})[3]$ arbitrarily large [19]. It is conjectured that for all primes p, there is an elliptic curve over $\mathbb{Q}$ such that Ш has an element of order p. It is known that there is such an abelian variety, as a consequence of a result of Kloosterman that for any prime there is an elliptic curve over some number field with Ш having an element of order p [55].

Much research has been done on the behaviour of the Selmer and Tate–Shafarevich groups under field extensions, especially those with dihedral Galois groups. For example, Bartel considered dihedral extensions of $\mathbb{Q}$, and showed that if we fix a prime p and a quadratic number field $M \neq \mathbb{Q}(\sqrt{p})$, there is a dihedral extension $F/\mathbb{Q}$ of order $2p$ containing M, and an elliptic curve $E/\mathbb{Q}$, with $\mathrm{Sel}_p(E/F)$ arbitrarily large [2]. Mazur and Rubin have proven a local formula which tells us about parity in the Selmer groups in D_{2p^n}-extensions F/k, for elliptic curves E/k, and applied this to give a lower bound (under mild local conditions) on $\mathrm{rk}_p(E/F)$

when $\mathrm{rk}_p(E/F^{C_{p^n}})$ is odd [65]. Chetty has proven this local formula is equivalent to the parity conjecture in a number of cases [25]. Vavasour and Wuthrich have shown that in some cases of D_{2p}-extensions F/k, with intermediate quadratic extension K, and elliptic curves E/k, the Galois module structure of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$ is determined by $\mathrm{rk}(E/k)$, $\mathrm{rk}(E/K)$ and local data [95]. They also give a lower bound in some cases for $Ш[p]$ over C_p-extensions of $\mathbb{Q}$. The behaviour of elliptic curves in dihedral extensions has also had applications towards proving parity results [41, 44].

Mazur and Rubin have considered the question of to what extent the Selmer groups determine an elliptic curve. They looked at the family of Selmer groups $\mathrm{Sel}_n(E_d/K)$ for a fixed integer n, where E_d is the quadratic twist of a curve E/K by d. They showed that it is possible for two elliptic curves over K to have the same Selmer groups in this family and not be isogenous [66]. Chiu has shown that if two elliptic curves have the same size Selmer groups $\mathrm{Sel}_p(E/F)$, where F ranges over all finite extensions of K and p over all but finitely many primes, then they must be isogenous [26]. This relies on a result of Faltings, which says that for any prime ℓ, the rational ℓ-adic Tate module determines the isogeny class of an abelian variety.

1.3 Results of the Thesis

In this thesis we will consider isogenies between abelian varieties, and what information we can obtain about Selmer groups from them. We will prove three main results.

The first theorem will be about abelian varieties with complex multiplication. These are abelian varieties which have a large number of self-isogenies. It is known that they have even rank and root number 1. We will use these isogenies to give some information about Ш in this case.

Theorem 1.3.1 (= Theorem 3.0.5)**.** *Let A/K be an abelian variety with complex multiplication, and p a prime. Then there is an even integer δ_p such that*

$$Ш(A/K)[p^\infty] \cong G \times (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p},$$

where G is a finite group.

Once we have defined $\mathrm{rk}_p(A/K)$, it will be clear that this is equivalent to showing that $\mathrm{rk}_p(A/K)$ is even, and hence to the p-parity conjecture.

As mentioned in Section 1.2, Česnavičius has proved this result for elliptic curves. His method does not generalise to abelian varieties as we do not have a corresponding p-parity result for abelian varieties admitting a p-isogeny. We give an alternative proof of this, considering the action of an isogeny and its dual on Ш, which works for all abelian varieties with complex multiplication.

The second main result tells us about the size of Ш assuming its finiteness. It is still hard to give information about the size of Ш for elliptic curves, beyond it being a square. We will consider how the size of Ш behaves under dihedral extensions, which is a setting of interest, as discussed in Section 1.2. We will do this by constucting isogenies between two abelian varieties whose Tate–Shafarevich groups are linked to that of an elliptic curve E over different fields.

Theorem 1.3.2 (= Theorem 4.0.1)**.** *Suppose E/k is an elliptic curve, F/k an extension with Galois group D_{2n} with n odd, and K the quadratic subfield of F. Assume $Ш(E/F)[p^\infty]$ is finite. Then if $p \nmid n$ is prime,*

$$|Ш(E/F)[p^\infty]| \equiv |Ш(E/K)[p^\infty]| \pmod{\mathbb{Q}^{*4}}.$$

We also show similar results for even n, and for the p-part of Ш (Proposition 4.1.4). As Cassels showed that $|Ш(E/F)[p^\infty]|$ is a square, this tells us which of the two cases we are in. When using a p-Selmer group to find the rank of elliptic curves, the method involves determining the p-part of Ш, so we can use this theorem and (assuming finiteness) produce a formula for the rank modulo 4, assuming we know the size of a Selmer group. This sometimes allows us to find the rank of E/F with less calculation done over F (either finding points or proving none exist). Example 4.1.6 shows how this can have an application.

In the same setting we also consider the $\mathrm{Gal}(F/K)$-module structure of $Ш(E/F)$, and prove that, for $p \neq 2$, $Ш(E/F)[p^\infty]$ is isomorphic to $X \oplus X$ for some module X (Theorem 4.2.3). This is analogous to the argument that properties

of the Cassels–Tate pairing imply that Ш has square order. We will show that for certain p and n this gives an alternative proof for Theorem 1.3.2. We then explain why we might expect this to have an application to a parity result for $\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle$, where F is a D_{2pq}-extension, ρ is a representation of D_{2pq}, and $\langle \_, \_ \rangle$ is the usual inner product on representations of D_{2pq}, but show that this method cannot give the desired result.

The final main result of this thesis considers how much Selmer groups and other invariants tell us about the isomorphism class of the abelian variety. Again, we consider dihedral extensions. We use Weil restrictions of curves over these extensions to define two abelian varieties with the same Mordell–Weil and Selmer groups, but unfortunately these examples turn out to be isomorphic, at least for low-degree extensions. However, a related construction gives examples which are not isomorphic.

More precisely, the main result is:

Theorem 1.3.3 (= Theorem 5.0.2)**.** *There exist abelian varieties A and B defined over $\mathbb{Q}$, which are not isomorphic, but over every number field F satisfy*

- $A(F)$ *and* $B(F)$ *are isomorphic groups*
- $\mathrm{Sel}_n(A/F)$ *and* $\mathrm{Sel}_n(B/F)$ *are isomorphic groups for every n*
- $Ш(A/F)$ *and* $Ш(B/F)$ *are isomorphic groups*
- $\mathrm{Reg}(A/F) = \mathrm{Reg}(B/F)$
- $T_\ell A \cong T_\ell B$ *as G_F-modules, where ℓ is any prime and $T_\ell A$ is the Tate module of A.*

This is different to the situation for elliptic curves, where the same list of invariants do determine the isogeny class of elliptic curves over $\mathbb{Q}$ (Corollary 5.3.3), but not over number fields (Theorem 5.3.6). This result is analogous to the work of Mazur, Rubin and Chiu discussed in Section 1.2, which used Selmer groups to determine the isogeny class of an elliptic curve.

1.4 Structure of the Thesis

In Chapter 2 of this thesis, we discuss the background material that will be assumed in later chapters. We will discuss abelian varieties, and their duals and polarisations. Then we give the main results and definitions about the Tate–Shafarevich and Selmer groups of an abelian variety. We give the statement of the Birch–Swinnerton-Dyer conjecture, including the prediction for the residue of the L-function, and explain Cassels' Theorem. Then we discuss twists of abelian varieties, and how we can generate isogenies between them, and finally state some algebraic lemmas which will be useful.

The rest of the thesis is divided into three chapters, one for each of the main theorems discussed in Section 1.3. In Chapter 3 we discuss abelian varieties with complex multiplication. The main result of this chapter is Theorem 1.3.1, p-parity for abelian varieties with complex multiplication. Česnavičius' proof for the elliptic curve case required an application of p-parity, in the case of elliptic curves admitting a p-isogeny; we present a new, simpler proof of p-parity in the complex multiplication case, and generalise it to abelian varieties.

To pass from a Selmer group to information about the Mordell–Weil group, we must attempt to understand the Tate–Shafarevich group. Chapter 4 looks specifically at the Tate–Shafarevich group of elliptic curves over number fields, and how it grows in dihedral extensions. Specifically, we prove Theorem 1.3.2, and a similar result for even n. We show how this can help compute ranks over dihedral extensions of $\mathbb{Q}$. We also discuss the Galois module structure of the Tate–Shafarevich group, and show that the theory of modules allows us to deduce the main result in some cases. In the other cases, the main theorem gives us some information about the module structure. In Section 4.3 we discuss the potential to apply this to a generalisation of the parity conjecture, but show that Brauer relations in D_{2pq} cannot give us the result we hope for.

In Chapter 5 we explore how much Selmer groups and other invariants can tell us about isomorphism classes of abelian varieties. The main result is Theorem 1.3.3. This gives a long list of invariants which does not determine the abelian variety up to

isomorphism. We show this by giving examples, and also give examples showing an equivalent result for elliptic curves over number fields. We prove that, in the setting of elliptic curves over $\mathbb{Q}$, this list of invariants does in fact determine the isomorphism class. We also attempt to construct an example of two non-isomorphic abelian varieties with the same invariants using a Brauer relation in D_{2pq}, but we find instead that the products of Weil restrictions must be isomorphic, at least for small pq.

1.5 Notation

Let K be a number field, L an extension of K and k a subfield of K. Suppose A and B are abelian varieties over K, and $f : A \to B$ an isogeny defined over K. The following table sets out some notation we will use relating to these. Definitions for some terms can be found in Chapter 2 as linked.

$\bar{K}$	The algebraic closure of K
G_K	The Galois group of $\bar{K}/K$
$A(K)$	The points of A defined over K
$A(K)_{\text{tors}}$	The torsion subgroup of A over K
$A[f]$	The kernel of f on A
$A(K)[f]$	The kernel of f on $A(K)$, and similarly for other groups on which f induces a homomorphism
$\hat{A}$	The dual abelian variety of A
$\hat{f}$	The dual isogeny of f
$\tilde{f}$	The conjugate isogeny of f - see Section 2.1.2
$\text{Sel}_n(A/K)$	The n-Selmer group of A/K - see Definition 2.3.1
$Ш(A/K)$	The Tate–Shafarevich group of A/K - see Definition 2.2.1
$Ш_{\text{d}}(A/K)$	The set of divisible elements of $Ш(A/K)$ - see Definition 2.2.2
$Ш_{\text{nd}}(A/K)$	The quotient $Ш(A/K)/Ш_{\text{d}}(A/K)$
δ_p	The multiplicity of $\mathbb{Q}_p/\mathbb{Z}_p$ in $Ш_{\text{d}}(A/K)[p^\infty]$ for a prime p
$f_{A(L)}$	The map induced by f on points of $A(L)$

$f_{Ш}$	The map induced by f on $Ш(A/K)$, and similarly for subgroups and quotients of Ш
$[n]$	The multiplication by n map on an abelian variety or group
$G[n]$	The kernel of $[n]$ on G
$G[n^\infty]$	The union of $G[n^k]$ over positive integers k
C_n	The cyclic group of order n
D_{2n}	The dihedral group of order $2n$
$\mathbb{Z}_{(p)}$	The localisation of $\mathbb{Z}$ at p
$\mathrm{Res}_{K/k}(A)$	The Weil restriction of A from K to k - see Section 2.5
A_L	The base change of A to L
$\mathrm{M}_n(\mathbb{Z})$	The set of $n \times n$ matrices over $\mathbb{Z}$
$\mathrm{GL}_n(\mathbb{Z})$	The subset of $\mathrm{M}_n(\mathbb{Z})$ consisting of matrices with determinant ± 1

If L/K is Galois with Galois group G, and $H \leq G$, let L^H be the fixed field of L under the automorphisms in H. Similarly if ρ is a representation of G, let ρ^H be the fixed part of ρ under the action of H.

Chapter 2

Background Material

This chapter covers the necessary background material to the thesis, and does not contain any new results. We cover the key properties of abelian varieties, their Selmer and Tate–Shafarevich groups, the full form of the Birch–Swinnerton-Dyer conjecture, and the construction of some abelian varieties and isogenies which we will need later.

2.1 Abelian Varieties

Abelian varieties are a generalisation of elliptic curves to higher dimensions. Specifically, an abelian variety is a smooth projective algebraic variety, with a group law where addition and the inverse map are given by morphisms. The Mordell–Weil theorem also holds for abelian varieties.

Theorem 2.1.1. *Let A/K be an abelian variety over a number field. Then*

$$A(K) \cong \mathbb{Z}^{\mathrm{rk}(A/K)} \times A(K)_{\mathrm{tors}},$$

where $\mathrm{rk}(A/K)$ *is a non-negative integer and* $A(K)_{\mathrm{tors}}$ *is finite.*

Many more of the definitions and theorems about elliptic curves have analogues for abelian varieties.

Most of the results in this section can be found in any set of notes on abelian varieties over number fields, for example [71].

2.1.1 The Dual Variety

Given an abelian variety A/K, there is a dual variety of the same dimension, $\hat{A}/K$. This satisfies double duality: $\hat{\hat{A}} \cong A$. It is functorial, that is, if we have an isogeny $f : A \to B$, then there is also an isogeny $\hat{f} : \hat{B} \to \hat{A}$, which is defined over K, and if we have another isogeny $g : B \to C$, then $\widehat{g \circ f} = \hat{f} \circ \hat{g}$. Note that $\deg(\hat{f}) = \deg(f)$ ([38] Section 9).

In the case of elliptic curves, we have $\hat{E} \cong E$, but this is not true in general. This means that some results about elliptic curves do not directly transfer to abelian varieties, and we must replace some copies of a variety with its dual. For example, the Weil pairing on elliptic curves is a map $E[m] \times E[m] \to \mu_m$, where μ_m is the group of m^{th} roots of unity. The analogous pairing for abelian varieties is a map $A[m] \times \hat{A}[m] \to \mu_m$ ([71] Chapter 1 Section 13).

A polarisation of A is an isogeny $\lambda : A \to \hat{A}$, satsifying some additional conditions. The only one of these conditions which will be relevant to this thesis is that $\hat{\lambda}$ (which by the above is also an isogeny $A \to \hat{A}$) is equal to λ ([38] Section 9). All abelian varieties admit a polarisation. Those which admit a polarisation which is an isomorphism are called principally polarisable; this includes elliptic curves.

2.1.2 The Conjugate Isogeny

In the elliptic curve case, dual isogenies have the additional property that, given an isogeny $f : E \to E'$, $\hat{f} \circ f = [\deg(f)]$ (where we implicitly use the principal polarisations to view $\hat{f}$ as an isogeny $E' \to E$ rather than $\hat{E}' \to \hat{E}$). This is not true in general, even when we have a principal polarisation. This is because the degree of $\hat{f} \circ f$ is $\deg(f)^2$, whereas the degree of $[\deg(f)]$ is $\deg(f)^{2\dim(A)}$. The analogous concept is the conjugate isogeny. This is an isogeny $\tilde{f}$ with the property that $\tilde{f} \circ f = [\deg(f)]$ ([38] Section 8).

Because of the existence of the conjugate isogeny, we can invert isogenies in $\mathrm{Hom}_K(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. This allows us to show that $f \circ \tilde{f} \circ f = f \circ [\deg(f)] = [\deg(f)] \circ f$, and by cancelling f we get $f \circ \tilde{f} = [\deg(f)]$ also. Given a polarisation λ, inverting isogenies also allows us to define the Rosati involution on $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ as the map $f \mapsto f^\dagger = \lambda^{-1} \circ \hat{f} \circ \lambda$. The property that $\hat{\lambda} = \lambda$ implies that this is an involution.

2.2 The Tate–Shafarevich Group

The constructions for the Tate–Shafarevich and Selmer groups, and many of their properties, are exactly the same as for elliptic curves, which can be found in [88] Section X.4.

Definition 2.2.1. The Tate–Shafarevich group of an abelian variety A/K is the kernel of the map $H^1(G_K,A) \to \prod_v H^1(G_{K_v},A)$. Equivalently, it is the group of homogeneous spaces (up to K-isomorphism) for A/K that possess a K_v-rational point for every place v of K ([93] Section 3).

The Tate–Shafarevich group is abelian and a torsion group, so can be expressed as a product of its p-primary parts $Ш(A/K)[p^\infty]$. Each of these is of the form $G \times (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$, where G is a finite group and δ_p is an integer (this follows from the fact that $Ш(A/K)[p^n]$ is a finite group for every integer n). It is conjectured that $Ш$ is finite, which would imply that δ_p is always 0. While computing $Ш(A/K)[p^\infty]$ can often be done in practice by descent methods, showing that $Ш$ is finite is much harder.

Definition 2.2.2. The subgroup of divisible elements of $Ш(A/K)$ is the set of elements α for which, given any positive integer N, we can find a $\beta \in Ш(A/K)$ satisfying $N\beta = \alpha$. Denote this set by $Ш_{\mathrm{d}}(A/K)$, and denote $Ш(A/K)/Ш_{\mathrm{d}}(A/K)$ by $Ш_{\mathrm{nd}}(A/K)$.

Remark 2.2.3. We can see that $Ш_{\mathrm{d}}(A/K) \cong \bigoplus_{p \text{ prime}} (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$. If $Ш$ is finite, this is trivial. Note also that $Ш(A/K) \cong Ш_{\mathrm{d}}(A/K) \oplus Ш_{\mathrm{nd}}(A/K)$.

Cassels introduced a pairing on $Ш(E/K)$ for elliptic curves E, now called the Cassels–Tate pairing [18]. This is a map $Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z}$ which is bilinear, alternating and Galois-equivariant. We will denote it by $(\_,\_)$. The kernel on either side is the set of divisible elements of $Ш$, i.e. if $(\alpha,\beta) = 0$ for all β, then $\alpha \in Ш_{\mathrm{d}}(A/K)$. The following is a consequence of this.

Theorem 2.2.4. *If $Ш(E/K)[p^\infty]$ is finite, then it is isomorphic to $G \oplus G$ for some group G (see* [78] *Lemma 4). Therefore if $Ш(E/K)$ is finite, it has square order.*

This conclusion comes from the fact that any finite abelian group with a non-degenerate alternating pairing is of this form, shown in [78] Lemma 4 or [35] Lemma 5.2. This is analogous to the fact that a finite-dimensional vector space with a non-degenerate alternating pairing has even dimension.

Corollary 2.2.5. *If* $Ш(E/K)[p^\infty]$ *is finite, then* $|Ш(E/K)[p]|$ *and* $|Ш(E/K)[p^\infty]|$ *are square.*

For more general abelian varieties a similar pairing exists, though it now takes pairs in $Ш(A/K) \times Ш(\hat{A}/K)$ ([93] Section 3). A choice of polarisation gives a pairing on $Ш(A/K)$, though this is no longer alternating. If it is a principal polarisation then the pairing will at least be skew-symmetric, which implies that the order of $Ш(A/K)$, if finite, is a square or twice a square ([48] Corollary after Theorem 2).

2.3 Selmer Groups

Selmer groups of elliptic curves are discussed in [88] Section X.4. The definitions and exact sequences work in the same way for abelian varieties.

Suppose we have an isogeny $\phi : A \to A'$, defined over K. We have a short exact sequence of G_K-modules

$$0 \to A[\phi] \to A \xrightarrow{\phi} A' \to 0.$$

Taking Galois cohomology, we get the exact sequence

$$0 \to A(K)[\phi] \to A(K) \xrightarrow{\phi} A'(K) \to H^1(G_K, A[\phi]) \to H^1(G_K, A) \xrightarrow{\phi} H^1(G_K, A').$$

From this we get

$$0 \to A'(K)/\phi(A(K)) \to H^1(G_K, A[\phi]) \to H^1(G_K, A)[\phi] \to 0.$$

We can do the same thing for each completion K_v of K. Note that as there is a map

$H^1(G_K,A) \to H^1(G_{K_v},A)$, for each place v we have a map

$$H^1(G_K,A[\phi]) \to H^1(G_K,A)[\phi] \to H^1(G_{K_v},A)[\phi].$$

Definition 2.3.1. The ϕ-Selmer group of A, $\mathrm{Sel}_\phi(A)$ is the kernel of the map

$$H^1(G_K,A[\phi]) \to \prod_{\text{places } v} H^1(G_{K_v},A)[\phi].$$

Theorem 2.3.2. *There is an exact sequence*

$$0 \to A'(K)/\phi(A(K)) \to \mathrm{Sel}_\phi(A) \to Ш(A/K)[\phi] \to 0.$$

If we apply this to the isogeny $[n]$ for some integer n, the left hand term becomes $A(K)/nA(K)$. Computing this allows us to find the rank of $A(K)$, as long as we can find its n-torsion. So computing the Selmer group is of interest. Fortunately, it is finite ([68] Proof of Lemma 2), and effectively computable. It is often also computable in practice, at least in the case of elliptic curves and isogenies of low degree. The difficulty in finding the rank, therefore, is in understanding which subgroup tells us about the points of A, and which quotient is the Tate–Shafarevich group. Without this, what we get is instead an upper bound on the rank of $A(K)$.

It is also useful to consider a family of Selmer groups at once. If $Ш(A/K)[p^\infty]$ is finite, then if we consider $\mathrm{Sel}_{p^n}(A/K)$ as n increases, the exact sequence shows that once n is sufficiently large, it will always increase in size by a factor of $p^{\mathrm{rk}(A)}$ when n increases by 1. In general, it will grow by a factor of $p^{\mathrm{rk}(A/K)+\delta_p}$, which will motivate our definition of the p^∞-Selmer rank $\mathrm{rk}_p(A/K)$.

We can consider this family of Selmer groups by taking direct limits in the exact sequence of Theorem 2.3.2. This gives

$$0 \to A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to \varinjlim_n \mathrm{Sel}_{p^n}(A) \to Ш(A/K)[p^\infty] \to 0.$$

We can then give a definition of $\mathrm{rk}_p(A/K)$.

Definition 2.3.3 (p^∞-Selmer rank)**.** Let A be an abelian variety over a number field K, and let p be a prime. Then

$$\mathrm{rk}_p(A/K) := \dim_{\mathbb{Q}_p}(\mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim_n \mathrm{Sel}_{p^n}(A), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

This construction (a form of Pontryagin duality) is used to give a vector space whose dimension is unaffected by the torsion points or the non-divisible part of Ш. We will show in Section 2.7.2 that this is equal to $\mathrm{rk}(A/K) + \delta_p$, which we can treat as an alternative definition. Throughout we will use the notation

$$X_p(A/K) := \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim_n \mathrm{Sel}_{p^n}(A), \mathbb{Q}_p/\mathbb{Z}_p),$$

and $\mathcal{X}_p(A/K) := X_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We will also use an equivalent for $Ш_{\mathrm{d}}$, and define

$$Y_p(A/K) := \mathrm{Hom}_{\mathbb{Z}_p}(Ш_{\mathrm{d}}(A/K)[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$$

and $\mathcal{Y}_p(A/K) := Y_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We will show in Section 2.7.2 that, as a $\mathbb{Q}_p$-vector space, this has dimension δ_p.

2.4 The Birch–Swinnerton-Dyer Conjecture

Attached to an abelian variety, there is an analytic object called the L-function. This can be defined as a product of local factors at the primes of K, and converges on a right half-plane. It is believed to encode a number of properties of the abelian variety, as conjectured by Birch and Swinnerton-Dyer.

Recall the following definition.

Definition 2.4.1. Given a prime p, the Tate module of an abelian variety A/K is the module $T_\ell A := \varprojlim_n A[\ell^n]$. It is a $\mathbb{Z}_\ell[G_K]$-module. We will also define the vector space $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

The local L-factor is defined in terms of the characteristic polynomial of a Frobenius element on the dual of $V_\ell A$. Its definition is not required for the work presented in this thesis, but is given below for completeness.

Definition 2.4.2. Let A/K be an abelian variety and v a non-archimedean place of K. Then the local L-factor of A at v is $L_v(A,s) := \chi_v(q_v^{-s})^{-1}$, where

$$\chi_v(X) := \det(1 - \sigma_v X | ((V_\ell A)^*)^{I_v}).$$

Here I_v is the inertia group at v, q_v is the size of the residue field of K_v, ℓ is a rational prime not dividing q_v or the Tamagawa number [1] of A at v and $(V_\ell A)^*$ denotes the dual vector space to $V_\ell A$. The element $\sigma_v \in G_{K_v}$ is any choice of Frobenius element.

Definition 2.4.3. The L-function of an abelian variety A/K is

$$L(A,s) := \prod_v L_v(A,s).$$

We now state Conjecture 1.1.1 more precisely:

Conjecture 2.4.4 (Birch–Swinnerton-Dyer [10], Tate [94])**.** *For any abelian variety A over a number field K,*

(i) $L(A,s)$ *has meromorphic continuation to* $\mathbb{C}$*, and has a zero of order* $\mathrm{rk}(A/K)$ *at* $s = 1$.

(ii) $Ш(A/K)$ *is finite.*

(iii) $\lim_{s\to 1} \frac{L(A,s)}{(s-1)^{\mathrm{rk}(A/K)}} = \frac{\mathrm{Reg}(A/K)|Ш(A/K)|\Omega(A/K)}{|A(K)_{\mathrm{tors}}||\hat{A}(K)_{\mathrm{tors}}|} =: \mathrm{BSD}(A/K).$

Here the regulator is defined in terms of the canonical height pairing $\langle \_, \_ \rangle : A(K) \times \hat{A}(K) \to \mathbb{R}$. This is a height function on A, analogous to the canonical height on an elliptic curve, which depends on an element of $\hat{A}$ and is bilinear. The regulator is the determinant of the matrix $(\langle a_i, b_j \rangle)_{i,j}$, where $\{a_i\}$ is a set of generators for $A(K)/A(K)_{\mathrm{tors}}$, and $\{b_j\}$ is a set of generators for $\hat{A}(K)/\hat{A}(K)_{\mathrm{tors}}$. $\Omega(A/K)$ is a volume term, and incorporates data about the abelian variety over local fields. For example, when A is an elliptic curve over $\mathbb{Q}$, it is the product of the Tamagawa numbers at all primes, as well as the real period. In general, it is a product including

[1] The Tamagawa number of A at v is $|A(K_v)/A_0(K_v)|$, where $A_0(K_v)$ is the set of points mapped to the identity component of the special fibre of the Neron model of A.

Tamagawa numbers, a period term at the infinite places, the discriminant of $K/\mathbb{Q}$ and an adjustment for the fact that we do not have a global minimal differential. For full definitions of both of these terms, see [72] Section I.7; in the notation of that chapter the volume term is $\frac{\prod_{v\in S}\mu_v(A,\omega)}{|\mu|^d}$.

As evidence for this conjecture, Cassels showed that if elliptic curves A and B are isogenous over K, then $\mathrm{BSD}(A/K) = \mathrm{BSD}(B/K)$ ([20] Theorem 1.3). This is consistent with the fact that $L(A,s) = L(B,s)$, and shows that if the conjecture holds for A then it also holds for B. Tate generalised this result to abelian varieties ([94] Theorem 2.1). It is not true that the individual terms in the definition of $\mathrm{BSD}(A/K)$ are invariant under isogeny, but their ratios are linked by the kernels and cokernels of the isogeny and its dual on K, on the completions of K and on Ш. More precisely,

Proposition 2.4.5. *Let $f : A \to B$ be an isogeny of abelian varieties over K, and assume $Ш(A/K)$ is finite. Then the following hold:*

(i) $\frac{\mathrm{Reg}(A/K)}{|A(K)_{\mathrm{tors}}||\hat{A}(K)_{\mathrm{tors}}|}\cdot\frac{|B(K)_{\mathrm{tors}}||\hat{B}(K)_{\mathrm{tors}}|}{\mathrm{Reg}(B/K)} = \frac{|\ker(\hat{f}_{\hat{B}(K)})|}{|\mathrm{coker}(\hat{f}_{\hat{B}(K)})|}\cdot\frac{|\mathrm{coker}(f_{A(K)})|}{|\ker(f_{A(K)})|}$.

(ii) $Ш(B/K)$ *is also finite, and* $\frac{|Ш(A/K)|}{|Ш(B/K)|} = \frac{|\ker(f_{Ш})|}{|\ker(\hat{f}_{Ш})|}$.

(iii) $\frac{\Omega(A/K)}{\Omega(B/K)} = \prod_v \frac{|\ker(f_{A(K_v)})|}{|\mathrm{coker}(f_{A(K_v)})|}$, *where the product is taken over all places v of K (note that all but finitely many of the terms are 1).*

Theorem 2.4.6. *Let $f : A \to B$ be an isogeny of abelian varieties over K. Then, independent of finiteness of* Ш*,*

$$\frac{|\ker(\hat{f}_{\hat{B}(K)})|}{|\mathrm{coker}(\hat{f}_{\hat{B}(K)})|}\cdot\frac{|\mathrm{coker}(f_{A(K)})|}{|\ker(f_{A(K)})|}\cdot\frac{|\ker(f_{Ш})|}{|\ker(\hat{f}_{Ш})|}\cdot\prod_v\frac{|\ker(f_{A(K_v)})|}{|\mathrm{coker}(f_{A(K_v)})|} = 1.$$

Therefore if $Ш(A/K)$ *is finite,* $\mathrm{BSD}(A/K) = \mathrm{BSD}(B/K)$.

This form of the result is due to Tate, though not stated explicitly ([94] Theorem 2.1 and discussion). For a more explicit statement see Milne ([72] Proof of Theorem I.7.3).

2.5 Weil Restrictions and Twists of Abelian Varieties

Given an abelian variety A over a number field L, with a subfield K, we can define the Weil Restriction $\mathrm{Res}_{L/K}(A)$. This is an abelian variety defined over K, which satisfies the property that $\mathrm{Res}_{L/K}(A)(S) = A(S \otimes_K L)$ for any K-algebra S; in particular, $\mathrm{Res}_{L/K}(A)(K) = A(L)$. This property uniquely determines $\mathrm{Res}_{L/K}(A)$. It is an abelian variety of dimension $[L:K]\dim(A)$.

Example 2.5.1. It is perhaps easier to understand this concept by way of an example. Suppose E is the elliptic curve over $\mathbb{Q}(i)$ given by $y^2 = x^3 - x$, and we want to find its Weil restriction to $\mathbb{Q}$. We can do this by writing $x = a + bi$, $y = c + di$, where $a, b, c, d \in \mathbb{Q}$. Then the solutions to E over $\mathbb{Q}(i)$ are the solutions to the equation $(c+di)^2 = (a+bi)^3 - (a+bi)$ for rational a, b, c and d. By expanding, we see that the solutions to this are precisely the solutions to

$$\begin{aligned} c^2 - d^2 &= a^3 - 3ab^2 - a \\ 2cd &= 3a^2b - 3b^3 - b \end{aligned}$$

over the rationals. As we have two equations in four variables, we can see that this is a surface over $\mathbb{Q}$, and we can define the group law by substituting into the equations for the group law on E.

In this example E has coefficients in $\mathbb{Q}$, which is the field we are restricting to. This is the context in which we will use Weil restriction, though the same method works in general.

Remark 2.5.2. For our purposes the construction and uniqueness of the Weil restriction will not be very important. We can think of it as an abelian variety over K of dimension $[L:K]\dim(A)$, which satisfies Theorem 2.5.3 and $\mathrm{Res}_{L/K}(A)(K) \cong A(L)$.

Theorem 2.5.3 ([69] Section 1)**.** *Fix a finite extension of number fields L/K, and let A/L be an abelian variety. Let $B = \mathrm{Res}_{L/K}(A)$. Then we have equalities $\Omega(A/L) = \Omega(B/K)$, $\mathrm{Reg}(A/L) = \mathrm{Reg}(B/K)$, $Ш(A/L) \cong Ш(B/K)$, and similarly for the torsion subgroups. It follows that the Birch–Swinnerton-Dyer conjecture holds for A/L if and only if it holds for B/K.*

In the cases we will need, we can also construct these Weil restrictions more explicitly, as a special case of a construction of Milne ([69] Section 2).

Definition 2.5.4. A $\bar{K}/K$ form of an abelian variety A defined over a number field K is an abelian variety A'/K, together with an isomorphism $\psi : A_{\bar{K}} \to A'_{\bar{K}}$, where $A_{\bar{K}}$ is the base change of A to $\bar{K}$.

These forms are in bijection with the group $H^1(G_K, \mathrm{Aut}_{\bar{K}}(A))$, where G_K acts on $\mathrm{Aut}_{\bar{K}}(A)$ by $\phi \mapsto \sigma\phi\sigma^{-1}$. In the case where all the automorphisms of A are defined over K, this becomes the trivial action. The map from forms to cohomology is as follows: given ψ as above and $\sigma \in G_K$, we set $s(\sigma) = \psi^{-1}\sigma\psi\sigma^{-1}$. The map $s : G_K \to \mathrm{Aut}_{\bar{K}}(A)$ is a cocycle.

Suppose we have a $\mathbb{Z}[G_K]$-module M with G_K acting through a finite quotient, with an isomorphism of groups $\psi_M : \mathbb{Z}^n \to M$. Now define $s_M : G_K \to \mathrm{GL}_n(\mathbb{Z})$ by $s_M(\sigma) = \psi_M^{-1}\psi_M^{\sigma}$. Here ψ_M^{σ} is the map given by applying σ to the image of ψ_M; if we view $\mathbb{Z}^n$ as a trivial Galois module this is analogous to the construction of $s(\sigma)$ above. In general, $\mathrm{GL}_n(\mathbb{Z})$ is naturally viewed as a subgroup of $\mathrm{Aut}_{\bar{K}}(A^n)$ for an abelian variety A/K, but note that they are isomorphic when $\mathrm{End}_{\bar{K}}(A) \cong \mathbb{Z}$, as in the case of an elliptic curve without complex multiplication over any number field. Thus s_M can be viewed as a cocycle in $H^1(G_K, \mathrm{Aut}_{\bar{K}}(A^n))$, and so (M, ψ_M) determines a form of A^n, which we will denote $(M \otimes A, \psi_{M\otimes A})$.

The map $(M, \psi_M) \mapsto (M \otimes A, \psi_{M\otimes A})$ extends to a functor. That is, if N is also an n-dimensional $\mathbb{Z}[G_K]$-module with G_K acting through a finite quotient, then a G_K-module homomorphism $\phi : M \to N$ induces a morphism ϕ_A from $M \otimes A$ to $N \otimes A$, which is defined over K. The map is such that $\psi_N^{-1}\phi\psi_M \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$ corresponds to $\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A} \in \mathrm{End}_{\bar{K}}(A^n)$. Where ϕ has finite cokernel, ϕ_A is an isogeny.

Lemma 2.5.5 (= [69] Prop. 6(a))**.** *Suppose M and N are $\mathbb{Z}[G_K]$-modules, isomorphic as groups to $\mathbb{Z}^n$, and on which G_K acts via a finite quotient. Suppose $\phi : M \to N$ is a homomorphism of $\mathbb{Z}[G_K]$-modules with finite cokernel. Then $\phi_A : M \otimes A \to N \otimes A$ is an isogeny defined over K, and its degree is $|\mathrm{coker}(\phi)|^{2\dim(A)}$.*

Remark 2.5.6. The Weil restriction is a special case of this construction. If A is defined over K, and L/K is Galois with Galois group G, then G_K can act via its

quotient $G_K/G_L \cong G$, so any $\mathbb{Z}[G]$-module is also a $\mathbb{Z}[G_K]$-module. Viewing $\mathbb{Z}[G]$ in this way, $\mathrm{Res}_{L/K}(A) = \mathbb{Z}[G] \otimes A$ ([69] Section 2). For a subfield of L given by L^H, where H is a subgroup of G, $\mathrm{Res}_{L^H/K}(A) = \mathbb{Z}[G/H] \otimes A$.

Proposition 2.5.7. *Let L/K be a quadratic extension, with $L = K(\sqrt{d})$. Let E/K be an elliptic curve and E_d its quadratic twist by d (i.e. if $E : y^2 = f(x)$, then $E_d : dy^2 = f(x)$). Then $E \times E_d$ is isogenous to $\mathrm{Res}_{L/K}(E)$ by an isogeny of degree 4.*

Proof. We will construct two $\mathbb{Z}[G_K]$-modules which are related by a map with cokernel size 2, and then use Lemma 2.5.5. Throughout, G_K will act via its quotient $G = \mathrm{Gal}(L/K)$; call the non-trivial element of this group σ.

As above, $\mathrm{Res}_{L/K}(E) = \mathbb{Z}[G] \otimes E$. The module $\mathbb{Z}[G]$ is a rank two $\mathbb{Z}$-module, with σ acting as $M_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ (in the basis $\langle 1, \sigma \rangle$). As in the example in [69] Section 2, we can show that $E_d = \mathbb{Z}_d \otimes E$, where $\mathbb{Z}_d$ is the set $\mathbb{Z}$ viewed as a $\mathbb{Z}[G]$-module with σ acting as multiplication by -1. To do this, use the map $\psi : E \to E_d$ defined over $\bar{K}$ by $(x, y) \mapsto (x, \sqrt{d}y)$. Then the cocycle s (in the notation above) maps σ to the automorphism $[-1]$ on E. Similarly using the natural map $\psi_M : \mathbb{Z} \to \mathbb{Z}_d$, we get the cocycle s_M mapping σ to the multiplication by -1 map on $\mathbb{Z}$. So these maps correspond under the inclusion of $\mathrm{Aut}(\mathbb{Z})$ in $\mathrm{Aut}_{\bar{K}}(E)$, and $E_d = \mathbb{Z}_d \otimes E$.

Therefore $E \times E_d = (\mathbb{Z} \oplus \mathbb{Z}_d) \otimes E$. The module $\mathbb{Z} \oplus \mathbb{Z}_d$ is a rank two $\mathbb{Z}$-module with σ acting as $M_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Take the map from $\mathbb{Z}[G]$ to this module given by the matrix $P = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. This satisfies $PM_1 = M_2P$ so it is a homomorphism of $\mathbb{Z}[G_K]$-modules with cokernel of size $|\det(P)| = 2$. Therefore, by Lemma 2.5.5, we have the required isogeny. □

2.6 Brauer Relations

One key example of the twisting construction in Section 2.5 is the case of Brauer relations. These will allow us to construct isogenies which give us information about Selmer groups and other properties of abelian varieties.

Definition 2.6.1. Given a group G, let S denote the set of formal sums of subgroups of G up to conjugacy. An element $\sum_i H_i - \sum_j H'_j \in S$ is a Brauer relation if $\bigoplus_i \mathbb{Q}[G/H_i] \cong \bigoplus_j \mathbb{Q}[G/H'_j]$ as $\mathbb{Q}[G]$-modules.

This is equivalent to the condition that $\bigoplus_i \mathrm{Ind}_{H_i}^G \mathbf{1} \cong \bigoplus_j \mathrm{Ind}_{H'_j}^G \mathbf{1}$. If we can replace $\mathbb{Q}$ by $\mathbb{Z}_{(\ell)}$ in this definition, call it a $\mathbb{Z}_{(\ell)}$-relation.

Example 2.6.2. Let $G \cong D_6$. This has a subroup C_3 of order 3, and three conjugate subgroups of order two; denote any one of them by C_2. Then G has three irreducible rational representations, the trivial representation $\mathbf{1}$, the sign representation ε, and a two-dimensional representation ρ. We find the decompositions

H	$\mathbb{Q}[G/H]$
1	$\mathbf{1} \oplus \varepsilon \oplus \rho^{\oplus 2}$
C_2	$\mathbf{1} \oplus \rho$
C_3	$\mathbf{1} \oplus \varepsilon$
G	$\mathbf{1}$

and deduce that $\mathbb{Q}[G/1] \oplus \mathbb{Q}[G/G]^{\oplus 2}$ and $\mathbb{Q}[G/C_2]^{\oplus 2} \oplus \mathbb{Q}[G/C_3]$ are isomorphic representations. We can see that

$$1 + 2G - 2C_2 - C_3,$$

and its integer multiples, are the only Brauer relations in G. We will see that this is also a $\mathbb{Z}_{(\ell)}$-relation for any $\ell \neq 3$.

Lemma 2.6.3 ([3] Section 2.1)**.** *Brauer relations occur in all non-cyclic groups. Specifically, they form a lattice with rank equal to the number of conjugacy classes of non-cyclic subgroups.*

This matches what we have observed for D_6, as D_6 has no non-cyclic subgroups other than itself.

We will also want some results on $\mathbb{Z}_{(\ell)}$-relations. These will help us control the degree of isogenies constructed.

Lemma 2.6.4 ([3] Proof of Proposition 3.9)**.** *The lattice of $\mathbb{Z}_{(\ell)}$-relations is saturated in the lattice of Brauer relations. That is, if Θ is a Brauer relation and $n\Theta$ is a $\mathbb{Z}_{(\ell)}$-relation for some non-zero integer n, then Θ is a Brauer relation.*

Definition 2.6.5. Given a prime ℓ, a finite group is ℓ-hypo-elementary if it has a normal Sylow ℓ-subgroup with a cyclic quotient.

Theorem 2.6.6 (Conlon's Induction Theorem ([3] Theorem 3.8))**.** *If H is a non-ℓ-hypo-elementary group, then there is a $\mathbb{Z}_{(\ell)}$-relation in H given by $nH - \sum n_i H_i$, where the H_i are proper subgroups of H and $n \neq 0$.*

Lemma 2.6.7. *Suppose Θ is a Brauer relation in the group D_{2n}, and ℓ a prime which does not divide n. Then Θ is a $\mathbb{Z}_{(\ell)}$-relation.*

Proof. This is shown in the proof of ([3] Proposition 3.9). We reproduce this proof, specialised for the case of D_{2n}, here.

By Lemma 2.6.4, it suffices to show that the rank of the lattice of $\mathbb{Z}_{(\ell)}$-relations is equal to the rank of the lattice of Brauer relations. Each conjugacy class of non-ℓ-hypo-elementary subgroup contains a Brauer relation by Theorem 2.6.6. These are also Brauer relations for D_{2n} by transitivity of induction, and they are linearly independent as each has a unique maximal subgroup which contains all the others. Therefore by Lemma 2.6.3 it suffices to show that the number of conjugacy classes of non-ℓ-hypo-elementary subgroups is equal to the number of conjugacy classes of non-cyclic subgroups of D_{2n}, or that every ℓ-hypo-elementary subgroup is cyclic.

Suppose H is an ℓ-hypo-elementary subgroup of D_{2n} with $\ell \nmid n$. If $\ell \neq 2$, then $\ell \nmid n$ implies that $\ell \nmid |H|$, so the ℓ-Sylow subgroup of H must be trivial and H is cyclic. If $\ell = 2$, then n is odd. Therefore $4 \nmid |H|$ and so H must have a normal subgroup of order 1 or 2. If it is trivial we are done, so assume it has order 2. Let the non-trivial element of this be s, and let r be an element of D_{2n} of order n. If $r^k \in H$, then normality implies $r^k s r^{-k} = s$, but this implies $r^{2k} = 1$, so as n is odd $r^k = 1$. Similarly no element of the form $r^k s$ can be in H except s itself, so $H \cong C_2$. □

Suppose L/K is a Galois extension of fields with Galois group G. Given a Brauer relation in G, $\bigoplus_i \mathbb{Z}[G/H_i]$ is a $\mathbb{Z}[G]$-module, and there is a map of $\mathbb{Z}[G]$-modules to $\bigoplus_j \mathbb{Z}[G/H'_j]$ which is injective so has finite cokernel. Therefore applying Lemma 2.5.5 proves the following:

Lemma 2.6.8. *Suppose L/K is a Galois extension with Galois group G. Consider a Brauer relation $\sum_i H_i - \sum_j H'_j$ in G. Then, given an abelian variety A/K, there exists an isogeny*

$$\prod_i \mathrm{Res}_{L^{H_i}/K}(A) \to \prod_j \mathrm{Res}_{L^{H'_j}/K}(A)$$

defined over K.

If the relation in Lemma 2.6.8 is a $\mathbb{Z}_{(\ell)}$-relation, we have a map of $\mathbb{Z}[G]$-modules with cokernel of order coprime to ℓ. In this case Lemma 2.5.5 tells us that the isogeny produced is of degree coprime to ℓ ([2] Section 4).

2.6.1 Regulator Constants

Given a Brauer relation Θ in a group G, and a self-dual rational representation ρ of G, there is an invariant $\mathcal{C}_\Theta(\rho)$ called the regulator constant. This takes values in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Definition 2.6.9. Let ρ be a self-dual rational representation of a finite group G and $\Theta = \sum_i H_i - \sum_j H'_j$ a Brauer relation in G. Pick a non-degenerate G-invariant bilinear pairing $\langle \_, \_ \rangle$ on ρ taking values in $\mathbb{Q}$. We then define

$$\mathcal{C}_\Theta(\rho) = \frac{\prod_i \det(\frac{1}{|H_i|}\langle \_, \_ \rangle | \rho^{H_i})}{\prod_j \det(\frac{1}{|H'_j|}\langle \_, \_ \rangle | \rho^{H'_j})} \in \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

Here the determinants are taken on some rational basis of the submodule ρ^{H_i}.

If we do the same thing for a $\mathbb{Z}_{(\ell)}$-representation ρ of G such that $\rho \otimes_{\mathbb{Z}_\ell} \mathbb{Q}$ is self-dual, and Θ a $\mathbb{Z}_{(\ell)}$-relation in G, we get a constant defined in $\mathbb{Q}^*/\mathbb{Z}^{*2}_{(\ell)}$, i.e. its ℓ-adic valuation is well-defined. We will also refer to this as a regulator constant.

Lemma 2.6.10 ([39] Corollary 2.18)**.** *Regulator constants are multiplicative in Θ and ρ, i.e. $\mathcal{C}_{\Theta_1+\Theta_2}(\rho) = \mathcal{C}_{\Theta_1}(\rho)\mathcal{C}_{\Theta_2}(\rho)$ and $\mathcal{C}_\Theta(\rho_1 \oplus \rho_2) = \mathcal{C}_\Theta(\rho_1)\mathcal{C}_\Theta(\rho_2)$.*

Example 2.6.11. Take the Brauer relation $1 + 2G - 2C_2 - C_3$ in $G = D_6$, as discussed in Example 2.6.2, and the sign representation (i.e. $\mathbb{Q}$, with elements of order 2 acting as multiplication by -1 and the others acting trivially). Use the pairing $\langle x, y \rangle = xy$.

The fixed part under the action of G or C_2 is trivial, so these give determinant 1. For the trivial subgroup, we need the determinant of the pairing on a basis of $\mathbb{Q}$, for example $\{1\}$. This is clearly 1. For the group C_3, we take the determinant of the same basis but the values of the pairing are divided by 3 so we get $1/3$. Therefore the regulator constant is $3 \pmod{\mathbb{Q}^{*2}}$.

Lemma 2.6.12 ([3] Lemma 3.6)**.** *Let G be a finite group, Θ a $\mathbb{Z}_{(\ell)}$-relation in G and ρ a representation of G. Then* $\mathrm{ord}_\ell(\mathcal{C}_\Theta(\rho)) = 0$.

This will be useful when showing that a Brauer relation is not a $\mathbb{Z}_{(\ell)}$-relation.

2.7 Algebra

This section introduces some miscellaneous algebraic results which will be used.

2.7.1 Products of rings

Lemma 2.7.1 ([87], Chapter II, Section 3, Theorem 1(iii))**.** *Suppose p is a prime, and M a number field. Then we have an isomorphism of rings $M \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_i M_{\mathfrak{p}_i}$, where the $\mathfrak{p}_i$ are the primes lying above p in M.*

We will use this decomposition to study modules over $M \otimes \mathbb{Q}_p$. To do this, we will also need the following results, which we will state in terms of more general rings. All rings are assumed to be commutative rings with unity.

Lemma 2.7.2. *Suppose R and S are rings, and A is a module over $R \times S$. Then $A \cong A_1 \times A_2$ as $R \times S$ modules, where A_1 can be viewed as an R-module and A_2 as an S-module.*

It is simple to check that $A_1 = (1,0)A$ and $A_2 = (0,1)A$ allows us to express A in this way. We view A_1 as an R-module by $ra = (r,0)a$ for all $a \in A_1 \subset A$ and $r \in R$, and similarly for A_2.

Applying this to the case where A is an ideal in $R \times S$ gives another useful result.

Lemma 2.7.3. *Suppose R and S are rings, and I is an ideal in $R \times S$. Then $I = I_1 \times I_2$, where I_1 is an ideal in R and I_2 an ideal in S.*

2.7.2 Pontryagin duality

Pontryagin duality is a type of duality defined on locally compact abelian groups, i.e. abelian topological groups where the topology is Hausdorff and every element has a compact neighbourhood. This includes finite groups (with the discrete topology), as well as $\mathbb{Q}_p$ and $\mathbb{Q}_p/\mathbb{Z}_p$.

Definition 2.7.4. The Pontryagin dual of a group G is the group $\mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{R}/\mathbb{Z})$.

We will only use this in the case of p-groups, so we can replace $\mathbb{R}/\mathbb{Z}$ by $\mathbb{Q}_p/\mathbb{Z}_p$.

Proposition 2.7.5 ([1] Introduction)**.** *The Pontryagin dual of $\mathbb{Q}_p/\mathbb{Z}_p$ is $\mathbb{Z}_p$.*

This duality is an exact contravariant functor. Denote the dual of a group A by A^*, and the dual of a continuous homomorphism f by f^*. Given a continuous homomorphism $f : A \to B$, we can apply exactness to the tautological exact sequence

$$0 \to \ker(f) \to A \to B \to \mathrm{coker}(f) \to 0$$

to show the following:

Lemma 2.7.6. *Suppose $f : A \to B$ is a continuous homomorphism. Then* $\mathrm{coker}(f^*) \cong (\ker(f))^*$.

Proposition 2.7.7. *Given an abelian variety A/K and a prime p, we have* $\mathrm{rk}_p(A/K) = \mathrm{rk}(A/K) + \delta_p$.

Proof. We begin with the exact sequence

$$0 \to A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to \varinjlim_n \mathrm{Sel}_{p^n}(A) \to Ш(A/K)[p^\infty] \to 0$$

from Section 2.3, and take Pontryagin duals. This gives an exact sequence

$$0 \to (Ш(A/K)[p^\infty])^* \to X_p(A/K) \to (A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p))^* \to 0,$$

as in this case the continuous homomorphisms are the $\mathbb{Z}_p$-linear ones.

The group $A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$ is a product of a finite group and $(\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rk}(A/K)}$. Its Pontryagin dual is therefore a product of a finite group and $\mathbb{Z}_p^{\mathrm{rk}(A/K)}$ by Proposition 2.7.5. Similarly $Ш(A/K)[p^\infty]$ is a product of a finite group and $(\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$, so its dual is a product of a finite group and $\mathbb{Z}_p^{\delta_p}$. Continuity of the maps implies that this is an exact sequence of $\mathbb{Z}_p$-modules. We now take a tensor product with $\mathbb{Q}_p$, which preserves exactness. This gives

$$0 \to \mathbb{Q}_p^{\delta_p} \to \mathcal{X}_p(A/K) \to \mathbb{Q}_p^{\mathrm{rk}(A/K)} \to 0$$

and the result follows. □

Note also that this argument shows that $\dim_{\mathbb{Q}_p}(\mathcal{Y}_p(A/K)) = \delta_p$, as the result depends only on the divisible part of Ш.

Chapter 3

Abelian Varieties with Complex Multiplication

In this chapter, we prove that the p-parity conjecture holds for abelian varieties with complex multiplication. The content of this chapter is based on my paper *p^∞-Selmer ranks of CM Abelian Varieties*, published at [4].

Introduction

The endomorphism ring of an elliptic curve E always contains a copy of $\mathbb{Z}$, as multiplication by a non-zero integer n is always an isogeny. If there are more endomorphisms, we say E has complex multiplication. In some ways these curves are easier to work with. Results such as modularity have been proven much sooner for these curves. They also have applications, for example in constructing ray class fields of imaginary quadratic fields.

Throughout this chapter we use 'complex multiplication' or 'CM' to mean complex multiplication defined over K, rather than over $\bar{K}$.

Example 3.0.1. Let $K = \mathbb{Q}(i)$ and E/K be given by $y^2 = x^3 - x$. Then there is an endomorphism $[i] : (x,y) \mapsto (-x, iy)$. We call this map $[i]$ because $[i]^2 = [-1]$. In fact, $\mathrm{End}_K(E) \cong \mathbb{Z}[i]$.

For an elliptic curve with complex multiplication, the endomorphism algebra will always be isomorphic to an order in the ring of integers of an imaginary quadratic

field L, that is, a subring $\mathcal{O}$ which is a lattice and spans L over $\mathbb{Q}$. We say the elliptic curve has complex multiplication by L or, more specifically, by $\mathcal{O}$.

A useful example of elliptic curves with complex multiplication being easier to control is the following well-known result.

Proposition 3.0.2. *Elliptic curves with complex multiplication always have even rank.*

Proof. Suppose E/K has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field L. Consider the $\mathbb{Q}$-vector space $E(K)\otimes_{\mathbb{Z}}\mathbb{Q}$. Its dimension is $\mathrm{rk}(E/K)$. Now $E(K)\otimes_{\mathbb{Z}}\mathbb{Q}$ is also a vector space over $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}=L$, and as $[L:\mathbb{Q}]=2$, its dimension over $\mathbb{Q}$ will be twice its dimension over L. Hence $\mathrm{rk}(E/K)$ is even. □

We can check on LMFDB [63] that the curve in Example 3.0.1 has rank 0.

It is not hard to prove that these curves also have root number 1 ([22], Prop. 6.3), so they satisfy the parity conjecture. We might hope that there is an analogous result for Selmer groups, i.e. that the p^∞-Selmer ranks are even, and hence the curves satisfy the p-parity conjecture. This is in fact true ([22] Theorem 1.6), however it is not so easy to prove. In this paper we will present a new proof of this result, and generalise it to abelian varieties (Theorem 3.0.5).

Remark 3.0.3. One might hope to find a simple proof of this, similar to the proof that their ranks are even. After all, we again need to find the rank of a vector space on which $\mathrm{End}_K(E)$ acts. However this does not work. To see why, note that the p^∞-Selmer rank can be defined as the rank of a $\mathbb{Q}_p$-vector space $\mathcal{X}$. Suppose as before that $\mathrm{End}_K(E)=\mathcal{O}$, an order in an imaginary quadratic field L. Previously, we used the fact that a $\mathbb{Q}$-vector space on which $\mathcal{O}$ acts must have even dimension, but this fails when we replace $\mathbb{Q}$ by $\mathbb{Q}_p$. For example, suppose $p=5$ and $L=\mathbb{Q}(i)$. Then L can act on a 1-dimensional $\mathbb{Q}_p$-vector space, as i can act as a square root of -1 in $\mathbb{Q}_5$. This proof does work when p is inert or ramified in L, as we do then find that $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}_p$ is a quadratic extension of $\mathbb{Q}_p$, but for the case when p splits in L, we will need another proof.

Recall the following alternative definition from Section 2.3. This is the definition we will work with in this chapter.

Definition 3.0.4 (p^∞-Selmer rank)**.** Suppose we have an abelian variety A over a number field K. Looking at its Tate–Shafarevich group $Ш(A/K)$, we find its p-primary part is isomorphic to (finite group) $\times (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p}$ for some integer δ_p. We will define the p^∞-Selmer rank to be $\mathrm{rk}_p(A/K) = \mathrm{rk}(A/K) + \delta_p$.

The aim of this chapter is to prove the following:

Theorem 3.0.5. *Suppose A/K is an abelian variety with complex multiplication (see Definition 3.0.9), and p a prime. Then $\mathrm{rk}_p(A/K)$ is even.*

The proof of Proposition 3.0.2 generalises to abelian varieties, so $\mathrm{rk}(A/K)$ is even. Therefore Theorem 3.0.5 is equivalent to the statement that the divisible part of $Ш(A/K)$ has even $\mathbb{Z}_p$-corank, i.e. δ_p is even. This is in fact expected to be 0, as $Ш(A/K)$ is conjectured to be finite.

Another reason to expect Theorem 3.0.5 to hold is the p-parity conjecture, which states that for an abelian variety A over a number field K, with root number $w(A/K)$,

$$(-1)^{\mathrm{rk}_p(A/K)} = w(A/K).$$

In the complex multiplication case, the root number is 1 ([69], Remark 2 after Theorem 4), so Theorem 3.0.5 is equivalent to the p-parity conjecture for abelian varieties with complex multiplication. The conjecture is known in the case where A is an elliptic curve over a number field admitting a p-isogeny thanks to T. and V. Dokchitser ([42] Corollary 5.8) and Česnavičius ([22] Theorem 1.4). Česnavičius then observed that, if A has complex multiplication, we can assume A has complex multiplication by a ring of integers $\mathcal{O}_L$, as any elliptic curve with complex multiplication by L is isogenous to one with complex multiplication by $\mathcal{O}_L$, and this preserves root numbers and rk_p. He showed that in the case where p splits, this curve admits a p-isogeny, and so it follows that for elliptic curves with complex multiplication, $\mathrm{rk}_p(A/K)$ is even. However there is no equivalent p-parity result to use for abelian varieties, so we must use a different method.

While we consider CM defined over K, one can also consider abelian varieties with CM defined over $\bar{\mathbb{Q}}$. In this setting, the p-parity conjecture has been proven for elliptic curves over totally real K, but is open in general. For $p \neq 2$ this is due to Nekovář ([74], Theorem 5.10) and for $p = 2$ Green and Maistret ([50], Theorem 6.5).

From Theorem 3.0.5 we can deduce the following:

Corollary 3.0.6. *Suppose A and p are as in Theorem 3.0.5. If $Ш(A/K)[p^\infty]$ is infinite, then it contains $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.*

Corollary 3.0.7. *Suppose A/K is a principally polarised abelian variety and $p \neq 2$ is a prime. Then $\dim_{\mathbb{F}_p} Ш(A/K)[p]$ is even.*

This follows from the fact that the Cassels–Tate pairing on $Ш_{\mathrm{nd}}(A/K)[p^\infty]$ is alternating, so $Ш_{\mathrm{nd}}(A/K)[p]$ has even dimension. $Ш_{\mathrm{d}}(A/K)[p]$ has dimension δ_p which is even by Theorem 3.0.5.

Notation

Throughout this chapter, let A and B be abelian varieties over a number field K and let $\lambda : A \to \hat{A}$ be some polarisation of A defined over K.

Recall from Section 2.3 the notation $Y_p(A/K)$ for $\mathrm{Hom}(Ш_{\mathrm{d}}[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$, the Pontryagin dual of $Ш_{\mathrm{d}}[p^\infty]$. Let $\mathcal{Y}_p(A/K) = Y_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note that this is a $\mathbb{Q}_p$-vector space of dimension δ_p, and an $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$-module.

Definition 3.0.8 (CM field)**.** A CM field is a totally complex field with an index two totally real subfield.

Definition 3.0.9 (CM abelian variety ([23] Definition 1.3.8.1))**.** A CM abelian variety over a number field K is an abelian variety A/K where $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ has a subalgebra P which is a product of CM fields and satisfies $[P : \mathbb{Q}] = 2\dim(A)$, together with a fixed embedding $P \hookrightarrow \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

For an element α of a CM field M, denote its complex conjugate by $\bar{\alpha}$. This is well-defined by the properties of M.

Note that we only consider complex multiplication defined over K, not over $\bar{K}$ (which is sometimes called potential complex multiplication).

3.1 Self-isogenies

Suppose A and B are abelian varieties over a number field K, and $f : A \to B$ an isogeny between them which is defined over K.

Recall the following theorem discussed in Section 2.4, which implies Cassels' Theorem.

Theorem 3.1.1 ([72], Proof of I.7.3, I.7.3.1)**.** *There is some finite set S of places of K such that*

$$\prod_{v \in S} \frac{|\ker(f_{A(K_v)})|}{|\mathrm{coker}(f_{A(K_v)})|} = \frac{|\ker(f_{A(K)})|}{|\mathrm{coker}(f_{A(K)})|} \cdot \frac{|\mathrm{coker}(\hat{f}_{\hat{B}(K)})|}{|\ker(\hat{f}_{\hat{B}(K)})|} \cdot \frac{|\ker(\hat{f}_{Ш})|}{|\ker(f_{Ш})|}.$$

Corollary 3.1.2. *Suppose that $A = B$, i.e. f is a self-isogeny. Then*

$$|\ker(\hat{f}_{Ш})| = |\ker(f_{Ш})|.$$

Proof. In the formula in theorem 3.1.1, the left hand side is equal to the ratio of the volume terms $\Omega(A/K)$ and $\Omega(B/K)$ which appear in the formula for $\frac{L^{(r)}(A,1)}{r!}$ predicted by the Birch–Swinnerton-Dyer conjecture (see [72] Section I.7 for a full definition; in the notation of that chapter the volume term is $\frac{\prod_{v \in S} \mu_v(A,\omega)}{|\mu|^d}$). These depend only on A and not f so when $A = B$, this is 1.

Similarly, the next two terms equal the ratio of the regulators of A and B and the orders of their torsion subgroups. Specifically,

$$\frac{|\ker(f_{A(K)})|}{|\mathrm{coker}(f_{A(K)})|} \cdot \frac{|\mathrm{coker}(\hat{f}_{\hat{B}(K)})|}{|\ker(\hat{f}_{\hat{B}(K)})|} = \frac{\mathrm{Reg}(B/K)|A(K)_{\mathrm{tors}}||\hat{A}(K)_{\mathrm{tors}}|}{\mathrm{Reg}(A/K)|B(K)_{\mathrm{tors}}||\hat{B}(K)_{\mathrm{tors}}|},$$

therefore when $A = B$ this is also 1. □

The following variant of this result will be useful.

Lemma 3.1.3. *Suppose f is a self-isogeny, and p any prime. Then*

$$|\ker(\hat{f}_{Ш[p^\infty]})| = |\ker(f_{Ш[p^\infty]})|.$$

Proof. For any prime p, the p-adic valuations of the kernels in Corollary 3.1.2 must be equal. As both kernels decompose as a product over primes l of their l-primary subgroups, the p-part of each side comes from $Ш[p^\infty]$, so we can replace Ш by $Ш[p^\infty]$ and still have equality. □

Lemma 3.1.4. *Suppose f is a self-isogeny. Then we can split the kernels into divisible and non-divisible parts. Specifically,*

$$|\ker(\hat{f}_{Ш_{\mathrm{d}}[p^\infty]})||\ker(\hat{f}_{Ш_{\mathrm{nd}}[p^\infty]})| = |\ker(f_{Ш_{\mathrm{d}}[p^\infty]})||\ker(f_{Ш_{\mathrm{nd}}[p^\infty]})|.$$

Proof. We will show $|\ker(f_{Ш[p^\infty]})| = |\ker(f_{Ш_{\mathrm{d}}[p^\infty]})||\ker(f_{Ш_{\mathrm{nd}}[p^\infty]})|$ and similarly for $\hat{f}$. This holds by an application of the snake lemma to the exact sequence

$$0 \to Ш_{\mathrm{d}}[p^\infty] \to Ш[p^\infty] \to Ш_{\mathrm{nd}}[p^\infty] \to 0$$

with the isogeny f, which is valid because f maps $Ш_{\mathrm{d}}[p^\infty]$ to $Ш_{\mathrm{d}}[p^\infty]$. We can also see that $|\mathrm{coker}(f_{Ш_{\mathrm{d}}[p^\infty]})| = 1$, because f has a conjugate isogeny $\tilde{f} : A \to A$. This has the property that $f \circ \tilde{f} = [\deg(f)]$, and multiplication by an integer is surjective on $Ш_{\mathrm{d}}[p^\infty]$. Therefore f is surjective on $Ш_{\mathrm{d}}[p^\infty]$, and the same is true for $\hat{f}$, so the result follows. □

Lemma 3.1.5. *Let A/K be an abelian variety, p a prime, and $f : A \to A$ an isogeny defined over K. Then*

$$|\ker(\hat{f}_{Ш_{\mathrm{d}}[p^\infty]})| = |\ker(f_{Ш_{\mathrm{d}}[p^\infty]})|.$$

Proof. By the functoriality and non-degeneracy of the Cassels-Tate pairing on $Ш_{\mathrm{nd}}$,

$$|\ker(\hat{f}_{Ш_{\mathrm{nd}}[p^\infty]})| = |\mathrm{coker}(f_{Ш_{\mathrm{nd}}[p^\infty]})|$$

([72], proof of I.7.3). Now $|\mathrm{coker}(f_{Ш_{\mathrm{nd}}[p^\infty]})|$ and $|\ker(f_{Ш_{\mathrm{nd}}[p^\infty]})|$ are equal, because $Ш_{\mathrm{nd}}[p^\infty]$ is a finite group. So the non-divisible parts of the equation in Lemma 3.1.4 cancel out, and we have equality of the divisible parts. □

3.2 Complex Multiplication

Recall $Y_p(A/K) := \mathrm{Hom}(Ш_{\mathrm{d}}[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathcal{Y}_p(A/K) := Y_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note this is an $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$-module. For ϕ a self-isogeny of A, denote the map induced on $Y_p(A/K)$ by ϕ_{Y_p}, and similarly if $\phi \in \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$, denote the map induced on $\mathcal{Y}_p(A/K)$ by $\phi_{\mathcal{Y}_p}$.

Definition 3.2.1 (Rosati involution)**.** For an abelian variety A with polarisation λ, the Rosati involution is the involution on $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ sending f to $f^\dagger := \lambda^{-1} \circ \hat{f} \circ \lambda$. We extend this by continuity to $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

Lemma 3.2.2. *Suppose A/K is a polarised abelian variety, p a prime, and ϕ an invertible element of* $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$*. Then*

$$\mathrm{ord}_p \det(\phi_{\mathcal{Y}_p}) = \mathrm{ord}_p \det(\phi^\dagger_{\mathcal{Y}_p}).$$

Proof. We prove this for the case where ϕ is an isogeny of A defined over K, as opposed to a $\mathbb{Q}_p$-linear combination of these, and the full result follows by linearity. By Lemma 2.7.6,

$$|\ker(\phi_{Ш_{\mathrm{d}}[p^\infty]})| = |\mathrm{coker}(\phi_{Y_p})|.$$

Now ϕ_{Y_p} can be represented over $\mathbb{Z}_p$ by a matrix P in Smith normal form, with all diagonal entries non-zero. Then

$$\mathrm{ord}_p \det(\phi_{\mathcal{Y}_p}) = \mathrm{ord}_p \det(P) = \mathrm{ord}_p |\mathrm{coker}(\phi_{Y_p})|.$$

It therefore follows from Lemma 3.1.5 that

$$\mathrm{ord}_p \det(\phi_{\mathcal{Y}_p}) = \mathrm{ord}_p \det(\hat{\phi}_{\mathcal{Y}_p}).$$

Now as $\hat{\phi} = \lambda \circ \phi^\dagger \circ \lambda^{-1}$, $\phi^\dagger_{\mathcal{Y}_p}$ will have the same determinant, and the result follows. □

Lemma 3.2.3. *It suffices to prove Theorem 3.0.5 in the case where*

- $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q} \supset M$*, where M is a CM field and* $[M : \mathbb{Q}] = 2\dim(A)$

- *The Rosati involution corresponds to complex conjugation on M.*

Proof. By [23] Propositions 1.3.2.1 and 1.3.6.4, if A is a CM abelian variety then, for each simple component A_i of A, $\mathrm{End}_K(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM field. Then by [23] Lemma 1.3.5.4, the Rosati involution corresponds to complex conjugation on this field, so A_i satisfies the properties given in the lemma. Now $\mathrm{rk}_p(A/K) = \sum_i \mathrm{rk}_p(A_i/K)$, so once we have proven that the conclusion of Theorem 3.0.5 holds for each A_i, we know it holds for A also. □

Suppose from now on that A/K satisfies the two conditions in the statement of Lemma 3.2.3, and let the fixed field of complex conjugation on M be L.

Now $\mathcal{Y}_p(A/K)$ is an $M \otimes_{\mathbb{Q}} \mathbb{Q}_p$-module. Recall that $M \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is isomorphic to $\prod_{\mathfrak{p}|p} M_{\mathfrak{p}}$, where the product is over primes $\mathfrak{p}$ of M lying above p, and $M_{\mathfrak{p}}$ is the completion of M at $\mathfrak{p}$. We can therefore decompose $\mathcal{Y}_p(A/K)$ into a sum of $\mathbb{Q}_p$-vector spaces

$$\mathcal{Y}_p(A/K) = \bigoplus_{\mathfrak{p}|p} V_{\mathfrak{p}},$$

where each $V_{\mathfrak{p}}$ is an $M_{\mathfrak{p}}$-vector space, using Lemma 2.7.2.

Lemma 3.2.4. *For each prime $\mathfrak{p}|p$, we have*

$$\dim_{\mathbb{Q}_p} V_{\mathfrak{p}} = \dim_{\mathbb{Q}_p} V_{\bar{\mathfrak{p}}}.$$

Proof. If $\mathfrak{p} = \bar{\mathfrak{p}}$, we are done, so suppose they are not equal. Then define α to be the element of $M \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\mathfrak{p}|p} M_{\mathfrak{p}}$ which corresponds to p in $M_{\mathfrak{p}}$ and 1 in all the other factors. Now we can view α as an element of $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$. Then

$$\mathrm{ord}_p \det(\alpha_{\mathcal{Y}_p(A/K)}) = \mathrm{ord}_p \det(p|V_{\mathfrak{p}}) = \dim_{\mathbb{Q}_p} V_{\mathfrak{p}}.$$

Now by assumption, $\alpha^\dagger$ acts as $\bar{\alpha}$. It therefore acts as the identity on $V_{\mathfrak{q}}$ for $\mathfrak{q} \neq \bar{\mathfrak{p}}$, and as multiplication by p on $V_{\bar{\mathfrak{p}}}$. So by the same argument we have

$$\mathrm{ord}_p \det(\alpha^\dagger_{\mathcal{Y}_p(A/K)}) = \dim_{\mathbb{Q}_p} V_{\bar{\mathfrak{p}}},$$

and by Lemma 3.2.2 the result follows. □

Proof of Theorem 3.0.5. It suffices to show that $\dim_{\mathbb{Q}_p}\mathcal{Y}_p(A/K) = \sum_{\mathfrak{p}|p}\dim_{\mathbb{Q}_p}V_{\mathfrak{p}}$ is even. Let L be the fixed field of complex conjugation on M. If $\mathfrak{p}$ is inert or ramified in M/L, then $[M_{\mathfrak{p}} : \mathbb{Q}_p]$ is even. Therefore

$$\dim_{\mathbb{Q}_p}V_{\mathfrak{p}} = [M_{\mathfrak{p}} : \mathbb{Q}_p]\dim_{M_{\mathfrak{p}}}V_{\mathfrak{p}}$$

is also even.

For the primes $\mathfrak{p}$ which split in M/L, we have $\mathfrak{p} \neq \bar{\mathfrak{p}}$, and, by Lemma 3.2.4,

$$\dim_{\mathbb{Q}_p}V_{\mathfrak{p}} = \dim_{\mathbb{Q}_p}V_{\bar{\mathfrak{p}}}.$$

Thus $\sum_{\mathfrak{p}|p}\dim_{\mathbb{Q}_p}V_{\mathfrak{p}}$ is even, and so is $\mathrm{rk}_p(A/K)$. □

Remark 3.2.5. A similar argument can also be applied directly to p^∞-Selmer groups instead of $Ш_{\mathrm{d}}$. Recall the notation $X_p(A/K) = \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(A/K), \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathcal{X}_p(A/K) = X_p(A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note that the $\mathbb{Q}_p$-rank of $\mathcal{X}_p(A/K)$ is $\mathrm{rk}_p(A/K)$. Then replace Corollary 3.1.2 with Theorem 4.3 from [41]. This tells us that for any self-isogeny ϕ, $Q(\phi) = Q(\hat{\phi})$, where, for an isogeny $\psi : A \to B$,

$$Q(\psi) := |\mathrm{coker}(\psi : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}})||\ker(\psi_{Ш_d})|.$$

Section 2 of [40] tells us that

$$\mathrm{ord}_p Q(\phi) = \mathrm{ord}_p|\mathrm{coker}(\phi : X_p(A/K) \to X_p(A/K))|.$$

By the same arguments as in the proof of Lemma 3.2.2, with Y_p and $\mathcal{Y}_p$ replaced by X_p and $\mathcal{X}_p$, we can show that for any invertible $\phi \in \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p$,

$$\mathrm{ord}_p\det(\phi_{\mathcal{X}_p}) = \mathrm{ord}_p\det(\hat{\phi}_{\mathcal{X}_p}) = \mathrm{ord}_p\det(\phi^\dagger_{\mathcal{X}_p}).$$

Here $\phi_{\mathcal{X}_p}$ denotes the map on $\mathcal{X}_p$ induced by ϕ. Then, by an argument similar to Lemma 3.2.4 and the proof of Theorem 3.0.5, $\mathrm{rk}_p(A/K) = \dim_{\mathbb{Q}_p}(\mathcal{X}_p(A/K))$ is

even.

Remark 3.2.6. The complex multiplication assumption can be weakened. Suppose A is an abelian variety with $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q} \supset M$, for some field M, and suppose the Rosati involution induces a non-trivial automorphism on M. Then we can still show that $\mathrm{rk}_p(A)$ is even. Denote this automorphism by $\phi \mapsto \bar{\phi}$, and its fixed field plays the role of L. Then the proof proceeds in the same way. This includes the case of simple abelian varieties whose endomorphism algebras (over K) are of Albert type IV (see [38], Theorem 9.6). The conclusion of Theorem 3.0.5 also holds for products of these.

Chapter 4

The Tate–Shafarevich Group in Dihedral Extensions

In this chapter, we provide a formula for the size of the Tate–Shafarevich group of an elliptic curve over a D_{2n}-extension of its base field, modulo 4^{th} powers and primes dividing n. We also consider its Galois module structure, and an application to computing the rank of the elliptic curve. The content of this chapter is based on the paper *A note on the growth of Sha in dihedral extensions*, published at [5].

Introduction

Computing the Tate–Shafarevich group of an elliptic curve is a difficult problem. It is conjectured to be finite, though this is not known for curves of analytic rank greater than 1. The main result about its size is due to Cassels, who proved that if it is finite, it must have square order ([18] Theorem 1.1). This has some applications, for example to the parity conjecture, so we might hope that knowing the size of Ш more precisely could allow us to say more about parity. This will be discussed in Section 4.3. Knowing the size of Ш can also help extract the rank of an elliptic curve from a Selmer group. Example 4.1.6 will show how this can help compute a rank quickly, conditional on finiteness of Ш.

Elliptic curves over dihedral extensions of the base field have been of interest for a number of reasons. Dihedral extensions can be used to prove that finiteness of Ш implies the parity conjecture for elliptic curves, with the order of Ш being

a key ingredient in this proof. In the D_{2p^n} case, Mazur and Rubin were able to give an expression for the rank of the ρ part of the p^∞-Selmer group of E, where ρ is a representation of D_{2p^n}, in terms of local data ([65] Theorem A). In a field extension, the Galois module structure of Ш and the Cassels–Tate pairing on it can place constraints on the size of Ш. In this chapter, we show that under some circumstances we can determine the order of Ш modulo 4^{th} powers, in terms of the order of Ш over smaller number fields. More precisely, we prove the following:

Theorem 4.0.1. *Let E be an elliptic curve over a number field k and F/k a dihedral extension of degree $2n$. Let p be a prime not dividing n and assume $Ш(E/F)[p^\infty]$ is finite* [1]*. Then*

- *if n is odd, and K is the quadratic extension of k contained in F, then there is an integer t such that*
$$\frac{|Ш(E/F)[p^\infty]|}{|Ш(E/K)[p^\infty]|} = p^{4t}.$$
- *if n is even, and K_1, K_2 and K_3 are the three quadratic extensions of k contained in F, then there is an integer t such that*
$$\frac{|Ш(E/F)[p^\infty]|}{|Ш(E/K_1)[p^\infty]||Ш(E/K_2)[p^\infty]||Ш(E/K_3)[p^\infty]|} = p^{4t}.$$

In some cases, this can be done purely from the Galois module structure, by an argument combining the Cassels–Tate pairing with the action of the Galois group. However, to prove this in all cases we need another method, and constructing isogenies will give that method.

The following remarks show why these conditions are required. As computing the exact order of Ш is difficult, for the sake of examples we use the analytic order of Ш, which is the order predicted by the Birch–Swinnerton-Dyer conjecture. The data for the number fields and curves over $\mathbb{Q}$ comes from LMFDB [63].

Remark 4.0.2. Although the conclusion for odd n compares two Tate–Shafarevich groups in a cyclic extension F/K, we do need this to be contained in a dihedral

[1] Note that $Ш[p^\infty]$ is finite over subfields of F by [41] Remark 2.10.

extension to get the result – it is not true for all cyclic extensions. For example, over the extension of $\mathbb{Q}$ given by adjoining a root of $x^3 - x^2 - 2x + 1$, which is cyclic of degree 3, consider the curve $y^2 + y = x^3 - x^2 - 10x - 20$ (LMFDB label 11.a2). Using Magma [15], we can calculate the analytic order of Ш over this extension. We find it is equal to 25, whereas $Ш(E/\mathbb{Q})$ is trivial. Therefore the 5^∞-part of Ш changes by a non-fourth-power.

Remark 4.0.3. The conclusion also does not hold if $p|n$. For example, take the curve $y^2 + xy + y = x^3 - 351233x - 80149132$ (LMFDB label 210.b1) over the number field given by adjoining a root of $x^6 - 30x^4 + 225x^2 - 200$, which is a D_6-extension of $\mathbb{Q}$. The analytic order of Ш is 4 over the quadratic extension and $2^{10}3^6$ over the D_6-extension [15]. This is equal to $2^8 3^6$ times the order of Ш over the quadratic extension, so the 3^∞-part changes by a non-fourth-power.

We can also say something about the Galois module structure of Ш. This is based on a lemma of Chetty, which he used in studying the structure of Ш for abelian varieties with endomorphisms other than multiplication by an integer, e.g. those with complex multiplication [24].

Theorem 4.0.4. *Suppose E, k, F, n and p are as in Theorem 4.0.1, and K is a quadratic subextension of F/k with $H := \mathrm{Gal}(F/K) \cong C_n$. Suppose also that p is odd. Assume that $Ш(E/F)[p^\infty]$ is finite. Then, as $\mathbb{Z}_p[H]$-modules, $Ш(E/F)[p^\infty] \cong X \oplus X$ for some submodule X, and $Ш(E/K)[p^\infty] \cong X^H \oplus X^H$.*

Moreover, when n is odd and $p^a \equiv -1 \mod n$ has a solution, $|X|/|X^H|$ is a square.

Remark 4.0.5. Note that the second part of Theorem 4.0.4 reproves Theorem 4.0.1 in this case, but not all cases. The isogeny argument goes further than what we get from just viewing Ш as a Galois module.

The size of Ш is a key ingredient in proving that its finiteness implies parity, and it is natural to ask whether knowing the size more precisely tells us anything more. If we have an extension K/k with Galois group G, and ρ is a self-dual representation of G, then we can ask about $\langle \rho, E(K) \otimes_{\mathbb{Z}} \mathbb{C} \rangle$, where $\langle \_, \_ \rangle$ is the usual inner product on

representations of G. There is an equivalent to the parity conjecture for these twists, which follows from finiteness of Ш in some cases. However this is not known for a number of dihedral groups, the smallest being D_{42}.

Definition 4.0.6. An Artin representation for a number field k is a continuous finite-dimensional complex representation of $\mathrm{Gal}(\bar{k}/k)$. Continuous means it factors through the Galois group of some finite extension K/k.

Conjecture 4.0.7 (Parity for twists)**.** *Let K/k be an extension of number fields with Galois group G, and ρ a self-dual Artin representation of* $\mathrm{Gal}(\bar{k}/k)$ *which factors through G. Let E/k be an elliptic curve. Then*

$$(-1)^{\langle \rho, E(K)\otimes_{\mathbb{Z}}\mathbb{C}\rangle} = w(E/k,\rho),$$

where $w(E/k,\rho) \in \{\pm 1\}$ is the root number for the twist of E by ρ.

As in the case of root numbers of elliptic curves, these root numbers have been classified in a number of cases ([43] Theorem 1). A particularly simple case is the following formula.

Theorem 4.0.8 ([43] Corollary 2)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and ρ a self-dual Artin representation of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *with conductor coprime to N. Then*

$$w(E/\mathbb{Q},\rho) = w(E/\mathbb{Q})^{\dim(\rho)}\mathrm{sign}(\alpha_\rho)\left(\frac{\alpha_\rho}{N}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol, $\alpha_\rho = 1$ if $\det(\rho) = \mathbf{1}$ and otherwise it is an integer such that $\det(\rho)$ factors through $\mathbb{Q}(\sqrt{\alpha_\rho})$.

Example 4.0.9 (= [28] Example 2.19)**.** Let $E/\mathbb{Q}$ be given by

$$y^2 + y = x^3 - x,$$

and let F be the field obtained by adjoining a root of

$$x^{10} - x^9 + 6x^8 - 3x^7 + 11x^6 - 3x^5 + 11x^4 - 3x^3 + 6x^2 - x + 1,$$

a D_{10}-extension. Let ε be the sign representation and ρ_1 and ρ_2 the two-dimensional irreducible complex representations of D_{10}.

We will compute the root number $w(E/\mathbb{Q},\rho_1)$ (where by an abuse of notation we let ρ_1 denote the Artin representation which factors through $\mathrm{Gal}(F/\mathbb{Q})$ and is equal on this group to ρ_1). Now $\dim(\rho_1)=2$, so $w(E/\mathbb{Q})^{\dim(\rho_1)}=1$. Next we compute α_{ρ_1}. As $\det(\rho_1)=\varepsilon$, we need the quadratic subextension of F, which is $\mathbb{Q}(\sqrt{-47})$. Therefore $\mathrm{sign}(\alpha_\rho)=-1$. Finally the conductor of E is 37, and we compute $\left(\frac{-47}{37}\right)=1$. Therefore $w(E/\mathbb{Q},\rho_1)=-1$.

This conjecture has applications to finding the rank.

Example 4.0.10 (= [28] Example 2.19)**.** Let E and F be as in Example 4.0.9. E has root number -1 over F and all of its subfields, so parity tells us that E/F has odd rank over all of these. We can also find that $\mathrm{rk}(E/\mathbb{Q})=1$, but together these facts only give a bound of $\mathrm{rk}(E/F)\geq 1$.

Parity for twists will allow us to do better. By decomposing the representation in to irreducibles we can write

$$E(F)\otimes_{\mathbb{Z}}\mathbb{C}\cong \mathbf{1}^{\oplus a}\oplus\varepsilon^{\oplus b}\oplus\rho_1^{\oplus c}\oplus\rho_2^{\oplus d},$$

for integers a, b, c and d. By comsidering the dimensions, we see that $\mathrm{rk}(E/F)=a+b+2c+2d$, and $1=\mathrm{rk}(E/\mathbb{Q})=a$.

As the representation is defined over $\mathbb{Q}$, it must have rational character, so we must have $c=d$. As computed in Example 4.0.9 the root number for ρ_1 is -1, so assuming parity for this twist we have $c\geq 1$. Therefore $\mathrm{rk}(E/F)\geq a+4c\geq 5$.

The p-parity conjecture is known for twists of elliptic curves and semistable principally polarised abelian varieties when $G\cong D_{2p^n}$ and $\rho=\mathbf{1}\oplus\sigma\oplus\det(\sigma)$, where σ is a two-dimensional representation ([7] Theorem 1.3.2, [36] Theorem 1.10, [42] Theorem 6.7). This has an application. Suppose $A/\mathbb{Q}$ is a semistable principally polarised abelian variety, and satisfies the parity conjecture over $\mathbb{Q}$ and all quadratic extensions of $\mathbb{Q}$. Then, assuming Ш is finite, parity holds for A over all number fields ([44] Theorem 1.1). We will ask in Section 4.3 whether understanding Ш

better in dihedral extensions leads to a parity result for twists in D_{2pq}-extensions, but unfortunately find that it does not.

Notation

Unless otherwise specified, let F/k be a dihedral extension of number fields of degree $2n$, with quadratic subextensions K (for odd n) or K_1, K_2 and K_3 (for even n), as in the statement of Theorem 4.0.1. Let p be a prime not dividing n.

We will assume that $Ш(E/F)[p^\infty]$ is finite.

4.1 The size of Ш

Brauer relations induce isogenies between products of Weil restrictions of elliptic curves (see Lemma 2.6.8). By considering the degree of the induced isogeny, we will show that the Tate–Shafarevich groups of two abelian varieties differ only in their p-parts for $p|n$, and relate these back, by factors which are 4^{th} powers, to the terms we want.

Lemma 4.1.1. *In D_{2n}, there are Brauer relations*

- $1 + 2D_{2n} - 2C_2 - C_n$ *when n is odd, and*
- $1 + 2D_{2n} - 2C_2 - C_n + D_n - D'_n$ *when n is even,*

where, if $D_{2n} = \langle r, s | r^n = s^2 = 1, srs = r^{-1} \rangle$, we let $C_2 = \langle s \rangle$, $C_n = \langle r \rangle$, $D_n = \langle r^2, s \rangle$ and $D'_n = \langle r^2, sr \rangle$.

Proof. Note that $\mathbb{C}[G/H] \cong \mathrm{Ind}_H^G \mathbf{1}$. For $H = 1$, we get the regular representation, and for $H = G$ we get the trivial representation.

In the odd case, the irreducible representations are the trivial representation $\mathbf{1}$, the sign representation ε, and $\frac{n-1}{2}$ two-dimensional representations which we will denote $\rho_1, \ldots, \rho_{\frac{n-1}{2}}$. Therefore we have

$$\mathbb{C}[D_{2n}/1] \cong \mathbf{1} \oplus \varepsilon \oplus \rho_1^{\oplus 2} \oplus \ldots \oplus \rho_{\frac{n-1}{2}}^{\oplus 2}$$

$$\mathbb{C}[D_{2n}/D_{2n}] \cong \mathbf{1}$$

$$\mathbb{C}[D_{2n}/1] \oplus \mathbb{C}[D_{2n}/D_{2n}]^{\oplus 2} \cong \mathbf{1}^{\oplus 3} \oplus \varepsilon \oplus \rho_1^{\oplus 2} \oplus \ldots \oplus \rho_{\frac{n-1}{2}}^{\oplus 2}.$$

Now we will compute $\mathrm{Ind}_{C_2}^{D_{2n}}\mathbf{1}$ using Frobenius reciprocity. For each irreducible representation ϕ of D_{2n}, we have $\langle \mathrm{Ind}_{C_2}^{D_{2n}}\mathbf{1}, \phi\rangle = \langle \mathbf{1}, \mathrm{Res}_{C_2}^{D_{2n}}\phi\rangle$. Computing $\mathrm{Res}_{C_2}^{D_{2n}}\phi$ for $\phi = \mathbf{1}$, we get the trivial representation on C_2, so $\langle \mathrm{Ind}_{C_2}^{D_{2n}}\mathbf{1}, \mathbf{1}\rangle = 1$. Doing the same for $\phi = \varepsilon$, we get the non-trivial irreducible representation on C_2, so ε does not appear in $\mathrm{Ind}_{C_2}^{D_{2n}}\mathbf{1}$. Restricting each representation ρ_i gives a sum of the trivial and non-trivial representations on C_2 [2], so each appears once. Therefore

$$\mathbb{C}[D_{2n}/C_2] \cong \mathrm{Ind}_{C_2}^{D_{2n}}\mathbf{1} \cong \mathbf{1} \oplus \rho_1 \oplus \ldots \oplus \rho_{\frac{n-1}{2}}.$$

Similarly we find that

$$\mathbb{C}[D_{2n}/C_n] \cong \mathrm{Ind}_{C_n}^{D_{2n}}\mathbf{1} = \mathbf{1} \oplus \varepsilon.$$

We conclude that $\mathbb{C}[D_{2n}/1] \oplus \mathbb{C}[D_{2n}/D_{2n}]^{\oplus 2} \cong \mathbb{C}[D_{2n}/C_n] \oplus \mathbb{C}[D_{2n}/C_2]^{\oplus 2}$.

Now as these representations are realisable over $\mathbb{Q}$ and isomorphic over $\mathbb{C}$, they are isomorphic over $\mathbb{Q}$ ([86] Ch. 12, Prop. 33 and discussion). Therefore we have the desired Brauer relation.

The proof for the even case proceeds similarly. We now have three non-trivial one-dimensional representations, ε_1, ε_2 and ε_3, with kernels C_n, D_n and D'_n respectively. The rest of the irreducible representations are two-dimensional ρ_i as before.

We find the induced representation from C_2 has irreducible summands $\mathbf{1}$, ε_2 and all the two-dimensional representations. Inducing from each subgroup of order n, we get $\mathbf{1} \oplus \varepsilon_i$ for the ε_i with kernel equal to the subgroup in question. Therefore

$$\mathbb{C}[D_{2n}/1] \oplus \mathbb{C}[D_{2n}/D_{2n}]^{\oplus 2} \oplus \mathbb{C}[D_{2n}/D_n] \cong \mathbf{1}^{\oplus 4} \oplus \varepsilon_1 \oplus \varepsilon_2^{\oplus 2} \oplus \varepsilon_3 \oplus (\bigoplus \rho_i)^{\oplus 2}.$$

We get the same result for $\mathbb{C}[D_{2n}/C_n] \oplus \mathbb{C}[D_{2n}/C_2]^{\oplus 2} \oplus \mathbb{C}[D_{2n}/D'_n]$. Putting this together and proceeding as before, we get the desired Brauer relation. □

Lemma 4.1.2. *For the Brauer relations $\sum_i H_i - \sum_j H'_j$ given in Lemma 4.1.1, there*

[2] To see this, it may help to view ρ_i as a two-dimensional representation where s acts as a reflection and r as a rotation by a multiple of $\frac{2\pi}{n}$.

are isogenies, defined over k, between $A = \prod_i \mathrm{Res}_{F^{H_i}/k}(E)$ *and* $B = \prod_j \mathrm{Res}_{F^{H'_j}/k}(E)$ *of degree coprime to p, where p is any prime not dividing n.*

Proof. By Lemma 2.6.7, these are $\mathbb{Z}_{(p)}$-relations. By ([3], discussion at the start of Section 3), this is equivalent to saying there is an injection of $\mathbb{Z}D_{2n}$-lattices, $\mathbb{Z}[S_1] \to \mathbb{Z}[S_2]$ with finite cokernel of order d, with $p \nmid d$. Here $S_1 = \bigsqcup_i D_{2n}/H_i$ and $S_2 = \bigsqcup_j D_{2n}/H'_j$. Then by Lemma 2.6.8 this induces an isogeny $A \to B$ of degree d^2, which is coprime to p. The same holds for an isogeny $B \to A$. □

Lemma 4.1.3. *Let A, B and p be as in Lemma 4.1.2. Then*

$$|Ш(A/k)[p^\infty]| = |Ш(B/k)[p^\infty]|.$$

Proof. As we have an isogeny $\phi : A \to B$ of degree d^2, with $p \nmid d$, it has a conjugate isogeny $\tilde{\phi}$ satisfying $\tilde{\phi} \circ \phi = \phi \circ \tilde{\phi} = [d^2]$. The isogeny ϕ induces a homomorphism $Ш(A/k)[p^\infty] \to Ш(B/k)[p^\infty]$, which is an isomorphism because $[d^2]$ is. □

Proof of Theorem 4.0.1. In the case where n is odd, Lemma 4.1.3 tells us that

$$|Ш(E/F)[p^\infty]||Ш(E/k)[p^\infty]|^2 = |Ш(E/K)[p^\infty]||Ш(E/F^{C_2})[p^\infty]|^2.$$

When the Tate–Shafarevich group of an elliptic curve is finite, it has square order, so $|Ш(E/F)[p^\infty]| \equiv |Ш(E/K)[p^\infty]| \pmod{\mathbb{Q}^{*4}}$.

In the case where n is even, the same argument tells us that, modulo 4^{th} powers,

$$|Ш(E/F)[p^\infty]||Ш(E/F^{D_n})[p^\infty]| \equiv |Ш(E/F^{D'_n})[p^\infty]||Ш(E/F^{C_n})[p^\infty]|,$$

again using the squareness of the order of Ш. These fixed fields are the three quadratic subextensions of F/k, so we can write this as

$$|Ш(E/F)[p^\infty]| \equiv |Ш(E/K_1)[p^\infty]||Ш(E/K_2)[p^\infty]||Ш(E/K_3)[p^\infty]| \pmod{\mathbb{Q}^{*4}}.$$

□

We can prove a similar statement about $Ш(E/F)[p]$, which has an application to computing $\mathrm{rk}(E/F)$.

Proposition 4.1.4. *Suppose E/k, K, F, n and p are as in Theorem 4.0.1. If n is odd, then*

$$|Ш(E/F)[p]| \equiv |Ш(E/K)[p]| \pmod{\mathbb{Q}^{*4}}.$$

If n is even, then

$$|Ш(E/F)[p]| \equiv |Ш(E/K_1)[p]||Ш(E/K_2)[p]||Ш(E/K_3)[p]| \pmod{\mathbb{Q}^{*4}}.$$

Proof. The proof is the same as that of Lemma 4.1.3 and Theorem 4.0.1. We can show that (in the notation of Lemma 4.1.3) $Ш(A/k)[p] \cong Ш(B/k)[p]$. This tells us that

$$Ш(E/F)[p] \oplus Ш(E/k)[p]^{\oplus 2} \cong Ш(E/K)[p] \oplus Ш(E/F^{C_2})[p]^{\oplus 2}.$$

By Corollary 2.2.5, $Ш(E/k)[p]$ and $Ш(E/F^{C_2})[p]$ have square order, and the conclusion follows. The proof for even n proceeds in the same way. □

Corollary 4.1.5. *Let E/k be an elliptic curve. Assume $Ш(E/F)$ is finite. Then*

$$p^{\mathrm{rk}(E/F)} \equiv \frac{|\mathrm{Sel}_p(E/F)|}{|Ш(E/K)[p]||E(F)[p]|} \pmod{\mathbb{Q}^{*4}}.$$

This is a consequence of Proposition 4.1.4 and the exact sequence in Theorem 2.3.2. It reduces the calculation of the rank modulo 4 to some slightly easier computations (assuming finiteness of Ш). If we can find points to give a lower bound on the rank, and use the Selmer group to give an upper bound that is close to this, computing the rank modulo 4 may be enough to give the exact answer.

Example 4.1.6. Let $E/\mathbb{Q}$ be given by $y^2 = x^3 - 7x - 6$ (LMFDB label 40.a2) and F be the extension given by adjoining a root of $x^6 + 34x^4 + 289x^2 + 983$. $F/\mathbb{Q}$ is a D_6-extension with intermediate field $\mathbb{Q}(\sqrt{-983})$. Using Magma [15], we can calculate in a few seconds (on a typical laptop) that $E(F)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}} \cong C_2 \oplus C_2$, that $\mathrm{Sel}_2(E/\mathbb{Q}(\sqrt{-983})) \cong C_2^2$ and that $\mathrm{Sel}_2(E/F) \cong C_2^6$. From this, we deduce that

$Ш(E/\mathbb{Q}(\sqrt{-983}))[2]$ is trivial. Applying Corollary 4.1.5, we find that $\mathrm{rk}(E/F)$ must be a multiple of 4. The Selmer group gives an upper bound of 4. We can very quickly compute some points of low height which are not in the torsion subgroup, so the rank must equal 4.

Attempting to do this using Magma's inbuilt rank functions, which will use the Selmer group to give an upper bound of four and then search until it has four independent points, could not compute the rank in an hour. The difficulty is in finding a third linearly-independent point, as there are none with low height. Once a third is found, the usual finiteness assumption tells us that $Ш(E/F)[2]$ is a square, so we would know that the rank is 4. Applying Corollary 4.1.5 instead avoids this difficult search over a degree 6 number field.

Remark 4.1.7. For $p \neq 2$, we can determine Ш from calculations on curves over k. This is because the Weil restriction $\mathrm{Res}_{K/k}(E)$ is related to $E \times E_d$ by a 4-isogeny, where E_d is the quadratic twist of E by some $d \in k$ such that $K = k(\sqrt{d})$ (Proposition 2.5.7). By the same proof as Lemma 4.1.3, we therefore have $|Ш(E/K)[p^\infty]| = |Ш(E_d/k)[p^\infty]||Ш(E/k)[p^\infty]|$.

In the case where $k = \mathbb{Q}$, this can make computation more practical. For example, consider the curve $E : y^2 + xy + y = x^3 - 5334x - 150368$ (LMFDB label 30.a1) and the number field F given by a root of $x^{10} + 5x^8 + 15x^6 + 20x^4 + 25x^2 + 15$, a D_{10}-extension of $\mathbb{Q}$. The intermediate quadratic field is $K = \mathbb{Q}(\sqrt{-15})$ [63]. We can compute the 3^∞-part of Ш for E and E_{-15} over $\mathbb{Q}$ by computing Selmer groups – in this case Magma [15] will show that they are both trivial. Hence the 3^∞-part of $Ш(E/F)$ has order 3^{4t} for some t (if it is finite). This can be verified analytically, again using Magma. It tells us that the analytic order of $Ш(E/F)$ is 6560.999998. This strongly suggests that the true value is $6561 = 3^8$, which would match our conclusion.

Remark 4.1.8. If we replace E by an abelian variety A, the same arguments work, except we no longer know that $Ш(A)[p^\infty]$ has square order. If A is principally polarised, and $p \neq 2$, this is still true and we can make the same conclusion. In general, we can conclude that $|Ш(A/F)[p^\infty]| \equiv |Ш(A/K)[p^\infty]| \pmod{\mathbb{Q}^{*2}}$ for odd

n, and analogously for even n.

4.2 Galois Module Structure

In some cases, the same result follows from the work of Chetty, which also gives information about the Galois module structure of Ш. Let n, p and $H \cong C_n$ be as in Theorem 4.0.4, and assume that $Ш(E/F)[p^\infty]$ is finite.

Lemma 4.2.1. *$\mathbb{Z}_p[C_n]$ is a direct sum of local rings with principal maximal ideals.*

Proof. The ring $\mathbb{Z}_p[C_n]$ is isomorphic to $\mathbb{Z}_p[T]/(T^n-1)$. By the Chinese Remainder Theorem, this is a direct sum of rings $\mathbb{Z}_p[T]/\Phi_d(T)$ for cyclotomic polynomials Φ_d with $d|n$. These further split into direct sums because $\Phi_d = \prod_i P_{d,i}$, a product of irreducible polynomials over $\mathbb{Z}_p$. Finally $\mathbb{Z}_p[T]/P_{d,i}(T)$ is the ring of integers of $\mathbb{Q}_p[T]/P_{d,i}(T)$ ([87], Ch. IV, Section 4, Prop. 16), a local field, so has principal maximal ideal. □

Recall the following result, Proposition 2.8 from [24]. Note that as stated there it has an error, specifically it may be false if the codomain of the pairing has an element of order 2. Here we restrict to a codomain $\mathbb{Q}_p/\mathbb{Z}_p$ for p odd, where this does not occur. This can be proven in exactly the same way as in [24].

Proposition 4.2.2. *Let p be an odd prime. Suppose A is a commutative ring which is a direct sum of local rings with principal maximal ideals, and such that $\mathbb{Q}_p/\mathbb{Z}_p$ is an A-module. Let M be a finite A-module. Suppose $[\_,\_] : M \times M \to \mathbb{Q}_p/\mathbb{Z}_p$ is a non-degenerate skew-symmetric pairing with $[ax,y] = [x,ay]$ for all $x, y \in M$ and $a \in A$. Then there exist submodules M' and M'' of M, with $M \cong M' \oplus M''$ and $M' \cong M''$.*

Theorem 4.2.3 (= Theorem 4.0.4)**.** *Suppose p is odd. Then $Ш(E/F)[p^\infty] \cong X \oplus X$ as $\mathbb{Z}_p[H]$-modules, for some submodule X, and $Ш(E/K)[p^\infty] \cong X^H \oplus X^H$.*

Moreover, when n is odd and $\mathrm{ord}_q(p)$ is even for all primes q dividing n, $|X|/|X^H|$ is a square.

Note that if $p^a \equiv -1 \mod n$ has a solution, the latter condition holds.

Proof. We will apply Lemma 4.2.1 and Proposition 4.2.2 to the ring $A = \mathbb{Z}_p[H]$, $M = Ш(E/F)[p^\infty]$ and $\mathbb{Q}_p/\mathbb{Z}_p$ an A-module with H acting trivially. The pairing will be $[x,y] := (x,sy)$, where $(\_,\_)$ is the Cassels–Tate pairing on $Ш(E/F)$ and s is a lift of the non-trivial element of $\mathrm{Gal}(K/k)$ to $\mathrm{Gal}(F/k)$ (i.e. an element of order 2 corresponding to a reflection in D_{2n}). This pairing is non-degenerate because the Cassels–Tate pairing is, and skew-symmetric because of the skew-symmetry and Galois equivariance of the Cassels–Tate pairing. Now, given $a \in H$, we have $(ax,sy) = (x,a^{-1}sy) = (x,say)$, where the first equality is Galois equivariance, and the second is because $\mathrm{Gal}(F/k)$ is dihedral. Therefore our pairing satisfies the condition $[ax,y] = [x,ay]$ for all $a \in H$, and by bilinearity this holds for all $a \in A$. Applying the proposition, we can conclude that $Ш(E/F)[p^\infty] \cong X \oplus X$.

Note that $Ш(E/F)[p^\infty]^H \cong Ш(E/K)[p^\infty]$ as $p \nmid |H| = n$ (see e.g. [78], Lemma 11).

Now by Lemma 4.2.1, $Ш(E/F)[p^\infty]$ is a direct sum of $\mathbb{Z}_p[T]/P_{d,i}(T)$-modules. Suppose that n is odd and $\mathrm{ord}_q(p)$ is even for all $q|n$. We will show that $|M|/|M^{C_n}|$ is a square for all $\mathbb{Z}_p[T]/P_{d,i}(T)$-modules M, from which it follows that $|X|/|X^H|$ is a square.

First consider the modules with $d \neq 1$. The condition implies that $\mathrm{ord}_d(p)$ is even for all $d|n$, because for any $q|d$, $\mathrm{ord}_q(p)|\mathrm{ord}_d(p)$. This equals the degree of $P_{d,i}$ (this is true for the factorisation of a cyclotomic polynomial over $\mathbb{F}_p$ by e.g. [61] Theorem 2.47, and we can lift the factorisation to $\mathbb{Z}_p$ by Hensel's lemma). For a uniformiser π, finite $\mathbb{Z}_p[T]/P_{d,i}(T)$-modules are direct sums of modules of the form $\mathbb{Z}_p[T]/(\pi^a, P_{d,i}(T))$ for some a ([46] Chapter 12 Theorem 6). As $p \nmid d$, the cyclotomic extension of $\mathbb{Z}_p$ is unramified, so these have size $p^{a\deg(P_{d,i})}$, which is a square as $\deg(P_{d,i})$ is even. They have no fixed part because a generator of H acts as multiplication by ζ_d, a root of $P_{d,i}$, and $1-\zeta_d$ is a unit in $\mathbb{Z}_p[T]/P_{d,i}(T)$.

When $d = 1$, we have $\mathbb{Z}_p$-modules with C_n acting trivially, so $M = M^{C_n}$, and $|M|/|M^{C_n}|$ is again a square. □

Remark 4.2.4. In the case where there is a prime $q|n$ with $\mathrm{ord}_q(p)$ odd, we may have some $\mathbb{Z}_p[H]$-modules M_i with size an odd power of p, with no fixed part. By

Theorem 4.0.1 we can conclude that if each of these M_i appears in the decomposition of $Ш(E/F)[p^\infty]$ with multiplicity $2a_i$, then $\sum_i a_i$ is even.

Remark 4.2.5. In the case where $n = q$ is a prime, the latter part of Theorem 4.2.3 holds when p has even order modulo q. If q varies and we fix p, this happens for a set of primes with Dirichlet density $2/3$ ([52], Section 3). It will happen less often when n has more factors, as more conditions must hold.

If instead we fix q and vary p, the condition will hold for at least half of the residue classes modulo q (more precisely, by considering the cyclic group $\mathbb{F}_q^*$ of order $q-1$, we can see that the proportion is $1-2^{-v_2(q-1)}$). So again we can apply the second part of Theorem 4.2.3 in at least half of cases.

4.3 Application to Parity

Beyond the parity conjecture, we are also interested in the parity conjecture for twists. In this setting, we consider an elliptic curve E/k, and a Galois field extension K/k with $\mathrm{Gal}(K/k) = G$. It is natural to ask what we can say about the structure of the representation $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$, i.e. if ρ is an irreducible representation of G, can we find $\langle \rho, E(K) \otimes_{\mathbb{Z}} \mathbb{C} \rangle$? It turns out that there is an equivalent to the root number, which is conjectured to predict its parity. This conjecture is known to follow from finiteness of Ш for the representations of some dihedral groups, with the smallest case not yet proven being being D_{42}.

Example 4.3.1. Consider the curve E and number field F from Example 4.1.6. We have a D_6-extension of number fields $F/\mathbb{Q}$. This has one two-dimensional irreducible representation ρ. We find using Theorem 1 of [43] that this twist has root number 1, so assuming finiteness of Ш it has even parity. This tells us that $\mathrm{rk}(E/F) \equiv \mathrm{rk}(E/\mathbb{Q}(\sqrt{-983})) = 0 \mod 4$, which is the same result we deduced from finiteness of Ш in that example.

We can approach such results using a Brauer relation. The idea is to relate a ratio of regulators to local data, specifically the Tamagawa numbers and valuations of $\frac{\omega}{\omega_v^0}$, where ω is a fixed k-rational differential, and ω_v^0 is a minimal differential

at a place v. Then we aim to relate this local data to the root numbers, to show it gives the same overall result. The method is shown in [39] Section 1.iv. We will sketch how this method works, and why one might hope to improve on it with better knowledge of the size of Ш.

Taking a Brauer relation, we will apply Lemma 2.6.8 together with isogeny-invariance of BSD to relate regulators to local data. Suppose E/k is an elliptic curve, K/k is a Galois extension with Galois group G, and $\sum_i n_i H_i$ is a Brauer relation in G. Then we get an isogeny

$$\prod_{n_i>0} \mathrm{Res}_{K^{H_i}/k}(E)^{n_i} \to \prod_{n_i<0} \mathrm{Res}_{K^{H_i}/k}(E)^{-n_i}.$$

Assuming finiteness of Ш, and applying isogeny-invariance to this, we get

$$\prod_i \frac{\mathrm{Reg}(E/K^{H_i})^{n_i}\Omega(E/K^{H_i})^{n_i}|Ш(E/K^{H_i})|^{n_i}}{|E(E/K^{H_i})_{\mathrm{tors}}|^{2n_i}} = 1.$$

In a Brauer relation, the terms in Ω, other than Tamagawa numbers and the valuations of a differential discussed earlier, cancel out ([41] Section 2.2). Let the product of these remaining terms for a given curve E/K^{H_i} be $C(E/K^{H_i})$. If we work modulo squares, the Tate–Shafarevich and torsion terms vanish. We can then conclude that

$$\prod_i \mathrm{Reg}(E/K^{H_i})^{n_i} \equiv \prod_i C(E/K^{H_i})^{n_i} \pmod{\mathbb{Q}^{*2}},$$

As a coarse example of the utility of this method, if we can calculate the local terms $C(E/K^{H_i})$ and show that the right hand side is not a square, then $\mathrm{rk}(E/K)$ is not 1. Note that the local terms can be calculated using Tate's algorithm. The following theorem will allow us to say something more precise.

Theorem 4.3.2 (= [41] Corollary 2.13)**.** *We can express the ratio of regulators purely in terms of regulator constants. Specifically, if Θ is a Brauer relation in $\mathrm{Gal}(K/k)$, and $E(K)\otimes_{\mathbb{Z}}\mathbb{Q} \cong \bigoplus_i \rho_i^{n_i}$, where the ρ_i are irreducible rational representations of $\mathrm{Gal}(K/k)$, then the ratio of regulators in Θ is equal to $\prod \mathcal{C}_\Theta(\rho_i)^{n_i}$.*

This implies that if $\mathcal{C}_\Theta(\rho_i)$ is not square, we have a hope of expressing the

parity of n_i in terms of local data and relating this to the root numbers. The main limiting factor here is Ш, about which we only say that its order is a square. If we know more about how Ш grows in dihedral extensions, we might hope to get more information. Of course, we will also have to deal with the other terms more precisely. The torsion subgroups can be calculated in practice for elliptic curves over fairly large fields, so they are not a major problem. Regulator constants can also be defined as rational numbers, rather than rational numbers modulo squares, as long as we consider $E(K)/E(K)_{\text{tors}}$ as an integral representation of G rather than a rational one ([3], comment after Theorem 2.6). Hence if we know something about $|Ш|$ modulo fourth powers, as in Theorem 4.0.1, we might hope to do something similar and get more information, such as in cases where the regulator constant is trivial modulo rational squares.

We will consider applying this refined method to representations of the simplest dihedral groups where parity is not already known, those of the form D_{2pq} for primes p and q.

Notation. Let p and q be odd primes, and as before let K_{2pq} be a Galois extension of $\mathbb{Q}$ with Galois group D_{2pq}. Fix a subfield L_{pq} of degree pq, and a subfield $L_p \subset L_{pq}$ of degree p. Let K_2, K_{2p} and K_{2q} be the subfields of degree 2, $2p$ and $2q$ respectively.

There is a faithful irreducible representation of D_{2pq}, which we cannot in general prove parity for. If we want to use this technique to prove parity for this representation, the simplest case is when this is the only irreducible rational representation which appears in $E(K_{2pq}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Equivalently, E has no points over K_{2p} or K_{2q}, but gains rank over K_{2pq}. If we can prove for some curve in this setting that the ratio of regulators is not 1, then we may be able to prove results towards parity.

Remark 4.3.3. Root number considerations do allow this setting to occur, so to prove a parity result we would have to be able to deal with this case. Take $K_2 = \mathbb{Q}(\sqrt{-7})$. By class field theory, it has extensions of degree 3, dihedral over $\mathbb{Q}$, one of which ramifies at 5 only, and one at 41 only. Their compositum contains a degree 3 extension which ramifies at both; let this be K_6. Similarly we can construct a degree

7 extension K_{14} which ramifies at 13 and 41. The compositum of these is dihedral of degree 42 over $\mathbb{Q}$. It ramifies at 5, 13 and 41 with ramification indices 3, 7 and 21 respectively, and residue degree 2. It is also ramified at 7.

If we find an elliptic curve with rank 0 over $\mathbb{Q}$, multiplicative reduction at 5, 13 and 41 and good reduction elsewhere, the formula in Theorem 1 of [43] tells us that the root numbers for the twists are -1 for exactly the representations we want. The curve with LMFDB label 2665.b1 has these properties [63].

Lemma 4.3.4. *The Brauer relations in D_{2pq} are*

$$\Theta = \{e\} + 2D_{2pq} - C_{pq} - 2C_2$$
$$\Theta_p = C_q + 2D_{2pq} - C_{pq} - 2D_{2q}$$
$$\Theta_q = C_p + 2D_{2pq} - C_{pq} - 2D_{2p}$$

and $\mathbb{Z}$-linear combinations of these.

Proof. It is simple to check that these are all Brauer relations and linearly independent, and in D_{2pq} there are three conjugacy classes of non-cyclic subgroups so there are three independent Brauer relations. Therefore these form a rational basis for the module of Brauer relations. In any Brauer relation, the multiplicity of Θ will equal that of $\{e\}$, so will be an integer, and similarly for the others, so these three relations form a lattice basis. □

Now we are interested in the setting where E has rank over K_{2pq} but not K_{2p} or K_{2q}. Here the ratio of regulators arising from Θ_p and Θ_q is 1. So to get a non-trivial ratio of regulators, without loss of generality we can use the relation Θ. So our aim is to use data about the torsion, Ш and local data to show that

$$\frac{\mathrm{Reg}(E/K_{2pq})\mathrm{Reg}(E/\mathbb{Q})^2}{\mathrm{Reg}(E/K_2)\mathrm{Reg}(E/L_{pq})^2} \neq 1.$$

Unfortunately this will never be the case.

Proposition 4.3.5. *Let E be an elliptic curve over $\mathbb{Q}$, and let p, q and K_{2pq} be as above. Suppose E has positive rank over K_{2pq} but not K_{2p} or K_{2q}. Then*

$$\frac{\mathrm{Reg}(E/K_{2pq})\mathrm{Reg}(E/\mathbb{Q})^2}{\mathrm{Reg}(E/K_2)\mathrm{Reg}(E/L_{pq})^2} = 1.$$

Proof. First consider the p-adic valuation. The ratio

$$\frac{\mathrm{Reg}(E/K_{2pq})\mathrm{Reg}(E/L_p)^2}{\mathrm{Reg}(E/L_{pq})^2\mathrm{Reg}(E/K_{2p})}$$

comes from a Brauer relation in the D_{2q} extension K_{2pq}/L_p. Hence it is a rational number, and its p-adic valuation is 0 by Lemma 2.6.7. The ratio

$$\frac{\mathrm{Reg}(E/K_{2p})\mathrm{Reg}(E/\mathbb{Q})^2}{\mathrm{Reg}(E/K_2)\mathrm{Reg}(E/L_p)^2}$$

is 1, because all of these regulators are 1 as the ranks are 0. We are interested in the product of these, which must also have p-adic valuation 0. Similarly the q-adic valuation is 0. The other primes give valuation 0 by Lemma 2.6.7. Therefore the ratio is 1. □

As the regulator constant is always 1 in this case, we cannot hope to use this method with Brauer relations in D_{2pq} to get a parity result for the faithful irreducible representation of D_{2pq}.

Chapter 5

Abelian Varieties with the Same Arithmetic Properties

In this chapter, we consider how much Selmer groups and other invariants tell us about the isomorphism class of an abelian variety. We give a list of invariants which determines the isomorphism class of an elliptic curve over $\mathbb{Q}$, but does not for abelian varieties of higher dimension. Some of the content of this chapter (in the introduction and Sections 5.1, 5.2 and 5.3) is based on the paper *Non-Isomorphic Abelian Varieties with the Same Arithmetic*. A pre-print of this is available at [6].

Introduction

A natural question to ask about abelian varieties is which invariants we can use to distinguish them. For example, if we have two varieties A and B defined over $\mathbb{Q}$, and $A(F) \cong B(F)$ for every number field F, must A and B be isomorphic over $\mathbb{Q}$?

Question 5.0.1. Is there a list of invariants which, if they are equal for two abelian varieties A and B over a number field k, guarantee that A and B are isomorphic over k? If so, which invariants do we need?

Here the invariants are properties of the curve which are not changed by isomorphism over k. This excludes properties like the discriminant, which depend on the model chosen.

Mazur and Rubin considered a similar question in [66], asking what the Selmer groups $\mathrm{Sel}_n(E_d/k)$ can tell us, for a fixed integer n and where E_d is the quadratic

twist of an elliptic curve E/k by d. They found that two non-isogenous curves could have isomorphic n-Selmer groups for all E_d, and gave sufficient conditions for this phenomenon to occur. It has since been shown by Chiu ([26] Theorem 1.8) that if two elliptic curves have the same size p-Selmer groups for all but finitely many p and over all finite extensions of k, they are isogenous. Chiu used a result of Faltings ([47] Corollary 1 after Theorem 4), which tells us that if the (rational) Tate modules of two abelian varieties are isomorphic for some prime, then the varieties must be isogenous. We consider the related question of determining elliptic curves up to isomorphism.

The main focus of this chapter is to prove the following theorem.

Theorem 5.0.2. *There exist abelian varieties A and B defined over $\mathbb{Q}$ which are not isomorphic to each other but satisfy the following, over every number field F:*

- $A(F) \cong B(F)$.
- *The n-Selmer groups of A and B are isomorphic.*
- *The Tamagawa numbers $c_v(A) = c_v(B)$, for every finite place v of F.*
- *The Tate–Shafarevich groups* $Ш(A/F) \cong Ш(B/F)$.
- *The L-functions $L(A/F,s) = L(B/F,s)$.*
- *The conductors of A and B are equal.*
- *The regulators* $\mathrm{Reg}(A/F) = \mathrm{Reg}(B/F)$.
- *For every prime ℓ, the Tate modules $T_\ell(A) \cong T_\ell(B)$.*

Here 'isomorphic' means isomorphism of groups, except for the Tate modules which are also isomorphic as G_F-modules.

In other words, if we wish to distinguish abelian varieties by their arithmetic properties, this list is insufficient. We will be able to give an explicit construction for these varieties A and B.

Remark 5.0.3. Theorem 5.0.2 tells us that knowing all the p-Selmer groups over every finite extension of k does not force the varieties to be isomorphic. We can compare this to Chiu's result ([26] Theorem 1.8), which tells us that, for elliptic curves, knowing these for all but finitely many p guarantees that they are isogenous.

Remark 5.0.4. For elliptic curves, the j-invariant tells us whether they are isomorphic over $\bar{k}$, but not whether they are isomorphic over k. We will also consider elliptic curves, and show that the properties listed in Theorem 5.0.2 do determine whether elliptic curves are isomorphic over $\mathbb{Q}$, but there are number fields where they do not.

Remark 5.0.5. This is analogous to questions about other mathematical objects, for example number fields. It is known that there exist non-isomorphic number fields with the same zeta function, class groups, regulators, discriminants, adele rings and other properties ([92] Proposition 3.7 and Remark 3.11). Another example is a certain eigenvalue problem on regions of the plane, which models what pure tones a drum of that shape can produce. In this case, the list of eigenvalues does not determine the shape of the region ([49] Section 1).

5.1 Properties of A and B

In this section we prove the following proposition:

Proposition 5.1.1. *Suppose A and B are abelian varieties over a number field k, and that there exist isogenies defined over k from A to B of degree coprime to ℓ, for all primes ℓ. Then A and B have the same properties as listed in the statement of Theorem 5.0.2, for all number fields F containing k.*

Lemma 5.1.2. *Suppose f is a functor from abelian varieties to the category of abelian groups G with $G[n]$ and G/nG finite for all positive integers n. Suppose also that $f([n]) = [n]$ for all n. Then for any isogeny ϕ, defined over k, of degree coprime to ℓ, $|\ker(f(\phi))|$ and $|\mathrm{coker}(f(\phi))|$ are finite and coprime to ℓ.*

Proof. This follows from the existence of conjugate isogenies. Given $\phi : X \to Y$, there exists $\tilde{\phi} : Y \to X$ such that $\tilde{\phi} \circ \phi = [\deg(\phi)]$ on X and $\phi \circ \tilde{\phi} = [\deg(\phi)]$ on Y.

Now $f(\tilde{\phi}) \circ f(\phi) = [\deg(\phi)]$, so $\ker(f(\phi)) \leq \ker([\deg(\phi)])$. As $\deg(\phi)$ is coprime to ℓ, the order of $\ker([\deg(\phi)])$ is coprime to ℓ, so the kernel of ϕ has the required property. Similarly $f(\phi) \circ f(\tilde{\phi}) = [\deg(\phi)]$, so $\mathrm{im}(f(\phi)) \geq \mathrm{im}([\deg(\phi)])$ and $\mathrm{coker}(f(\phi))$ is a quotient of $\mathrm{coker}([\deg(\phi)])$. Therefore the cokernel also has the required property. □

Note that this is a generalisation of Lemma 4.1.3. For that case, the only subgroups or quotient groups of $Ш[p^\infty]$ with order coprime to p are trivial, so the groups have to be the same size.

Lemma 5.1.3. *Suppose f is a functor as in Lemma 5.1.2, and which maps to finite groups. Let A and B be abelian varieties over a number field k, and suppose that for every prime ℓ, there exists an isogeny from A to B, defined over k, of degree coprime to ℓ. Then $f(A) \cong f(B)$.*

Proof. We first prove a weaker result, that $|f(A)| = |f(B)|$. Suppose $\phi : A \to B$ is an isogeny. Then, by considering the exact sequence

$$0 \to \ker(f(\phi)) \to f(A) \to f(B) \to \mathrm{coker}(f(\phi)) \to 0,$$

we see that

$$\frac{|f(A)|}{|f(B)|} = \frac{|\ker(f(\phi))|}{|\mathrm{coker}(f(\phi))|}.$$

By the previous lemma, if we pick a ϕ of degree coprime to a prime ℓ, the right hand side has ℓ-adic valuation 0. By doing this for a range of isogenies of different degrees, we can show that it is equal to 1, so $|f(A)| = |f(B)|$.

Now consider $X \to f(X)[n]$ for some integer n. This is a functor meeting the required conditions to apply the weaker result, so $|f(A)[n]| = |f(B)[n]|$ for all n. By the structure theorem for finite abelian groups, this is enough to show that $f(A) \cong f(B)$. □

Lemma 5.1.4. *Let A and B be as in Lemma 5.1.3. Suppose f is a functor as in Lemma 5.1.2, and which maps to finitely-generated groups. Then $f(A) \cong f(B)$.*

Proof. The groups $f(A)$ and $f(B)$ must have the same rank, as the cokernels of the maps between them are finite. Then we can apply Lemma 5.1.3 to their torsion parts. □

Proof of Proposition 5.1.1. The Mordell–Weil groups and n-Selmer groups are isomorphic by a direct application of Lemmas 5.1.3 and 5.1.4, and so are the Tamagawa numbers as $c_v(A) = |A(F_v)/A_0(F_v)|$, where $A_0(F_v)$ is the set of points mapped to the identity component of the special fibre of the Neron model of A. The Tate–Shafarevich groups are isomorphic as they are determined by the finite groups $Ш(A/F)[\ell^n]$ for all primes ℓ and positive integers n, and we can apply Lemma 5.1.3 to these. The equality of the L-functions and conductors holds for any pair of abelian varieties with an isogeny between them.

To prove that the regulators are equal, note that given an isogeny $\phi : A \to B$,

$$\frac{\mathrm{Reg}(A/F)}{\mathrm{Reg}(B/F)} = \frac{|\mathrm{coker}(\phi : A(F)/A(F)_{\mathrm{tors}} \to B(F)/B(F)_{\mathrm{tors}})|}{|\mathrm{coker}(\hat{\phi} : \hat{B}(F)/\hat{B}(F)_{\mathrm{tors}} \to \hat{A}(F)/\hat{A}(F)_{\mathrm{tors}})|},$$

where $\hat{B}$ and $\hat{\phi}$ are the duals of B and ϕ ([14] Section 2.2). By picking suitable isogenies, we can use Lemma 5.1.2 to show that the right hand side is coprime to any prime, and hence the regulators are equal.

Finally, for the Tate modules $T_\ell(A)$ and $T_\ell(B)$, pick an isogeny ϕ of degree coprime to ℓ. The map $[\deg(\phi)]$ is an isomorphism on $T_\ell(A)$ and $T_\ell(B)$, so the proof of Lemma 5.1.2 implies that ϕ induces an isomorphism of Tate modules as groups. Because ϕ commutes with the action of G_F on points, it does on the Tate module also, so they are isomorphic as $\mathbb{Z}[G_F]$-modules.

□

Remark 5.1.5. This equality of properties would also be true if A and B were isomorphic, but we shall show that this does not have to be the case.

5.2 Existence of Abelian Varieties

Theorem 5.2.1. *There exist abelian varieties A and B, defined over $\mathbb{Q}$, which are not isomorphic over $\mathbb{Q}$, but for any prime ℓ there exists an isogeny between them,*

defined over $\mathbb{Q}$, of degree coprime to ℓ.

Combined with Proposition 5.1.1, this proves Theorem 5.0.2. We will construct abelian varieties with isogenies between them by considering $\mathbb{Z}[G]$-modules, as discussed in Section 2.5 and in [69]. One example where this can give the right properties is for $\mathbb{Z}[C_p]$-modules.

5.2.1 Modules in the Same Genus

Let p be a prime, K the p^{th} cyclotomic field, and $\mathcal{O}_K = \mathbb{Z}[\zeta]$ its ring of integers, where ζ is a primitive p^{th} root of unity. Let G be the group C_p, generated by an element g. Note that an ideal in $\mathcal{O}_K$ is a $\mathbb{Z}[G]$-module, with g acting as multiplication by ζ.

Lemma 5.2.2. *Two ideals in $\mathcal{O}_K$ are isomorphic as $\mathbb{Z}[G]$-modules if and only if they are in the same ideal class.*

Proof. See Curtis–Reiner ([31], Section 74). □

Thus if we pick two ideals which are not in the same ideal class, we have two $\mathbb{Z}[G]$-modules which are not isomorphic. This can be done for any $p \geq 23$ ([96] Theorem 11.1).

Definition 5.2.3 (Genus)**.** Two $\mathbb{Z}[G]$-modules M and N are in the same genus if, for all primes ℓ, $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell[G]$-modules.

Lemma 5.2.4. *Let M and N be ideals in $\mathcal{O}_K$. Then M and N are in the same genus.*

Proof. $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a $\mathbb{Z}_\ell[G]$-module, and in fact it is an ideal in $\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \frac{\mathbb{Z}_\ell[X]}{(1+X+\ldots+X^{p-1})}$. This cyclotomic polynomial factorises into distinct irreducible factors $P_1, \ldots, P_t$ over $\mathbb{Z}_\ell$. The only prime that divides the discriminant of $1 + X + \ldots + X^{p-1}$ is p, so for $\ell \neq p$ the polynomials $P_1, \ldots, P_t$ are coprime. If $\ell = p$, then $1 + X + \ldots + X^{p-1}$ is irreducible so $t = 1$. Therefore in either case we have

$$\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \frac{\mathbb{Z}_\ell[X]}{P_1(X)} \times \ldots \times \frac{\mathbb{Z}_\ell[X]}{P_t(X)}.$$

Therefore by Lemma 2.7.3, the ideal $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a product of ideals M_i in $\frac{\mathbb{Z}_\ell[X]}{P_i(X)}$. Considering the $\mathbb{Z}_\ell$-rank of these tells us that M_i is never the zero ideal, as

$$p-1 = \mathrm{rk}_{\mathbb{Z}}(M) = \mathrm{rk}_{\mathbb{Z}_\ell}(M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell) = \sum_i \mathrm{rk}_{\mathbb{Z}_\ell}(M_i) \leq \sum_i \mathrm{rk}_{\mathbb{Z}_\ell}\left(\frac{\mathbb{Z}_\ell[X]}{P_i(X)}\right) = p-1.$$

Each ring $\frac{\mathbb{Z}_\ell[X]}{P_i(X)}$ is the ring of integers of the cyclotomic extension $\frac{\mathbb{Q}_\ell[X]}{P_i(X)}$ ([87] Ch. IV, §4, Prop. 16 and 17), a local field, so is a principal ideal domain. Therefore M_i is a non-zero principal ideal so is isomorphic to $\frac{\mathbb{Z}_\ell[X]}{P_i(X)}$ as $\mathbb{Z}_\ell[G]$-modules [1], so $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. The same is true for $N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and the result follows. □

Example 5.2.5. We can make the construction above explicit, and verify computationally that we have two modules in the same genus which are not isomorphic. Let K be the 23rd cyclotomic field, and let $\mathcal{O}_K$ be its ring of integers. Let ζ be a 23rd root of unity. Let I be the ideal of $\mathcal{O}_K$ generated by 2 and $1+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^{10}+\zeta^{11}$, i.e. one of the primes above 2, which is not principal. We will show explicitly that $\mathcal{O}_K$ and I are not isomorphic as $\mathbb{Z}[G]$-modules, but are in the same genus.

We will use the basis $\{\zeta^i : 0 \leq i \leq 21\}$ for $\mathcal{O}_K$. A generator g which acts as multiplication by ζ is represented by a matrix

$$A = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 & -1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 & -1
\end{pmatrix}.$$

We can compute a lattice basis for the ideal I with Magma [15]. In the same basis as

[1] Analogously to Lemma 5.2.2, if M_i is a principal ideal it is of the form $\alpha\frac{\mathbb{Z}_\ell[X]}{P_i(X)}$ for some non-zero $\alpha \in \frac{\mathbb{Z}_\ell[X]}{P_i(X)}$, which gives an isomorphism.

before, it is the columns of the matrix

$$M = \begin{pmatrix}
2&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&1&1\\
0&2&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0&\\
0&0&0&2&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&\\
0&0&0&0&2&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&\\
0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&0&1&0&1&1&1&0&0\\
0&0&0&0&0&0&2&0&0&0&0&1&1&1&1&0&0&0&1&0&0&1&\\
0&0&0&0&0&0&0&2&0&0&0&1&1&0&1&1&1&0&0&0&1&1&\\
0&0&0&0&0&0&0&0&2&0&0&0&1&1&0&1&1&1&0&0&0&1&\\
0&0&0&0&0&0&0&0&0&2&0&1&0&0&1&0&0&1&1&1&1&1&\\
0&0&0&0&0&0&0&0&0&0&2&0&1&0&0&1&0&0&1&1&1&1&\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}.$$

Thus the action of g on the ideal I, in a basis given by the columns of M, is given by

$$A' = M^{-1}AM = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&-1&0&-1&0&0&-1&0&0&-1&-1&-1&2\\
1&0&0&0&0&0&0&0&0&0&0&-1&0&-1&0&0&-1&0&0&-1&0&0&3\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&0&0&0&1&0&0&0&0&0&0&-1&0&-1&0&0&0&0&0&-1&0&0&2\\
0&0&0&0&0&1&0&0&0&0&0&-1&0&-1&0&0&0&0&0&0&0&-1&2\\
0&0&0&0&0&0&1&0&0&0&0&-1&0&0&0&0&-1&0&0&0&-1&-1&3\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&0&0&0&0&0&0&0&1&0&0&-1&0&0&0&0&0&0&0&-1&-1&-1&3\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&0&0&0&0&0&0&0&0&0&1&2&0&1&0&0&1&0&0&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1
\end{pmatrix}.$$

Magma can test that this matrix is similar to A, and produces a matrix B with

the property that $B^{-1}AB = A'$. The B it produces is not M, but

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
6&1&0&0&0&0&0&0&0&0&0&0&3&0&3&0&0&3&0&0&3&2&2\\
5&6&1&0&0&0&0&0&0&0&0&5&3&5&3&0&5&3&0&5&2&1\\
4&5&6&1&0&0&0&0&0&0&0&4&5&7&5&3&4&5&3&4&4&1\\
3&4&5&6&1&0&0&0&0&0&0&3&4&8&7&5&6&4&5&6&3&3\\
3&3&4&5&6&1&0&0&0&0&0&3&3&7&8&7&7&6&4&8&5&2\\
3&3&3&4&5&6&1&0&0&0&0&6&3&9&7&8&6&7&6&9&4&2\\
2&3&3&3&4&5&6&1&0&0&0&8&6&10&9&7&5&6&7&7&3&4\\
2&2&3&3&3&4&5&6&1&0&0&9&8&9&10&9&7&5&6&5&5&6\\
2&2&2&3&3&3&4&5&6&1&0&8&9&10&9&10&9&7&5&5&4&8\\
1&2&2&2&3&3&3&4&5&6&1&9&8&8&10&9&7&9&7&7&6&8\\
1&1&2&2&2&3&3&3&4&5&6&8&9&7&8&10&5&7&9&8&7&9\\
0&1&1&2&2&2&3&3&3&4&5&9&8&5&7&8&4&5&7&6&5&7\\
0&0&1&1&2&2&2&3&3&3&4&7&9&4&5&7&3&4&5&4&4&5\\
0&0&0&1&1&2&2&2&3&3&3&6&7&6&4&5&2&3&4&3&2&4\\
0&0&0&0&1&1&2&2&2&3&3&5&6&4&6&4&1&2&3&2&2&3\\
0&0&0&0&0&1&1&2&2&2&3&4&5&3&4&6&1&1&2&1&1&2\\
0&0&0&0&0&0&1&1&2&2&2&3&4&2&3&4&3&1&1&0&0&1\\
0&0&0&0&0&0&0&1&1&2&2&2&3&1&2&3&2&3&1&0&0&0\\
0&0&0&0&0&0&0&0&1&1&2&1&2&1&1&2&1&2&3&0&-1&-1\\
0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&2&2&-1&-2\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&1&1&-2
\end{pmatrix}.$$

So we have $A' = B^{-1}AB = M^{-1}AM$. The two matrices B and M are defined over $\mathbb{Z}$ and have determinants $126823 \cdot 2665931$ and 2^{11} respectively, so for each prime ℓ one of them will provide an isomorphism over $\mathbb{Z}_\ell$. Therefore the modules are in the same genus. However we can verify using Oscar [77] that A and A' are not conjugate in $\mathrm{GL}_{22}(\mathbb{Z})$ and so the integral representations are not isomorphic.

5.2.2 Abelian Varieties from Modules

For the construction of abelian varieties from these $\mathbb{Z}[G]$-modules, we follow the construction of Milne detailed in Section 2.5. Recall that given a $\mathbb{Z}[G_k]$-module M and an abelian variety A/k, we can construct an abelian variety $M \otimes A$. This is defined over k, but over $\bar{k}$ it becomes isomorphic to a power of A. Recall Lemma 2.5.5:

Lemma 5.2.6 (= [69] Prop. 6(a))**.** *Suppose M and N are $\mathbb{Z}[G_k]$-modules, isomorphic as groups to $\mathbb{Z}^n$, and on which G_k acts via a finite quotient. Suppose $\phi : M \to N$ is a homomorphism of $\mathbb{Z}[G_k]$-modules with finite cokernel. Then $\phi_A : M \otimes A \to N \otimes A$ is an isogeny defined over k, and its degree is $|\mathrm{coker}(\phi)|^{2\dim(A)}$.*

The following result is a partial converse to this lemma.

Lemma 5.2.7. *Suppose A/k is an abelian variety with $\mathrm{End}_{\bar{k}}(A) \cong \mathbb{Z}$. Then if M and N are as in Lemma 5.2.6, and $M \otimes A$ is isogenous to $N \otimes A$ by an isogeny of degree d*

over k, then there is a homomorphism of $\mathbb{Z}[G_k]$-modules from M to N with cokernel of size $d^{1/2\dim(A)}$. In particular, if $M \otimes A$ and $N \otimes A$ are isomorphic over k, then M and N are isomorphic as $\mathbb{Z}[G_k]$-modules.

Proof. First, let us fix some notation. By the construction of $M \otimes A$, detailed in Section 2.5, we have isomorphisms $\psi_M : \mathbb{Z}^n \to M$ and $\psi_{M\otimes A} : (A_{\bar{k}})^n \to (M \otimes A)_{\bar{k}}$ defined over $\bar{k}$, and similarly for N. Denote the ring isomorphism $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n) \to \mathrm{End}_{\bar{k}}(A^n)$ used in the construction of $M \otimes A$ and $N \otimes A$ by ρ (this also induces an isomorphism between the corresponding automorphism groups). For now, let the action of $\sigma \in G_k$ on a module or variety X be written as $\chi_X(\sigma)$, and then define cocycles from G_k to $\mathrm{Aut}(\mathbb{Z}^n)$ and $\mathrm{Aut}_{\bar{k}}(A^n)$ by

$$s_M(\sigma) = \psi_M^{-1} \circ \chi_M(\sigma) \circ \psi_M \circ \chi_{\mathbb{Z}^n}(\sigma^{-1})$$
$$s_{M\otimes A}(\sigma) = \psi_{M\otimes A}^{-1} \circ \chi_{(M\otimes A)_{\bar{k}}}(\sigma) \circ \psi_{M\otimes A} \circ \chi_{(A_{\bar{k}})^n}(\sigma^{-1})$$

and similarly for N. Note that we view $\mathbb{Z}^n$ as a trivial Galois module. These may also be written as $s_M(\sigma) = \psi_M^{-1}\psi_M^{\sigma}$ and $s_{M\otimes A}(\sigma) = \psi_{M\otimes A}^{-1}\psi_{M\otimes A}^{\sigma}$. By construction of $M \otimes A$, $\rho(s_M) = s_{M\otimes A}$ and likewise for N. Henceforth, we will drop the notation χ_X.

Now suppose there is an isogeny $\phi_A : M \otimes A \to N \otimes A$ defined over k. We will reverse the construction from Section 2.5, and show that there is a $\mathbb{Z}[G_k]$-module homomorphism $\phi : M \to N$.

We define ϕ to be the map satisfying $\psi_N^{-1}\phi\psi_M = \rho^{-1}(\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A})$. We can illustrate this with reference to a diagram with two commutative squares. The map ϕ_A gives rise to an isogeny $A^n \to A^n$ (the second vertical arrow), i.e. an element of $\mathrm{End}_{\bar{k}}(A^n)$. Under the isomorphism ρ, this gives a homomorphism $\mathbb{Z}^n \to \mathbb{Z}^n$ (the third vertical arrow), and commutativity defines the map ϕ, which is therefore also a group homomorphism.

$$\begin{array}{ccc} M\otimes A & \xleftarrow{\psi_{M\otimes A}} & A^n \\ \downarrow{\scriptstyle \phi_A} & & \downarrow \\ N\otimes A & \xleftarrow{\psi_{N\otimes A}} & A^n \end{array} \qquad \begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\psi_M} & M \\ \downarrow & & \downarrow{\scriptstyle \phi} \\ \mathbb{Z}^n & \xrightarrow{\psi_N} & N \end{array}$$

Note that if ϕ_A is an isogeny, so is $\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A}$, which therefore corresponds to a matrix of rank n in $\mathrm{End}_{\bar{k}}(A^n) \cong \mathrm{End}(\mathbb{Z}^n) \cong M_n(\mathbb{Z})$. Hence ϕ is surjective and has finite cokernel, with order determined by Lemma 5.2.6.

Now we must prove that ϕ is a homomorphism of $\mathbb{Z}[G_k]$-modules. We need to show that $\sigma\phi = \phi\sigma$ for all $\sigma \in G_k$. To do this, we will use the fact that ϕ_A is defined over k, which is equivalent to the fact that $\sigma\phi_A = \phi_A\sigma$ for all $\sigma \in G_k$.

Note that $\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A}$ is an endomorphism of A^n defined over $\bar{k}$. However, in our case, because $\mathrm{End}_{\bar{k}}(A) \cong \mathbb{Z}$, all of these are given by $M_n(\mathbb{Z})$ and defined over k, so this map commutes with the action of G_k. Hence for any $\sigma \in G_k$, we have the following equality of maps $(A_{\bar{k}})^n \to (A_{\bar{k}})^n$:

$$\begin{aligned} s_{N\otimes A}(\sigma)\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A} &= \psi_{N\otimes A}^{-1}\sigma\psi_{N\otimes A}\sigma^{-1}\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A} \\ &= \psi_{N\otimes A}^{-1}\sigma\phi_A\psi_{M\otimes A}\sigma^{-1} \\ &= \psi_{N\otimes A}^{-1}\phi_A\sigma\psi_{M\otimes A}\sigma^{-1} \\ &= \psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A}s_{M\otimes A}(\sigma), \end{aligned}$$

where the second equality holds because σ commutes with $\psi_{N\otimes A}^{-1}\phi_A\psi_{M\otimes A}$, and the third because it commutes with ϕ_A.

Now apply ρ^{-1} to this to get

$$s_N(\sigma)\psi_N^{-1}\phi\psi_M = \psi_N^{-1}\phi\psi_M s_M(\sigma).$$

Because Galois acts trivially on $\mathbb{Z}^n$, this implies

$$\psi_N^{-1}\sigma\phi\psi_M = \psi_N^{-1}\phi\sigma\psi_M,$$

which tells us that ϕ commutes with σ. Hence ϕ is a homomorphism of $\mathbb{Z}[G_k]$-modules as required. Moreover, if $M\otimes A$ and $N\otimes A$ are isomorphic over k, M and N are isomorphic as $\mathbb{Z}[G_k]$-modules. □

Proof of Theorem 5.2.1. Let M and N be the two $\mathbb{Z}[C_{23}]$-modules which are not isomorphic but are in the same genus, as in Example 5.2.5. Let ℓ be any prime. As

$M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, we also have $M \otimes_{\mathbb{Z}} \mathbb{Z}_{(\ell)} \cong N \otimes_{\mathbb{Z}} \mathbb{Z}_{(\ell)}$ ([31], Cor. 76.9). This implies there is an injective homomorphism $M \to N$ with finite cokernel of order coprime to ℓ. Pick a number field L with $\mathrm{Gal}(L/\mathbb{Q}) \cong C_{23}$, for example $\mathbb{Q}(\zeta_{47})^+$, and let $G_{\mathbb{Q}}$ act on M and N via the corresponding C_{23} quotient.

Now pick an elliptic curve E over $\mathbb{Q}$, with no potential complex multiplication. By Lemma 5.2.6, $M \otimes E$ and $N \otimes E$ are related by an isogeny of degree coprime to ℓ for each ℓ. However, by Lemma 5.2.7 they are not isomorphic over $\mathbb{Q}$. □

Remark 5.2.8. $M \otimes E$ and $N \otimes E$ are defined over $\mathbb{Q}$, and isomorphic over $\bar{\mathbb{Q}}$ to E^{22}. In fact, they are isomorphic over L, because M and N are isomorphic as $\mathbb{Z}[G_L]$-modules, where G_L acts trivially.

Remark 5.2.9. We can do a similar construction for modules over $\mathbb{Z}[G]$ for other G, giving abelian varieties which become isomorphic over extensions with Galois group G. Examples which work include all cyclic groups C_p with p a prime at least 23, as $\mathbb{Q}(\zeta_p)$ always has class number greater than 1 ([96] Theorem 11.1). We can also use any group with non-trivial locally free class group (see Definition 5.4.6), as for these groups there exists a $\mathbb{Z}[G]$-module in the genus of $\mathbb{Z}[G]$ but not isomorphic to it. The smallest of these is Q_8. This set includes all non-abelian, non-dihedral groups other than A_4, A_5 and S_4 ([33], Theorem 50.29), with C_{12} and D_{80} being the smallest abelian and dihedral examples respectively.

5.3 Elliptic Curves

It is natural to ask whether we can have a similar example with elliptic curves. In this section we shall show that this is possible over number fields, but not over $\mathbb{Q}$. We will begin by showing a converse to Proposition 5.1.1, specifically that if all the Tate modules of two abelian varieties are isomorphic, then for any prime ℓ we have an isogeny between them of degree coprime to ℓ.

Lemma 5.3.1. *Suppose A and B are n-dimensional abelian varieties over a number field k with $T_\ell A \cong T_\ell B$ as G_k-modules. Then there is an isogeny $A \to B$ with degree coprime to ℓ.*

Proof. Faltings ([47], Section 5 Cor. 1) showed that

$$\mathrm{Hom}_{G_k}(T_\ell A, T_\ell B) \cong \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B),$$

so if $T_\ell A \cong T_\ell B$, there must be an isogeny $A \to B$. Suppose for contradiction that all isogenies $A \to B$ have degrees divisible by ℓ. Now consider the map induced by an isogeny ϕ on $T_\ell A$. As it has degree divisible by ℓ, ϕ maps some element of $A[\ell]$ to 0. So the induced map $T_\ell A \to T_\ell B$ cannot be surjective. As it is not invertible, when written as a matrix in $M_{2n}(\mathbb{Z}_\ell)$ in any basis, it must have determinant divisible by ℓ.

Now $\mathrm{Hom}_k(A,B) = \langle \phi_1, \phi_2, \ldots, \phi_t \rangle$ for some isogenies ϕ_i. Let each ϕ_i induce a linear map with matrix M_i on the Tate modules. Now any non-zero $\mathbb{Z}$-linear combination of these M_i comes from an isogeny, so must have determinant divisible by ℓ.

Suppose $T_\ell A$ and $T_\ell B$ are isomorphic. Then by Faltings' result the isomorphism between them corresponds to some $\sum_i \beta_i \phi_i$, with $\beta_i \in \mathbb{Z}_\ell$. This has matrix $\sum_i \beta_i M_i$, with determinant $P(\beta_1, \ldots, \beta_t)$ which is not divisible by ℓ. Here P is some polynomial with coefficients in $\mathbb{Z}_\ell$. Now pick $\alpha_i \in \mathbb{Z}$ with $\alpha_i \equiv \beta_i \pmod{\ell}$. Then $\det(\sum_i \beta_i M_i) \equiv \det(\sum_i \alpha_i M_i) \pmod{\ell}$, as the determinant of $\sum_i \alpha_i M_i$ is $P(\alpha_1, \ldots, \alpha_t)$ and P is a polynomial. But $\sum_i \alpha_i M_i$ is the matrix corresponding to $\sum_i \alpha_i \phi_i$ which has determinant divisible by ℓ, because it is an isogeny (or the zero map). This is a contradiction, so we must have an isogeny of degree coprime to ℓ. □

Remark 5.3.2. Combining this theorem with Proposition 5.1.1, we see that if $T_\ell A \cong T_\ell B$ for all primes ℓ, then A and B have the same Selmer groups, regulators, and all the other properties listed in Theorem 5.0.2.

Corollary 5.3.3. *If A is an abelian variety with $\mathrm{End}_k(A) \cong \mathbb{Z}$, and $T_\ell A \cong T_\ell B$ as G_k-modules for all primes ℓ, then A and B are isomorphic over k.*

Proof. Pick isogenies $\phi : A \to B$, and $\phi' : B \to A$. We have an injective map $\mathrm{End}_k(A) \to \mathrm{Hom}_k(A,B)$ given by $\psi \mapsto \phi \circ \psi$, and also an injective map $\mathrm{Hom}_k(A,B) \to \mathrm{End}_k(A)$ given by $\psi \to \phi' \circ \psi$. Hence $\mathrm{Hom}_k(A,B) \cong \mathbb{Z}$. This must

be the set of multiples of some isogeny $\bar{\phi}$, with all degrees divisible by $\deg(\bar{\phi})$. Hence by Lemma 5.3.1, $\bar{\phi}$ must be an isomorphism. □

Remark 5.3.4. For elliptic curves E over $\mathbb{Q}$, $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathbb{Z}$, so knowing the Tate modules determines the elliptic curve up to isomorphism.

Proposition 5.3.5. *Suppose E and E' are elliptic curves over a number field k, and $\mathrm{End}_k(E)$ is an order of class number 1. Then if $T_\ell E \cong T_\ell E'$ as G_k-modules for all primes ℓ, then E and E' are isomorphic over k.*

Proof. E and E' are isogenous, so fix an isogeny $\psi : E' \to E$ defined over k. Then the map $\mathrm{Hom}_k(E,E') \to \mathrm{End}_k(E)$ given by $\phi \mapsto \psi\phi$ is an injection. If $\beta \in \mathrm{End}_k(E)$, $\phi\beta \in \mathrm{Hom}_k(E,E')$ maps to $\psi\phi\beta$. Therefore the image of this map is an ideal in $\mathrm{End}_k(E)$, hence generated by some element α. Let the preimage of α be ϕ_1. Then each element of the ideal is of the form $\alpha\beta$, which is the image of $\phi_1\beta$. Thus by injectivity all elements of $\mathrm{Hom}_k(E,E')$ are of this form and have degree divisible by $\deg(\phi_1)$. So as there are isogenies $E \to E'$ of degree coprime to any prime, E and E' are isomorphic. □

It is however possible to have non-isomorphic elliptic curves with isogenies of coprime degrees between them. By Corollary 5.3.3 and Proposition 5.3.5, we know this can only happen for elliptic curves with complex multiplication by an order which has class number greater than 1. This allows us to prove the following:

Theorem 5.3.6. *There exists a number field k, and elliptic curves E and E' defined over k, which are not isomorphic over $\bar{k}$, such that E and E' have the same properties as listed in Theorem 5.0.2 over all number fields F containing k.*

Proof. Take the lattices $\Lambda = \mathbb{Z}[\sqrt{-5}]$ and $\Lambda' = (2, 1+\sqrt{-5})\Lambda$. Then $E := \mathbb{C}/\Lambda$ and $E' := \mathbb{C}/\Lambda'$ have complex multiplication by $\mathbb{Z}[\sqrt{-5}]$ ([89], Chapter II Section 1). By ([89] Proposition II.1.2), the corresponding elliptic curves are not isomorphic, as $(2, 1+\sqrt{-5})$ is not a principal ideal. However, there is an isogeny of degree $\mathrm{N}(\mathbf{a})$ for any ideal $\mathbf{a}$ in the class of $(2, 1+\sqrt{-5})$, and hence there are isogenies of degrees 2 and 3 ([89], Corollary II.1.5). These curves are defined and have

complex multiplication over the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$, which is $\mathbb{Q}(i,\sqrt{5})$ ([89] Section II.2 and Theorem II.4.3(a)). The isogenies may be defined over some finite extension. Then, by Proposition 5.1.1, the curves over that extension have the same properties as listed in Theorem 5.0.2. □

Example 5.3.7. We can construct an example of these elliptic curves entirely explicitly, giving Weierstrass equations. Using Sage [91], we can approximate the j-invariant of Λ to a high precision, and then search for polynomials this may satisfy. We find that the j-invariant is likely to be $632000+282880\sqrt{5}$. An elliptic curve with this j-invariant is

$$E_1 : y^2 = x^3 - (2395312128000 + 1071214510080\sqrt{5})x$$
$$-2016549312397312000 + 901828270977187840\sqrt{5}.$$

Sage can compute the 2- and 3-isogenies from this curve. We find that over $\mathbb{Q}(i,\sqrt{5})$ it admits a 2-isogeny and two 3-isogenies, all to the same curve

$$E_2 : y^2 = x^3 + (-272250 + 41745\sqrt{5})x + 12644500 - 32369920\sqrt{5}.$$

Note that this is consistent with there being one ideal of norm 2, and two of norm 3, in $\mathbb{Z}[\sqrt{-5}]$. The elliptic curve E_2 has j-invariant $632000-282880\sqrt{5}$, so unlike the abelian varieties constructed in Section 5.2, E_1 and E_2 are not isomorphic over any number field. We can verify using Sage that these curves have complex multiplication by $\mathbb{Z}[\sqrt{-5}]$ by computing the CM discriminant to be -20. We can also calculate their period lattices and find that the ratios of their generators are very close to $\sqrt{-5}$ and $\frac{1+\sqrt{-5}}{2}$, matching the pair of elliptic curves used in the proof of Theorem 5.3.6.

5.4 A Weil restriction construction

5.4.1 Brauer Relations

In Section 5.2, we used the twisting construction to produce two isogenous abelian varieties. Recall that a particularly useful case of this construction is on modules of the form $\mathbb{Z}[G/H]$. This gives Weil restrictions, whose properties are strongly linked

to those of the elliptic curve we start with. Therefore we might ask whether we can do a similar construction with these modules. We will consider dihedral groups of order D_{2pq}, as these can give isogenies of different degrees.

Lemma 5.4.1. *Let p be an odd prime, and suppose F/k is a D_{2p}-extension of number fields, with intermediate fields L and K of degrees p and 2 respectively. Let E be an elliptic curve over k. Let ℓ be a prime different to p. Then there is an isogeny $\mathrm{Res}_{F/k}(E) \times E^2 \to \mathrm{Res}_{K/k}(E) \times \mathrm{Res}_{L/k}(E)^2$ defined over k, whose degree is not divisible by ℓ. There is a similar isogeny in the other direction.*

Proof. This follows from the existence of the Brauer relation $\{e\} + 2D_{2p} - C_p - 2C_2$ in D_{2p}. We can apply Lemma 4.1.2 to this to get the desired result. □

Now fix an elliptic curve E over k, and a dihedral extension K_{2pq} of order $2pq$, where $p \neq q$ are distinct odd primes. Let the Galois subextensions be K_2, K_{2p} and K_{2q}, and pick non-Galois subfields L_p and L_q contained in L_{pq}, where in each case the subscript is equal to the degree over k.

Now define abelian varieties by

$$A := \mathrm{Res}_{K_{2pq}/k}(E) \times \mathrm{Res}_{L_q/k}(E)^2 \times \mathrm{Res}_{L_p/k}(E)^2 \times \mathrm{Res}_{K_2/k}(E)$$
$$B := \mathrm{Res}_{L_{pq}/k}(E)^2 \times \mathrm{Res}_{K_{2q}/k}(E) \times \mathrm{Res}_{K_{2p}/k}(E) \times E^2.$$

Proposition 5.4.2. *For all primes ℓ, there is an isogeny $A \to B$, defined over k, with degree not divisible by ℓ.*

Proof. Suppose $\ell \neq p$. Then K_{2pq}/L_q is a D_{2p}-extension, and by Lemma 5.4.1 there is an isogeny

$$\mathrm{Res}_{K_{2pq}/L_q}(E) \times \mathrm{Res}_{L_q/L_q}(E)^2 \to \mathrm{Res}_{L_{pq}/L_q}(E)^2 \times \mathrm{Res}_{K_{2q}/L_q}(E)$$

with degree coprime to ℓ. Therefore the same holds when we take the Weil restrictions

to $\mathbb{Q}$. Similarly there is an isogeny

$$\mathrm{Res}_{L_p/k}(E)^2 \times \mathrm{Res}_{K_2/k}(E) \to \mathrm{Res}_{K_{2p}/k}(E) \times E^2$$

with degree coprime to ℓ, thus there is such an isogeny $A \to B$. In the case $\ell = p$, we instead break it down as $\mathrm{Res}_{K_{2pq}/k}(E) \times \mathrm{Res}_{L_p/k}(E)^2 \to \mathrm{Res}_{L_{pq}/k}(E)^2 \times \mathrm{Res}_{K_{2p}/k}(E)$ and $\mathrm{Res}_{L_q/k}(E)^2 \times \mathrm{Res}_{K_2/k}(E) \to \mathrm{Res}_{K_{2q}/k}(E) \times E^2$. Using Lemma 5.4.1 again on both of these we get an isogeny of degree coprime to ℓ. □

Remark 5.4.3. A slightly different construction works when one of the primes is equal to 2. There are two non-conjugate subgroups of D_{4q} isomorphic to D_{2q}; call them D_{2q}^a and D_{2q}^b with subgroups of order 2 C_2^a and C_2^b respectively, chosen such that the product of their generators is a rotation of order 2. Call the subgroup generated by this rotation C_2', and the union of these three groups $C_2 \times C_2$.

Let K be an extension of k with Galois group D_{4q}. Now define varieties by

$$A := \mathrm{Res}_{K/k}(E)^2 \times \mathrm{Res}_{K^{D_{2q}^a}/k}(E)^2 \times \mathrm{Res}_{K^{D_{2q}^b}/k}(E)^2 \times \mathrm{Res}_{K^{C_2 \times C_2}/k}(E)^4 \times \mathrm{Res}_{K^{C_{2q}}/k}(E)^2$$

$$B := \mathrm{Res}_{K^{C_2^a}/k}(E)^2 \times \mathrm{Res}_{K^{C_2^b}/k}(E)^2 \times \mathrm{Res}_{K^{C_2'}/k}(E)^2 \times \mathrm{Res}_{K^{C_q}/k}(E)^2 \times E^4.$$

Then we can prove the same conclusion as in Proposition 5.4.2 by similar arguments. We will need an equivalent to Lemma 5.4.1 for the Brauer relation in $C_2 \times C_2$ given by $\{e\} + 2C_2 \times C_2 - C_2^a - C_2^b - C_2'$. Here we can get isogenies of degree coprime to any prime $\ell \neq 2$, by the same arguments as in Lemma 4.1.2.

The existence of isogenies between these varieties A and B can be seen from a Brauer relation in D_{2pq}. The next proposition will show that this is the only Brauer relation in D_{2pq} which works.

Proposition 5.4.4. *In the pq odd case, the Brauer relation*

$$\Theta = \{e\} + 2D_{2p} + 2D_{2q} + C_{pq} - 2C_2 - C_p - C_q - 2D_{2pq}$$

is the only one in D_{2pq} which gives an isogeny of degree coprime to any prime ℓ.

Proof. The rank of the lattice of Brauer relations in G is 3 by Lemma 2.6.3. To give the desired property for all elliptic curves, Lemma 5.2.7 implies that there must be a homomorphism of $\mathbb{Z}[G]$-modules between $\sum_i \mathbb{Z}[G/H_i]$ and $\sum_j \mathbb{Z}[G/H_j]$ with kernel coprime to any prime ℓ. Therefore the Brauer relation must be a $\mathbb{Z}_{(\ell)}$-relation for all ℓ, and in particular for p and q.

Now let $\Theta_p = \{e\} + 2D_{2p} - 2C_2 - C_p$. Θ_p is not a $\mathbb{Z}_{(p)}$-relation, as its regulator constant for the trivial module $\mathbf{1}$ is $1/p$. This contradicts Lemma 2.6.12, which tells us that if it were a $\mathbb{Z}_{(p)}$-relation, it would give a regulator constant with valuation 0. As the lattice of $\mathbb{Z}_{(p)}$-relations is saturated (Lemma 2.6.4), it must have rank at most 2. Similarly the lattice of $\mathbb{Z}_{(q)}$-relations is also of rank at most 2, however it does contain Θ_p. This is because D_{2p} is not q-hypo-elementary, so by Theorem 2.6.6 it contains a $\mathbb{Z}_{(q)}$-relation, which must be Θ_p as it is the only Brauer relation in D_{2p}. As these two lattices of rank at most 2 are saturated and not equal, their intersection has rank at most 1, so is spanned by Θ. □

Proposition 5.4.5. *In the case where $p = 2$, the only relations which are both $\mathbb{Z}_{(2)}$- and $\mathbb{Z}_{(q)}$-relations are multiples of*

$$\Theta = 1 + D_{2q}^a + D_{2q}^b + 2C_2 \times C_2 + C_{2q} - C_2^a - C_2^b - C_2' - C_q - 2D_{4q}.$$

Note that this is actually half of the relation that gives the A and B defined in Remark 5.4.3, however it is still a $\mathbb{Z}_{(2)}$- and $\mathbb{Z}_{(q)}$-relation by the saturation property, and the distinction will not matter for the proofs in Section 5.4.2.

Proof. The proof uses the same ideas as the odd case. We now have a four-

dimensional lattice of Brauer relations, spanned (over the rationals) by Θ and

$$\Theta_1 := 1 + 2D^a_{2q} - C_q - 2C^a_2$$
$$\Theta_2 := 1 + 2D^b_{2q} - C_q - 2C^b_2$$
$$\Theta_3 := 1 + 2C_2 \times C_2 - C^a_2 - C^b_2 - C'_2.$$

We know already that Θ is a $\mathbb{Z}_{(2)}$-relation because 2Θ is, and the lattice of $\mathbb{Z}_{(2)}$-relations is saturated. Also Θ_1 is the Brauer relation appearing in the non-2-hypo-elementary subgroup D^a_{2q}, so it is a $\mathbb{Z}_{(2)}$-relation, and similarly so is Θ_2. However Θ_3 is not a $\mathbb{Z}_{(2)}$-relation, because its regulator constant for the trivial representation is $\frac{1}{2}$. Therefore by the saturation property the lattice of $\mathbb{Z}_{(2)}$-relations is $\langle \Theta, \Theta_1, \Theta_2 \rangle$ (allowing rational multiples, as $\frac{1}{2}(\Theta_1 - \Theta_2)$ is a Brauer relation).

Now if there is another relation which is both a $\mathbb{Z}_{(2)}$-relation and a $\mathbb{Z}_{(q)}$-relation, it must be of the form $l\Theta + m\Theta_1 + n\Theta_2$ for rationals l, m and n. Therefore $m\Theta_1 + n\Theta_2$ must also be a $\mathbb{Z}_{(q)}$-relation. If we take its regulator constant with for the trivial representation, by the multiplicative property (Lemma 2.6.10), we find it to be $q^{-(m+n)}$, so we must have $m + n = 0$. Therefore the relation is a multiple of $\frac{1}{2}(\Theta_1 - \Theta_2) = D^a_{2q} - D^b_{2q} - C^a_2 + C^b_2$.

Now take the one-dimensional representation ε where D^a_{2q} acts trivially and the other elements act as -1. Its regulator constant for the relation $\frac{m}{2}(\Theta_1 - \Theta_2)$ is q^{-m}. Therefore to be a $\mathbb{Z}_{(q)}$-relation, we must have $m = 0$, so only Θ is both a $\mathbb{Z}_{(2)}$-relation and a $\mathbb{Z}_{(q)}$-relation.

□

5.4.2 Dihedral Modules are Isomorphic

Unfortunately, for small p and q the property proven in Proposition 5.4.2 forces the corresponding integral representations to be isomorphic.

As before, let $p \neq q$ be primes and let G be the dihedral group of order $2pq$. If

p and q are odd, define two $\mathbb{Z}[G]$-modules by

$$M := \mathbb{Z}[G/1] \oplus \mathbb{Z}[G/D_{2p}]^{\oplus 2} \oplus \mathbb{Z}[G/D_{2q}]^{\oplus 2} \oplus \mathbb{Z}[G/C_{pq}]$$
$$N := \mathbb{Z}[G/C_2]^{\oplus 2} \oplus \mathbb{Z}[G/C_p] \oplus \mathbb{Z}[G/C_q] \oplus \mathbb{Z}[G/G]^{\oplus 2}.$$

If $p = 2$, take instead the sum of two copies of these, one with each non-conjugate subgroup D_{2q} and corresponding C_2. Then A and B, as defined in Section 5.4, are given by $A = M \otimes E$ and $B = N \otimes E$, using the construction in [69] detailed in Section 2.5.

Take E to be such that $\mathrm{End}_{\bar{k}}(E) \cong \mathbb{Z}$. Now by Proposition 5.4.2 and Lemma 5.2.7, for any prime ℓ there is a map of $\mathbb{Z}[G]$-modules $M \to N$ with finite cokernel of order coprime to ℓ. This is equivalent to saying that $M \otimes_{\mathbb{Z}} \mathbb{Z}_{(\ell)} \cong N \otimes_{\mathbb{Z}} \mathbb{Z}_{(\ell)}$ as $\mathbb{Z}_{(\ell)}[G]$-modules, and hence by ([31], Cor. 76.9) that $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell[G]$-modules. This is true for all ℓ, that is, M and N are in the same genus.

Definition 5.4.6 (As in [33], 49.10)**.** Let H be a finite group. The locally free class group of $\mathbb{Z}[H]$ is the set of equivalence classes of $\mathbb{Z}[H]$-modules in the genus of $\mathbb{Z}[H]$, with the relation $X \sim Y$ if $X \oplus \mathbb{Z}[H]^m \cong Y \oplus \mathbb{Z}[H]^m$ for some integer m.

Example 5.4.7. The smallest group with non-trivial locally free class group is the quaternion group Q_8, which has class group of order 2. The elements can be given explicitly, as in [64] Section 1.

Proposition 5.4.8. *The class group of G is trivial for all $pq < 65$.*

Proof. These can be calculated using the algorithm in [13], for which Bley has made Magma code available [12]. □

Given integral representations M_1, M_2 and M_3 of a group H, in general we cannot say that $M_1 \oplus M_3 \cong M_2 \oplus M_3$ implies $M_1 \cong M_2$. This is unlike the case of representations over $\mathbb{Q}$. However, if M_2 and M_3 are both powers of the group ring $\mathbb{Z}[H]$, this cancellation often does hold.

Definition 5.4.9 (As in [76])**.** Let H be a finite group. We say $\mathbb{Z}[H]$ has stably

free cancellation if, whenever M' is a finitely-generated $\mathbb{Z}[H]$-module satisfying $M' \oplus \mathbb{Z}[H]^m \cong \mathbb{Z}[H]^{m+n}$, we have $M' \cong \mathbb{Z}[H]^n$.

Example 5.4.10. For all abelian groups H, $\mathbb{Z}[H]$ has stably free cancellation.

Proposition 5.4.11. *$\mathbb{Z}[G]$ has stably free cancellation.*

Proof. By ([76], Introduction), it suffices to show that G does not have a generalised quaternion group as a quotient, or one of the binary tetrahedral, octahedral or icosahedral groups as a proper quotient. The generalised quaternion groups are groups of the form $\langle x,y|x^{2n} = y^4 = 1, x^n = y^2, y^{-1}xy = x^{-1}\rangle$ for $n \geq 2$, which have order $4n$. The only quotients of D_{2pq} with size divisible by 4 are when $p = 2$, and are $C_2 \times C_2$ or the whole group. The group D_{4q} is not isomorphic to a generalised quaternion group as it contains $C_2 \times C_2$, whereas every abelian subgroup of a generalised quaternion group is cyclic. The binary tetrahedral, octahedral and icosahedral groups all have order divisible by 24, so cannot be a proper quotient of D_{2pq} for primes p and q. □

Lemma 5.4.12. *If the class group of G is trivial, $M \oplus \mathbb{Z}[G] \cong N \oplus \mathbb{Z}[G]$.*

Proof. Apply ([32], Theorem 31.28) to the faithful lattice $\mathbb{Z}[G]$, to deduce that $M \oplus \mathbb{Z}[G] \cong N \oplus F$ for some F in the genus of $\mathbb{Z}[G]$. Now F is an element of the class group of G, which is trivial, so there is some m satisfying $F \oplus \mathbb{Z}[G]^m \cong \mathbb{Z}[G]^{m+1}$. $\mathbb{Z}[G]$ has stably free cancellation, so $F \cong \mathbb{Z}[G]$, which proves the lemma. □

Definition 5.4.13. (As in [33], Definition 45.4) Suppose R is a Dedekind domain whose field of fractions is a global field K, and A is a simple K-algebra. Let a non-R prime of K be a prime not arising from a maximal ideal of R. For a prime P of K, let A_P be the P-adic completion of A. Then A satisfies the Eichler condition over R unless A_P is a direct sum of non-commutative skew-fields for every non-R prime P.

If A is a finite-dimensional semisimple K-algebra, we say it satisfies the Eichler condition over R if all its Wedderburn components do.

We will use this only in the case where $R = \mathbb{Z}$ and $K = \mathbb{Q}$, so the only non-R prime is the infinite place. All we need to know is the following lemma, together with the fact that products of algebras satisfying the Eichler condition also satisfy it.

Lemma 5.4.14. *([33], Proposition 51.2(ii)) Suppose $K = \mathbb{Q}$ and $R = \mathbb{Z}$. Then if D is a finite dimensional (over $\mathbb{Q}$) division algebra and $n > 1$, $M_n(D)$ is Eichler over $\mathbb{Z}$.*

Proposition 5.4.15. *M is an Eichler lattice, that is, $\mathrm{End}_{\mathbb{Q}[G]}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$ satisfies the Eichler condition over $\mathbb{Z}$.*

Proof. Let $\mathbb{Q} \otimes_{\mathbb{Z}} M \cong \bigoplus_i \rho_i^{n_i}$, where the ρ_i are irreducible rational representations of G. In this case we will show each $n_i \geq 2$, and hence $\mathrm{End}_{\mathbb{Q}[G]}(\mathbb{Q} \otimes_{\mathbb{Z}} M) \cong \bigoplus_i M_{n_i}(\mathrm{End}(\rho_i))$. We know $\mathrm{End}(\rho_i)$ is a division algebra and so by the previous lemma we are done.

First consider the odd case, and let the trivial representation be $\mathbf{1}$, the sign representation be ε, and the sum of all the two-dimensional irreducible complex representations be ρ. Then, by the same methods as in the proof of Lemma 4.1.1, we see that $\mathrm{Ind}_{C_2}^G(\mathbf{1}) = \mathbf{1} \oplus \rho$, so ρ is a rational representation. Now $\mathbb{Z}[G] \cong \mathbf{1} \oplus \varepsilon \oplus \rho^{\oplus 2}$, and $\mathbb{Z}[G/C_{pq}] \cong 1 \oplus \varepsilon$. Therefore each of $\mathbf{1}$, ε and ρ appears in M with multiplicity at least 2, so the same is true of the irreducible representations ρ_i.

The even case proceeds in a similar way. In the notation of the previous section, we now have the trivial representation $\mathbf{1}$, and one-dimensional representations ε_1, ε_2 and ε_3 with kernels C_{2q}, D_{2q}^a and D_{2q}^b respectively. Let ρ be the sum of the other complex irreducible representations. We can calculate that $\mathrm{Ind}_{C_2^a}^G(\mathbf{1}) = \mathbf{1} \oplus \varepsilon_2 \oplus \rho$, so ρ is a rational representation. We find that $\mathbb{Z}[G/C_{2q}] \cong 1 \oplus \varepsilon_1$, $\mathbb{Z}[G/D_{2q}^a] \cong 1 \oplus \varepsilon_2$ and $\mathbb{Z}[G/D_{2q}^b] \cong 1 \oplus \varepsilon_3$. The sum of these, together with $\mathbb{Z}[G]$, therefore contains every irreducible rational representation, with multiplicity at least 2, so M is an Eichler lattice. □

Theorem 5.4.16. *If the class group of G is trivial, then $M \cong N$ as $\mathbb{Z}[G]$-modules.*

Proof. Recall Jacobinski cancellation ([33], Theorem 51.28) tells us that if M is an Eichler lattice, $\mathbb{Z}[G]$ is a direct summand of M and $M \oplus \mathbb{Z}[G] \cong N \oplus \mathbb{Z}[G]$, then $M \cong N$. These conditions hold by Proposition 5.4.15, the construction of M and Lemma 5.4.12 respectively. □

Remark 5.4.17. This shows that $M \cong N$ for all $pq < 65$. However this proof fails infinitely often, beginning with $pq = 65$. This is because Cassou-Noguès proved that

the class group is non-trivial for infinitely many pairs of odd p and q ([21], Section 7).

Corollary 5.4.18. *For $pq < 65$, the abelian varieties A and B are isomorphic. It is therefore possible for distinct products of Weil restrictions of a single elliptic curve to be isomorphic.*

Question 5.4.19. Are M and N always isomorphic over $\mathbb{Z}[G]$? If so, are there other permutation modules in the same genus which are not isomorphic, leading to non-isomorphic products of Weil restrictions of a curve which cannot be distinguished by the properties listed in Theorem 5.0.2?

Bibliography

[1] David L. Armacost and William L. Armacost, *On p-thetic groups*, Pacific J. Math. **41** (1972), 295–301. MR330343

[2] Alex Bartel, *Large Selmer groups over number fields*, Math. Proc. Cambridge Philos. Soc. **148** (2010), no. 1, 73–86. MR2575373

[3] ———, *On Brauer-Kuroda type relations of S-class numbers in dihedral extensions*, J. Reine Angew. Math. **668** (2012), 211–244. MR2948877

[4] Jamie Bell, *p^∞-Selmer ranks of CM abelian varieties*, Bull. Lond. Math. Soc. **56** (2024), no. 8, 2711–2717. MR4795354

[5] ———, *A note on the growth of Sha in dihedral extensions*, Functiones et Approximatio Commentarii Mathematici (2025), 1 –6.

[6] ———, *Non-isomorphic abelian varieties with the same arithmetic*, 2025. URL: `https://arxiv.org/abs/2502.02254`.

[7] L. Alexander Betts and Vladimir Dokchitser, *Variation of Tamagawa numbers of semistable abelian varieties in field extensions*, Math. Proc. Cambridge Philos. Soc. **166** (2019), no. 3, 487–521. With an appendix by Dokchitser and Adam Morgan. MR3933907

[8] Manjul Bhargava and Arul Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621. MR3275847

[9] Bryan J. Birch and Nelson M. Stephens, *The parity of the rank of the Mordell–Weil group*, Topology **5** (1966), 295–299. MR201379

[10] Bryan J. Birch and Peter Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. MR179168

[11] Matthew Bisatt, *Explicit root numbers of abelian varieties*, Trans. Amer. Math. Soc. **372** (2019), no. 11, 7889–7920. MR4029685

[12] Werner Bley, *Publications of Werner Bley*. [Online; accessed 22 March 2025. URL: `https://www.mathematik.uni-muenchen.de/~bley/pub.php`. Code available at `https://www.mathematik.uni-muenchen.de/~bley/lfc/RelAlgKTheory.m`].

[13] Werner Bley and Robert Boltje, *Computation of locally free class groups*, Algorithmic number theory, 2006, pp. 72–86.

[14] Jeremy Booher, *Isogeny invariance of the BSD conjecture over number fields*, 2015. [Online; accessed 14 February 2025. URL: `https://virtualmath1.stanford.edu/~conrad/BSDseminar/Notes/L6.pdf`].

[15] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478

[16] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR1839918

[17] John W. S. Cassels, *Arithmetic on curves of genus* 1. *III. The Tate–Šafarevič and Selmer groups*, Proc. London Math. Soc. (3) **12** (1962), 259–296. MR163913

[18] ———, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. MR163915

[19] ———, *Arithmetic on curves of genus* 1. *VI. The Tate–Šafarevič group can be arbitrarily large*, J. Reine Angew. Math. **214/215** (1964), 65–70. MR162800

[20] ———, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR179169

[21] Philippe Cassou-Noguès, *Groupe des classes de l'algèbre d'un groupe métacyclique*, J. Algebra **41** (1976), no. 1, 116–136. MR417126

[22] Kęstutis Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math. **719** (2016), 45–73. MR3552491

[23] Ching-Li Chai, Brian Conrad, and Frans Oort, *Complex multiplication and lifting problems*, American Mathematical Society, United States, 2013 (English).

[24] Sunil Chetty, *Arithmetic local constants for abelian varieties with extra endomorphisms*, Funct. Approx. Comment. Math. **55** (2016), no. 1, 59–81. MR3549013

[25] ———, *Comparing local constants of ordinary elliptic curves in dihedral extensions*, Funct. Approx. Comment. Math. **54** (2016), no. 2, 241–250. MR3513580

[26] Ching-Heng Chiu, *Strong Selmer companion elliptic curves*, J. Number Theory **217** (2020), 376–421. MR4140635

[27] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), no. 1, 19–97. MR2551757

[28] Lilybelle Cowland Kellock and Vladimir Dokchitser, *Root numbers and parity phenomena*, Bull. Lond. Math. Soc. **55** (2023), no. 6, 2557–2597. MR4689540

[29] John Cremona, *Numerical evidence for the Birch—Swinnerton-Dyer conjecture*, 2011. [Online; accessed 19 March 2025. URL: `https://johncremona.github.io/papers/bsd50.pdf`].

[30] Brendan Creutz and Robert L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, J. Algebra **372** (2012), 673–701. MR2990032

[31] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, A Wiley-Interscience publication, Interscience Publishers, 1962.

[32] ———, *Methods of representation theory with applications to finite groups and orders*, Pure and applied mathematics, John Wiley & Sons, 1981.

[33] ———, *Methods of representation theory with applications to finite groups and orders*, Pure and applied mathematics, John Wiley & Sons, 1987.

[34] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. MR2020572

[35] Alexei Davydov, *Twisted automorphisms of group algebras*, Noncommutative structures in mathematics and physics, 2010, pp. 131–150. MR2742735

[36] Thomas de La Rochefoucauld, *Invariance of the parity conjecture for p-Selmer groups of elliptic curves in a D_{2p^n}-extension*, Bull. Soc. Math. France **139** (2011), no. 4, 571–592. MR2869306

[37] Max Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. III*, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1956** (1956), 37–76. MR79611

[38] Tim Dokchitser, *Notes on abelian varieties [part I]*. [Online; accessed 20 March 2025. URL: `https://people.maths.bris.ac.uk/~matyd/av1.pdf`].

[39] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71. MR2534092

[40] ———, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 2, 257–267. MR2475965

[41] ———, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596. MR2680426

[42] ———, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64. MR2831512

[43] Vladimir Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) **91** (2005), no. 2, 300–324. With an appendix by Tom Fisher. MR2167089

[44] ———, *A note on the parity conjecture and base change*, 2024. URL: `https://arxiv.org/abs/2407.18260`.

[45] Vladimir Dokchitser and Céline Maistret, *On the parity conjecture for abelian surfaces*, Proc. Lond. Math. Soc. (3) **127** (2023), no. 2, 295–365. With appendix A by Adam Morgan and appendix B by Tim Dokchitser and Vladimir Dokchitser. MR4626712

[46] David S. Dummit and Richard M. Foote, *Abstract algebra*, Third, John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[47] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **7**3 (1983), no. 3, 349–366; MR0718935; ibid. **7**5 (1984), no. 2, 381; MR0732554] by Edward Shipz. MR861971

[48] Matthias Flach, *A generalisation of the Cassels–Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. MR1079004

[49] Carolyn Gordon, David L. Webb, and Scott Wolpert, *One cannot hear the shape of a drum*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), no. 1, 134–138. MR1136137

[50] Holly Green and Céline Maistret, *The 2-parity conjecture for elliptic curves with isomorphic 2-torsion*, Proc. A. **478** (2022), no. 2265, Paper No. 20220112, 16. MR4492216

[51] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR833192

[52] Helmut Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod.p ist*, Math. Ann. **166** (1966), 19–23. MR205975

[53] Kazuya Kato and Fabien Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*, Invent. Math. **153** (2003), no. 3, 537–592. MR2000469

[54] Timo Keller and Michael Stoll, *Complete verification of strong BSD for many modular abelian surfaces over* $\mathbf{Q}$, Forum Math. Sigma **13** (2025), Paper No. e20, 82. MR4856933

[55] Remke Kloosterman, *The p-part of the Tate–Shafarevich groups of elliptic curves can be arbitrarily large*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 787–800. MR2212126

[56] Victor A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671. MR954295

[57] Alexandros Konstantinou, *A note on the order of the Tate–Shafarevich group modulo squares*, 2024. URL: `https://arxiv.org/abs/2404.16785`.

[58] Kenneth Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR597871

[59] Kenneth Kramer and Jerrold Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352. MR664648

[60] Serge Lang and John Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684. MR106226

[61] Rudolf Lidl and Harald Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1996.

[62] Carl-Erik Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, University of Uppsala, Uppsala, 1940. Thesis. MR22563

[63] The LMFDB Collaboration, *The L-functions and modular forms database*, 2025. [Online; accessed 14 February 2025. URL: `https://www.lmfdb.org`].

[64] Jacques Martinet, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 399–408. MR291208

[65] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. MR2373150

[66] ———, *Selmer companion curves*, Trans. Amer. Math. Soc. **367** (2015), no. 1, 401–421. MR3271266

[67] Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, Math. Comp. **82** (2013), no. 281, 513–529. MR2983034

[68] James S. Milne, *Elements of order p in the Tate–Šafarevič group*, Bull. London Math. Soc. **2** (1970), 293–296. MR277507

[69] ———, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR330174

[70] ———, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533. MR414558

[71] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 103–150. MR861974

[72] ———, *Arithmetic duality theorems*, Second Edition, BookSurge, LLC, 2006.

[73] Adam Morgan, *2-Selmer parity for hyperelliptic curves in quadratic extensions*, Proc. Lond. Math. Soc. (3) **127** (2023), no. 5, 1507–1576. MR4668529

[74] Jan Nekovář, *Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)*, Compos. Math. **151** (2015), no. 9, 1626–1646. MR3406439

[75] ———, *Compatibility of arithmetic and algebraic local constants, II: the tame abelian potentially Barsotti–Tate case*, Proc. Lond. Math. Soc. (3) **116** (2018), no. 2, 378–427. MR3764064

[76] John Nicholson, *A cancellation theorem for modules over integral group rings*, Math. Proc. Cambridge Philos. Soc. **171** (2021), no. 2, 317–327. MR4299591

[77] The OSCAR Team, *Oscar – Open Source Computer Algebra Research system, Version 1.3.0-DEV*, 2025. [`https://www.oscar-system.org`].

[78] Hwasin Park, *Relations among Shafarevich–Tate groups*, Sūrikaisekikenkyūsho Kōkyūroku **998** (1997), 117–125. Algebraic number theory and related topics (Japanese) (Kyoto, 1996). MR1622099

[79] Bjorn Poonen and Michael Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984

[80] David E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compositio Math. **100** (1996), no. 3, 311–349. MR1387669

[81] Karl Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), no. 3, 527–559. MR903383

[82] Igor R. Šafarevič, *The group of principal homogeneous algebraic manifolds*, Dokl. Akad. Nauk SSSR **124** (1959), 42–43. MR106227

[83] Ernst S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362 (1 plate). MR41871

[84] ———, *A conjecture concerning rational points on cubic curves*, Math. Scand. **2** (1954), 49–54. MR62767

[85] Jean-Pierre Serre, *Facteurs locaux des fonctions zêta des varietés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 1: Exposés 1 à 15; Fasc. 2: Exposés 16 à 24, 1970, pp. 15. MR3618526

[86] ———, *Linear representations of finite groups*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. MR0450380 (56 #8675)

[87] ———, *Local fields*, Graduate texts in mathematics, Springer, 1979.

[88] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210

[89] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate texts in mathematics, vol. 151, Springer-Verlag, 1994.

[90] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for GL_2*, Invent. Math. **195** (2014), no. 1, 1–277. MR3148103

[91] William A. Stein et al., *Sage Mathematics Software (Version 9.1)*, The Sage Development Team, 2020. [`http://www.sagemath.org`].

[92] Andrew V. Sutherland, *Stronger arithmetic equivalence*, Discrete Anal. (2021), Paper No. 23, 23. MR4341956

[93] John Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 1963, pp. 288–295. MR175892

[94] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, 1966, pp. 277–312.

[95] Thomas Vavasour and Christian Wuthrich, *Mordell–Weil group as Galois modules*, 2023. URL: `https://arxiv.org/abs/2306.13365`.

[96] Lawrence C. Washington, *Introduction to cyclotomic fields*, Second Edition, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575