Galois covers of curves and the Birch and Swinnerton-Dyer conjecture

Alexandros Konstantinou

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

December 28, 2024

I, Alexandros Konstantinou, 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. Chapters 2 (§§2.1–2.2), 3 and Appendix A are a result of joint work with A. Morgan. Chapters 4 and 5 are a result of joint work with V. Dokchitser, H. Green and A. Morgan.

Impact Statement

The Birch and Swinnerton-Dyer conjecture is one of the seven Millennium Prize Problems with significant implications for number theory and arithmetic geometry.

A major focus of this thesis is the parity conjecture which is a direct consequence of this conjecture. While considerable progress has been made for elliptic curves, much less is known in higher dimensions. A key result of this thesis is the development of a method for studying parities of ranks of Jacobians using local data. Such expressions are significant in number theory, as most progress towards the parity conjecture proceeds via the derivation of a local formula. Notably, in a joint work, we provide a local formula for arbitrary Jacobians, which could be a crucial first step toward proving the parity conjecture for Jacobians.

Another key focus of this thesis is the Tate–Shafarevich group, which poses a significant challenge in resolving the Birch and Swinnerton-Dyer conjecture. We provide a positive answer to a conjecture by Stein concerning the possible orders of this group, shedding some light on this group's enigmatic nature.

Beyond academia, this work has potential implications in cryptography, a field that draws on the arithmetic of elliptic curves and, increasingly, higher-dimensional abelian varieties. Although our main focus is not on such applications, the methods developed here may be relevant to ongoing research in this area.

Abstract

The calculation of the rank of an abelian variety over a number field is a central, yet notoriously difficult, problem in number theory, intimately tied to the Birch and Swinnerton-Dyer conjecture.

In this work, we study two main aspects of this conjecture: the parity conjecture and the Tate–Shafarevich group. For the former, we investigate parities of ranks by using Galois covers of curves, isogenies and certain relations between permutation representations; for the latter, we use Galois extensions and isogenies to give a positive answer to a conjecture by Stein regarding the possible orders of Tate–Shafarevich groups of abelian varieties.

Acknowledgements

Having traversed the labyrinth of thesis writing, I now find calm waters in writing the acknowledgements.

First and foremost, I want to express my deepest gratitude to my advisor, Vladimir Dokchitser, for his constant support and guidance. His knowledge and generosity in sharing it have made this work possible. Thank you, Vladimir.

I am deeply grateful to my collaborators, Adam and Holly, for their invaluable contributions and many hours of collaboration. I would also like to extend my heartfelt thanks to my academic siblings: Lilybelle, Harry, David and Jamie. The sense of belonging you provided over the last four years has been greatly appreciated.

A warm thanks to my friends for providing a welcome escape from the rigours of research. Special thanks to Katerina, Eugenia, Costas, Pantelis, TD, Matthew and my brother Konstantinos.

Last, but certainly not least, I want to thank my parents, to whom I dedicate this work:

Αφιερώνω τη διδακτορική μου διατριβή στους γονείς μου, Αλεξάνδρα και Στέφανο. Σας ευχαριστώ για την αγάπη, την υπομονή και την ασταμάτητη υποστήριξή σας καθ' όλη τη διάρκεια αυτής της πορείας.

Contents

1 Introduction **9**

1.1 Birch and Swinnerton-Dyer and parities of ranks 9

1.2 Our approach: Galois covers 12

1.3 Arithmetic of Jacobians 14

1.4 The Tate–Shafarevich group up to squares 15

1.4.1 Tate–Shafarevich groups of non-square order 16

1.5 Brauer relations and isogenies 17

1.5.1 Uniform results for isogenies 19

1.6 Parities of ranks and Selmer groups 20

1.6.1 BSD and the parity conjecture for abelian varieties . . . 21

1.6.2 Parity of ranks through local expressions 22

1.6.3 A machine for computing parities of ranks 24

1.6.4 Parity of ranks of Jacobians 26

1.7 Structure of the thesis 27

1.8 Notation 28

2 Background **30**

2.1 Curves and their function fields 30

2.1.1 Definitions and conventions 30

2.1.2 Function fields 31

2.1.3 Generalisation to disconnected curves 35

2.2 Jacobians of curves 36

2.3 Birch and Swinnerton-Dyer invariants 39

2.3.1 Regulators, Tamagawa numbers and periods 39
2.3.2 Tate–Shafarevich group and deficiency 41

3 Arithmetic of Jacobians 43
3.1 Equivariant Riemann–Hurwitz formula 45
3.2 Galois descent and isotypic components 48
3.3 Self-duality of Selmer groups 50

4 Pseudo Brauer relations and regulator constants 52
4.1 Pseudo Brauer relations 52
4.2 Regulator constants 54
4.3 Computable sets of representations 59
4.4 Alternative definition of regulator constants 60

5 Rank parity from pseudo Brauer relations 66
5.1 Isogenies from pseudo Brauer relations 66
5.2 Local formulae for Selmer rank parities 70
5.2.1 A local formula in $\lambda_{\Theta,\Phi}(X/\mathcal{K})$ 72
5.2.2 The local invariant $\tilde{\lambda}_{\Theta}(X/\mathcal{K})$ 74
5.2.3 The invariant $\Lambda_{\Theta}(X/\mathcal{K})$ and a local formula 76

6 Applications of pseudo Brauer relations 81
6.1 Uniform approach: isogenies and parity 81
6.1.1 Isogenies from pseudo Brauer relations 82
6.1.2 Local formulae from regulator constants 83
6.2 Hyperelliptic curves over $K(\sqrt{d})$ 84
6.3 Richelot Isogeny 86
6.4 Prym varieties of trigonal curves 89
6.5 Elliptic curves with cyclic isogeny 91
6.6 Genus two curves with covers to elliptic curves 94
6.6.1 Genus two curves with extra involutions 94
6.6.2 Covers to elliptic curves of odd prime degree 95

6.6.3 Split genus two Jacobians and rank parity 99
6.7 Products of Weil-restrictions 102

7 Abelian varieties with prescribed Tate–Shafarevich group orders up to squares 104
7.1 The square-free part of the Tate–Shafarevich group 104
7.1.1 Cassels–Tate formula 104
7.1.2 An isogeny decomposition for the Weil-restriction 106
7.1.3 An expression for $|Ш(Y/L)|$ modulo squares 107
7.2 Tate–Shafarevich group of non-square order 108

A Homomorphisms between Jacobians from G-maps 114
A.1 Construction of f_Φ 115

Bibliography 118

Chapter 1

Introduction

A central problem in number theory is determining the set of rational solutions to polynomial equations. While this proves to be relatively straightforward for linear and quadratic polynomials, finding rational points on cubic equations requires a deeper theoretical approach.

This pursuit leads to the study of elliptic curves. In contrast to lower-degree cases, the rational points on an elliptic curve form a finitely generated abelian group, as established by the Mordell–Weil theorem.

Theorem 1.1 (Mordell–Weil)**.** *Let E be an elliptic curve over a number field K. Then the group $E(K)$ of K-rational points on E is finitely generated.*

1.1 Birch and Swinnerton-Dyer and parities of ranks

The rank of E/K, defined as $\mathrm{rk}(E/K) := \mathrm{rank}_{\mathbb{Z}}(E(K))$, is its main arithmetic invariant, though its computation is notoriously difficult. At the core of this problem lies the *Birch and Swinnerton–Dyer conjecture*, which relates the rank to the behaviour of a fundamental object associated with E/K, namely its Hasse–Weil L-function denoted $L(E/K, s)$.

Conjecture 1.2 (Birch–Swinnerton-Dyer)**.** *Let E be an elliptic curve over a number field K of discriminant Δ_K. Assume that $L(E/K, s)$ extends to an analytic function on $\mathbb{C}$. Then the following hold:*

1. $\mathrm{rk}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$,

2. *the Tate–Shafarevich group* $Ш(E/K)$ *is finite, and the leading coefficient of* $L(E/K, s)$ *at* $s = 1$ *is*

$$\mathrm{BSD}(E/K) := \frac{|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \cdot C(E/K)}{|E(K)_{\mathrm{tors}}|^2 \cdot \sqrt{|\Delta_K|}},$$

where $\mathrm{Reg}(E/K)$ *is the regulator,* $C(E/K)$ *the product of Tamagawa numbers (including real and complex periods) and* $E(K)_{\mathrm{tors}}$ *is the torsion subgroup of* $E(K)$*, see §2.3.*

We can then define a completed L-function $L^*(E/K, s)$ by multiplying $L(E/K, s)$ by a finite number of elementary factors. The *Hasse–Weil conjecture* predicts that that this satisfies a functional equation

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

where $w(E/K) \in \{\pm 1\}$. The vanishing assertion made by the Birch and Swinnerton-Dyer conjecture combines with this to give the parity conjecture.

Conjecture 1.3 (Parity conjecture)**.** *Let* E *be an elliptic curve over a number field* K*. Then,*

$$(-1)^{\mathrm{rk}(E/K)} = w(E/K),$$

and $w(E/K)$ *is the global root number of* E/K*.*

Variants of the parity conjecture are widespread in the literature. Applications include solving Hilbert's tenth problem [61] and proving the Birch and Swinnerton-Dyer conjecture for a positive proportion of elliptic curves defined over $\mathbb{Q}$ [5].

These works rely crucially on studying the global root number $w(E/K)$. This is defined independently of the L-function as a product over all places of its local root numbers, $\prod_v w(E/K_v)$, where the latter are purely local invariants defined in terms of the underlying local Galois representations.

Therefore, the parity conjecture predicts the following *local-to-global* expression:

$$(-1)^{\mathrm{rk}(E/K)} = \prod_v w_v(E/K_v).$$

The main advantage of this lies in the relative ease of calculating local invariants, a sharp contrast to the difficulty of determining the rank. Specifically, in the case of elliptic curves, local root numbers have been classified at all places. The majority of this classification is found in [30, Theorem 3.1]. To be precise, we have

$$w(E/K_v) = \begin{cases} -1, & \text{if } E \text{ has split multiplicative reduction or } v|\infty, \\ 1, & \text{if } E \text{ has good or non-split multiplicative reduction.} \end{cases}$$

Therefore, if E/K is semistable, then $w(E/K) = (-1)^{n+m}$, where n (resp., m) is the number of places with split multiplicative reduction (resp., archimedean places).

Example 1.4. Let $E/\mathbb{Q}$ be the elliptic curve with Weierstrass equation $y^2 + y = x^3 - x^2$. Then, $E/\mathbb{Q}$ has split multiplicative reduction at 11 and good reduction otherwise. Therefore,

$$w(E/\mathbb{Q}) = w(E/\mathbb{Q}_{11}) \cdot w(E/\mathbb{R}) = (-1)^2 = 1.$$

Consider K, an imaginary quadratic extension of $\mathbb{Q}$ in which 11 splits, say, into v_1 and v_2. Then, E/K has split multiplicative reduction at v_1, v_2. Therefore,

$$w(E/K) = w(E/K_{v_1}) \cdot w(E/K_{v_2}) \cdot w(E/\mathbb{C}) = (-1)^3 = -1.$$

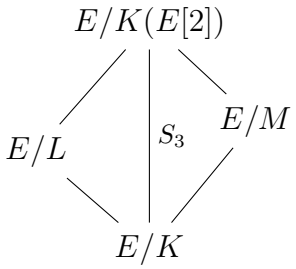
Assuming the parity conjecture, we expect that $\mathrm{rk}(E/\mathbb{Q}) < \mathrm{rk}(E/K)$ and therefore a point of infinite order in $E(K)$.

1.2 Our approach: Galois covers

Our work focuses on curves equipped with automorphisms, or equivalently field extensions of *function fields*. Recall there is a bijective correspondence between function fields over K (finitely generated extensions of K of transcendence degree one) and (smooth, projective) curves over K. This is established by the map $X \mapsto K(X)$ which sends X to its function field.

Under this equivalence, a Galois extension of function fields corresponds to a *Galois cover of curves* $f : X \to X/G$, where G is the Galois group. In addition, the function field of the quotient curve X/G coincides with the field of G-invariant functions $K(X)^G$, while the inclusion $K(X)^G \hookrightarrow K(X)$ corresponds to the cover $f : X \to X/G$.

This approach has proven particularly useful in the case where $\mathrm{Gal}(F/K)$ acts on the function field $F(X)$ of the base change of a curve X/K to F. In particular, this approach is found in various parity conjecture results including [31, 33, 55, 70]. For example, [31] shows the parity conjecture for elliptic curves over number fields follows from the finiteness of the Tate–Shafarevich group by studying an elliptic curve $E : y^2 = f(x)$ over its 2-torsion field $K(E[2])$. This generically forms the following S_3-extension of K:



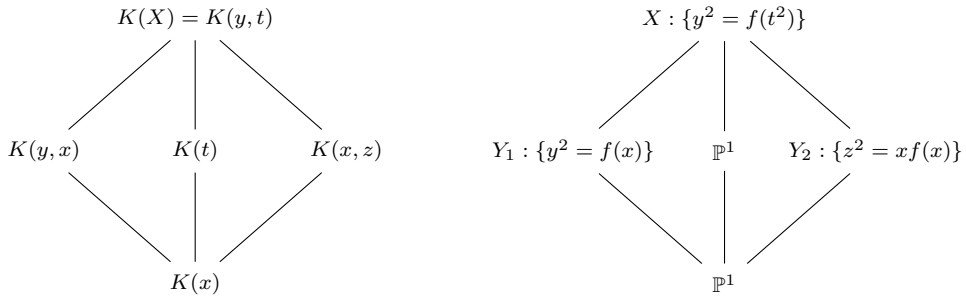
Here, $M = K[x]/(f(x))$ and $L = K(\sqrt{\mathrm{Disc} f(x)})$ are the respective cubic and quadratic extensions of K.

Example 1.5 (Hyperelliptic curve with extra involution)**.** Let X be a hyperelliptic curve with affine equation $y^2 = f(t^2)$. Then, its function field $K(X) = K(t, y)/(y^2 - f(t^2))$ has a $C_2 \times C_2$ action given $\sigma : (t, y) \mapsto (t, -y)$

and $\tau : (t, y) \mapsto (-t, y)$. It follows that

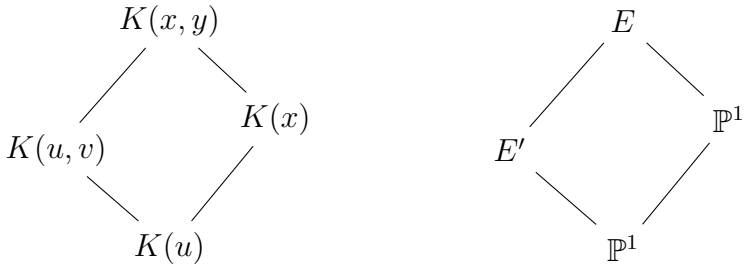
$$K(X)^{\langle\sigma\rangle} = K(t), \quad K(X)^{\langle\tau\rangle} = K(y, t^2), \quad K(X)^{\langle\sigma\tau\rangle} = K(t^2, yt).$$

Let $x = t^2$ and $z = yt$. The quotient of X by $\langle\sigma\rangle$ is a curve of genus 0 parametrised by t, while the quotients by $\langle\tau\rangle$ and $\langle\sigma\tau\rangle$ are $Y_1 : y^2 = f(x)$ and $Y_2 : z^2 = xf(x)$, respectively. This leads to the following extension of function fields with the corresponding covers on the right:



Example 1.6 (Elliptic curve with rational p-torsion)**.** Let E/K be the elliptic curve $y^2 = x^3 + ax + b$. Therefore, $K(E) \cong K(x, y)/(y^2 - (x^3 + ax + b))$.

Suppose that E has a K-rational point P of order p. Then $K(E)$ has a finite action by the dihedral group D_p induced by the translation morphism $Q \mapsto Q + P$ and the hyperelliptic involution $(x, y) \mapsto (x, -y)$. Write E' for the target of the isogeny $E \to E/\langle P\rangle$. By Vélu's formulae, there are functions $u, v \in K(x, y)/(y^2 - f(x))$ for which $E' = \{v^2 = g(u)\}$. We acquire the following Galois diagram:



We conclude this section with the following technical remark.

Remark 1.7. Throughout this thesis, our notion of a curve is somewhat broader than is perhaps standard. Specifically, we adhere to Convention 2.1, which does not require curves to be geometrically connected. With this convention in place, we can treat Galois diagrams involving base-change, such as those in §1.2, as Galois covers of curves. See §§2.1- 2.2 for more details.

1.3 Arithmetic of Jacobians

A key component of our work involves studying the induced action of a finite group G on Jac_X, the Jacobian variety of X, and associated G-representations. We show that many fundamental properties of rational points, ℓ-adic representations and Tate–Shafarevich groups extend from the case of base-change.

Notation 1.8. We write $\langle , \rangle$ to denote the standard inner product on characters/representations of a finite group G. In order to compare characters, we fix arbitrary embeddings $\bar{\mathbb{Q}}_\ell \subseteq \mathbb{C}$ for all primes.

For a prime ℓ, we write $V_\ell(\mathrm{Jac}_X) = T_\ell(\mathrm{Jac}_X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, where $T_\ell(\mathrm{Jac}_X) := \varprojlim \mathrm{Jac}_X[\ell^n]$ denotes the integral ℓ-adic Tate module of Jac_X.

Proposition 1.9 (cf. Theorem 3.1)**.** *Let X/K be a curve over a number field and G a finite subgroup of K-automorphisms of X. Then, rational points and ℓ-adic Tate modules satisfy "Galois descent":*

1. $(\mathrm{Jac}_X(K) \otimes \mathbb{Q})^G \cong \mathrm{Jac}_{X/G}(K) \otimes \mathbb{Q}$,

2. *For any prime ℓ, $V_\ell(\mathrm{Jac}_X)^G \cong V_\ell(\mathrm{Jac}_{X/G})$,*

Moreover, if $Ш(\mathrm{Jac}_X)$ is finite, then so is $Ш(\mathrm{Jac}_{X/G})$.

Example 1.10. We consider Example 1.5 with $C_2 \times C_2 = \langle \sigma, \tau \rangle$. There are four irreducible representations $C_2 \times C_2 \to \{\pm 1\}$, and these are determined by the images of σ, τ. Let ψ, χ be the irreducible representations determined by by $\psi(\tau) = 1, \psi(\sigma) = -1$ and $\chi(\sigma) = \chi(\tau) = -1$.

Consider the decomposition $\mathrm{Jac}_X(K) \otimes \mathbb{Q} \cong \mathbb{1}^{\oplus a} \oplus \psi^{\oplus b} \oplus \chi^{\oplus c} \oplus (\psi \otimes \chi)^{\oplus d}$. Using Proposition 1.9(1) with $G = C_2 \times C_2$,

$$a = \langle \mathbb{1}, \mathrm{Jac}_X(K) \otimes \mathbb{Q} \rangle = \dim(\mathrm{Jac}_X(K) \otimes \mathbb{Q})^G \overset{\text{Prop. 1.9(1)}}{=} \mathrm{rk}(\mathrm{Jac}_{\mathbb{P}^1}(K)) = 0.$$

A similar computation with $G = \langle \tau \rangle$ gives

$$a + b = \langle \mathrm{Ind}_{\langle \tau \rangle}^G \mathbb{1}, \mathrm{Jac}_X(K) \otimes \mathbb{Q} \rangle = \dim(\mathrm{Jac}_X(K) \otimes \mathbb{Q})^{\langle \sigma \rangle} \overset{\text{Prop. 1.9(1)}}{=} \mathrm{rk}(\mathrm{Jac}_{Y_1}).$$

Thus, $b = \mathrm{rk}(\mathrm{Jac}_{Y_1})$. In particular, $\mathrm{Jac}_X(K) \otimes \mathbb{Q} \cong \psi^{\oplus \mathrm{rk}(\mathrm{Jac}_{Y_1})} \oplus \chi^{\oplus \mathrm{rk}(\mathrm{Jac}_{Y_2})}$. By arguing similarly, but applying Proposition 1.9(2) instead, we find that for any prime ℓ, $V_\ell(\mathrm{Jac}_X) \cong \psi^{\oplus 2\mathrm{dim}\mathrm{Jac}_{Y_1}} \oplus \chi^{\oplus 2\mathrm{dim}\mathrm{Jac}_{Y_2}}$.

Example 1.11. We consider Example 1.6. The irreducible representations of D_p over $\mathbb{Q}$ are $\mathbb{1}$ (trivial), τ (sign) and a $(p-1)$-dimensional ρ. As in Example 1.10, we decompose $E(K) \otimes \mathbb{Q} \cong \mathbb{1}^{\oplus a} \oplus \tau^{\oplus b} \oplus \rho^{\oplus c}$.

By applying Proposition 1.9(1) with $G = D_p$, we get $a = \mathrm{rk}(\mathrm{Jac}_{\mathbb{P}^1}) = 0$. Repeating the calculation with respect to C_p and C_2 we deduce that $b = \mathrm{rk}(E)$ and $c = 0$. Therefore, $\mathrm{E}(K) \otimes \mathbb{Q} \cong \tau^{\oplus \mathrm{rk}(E)}$. An identical argument shows that $V_\ell(E) \cong \tau^{\oplus 2}$ for any prime ℓ.

1.4 The Tate–Shafarevich group up to squares

The Tate–Shafarevich group is a fundamental object in the study of rational points on abelian varieties. Despite its central role, many foundational questions about $Ш(A/K)$ remain unresolved. Paramount among these is the Tate–Shafarevich conjecture which asserts its finiteness. Although proven in specific cases [48, Corollary 14.3], [52, §4], the conjecture remains largely open.

Its asserted finiteness has significant implications for the Birch and Swinnerton-Dyer conjecture. In particular, Dokchitser–Dokchitser [31] show that the Tate–Shafarevich conjecture implies the parity conjecture for elliptic curves over number fields, while Kato–Trihan [47] prove that it implies the Birch and Swinnerton-Dyer conjecture for abelian varieties over function fields

over finite fields.

A natural question arises: assuming the finiteness of $Ш(A/K)$, what can be said about its size? The Cassels–Tate pairing sheds light on this question, as it imposes significant constraints on the structure of the Tate–Shafarevich group. This pairing was originally defined by Cassels for elliptic curves, later extended to abelian varieties by Tate to give a bilinear pairing

$$\langle , \rangle_{\mathrm{CT}} : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z},$$

where $A^\vee$ is the dual abelian variety. When $A = E$ is an elliptic curve, Cassels shows that this pairing is alternating under the natural identification of E with its dual $E^\vee$ [12]. In addition, Cassels shows that when $Ш(E/K)$ is finite, the pairing is also non-degenerate which implies that the order of $Ш(E/K)$ must be a perfect square (if finite).

The work of Flach [36] establishes the slightly weaker antisymmetric condition $\langle x, y\rangle = -\langle y, x\rangle$ for higher dimensional principally polarised abelian varieties. Tate notes that when $Ш(A/K)$ is finite, the pairing is non-degenerate [86] from which we can deduce that if A is principally polarised (i.e., has a polarisation of degree one), then $|Ш(A/K)|$ can only be a square or twice a square (again, if finite).

Building upon this, Poonen–Stoll [75] give a criterion for deducing if $|Ш(A/K)|$ is of square order when A is a principally polarised abelian variety. This purely depends on the vanishing of $\langle \xi, \xi \rangle_{\mathrm{CT}}$ for an element $\xi \in Ш(A/K)[2]$ canonically associated to A. They then use their criterion to present the first examples of abelian varieties for which the order of their Tate–Shafarevich groups is twice a square [75, Proposition 27].

1.4.1 Tate–Shafarevich groups of non-square order

The next natural question is whether there exists an abelian variety A for which $|Ш(A)|$ is neither a square nor twice a square. By drawing upon Mazur's notion of visibility, Stein [84] shows that for odd $p \leq 25000$, there exists an

abelian variety $A/\mathbb{Q}$ with $|Ш(A/\mathbb{Q})| \equiv p \bmod \mathbb{Q}^{\times 2}$. Additionally, Keil [49] gives explicit examples of abelian surfaces where the Tate–Shafarevich group is of order m times a square with $m \in \{2, 3, 5, 6, 7, 10, 13, 14\}$.

Motivated by this, Stein conjectures that every square-free natural number appears as the square-free part of $|Ш(A/\mathbb{Q})|$ for some abelian variety $A/\mathbb{Q}$. We give a positive answer to this conjecture.

Theorem 1.12 (Corollary 7.14)**.** *For every square-free natural number n, there exists an abelian variety $A/\mathbb{Q}$ with finite Tate–Shafarevich group of order nm^2 for some integer $m \geq 1$.*

The proof of this result relies on the isogeny decomposition of a Weil–restriction of an elliptic curve. Using a formula of Cassels–Tate (see (1.1) below), we relate the order of the Tate–Shafarevich group to Birch–Swinnerton-Dyer invariants. This, combined with known results on L-functions and the Birch–Swinnerton-Dyer conjecture, leads to the main result. Similar ideas are also used in [81] to construct geometrically simple abelian varieties $A_p/\mathbb{Q}$ with non-trivial $Ш(A_p/\mathbb{Q})[p]$. A similar result is found in [37], where geometrically simple abelian varieties over $\mathbb{Q}$ are constructed with arbitrarily large p-torsion in their Tate–Shafarevich groups.

1.5 Brauer relations and isogenies

A significant aspect of our work focuses on isogenies arising from *Brauer relations*. These are $\mathbb{Z}$-linear combinations of subgroups of a finite group G, say $\Theta = \sum_i H_i - \sum_j H'_j$, corresponding to permutation representation isomorphisms

$$\bigoplus_i \mathbb{Q}[G/H_i] \cong \bigoplus_j \mathbb{Q}[G/H'_j].$$

Applications of Brauer relations are significant in both number theory and geometry. In particular, Brauer and Kuroda were the first to consider these to study certain relations among class groups of number fields [8, 56]. Other applications include [2, 22] for studying relations among invariants of

number fields, [28, 30] for investigating parities of ranks and [3] for studying Riemannian manifolds.

Our work relies on a formalism originating in the work of Kani–Rosen [46] for constructing isogenies from Brauer relations. This finds applications in several works including [10, 17, 28].

Theorem 1.13 ([46, Theorem 2])**.** *Let X/K be a curve defined over a number field, G a finite subgroup of $\mathrm{Aut}_K(X)$ and $\Theta = \sum_i H_i - \sum_j H'_j$ a Brauer relation for G. Then, there exists an isogeny*

$$\prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i}.$$

Example 1.14. $C_2 \times C_2$ has a Brauer relation

$$\Psi = C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}.$$

By applying Theorem 1.13 to Example 1.5, we get an isogeny

$$\mathrm{Jac}_X \to \mathrm{Jac}_{Y_1} \times \mathrm{Jac}_{Y_2},$$

where $X : y^2 = f(t^2), Y_1 : y^2 = f(x)$ and $Y_2 : z^2 = xf(x)$. In particular, when f is a square-free cubic polynomial, this recovers the classical result that the Jacobian of the genus 2 curve $y^2 = f(t^2)$ is isogenous to a product of two elliptic curves.

Example 1.15. D_p has a Brauer relation

$$\Theta = C_p + 2C_2 - \{e\} - 2D_p.$$

Therefore, by applying Theorem 1.13 to Example 1.6, we get an isogeny

$$E \to E'.$$

This recovers the classical fact that, if E has a K-rational point P of order p, then there exists an isogeny $E \to E/\langle P \rangle$.

1.5.1 Uniform results for isogenies

We use a refined version of the Kani–Rosen construction, given in Theorem 5.3 below, based on *pseudo Brauer relations*. These are introduced in Chapter 4, and they extend the notion of Brauer relations.

We show that this refinement provides a powerful framework for inducing isogenies between Jacobians and for revisiting and reconstructing a wide range of classical isogenies. This idea stems from de Smit–Edixhoven [21], who verified that an isogeny between modular Jacobians arises from a Brauer relation for $\mathrm{PGL}_2(\mathbb{F}_p)$. This was originally derived by Chen [16] using the Selberg trace formula.

Adding on, in Examples 1.14–1.15 we show that we can use Brauer relations to reconstruct cyclic isogenies between elliptic curves and isogenies between Jacobians of genus 2 curves and products of elliptic curves. Theorem 6.4 below shows that we obtain the following isogenies using suitable pseudo Brauer relations (with certain assumptions in (3)–(5)):

1. Isogenies between elliptic curves,
2. Isogenies $\mathrm{Jac}_X \times \mathrm{Jac}_{X^d} \to \mathrm{Res}_K^{K(\sqrt{d})}\mathrm{Jac}_X$, where X/K is a hyperelliptic curve, X^d is its quadratic twist by $d \in K^\times$, and $\mathrm{Res}_K^{K(\sqrt{d})}$ denotes Weil-restriction from $K(\sqrt{d})$ to K,
3. Richelot isogenies between Jacobians of genus 2 curves,
4. Isogenies from Jacobians of genus 2 curves to products of elliptic curves,
5. Isogenies $\mathrm{Jac}_X \to \mathrm{Jac}_Y \times \mathrm{Jac}_Z$, where X is a curve that admits an unramified double cover to a trigonal curve Y, and Jac_Z is the associated Prym,
6. Isogenies between products of Weil-restrictions, $\prod_i \mathrm{Res}_K^{F^{H_i}}\mathrm{Jac}_Y \to \prod_i \mathrm{Res}_K^{F^{H'_j}}\mathrm{Jac}_Y$, where Y is a curve over K, F/K is a Galois extension

and $\sum H_i - \sum H'_j$ is a Brauer relation for the Galois group $\mathrm{Gal}(F/K)$ (see [60, Lemma 2.4]).

While establishing this result, we also address a question posed by Kuhn [57] regarding split genus 2 Jacobians. Specifically, for a genus 2 curve Y with a non-constant map $\phi : Y \to E$ to an elliptic curve, the Jacobian of Y is isogenous to the product of two elliptic curves, E and $\tilde{E}$. Kuhn notes that it is neither obvious nor always true that $\tilde{E}$ is uniquely determined, posing the problem of determining $\tilde{E}$. To address this, Kuhn constructs $\tilde{E}$ as a quotient of Jac_Y.

In our work, we use Galois theory to provide a canonical choice for $\tilde{E}$, identifying it as the Jacobian of a quotient curve under certain assumptions on the cover ϕ, see §6.6.3.

1.6 Parities of ranks and Selmer groups

Thus far, we have focused on two arithmetic invariants of an elliptic curve: the Mordell–Weil group $E(K)$ and the Tate–Shafarevich group $Ш(E/K)$. However, extracting information about these groups separately can be challenging without assuming the finiteness of $Ш(E/K)$.

As a result, it is often more convenient to work with *Selmer groups*, which are constructed from both of these. In particular, all progress towards the parity conjecture usually proceeds through a weaker version known as the p-parity conjecture formulated in terms of Selmer ranks.

For a fixed prime p, we write $X_p(E) := \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim \mathrm{Sel}_{p^n}(E/K), \mathbb{Q}_p/\mathbb{Z}_p)$ to denote the *dual p^∞-Selmer group*. Then, the p^∞-Selmer rank is defined as

$$\mathrm{rk}_p(E/K) = \dim_{\mathbb{Q}_p}(X_p(E/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

This satisfies $\mathrm{rk}_p(E/K) = \mathrm{rk}(E/K) + \delta_p(E/K)$, where $\delta_p(E/K)$ is determined by the decomposition $Ш(E/K)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p(E/K)} \times (\text{finite } p\text{-group})$ into its divisible and reduced parts.

Conjecture 1.16 (p-parity conjecture)**.** *Let E/K be an elliptic curve defined over a number field K and p a fixed prime. Then,*

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

We note that under the assumption that the Tate–Shafarevich group is finite, the p-parity conjecture is equivalent to the parity conjecture. Without a priori knowledge for this group however, this equivalence can fail, and these conjectures may even be inequivalent for different primes.

For elliptic curves over $\mathbb{Q}$, the p-parity conjecture is known for all p by the work of Dokchitser–Dokchitser [30]. This builds on works by Birch–Stephens [7], Greenberg [43], Guo [44], Kramer [54], Monsky [69], Nekovář [71] and Kim [50]. The p-parity conjecture was later extended to totally real fields by Nekovář [72], [73], [74], excluding some cases of potential complex multiplication when $p = 2$. These cases were later completed in [42]. For elliptic curves over number fields admitting a p-isogeny, the p-parity conjecture was proven by Dokchitser–Dokchitser in [27], [31] with some very mild assumptions on p. These exceptional cases were later dealt with in [15]. Additionally, the 2-parity conjecture for an elliptic curve E/K over a quadratic extension of K was proven by Kramer–Tunnell [55] and Dokchitser–Dokchitser [31].

1.6.1 BSD and the parity conjecture for abelian varieties

We will frequently consider parities of ranks of abelian varieties that are not elliptic curves. Most of the preceding discussion on rank parities (§§1.1 & 1.6) extends seamlessly to higher-dimensional cases.

To be precise, we can replace "E/K, an elliptic curve" with "A/K, an abelian variety" in the statements of Theorem 1.1 and Conjectures 1.2, 1.3, and 1.16 with the only exception being that $\mathrm{BSD}(E/K)$ is replaced with

$$\mathrm{BSD}(A/K) := \frac{|Ш(A/K)| \cdot \mathrm{Reg}(A/K) \cdot C(A/K)}{|A(K)_{\mathrm{tors}}| \cdot |A^\vee(K)_{\mathrm{tors}}| \cdot \sqrt{|\Delta_K|}^{\dim(A)}} \qquad (\dagger)$$

in Conjecture 1.2(2).

Parity-related problems for abelian varieties prove to be far more challenging. The most general result is by Coates–Fukaya–Kato–Sujatha [19], where the authors prove the p-parity conjecture for any abelian variety with a suitable p-power degree isogeny when p is an odd prime. For $p = 2$, V. Dokchitser–Maistret [33] prove the 2-parity conjecture for a broad class of semistable abelian surfaces. In addition, Morgan [70] proves the 2-parity conjecture for Jacobians of hyperelliptic curves over quadratic extensions with mild assumptions.

1.6.2 Parity of ranks through local expressions

Most parity-related results, including [19, 30, 31, 33, 42, 62, 70], rely crucially on the derivation of an expression of the form

$$\mathrm{rk}_p(A) = \sum_{v \text{ place of } K} \Lambda_v \mod 2,$$

where Λ_v is an explicit local invariant. The idea of such *local-to-global* expressions was first introduced by Birch [6, pp. 110] who noted that for an elliptic curve E with a p-isogeny $E \to E'$, "the parity of g (the rank of E) is determined by the Tamagawa ratio". Cassels later formalised this observation [14, Theorem 1.1] with the local formula

$$\mathrm{rk}_p(E/K) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_p \frac{C_v(E,\omega)}{C_v(E',\omega')} \mod 2, \qquad (\dagger\dagger)$$

where C_v denotes the Tamagawa number contribution as in §2.3.1. This formula is widely discussed in the literature, including works by Fisher [38, Appendix], Monsky [69, Corollary 2.8] and Dokchitser–Dokchitser [31, Theorem 5.2], [30, Remark 4.4]. Consequently, Kramer [54, Theorem 1] shows that if $K \subset F$ is a quadratic extension and E/K an elliptic curve, then

$$\mathrm{rk}_2(E/F) \equiv \sum_{v \text{ place of } K} \dim_{\mathbb{F}_2}\big(E(K_v)/\mathrm{Norm}_{F'_v/K_v} E(F_{v'})\big) \mod 2,$$

where v' is any place of F above v.

Both expressions closely resemble the assertion made by the parity conjecture but are independent of the Birch and Swinnerton-Dyer conjecture. This gives a natural strategy for proving the p-parity conjecture involving verifying compatibility between local root numbers and these local invariants. In the case of a p-isogeny between elliptic curves, this reduces to checking the following equality:

$$\prod_v w_v(E/K) \stackrel{?}{=} \prod_v (-1)^{\mathrm{ord}_p \frac{C_v(E,\omega)}{C_v(E',\omega')}}.$$

This is verified in [27] (under very mild assumptions) thereby proving the p-parity conjecture for elliptic curves with a p-isogeny.

The derivation of these expressions usually relies on a result by Cassels [14] and Tate [87], which proves that the Birch and Swinnerton-Dyer quotient (†) remains invariant under isogeny. Therefore, if $\phi : A \to B$ is an isogeny of abelian varieties, and assuming that the Tate–Shafarevich group is finite, we have the following relation:

$$\frac{\mathrm{Reg}(A/K)}{\mathrm{Reg}(B/K)} = \frac{|A(K)_{\mathrm{tors}}|\,|A^\vee(K)_{\mathrm{tors}}|\,C(B/K)}{|B(K)_{\mathrm{tors}}|\,|B^\vee(K)_{\mathrm{tors}}|\,C(A/K)} \prod_{p|\deg(\phi)} \frac{|Ш(B)[p^\infty]|}{|Ш(A)[p^\infty]|}. \qquad (1.1)$$

As an example, consider an elliptic curve E/K with a p-isogeny $E \to E'$. Then, both $Ш(E/K)[p^\infty]$ and $Ш(E'/K)[p^\infty]$ are of square order [12] (if finite) which gives

$$\frac{\mathrm{Reg}(E/K)}{\mathrm{Reg}(E'/K)} = \prod_v \frac{C_v(E,\omega)}{C_v(E',\omega')} \cdot \square.$$

(Here and below, $\square$ denotes a square of a rational number). A computation with heights shows that the ratio of regulators is $p^{\mathrm{rk}(E/K)} \cdot \square$ which gives the following expression

$$\mathrm{rk}(E/K) \equiv \sum_v \mathrm{ord}_p \frac{C_v(E,\omega)}{C_v(E',\omega')} \mod 2,$$

which agrees the formula of Birch (††).

1.6.3 A machine for computing parities of ranks

We develop a mechanism which automates the derivation of local expressions using Brauer relations. A crucial input for this is the following result.

Theorem 1.17 (Corollary 3.11)**.** *Let X be a curve defined over a number field and G be a finite subgroup of automorphisms of X. For every prime p, $\mathcal{X}_p(\mathrm{Jac}_X)$ is a self-dual G-representation.*

At the heart of all this is the theory of "regulator constants". This associates to a Brauer relation Θ and a prime p, a set $S_{\Theta,p}$ of self-dual G-representations. The following theorem shows we can control the multiplicities of these representations in Selmer groups in terms of local data.

Theorem 1.18 (Theorem 5.7)**.** *Let X/K be a curve defined over a number field, G a finite subgroup of $\mathrm{Aut}_K(X)$, Θ a Brauer relation for G and p a prime. Suppose that $\Omega^1(\mathrm{Jac}_X)$ is self-dual as a G-representation. Then,*

$$\sum_{\rho \in S_{\Theta,p}} \frac{\langle \rho, \mathcal{X}_p(\mathrm{Jac}_X)\rangle}{\langle \rho, \rho\rangle} = \sum_{v \text{ place of } K} \mathrm{ord}_p \Lambda_\Theta(X/K_v) \mod 2,$$

where $\Lambda_\Theta(X/K_v)$ is the local invariant of Definition 5.24, and $S_{\Theta,p}$ is the set of representations from Definition 4.18.

Remark 1.19. The self-duality assumption on $\Omega^1(\mathrm{Jac}_X)$ is automatically satisfied if all representations of G are self-dual (e.g. if G is a symmetric or dihedral group) or if K has a real place (in which case $\Omega^1(\mathrm{Jac}_X)$ is realisable over $\mathbb{R}$) .

For the purposes of the introduction, the precise definition for Λ_Θ is not important; the key point is that it is a purely local arithmetic invariant. To give an idea, let us mention that when $v|p$,

$$\Lambda_\Theta(X/K_v) = \frac{\prod_i c_v(\mathrm{Jac}_{X/H_i})}{\prod_j c_v(\mathrm{Jac}_{X/H'_j})} \cdot (\text{powers of 2 and } p),$$

where c_v denotes the Tamagawa number at v.

Adding on, the determination of the set $S_{\Theta,p}$ is a problem in finite group representation theory. In particular, in the case of Examples 1.5–1.6, $S_{\Theta,p}$ is given as follows:

Example	G	Brauer relation	p	$S_{\Theta,p}$
1.5	$C_2 \times C_2$	$\Psi = C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}$	2	$\{\psi, \chi\}$
1.6	D_p	$\Theta = C_p + 2C_2 - \{e\} - 2D_p$	p	$\{\tau\}$

where ψ, χ and τ are the representations from Examples 1.10–1.11.

Theorem 1.18 readily recovers the formula of Birch–Cassels derived in §1.6.2. For simplicity, we assume that E has rational p-torsion (see Theorem 6.17(2) for the general case). By Example 1.15, the p-isogeny $E \to E'$ comes from the Brauer relation $\Theta = C_p + 2C_2 - \{e\} - 2D_p$ for D_p. Therefore, by applying Theorem 1.18, we get the following expression:

$$\mathrm{rk}_p(E/K) \overset{\text{Ex. 1.11}}{=} \langle \tau, \mathcal{X}_p(E) \rangle \overset{\text{Thm. 1.18}}{=} \sum_v \mathrm{ord}_p \Lambda_\Theta(E/K_v) \mod 2 \qquad (\dagger\,\dagger\,\dagger)$$

Adding on, in the case of Example 1.5, Theorem 1.18 applied with respect to Ψ and with $p = 2$ gives $\mathrm{rk}_2(\mathrm{Jac}_X/K) \equiv \sum_v \mathrm{ord}_2 \Lambda_\Psi(X/K_v) \mod 2$.

We give a generalisation of this formula to arbitrary primes in §6.6, in agreement with [19, Theorem 2.3].

Example 1.20. Consider $E/\mathbb{Q} : y^2 + y = x^3 + x^2 - 10x + 10$ with conductor $123 = 3 \cdot 41$. This is 5-isogenous to $E'/\mathbb{Q} : Y^2 + Y = X^3 + X^2 + 20X - 890$.

We now compute the parity of the 5^∞-Selmer rank $\mathrm{rk}_5(E/\mathbb{Q})$ by using $\Lambda_\Theta(E/\mathbb{Q}_\ell)$ and $(\dagger\,\dagger\,\dagger)$.

Finite places: By Theorem 5.25(3),

$$\Lambda_\Theta(E/\mathbb{Q}_\ell) = \frac{|\mathrm{coker}(\phi : E(\mathbb{Q}_\ell) \to E'(\mathbb{Q}_\ell))|}{|\ker(\phi : E(\mathbb{Q}_\ell) \to E'(\mathbb{Q}_\ell))|} \cdot |5|_\ell.$$

where $|x|_\ell$ denotes the normalised absolute value of x. In this case, $\mathrm{ord}_5 \frac{|\mathrm{coker}|_{\mathbb{Q}_\ell}|}{|\ker|_{\mathbb{Q}_\ell}|} = \mathrm{ord}_5 \frac{c_\ell(E/\mathbb{Q})}{c_\ell(E'/\mathbb{Q})} \mod 2$ (see [78, Lemma 3.8 & pp. 92] for $\ell \neq 5$,

and combine [78, Lemma 3.8] with [27, §6] for $\ell = 5$). By Tate's algorithm, E has reduction types I_1 at $\ell = 3$ and I_5 at $\ell = 41$, while E' has I_5 at $\ell = 3$ and I_1 at $\ell = 41$. Therefore, $\mathrm{ord}_5\Lambda_\Theta(E/\mathbb{Q}_\ell) = 1 \bmod 2$ when $\ell = 3, 5, 41$, and $0 \bmod 2$ otherwise.

Infinite place: We now consider

$$\Lambda_\Theta(E/\mathbb{R}) = \frac{|\mathrm{coker}(\phi : E(\mathbb{R}) \to E'(\mathbb{R}))|}{|\ker(\phi : E(\mathbb{R}) \to E'(\mathbb{R}))|} \cdot 5.$$

Since $\deg(\phi) = 5$, $|\mathrm{coker}|_{\mathbb{R}}| = 1$. In addition, $|\ker|_{\mathbb{R}}| = 5$, as $(2, 1) \in \ker(\phi)$. Therefore, $\mathrm{ord}_5\Lambda_\Theta(E/\mathbb{R}) = 0 \bmod 2$.

By $(\dagger\,\dagger\,\dagger)$, we deduce that $\mathrm{rk}_5(E/\mathbb{Q}) \equiv (1 + 1 + 1) \equiv 1 \bmod 2$.

Isogenies have been extensively used to derive formulae for the parities of ranks in terms of local data. This includes all of those listed in §1.5.1:

1. Birch–Cassels ([14, Theorem 1.1], cf. §1.6.2),
2. Kramer for X elliptic [54, Theorem 1] and Morgan for X hyperelliptic [70, Theorem 1.6],
3. V. Dokchitser–Maistret [33, Theorem 3.2],
4. Coates–Fukaya–Kato–Sujatha if $p \neq 2$ [19, Theorem 2.3], Green–Maistret if $p = 2$ [42, Theorem 2.4],
5. Docking [25, Theorem 3.4],
6. Mazur–Rubin for dihedral groups [62, Theorem A] and Dokchitser–Dokchitser [30, Theorem 1.14] for arbitrary Galois groups.

We show that Theorem 1.18 provides a means for deriving local formulae for all of these rank expressions in a uniform way, see Theorem 6.6 below.

1.6.4 Parity of ranks of Jacobians

In a joint work with V. Dokchitser, Green, Morgan, we use this framework to define local constants $w_{\mathrm{arithm}}(X/K_v)$ that determine the parity of the rank of

arbitrary Jacobians Jac_X. These is an arithmetic analogue of the local root number $w(\mathrm{Jac}_X/K_v)$ and are constructed using Brauer relations and the local invariant Λ_Θ.

Theorem 1.21 ([32, Theorem 7.3(i)]). *Suppose that the Tate–Shafarevich group* Ш *is finite for the Jacobians of all curves over number fields. Then for all curves X/K*

$$(-1)^{\mathrm{rk}(\mathrm{Jac}_X)} = \prod_{v \text{ place of } K} w_{\mathrm{arithm}}(X/K_v).$$

We do not address questions regarding the compatibility of these constant $w_{\mathrm{arith}}(X/K_v)$ with local root numbers $w(X/K_v)$ in general. Nonetheless, we use these to give a new proof of the parity conjecture for elliptic curves. (A similar result is given in [31, Theorem 1.2] with different assumptions on the Tate-–Shafarevich group).

Theorem 1.22 ([32, Theorem 6.1]). *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over a number field K with $a \neq 0$. Let E' be the elliptic curve with an affine model $y^2 = x^3 - 27bx^2 - 27a^3x$. If $Ш(E/K)$ has finite 3-primary part and $Ш(E'/K)$ has finite 2- and 3-primary parts, then the parity conjecture holds for E/K.*

1.7 Structure of the thesis

This thesis is organised as follows.

In Chapter 2, we provide preliminaries that will be useful for this work. In particular, we focus on curves and their Jacobians, establish relevant conventions, and present foundational results for studying their arithmetic.

In Chapter 3, we focus on curves equipped with automorphisms and associated G-representations. These include ℓ-adic Tate modules $V_\ell(\mathrm{Jac}_X)$, Selmer groups $\mathcal{X}_p(\mathrm{Jac}_X)$ and rational points $\mathrm{Jac}_X(K) \otimes \mathbb{Q}$. The main results of this chapter are summarised in Theorem 3.1.

Chapters 4 and 5 are dedicated to proving Theorem 1.18.

In Chapter 4, we define pseudo Brauer relations and their regulator constants. These extend the notion of regulator constants of Brauer relations found in [28].

Chapter 5 focuses on proving Theorem 1.18. We first use the construction detailed in Appendix A to present a method for constructing isogenies from pseudo Brauer relations (Theorem 5.3). Next, we introduce $\Lambda_\Theta(X/\mathcal{K})$, an explicit invariant associated with curves over local fields $\mathcal{K}$. Along the way, we briefly discuss versions of Theorem 1.18 that involve different local invariants.

In Chapter 6, we apply pseudo Brauer relations and regulator constants to reconstruct classical isogenies using Theorem 5.3 and derive known local expressions for Selmer rank parities with Theorem 1.18 in a uniform way.

In Chapter 7, we address a question of Stein concerning the order of the Tate–Shafarevich group $Ш(A/\mathbb{Q})$. Our main result is Theorem 1.12.

In Appendix A, we describe an explicit construction of homomorphisms between Jacobians, derived from certain G-equivariant maps between permutation modules.

1.8 Notation

We write K for a number field and v for one of its places. We write L for any field and $\mathcal{K}$ for a local field of characteristic 0.

X	a curve (see Convention 2.1)
Jac_X	the Jacobian variety of X
X/H	quotient of X defined over L by a finite group $H \leq \mathrm{Aut}_L(X)$
$\mathcal{X}_p(A)$	$\mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim \mathrm{Sel}_{p^n}(A), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$, the dual p^∞-Selmer group
$\mathrm{rk}_p A$	the p^∞-Selmer rank of A, that is $\dim_{\mathbb{Q}_p} \mathcal{X}_p(A)$
$V_\ell(A)$	$T_\ell(A) \otimes \mathbb{Q}_\ell$, where $T_\ell(A)$ is the integral ℓ-adic Tate module
$\Omega^1(A)$	the L-vector space of regular differentials on A defined over a field L
$c(A)$	the Tamagawa number of A defined over a non-archimedean local field

$\lvert\cdot\rvert_{\mathcal{K}}$, $\lvert\cdot\rvert_v$	the normalised absolute value on $\mathcal{K}$ (resp. K_v), extended to $\overline{\mathcal{K}}$ (resp. $\overline{K_v}$)
$\langle\cdot,\cdot\rangle$	the inner product of characters of G-representations
ρ^*, ρ^H	the dual (resp. H-invariant vectors, for $H \leq G$) of a G-representation ρ
Θ	a (pseudo) Brauer relation, see Definition 4.1
$\mathcal{C}_\Theta(\mathcal{V})$	regulator constant for $\mathcal{V}$, see Definition 4.9
$\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(\mathcal{V})$	$\mathcal{C}_\Theta(\mathcal{V})$ computed with the bases $\mathcal{B}_1$, $\mathcal{B}_2$, see Definition 4.9
$S_{\Theta,p}$	set of computable combinations of representations encoding regulator constants, see Definition 4.18
$\Lambda_\Theta(X/\mathcal{K})$	an explicit local invariant of X, see Definition 5.24
D_n	the dihedral group of order $2n$
$\mathbb{1}$	the trivial representation

Chapter 2

Background

The majority of this chapter is dedicated to providing definitions and establishing conventions for curves and their Jacobians. We note that the results in §§2.1.1–2.1.2 are mostly standard. Additionally, the results presented in §2.1.3 and §2.2 are available in a joint paper with Morgan [53], whose contributions are greatly appreciated.

In the final section, we provide definitions for the Birch and Swinnerton-Dyer invariants appearing in Conjecture 1.2(2).

2.1 Curves and their function fields

Throughout this chapter, K will be a field of characteristic 0.

2.1.1 Definitions and conventions

By a curve X/K, we mean a K-variety which is pure of dimension one, that is all of its irreducible components are of dimension one. In addition, we adhere to the following convention.

Convention 2.1. *Curves are assumed to be smooth, proper and connected but are not assumed to be geometrically connected.*

The reason for considering curves which can fail to be geometrically connected is that they appear naturally in the context of Galois covers of curves; see Example 2.11.

2.1.2 Function fields

We will use the following equivalence between curves over K and function fields. By a function field F over K, we mean a field extension F/K such that F is a finite algebraic extension of $K(x)$ for some $x \in F$ that is transcendental over K.

Theorem 2.2 ([83, Tag 0BY1])**.** *The map which sends a curve X/K to its function field $K(X)$ induces a contravariant equivalence of categories:*

1. *K-curves and non-constant K-morphisms,*
2. *finitely generated field extensions F/K of transcendence degree one and K-algebra homomorphisms.*

Example 2.3. Let E/K be an elliptic curve given by the Weierstrass equation $y^2 = f(x)$ for $f \in K[x]$ a square-free cubic. Then, its function field $K(E)$ is isomorphic to $K(x, y)/(y^2 - f(x))$. The field inclusion $K(x) \hookrightarrow K(E)$ corresponds by Theorem 2.2 to the map $E \to \mathbb{P}^1$ determined by $(x, y) \mapsto x$.

Remark 2.4. We note that when we give a curve by affine equations, we will always mean the (unique) smooth, projective curve birational to it.

The *field of constants* K' of F/K is the algebraic closure K in F, that is $K' = F \cap \overline{K}$. The curve X/K afforded by Theorem 2.2 is geometrically connected if and only if $K' = K$, see [58, Chapter 3, Cor. 2.14(d)].

If, on the other hand, $K' \neq K$, then F is also a function field over K'; indeed, the same x from above is still transcendental over K', and $F/K'(x)$ is a finite extension. Therefore, by first viewing F as a function field over K', then over K, we can associate to it the following using Theorem 2.2:

1. a geometrically connected curve X'/K',
2. a curve X/K satisfying Convention 2.1.

In this case, X is simply X' viewed as a curve over K.

Notation 2.5. Let X'/K' be the geometrically connected associated to a function field F/K. We write $X'_{K'/K}$ to denote the curve obtained from X' by forgetting the K'-structure, i.e. the K-scheme given by X' equipped with the structure map $X' \to \mathrm{Spec}(K') \to \mathrm{Spec}(K)$.

2.1.2.1 Automorphisms on curves.

Definition 2.6. We say that $f : X \to Y$ is a *cover of curves* if it is a non-constant K-morphism. The *degree of* f, denoted $\deg(f)$, is defined to be the degree of the field extension $K(X)/K(Y)$ afforded by Theorem 2.2.

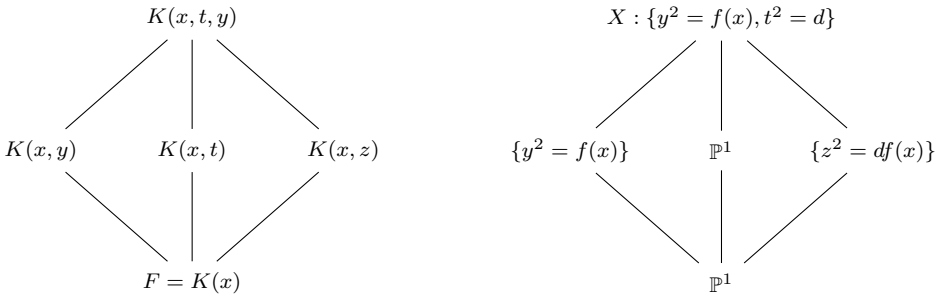
We say that a cover $f : X \to Y$ is *Galois* if the field extension $K(X)/K(Y)$ is Galois in the field-theoretic sense. We also say that $f : X \to Y$ is a *G-Galois* cover when the Galois group of $K(X)/K(Y)$ is isomorphic to G.

In the case of a G-Galois cover $f : X \to Y$, the group G acts on the function field $K(X)$ via K-automorphisms. By Theorem 2.2, we deduce that G is a subgroup of K-automorphisms on X. We can then consider the field of G-invariant functions $K(X)^G$. By construction, this coincides with the function field of the quotient curve X/G and so $K(X)^G = K(X/G)$. The function field inclusion $K(X)^G \hookrightarrow K(X)$ corresponds to the quotient map $\pi : X \to X/G$. Consequently, we get the following commutative diagrams:

$$\begin{array}{ccc} K(X)^G & \hookrightarrow & K(X) \\ \simeq\uparrow & \nearrow_{f^*} & \\ K(Y) & & \end{array} \qquad \begin{array}{ccc} X/G & \xleftarrow{\pi} & X \\ \simeq\downarrow & \swarrow_{f} & \\ Y & & \end{array}$$

Example 2.7. Let E/K be an elliptic curve with Weierstrass model $y^2 = f(x)$ for $f \in K[x]$, a square-free cubic. Then, the involution $h_E : (x, y) \mapsto (x, -y)$ acts on E. In particular, after identifying $K(E) \cong K(x, y)/(y^2 - f(x))$, the field of invariant functions $K(E)^{\langle h_E \rangle} = K(x, y^2) \cong K(x)$. It follows that the quotient curve is of genus 0 with parameter x.

Example 2.8. Let $f(x) \in K[x]$ be a square-free polynomial and $K(\sqrt{d})$ a quadratic extension. We let $y = \sqrt{f(x)}$, $t = \sqrt{d}$ and $z = yt$. Consider the following bi-quadratic extension of $K(x)$ with its corresponding cover of curves on the right.



Then, $C_2 \times C_2$ acts on $K(x,t,y)$ by separately inverting t and y. By Theorem 2.2, this gives two involutions on $X : \{y^2 = f(x), t^2 = d\}$, namely

$$g_1 : (t, y, x) \mapsto (-t, y, x) \quad \text{and} \quad g_2 : (t, y, x) \mapsto (t, -y, x).$$

Then, $K(X)^{\langle g_1 \rangle} \cong K(y,x)/(y^2 - f(x))$ and $K(X)^{\langle g_1 g_2 \rangle} \cong K(x,z)/(z^2 - df(x))$, while $K(X)^{\langle g_2 \rangle}$ and $K(X)^{\langle g_1, g_2 \rangle}$ are isomorphic to $K(x, \sqrt{d})$ and $K(x)$ respectively. Following Notation 2.5, X agrees with $X'_{K(\sqrt{d})/K}$ where $X'/K(\sqrt{d})$ is the hyperelliptic curve with affine model $y^2 = f(x)$. Therefore, X is not geometrically connected in this case. Similarly, the quotient of X by $\langle g_2 \rangle$ is $\mathbb{P}^1_{K(\sqrt{d})/K}$.

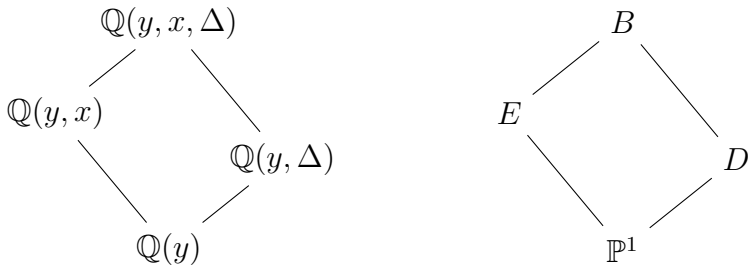
2.1.2.2 Galois closure. We let $f : X \to Y$ be a cover of curves. By Theorem 2.2, this corresponds to a finite and separable field extension $K(X)/K(Y)$. As with any such extension, we can then consider the Galois closure of $K(X)$ over $K(Y)$.

Definition 2.9. We let $f : X \to Y$ be a cover of curves, and we let $F/K(Y)$ be the Galois closure of $K(X)/K(Y)$ in the field-theoretic sense. We then define the *Galois closure* of $f : X \to Y$ to be the cover $g : Z \to Y$ afforded by the function field extension $F/K(Y)$.

We note that if $\mathrm{Gal}(K(X)/K(Y)) \cong G$, then by construction G acts on the function field $K(Z)$ via K-automorphisms. By Theorem 2.2, this induces a G-action on Z via K-automorphisms.

Example 2.10. Let E be an elliptic curve over a number field $\mathbb{Q}$ given by $E : y^2 = x^3 + ax + b$ with $a \neq 0$. We let $f : E \to \mathbb{P}^1$ be the degree 3 cover of $\mathbb{P}^1$ determined by $(x, y) \mapsto y$.

The condition $a \neq 0$ ensures that $h(y) = \mathrm{Disc}(x^3 + ax + b - y^2) = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ has no repeated roots. In particular, $\mathbb{Q}(y, x)/\mathbb{Q}(y)$ is non-Galois and its Galois closure is an S_3-extension of $\mathbb{Q}(y)$ obtained by adjoining $\Delta := \sqrt{h(y)}$ to $\mathbb{Q}(y, x)$. It has the following field diagram, with the corresponding covers of curves given on the right.



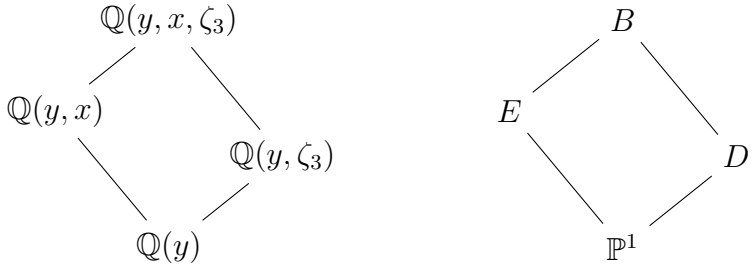
Here D and B are the curves given by the affine equations $\Delta^2 = h(y)$ and by $\{y^2 = f(x),\ \Delta^2 = h(y)\}$ respectively. By construction, S_3 acts on B via K-automorphisms.

We note that all curves appearing in the Galois diagram of Example 2.10 are geometrically connected. We highlight that this is not always the case; geometrically disconnected curves can arise when considering the Galois closure of covers $f : X \to Y$, even if X and Y are themselves geometrically connected. We consider the following modification of Example 2.10.

Example 2.11. Let $E/\mathbb{Q}$ be an elliptic curve over a number field $\mathbb{Q}$ given by $E : y^2 = x^3 + b$, and we let $f : E \to \mathbb{P}^1$ be the map determined by $(x, y) \mapsto y$.

It follows that $h(y) = \mathrm{Disc}(x^3 + b - y^2) = -27(y^2 - b)^2$. Then, the Galois closure of $f : E \to \mathbb{P}^1$ is an S_3-extension of $\mathbb{Q}(y)$ obtained by adjoining

$\Delta := \sqrt{h(y)}$ to $\mathbb{Q}(y,x)$. Since $\pm\sqrt{-3} = \frac{\Delta}{3(y^2-b)}$, we acquire the following function field extension with the corresponding cover appearing on the right:



The field of constant functions in $\mathbb{Q}(D)$ is $\mathbb{Q}(\zeta_3)$, and so D has two geometric components defined over $\mathbb{Q}(\zeta_3)$. The same conclusion holds for B.

In this case, B is given by $E_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$, i.e., the product $E \times_{\mathbb{Q}} \mathbb{Q}(\zeta_3)$ viewed as a curve over $\mathbb{Q}$ (see Notation 2.5). Similarly, D is $\mathbb{P}^1_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$.

2.1.3 Generalisation to disconnected curves

We end this section by briefly mentioning a generalisation of the above results to curves that are (smooth, proper but) *not* assumed to be connected. These emerge by considering curves of Convention 2.1 after base-change. In particular, let X'/K' and X/K be as in Notation 2.5, and write L for the Galois closure of K'/K. Then,

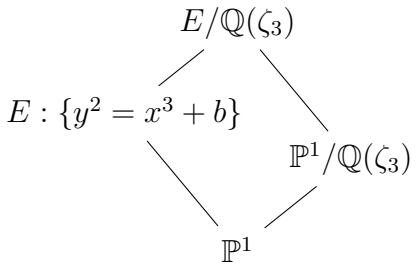
$$X \times_K L = X'_{K'/K} \times_K L \cong X' \times_{K'} K' \times_K L \cong X' \times_{K'} (K' \otimes_K L).$$

It follows that $X \times_K L$ is a disjoint union of $[K' : K]$-many copies of $X' \times_{K'} L$.

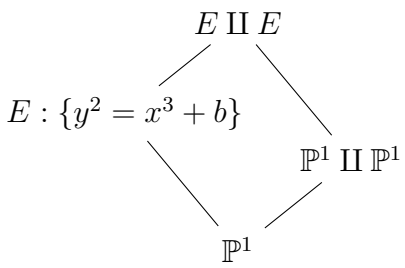
Motivated by this observation, in a joint work [53] with Morgan, we study the arithmetic of curves (and their Jacobians) that are (smooth, proper but) *not* assumed to be connected. For convenience, let us call these *general curves*. Under these assumptions, a general curve X/K admits a decomposition $X = \bigsqcup_i X_i$ as a disjoint union of curves $\{X_i/K\}_i$ which satisfy Convention 2.1.

The curves–fields equivalence of Theorem 2.2 extends to one involving general curves and certain finite étale algebras [53, Proposition 1.1(3)] (in this case, this is simply a product of function fields over K).

To illustrate this, let us consider the base change of the curves appearing in the S_3 diagram of Example 2.11 to $\mathbb{Q}_7$. Then, the (normalisation of the) discriminant curve $D : \Delta^2 = -27(y^2 - b)^2$ is not irreducible over $\mathbb{Q}_7$. In this case, its corresponding 'function field' $\mathbb{Q}_7(y, \Delta)$ (defined in the sense of [53, Notation 2.14]) is the $\mathbb{Q}_7$-algebra $\mathbb{Q}_7(y)[\Delta]/(\Delta^2 + 27) \cong \mathbb{Q}_7(y) \times \mathbb{Q}_7(y)$. By using the equivalence between general curves–étale algebras [53, Proposition 1.1(3)], we deduce that $D/\mathbb{Q}_7$ is given as a disjoint union $\mathbb{P}^1 \amalg \mathbb{P}^1$. The corresponding covers over $\mathbb{Q}$ and $\mathbb{Q}_7$ are as follows:



Case 1: over $\mathbb{Q}$



Case 2: over $\mathbb{Q}_7$

Most results mentioned in §2.2 will apply to general curves, and we will highlight instances where such generalisations are possible. However, to avoid obscuring the main ideas, we have chosen to primarily focus on curves of Convention 2.1 and only use general curves when absolutely necessary (for example in §2.2.0.3 and §2.3.2).

2.2 Jacobians of curves

We now turn our focus from curves X/K to their Jacobians, denoted Jac_X. The theory of Jacobians of geometrically connected curves is classical; see [67] for a thorough treatment. We now explain how this generalises to curves satisfying Convention 2.1.

By definition, we will write Jac_X to denote the identity component of the relative Picard functor of X/K, i.e., the functor of line bundles whose restriction to each geometric component of X has degree 0. As detailed in [51, Remark 5.6], Jac_X is an abelian variety over K when X is a curve following Convention 2.1.

As in §2.1.2, to any X/K satisfying Convention 2.1, we can associate a geometrically connected curve X'/K' such that $X = X'_{K'/K}$ (see Notation 2.5).

Lemma 2.12. *As abelian varieties over K,*

$$\mathrm{Jac}_X \cong \mathrm{Res}_K^{K'} \mathrm{Jac}_{X'},$$

where $\mathrm{Res}_K^{K'}$ denotes the Weil-restriction of scalars from K' to K. In particular, Jac_X is principally polarised.

Proof. The first claim follows from [53, Lemma 3.7]. The second claim is immediate as Jacobians of geometrically connected curves are known to be principally polarised [67, p. 24], and Weil-restrictions of principally polarised abelian varieties are themselves principally polarised [24, Prop. 2]. □

Remark 2.13. This lemma extends to the general curves discussed in §2.1.3; see [53, Lemma 3.7] for the full generalisation.

2.2.0.1 Induced maps between Jacobians. In this subsection, we provide a description for $\overline{K}$-points on Jac_X, their group structure, and how they behave under pullback f^*, and pushforward f_* maps. We first consider the case where X is geometrically connected.

2.2.0.2 Geometrically connected curves. We let X/K be a geometrically connected curve and K a characteristic 0 field. A *divisor* D on X is a $\mathbb{Z}$-linear combination

$$D = \sum_{P \in X(\overline{K})} n_p P,$$

where $n_P = 0$ for all but finitely many P. The *degree of* D is $\sum_P n_P$. The set of divisors forms an abelian group under addition denoted $\mathrm{Div}(X)$. We write $\mathrm{Div}^0(X)$ to denote the subgroup of divisors of degree 0.

In addition, we say that a divisor D is *principal* if there exists a non-zero $f \in K(X)$ such that $D = \mathrm{div}(f)$ where

$$\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f) P,$$

and $\mathrm{ord}_P(f)$ denotes the order of the function f at the point P. Since $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, the set of principal divisors form a group denoted $\mathrm{Prin}(X)$. As abelian groups, there exists a canonical identification

$$\mathrm{Jac}_X(\overline{K}) = \mathrm{Div}^0(X)/\mathrm{Prin}(X).$$

Adding on, given a K-rational cover $f : X \to Y$, we write $f_* : \mathrm{Jac}_X \to \mathrm{Jac}_Y$ and $f^* : \mathrm{Jac}_Y \to \mathrm{Jac}_X$ to denote the pushforward and the pullback maps respectively. These are given on divisors by

$$f_* : [P] \mapsto [f(P)], \quad \text{and} \quad f^* : [Q] \mapsto \sum_{Q \in f^{-1}(P)} e_f(P)[P],$$

where $e_f(P)$ denotes the ramification index of f at $P \in Y(\overline{K})$.

We write λ_X and λ_Y to denote the canonical principal polarisations on the geometrically connected curves X and Y as in [67, pp. 24]. It follows that the pullback and the pushforward are duals of each other in the following sense.

Lemma 2.14. *We have $f_* = \lambda_Y^{-1} \circ (f^*)^\vee \circ \lambda_X$, where $(f^*)^\vee$ denotes the dual morphism of f^*.*

Proof. This result is well known. For details, see [53, Lemma 3.1]. □

2.2.0.3 Curves of Convention 2.1. The story is very similar for the curves of Convention 2.1.

We write $\overline{X} = X \times_K \overline{K}$ to denote the base change to the algebraic closure $\overline{K}$. As in §2.1.3, $\overline{X} = \bigsqcup_i X_i$ decomposes as a disjoint union of its (geometric) connected components $X_i/\overline{K}$. We get a description for $\mathrm{Jac}_X(\overline{K})$ in terms of divisors as follows.

We write $\mathrm{Div}^0(\overline{X})$ to denote the set of divisors whose restriction to each geometric component is a degree 0 divisor. We write $\overline{K}(\overline{X})$ to denote the function field of $\overline{X}$ in the sense of [53, Notation 2.14] and $\mathrm{Prin}(\overline{X})$ for the subgroup of divisors arising from rational functions $f \in \overline{K}(\overline{X})$. In this case, these are determined by a tuple $f = (f_i)_i$ where $f_i \in \overline{K}(X_i)$, and so $\mathrm{div}(f) =$

$\sum_i \operatorname{div}(f_i)$. To conclude, we have

$$\overline{K}(\overline{X}) \cong \prod_i \overline{K}(X_i), \quad \operatorname{Div}^0(\overline{X}) = \bigoplus_i \operatorname{Div}^0(X_i), \quad \operatorname{Prin}(\overline{X}) = \bigoplus_i \operatorname{Prin}(X_i).$$

It follows that $\operatorname{Jac}_{\overline{X}} \cong \prod_i \operatorname{Jac}_{X_i}$, and as before, we get a canonical identification

$$\operatorname{Jac}_X(\overline{K}) = \operatorname{Div}^0(\overline{X})/\operatorname{Prin}(\overline{X}).$$

We write f^* to denote the pullback map, and we now *define* $f_* = \lambda_Y^{-1} \circ (f^*)^\vee \circ \lambda_X$, where λ_X and λ_Y denote the principal polarisations from [53, Lemma 3.4].

Lemma 2.15. *Suppose that $f : X \to Y$ is a G-Galois cover. Then,*

$$f_* \circ f^* = |G| \quad \text{and} \quad f^* \circ f_* = \sum_{\sigma \in G} \sigma_*.$$

Proof. This follows by a direct computation when X and Y are geometrically connected. For the curves of Convention 2.1, we can reduce to the geometrically connected case; see [53, Proposition 4.1] for details. □

2.3 Birch and Swinnerton-Dyer invariants

In this section, we define the Birch and Swinnerton-Dyer constants appearing in Conjecture 1.2(2).

2.3.1 Regulators, Tamagawa numbers and periods

Suppose that A is an abelian variety defined over a number field K. Write $\langle , \rangle_{\mathrm{NT}}$ to denote the Néron–Tate height pairing corresponding to the Poincaré line bundle on $A \times A^\vee$. Then, let $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_r$ be a bases for free, finite index subgroups in the lattices $A(K)/A(K)_{\mathrm{tors}}$ and $A^\vee(K)/A^\vee(K)_{\mathrm{tors}}$. Then, we define the *regulator of* A/K to be

$$\operatorname{Reg}(A/K) = \frac{\left|\det\left(\langle P_i, Q_j \rangle_{\mathrm{NT}}\right)_{i,j}\right|}{u_1 \cdot u_2},$$

where $u_1 = [A(K)/A(K)_{\text{tors}} : \bigoplus_i \mathbb{Z}P_i]$ and $u_2 = [A^\vee(K)/A^\vee(K)_{\text{tors}} : \bigoplus_j \mathbb{Z}Q_j]$.

Let $A/\mathcal{K}$ be an abelian variety over a local field $\mathcal{K}$ of characteristic 0.

Then, when $\mathcal{K}$ is a p-adic field with residue field k, we write $\mathcal{A}$ to denote the Néron model of $A/\mathcal{O}_\mathcal{K}$, and Φ to denote its component group (i.e. the quotient of the special fibre $\mathcal{A}_k$ by its connected component of 0).

The *Tamagawa number of* $A/\mathcal{K}$, denoted $c(A/\mathcal{K})$, is defined as the order $|\Phi(k)|$ of the subgroup of $\Phi(\overline{k})$ consisting of k-rational points. When $\mathcal{K} = K_v$ is the completion of a number field at a place v, we will usually write $c_v(A/K)$ to denote the Tamagawa number at v.

We write $\Omega^1(A/\mathcal{K})$ for the $\mathcal{K}$-vector space of regulator differentials on $A/\mathcal{K}$. Then, a non-zero exterior form w on A is any non-zero element of $\Omega^{\dim(A)}(A/\mathcal{K}) := \bigwedge_{i=1}^{\dim(A)} \Omega^1(A/\mathcal{K})$. In addition, for a choice of Néron minimal exterior form, ω_0, on A, we write $\frac{\omega}{\omega_0} \in \mathcal{K}^\times$ for the constant determined by $\omega = (\frac{\omega}{\omega_0}) \cdot \omega_0$.

We define

$$C(A/\mathcal{K}, \omega) := \begin{cases} c(A/\mathcal{K}) \cdot \left|\frac{\omega}{\omega_0}\right|_\mathcal{K} & \text{when } \mathcal{K}/\mathbb{Q}_p \text{ is finite,} \\ \int_{A(\mathcal{K})} |\omega| & \text{when } \mathcal{K} = \mathbb{R}, \\ 2^{\dim(A)} \int_{A(\mathcal{K})} |\omega \wedge \overline{\omega}| & \text{when } \mathcal{K} = \mathbb{C}. \end{cases} \tag{2.1}$$

If K is a number field, we write

$$C(A/K) := \prod_{v \text{ place of } K} C(A/K_v, \omega),$$

where ω is a non-zero global exterior form on A/K. By the product formula, this is independent of the choice of global exterior form ω.

2.3.2 Tate–Shafarevich group and deficiency

The Tate–Shafarevich group of an abelian variety A/K over a number field is defined as

$$Ш(A/K) := \ker\left(H^1(\mathrm{Gal}(\overline{K}/K), A(\overline{K})) \to \prod_v H^1(\mathrm{Gal}(\overline{K}_v/K_v), A(\overline{K_v})) \right),$$

where the product is taken over all places v of K.

The work of Poonen–Stoll [75] shows that when $A = \mathrm{Jac}_X$, for X a geometrically connected curve, the concept of *deficiency* controls the size of the 2-primary part of this group, up to rational squares. We now present how this result extends to the curves of Convention 2.1.

For the remainder of this subsection, we have to work with the general curves mentioned in §2.1.3. The reason for this is that curves of Convention 2.1 may become disconnected after base-change.

Definition 2.16 (cf. [53], Definition 5.13)**.** Let $\mathcal{K}$ be a local field of characteristic 0.

A geometrically connected curve $X/\mathcal{K}$ of genus g is called *deficient* if it has no $\mathcal{K}$-rational divisor of degree $g-1$. For such X, we define

$$\mu_{\mathcal{K}}(X) = \begin{cases} 2 & \text{if } X \text{ is deficient,} \\ 1 & \text{otherwise.} \end{cases}$$

Suppose that $X/\mathcal{K}$ is a curve satisfying Convention 2.1. We write $\mathcal{K}'$ for the minimal field of definition of one of its geometric components, X' say, and define $\mu_{\mathcal{K}}(X) = \mu_{\mathcal{K}'}(X')$.

Finally, suppose that $X/\mathcal{K}$ is given as a disjoint union $\bigsqcup_i X_i$ of curves $X_i/\mathcal{K}$ all of which satisfy Convention 2.1. We define $\mu_{\mathcal{K}}(X) = \prod_i \mu_{\mathcal{K}}(X_i)$.

If the field $\mathcal{K}$ is clear from context, we will often omit it from the notation. Further, when $\mathcal{K} = K_v$ is the completion of a number field K at a place v, we write $\mu_v(X)$ in place of $\mu_{K_v}(X)$.

Proposition 2.17. *Let X be a curve satisfying Convention 2.1 defined over a number field K. Then,*

$$|Ш_0(\mathrm{Jac}_X/K)[2^\infty]| = \prod_{v \text{ place of } K} \mu_v(X) \mod \mathbb{Q}^{\times 2}.$$

Proof. By Lemma 2.12, $\mathrm{Jac}_X \cong \mathrm{Res}_K^{K'} \mathrm{Jac}_{X'}$, while Shapiro's lemma gives $Ш_0(\mathrm{Jac}_X/K) \cong Ш_0(\mathrm{Jac}_{X'}/K')$. Adding on, $X \times_K K_v = X' \times_{K'} K' \times_K K_v$. Since $K' \otimes_K K_v = \prod_{w|v} K'_w$, we deduce that $X \times_K K_v$ is given as a disjoint union $\bigsqcup_{w|v}(X' \times_{K'} K'_w)$. By Definition 2.16, $\mu_v(X) = \prod_{w|v} \mu_w(X')$. Therefore,

$$\prod_{v \text{ place of } K} \mu_v(X) = \prod_{w \text{ place of } K'} \mu_w(X') \overset{[75,\ \text{Cor. } 12]}{\equiv} |Ш_0(\mathrm{Jac}_{X'}/K')[2^\infty]| \mod \mathbb{Q}^{\times 2}.$$

This gives the required result. □

Chapter 3

Arithmetic of Jacobians

In this chapter, we focus on G-representation arising from G-Galois covers $f : X \to Y$, including ℓ-adic Tate module $V_\ell(\mathrm{Jac}_X)$, Mordell–Weil groups $\mathrm{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ and dual p^∞-Selmer groups $\mathcal{X}_p(\mathrm{Jac}_X)$.

We implicitly fix arbitrary embeddings $\overline{\mathbb{Q}}_\ell, \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ for every prime. The following theorem summarises the main results of this chapter.

Theorem 3.1 (Theorems 3.9 & 3.10)**.** *Let X be a curve defined over a characteristic 0 field K. Suppose that G is a finite subgroup of $\mathrm{Aut}_K(X)$.*

1. *For any prime ℓ, the ℓ-adic Tate-module satisfies*

$$V_\ell(\mathrm{Jac}_{X/G}) \cong V_\ell(\mathrm{Jac}_X)^G.$$

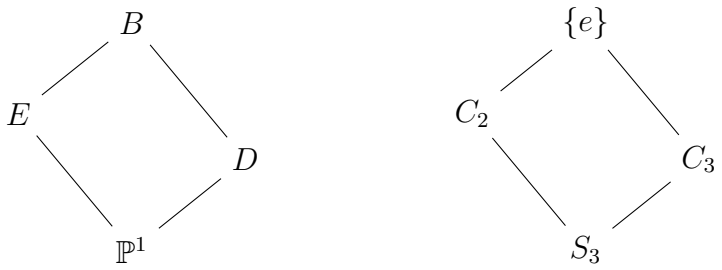
In addition, when K is a number field, the following hold.

2. *For any prime p, $\mathcal{X}_p(\mathrm{Jac}_X)$ is a self-dual G-representation. In addition, $\mathcal{X}_p(\mathrm{Jac}_{X/G}) \cong \mathcal{X}_p(\mathrm{Jac}_X)^G$.*
3. $\mathrm{Jac}_{X/G}(K) \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathrm{Jac}_X(K) \otimes \mathbb{Q})^G$.
4. *For any prime p, if $Ш(\mathrm{Jac}_X)[p^\infty]$ is finite, then $Ш(\mathrm{Jac}_{X/G})[p^\infty]$ is finite. In addition, if $Ш(\mathrm{Jac}_X)$ is finite, then $Ш(\mathrm{Jac}_{X/G})$ is also finite.*
5. *if ρ is a $\mathbb{C}[G]$-representation satisfying $\langle \rho, V_\ell(\mathrm{Jac}_X) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \rangle = 0$, then*

$$\langle \rho, \mathrm{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = \langle \rho, \mathcal{X}_p(\mathrm{Jac}_X) \otimes_{\mathbb{Q}_p} \mathbb{C} \rangle = 0.$$

We prove this result in §§3.2–3.3. We first illustrate applications through examples (see Examples 1.10–1.11 for more applications of Theorem 3.1(1)&(3)).

Example 3.2. We revisit Example 2.10. The situation is described by the following Galois cover with the corresponding groups on the right:



The action of S_3 on B induces, by functoriality, an S_3-action on rational points $\mathrm{Jac}_B(K)$. We can then decompose $\mathrm{Jac}_B(K) \otimes \mathbb{Q} \cong \mathbb{1}^{\oplus n} \oplus \epsilon^{\oplus m} \oplus \rho^{\oplus s}$ into irreducible representations where $\mathbb{1}$, ϵ, ρ denote, respectively, the trivial, sign and the two-dimensional irreducible representations of S_3.

By applying Theorem 3.1(3) with $G = S_3$, we get $n = \mathrm{rkJac}_{\mathbb{P}^1} = 0$. Repeating this with $G = C_2$ and $G = C_3$, we get $\mathrm{rk}E = s$ and $\mathrm{rkJac}_D = m$. To conclude,

$$\mathrm{Jac}_B(K) \cong \epsilon^{\oplus \mathrm{rk}(\mathrm{Jac}_D)} \oplus \rho^{\oplus \mathrm{rk}(\mathrm{Jac}_E)}.$$

Arguing similarly, we get $\mathcal{X}_p(\mathrm{Jac}_B) \cong \epsilon^{\oplus \mathrm{rk}_p \mathrm{Jac}_D} \oplus \rho^{\oplus \mathrm{rk}_p E}$ for any prime p.

Example 3.3. We now revisit Example 2.11. The same computation as in Example 3.2 shows that $\mathrm{Jac}_B(K) \otimes \mathbb{Q} \cong \epsilon^{\oplus \mathrm{rkJac}_D} \oplus \rho^{\oplus \mathrm{rk}E}$. By Lemma 2.12, $\mathrm{Jac}_D \cong \mathrm{Res}^{\mathbb{Q}(\zeta_3)}_{\mathbb{Q}} \mathrm{Jac}_{\mathbb{P}^1}$ is trivial, and therefore

$$\mathrm{Jac}_B(K) \otimes \mathbb{Q} \cong \rho^{\oplus \mathrm{rk}E}.$$

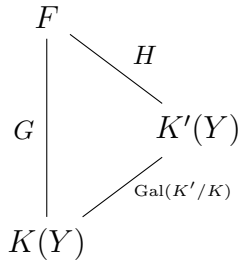
Similarly, $\mathcal{X}_p(\mathrm{Jac}_B) \cong \rho^{\oplus \mathrm{rk}_p E}$ for all p.

3.1 Equivariant Riemann–Hurwitz formula

In the following section, we consider G-Galois covers $f : X \to Y$ with the assumption that Y is geometrically connected. The main result provides an extension of the equivariant Riemann–Hurwitz formula found, for example, in [35]. This provides a description of the G-module structure on $V_\ell(\mathrm{Jac}_X)$ in terms of permutation modules.

We write $F = K(X)$ for the function field of a curve X satisfying Convention 2.1, and K' for its field of constant functions (i.e., the maximal algebraic extension of K in F). As in §2.1.2, we can view F as a function field over K', and as such we can associate to it a geometrically connected curve X' over K' by Theorem 2.2.

We write $H = \mathrm{Gal}(F/K' \cdot K(Y))$ to denote the subgroup of automorphisms of F which fix the subfield $K'(Y)$. This gives the following diagram:



Lemma 3.4. *H is a subgroup of K'-automorphisms of X'. In addition, we have an H-Galois cover $f_H : X' \to Y$ of geometrically connected curves defined over K'.*

Proof. By construction, H acts on F by automorphisms fixing K'.Therefore, we have an action on X' by K'-automorphisms by Theorem 2.2. The field of H-invariants satisfies $F^H \cong K'(Y)$. The inclusion $F^H \hookrightarrow F$ gives the required cover $X' \to Y$. □

The action of H on X' induces an action on its Jacobian $\mathrm{Jac}_{X'}/K'$. The following result relates the action of H on X'/K' to the G-action on X/K.

Lemma 3.5. *We have an isomorphism of $\mathbb{Q}_\ell[G]$-modules*

$$V_\ell(\mathrm{Jac}_X) \cong \mathrm{Ind}_H^G V_\ell(\mathrm{Jac}_{X'}). \tag{3.1}$$

Similarly, we have an isomorphism of $K[G]$-modules

$$\Omega^1(\mathrm{Jac}_X) \cong \mathrm{Ind}_H^G \Omega^1(\mathrm{Jac}_{X'}). \tag{3.2}$$

Proof. We consider $X_{K'}$, the base change of X to K', along with the induced action of G on the set of geometric connected components of $X_{K'}$. Since Y is assumed to be geometrically connected, G acts transitively on this set. Indeed, the number of orbits under the G-action on the irreducible components of $X_{K'}$ coincides with the number of geometric connected components of the quotient.

Recall that, as always, we write X' to denote a geometric component of X. By definition, H coincides (up to conjugacy) with the subgroup of automorphisms in G which restrict to automorphisms of the geometric component X' denoted $\mathrm{Stab}_G(X')$ (choosing a different geometric component simply results in conjugating H by an element in G).

We let $y_1, ..., y_n$ denote a left transversal for H in G, so that $y_1(X'), ..., y_n(X')$ is the collection of the geometric components of $X_{K'}$. As a result, we can decompose $X_{K'} = \bigsqcup_{i=1}^n y_i(X')$. Then, we have an isomorphism of K'-schemes

$$\alpha : \mathrm{Jac}_X \xrightarrow{\sim} \prod_{i=1}^n \mathrm{Jac}_{y_i(X')}$$

induced by pullback along the inclusions $y_i(X') \hookrightarrow X_{K'}$. This induces isomorphisms

$$V_\ell(\mathrm{Jac}_X) \cong \bigoplus_{i=1}^n V_\ell(\mathrm{Jac}_{y_i(X')}) \quad \text{and} \quad \Omega^1(\mathrm{Jac}_X) \cong \bigoplus_{i=1}^n \Omega^1(\mathrm{Jac}_{y_i(X')}),$$

which give the isomorphisms of representations claimed in the statement once the G-action is taken into account. □

Theorem 3.6. *Let $f : X \to Y$ be a G-Galois cover of curves and assume that Y is geometrically connected. Denote by $\{q_1, \dots, q_r\} \subseteq Y(\overline{K'})$ the branch points of $f_H : X' \to Y$, and for each $1 \leq i \leq r$, let $t_i \in f_H^{-1}(q_i)$ be any choice of preimage q_i. Then, for every prime ℓ, the G-representations*

$$V_\ell(\mathrm{Jac}_X) \quad \text{and} \quad \mathrm{Ind}_H^G(\mathbb{1})^{\oplus 2} \oplus \mathrm{Ind}_{\{e\}}^G(\mathbb{1})^{\oplus(r+2\mathrm{g}(Y)-2)} \ominus \bigoplus_{i=1}^{r} \mathrm{Ind}_{\mathrm{Stab}_H(t_i)}^G \mathbb{1}$$

are isomorphic after extending scalars to $\mathbb{C}$. (Here $\mathrm{Stab}_H(t_i)$ denotes the stabiliser of t_i in H).

Proof. Lemma 3.5 gives an isomorphism of $\mathbb{Q}_\ell[G]$-representations

$$V_\ell(\mathrm{Jac}_X) \cong \mathrm{Ind}_H^G V_\ell(\mathrm{Jac}_{X'}). \tag{3.3}$$

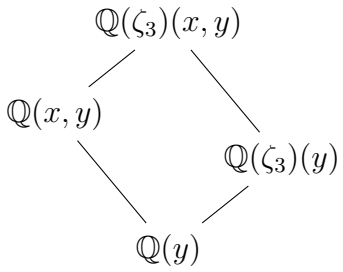
To complete the proof we can appeal to the more standard form of equivariant Riemann–Hurwitz, in which X' is assumed geometrically connected. Specifically, by Lemma 3.4, $f_H : X' \to Y$ is an H-cover of geometrically connected curves. It follows from [35, Proposition 1.1] that, after extending scalars to $\mathbb{C}$, the H-representation $V_\ell(\mathrm{Jac}_{X'}) \otimes \mathbb{C}$ is isomorphic to

$$\mathbb{1}^{\oplus 2} \oplus \mathrm{Ind}_{\{e\}}^H \mathbb{1}^{\oplus(2\mathrm{g}(Y)-2)} \oplus \bigoplus_{i=1}^{r} \big(\mathrm{Ind}_{\{e\}}^H \mathbb{1} \ominus \mathrm{Ind}_{\mathrm{Stab}_H(t_i)}^H \mathbb{1}\big).$$

The result now follows by inducing from H to G and using (3.3). □

Remark 3.7. Lemma 3.5 and 3.6 generalise to general curves of §2.1.3. For details, see [53, Lemma 4.6 & Proposition 4.6].

Example 3.8. We consider the S_3-action given in Example 2.11. This fits in the following Galois diagram:



To apply Theorem 3.6, we consider the cubic cover $E/\mathbb{Q}(\zeta_3) \xrightarrow{3} \mathbb{P}^1/\mathbb{Q}(\zeta_3)$ determined by $(x,y) \to x$. This is branched at $\{\infty, \sqrt{b}, -\sqrt{b}\}$ each with ramification degree 3. By applying Theorem 3.6 with $G = S_3$, $H = C_3$, $r = 3$ and $\mathrm{Stab}_H(t_i) = C_3$ for $i = 1, 2, 3$, we deduce that $V_\ell(\mathrm{Jac}_B) \cong \rho^{\oplus 2}$, where ρ denotes the two-dimensional irreducible representation of S_3.

3.2 Galois descent and isotypic components

Recall that we have fixed arbitrary embedding $\overline{\mathbb{Q}}_\ell, \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$.

Theorem 3.9. *Let X be a curve defined over a field of characteristic 0, and suppose that G is a subgroup of K-automorphisms of X.*

1. *For any prime ℓ, $V_\ell(\mathrm{Jac}_{X/G}) \cong V_\ell(\mathrm{Jac}_X)^G$,*
2. *$\Omega^1(\mathrm{Jac}_{X/G}) \cong \Omega^1(\mathrm{Jac}_X)^G$.*

In addition, when K is a number field, we also have

3. *For any prime p, $\mathcal{X}_p(\mathrm{Jac}_{X/G}) \cong \mathcal{X}_p(\mathrm{Jac}_X)^G$,*
4. *$\mathrm{Jac}_{X/G}(K) \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathrm{Jac}_X(K) \otimes \mathbb{Q})^G$,*
5. *For any prime p, if $Ш(\mathrm{Jac}_X)[p^\infty]$ is finite, then $Ш(\mathrm{Jac}_{X/G})[p^\infty]$ is finite. In addition, if $Ш(\mathrm{Jac}_X)$ is finite, then $Ш(\mathrm{Jac}_{X/G})$ is also finite.*
6. *if ρ is a $\mathbb{C}[G]$-representation satisfying $\langle \rho, V_\ell(\mathrm{Jac}_X) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \rangle = 0$, then*

$$\langle \rho, \mathrm{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = \langle \rho, \mathcal{X}_p(\mathrm{Jac}_X) \otimes_{\mathbb{Q}_p} \mathbb{C} \rangle = 0.$$

Further, if $\langle \rho, V_\ell(\mathrm{Jac}_X) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \rangle = 0$, *then* $\langle \rho, \Omega^1(\mathrm{Jac}_X \otimes_K \mathbb{C} \rangle = 0$ *for any characteristic* 0 *field* K.

Proof. We let $\pi : X \to X/G$ be the quotient map induced by the subgroup $G \leq \mathrm{Aut}_K(X)$. Then, $\pi \circ g = \pi$ for all $g \in G$ and therefore $g^* \circ \pi^* = \pi^*$ on Jacobians. It's easy to check that $g^* = (g_*)^{-1} = (g^{-1})_*$, and so G acts trivially on $\pi^*(\mathrm{Jac}_{X/G})$.

Therefore, the induced map $\pi^* : V_\ell(\mathrm{Jac}_{X/G}) \to V_\ell(\mathrm{Jac}_X)$ factors through $V_\ell(\mathrm{Jac}_X)^G$. This gives maps

$$\pi_* : V_\ell(\mathrm{Jac}_X)^G \to V_\ell(\mathrm{Jac}_{X/G}) \quad \text{and} \quad \pi^* : V_\ell(\mathrm{Jac}_{X/G}) \to V_\ell(\mathrm{Jac}_X)^G,$$

and by Lemma 2.15, their compositions in each direction is equal to the multiplication-by-$|G|$ map. Therefore, $\pi^* : V_\ell(\mathrm{Jac}_{X/G}) \to V_\ell(\mathrm{Jac}_X)^G$ is an isomorphism of $\mathbb{Q}_\ell$-vector spaces, which proves (1). Parts (2)–(4) follow in the same way. For the first assertion in (5), combine parts (3)–(4). The second assertion in (5) follows from the first. To see this, we note that $\pi^* : \mathrm{Jac}_{X/G} \to \mathrm{Jac}_X$ induces an isomorphism $Ш(\mathrm{Jac}_{X/G})[q^\infty] \cong Ш(\mathrm{Jac}_X)[q^\infty]$ when $q \nmid |G|$.

For (6), we argue as follows. After fixing an embedding $K \hookrightarrow \mathbb{C}$, we have a G-module isomorphism $H_1(\mathrm{Jac}_X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong V_\ell(\mathrm{Jac}_X)$ by [1, Exposé XI, Theorem 4.4]. Therefore, $V_\ell(\mathrm{Jac}_X)$ has rational character. We denote by F_ρ the field obtained by extending $\mathbb{Q}$ by the values of the characters of ρ. Then, a positive power of the representation $\bigoplus_{\sigma \in \mathrm{Gal}(F_\rho/\mathbb{Q})} \rho^\sigma$ is realisable over $\mathbb{Q}$ [79, §12.1, Prop. 34] and shares no common constituent with $V_\ell(\mathrm{Jac}_X)$. It therefore suffices to consider the case where ρ is realisable over $\mathbb{Q}$. Denote by e_ρ the idempotent in $\mathbb{Q}[G]$ which projects onto the ρ-isotypic part. Clearing denominators, there exists a positive integer n for which ne_ρ lies in $\mathbb{Z}[G]$. Viewed as an endomorphism of Jac_X, ne_ρ induces the zero map on $T_\ell(\mathrm{Jac}_X)$. In view of [66, Proposition 12.2], ne_ρ is the zero endomorphism on Jac_X, and therefore induces the zero map on $\mathcal{X}_p(\mathrm{Jac}_X)$, $\mathrm{Jac}_X(K) \otimes \mathbb{Q}$ and $\Omega^1(\mathrm{Jac}_X)$. □

3.3 Self-duality of Selmer groups

We let K be a number field. We write (A, λ) to denote an abelian variety A/K with a principal polarisation λ. We denote by $\mathrm{Aut}(A, \lambda)$ the group of K-automorphisms g of A preserving the principal polarisation λ, that is $g^\vee = \lambda \circ g^{-1} \circ \lambda^{-1}$. The proof of the following result is modelled on [29, Theorem 2.1].

Theorem 3.10. *Let (A, λ) be a principally polarised abelian variety, and let G be a subgroup of $\mathrm{Aut}(A, \lambda)$. Then $\mathcal{X}_p(A)$ is self-dual as a $\mathbb{Q}_p[G]$-representation.*

Proof. As in [30], given a K-isogeny of abelian varieties $f : A \to B$, we write

$$Q(f) = \#\mathrm{coker}(f : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}}) \cdot \#\ker(f : Ш(A)_{\mathrm{div}} \to Ш(B)_{\mathrm{div}}),$$

where $Ш_{\mathrm{div}}$ denotes the divisible part of Ш. We decompose $\mathcal{X}_p(A)$ into $\mathbb{Q}_p$-irreducible representations, and decompose the corresponding $\mathbb{Z}_p$-lattice

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

into G-stable $\mathbb{Z}_p$-sublattices such that

$$\mathcal{X}_p(A) \cong \bigoplus_i \tau_i^{n_{\tau_i}}, \quad X_p(A) \cong \bigoplus_i \Lambda_{\tau_i} \quad \text{and} \quad \Lambda_{\tau_i} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \tau_i^{n_{\tau_i}},$$

where the τ_i are distinct $\mathbb{Q}_p$-irreducible representations of G.

We now construct a self-isogeny of A with a specified action on the sublattices Λ_{τ_i} of $X_p(A)$. For an irreducible $\mathbb{Q}_p[G]$-representation τ satisfying $\langle \tau, \mathcal{X}_p \rangle > 0$, the operator $\dim(\tau) \sum_{g \in G} \mathrm{Tr}(\tau(g)) g^{-1} \in \mathbb{Z}_p[G]$ kills every irreducible G-constituent τ' of $\mathcal{X}_p$ not isomorphic to τ, and acts by multiplication by $\langle \tau, \tau \rangle \cdot |G|$ on every constituent of $\mathcal{X}_p$ which is isomorphic to τ. We define

$$z_\tau := |G| \cdot \langle \tau, \tau \rangle + (p-1) \cdot \dim(\tau) \cdot \sum_{g \in G} \mathrm{Tr}(\tau(g)) g^{-1} \in \mathbb{Z}_p[G].$$

Elements in a small neighbourhood U_τ of z_τ in $\mathbb{Z}_p[G]$ act via multiplication by $p \cdot |G| \cdot \langle \tau, \tau \rangle$ composed with some isomorphism on Λ_τ, and via multiplication by $|G| \cdot \langle \tau, \tau \rangle$ composed with some isomorphism on Λ_{τ_i} when $\tau_i \neq \tau$. Similarly, there's a corresponding neighbourhood U_{τ^*} of z_{τ^*}, where τ^* is the dual representation. Since the inversion map $g \mapsto g^{-1}$ is continuous in $\mathbb{Q}_p[G]$ and maps z_τ to z_{τ^*}, we can find $\sigma = \sum_{g \in G} x_g g \in \mathbb{Z}[G] \cap U_\tau$ such that $\sum_{g \in G} x_g g^{-1}$ lies in U_{τ^*}. We write ϕ_σ to denote the endomorphism of A determined by σ. Since G is a subgroup of $\mathrm{Aut}(A, \lambda)$, then $\sum_{g \in G} x_g g^{-1}$ corresponds to the dual isogeny $\phi_\sigma^\vee$. By considering their induced actions on the Λ_{τ_i}, we deduce that

$$Q(\phi_\sigma) = (|G| \cdot \langle \tau, \tau \rangle)^{\mathrm{rk}_p A} \cdot p^{n_\tau \dim(\tau)} \quad \text{and} \quad Q(\phi_\sigma^\vee) = (|G| \cdot \langle \tau^*, \tau^* \rangle)^{\mathrm{rk}_p A} \cdot p^{n_{\tau^*} \dim(\tau^*)}.$$

Since $\langle \tau, \tau \rangle = \langle \tau^*, \tau^* \rangle$ and $Q(\phi_\sigma) = Q(\phi_\sigma^\vee)$ (see [30, Theorem 4.3]), we deduce that $n_\tau = n_{\tau^*}$, as required. □

Corollary 3.11. *Let G be a finite subgroup of $\mathrm{Aut}_K(X)$. Then $\mathcal{X}_p(\mathrm{Jac}_X)$ is a self-dual $\mathbb{Q}_p[G]$-representation.*

Proof. Since $g_*^\vee = \lambda_X^{-1} \circ (g^*) \circ \lambda_X$, it suffices to show that $g^* = (g_*)^{-1}$. It is easy to see that $g_* \circ g^* = 1$, which gives the required result. □

Chapter 4

Pseudo Brauer relations and regulator constants

In this chapter, we define pseudo Brauer relations and their regulator constants, extending the notion of regulator constants for Brauer relations considered in [28]. We will see that most key properties are retained in this expanded framework.

4.1 Pseudo Brauer relations

Throughout this section, L is a field of characteristic 0 with a fixed embedding $L \hookrightarrow \mathbb{C}$, G is a finite group, $\mathcal{H}$ is a set of representatives of the subgroups of G up to conjugacy and $\langle , \rangle$ is the standard inner product on characters. All representations are assumed to be finite dimensional.

Definition 4.1. Let $\mathcal{V}$ be an $L[G]$-representation. We say that an element $\Theta = \sum_i H_i - \sum_j H'_j \in \mathbb{Z}[\mathcal{H}]$ is a *pseudo Brauer relation relative to* $\mathcal{V}$ if there are $\mathbb{C}[G]$-representations ρ_1 and ρ_2, satisfying $\langle \rho_1, \mathcal{V} \rangle = \langle \rho_2, \mathcal{V} \rangle = 0$, such that

$$\rho_1 \oplus \bigoplus_i \mathbb{C}[G/H_i] \cong \rho_2 \oplus \bigoplus_j \mathbb{C}[G/H'_j].$$

Remark 4.2. The choice of representatives in $\mathcal{H}$ will be immaterial in practice (see Remark 4.31 for a thorough discussion). When specific choices are required, these will be explicitly stated.

Remark 4.3. When $\mathcal{V} = L[G]$, we necessarily have $\rho_1 = \rho_2 = 0$. In this case, Definition 4.1 coincides with the existing notion of a Brauer relation, see for example [28, §1.ii].

Example 4.4. $\Theta = C_3 + 2C_2 - \{e\} - 2S_3$ is a Brauer relation for S_3. Indeed, let $\mathbb{1}$ (trivial), ϵ (sign) and ρ (standard) be the set of irreducible representations of S_3. It follows that

$$\mathbb{C}[S_3/H] \cong \begin{cases} \mathbb{1}, & H = S_3, \\ \mathbb{1} \oplus \epsilon, & H = C_3, \\ \mathbb{1} \oplus \rho, & H = C_2, \\ \mathbb{1} \oplus \epsilon \oplus \rho^{\oplus 2}, & H = \{e\}, \end{cases}$$

which gives the required Brauer relation.

Example 4.5. $\Psi = C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}$ is a Brauer relation for $C_2 \times C_2$ where C_2^i denote the proper subgroups of $C_2 \times C_2$.

To see this, let $\epsilon_i : C_2 \times C_2 \to \{\pm 1\}$ be the non-trivial one-dimensional character determined by $\epsilon_i(C_2^i) = 1$. Then, it follows that $\mathbb{C}[(C_2 \times C_2)/C_2^i] \cong \mathbb{1} \oplus \epsilon_i$, $\mathbb{C}[C_2 \times C_2] \cong \mathbb{1} \oplus \epsilon_a \oplus \epsilon_b \oplus \epsilon_c$. This gives the required Brauer relation.

Example 4.6. $\Xi = C_p - \{e\}$ is a pseudo Brauer relation relative to the trivial representation $\mathbb{1}$ of the cyclic group C_p.

The set of all pseudo Brauer relations relative to $\mathcal{V}$ forms an abelian subgroup of $\mathbb{Z}[\mathcal{H}]$. In Examples 4.3-4.6, it is easy to see that this is free of rank 1 generated by Θ, Ψ and Ξ respectively. In general, the rank of this group is as follows.

Proposition 4.7. *Let $\mathcal{V}$ be an $L[G]$ representation and let $\mathrm{Irr}_{\mathbb{Q}}(G)$ be the set of isomorphism classes of irreducible representations of G over $\mathbb{Q}$. Then,*

$$\mathrm{rk}_{\mathbb{Z}}\mathrm{PBR}(\mathcal{V}) = |\{\text{conj. classes of non-cyclic } H \leq G\}| + |\{\rho \in \mathrm{Irr}_{\mathbb{Q}}(G) : \langle \rho, \mathcal{V} \rangle = 0\}|,$$

where $\mathrm{PBR}(\mathcal{V}) \subseteq \mathbb{Z}[\mathcal{H}]$ *denotes the subgroup of pseudo Brauer relations relative to* $\mathcal{V}$*.*

Proof. Denote by $BR \subseteq \mathbb{Z}[\mathcal{H}]$ the subgroup of Brauer relations. It's well known that the rank of BR is equal to the number of conjugacy classes of non-cyclic subgroups of G. Indeed, denoting by $R(G)$ the rational representation ring, we have a natural linear map $\alpha : \mathbb{Q}[\mathcal{H}] \to R(G) \otimes \mathbb{Q}$ sending $\sum_i n_i H_i$ to $\sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1}$. The kernel of α is $BR \otimes \mathbb{Q}$, the dimension of $R(G) \otimes \mathbb{Q}$ is equal to the number of conjugacy classes of cyclic subgroups of G by [79, §13.1, Cor. 1], and α is surjective by the induction theorem [79, §13.1, Theorem 30].

The restriction of α to $PBR(\mathcal{V}) \otimes \mathbb{Q}$ is readily seen to have image contained in the subspace of $R(G) \otimes \mathbb{Q}$ spanned by irreducible rational representations ρ with $\langle \rho, \mathcal{V} \rangle = 0$. To complete the proof we need to show that, conversely, any such ρ lies in the image of α. This, again, is a consequence of the induction theorem [79, §13.1, Theorem 30]. □

4.2 Regulator constants

In this section, we define regulator constants of pseudo Brauer relations.

Notation 4.8. Let $\Theta = \sum_i H_i - \sum_j H'_j \in \mathbb{Z}[\mathcal{H}]$ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$. Given a non-degenerate, G-invariant, L-bilinear pairing $\langle\langle , \rangle\rangle$ on $\mathcal{V}$, we denote by $\langle , \rangle_1$ the pairing

$$\langle , \rangle_1 = \bigoplus_i \frac{1}{|H_i|} \langle\langle , \rangle\rangle \quad \text{on the vector space} \quad \bigoplus_i \mathcal{V}^{H_i},$$

and define the pairing $\langle , \rangle_2$ on $\bigoplus_j \mathcal{V}^{H'_j}$ similarly. Given a basis $\mathcal{B} = \{v_i\}$ for $\bigoplus_i \mathcal{V}^{H_i}$, we denote by $\langle \mathcal{B}, \mathcal{B} \rangle_1$ the matrix with (i,j)th entry $\langle v_i, v_j \rangle_1$, and define $\langle \mathcal{B}', \mathcal{B}' \rangle_2$ for a basis $\mathcal{B}'$ of $\bigoplus_j \mathcal{V}^{H'_j}$ similarly. By [28, Lemma 2.15], both $\langle , \rangle_1$ and $\langle , \rangle_2$ are non-degenerate.

Definition 4.9. Let $\Theta = \sum_i H_i - \sum_j H'_j \in \mathbb{Z}[\mathcal{H}]$ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$, and let $\langle\langle , \rangle\rangle$ be a non-degenerate,

G-invariant, L-bilinear pairing on $\mathcal{V}$ taking values in some field extension L' of L. Given bases $\mathcal{B}$ for $\bigoplus_i \mathcal{V}^{H_i}$ and $\mathcal{B}'$ for $\bigoplus_j \mathcal{V}^{H'_j}$, we define

$$\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V}) = \frac{\det\langle \mathcal{B}, \mathcal{B}\rangle_1}{\det\langle \mathcal{B}', \mathcal{B}'\rangle_2} \in L'^{\times}.$$

We then define the *regulator constant of* $\mathcal{V}$ *relative to* Θ, denoted $\mathcal{C}_\Theta(\mathcal{V})$, to be the class of $\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V})$ in $L'^{\times}/L^{\times 2}$ for any choice of bases $\mathcal{B}$, $\mathcal{B}'$ (the result being independent of this choice).

Remark 4.10. By Theorem 4.14, the quantity $\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V})$ is non-zero and independent of the choice of pairing. Therefore, by choosing an L-valued pairing on $\mathcal{V}$ we deduce that $\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V}) \in L^{\times}$.

In addition, its class $\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V})$ in $L^{\times}/L^{\times 2}$ is independent of the choice of bases $\mathcal{B}, \mathcal{B}'$. This is seen by the transformation rule $A \mapsto M^{\vee}AM$ for matrices of bilinear forms A with respect to the change of basis matrix M (where $M^{\vee}$ denotes the transposed matrix).

In particular, by choosing diagonal bases for $\oplus_i \mathcal{V}^{H_i}$ and $\oplus_j \mathcal{V}^{H'_j}$, then

$$\mathcal{C}_\Theta(\mathcal{V}) = \frac{\prod_i \det\big(\frac{1}{|H_i|}\langle\!\langle , \rangle\!\rangle|\mathcal{V}^{H_i}\big)}{\prod_j \det\big(\frac{1}{|H'_j|}\langle\!\langle , \rangle\!\rangle|\mathcal{V}^{H'_j}\big)},$$

where $\det\big(\frac{1}{|H_i|}\langle\!\langle , \rangle\!\rangle|\mathcal{V}^{H_i}\big) \in L'^{\times}/L^{\times 2}$ denotes $\det(\frac{1}{|H_i|}\langle\!\langle e_i, e_j\rangle\!\rangle)$ evaluated in any L-basis $\{e_i\}$ for $\mathcal{V}^{H_i}$ (and similarly for $\mathcal{V}^{H'_j}$). By convention, we take an empty determinant to be 1.

Example 4.11. Consider the Brauer relation $\Theta = C_3 + 2C_2 - \{e\} - 2S_3$ from Example 4.4. We let ρ denote the two-dimensional S_3-representation determined by $V = \{(x_1, x_2, x_3) | \sum_{i=1}^3 x_i = 0\} \subseteq \mathbb{Q}^3$ with the S_3-action given by $g \cdot (x_1, x_2, x_3) = (x_{g(1)}, x_{g(2)}, x_{g(3)})$.

Then, $v_1 = (1, -1, 0), v_2 = (0, 1, -1)$ form a basis for V and a G-invariant inner product $\langle\!\langle , \rangle\!\rangle$ on V with respect to this basis is given by the following matrix:

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Let's suppose that $C_2 = \langle(1,2)\rangle$. Then, ρ^H is 0-dimensional when $H = C_3, S_3$ and one-dimensional spanned by $v_1 + 2v_2$ when $H = C_2$. Therefore,

$$\mathcal{C}_\Theta(\rho) = \frac{(1)\cdot\left(\frac{1}{2}\langle\!\langle v_1+2v_2, v_1+2v_2\rangle\!\rangle\right)^2}{\det\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}\cdot(1)^2} = 3 \mod \mathbb{Q}^{\times 2}.$$

Now consider $\epsilon = \det(\rho)$, the 1-dimensional sign representation of S_3. Then, ϵ^H is 0-dimensional when $H = C_2, S_3$, while C_3 acts trivially on ϵ. Therefore, by choosing any non-trivial pairing on ϵ (for example, $\langle\!\langle v, v\rangle\!\rangle = 1$ for v any non-zero vector in ϵ), we deduce

$$\mathcal{C}_\Theta(\epsilon) = \frac{\frac{1}{3}\cdot(1)^2}{\frac{1}{1}\cdot(1)^2} = 3 \mod \mathbb{Q}^{\times 2}.$$

It's also easy to show that

$$\mathcal{C}_\Theta(\mathbb{1}) = \frac{\frac{1}{3}\cdot(\frac{1}{2})^2}{\frac{1}{1}\cdot(\frac{1}{6})^2} = 3.$$

Therefore, the regulator constants for the irreducible S_3-representations are:

	$\mathbb{1}$	ϵ	ρ
$\mathcal{C}_\Theta$	3	3	3

Example 4.12. Consider the Brauer relation $\Psi = C_2^a + C_2^b + C_2^c - 2C_2\times C_2 - \{e\}$ from Example 4.5. Let $\langle\!\langle , \rangle\!\rangle$ be any non-zero pairing on $\mathbb{1}$. Then,

$$\mathcal{C}_\Psi(\mathbb{1}) = \frac{(\frac{1}{2})\cdot(\frac{1}{2})\cdot(\frac{1}{2})}{(\frac{1}{4})^2\cdot(\frac{1}{1})} = 2 \mod \mathbb{Q}^{\times 2}.$$

In addition, let ϵ_a be the non-trivial, irreducible character of $C_2\times C_2$ determined by $\epsilon_a(C_2^a) = 1$. It follows that

$$\mathcal{C}_\Psi(\epsilon_a) = \frac{(\frac{1}{2})\cdot(1)\cdot(1)}{(1)^2\cdot(\frac{1}{1})} = 2 \mod \mathbb{Q}^{\times 2}.$$

An identical calculation shows that $\mathcal{C}_\Psi(\epsilon_b) = \mathcal{C}_\Psi(\epsilon_c) = 2$, where ϵ_b, ϵ_c are the remaining, non-trivial irreducible representations of $C_2 \times C_2$.

To summarise, the regulator constants for the irreducible representations of $C_2 \times C_2$ are as follows:

	$\mathbb{1}$	ϵ_a	ϵ_b	ϵ_c
$\mathcal{C}_\Theta$	2	2	2	2

Example 4.13. Consider the pseudo Brauer relation $\Xi = C_p - \{e\}$ relative to $\mathbb{1}$ from Example 4.6. It follows that

$$\mathcal{C}_\Xi(\mathbb{1}) = \frac{(\frac{1}{p})}{(1)} = \frac{1}{p}.$$

Therefore, $\mathcal{C}_\Xi(\mathbb{1}) = p \bmod \mathbb{Q}^{\times 2}$.

Many properties of regulator constants associated to Brauer relations [28, §2.ii] continue to hold for the pseudo Brauer relations of Definition 4.9. Specifically, we have the following:

Theorem 4.14. *Let L be a field of characteristic 0, G be a finite group and $\mathcal{V}, \mathcal{V}_1, \mathcal{V}_2$ be finite dimensional self-dual $L[G]$-representations. Then,*

1. *given a pseudo Brauer relation Θ relative to $\mathcal{V}$, $\mathcal{C}_\Theta(\mathcal{V})$ is independent of the choice of pairing $\langle\langle , \rangle\rangle$, and takes values in $L^\times/L^{\times 2}$,*

2. *given pseudo Brauer relations Θ_1 and Θ_2 relative to $\mathcal{V}$, we have*

$$\mathcal{C}_{\Theta_1+\Theta_2}(\mathcal{V}) = \mathcal{C}_{\Theta_1}(\mathcal{V})\,\mathcal{C}_{\Theta_2}(\mathcal{V}),$$

3. *if Θ is a pseudo Brauer relation relative to both $\mathcal{V}_1$ and $\mathcal{V}_2$, then*

$$\mathcal{C}_\Theta(\mathcal{V}_1 \oplus \mathcal{V}_2) = \mathcal{C}_\Theta(\mathcal{V}_1)\mathcal{C}_\Theta(\mathcal{V}_2).$$

   In particular, if $\mathcal{V} \cong \bigoplus_i \mathcal{V}_i^{n_i}$ is a decomposition into self-dual $L[G]$-representations, then $\mathcal{C}_\Theta(\mathcal{V}) = \prod_i \mathcal{C}_\Theta(\mathcal{V}_i)^{n_i}$.

Remark 4.15. We note that $\mathcal{C}_\Theta$ is compatible with extension of scalars: if M/L is a field extension, then $\mathcal{C}_\Theta(\mathcal{V}) = \mathcal{C}_\Theta(\mathcal{V} \otimes_L M)$ in $M^\times/M^{\times 2}$. On the

other hand, if $\mathcal{V}$ descends to a $K[G]$-representation $\mathcal{W}$ for a subfield $K \subseteq L$, then $\mathcal{W}$ is unique up to $K[G]$-isomorphism. In particular, we can associate to $\mathcal{V}$ a well-defined regulator constant $\mathcal{C}_\Theta(\mathcal{W}) \in K^\times/K^{\times 2}$. We will often omit $\mathcal{W}$ from the notation and simply view $\mathcal{C}_\Theta(\mathcal{V})$ as an element of $K^\times/K^{\times 2}$ without comment.

Theorem 4.14 is a generalisation of [28, Theorem 2.17 & Corollary 2.18]. In addition, the following result generalises [28, Corollary 2.25 & Lemma 2.26]. Recall that a G-representation $\mathcal{V}$ is said to be *symplectic* if its space admits a non-degenerate alternating and G-invariant pairing.

Lemma 4.16. *Let $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation relative to $\mathcal{V}$. If either*

1. *$\mathcal{V}$ is symplectic, or*
2. *$\langle \mathcal{V}, L[G/H_i]\rangle = \langle \mathcal{V}, L[G/H'_j]\rangle = 0$ for all i, j,*

then $\mathcal{C}_\Theta(\mathcal{V}) \equiv 1 \bmod L^{\times 2}$.

Proof. See [28, Corollary 2.25, Lemma 2.26]. □

We use this to show that $\mathcal{C}_\Theta(\mathcal{V})$ can be taken to be a positive real number.

Lemma 4.17. *Let Θ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$. Then, there exists a positive real number in the same class as $\mathcal{C}_\Theta(\mathcal{V})$ in $L^\times/L^{\times 2}$. (Recall that we fixed an embedding $L \hookrightarrow \mathbb{C}$ at the start of the section.)*

Proof. Write $\mathcal{V} \cong \psi_1 \oplus \psi_2$ where ψ_1 (resp. ψ_2) is an orthogonal (resp. symplectic) respresentation. Then $\mathcal{C}_\Theta(\mathcal{V}) = \mathcal{C}_\Theta(\psi_1)\mathcal{C}_\Theta(\psi_2) = \mathcal{C}_\Theta(\psi_1)$ by Theorem 4.14(3) and Lemma 4.16(1). Now ψ_1 is realisable over $\mathbb{R}$, say on a real vector space $\mathcal{W}$, which necessarily admits a positive definite G-invariant pairing (take the average, over $g \in G$, of any inner product). The associated pairings $\langle , \rangle_1, \langle , \rangle_2$ (as in Notation 4.8) are then positive definite. Computing $\mathcal{C}_\Theta(\mathcal{W})$ with respect to these pairings we obtain a positive real number. By Remark 4.15, this gives the result. □

4.3 Computable sets of representations

We now introduce a special set of representations in the case $L = \mathbb{Q}_p$. For an analogous formulation in terms of a special class of representations, denoted $\tau_{\Theta,p}$, see [32, §3.3].

Definition 4.18. Let Θ be a pseudo Brauer relation relative to a self-dual $\mathbb{Q}_p[G]$-representation $\mathcal{V}$. Consider the set $\mathcal{R}_{\mathcal{V}}$ of all $\mathbb{Q}_p$-irreducible representations which are self-dual and satisfy $\langle \tau, \mathcal{V} \rangle > 0$. Then, we define

$$S_{\Theta,p}(\mathcal{V}) = \{\tau \in \mathcal{R}_{\mathcal{V}} \mid \mathrm{ord}_p \mathcal{C}_\Theta(\tau) \equiv 1 \mod 2\}.$$

When there is no confusion, we will simply write $S_{\Theta,p}$ to denote this set.

Any self-dual representation $\mathcal{V}$ admits a decomposition of the form $\mathcal{V} \cong \bigoplus_{\tau \in \mathcal{R}_{\mathcal{V}}} \tau^{n_\tau} \oplus \rho$, where ρ satisfies $\rho \otimes \overline{\mathbb{Q}}_p \cong \sigma \oplus \sigma^*$ for $\sigma \neq \sigma^*$. The set $S_{\Theta,p}$ computes the parity of $\mathrm{ord}_p \mathcal{C}_\Theta(\mathcal{V})$ in the following sense.

Lemma 4.19. *We have* $\mathrm{ord}_p \mathcal{C}_\Theta(\mathcal{V}) \equiv \sum_{\tau \in S_{\Theta,p}} \frac{\langle \mathcal{V}, \tau \rangle}{\langle \tau, \tau \rangle} \mod 2$.

Proof. As in [28, proof of Cor. 2.25], $\rho \otimes \overline{\mathbb{Q}}_p$ admits a non-degenerate alternating and G-invariant pairing, and using [28, proof of Thm. 2.24], we deduce that ρ does too. Therefore, $\mathcal{C}_\Theta(\rho) = 1$ by Lemma 4.16(1). Then,

$$\mathrm{ord}_p \mathcal{C}_\Theta(\mathcal{V}) \overset{\text{Thm. 4.14(3)}}{\equiv} \sum_{\tau \in \mathcal{R}_v} n_\tau \mathrm{ord}_p \mathcal{C}_\Theta(\tau) + \mathrm{ord}_p \mathcal{C}_\Theta(\rho) \overset{\substack{\text{Lem. 4.16(1)} \\ \text{Def. 4.18}}}{\equiv} \sum_{\tau \in S_{\Theta,p}} n_\tau \mod 2.$$

Since $n_\tau = \frac{\langle \mathcal{V}, \tau \rangle}{\langle \tau, \tau \rangle}$, the result follows. □

Example 4.20. The following table gives the computable sets $S_{\Theta,p}$ in the case of Examples 4.4–4.6. For details, see Examples 4.11–4.13.

$\mathcal{V}$	G	Θ	p	$S_{\Theta,p}$
$\mathbb{Q}[G]$	S_3	$C_3 + 2C_2 - \{e\} - 2S_3$	3	$\{\mathbb{1}, \epsilon, \rho\}$
$\mathbb{Q}[G]$	$C_2 \times C_2$	$C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}$	2	$\{\mathbb{1}, \epsilon_a, \epsilon_b, \epsilon_c\}$
$\mathbb{1}$	C_p	$C_p - \{e\}$	p	$\{\mathbb{1}\}$

4.4 Alternative definition of regulator constants

The following reinterpretation of regulator constants is based on expositions, in the case of Brauer relations, given in [2, §3] and [29, Lemma 3.2]. We begin with some notation.

Notation 4.21. Let M be a $\mathbb{Z}[G]$-module (below we will take $M = \mathcal{V}$ to be a self-dual $L[G]$-representation, but this greater generality will be useful in Chapters 5&6). For each subgroup H of G we have an isomorphism

$$\mathrm{Hom}_G(\mathbb{Z}[G/H], M) \xrightarrow{\sim} M^H \qquad (*)$$

given by evaluating homomorphisms at the trivial coset. Given subgroups $H_1, \ldots, H_n$ and $H'_1, \ldots, H'_m$ of G, define G-sets $S = \bigsqcup_{i=1}^n G/H_i$ and $S' = \bigsqcup_{j=1}^m G/H'_j$. Taking $\mathbb{Z}[S]$ and $\mathbb{Z}[S']$ to be the corresponding permutation modules, $(*)$ induces isomorphisms

$$\mathrm{Hom}_G(\mathbb{Z}[S], M) \cong \bigoplus_i M^{H_i} \quad \text{and} \quad \mathrm{Hom}_G(\mathbb{Z}[S'], M) \cong \bigoplus_j M^{H'_j}.$$

Consequently, given $\Phi \in \mathrm{Hom}_G(\mathbb{Z}[S], \mathbb{Z}[S'])$, the map from $\mathrm{Hom}_G(\mathbb{Z}[S'], M)$ to $\mathrm{Hom}_G(\mathbb{Z}[S], M)$ sending f to $f \circ \Phi$ induces a homomorphism

$$\Phi^* : \bigoplus_j M^{H'_j} \to \bigoplus_i M^{H_i}.$$

The G-module $\mathbb{Z}[S]$ (resp. $\mathbb{Z}[S']$) is canonically self-dual, via the pairing making the elements of S (resp. S') an orthonormal basis. Given $\Phi \in \mathrm{Hom}_G(\mathbb{Z}[S], \mathbb{Z}[S'])$ we denote by $\Phi^\vee$ the corresponding dual homomorphism $\Phi^\vee : \mathbb{Z}[S'] \to \mathbb{Z}[S]$.

Definition 4.22. Let $\Theta = \sum_i H_i - \sum_j H'_j \in \mathbb{Z}[\mathcal{H}]$ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$. We say that a $\mathbb{Z}[G]$-module

homomorphism $\Phi : \bigoplus_i \mathbb{Z}[G/H_i] \to \bigoplus_j \mathbb{Z}[G/H'_j]$ *realises* Θ if the induced map

$$\Phi^* : \bigoplus_j \mathcal{V}^{H'_j} \to \bigoplus_i \mathcal{V}^{H_i}$$

is an isomorphism.

Remark 4.23. If $\Theta = \sum_i H_i - \sum_j H'_j$ is a Brauer relation (see Remark 4.3), then a G-map realising it is a G-injection $\Phi : \bigoplus_i \mathbb{Z}[G/H_i] \to \bigoplus_j \mathbb{Z}[G/H'_j]$ with finite cokernel.

Example 4.24. We consider $\Theta = C_3 + 2C_2 - \{e\} - 2S_3$, the Brauer relation for S_3 from Example 4.4. We fix generators g, h for S_3 so that $S_3 = \langle g, h | g^3 = h^2 = hghg = e \rangle$. Let θ denote the injective S_3-module homomorphism

$$\theta : \mathbb{Z}[S_3/\langle g \rangle]y_1 \oplus \mathbb{Z}[S_3/\langle h \rangle]y_2 \oplus \mathbb{Z}[S_3/\langle h \rangle]y_3 \to \mathbb{Z}[S_3]x_1 \oplus \mathbb{Z}x_2 \oplus \mathbb{Z}x_3$$

determined by $y_1 \mapsto (e + g + g^2)x_1 + x_3$, $y_2 \mapsto (e + h)x_1 + x_2$, and $y_3 \mapsto (e + h)gx_1$. With respect to the bases $\{y_1, hy_1, y_2, gy_2, g^2y_2, y_3, gy_3, g^2y_3\}$ and $\{x_1, gx_1, g^2x_1, hx_1, hgx_1, hg^2x_1, x_2, x_3\}$, θ is given by the following matrix.

$$\left[\begin{array}{cc|ccc|ccc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

This matrix has full rank. Therefore, θ realises $\Theta = C_3 + 2C_2 - \{e\} - 2S_3$.

Example 4.25. We consider $\Psi = C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}$, the Brauer relation for $C_2 \times C_2$ from Example 4.5. We fix generators σ, τ for it so that $C_2 \times C_2 = \langle \sigma, \tau | \sigma^2 = \tau^2 = \sigma\tau\sigma\tau = e \rangle$. Let ψ denote the injective G-module

homomorphism

$$\psi : \mathbb{Z}[G/\langle\sigma\rangle]y_1 \oplus \mathbb{Z}[G/\langle\tau\rangle]y_2 \oplus \mathbb{Z}[G/\langle\sigma\tau\rangle]y_3 \to \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \mathbb{Z}[G]x_3$$

determined by $y_1 \mapsto x_1+(e+\sigma)x_3,\ y_2 \mapsto x_2+(e+\tau)x_3,\ y_3 \mapsto (1+\sigma\tau)x_3$. With respect to the bases $\{y_1, \tau y_1, y_2, \sigma y_2, y_3, \sigma y_3\}$ and $\{x_1, x_2, x_3, \sigma x_3, \tau x_3, \sigma\tau x_3\}$, ψ is given by the following matrix.

$$\left[\begin{array}{cc|cc|cc} 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right]$$

This matrix has full rank. Therefore, ψ realises Ψ.

Example 4.26. Consider $\Xi = C_p - \{e\}$, the pseudo Brauer relation relative to $\mathbb{1}$ from Example 4.6, and let g be a generator for C_p. We let $\xi : \mathbb{Z} \to \mathbb{Z}[C_p]$ be the map determined by $1 \mapsto \sum_{i=0}^{p-1} g^i$. Then, the induced map $\xi^* : \mathbb{1} \to \mathbb{1}$ is the multiplication-by-p map. Therefore, ξ realises $\Xi = C_p - \{e\}$

Lemma 4.27. *Let $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation relative to an $L[G]$-representation $\mathcal{V}$. Then, there exists a G-module homomorphism Φ realising Θ.*

Proof. By Definition 4.1, we can find $\mathbb{C}G$-representations ρ_1, ρ_2 such that $\rho_1 \oplus \bigoplus_i \mathbb{C}[G/H_i]$ is isomorphic to $\rho_2 \oplus \bigoplus_j \mathbb{C}[G/H'_j]$. We may assume that ρ_1 and ρ_2 have no common irreducible constituents ensuring that both ρ_1, ρ_2 are realisable over $\mathbb{Q}$. We can then find free $\mathbb{Z}[G]$-modules V_1 and V_2 such that $V_1 \otimes_{\mathbb{Z}} \mathbb{C} \cong \rho_1$ and $V_2 \otimes_{\mathbb{Z}} \mathbb{C} \cong \rho_2$, and a G-module homomorphism

$$\phi : V_1 \oplus \bigoplus_i \mathbb{Z}[G/H_i] \to V_2 \oplus \bigoplus_j \mathbb{Z}[G/H'_j]$$

with finite kernel and cokernel. Denoting by ι and π the inclusion/projection in/out of the permutation modules, one checks that $\Phi = \pi \circ \phi \circ \iota$ realises the

pseudo Brauer relation Θ. □

Notation 4.28. Given finite dimensional L-vector spaces V, W, with bases $\mathcal{B}_1 = \{v_i\}_i, \mathcal{B}_2 = \{w_j\}_j$ respectively, and given an L-linear map $T : V \to W$, we write $[T]_{\mathcal{B}_1}^{\mathcal{B}_2}$ to denote the matrix of T relative to $\mathcal{B}_1$ and $\mathcal{B}_2$. Similarly to Notation 4.8, given a pairing $\langle\langle , \rangle\rangle$ between V and W, we denote by $\langle\langle \mathcal{B}_1, \mathcal{B}_2 \rangle\rangle$ the matrix with (i, j)th entry $\langle\langle v_i, w_j \rangle\rangle$.

The following proposition (along with Corollary 4.30) gives the promised alternative description of regulator constants.

We highlight that, while we have not yet shown that $\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V})$ is independent of the choice of pairing $\langle\langle , \rangle\rangle$ made in its definition, the proof of the proposition applies regardless of the choice made. As a by-product, this will prove the sought independence.

Proposition 4.29. *Let $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$. For any G-module homomorphism Φ realising Θ, we have*

$$\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V}) = \frac{\det[(\Phi^\vee)^*]_{\mathcal{B}}^{\mathcal{B}'}}{\det[\Phi^*]_{\mathcal{B}'}^{\mathcal{B}}}$$

where $\mathcal{B}$, $\mathcal{B}'$ are bases for $\bigoplus_i \mathcal{V}^{H_i}$, $\bigoplus_j \mathcal{V}^{H'_j}$ respectively.

Proof. Fix a non-degenerate G-invariant pairing $\langle\langle , \rangle\rangle$ on $\mathcal{V}$. We follow the proof of [29, Lemma 3.2]. For a finite G-set T we define the pairing $(,)_T$ on $\mathrm{Hom}_G(\mathbb{Z}[T], \mathcal{V})$ by setting

$$(f_1, f_2)_T = \frac{1}{|G|} \sum_{t \in T} \langle\langle f_1(t), f_2(t) \rangle\rangle.$$

Take $S = \bigsqcup_i G/H_i$ and $S' = \bigsqcup_j G/H'_j$. After identifying $\mathrm{Hom}_G(\mathbb{Z}[S], \mathcal{V})$ with $\bigoplus_i \mathcal{V}^{H_i}$ as in Notation 4.21, the pairing $(,)_S$ identifies with the pairing $\langle , \rangle_1$ of Notation 4.8. Similarly, the pairing $(,)_{S'}$ identifies with the pairing $\langle , \rangle_2$. A straightforward computation then shows that Φ^* and $(\Phi^\vee)^*$ are adjoint for the

pairings $\langle , \rangle_1$ and $\langle , \rangle_2$ (see [2, Theorem 3.2] for details). We now compute

$$\mathcal{C}_\Theta^{\mathcal{B},\mathcal{B}'}(\mathcal{V}) = \frac{\det\langle \mathcal{B}, \mathcal{B}\rangle_1}{\det\langle \mathcal{B}', \mathcal{B}'\rangle_2} = \frac{\det\langle \mathcal{B}, \Phi^*\mathcal{B}'\rangle_1}{\det[\Phi^*]_{\mathcal{B}'}^{\mathcal{B}}} \cdot \frac{\det[(\Phi^\vee)^*]_{\mathcal{B}}^{\mathcal{B}'}}{\det\langle (\Phi^\vee)^*\mathcal{B}, \mathcal{B}'\rangle_2} = \frac{\det[(\Phi^\vee)^*]_{\mathcal{B}}^{\mathcal{B}'}}{\det[\Phi^*]_{\mathcal{B}'}^{\mathcal{B}}}. \quad \square$$

Given a G-map Φ realising Θ and a basis $\mathcal{B}$ for $\bigoplus_i \mathcal{V}^{H_i}$, we write $\Phi^\vee\mathcal{B}$ for the basis for $\bigoplus_j \mathcal{V}^{H'_j}$ obtained by applying $(\Phi^\vee)^*$ (cf. Notation 4.21) to the basis vectors in $\mathcal{B}$.

Corollary 4.30. *Let Θ be a pseudo Brauer relation relative to a self-dual $L[G]$-representation $\mathcal{V}$. Then*

$$\mathcal{C}_\Theta^{\mathcal{B},\Phi^\vee\mathcal{B}}(\mathcal{V}) = \frac{1}{\det(\Phi^\vee\Phi)^*}.$$

In particular, $\mathcal{C}_\Theta^{\mathcal{B},\Phi^\vee\mathcal{B}}(\mathcal{V})$ is independent of $\mathcal{B}$.

Proof. Immediate from Proposition 4.29. $\square$

We can now prove Theorem 4.14.

Proof of Theorem 4.14. Parts (2) and (3) follow readily from part (1). To prove (1), pick some Φ realising the pseudo Brauer relation Θ (this always exists by Lemma 4.27), and pick a pairing $\langle\langle , \rangle\rangle$ as in the definition of $\mathcal{C}_\Theta(\mathcal{V})$. The proof of Proposition 4.29 then shows that

$$\mathcal{C}_\Theta(\mathcal{V}) \equiv \det(\Phi^\vee\Phi)^* \mod L^{\times 2}.$$

Since the right hand side is an element of $L^\times$ which is independent of $\langle\langle , \rangle\rangle$, the result follows. $\square$

Remark 4.31. The choice of representatives in $\mathcal{H}$ made at the start of this section does not affect the above results in any meaningful way. For instance, if $\Theta = \sum_i H_i - \sum_j H'_j \in \mathbb{Z}[\mathcal{H}]$ is a pseudo Brauer relation relative to $\mathcal{V}$, and we set $M_i = g_i H_i g_i^{-1}$, $M'_i = g'_i H'_i g_i'^{-1}$ for some $g_i, g'_i \in G$, then we have canonical isomorphisms $\bigoplus_i \mathcal{V}^{H_i} \simeq \bigoplus_i \mathcal{V}^{M_i}$ and $\bigoplus_i \mathbb{Z}[G/M_i] \simeq \bigoplus_i \mathbb{Z}[G/H_i]$ given by $(x_i) \mapsto (g_i x_i)$ and $(y_i M_i) \mapsto (y_i g_i H_i)$ respectively. Similarly for H'_j.

We conclude that the calculation of a regulator constant from Definition 4.9 and the notion of realising a pseudo Brauer relation from Definition 4.22 are consistent even after a change from Θ to $\Theta' = \sum_i M_i - \sum_j M'_j$. In addition, a change from Θ to Θ' does not affect Proposition 4.29 or Corollary 4.30.

Chapter 5

Rank parity from pseudo Brauer relations

In this chapter, we apply regulator constants and pseudo Brauer relations to study parities of ranks of Jacobians.

We first present a formalism which associates to a pseudo Brauer relation relative to the ℓ-adic Tate module an isogeny, see Theorem 5.3. In particular, we show that if Φ is a G-map realising this pseudo Brauer relation, then the induced homomorphism f_Φ given in Definition A.5 is an isogeny.

We then use the induced isogeny to give a definition of a purely local arithmetic invariant Λ_Θ and a method for studying Selmer rank parities of Jacobians in terms of these local invariants, see Theorem 5.7.

5.1 Isogenies from pseudo Brauer relations

We let X be a curve defined over a characteristic 0 field K, and let G be a finite subgroup of $\mathrm{Aut}_K(X)$.

Definition 5.1. We say that Θ is a pseudo Brauer relation for G and X if Θ is a pseudo Brauer relation relative to $V_\ell(\mathrm{Jac}_X)$ in the sense of Definition 4.1. When there is no ambiguity, we call these pseudo Brauer relations for X.

Remark 5.2. Having fixed an embedding $K \hookrightarrow \mathbb{C}$, we have a $\mathbb{Q}_\ell[G]$-module isomorphism

$$H_1(\mathrm{Jac}_X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Q}_\ell \cong V_\ell(\mathrm{Jac}_X)$$

for every prime ℓ [1, Exposé XI, Theorem 4.4]. Therefore the notion of a pseudo Brauer relation for X is independent of ℓ.

Theorem 5.3. *Let X be a curve over a field K of characteristic 0, and G be a finite subgroup of $\mathrm{Aut}_K(X)$. Let $\sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation for X realised by Φ (in the sense of Definition 4.22). Then, the following hold:*

1. *The induced homomorphism*

$$f_\Phi : \prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i}$$

   afforded by Theorem A.1 is a K-isogeny.

2. *If Φ' realises a pseudo Brauer relation $\sum_j H'_j - \sum_k H''_k$ for X, then the composition $\Phi'\Phi$ realises $\sum_i H_i - \sum_k H''_k$ and $f_{\Phi'\Phi} = f_\Phi f_{\Phi'}$.*

3. *The dual homomorphism $\Phi^\vee$ (as in Notation 4.21) realises the pseudo Brauer relation $\sum_j H'_j - \sum_i H_i$ for X, and we have $f_{\Phi^\vee} = (f_\Phi)^\vee$ where $(f_\Phi)^\vee$ denotes the dual of f_Φ with respect to the canonical principal polarisations.*

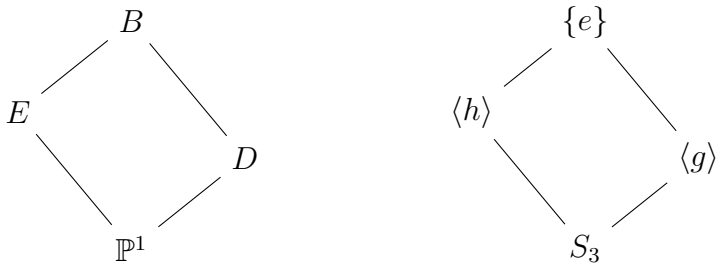
Proof. For (1), we first show that $V_\ell(f_\Phi) : \prod_j V_\ell(\mathrm{Jac}_{X/H'_j}) \to \prod_i V_\ell(\mathrm{Jac}_{X/H_i})$ agrees with the pull-back map $\Phi^* : \prod_j V_\ell(\mathrm{Jac}_X)^{H'_j} \to \prod_i V_\ell(\mathrm{Jac}_X)^{H_i}$ of Notation 4.21 after identifying $V_\ell(\pi_H^*) : V_\ell(\mathrm{Jac}_{X/H}) \xrightarrow{\sim} V_\ell(\mathrm{Jac}_X)^H$ using Theorem 3.9(1). By additivity, it suffices to prove this in the case where Φ is a map $\mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$. A direct consequence of Lemma A.4 is that $\pi_H^* f_\Phi = \tilde{\Phi}\pi_{H'}^*$. Applying $V_\ell(-)$ to this composition gives rise to a commutative diagram

$$\begin{array}{ccc} V_\ell(\mathrm{Jac}_{X/H'}) & \xrightarrow{V_\ell(f_\Phi)} & V_\ell(\mathrm{Jac}_{X/H}) \\ {\scriptstyle V_\ell(\pi_{H'}^*)}\downarrow \cong & & {\scriptstyle V_\ell(\pi_H^*)}\downarrow \cong \\ V_\ell(\mathrm{Jac}_X)^{H'} & \xrightarrow{\Phi^*} & V_\ell(\mathrm{Jac}_X)^H \end{array}$$

It therefore follows that $V_\ell(f_\Phi)$ agrees with Φ^*. Since Φ realises Θ, then the induced map $\Phi^* : \prod_j V_\ell(\mathrm{Jac}_X)^{H'_j} \to \prod_i V_\ell(\mathrm{Jac}_X)^{H_i}$ is an isomorphism. Since this agrees with $V_\ell(f_\Phi)$, claim (1) follows from Faltings' isogeny theorem.

For (2), it is clear that $\Phi'\Phi$ realises the pseudo Brauer relation $\sum_i H_i - \sum_k H''_k$, while the equality $f_{\Phi'\Phi} = f_\Phi f_{\Phi'}$ follows from Theorem A.1(1). The duality assertion of (3) follows from Theorem A.1(2). □

Example 5.4. We consider Example 2.10 with $\Theta = C_3 + 2C_2 - \{e\} - 2S_3$, the Brauer relation for S_3 from Example 4.4. We also fix generators g, h so that $S_3 = \langle g, h | g^3 = h^2 = hghg = e \rangle$. We then have the following Galois cover with the corresponding lattice of subgroups on the right:



Let θ denote the injective S_3-module homomorphism from Example 4.24. By Theorem 5.3, there are isogenies

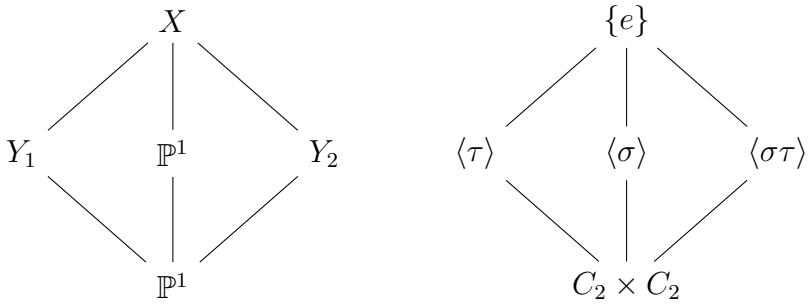
$$f_\theta : \mathrm{Jac}_B \to E \times E \times \mathrm{Jac}_D \quad \text{and} \quad f_{\theta^\vee} = f_\theta^\vee : E \times E \times \mathrm{Jac}_D \to \mathrm{Jac}_B.$$

Explicitly, the isogenies associated to θ and $\theta^\vee$ are given by

$$f_\theta = (\pi_{E*}, \pi_{E*} \circ g_*, \pi_{D*}) \quad \text{and} \quad (f_\theta)^\vee = \pi_E^* + g^* \circ \pi_E^* + \pi_D^*,$$

where $\pi_E : B \to E$, $\pi_D : B \to D$ denote the quotient maps.

Example 5.5. We consider Example 1.5 with $\Psi = C_2^a + C_2^b + C_2^c - 2C_2 \times C_2 - \{e\}$, the Brauer relation for $C_2 \times C_2$ from Example 4.5. Then, the Galois cover is as follows:



Theorem 5.3 associates an isogeny $f_\psi : \mathrm{Jac}_X \to \mathrm{Jac}_{Y_1} \times \mathrm{Jac}_{Y_2}$ to the homomorphism ψ from Example 4.25. Explicitly, $f_\psi = (\pi_{1*}, \pi_{2*})$, with the dual isogeny given by $f_\psi^\vee = \pi_1^* + \pi_2^*$, where $\pi_1 : X \to Y_1$ and $\pi_2 : X \to Y_2$ are the natural quotient maps.

The next result concerns the degree of the induced isogeny of Theorem 5.3. Recall that a G-representation $\mathcal{V}$ is said to be *orthogonal* if its space admits a non-degenerate symmetric bilinear form invariant under G.

Proposition 5.6. *Suppose that $\Omega^1(\mathrm{Jac}_X)$ is a self-dual G-representation. Fix any basis $\mathcal{B}_1$ for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i})$ and let $\Phi^\vee\mathcal{B}_1$ be the basis for $\Omega^1(\prod_j \mathrm{Jac}_{X/H'_j})$ obtained by applying $(\Phi^\vee)^*$ to the basis vectors in $\mathcal{B}_1$.*

1. *We have*
$$\mathcal{C}_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(\Omega^1(\mathrm{Jac}_X))^{-1} = \pm\deg(f_\Phi).$$

2. *If $\Omega^1(\mathrm{Jac}_X)$ is orthogonal, then*
$$\mathcal{C}_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(\Omega^1(\mathrm{Jac}_X))^{-1} = \deg(f_\Phi).$$

3. *For any G-maps Φ_1, Φ_2 realising Θ, $\deg(f_{\Phi_1})/\deg(f_{\Phi_2})$ lies in $\mathbb{Q}^{\times 2}$.*

Proof. For (1), we compute

$$\begin{aligned}
\mathcal{C}_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(\Omega^1(\mathrm{Jac}_X))^{-2} &\overset{\text{Cor. 4.30 \& [53, Lem. 5.10(1)]}}{=} \det\big((\Phi^\vee\Phi)^* \mid V_\ell(\prod \mathrm{Jac}_{X/H_i})\big)\\
&\overset{\text{[53, Lem. 4.28]}}{=} \det\big(f_{\Phi^\vee\Phi} \mid V_\ell(\prod \mathrm{Jac}_{X/H_i})\big)\\
&\overset{\text{[66, Prop. 12.9]}}{=} \deg(f_{\Phi^\vee\Phi})\\
&\overset{\text{Thm. 5.3 (2),(3)}}{=} \deg(f_\Phi)^2.
\end{aligned}$$

For (2), the G-representation $\Omega^1(\mathrm{Jac}_X)$ is realisable over $\mathbb{R}$ [79, §13.2, Thm. 31], say on an $\mathbb{R}$-vector space $W_\mathbb{R}$. By evaluating $\mathcal{C}_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(\Omega^1(\mathrm{Jac}_X))$ with respect to an $\mathbb{R}$-basis $\mathcal{B}_1$ for $\prod_i (W_\mathbb{R})^{H_i}$, Lemma 4.17 combined with Theorem 4.14(1) tell us that $\mathcal{C}_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(\Omega^1(\mathrm{Jac}_X))$ is a positive real number. Since the equality in (1) holds for any $\mathcal{B}_1$, we obtain the result. For (3), note that $\Omega^1(\mathrm{Jac}_X)^{\oplus 2}$ is realisable over $\mathbb{Q}$ by [53, Lemma 5.10(2)]. It follows from [76, Theorem 32.15] that there exist infinitely many distinct quadratic extensions $L/\mathbb{Q}$ such that $\Omega^1(\mathrm{Jac}_X)$ is realisable over L. For each such, we deduce from part (1) and Theorem 4.14(1) that $\pm\frac{\deg(f_{\Phi_1})}{\deg(f_{\Phi_2})} \in L^{\times 2}$. This is only possible if $\frac{\deg(f_{\Phi_1})}{\deg(f_{\Phi_2})} \in \mathbb{Q}^{\times 2}$. □

5.2 Local formulae for Selmer rank parities

The main result of this section is the following.

Theorem 5.7. *Let X be a curve over a number field K and G be a finite subgroup of $\mathrm{Aut}_K(X)$. Let Θ be a pseudo Brauer relation for X, and suppose that $\Omega^1(\mathrm{Jac}_X)$ is a self-dual G-representation. Then*

$$\mathrm{ord}_p\mathcal{C}_\Theta(\mathcal{X}_p(\mathrm{Jac}_X)) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_p\Lambda_\Theta(X/K_v) \mod 2,$$

where the local invariant $\Lambda_\Theta(X/K_v)$ is as in Definition 5.24. In particular, we have

$$\sum_{\tau\in S_{\Theta,p}} \frac{\langle \mathcal{X}_p(\mathrm{Jac}_X),\tau\rangle}{\langle\tau,\tau\rangle} \equiv \sum_{v \text{ place of } K} \mathrm{ord}_p\ \Lambda_\Theta(X/K_v) \mod 2,$$

where $S_{\Theta,p}$ is the set from Definition 4.18 considered with respect to $\mathcal{X}_p(\mathrm{Jac}_X)$.

Given a K-rational isogeny $f_\Phi : \prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i}$, we write $f_\Phi(K_v)$ to denote the induced map on K_v-rational points. In order to prove Theorem 5.7, we begin by defining the following local invariant

$$\lambda_{\Theta,\Phi}(X/K_v) = \frac{\#\mathrm{coker} f_\Phi(K_v)}{\#\ker f_\Phi(K_v)} \cdot \frac{\prod_i \mu_v(X/H_i)}{\prod_j \mu_v(X/H'_j)},$$

where Φ is a G-map realising Θ and μ_v encodes whether a curve is deficient at a place v (see Definition 2.16). We prove an analogue of the above formula (see Theorem 5.14) with $\lambda_{\Theta,\Phi}$ in place of Λ_Θ. Unfortunately, $\lambda_{\Theta,\Phi}$ depends on the choice of Φ. We remove this dependence (see Lemma 5.17(1)) in the case when $\Omega^1(\mathrm{Jac}_X)$ is self-dual by introducing a revised invariant

$$\tilde{\lambda}_\Theta(X/K_v) = \lambda_{\Theta,\Phi}(X/K_v) \cdot \left|\sqrt{\deg(f_\Phi)}\right|_v.$$

The drawback now is that $\mathrm{ord}_p \tilde{\lambda}_\Theta \equiv 0, \frac{1}{2}, 1$ or $\frac{3}{2} \bmod 2$. We finally fix this (see Theorem 5.25(1)) by defining

$$\Lambda_\Theta(X/K_v) = \tilde{\lambda}_\Theta(X/K_v) \cdot \left|\sqrt{\mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_X))}\right|_v,$$

where $\mathcal{C}_\Theta^{\mathrm{sf}} \in \mathbb{N}$ denotes the square-free part of $\deg(f_\Phi)$, calculated with respect to any Φ. We caution that whilst $\tilde{\lambda}_\Theta$ is multiplicative in Θ, in general Λ_Θ is not.

Remark 5.8. When $K_v/\mathbb{Q}_\ell$ is a finite extension and $p \neq 2$ or ℓ, we will additionally show (see Theorem 5.25(3)) that

$$\mathrm{ord}_p \Lambda_\Theta(X/K_v) = \mathrm{ord}_p \frac{\prod_i c_v(\mathrm{Jac}_{X/H_i})}{\prod_j c_v(\mathrm{Jac}_{X/H'_j})},$$

where $c_v(A)$ denotes the Tamagawa number of an abelian variety A/K_v, see §2.3.1. Lemma 5.27 gives an analogue of this formula for arbitrary prime p.

Remark 5.9. By Theorem 3.1(2), $\mathcal{X}_p(\mathrm{Jac}_X)$ is a self-dual G-representation

for all p, and any pseudo Brauer relation for X is a pseudo Brauer relation relative to $\mathcal{X}_p(\mathrm{Jac}_X)$. Thus, the left-hand side of the formula in Theorem 5.7 is well-defined.

Remark 5.10. In Theorem 5.7, we consider the base change of X/K to all completions K_v, alongside the base-changed action of G on X/K_v. We note that X/K_v may not remain connected after base change (see proof of Proposition 2.17 for example). Consequently, the framework of general curves discussed in §2.1.3 and detailed in [53] is essential for studying parities of Selmer ranks using Theorem 5.7.

5.2.1 A local formula in $\lambda_{\Theta,\Phi}(X/\mathcal{K})$

Here we prove an analogue of Theorem 5.7 obtained by replacing Λ_Θ with the local invariant $\lambda_{\Theta,\Phi}$. As in §2.3.1, we use the following notation for Tamagawa numbers and real/complex periods.

Notation 5.11. For an abelian variety A over a local field $\mathcal{K}$ of characteristic 0, and choice of non-zero exterior form ω on A, we write

$$C(A,\omega) = \begin{cases} c(A)\cdot|\omega/\omega^0| & \text{when } \mathcal{K}/\mathbb{Q}_p \text{ is finite,} \\ \int_{A(\mathcal{K})}|\omega| & \text{when } \mathcal{K}=\mathbb{R}, \\ 2^{\dim(A)}\int_{A(\mathcal{K})}|\omega\wedge\bar{\omega}| & \text{when } \mathcal{K}=\mathbb{C}. \end{cases}$$

Here $\omega/\omega^0 \in \mathcal{K}^\times$ is such that $\omega = (\omega/\omega^0)\cdot\omega^0$, where ω^0 is a Néron exterior form on A.

Definition 5.12. Let $\mathcal{K}$ be a local field of characteristic 0, $X/\mathcal{K}$ be a curve, G be a finite subgroup of $\mathrm{Aut}_{\mathcal{K}}(X)$ and $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation for X. Fix bases $\mathcal{B}_1$, $\mathcal{B}_2$ for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i})$, $\Omega^1(\prod_j \mathrm{Jac}_{X/H'_j})$ and write $\omega(\mathcal{B}_1)$, $\omega(\mathcal{B}_2)$ for the exterior forms given by the wedge product of the elements in $\mathcal{B}_1$, $\mathcal{B}_2$ respectively. We define

$$\lambda_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(X/\mathcal{K}) = \frac{C(\prod_i \mathrm{Jac}_{X/H_i}, \omega(\mathcal{B}_1))}{C(\prod_j \mathrm{Jac}_{X/H'_j}, \omega(\mathcal{B}_2))}\cdot\frac{\prod_i \mu(X/H_i)}{\prod_j \mu(X/H'_j)}$$

where C is given in Notation 5.11 and μ is as in Definition 2.16.

Given a G-map Φ realising Θ, write $\Phi^\vee\mathcal{B}_1$ for the basis obtained by applying $(\Phi^\vee)^*$ to the elements of $\mathcal{B}_1$ (cf. Notation 4.21). We additionally define

$$\lambda_{\Theta,\Phi}(X/\mathcal{K}) = \lambda_\Theta^{\mathcal{B}_1,\Phi^\vee\mathcal{B}_1}(X/\mathcal{K}).$$

We write $f_\Phi(\mathcal{K})$ for the map on $\mathcal{K}$-points induced by the isogeny f_Φ.

Lemma 5.13. *We have*

$$\lambda_{\Theta,\Phi}(X/\mathcal{K}) = \frac{\#\mathrm{coker} f_\Phi(\mathcal{K})}{\#\ker f_\Phi(\mathcal{K})} \cdot \frac{\prod_i \mu(X/H_i)}{\prod_j \mu(X/H'_j)}.$$

In particular, $\lambda_{\Theta,\Phi}(X/\mathcal{K}) \in \mathbb{Q}^\times$ and is independent of the choice of $\mathcal{B}_1$.

Proof. By applying [53, Remark 4.29] with $F = \Omega^1(-)$, and taking exterior powers, we deduce that $f_\Phi^*\omega(\mathcal{B}_1) = \omega(\Phi^\vee\mathcal{B}_1)$ (alternatively, argue as in the proof of Theorem 5.3(1)). As in the proof of [65, Theorem 7.3], we have

$$\frac{C(\prod_i \mathrm{Jac}_{X/H_i}, \omega(\mathcal{B}_1))}{C(\prod_j \mathrm{Jac}_{X/H'_j}, \omega(\Phi^\vee\mathcal{B}_1))} = \frac{\#\mathrm{coker} f_\Phi(\mathcal{K})}{\#\ker f_\Phi(\mathcal{K})},$$

giving the required result. □

Theorem 5.14. *Let X be a curve over a number field K and G be a finite subgroup of $\mathrm{Aut}_K(X)$. Let Θ be a pseudo Brauer relation for X, Φ a G-map realising Θ and p a prime. Then,*

$$\mathrm{ord}_p\mathcal{C}_\Theta(\mathcal{X}_p(\mathrm{Jac}_X)) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_p\lambda_{\Theta,\Phi}(X/K_v) \mod 2.$$

Proof. For a K-isogeny $f : A \to B$, we write

$$Q(f) = \#\mathrm{coker}(f : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}}) \cdot \#\ker(f : Ш(A)_{\mathrm{div}} \to Ш(B)_{\mathrm{div}}),$$

where $Ш_{\mathrm{div}}$ denotes the divisible part of Ш. Thus, if f is a self-isogeny of A, then $\mathrm{ord}_pQ(f) = \mathrm{ord}_p\det(f|\mathcal{X}_p(A))$ (see for example [29, §2]). We let $\mathcal{B}_1$ be

a global basis for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i}/K)$ and write $\omega(\mathcal{B}_1)$ for the exterior form on $\prod_i \mathrm{Jac}_{X/H_i}/K$ obtained by taking the wedge product of elements in $\mathcal{B}_1$, and similarly for $\omega(\Phi^\vee\mathcal{B}_1)$. As in the proof of Lemma 5.13, $\omega(\Phi^\vee\mathcal{B}_1) = f_\Phi^*\omega(\mathcal{B}_1)$ and so

$$\begin{aligned}\frac{Q(f_\Phi)}{Q(f_\Phi^\vee)} &\overset{[30,\ \text{Thm. } 4.3]}{\equiv} \frac{\prod_v C_v(\prod_i \mathrm{Jac}_{X/H_i}, \omega(\mathcal{B}_1))}{\prod_v C_v(\prod_j \mathrm{Jac}_{X/H'_j}, f_\Phi^*\omega(\mathcal{B}_1))} \cdot \frac{\prod_i \#Ш_0(\mathrm{Jac}_{X/H_i})[2^\infty]}{\prod_j \#Ш_0(\mathrm{Jac}_{X/H'_j})[2^\infty]} \\ &\overset{\text{Prop. 2.17 \& Lem. 5.13}}{\equiv} \prod_v \lambda_{\Theta,\Phi}(X/K_v) \mod \mathbb{Q}^{\times 2}\end{aligned}$$

where $C_v(A,\omega)$ denotes $C(A,\omega)$ for A/K_v. Adding on, by Theorem 5.3(2)–(3),

$$\frac{Q(f_\Phi)}{Q(f_\Phi^\vee)} \equiv Q(f_\Phi)Q(f_\Phi^\vee) = Q(f_\Phi f_\Phi^\vee) = Q(f_\Phi f_{\Phi^\vee}) = Q(f_{\Phi^\vee\Phi}) \mod \mathbb{Q}^{\times 2}.$$

Putting everything together, we get

$$\begin{aligned}\mathrm{ord}_p \prod_v \lambda_{\Theta,\Phi}(X/K_v) &\equiv \mathrm{ord}_p \det\big(f_{\Phi^\vee\Phi} \mid \mathcal{X}_p\big(\prod_i \mathrm{Jac}_{X/H_i}\big)\big) \\ &\overset{[53,\ \text{Lem. } 4.28]}{\equiv} \mathrm{ord}_p \det\big((\Phi^\vee\Phi)^* \mid \mathcal{X}_p\big(\prod_i \mathrm{Jac}_{X/H_i}\big)\big) \\ &\overset{\text{Cor. } 4.30}{\equiv} \mathrm{ord}_p \mathcal{C}_\Theta(\mathcal{X}_p(\mathrm{Jac}_X)) \mod 2\end{aligned}$$

This completes the proof. □

5.2.2 The local invariant $\tilde{\lambda}_\Theta(X/\mathcal{K})$

Assuming that $\Omega^1(\mathrm{Jac}_X)$ is a self-dual $\mathcal{K}[G]$-representation, we now define a revised version of the local invariant $\lambda_{\Theta,\Phi}$.

Definition 5.15. Let $\mathcal{K}$ be a local field of characteristic 0, $X/\mathcal{K}$ be a curve, G be a finite subgroup of $\mathrm{Aut}_{\mathcal{K}}(X)$ and $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation for X. Fix bases $\mathcal{B}_1$, $\mathcal{B}_2$ for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i})$, $\Omega^1(\prod_j \mathrm{Jac}_{X/H'_j})$. Assuming that $\Omega^1(\mathrm{Jac}_X)$ is self-dual as a $\mathcal{K}[G]$-representation, we define

$$\tilde{\lambda}_\Theta(X/\mathcal{K}) = \frac{\lambda_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(X/\mathcal{K})}{\left|\sqrt{\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(\Omega^1(\mathrm{Jac}_X))}\right|_{\mathcal{K}}},$$

where $\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}$ is the regulator constant evaluated with respect to $\mathcal{B}_1$, $\mathcal{B}_2$ as in Definition 4.9.

Remark 5.16. By Theorem 3.9(6), any pseudo Brauer relation Θ for X is also a pseudo Brauer relation relative to $\Omega^1(\mathrm{Jac}_X)$. Thus, $\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(\Omega^1(\mathrm{Jac}_X))$ is well-defined.

Lemma 5.17. *Suppose that $\Omega^1(\mathrm{Jac}_X)$ is a self-dual $\mathcal{K}[G]$-representation.*

1. *$\tilde{\lambda}_\Theta(X/\mathcal{K})$ is independent of the bases $\mathcal{B}_1$, $\mathcal{B}_2$.*
2. *$\tilde{\lambda}_\Theta(X/\mathcal{K})$ is independent of how Θ is expressed as a formal linear combination of conjugacy classes of subgroups of G. That is, for all subgroups H of G,*
$$\tilde{\lambda}_\Theta(X/\mathcal{K}) = \tilde{\lambda}_{\Theta+(H-H)}(X/\mathcal{K}).$$
3. *Given pseudo Brauer relations Θ_1, Θ_2 for X,*
$$\tilde{\lambda}_{\Theta_1+\Theta_2}(X/\mathcal{K}) = \tilde{\lambda}_{\Theta_1}(X/\mathcal{K})\tilde{\lambda}_{\Theta_2}(X/\mathcal{K}).$$
4. *For every G-map Φ realising Θ,*
$$\tilde{\lambda}_\Theta(X/\mathcal{K}) = \frac{\#\mathrm{coker} f_\Phi(\mathcal{K})}{\#\ker f_\Phi(\mathcal{K})} \cdot \frac{\prod_i \mu(X/H_i)}{\prod_j \mu(X/H'_j)} \cdot \left|\sqrt{\deg(f_\Phi)}\right|_{\mathcal{K}}.$$

Proof. (1) holds since, using Notation 4.28,

$$\frac{\lambda_\Theta^{\tilde{\mathcal{B}}_1,\tilde{\mathcal{B}}_2}(X/\mathcal{K})}{\lambda_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(X/\mathcal{K})} = \frac{|\det\left([\mathrm{Id}]_{\tilde{\mathcal{B}}_1}^{\mathcal{B}_1}\right)|_{\mathcal{K}}}{|\det\left([\mathrm{Id}]_{\tilde{\mathcal{B}}_2}^{\mathcal{B}_2}\right)|_{\mathcal{K}}} \quad \text{and} \quad \frac{\mathcal{C}_\Theta^{\tilde{\mathcal{B}}_1,\tilde{\mathcal{B}}_2}(\Omega^1(\mathrm{Jac}_X))}{\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(\Omega^1(\mathrm{Jac}_X))} = \frac{\det\left([\mathrm{Id}]_{\tilde{\mathcal{B}}_1}^{\mathcal{B}_1}\right)^2}{\det\left([\mathrm{Id}]_{\tilde{\mathcal{B}}_2}^{\mathcal{B}_2}\right)^2}.$$

For (2), given a basis $\mathcal{B}_H$ for $\Omega^1(\mathrm{Jac}_{X/H})$, we write $\mathcal{B}'_1 = \mathcal{B}_1 \sqcup \mathcal{B}_H$ for the corresponding basis for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i} \times \mathrm{Jac}_{X/H})$. Similarly, we write $\mathcal{B}'_2 = \mathcal{B}_2 \sqcup \mathcal{B}_H$. Evaluating $\tilde{\lambda}_{\Theta+(H-H)}(X/\mathcal{K})$ with respect to $\mathcal{B}'_1$, $\mathcal{B}'_2$ and $\tilde{\lambda}_\Theta(X/\mathcal{K})$ with respect to $\mathcal{B}_1$, $\mathcal{B}_2$, gives the desired equality, which holds for any choice of bases by (1). (3) follows in the same way as (2). (4) follows from part (1), Lemma 5.13 and Proposition 5.6(1). □

Theorem 5.18. *With the same set up as in Theorem 5.14, and supposing that* $\Omega^1(\mathrm{Jac}_X)$ *is a self-dual* $K[G]$*-representation, we have*

$$\mathrm{ord}_p\mathcal{C}_\Theta(\mathcal{X}_p(\mathrm{Jac}_X)) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_p\tilde{\lambda}_\Theta(X/K_v) \mod 2\mathbb{Z},$$

where we extend ord_p *to* $\mathbb{Q}(\sqrt{p})$ *so that* $\mathrm{ord}_p\tilde{\lambda}_\Theta(X/K_v) \in \frac{1}{2}\mathbb{Z}$.

Proof. Let Φ be any G-map realising Θ. By Lemma 5.17(4), $\tilde{\lambda}_\Theta(X/K_v) = \lambda_{\Theta,\Phi}(X/\mathcal{K}) \cdot |\deg(f_\Phi)|_v^{1/2}$ for all v independently of Φ. Since $\prod_v |\deg(f_\Phi)|_v = 1$, we deduce that

$$\mathrm{ord}_p \prod_v \tilde{\lambda}_\Theta(X/K_v) = \mathrm{ord}_p \prod_v \lambda_{\Theta,\Phi}(X/K_v) \overset{\text{Thm. 5.14}}{\equiv} \mathrm{ord}_p\mathcal{C}_\Theta(\mathcal{X}_p(\mathrm{Jac}_X)) \mod 2.$$

□

Although $\tilde{\lambda}_\Theta(X/\mathcal{K})$ is independent of the underlying bases of differentials, it is difficult to work with in practice since it may not be rational.

5.2.3 The invariant $\Lambda_\Theta(X/\mathcal{K})$ and a local formula

Here we detail how Λ_Θ is obtained from the local invariant $\tilde{\lambda}_\Theta(X/\mathcal{K})$ introduced in Definition 5.15. This involves introducing a correction term which we will denote by $\mathcal{C}_\Theta^{\mathrm{sf}}$. We show that Λ_Θ is rational and conclude the section by proving Theorem 5.7.

Definition 5.19. Let L be a field of characteristic 0, X/L be a curve, G be a finite subgroup of $\mathrm{Aut}_L(X)$ and Θ be a pseudo Brauer relation for X realised by a G-map Φ. Assuming that $\Omega^1(\mathrm{Jac}_X)$ is self-dual as an $L[G]$-representation, we define $\mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_X))$ to be the square-free integer equivalent to $\deg(f_\Phi)$ mod $\mathbb{Q}^{\times 2}$. This is independent of Φ by Proposition 5.6(3).

Example 5.20. We revisit $f_\psi : \mathrm{Jac}_X \to \mathrm{Jac}_{Y_1} \times \mathrm{Jac}_{Y_2}$ from Example 5.5. A direct computation shows that $f_\psi^\vee f_\psi = [2]_{\mathrm{Jac}_X}$, from which we deduce that

$\deg(f_\psi) = 2^g$ where $g = \dim(\mathrm{Jac}_X)$. In this case, it follows that

$$\mathcal{C}^{\mathrm{sf}}_\Psi(\Omega^1(\mathrm{Jac}_X)) = \begin{cases} 2, & \text{if } g \text{ is odd,} \\ 1, & \text{if } g \text{ is even.} \end{cases}$$

When the G-representation $\Omega^1(\mathrm{Jac}_X)$ is realisable over $\mathbb{Q}$, we view $\mathcal{C}_\Theta(\Omega^1(\mathrm{Jac}_X))$ as an element of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ via Remark 4.15.

Lemma 5.21. *Suppose that $\Omega^1(\mathrm{Jac}_X)$ is realisable over $\mathbb{Q}$. Then,*

$$\mathcal{C}^{\mathrm{sf}}_\Theta(\Omega^1(\mathrm{Jac}_X)) \equiv \mathcal{C}_\Theta(\Omega^1(\mathrm{Jac}_X)) \bmod \mathbb{Q}^{\times 2}.$$

Proof. Let Φ be any G-map realising Θ. Then, up to rational squares, we have

$$\mathcal{C}^{\mathrm{sf}}_\Theta(\Omega^1(\mathrm{Jac}_X)) \equiv \deg(f_\Phi) \overset{\text{Prop. } 5.6(2)}{\equiv} \mathcal{C}^{\mathcal{B},\Phi^\vee\mathcal{B}}_\Theta(\Omega^1(\mathrm{Jac}_X)) \overset{\text{Thm. } 4.14(1)}{\equiv} \mathcal{C}_\Theta(\Omega^1(\mathrm{Jac}_X)).$$

This completes the proof. □

Remark 5.22. By [53, Lemma 5.10(2)], if $\mathcal{K} = \mathbb{R}$ or if we are considering the base-change of a curve defined over a number field with a real place, then $\Omega^1(\mathrm{Jac}_X)$ is realizable over $\mathbb{Q}$. The same holds if all representations of G are realizable over $\mathbb{Q}$ (e.g., if $G = S_n$ or $G = C_2 \times C_2$). This conclusion also applies if $G = D_p$, the dihedral group of order $2p$, because $\Omega^1(\mathrm{Jac}_X)$ has rational character by [53, Lemma 5.10(2)], and all D_p-representations with rational character are realizable over $\mathbb{Q}$. Consequently, Lemma 5.21 usually suffices for applications.

Example 5.23. We revisit $f_\theta : \mathrm{Jac}_B \to E \times E \times \mathrm{Jac}_D$ from Example 5.4, where $E : y^2 = x^3 + ax + b$ is an elliptic curve. Arguing as in Example 3.2, we deduce that $\Omega^1(\mathrm{Jac}_B) \cong \rho \oplus \epsilon^{\oplus \dim(\mathrm{Jac}_D)}$, where ϵ (sign) and ρ (2-dim) are the non-trivial irreducible representations of S_3. From Example 4.11, we deduce that $\mathcal{C}_\Theta(\Omega^1) = 3^{1+\dim(\mathrm{Jac}_D)}$. As observed in Example 3.3, $\dim(\mathrm{Jac}_D) = 0$ when the Weierstrass coefficient $a = 0$, while Example 2.10 shows that $\dim(\mathrm{Jac}_D) = 1$

when $a \neq 0$. It follows that

$$\mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_B)) = \begin{cases} 1, & \text{if } a \neq 0, \\ 3, & \text{if } a = 0. \end{cases}$$

Definition 5.24. Let $\mathcal{K}$ be a local field of characteristic 0, $X/\mathcal{K}$ be a curve, G be a finite subgroup of $\mathrm{Aut}_{\mathcal{K}}(X)$ and $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation for X. Fix bases $\mathcal{B}_1$, $\mathcal{B}_2$ for $\Omega^1(\prod_i \mathrm{Jac}_{X/H_i})$, $\Omega^1(\prod_j \mathrm{Jac}_{X/H'_j})$ and write $\omega(\mathcal{B}_1)$, $\omega(\mathcal{B}_2)$ for the exterior forms given by the wedge product of the elements in $\mathcal{B}_1$, $\mathcal{B}_2$ respectively. Assuming that $\Omega^1(\mathrm{Jac}_X)$ is self-dual as a $\mathcal{K}[G]$-representation, we define

$$\Lambda_\Theta(X/\mathcal{K}) = \frac{C(\prod_i \mathrm{Jac}_{X/H_i}, \omega(\mathcal{B}_1))}{C(\prod_j \mathrm{Jac}_{X/H'_j}, \omega(\mathcal{B}_2))} \cdot \frac{\prod_i \mu(X/H_i)}{\prod_j \mu(X/H'_j)} \cdot \left| \sqrt{\frac{\mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_X))}{\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}(\Omega^1(\mathrm{Jac}_X))}} \right|_{\mathcal{K}}.$$

For the definitions of C, μ, $\mathcal{C}_\Theta^{\mathcal{B}_1,\mathcal{B}_2}$ and $\mathcal{C}_\Theta^{\mathrm{sf}}$, see Notation 5.11 and Definitions 2.16, 4.9 and 5.19. In particular, $\Lambda_\Theta(X/\mathcal{K}) = \tilde{\lambda}_\Theta(X/\mathcal{K}) \cdot |\mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_X))|_{\mathcal{K}}^{1/2}$.

Theorem 5.25. *Let X be a curve over a local field $\mathcal{K}$ of characteristic 0, and G be a finite subgroup of $\mathrm{Aut}_{\mathcal{K}}(X)$. Let $\Theta = \sum_i H_i - \sum_j H'_j$ be a pseudo Brauer relation for X, and suppose that $\Omega^1(\mathrm{Jac}_X)$ is a self-dual $\mathcal{K}[G]$-representation. Then, the following hold.*

1. *$\Lambda_\Theta(X/\mathcal{K})$ is a rational number independent of $\mathcal{B}_1$, $\mathcal{B}_2$.*

2. *$\Lambda_\Theta(X/\mathcal{K})$ is independent of how Θ is expressed as a formal linear combination of conjugacy classes of subgroups of G. That is, for any subgroup H of G,*
$$\Lambda_\Theta(X/\mathcal{K}) = \Lambda_{\Theta+(H-H)}(X/\mathcal{K}).$$

3. *For any G-map Φ realising Θ,*
$$\Lambda_\Theta(X/\mathcal{K}) = \frac{\#\mathrm{coker} f_\Phi(\mathcal{K})}{\#\ker f_\Phi(\mathcal{K})} \cdot \frac{\prod_i \mu(X/H_i)}{\prod_j \mu(X/H'_j)} \cdot \left| \sqrt{\deg(f_\Phi) \cdot \mathcal{C}_\Theta^{\mathrm{sf}}(\Omega^1(\mathrm{Jac}_X))} \right|_{\mathcal{K}}.$$

4. If $\mathcal{K} = \mathbb{C}$, then $\Lambda_\Theta(X/\mathbb{C}) = \mathcal{C}^{\mathrm{sf}}_\Theta(\Omega^1(\mathrm{Jac}_X))$.

Proof. Independence of the bases $\mathcal{B}_1$, $\mathcal{B}_2$ follows from Lemma 5.17(1). (2) follows from Lemma 5.17(2), provided we show that $\mathcal{C}^{\mathrm{sf}}_\Theta = \mathcal{C}^{\mathrm{sf}}_{\Theta'}$ where $\Theta' = \Theta + (H - H)$. Let Φ be any G-map realising Θ, and consider $\Phi' := \Phi \oplus \mathrm{id}$, where id is the identity on $\mathbb{Z}[G/H]$. Then, Φ' realises Θ' and $f_{\Phi'} = f_\Phi \times \mathrm{id}|_{\mathrm{Jac}_{X/H}}$. Therefore, $\mathcal{C}^{\mathrm{sf}}_{\Theta'} \equiv \deg(f_{\Phi'}) = \deg(f_\Phi) \equiv \mathcal{C}^{\mathrm{sf}}_\Theta \bmod \mathbb{Q}^{\times 2}$, and so they must be equal. (3) follows from Lemma 5.17(4), and (4) follows from (3) since $\mathrm{coker} f_\Phi(\mathcal{K})$ is trivial when $\mathcal{K} = \mathbb{C}$. It remains to show that Λ_Θ is rational, to complete the proof of (1). By Proposition 5.6(3), $\deg(f_\Phi) \cdot \mathcal{C}^{\mathrm{sf}}_\Theta \in \mathbb{Q}^{\times 2}$ independently of Φ, and so rationality follows from (3). □

We are now able to prove Theorem 5.7.

Proof of Theorem 5.7. We note that

$$\Lambda_\Theta(X/K_v) = \lambda_{\Theta,\Phi}(X/K_v) \cdot |\deg(f_\Phi) \cdot \mathcal{C}^{\mathrm{sf}}_\Theta(\Omega^1(\mathrm{Jac}_X))|_v^{1/2}.$$

Therefore, $\prod_v \Lambda_\Theta(X/K_v) = \prod_v \lambda_{\Theta,\Phi}(X/K_v)$ since $\deg(f_\Phi) \cdot \mathcal{C}^{\mathrm{sf}}_\Theta \in \mathbb{Q}^{\times 2}$. By Theorem 5.25(1), $\mathrm{ord}_p \prod_v \Lambda_\Theta(X/K_v) = \sum_v \mathrm{ord}_p \Lambda_\Theta(X/K_v)$ and the result then follows by Theorem 5.14. The second assertion follows from Lemma 4.19. □

Unfortunately, one drawback of the invariant Λ_Θ is that it is generally not multiplicative in Θ (unlike $\tilde{\lambda}_\Theta$, see Lemma 5.17(3)). This is the case since generally $\mathcal{C}^{\mathrm{sf}}_{\Theta_1+\Theta_2} \neq \mathcal{C}^{\mathrm{sf}}_{\Theta_1} \cdot \mathcal{C}^{\mathrm{sf}}_{\Theta_2}$.

Lemma 5.26. *Let $\Theta, \Theta_1, \Theta_2$ be pseudo Brauer relations for X. Then,*

1. $\dfrac{\Lambda_{\Theta_1+\Theta_2}(X/\mathcal{K})}{\Lambda_{\Theta_1}(X/\mathcal{K})\Lambda_{\Theta_2}(X/\mathcal{K})} = \left| \sqrt{\dfrac{\mathcal{C}^{\mathrm{sf}}_{\Theta_1+\Theta_2}(\Omega^1(\mathrm{Jac}_X))}{\mathcal{C}^{\mathrm{sf}}_{\Theta_1}(\Omega^1(\mathrm{Jac}_X))\mathcal{C}^{\mathrm{sf}}_{\Theta_2}(\Omega^1(\mathrm{Jac}_X))}} \right|_{\mathcal{K}}$,
2. $\Lambda_\Theta(X/\mathcal{K})\Lambda_{-\Theta}(X/\mathcal{K}) = |\mathcal{C}^{\mathrm{sf}}_\Theta(\Omega^1(\mathrm{Jac}_X))|_{\mathcal{K}}$.

Proof. (1) follows from Lemma 5.17(3). For (2), let Ψ be the trivial pseudo Brauer relation (i.e. one of the form $\sum_i H_i - \sum_i H_i$). Then, $\Lambda_\Psi(X/\mathcal{K}) =$

$\mathcal{C}^{\mathrm{sf}}_{\Psi}(\Omega^1(\mathrm{Jac}_X)) = 1$. By part (1), we get

$$\Lambda_\Theta(X/\mathcal{K})\Lambda_{-\Theta}(X/\mathcal{K}) = \left|\sqrt{\mathcal{C}^{\mathrm{sf}}_{\Theta}(\Omega^1(\mathrm{Jac}_X))\mathcal{C}^{\mathrm{sf}}_{-\Theta}(\Omega^1(\mathrm{Jac}_X))}\right|_{\mathcal{K}}.$$

Let Φ be any G-map realising Θ. Then $\Phi^\vee$ realises $-\Theta$ and $\mathcal{C}^{\mathrm{sf}}_{\Theta} \equiv \deg(f_\Phi) = \deg(f^\vee_\Phi) \overset{\text{Thm. } 5.3(3)}{=} \deg(f_{\Phi^\vee}) \equiv \mathcal{C}^{\mathrm{sf}}_{-\Theta} \bmod \mathbb{Q}^{\times 2}$. Since $\mathcal{C}^{\mathrm{sf}}_{\Theta}$ and $\mathcal{C}^{\mathrm{sf}}_{-\Theta}$ are square-free integers, they must be equal. □

The following lemma provides a simplification of $\Lambda_\Theta(X/\mathcal{K})$ when $\mathcal{K}$ is non-archimedean.

Lemma 5.27. *Let $\mathcal{K}$ be a non-archimedean local field of characteristic 0. Let $\mathcal{J}_H$ be the Néron model of $\mathrm{Jac}_{X/H}$ over $\mathcal{O}_\mathcal{K}$ and let $\mathcal{B}(\mathcal{J}_H)$ be a basis for the $\mathcal{O}_\mathcal{K}$-module $\Omega^1(\mathcal{J}_H)$. Letting $\mathcal{N}_1 = \bigsqcup_i \mathcal{B}(\mathcal{J}_{H_i})$ and $\mathcal{N}_2 = \bigsqcup_j \mathcal{B}(\mathcal{J}_{H'_j})$,*

$$\Lambda_\Theta(X/\mathcal{K}) = \frac{\prod_i c(\mathrm{Jac}_{X/H_i}) \cdot \mu(X/H_i)}{\prod_j c(\mathrm{Jac}_{X/H'_j}) \cdot \mu(X/H'_j)} \cdot \left|\sqrt{\frac{\mathcal{C}^{\mathrm{sf}}_{\Theta}(\Omega^1(\mathrm{Jac}_X))}{\mathcal{C}^{\mathcal{N}_1,\mathcal{N}_2}_{\Theta}(\Omega^1(\mathrm{Jac}_X))}}\right|_{\mathcal{K}}.$$

Proof. For a Néron basis $\mathcal{B}(\mathcal{J}_H)$, the exterior form $\omega(\mathcal{B}(\mathcal{J}_H))$ on $\mathrm{Jac}_{X/H}$ coincides with the exterior form on the Néron model of $\mathcal{J}_H$ over $\mathcal{O}_\mathcal{K}$. □

Chapter 6

Applications of pseudo Brauer relations

In the following chapter, we illustrate applications of pseudo Brauer relations and their regulator constants introduced in Chapter 5. Our focus will be on isogenies between Jacobians and local formulae for Selmer rank parities.

6.1 Uniform approach: isogenies and parity

Let X be a curve over a characteristic 0 field K and G a finite subgroup of $\mathrm{Aut}_K(X)$. By Theorem 5.3, we can associate to a pseudo Brauer relation $\Theta = \sum_i H_i - \sum_j H'_j$ for X an isogeny

$$\prod_i \mathrm{Jac}_{X/H_i} \to \prod_j \mathrm{Jac}_{X/H'_j}.$$

This provides the means for deducing if two Jacobians are isogenous. We will call isogenies obtained in this way *pseudo Brauer verifiable* formally defined as follows.

Definition 6.1. We say that a pseudo Brauer relation $\Theta = \sum_{i=1}^m H_i - \sum_{j=1}^r H'_j$ for X *verifies an isogeny* $A \to B$ if there exist isomorphisms $A \cong \prod_{i=1}^m \mathrm{Jac}_{X/H_i}$ and $B \cong \prod_{j=1}^r \mathrm{Jac}_{X/H'_j}$ as abelian varieties over K. In addition, we say that an isogeny $A \to B$ is *pseudo Brauer verifiable* if we can find a curve and a pseudo Brauer relation Θ for it verifying this isogeny.

In Examples 1.14–1.15, we showed that certain isogenies between elliptic curves and between the Jacobian of a genus 2 curve and a product of two elliptic curves are pseudo Brauer verifiable. The following examples include previously discussed instances of pseudo Brauer verifiable isogenies from the literature.

Example 6.2 (Fermat Curves, cf. [46, §5])**.** Let X_m be the Fermat curve with affine model $x^m + y^m = 1$. Let K be any field of characteristic 0 containing ζ_p where $p|m$. Then $C_p \times C_p$ acts on X_m via $\sigma(x, y) = (\zeta_p x, y)$ and $\tau(x, y) = (x, \zeta_p y)$. Let $\{C_p^i\}_{i=0}^p$ denote all proper subgroups of $C_p \times C_p$, and write $X_i{}'$ to denote the (normalisation of) the curve with affine model $y_i^m = x_i^{im/p}(1-x_i^{m/p})$. Then, the Brauer relation $\{e\} + p(C_p \times C_p) - \sum_{i=0}^p C_p^i$ for X_m verifies an isogeny $\mathrm{Jac}_{X_m} \times \mathrm{Jac}^p_{X_{m/p}} \to \prod_{i=0}^p \mathrm{Jac}_{X_i'}$.

Example 6.3 (Modular Jacobians, cf. [21])**.** Let S be the subgroup of scalar matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ and write X_S to denote the quotient of $X(p)/\mathbb{Q}$, the classical modular curve classifying elliptic curves with full level p structure, by S. Then, X_S is endowed with a $\mathrm{PGL}_2(\mathbb{F}_p)$-action. The main result in [21] shows that the isogeny $\mathrm{Jac}_{X^+_{\mathrm{sp}}(p)} \to \mathrm{Jac}_{X_0(p)} \times \mathrm{Jac}_{X^+_{\mathrm{nsp}}(p)}$ between certain modular Jacobians can be deduced from a Brauer relation for X_S. As a result, this isogeny is pseudo Brauer verifiable.

6.1.1 Isogenies from pseudo Brauer relations

In what follows, we show that the above formalism provides a powerful tool for revisiting and constructing a wide range of classical isogenies. In particular, we show that each of the following isogenies can be obtained by applying Theorem 5.3 to suitable pseudo Brauer relations.

Theorem 6.4 (Propositions 6.8(1), 6.11(1), 6.15(1), 6.17(1), 6.25(1), 6.27(1))**.** *Let K be a field of characteristic 0. Each of the following isogenies $A \to A'$ are pseudo Brauer verifiable.*

1. *$A = \mathrm{Res}_K^{K(\sqrt{d})}\mathrm{Jac}_Y$ and $A' = \mathrm{Jac}_Y \times \mathrm{Jac}_{Y^d}$ for Y/K a hyperelliptic curve and Y^d its quadratic twist by $d \in K^\times$,*

2. *A is the Jacobian of a genus 2 curve with* $\mathrm{Gal}(K(A[2])/K)$ *a 2-group, while A' is the target of a Richelot isogeny,*

3. $A = \mathrm{Jac}_Z \times \mathrm{Jac}_Y$ *and* $A' = \mathrm{Jac}_{\tilde{Z}}$*, where $\tilde{Z}$ admits an unramified double cover $\tilde{Z} \to Z$, Z is a trigonal curve and the Jacobian of Y is the associated prym variety* $\mathrm{Prym}(\tilde{Z}/Z)$,

4. *A and A' are elliptic curves with a cyclic isogeny of prime degree p,*

5. $A = \mathrm{Jac}_Y$ *for Y a genus 2 curve with a generic*[1] *cover $Y \to E$ to an elliptic curve E of prime degree p and $A' = E \times \tilde{E}$ is a product of two elliptic curves,*

6. $A = \prod_i \mathrm{Res}_K^{F^{H_i}} \mathrm{Jac}_Y$ *and* $A' = \prod_j \mathrm{Res}_K^{F^{H'_j}} \mathrm{Jac}_Y$ *for Y a geometrically connected curve defined over K and* $\Theta = \sum_i H_i - \sum_j H'_j$ *a Brauer relation for* $G = \mathrm{Gal}(F/K)$.

Remark 6.5. The pseudo Brauer relation Θ and the automorphism group G we use to verify the isogenies in Theorem 6.4 are as follows. For details on the curve X and the action of G, refer the relevant theorem in the table.

Case	G	Θ	Proposition
(1)	$C_2 \times C_2$	$\{e\} + 2(C_2 \times C_2) - C_2^a - C_2^b - C_2^c$	6.8(1)
(2)	D_4	$C_2^a - C_2^b + (C_2^2)^b - (C_2^2)^a$	6.11(1)
(3)	S_4	$C_2^2 - D_4 - S_3 + S_4$	6.15(1)
(4)	$C_p \rtimes C_m$	$C_m - (C_p \rtimes C_m)$	6.17(1)
(5)	$S_p \times C_2$	$(S_{p-1} \times \{e\}) - (S_p \times \{e\}) - (S_{p-2} \times C_2)$	6.25(1)
(6)	$\mathrm{Gal}(F/K)$	$\sum_i H_i - \sum_j H'_j$	6.27(1)

6.1.2 Local formulae from regulator constants

Isogenies have been widely used to derive formulae for the parities of various ranks in terms of local data, including those from Theorem 6.4. For a more detailed discussion of the relevant literature, see §1.6.3. The next results shows that all these can be derived uniformly using regulator constants.

[1] see Definition 6.19

Theorem 6.6 (Propositions 6.8(2), 6.11(2), 6.15(2), 6.17(2), 6.25(2), 6.27(2))**.** *Let A/K be as in Theorem 6.4, and suppose that K is a number field. For $p = 2$ in cases (1)–(3) and for p as in Theorem 6.4 in cases (4)–(5), we have*

$$\mathrm{rk}_p(A) = \sum_{v \text{ place of } K} \mathrm{ord}_p\ \Lambda_\Theta(X/K_v) \mod 2,$$

where $\Lambda_\Theta(X/K_v)$ is the local invariant of Definition 5.24.

In addition, in case (6) and for p an arbitrary prime,

$$\sum_{\tau \in S_{\Theta,p}} \frac{\langle \tau, \mathcal{X}_p(\mathrm{Res}^F_K \mathrm{Jac}_Y)\rangle}{\langle \tau, \tau\rangle} = \sum_{v \text{ place of } K} \mathrm{ord}_p \Lambda_\Theta(Y_{F/K}/K_v) \mod 2,$$

where $S_{\Theta,p}$ is as in Definition 4.18 (considered with $\mathcal{V} = \mathbb{Q}[\mathrm{Gal}(F/K)]$).

6.2 Hyperelliptic curves over $K(\sqrt{d})$

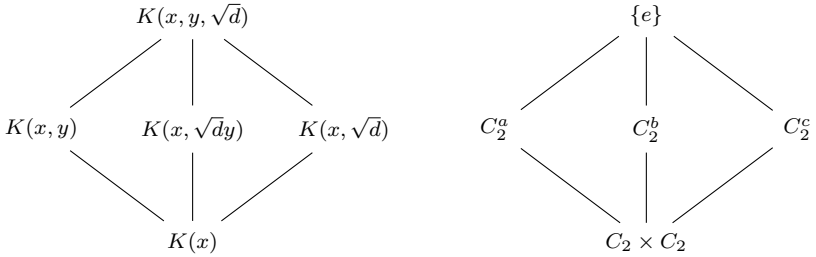
In this section, we let Y/K be a hyperelliptic curve, and write $L = K(\sqrt{d})$ be a quadratic extension. We consider the isogeny

$$\mathrm{Res}^L_K \mathrm{Jac}_Y \to \mathrm{Jac}_Y \times \mathrm{Jac}_{Y^d},$$

where Y^d is the quadratic twist of Y by d. We write Y_L for the base change of Y to L and $Y_{L/K}$ for the corresponding curve over K as in Notation 2.5.

Lemma 6.7. *Let Y/K be a hyperelliptic curve with affine model $y^2 = f(x)$, and let $L = K(\sqrt{d})$ be a quadratic extension of K. Then, the following hold.*

1. *$C_2 \times C_2$ acts on the function field $L(Y)$. This action fits into the following Galois diagram with the corresponding subgroups on the right.*



2. *$C_2 \times C_2$ acts on $Y_{L/K}$ via K-automorphisms.*

3. *The quotients satisfy $Y_{L/K}/C_2^a \cong Y$ and $Y_{L/K}/C_2^b \cong Y^d$.*

Proof. The proof of (1) is given in Example 2.8. For (2), we note that $C_2 \times C_2$ acts on $K(x, y, \sqrt{d})$ via K-automorphisms by part (1). Theorem 2.2 gives a $C_2 \times C_2$-action on $Y_{L/K}$ completing the proof. For (3), we note that $K(x, y)$, $K(x, \sqrt{d}y)$ are the function fields of Y and Y^d respectively. The result follows by the function field isomorphism $K(X/H) \cong K(X)^H$, see [53, Remark 4.2]. □

Proposition 6.8. *Let Y/K be a hyperelliptic curve and L/K a quadratic extension.*

1. *$\{e\} - C_2^a - C_2^b + 2(C_2 \times C_2) - C_2^c$ is a pseudo Brauer relation for $Y_{L/K}$ that verifies an isogeny $\mathrm{Res}_K^L \mathrm{Jac}_Y \to \mathrm{Jac}_Y \times \mathrm{Jac}_{Y^d}$.*

2. *If K is a number field,*

$$\mathrm{rk}_2(\mathrm{Jac}_Y/L) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2\ \Lambda_\Theta(Y_{L/K}/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. Since Θ is a Brauer relation for $C_2 \times C_2$, then it's a pseudo Brauer relation for $Y_{L/K}$. The Jacobians of the curves corresponding to the function fields $K(x)$ and $K(x, \sqrt{d})$ are trivial (for the latter use Lemma 2.12).

Therefore, Θ induces an isogeny $\mathrm{Jac}_{Y_{L/K}} \to \mathrm{Jac}_{Y/K} \times \mathrm{Jac}_{Y^d/K}$. By Lemma 2.12, $\mathrm{Jac}_{Y_{L/K}} \cong \mathrm{Res}_K^L \mathrm{Jac}_Y$ completing the proof of (1). For (2), we let $\epsilon_a, \epsilon_b : C_2 \times C_2 \to \{\pm 1\}$ be the non-trivial, irreducible representations satisfying $\epsilon_a(C_2^a) = 1$ and $\epsilon_b(C_2^b) = 1$. As in Example 1.10, $\mathcal{X}_2(\mathrm{Jac}_X) \cong \epsilon_a^{\oplus \mathrm{rk}_2 \mathrm{Jac}_Y} \oplus \epsilon_b^{\oplus \mathrm{rk}_2 \mathrm{Jac}_{Y^d}}$. Using Example 4.12, we deduce that $S_{\Theta,2} = \{\epsilon_a, \epsilon_b\}$. By applying Theorem 5.7 to this Θ with $p = 2$, we get the required result. □

6.3 Richelot Isogeny

In this section, we consider Jacobians of genus 2 curves admitting a *Richelot isogeny*. For a detailed discussion on these isogenies, we refer the reader to [9, 82].

Let $C : y^2 = F(x)$ be a genus two curve where F is a degree 6 polynomial. The existence of a Richelot isogeny can be determined by the Galois group of $F(x)$. In particular, if $\mathrm{Gal}(F) \subseteq C_2^3 \rtimes S_3$, then Jac_C admits a Richelot isogeny (assuming the non-vanishing of a constant δ $(\star)$). In what follows, we focus on the case where the $\mathrm{Gal}(F)$ is a subgroup of $D_4 \times C_2 \subseteq C_2^3 \rtimes S_3$. Following [33], we refer to these curves as *C2D4 curves*.

Definition 6.9 (cf. [33, Definition 1.6])**.** Let C/K be a genus 2 curve with an affine model $y^2 = cf(x)$, where $c \in K^\times$ and f a degree 6 and monic polynomial. We say that C is a *C2D4 curve* if $\mathrm{Gal}(f) \subseteq D_4 \times C_2$ as a permutation group on 6 roots, in which case the two factors D_4 and C_2 act separately on 4 and 2 roots respectively.

The Galois group specifies a factorisation $f(x) = f_1(x)f_2(x)f_3(x)$ into three coprime monic quadratics. We can assume $f_3 \in K[x]$ and that $\{f_1, f_2\}$ is invariant under $\mathrm{Gal}(\overline{K}/K)$. Since $(x, y) \to (x, cy)$ gives an isomorphism $C \to \{y^2 = c^3 f(x)\}$, we can also suppose $c = q^3$. This allows us to distribute the constant term so that $cf(x) = F_1(x)F_2(x)F_3(x)$ with $F_i(x) = qf_i(x)$.

Let $\{w_1, w_2\}, \{w_3, w_4\}, \{w_5, w_6\}$ be the roots of F_1, F_2, F_3 respectively. The factorisation $cf(x) = F_1(x)F_2(x)F_3(x)$ specifies a subgroup $\{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$ in $\mathrm{Jac}_C[2]$. The target of the isogeny determined by this subgroup depends on the vanishing of a constant $\delta \in K$ defined as follows. For $i = 1, 2, 3$, we let $F_i(x) = f_{i,0} + f_{i,1}x + qx^2$. Then,

$$\delta := \det \begin{pmatrix} f_{1,0} & f_{1,1} & q \\ f_{2,0} & f_{2,1} & q \\ f_{3,0} & f_{3,1} & q \end{pmatrix} \in K. \qquad (\star)$$

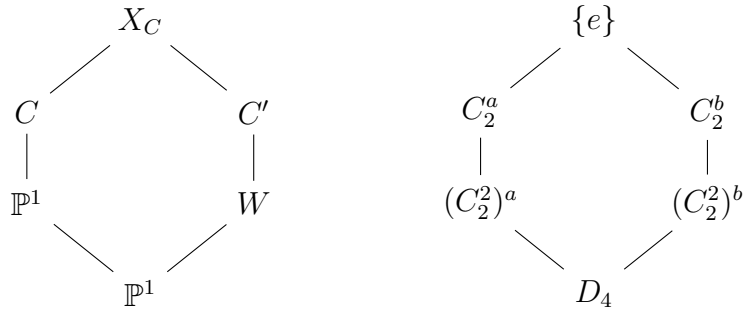
By [9, Lemma 4.2], the condition $\delta \neq 0$ implies that the target of the isogeny is a Jacobian of a genus 2 curve (as opposed to a product of two elliptic curves).

In the following lemma, we write T to denote

$$T = \begin{cases} \frac{f_{1,1}F_1(x) - f_{2,1}F_2(x)}{F_2(x) - F_1(x)}, & \text{if } f_{1,1} \neq f_{2,1}, \\ \frac{f_{1,0}F_1(x) - f_{2,0}F_2(x)}{F_2(x) - F_1(x)}, & \text{if } f_{1,1} = f_{2,1}. \end{cases}$$

It follows that $T \in K(x)$, since $\mathrm{Gal}(\overline{K}/K)$ permutes $F_1 \leftrightarrow F_2$ and the corresponding coefficients, when F_1 and F_2 are not individually defined over K. In addition, we write C_2^a, C_2^b for conjugacy classes of non-normal order 2 subgroups in D_4.

Lemma 6.10. *Let $C/K : y^2 = F_1(x)F_2(x)F_3(x)$ be a C2D4 curve with $\delta \neq 0$. Then, the Galois closure of $C \xrightarrow{2} \mathbb{P}^1 \xrightarrow{2} \mathbb{P}^1$, where the first map is the hyperelliptic cover $(x, y) \mapsto x$ and the second is given by $x \mapsto T$, fits in the following Galois diagram with the corresponding subgroups on the right.*



In addition, W is a curve of genus zero.

Proof. To distinguish between the two $\mathbb{P}^1$'s, we write $\mathbb{P}^1_x$ and $\mathbb{P}^1_T$ to denote $\mathbb{P}^1$ with parameters x and T, respectively. In order to show that the Galois group is D_4 (instead of $C_2 \times C_2$), it suffices to show that the discriminant cover $W \xrightarrow{2} \mathbb{P}^1_T$ ([53, Lemma 2.7], [26, §2.2]) of $C \xrightarrow{2} \mathbb{P}^1_x \xrightarrow{2} \mathbb{P}^1_T$ is non-trivial.

Let $\{w_1, w_2\}, \{w_3, w_4\}, \{w_5, w_6\}$ be the roots of F_1, F_2 and F_3 respectively. Keeping track of ramification, we see that the branch locus of $C \to \mathbb{P}^1_T$ consists of 4 distinct points T_1, T_2, T_3, T_4, where $T_1 = T(w_1) = T(w_2), T_2 = T(w_3) =$

$T(w_4), T_3 = T(w_5)$ and $T_4 = T(w_6)$ (It is clear that $T(w_1) = T(w_2)$ and $T(w_3) = T(w_4)$ and easy to check that $T_1 \neq T_2$. To see that $T_3 \neq T_4$, we note that $T_3 = T_4$ is only possible when $\delta = 0$). By [26, Lemma 2.3], the branch locus of $W \to \mathbb{P}^1_T$ consists of T_3, T_4. Therefore, the Galois group is indeed D_4.

To complete the proof, it suffices to show that $W = X_C/(C_2^2)^b$ is of genus 0. Since $W \xrightarrow{2} \mathbb{P}^1_T$ is branched at 2 points, the result follows. □

Proposition 6.11. *Let $C/K : y^2 = cf(x)$ be a C2D4 curve with $\delta \neq 0$.*

1. *$C_2^a - C_2^b + (C_2^2)^b - (C_2^2)^a$ is a pseudo Brauer relation for X_C that verifies an isogeny $\mathrm{Jac}_C \to \mathrm{Jac}_{C'}$.*

2. *When K is a number field,*

$$\mathrm{rk}_2(\mathrm{Jac}_C/K) = \sum_{v \text{ place of } K} \mathrm{ord}_2\ \Lambda_\Theta(X_C/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. $\Theta = C_2^a - C_2^b + (C_2^2)^b - (C_2^2)^a$ is a Brauer relation for D_4. Part (1) follows by Lemma 6.10. We let ϵ be the non-trivial 1-dimensional representation of D_4 lifted from the quotient $D_4/C_4 \cong C_2$. By applying the Galois descent result of Theorem 3.1(2), we deduce that

$$\mathcal{X}_2(\mathrm{Jac}_{X_C}) \quad \text{and} \quad \epsilon^{\oplus a} \oplus \rho^{\oplus \mathrm{rk}_2 \mathrm{Jac}_C}$$

where ρ is the irreducible D_4-representation of dimension 2 and $a \in \mathbb{N}$. By Lemma 4.16, $\mathcal{C}_\Theta(\epsilon) = 1$. It's also easy to show that $\mathcal{C}_\Theta(\rho) = 2$. Therefore, $S_{\Theta,2} = \{\rho\}$. Part 2 follows by applying Theorem 5.7 to this Θ with $p = 2$. □

Remark 6.12. We note that the isogeny $\phi : \mathrm{Jac}_C \to \mathrm{Jac}_{C'}$ considered in Proposition 6.11(1) is given by the pullback of $X_C \xrightarrow{2} C$ followed by the push-forward $X_C \xrightarrow{2} C'$. It follows that ϕ satisfies $\phi^\vee \phi = [2]$, and its kernel is given by $\{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$. By [9, Proposition 4.3], the target of this isogeny is $\mathrm{Jac}_{\tilde{C}_d}$, where $\tilde{C}_d$ is a genus 2 curve constructed from the quadratic factors F_1, F_2, F_3; see [9, Eqn. (4.5)] for details.

6.4 Prym varieties of trigonal curves

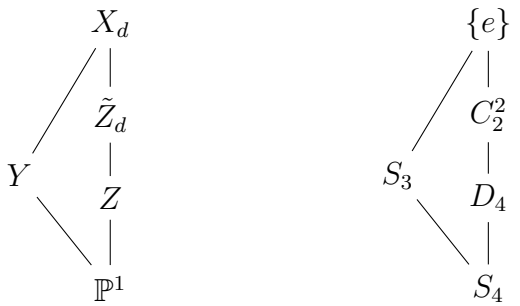
We let $\pi : \tilde{Z} \to Z$ be an unramified double cover of geometrically connected curves over K. The *Prym variety* denoted $\mathrm{Prym}(\tilde{Z}/Z)$ of π is the abelian variety given by the connected component of $\mathrm{Ker}(\pi_*)$ containing the identity. The C_2 action on $\tilde{Z}$ allows us to decompose $\mathrm{Jac}_{\tilde{Z}}$ into its isotypic components which gives an isogeny

$$\mathrm{Jac}(\tilde{Z}) \to \mathrm{Jac}(Z) \times \mathrm{Prym}(\tilde{Z}/Z).$$

In general, $\mathrm{Prym}(\tilde{Z}/Z)$ is not necessarily a Jacobian, but it is principally polarised. The trigonal construction [26, §2.4] shows that when Z is a trigonal curve over an algebraically closed field, the Prym variety is the Jacobian of a tetragonal curve; a generalization for non-algebraically closed fields [11, §2.2] shows the Prym is a Jacobian after considering a twist of the cover $\pi : \tilde{Z} \to Z$.

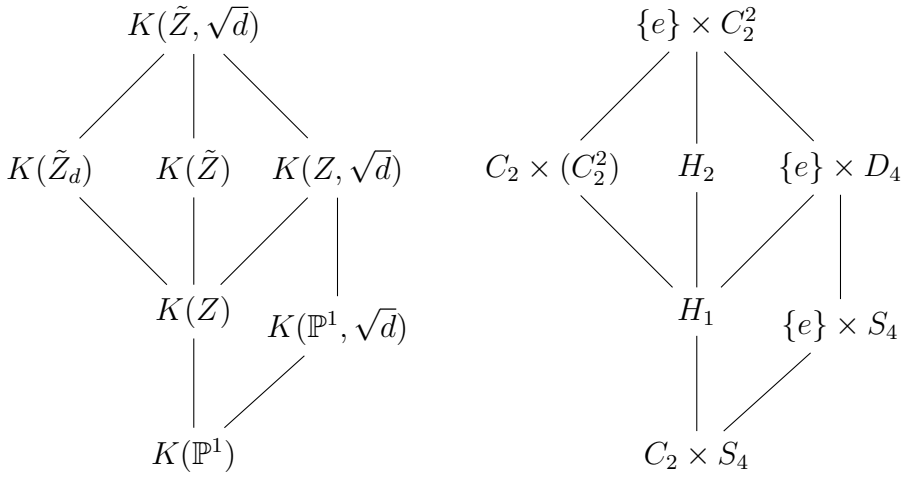
Definition 6.13 (cf. [11, Def. 2.2])**.** Let $\pi : \tilde{Z} \to Z$ be a degree 2 cover. We say that $\pi_d : \tilde{Z}_d \to Z$ is a quadratic twist of π by $d \in K^\times$ if there exists an isomorphism $\psi : \tilde{Z}_d \xrightarrow{\sim} \tilde{Z}$ defined over $K(\sqrt{d})$ such that $\pi_d = \pi \circ \psi$.

Lemma 6.14. *Let $\tilde{Z} \to Z$ be an unramified double cover of a trigonal curve Z. Then, there exists $d \in K^\times$ such that the Galois closure, say $X_d \to \mathbb{P}^1$, of $\tilde{Z}_d \xrightarrow{2} Z \xrightarrow{3} \mathbb{P}^1$ is an S_4-Galois cover. With this choice of $d \in K^\times$, we have the following Galois cover with the corresponding subgroups on the right.*



Here $D_4 = \langle (1,2), (1324) \rangle$ and $C_2^2 = \langle (1,2), (3,4) \rangle$.

Proof. This claim is essentially given in [11, §2.2], as we now explain. Let $X \to \mathbb{P}^1$ be the Galois closure of $\tilde{Z} \xrightarrow{2} Z \xrightarrow{3} \mathbb{P}^1$. As detailed therein, X need not be geometrically connected in which case its geometric components are defined over a quadratic extension $K(\sqrt{d})$. Then, the Galois group of $X \to \mathbb{P}^1$ is $C_2^3 \rtimes S_3 \cong C_2 \times S_4$ (viewed as the group of permutations of $\{x_i^{\pm}\}_{1 \leq i \leq 3}$ which preserve the pairs $\{x_i^+, x_i^-\}$). Since X is not geometrically connected, then the field of $\{e\} \times S_4$-invariant functions in its function field is $K(\mathbb{P}^1, \sqrt{d})$. By construction, we get the following function field extension, with the corresponding lattice of subgroups of $C_2 \times S_4$:



In this diagram, H_1 and H_2 are determined, up to conjugacy, by the subgroups of $C_2^3 \rtimes S_3 \cong C_2 \times S_4$ stabilising $\{x_1^+, x_1^-\}$ and $\{x_1^+\}$, respectively. It follows that $H_1 \cong C_2 \times D_4$ and $H_2 \cong D_4$. By considering the quotient of X by the subgroup $C_2 \times \{e\} \subseteq C_2 \times S_4$, we obtain an S_4-Galois cover, denoted $X_d \to \mathbb{P}^1$. By construction, this is the Galois closure of $\tilde{Z}_d \to Z \to \mathbb{P}^1$, which gives the required result.

If, on the other hand, $X \to \mathbb{P}^1$ is a cover of geometrically connected curves, then after base change to an algebraic closure, we can assume K is algebraically closed. Then, the required result follows from [26, pp. 73]. In this case, we can take $d = 1$. □

Proposition 6.15. *Let $\tilde{Z} \to Z$ be an unramified double cover of geometrically*

connected curves, and suppose that Z admits a degree 3 cover $Z \xrightarrow{3} \mathbb{P}^1$. Let $d \in K^\times$ be as in Lemma 6.14. Then, the following hold.

1. *$C_2^2 - D_4 - S_3 + S_4$ is a pseudo Brauer relation for X_d that verifies an isogeny $\mathrm{Jac}_{\tilde{Z}_d} \to \mathrm{Jac}_Z \times \mathrm{Prym}(\tilde{Z}_d/Z)$.*

2. *If K is a number field,*

$$\mathrm{rk}_2(\mathrm{Jac}_{\tilde{Z}_d}/K) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2\ \Lambda_\Theta(X_d/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. Since Θ is a Brauer relation for the group S_4, it's also a pseudo Brauer relation for X_d. By Lemma 6.14, $X_d/D_4 = Z, X_d/C_2^2 = \tilde{Z}_d$, while [11, Proposition 2.4] asserts that the Jacobian of $Y = X_d/S_3$ is isomorphic to $\mathrm{Prym}(\tilde{Z}_d/Z)$. This proves (1).

For (2), write σ for the standard 3-dimensional irreducible representation of S_4, τ for the irreducible 2-dimensional representation of S_4 lifted from the S_3 quotient and set $\mathcal{X}_2 = \mathcal{X}_2(\mathrm{Jac}_{X_d})$. After decomposing $\mathbb{C}[S_4/S_3] = \mathbb{1} \oplus \sigma$ and $\mathbb{C}[S_4/D_4] = \mathbb{1} \oplus \tau$, we see that

$$\langle \sigma, \mathcal{X}_2 \rangle = \langle \mathbb{C}[S_4/S_3], \mathcal{X}_2 \rangle - \langle \mathbb{1}, \mathcal{X}_2 \rangle \overset{\text{Thm. 3.1(2)}}{\underset{\text{\& Lem. 6.14}}{=}} \mathrm{rk}_2 \mathrm{Jac}_Y,$$

and $\langle \tau, \mathcal{X}_2 \rangle = \mathrm{rk}_2(\mathrm{Jac}_Z)$. Therefore, $\mathcal{X}_2 \cong \sigma^{\oplus \mathrm{rk}_2 \mathrm{Jac}_Y} \oplus \tau^{\oplus \mathrm{rk}_2 \mathrm{Jac}_Z} \oplus \rho$, where ρ is an S_4-representation satisfying $\langle \rho, \sigma \rangle = \langle \rho, \tau \rangle = \langle \rho, \mathbb{1} \rangle = 0$. This ensures that Lemma 4.16(2) is applicable for ρ, and therefore $\mathcal{C}_\Theta(\rho) = 1$. On the other hand, an elementary computation shows that $\mathcal{C}_\Theta(\tau) = \mathcal{C}_\Theta(\sigma) = 2$. Thus, $S_{\Theta,2} = \{\tau, \sigma\}$. Part (2) follows by applying Theorem 5.7 to Θ with $p = 2$. □

6.5 Elliptic curves with cyclic isogeny

In this section, we consider cyclic isogenies isogenies $E \to E'$ of elliptic curves of prime degree p.

For the rest of this section, we let M be the extension of K generated by the points in the kernel of this isogeny and τ_P the translation-by-P automorphism on E, where P is any non-trivial point in the kernel of this isogeny. This defines a group homomorphism

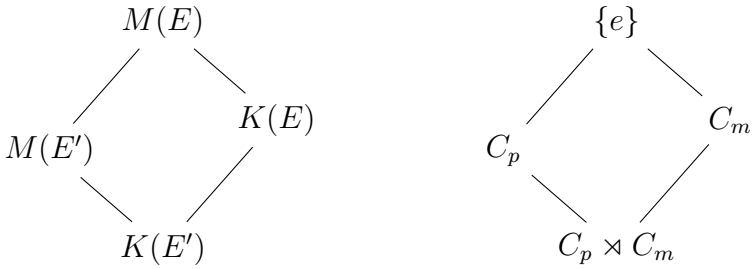
$$\begin{aligned} \psi : \mathrm{Gal}(M/K) &\to \mathrm{Aut}(\langle \tau_P \rangle) \\ \sigma &\mapsto (\tau_P \mapsto \tau_{P^\sigma}), \end{aligned}$$

which can be seen to be injective. Consequently, $\mathrm{Gal}(M/K)$ is cyclic, and we denote $m := [M : K]$.

We write E_M to denote the base change of E to M and $E_{M/K}$ for the corresponding curve over K, see Notation 2.5. We also write E' for the target of this isogeny.

Lemma 6.16. *Write $C_p \rtimes C_m$ to denote the semi-direct product $\langle \tau_P \rangle \rtimes_\psi \mathrm{Gal}(M/K)$. The following hold.*

1. *$C_p \rtimes C_m$ acts on the function field $M(E)$. This action fits into the following Galois diagram with the corresponding subgroups on the right.*



   where C_m and C_p denote the subgroups $\{e\} \times C_m$ and $C_p \times \{e\}$ of $C_p \rtimes C_m$ respectively.

2. *$C_p \rtimes C_m$ acts on $E_{M/K}$ via K-automorphisms.*

3. *The quotients of $E_{M/K}$ by C_m and $C_p \rtimes C_m$ are isomorphic to E and E' respectively.*

Proof. The proof of part (1) can be found in [23, Exercise 7.8.2]. Theorem 2.2 gives a $C_p \rtimes C_m$-action on $E_{M/K}$ which proves part (2). Part (3) follows by combining [53, Remark 4.2] with the Galois diagram appearing in part (1). □

Proposition 6.17. *Let E/K be an elliptic curve which admits an isogeny of prime degree p. Then, the following hold.*

1. *$C_m - C_p \rtimes C_m$ is a pseudo Brauer relation for $E_{M/K}$ that verifies an isogeny $E \to E'$.*
2. *If K is a number field,*

$$\mathrm{rk}_p(E/K) = \sum_{v \text{ place of } K} \mathrm{ord}_p\ \Lambda_\Theta(E_{M/K}/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. For brevity, we write $G = C_p \rtimes C_m$ and $V_\ell = V_\ell(\mathrm{Res}^M_K E)$. We decompose $\mathbb{C}[G/C_m] \cong \mathbb{1} \oplus T$. Then,

$$\langle V_\ell, T\rangle \overset{\text{Frob.rec.}}{=} \dim V_\ell^{C_m} - \dim V_\ell^G \overset{\text{Thm 3.1(1) \& Lem. 6.16(3)}}{=} \dim V_\ell(E) - \dim V_\ell(E') = 0.$$

This completes the proof of part (1). For part (2), we first prove that $\Omega^1(\mathrm{Res}^M_K E)$ is self-dual as a G-representation. By Lemma 3.5, $\Omega^1(\mathrm{Res}^M_K E) \cong \mathrm{Ind}_{C_p}^G \Omega^1(E_M)$ where the C_p action on $\Omega^1(E_M)$ is given by the translation morphism τ_P. Since the pushforward $(\tau_P)_*$ on the Jacobian of E_M is trivial, then $\Omega^1(\mathrm{Res}^M_K E) \cong \mathrm{Ind}_{C_p}^G \mathbb{1}$, which is a self-dual G-representation. Similarly, $V_\ell(\mathrm{Res}^M_K E) \cong \mathrm{Ind}_{C_p}^G \mathbb{1}^{\oplus 2}$.

We write $\mathcal{X}_p$ to denote $\mathcal{X}_p(\mathrm{Res}^M_K E)$. Then, by Theorem 3.1(2), we have $\mathrm{rk}_p(E/K) = \langle \mathbb{1}, \mathcal{X}_p\rangle$. Now decompose $\mathcal{X}_p \cong \mathbb{1}^{\oplus \mathrm{rk}_p(E)} \oplus \rho$. It follows that

$$\langle \rho, \mathbb{C}[G/C_m]\rangle = \langle \mathcal{X}_p \ominus \mathbb{1}^{\oplus \mathrm{rk}_p(E)}, \mathbb{C}[G/C_m]\rangle = \dim \mathcal{X}_p^{C_m} - \mathrm{rk}_p(E) \overset{\text{Thm 3.1(2) \& Lem. 6.16}}{=} 0.$$

By Lemma 4.16(2), we deduce $\mathcal{C}_\Theta(\rho) = 1$. By choosing the trivial pairing on $\mathbb{1}$, we deduce that $\mathcal{C}_\Theta(\mathbb{1}) \equiv \frac{m}{pm} \equiv p \bmod \mathbb{Q}^{\times 2}$, and therefore $S_{\Theta,p} = \{\mathbb{1}\}$. Since

$\Omega^1(\mathrm{Res}_K^M E)$ is a self-dual G-representation, then Theorem 5.7 is applicable. This completes the proof of part (2). □

6.6 Genus two curves with covers to elliptic curves

In this section, we consider a genus 2 curve Y/K with a cover $\phi : Y \to E$ of prime degree p to an elliptic curve E/K. As detailed in [39, §1], its Jacobian, Jac_Y, is isogenous to $E \times E'$ for some complementary elliptic curve E'. Nonetheless, the complementary elliptic curve E' is not uniquely determined by the pair (Y, E), see [80].

This section aims to achieve three distinct goals. Firstly, under some mild assumptions on the cover ϕ (see Definition 6.19), we provide a canonical choice for the complementary elliptic curve E'. We then prove pseudo Brauer verifiability for the isogeny $\mathrm{Jac}_Y \to E \times E'$. Finally, we use regulator constants to obtain a local expression for the parity of the p^∞-Selmer rank of Jac_Y/K when K is a number field.

A central part of our argument is the following commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{\phi} & E \\ \downarrow{\scriptstyle \pi_Y} & & \downarrow{\scriptstyle \pi_E} \\ \mathbb{P}^1_x & \xrightarrow{\Phi} & \mathbb{P}^1_u \end{array}$$

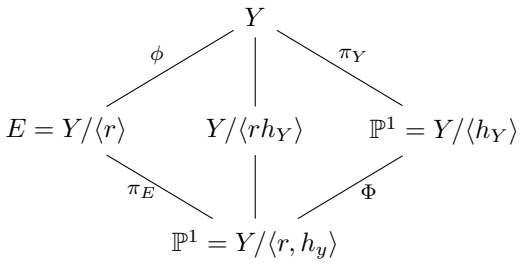
where π_Y and π_E are the natural hyperelliptic covers of $Y : \{y^2 = f(x)\}$ and $E : \{v^2 = g(u)\}$ respectively, Φ is determined by $x \mapsto u$, and $\mathbb{P}^1_x$, $\mathbb{P}^1_u$ indicate the choice of parameters x and u on $\mathbb{P}^1/K$.

6.6.1 Genus two curves with extra involutions

For ease of exposition, we consider the $p = 2$ case separately. In this case, $\phi : Y \xrightarrow{2} E$ is Galois induced by an involution r on Y. In addition, we write h_Y to denote the hyperelliptic involution on Y.

Proposition 6.18. *Let $\phi : Y \xrightarrow{2} E$ be a degree 2 cover from a genus 2 curve to an elliptic curve. Then, the following hold.*

1. *$C_2 \times C_2 \cong \langle r, h_Y \rangle$ acts on Y via K-automorphisms. This action fits into a Galois diagram*



2. *$\{e\} - \langle r \rangle - \langle r h_Y \rangle - \langle h_Y \rangle + 2(C_2 \times C_2)$ is a pseudo Brauer relation for Y which verifies an isogeny $\mathrm{Jac}_Y \to E \times \mathrm{Jac}_{Y/\langle r h_Y \rangle}$.*

3. *If K is a number field,*

$$\mathrm{rk}_2(\mathrm{Jac}_Y/K) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2\ \Lambda_\Theta(Y/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (2).

Proof. Since h_Y lies in the centre of $\mathrm{Aut}_K(Y)$ we deduce that r and h_Y commute. Therefore, $\langle r, h_Y \rangle \cong C_2 \times C_2$, and, by assumption, $E = Y/\langle r \rangle$. This proves (1). Parts (2)–(3) follow similarly to Proposition 6.8(1)–(2). □

We note that Proposition 6.18 gives a canonical choice for the complementary elliptic curve E' as the Jacobian of $Y/\langle r h_Y \rangle$ when $p = 2$. Proposition 6.25 below extends this result to any prime p.

6.6.2 Covers to elliptic curves of odd prime degree

We now consider the case where ϕ is a *generic* odd degree cover.

Definition 6.19 ([57, pp. 44])**.** We say that a cover $\phi : Y \to E$ to an elliptic curve E is *generic* if it is unramified over $E[2]$, i.e., the Weierstrass points of E.

For the remainder of this subsection, we impose the following assumption:

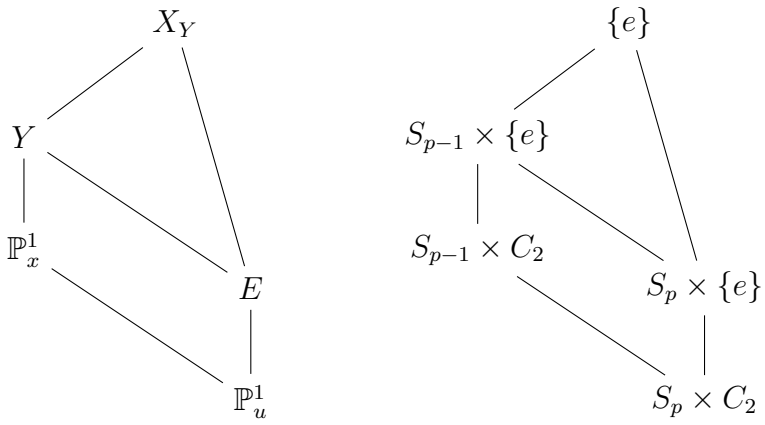
Assumption 6.20. All covers $\phi : Y \to E$ are assumed to be generic.

The relevance of this assumption is that it guarantees the Galois groups of both Φ and ϕ are equal to S_p (see Proposition 6.21). Without this assumption, this may not hold; see, for example, [40, Corollary 3.7(b)].

Proposition 6.21. *Let Y/K be a genus 2 curve which admits a generic cover $\phi : Y \to E$ of odd prime degree p. Write $X_Y \to \mathbb{P}^1_u$ to denote the Galois closure of $Y \xrightarrow{p} E \xrightarrow{2} \mathbb{P}^1_u$.*

1. *The cover $X_Y \to \mathbb{P}^1_u$ has Galois group $S_p \times C_2$. In addition, X_Y is geometrically connected.*

2. *This action fits into a Galois diagram with the corresponding subgroups on the right.*



Proof. Let $\{u_1, u_2, u_3, u_4\}$ be the branch locus of $E \to \mathbb{P}^1_u$, i.e., $u(E[2])$, and suppose that $u_4 = \infty$. The ramification locus of Φ is given by $\{u_1, u_2, u_3, u_4, u_5\}$ for $p \geq 5$ and $\{u_1, u_2, u_3, u_5\}$ for $p = 3$ where $u_5 \notin u(E[2])$, see [57, §1]. Also, the ramification is determined by the tuple $\left((2)^{\frac{p-1}{2}}, (2)^{\frac{p-1}{2}}, (2)^{\frac{p-1}{2}}, (2)^{\frac{p-3}{2}}, (2)^1\right)$ (i.e., there are $\frac{p-1}{2}$ doubly ramified points above u_1, u_2, u_3, $\frac{p-3}{2}$ above u_4, and a doubly ramified point above u_5).

We write $\overline{\Phi}$ for the base change to $\overline{K}$. Then, [68, Corollary 4.10] induces five involutions $(\sigma_1, \ldots, \sigma_5)$ and their cycle types match the ramification over

$(u_1, \ldots, u_5)$. In addition, [4, §4.3] asserts that these involutions generate the Galois group of $\overline{\Phi}$ which must be a transitive subgroup of S_p. Since σ_5 is a 2-cycle (i.e., a transposition), then the Galois group is all of S_p (see [45, II.4.5b]). Write $X_{\mathbb{P}^1} \to \mathbb{P}^1_u$ to denote the Galois closure of $\Phi : \mathbb{P}^1_x \to \mathbb{P}^1_u$. It follows that $X_{\mathbb{P}^1}$ is geometrically connected, and $X_{\mathbb{P}^1} \to \mathbb{P}^1_u$ has Galois group S_p.

To show that the Galois group of $X_Y \to \mathbb{P}^1_u$ is $S_p \times C_2$, write $W := X_{\mathbb{P}^1}/A_p$ for the discriminant curve of $X_{\mathbb{P}^1} \to \mathbb{P}^1_u$ (as in [53, Lemma 2.7]). The fibre of $W \xrightarrow{2} \mathbb{P}^1_u$ over u_i is in bijection with the double coset space $\langle \sigma_i \rangle \backslash S_p / A_p$ [59, Remark 3.19]. When $p \equiv 1 \bmod 4$, $\sigma_1, \sigma_2, \sigma_3$ are even permutations, while σ_4, σ_5 are odd permutations. Thus, the branch locus of $W \to \mathbb{P}^1_u$ is $\{u_4, u_5\}$. On the other hand, when $p \equiv 3 \bmod 4$, the branch locus is $\{u_1, u_2, u_3, u_5\}$. Since the branch locus of $E \to \mathbb{P}^1_u$ is $\{u_1, u_2, u_3, u_4\}$, it follows that $W \ncong E$. By construction, $K(X_Y) = K(X_{\mathbb{P}^1}) \cdot K(E)$ and $K(E) \cap K(X_{\mathbb{P}^1}) = K(u)$. Therefore, the Galois group of $X_Y \to \mathbb{P}^1_u$ is $S_p \times C_2$.

We now show X_Y is geometrically connected. Aiming for a contradiction, suppose it is not. Recall that $X_{\mathbb{P}^1}$ is geometrically connected, and so K is algebraically closed in $K(X_{\mathbb{P}^1})$. Given that $[K(X_Y) : K(X_{\mathbb{P}^1})] = 2$, if X_Y were not geometrically connected, its geometric components would have to be defined over a quadratic extension of K, say $K(\sqrt{m})$. Therefore, $K(u, \sqrt{m})$ is an intermediate field of $K(u) \subseteq K(X_Y)$. There are three index-2 subgroups in $S_p \times C_2$, namely $S_p \times \{e\}$, $A_p \times C_2$ and a mixed group determined by the kernel of the map $C_2 \times S_p \to \{\pm 1\}$ given by $(a, b) \mapsto \mathrm{sign}(a)\mathrm{sign}(b)$. Keeping track of ramification, we see that their corresponding branch loci are $\{u_1, u_2, u_3, u_4\}$, $\{u_4, u_5\}$, and $\{u_1, u_2, u_3, u_5\}$ when $p \equiv 1 \bmod 4$, and $\{u_1, u_2, u_3, u_4\}$, $\{u_1, u_2, u_3, u_5\}$, and $\{u_4, u_5\}$ when $p \equiv 3 \bmod 4$. Therefore, $K(u, \sqrt{m})$ cannot be an intermediate field. This gives part (1).

The Galois diagram given in part (2) is immediate by construction. □

The $S_p \times C_2$ action on X_Y induces an $S_p \times C_2$ action on the ℓ-adic Tate module $V_\ell(\mathrm{Jac}_{X_Y})$. We now find the structure of this representation. We first fix some notation.

Notation 6.22. For $1 \leq i \leq 5$, we define $\tau_i = (\sigma_i, g_i)$ to be any elements in $S_p \times C_2$, determined up to conjugacy, as follows:

1. The conjugacy classes $\mathrm{cl}(\sigma_i)$ in S_p (determined by their cycle decompositions) are

$$\mathrm{cl}(\sigma_1) = \mathrm{cl}(\sigma_2) = \mathrm{cl}(\sigma_3) = (2)^{\frac{p-1}{2}}, \quad \mathrm{cl}(\sigma_4) = (2)^{\frac{p-3}{2}}, \quad \mathrm{cl}(\sigma_5) = (2)^1.$$

2. The element $g_i \in C_2$ is non-trivial for $1 \leq i \leq 4$ and trivial for $i = 5$.

Theorem 6.23. *Let p an odd prime. Then, for any prime ℓ, and in the situation of Proposition 6.21, the $S_p \times C_2$-representations*

$$V_\ell(\mathrm{Jac}_{X_Y}) \quad \text{and} \quad \mathbb{1}^{\oplus 2} \oplus (\mathrm{Ind}_{\{e\}}^{S_p \times C_2} \mathbb{1})^{\oplus 3} \ominus \bigoplus_{i=1}^{5} \mathrm{Ind}_{\langle \tau_i \rangle}^{S_p \times C_2} \mathbb{1}$$

become isomorphic after extending scalars to $\mathbb{C}$.

Proof. Since $X_Y \to \mathbb{P}^1_u$ is the Galois closure of $Y \xrightarrow{2} \mathbb{P}^1_x \xrightarrow{p} \mathbb{P}^1_u$, then their branch loci are the same [85, Corollary 3.9.3(b)]. As mentioned in the proof of Proposition 6.21, the branch locus is $\{u_1, u_2, u_3, u_4, u_5\}$, and there is a 5-tuple $(\tau_1, \ldots, \tau_5)$ of elements in $S_p \times C_2$ such that the subgroup $\langle \tau_i \rangle \subseteq S_p \times C_2$ is the stabiliser of some point $y_i \in X_Y$ in the fibre of u_i. Adding on, $\mathrm{Gal}(X_Y/\mathbb{P}^1_u) \cong \mathrm{Gal}(X_{\mathbb{P}^1}/\mathbb{P}^1_u) \times \mathrm{Gal}(E/\mathbb{P}^1_u)$, where $X_{\mathbb{P}^1} \to \mathbb{P}^1_u$ is the Galois closure of Φ.

Let $x_i \in X_{\mathbb{P}^1}$ and $p_i \in E$ be images of y_i under the covers $X_Y \to X_{\mathbb{P}^1}$ and $X_Y \to E$. Then, the quotient map $\mathrm{Gal}(X_Y/\mathbb{P}^1_u) \to \mathrm{Gal}(X_{\mathbb{P}^1}/\mathbb{P}^1_u)$ restricts to a surjective homomorphism $\mathrm{Stab}_{S_p \times C_2}(y_i) \to \mathrm{Stab}_{S_p}(x_i)$. Similarly, we get a surjection $\mathrm{Stab}_{S_p \times C_2}(y_i) \to \mathrm{Stab}_{C_2}(p_i)$. It follows that if $\tau_i = (\sigma_i, g_i) \in S_p \times C_2$, then the subgroup $\langle \sigma_i \rangle \subseteq S_p$ is the stabiliser of x_i, and $\langle g_i \rangle \subseteq C_2$ is the stabiliser of p_i. Since $\{u_1, u_2, u_3, u_4\}$ is the branch locus of $E \to \mathbb{P}^1_u$, then g_i is the non-trivial element in C_2 for $i = 1, 2, 3, 4$, while g_5 must be trivial. The conjugacy class of σ_i in S_p is determined by its cycle type, which in turn is determined by the ramification structure of $X_{\mathbb{P}^1} \to \mathbb{P}^1_u$ at $(u_i)_{i=1}^5$. By [57, §1],

this is given by the tuple $\left((2)^{\frac{p-1}{2}}, (2)^{\frac{p-1}{2}}, (2)^{\frac{p-1}{2}}, (2)^{\frac{p-3}{2}}, (2)^1\right)$. Therefore, the elements $\tau_i \in S_p \times C_2$ appearing in the 5-tuple for $X_Y \to \mathbb{P}^1_u$ agree with the elements given in Notation 6.22.

The result follows from [35, Proposition 1.1], which is applicable since $X_Y \to \mathbb{P}^1$ is a cover of geometrically connected curves by Proposition 6.21. □

6.6.3 Split genus two Jacobians and rank parity

In the following subsection, we provide a canonical choice for the complementary elliptic curve E' as the Jacobian of the quotient of X_Y by a subgroup H'. We note that this choice is also specified in [59, Table 4] when $p \leq 7$. Furthermore, [41] shows that this choice remains valid when ϕ is non-generic, albeit under the assumption that Y, E, and the cover $\phi : Y \to E$ are defined over an algebraically closed field.

Notation 6.24. View $S_p \times C_2$ as a subgroup of permutations on $\{1, \ldots, p+2\}$ by letting $S_p \times \{e\}$ and $\{e\} \times C_2$ act separately on $\{1, \ldots, p\}$ and $\{p+1, p+2\}$. We write H' to denote the subgroup of $S_p \times C_2$ generated by

$$H' = \begin{cases} \langle (1, \ldots, p-2), (1,2), (p-1,p)(p+1,p+2) \rangle & p \geq 5, \\ \langle (2,3)(4,5) \rangle & p = 3. \end{cases}$$

As an abstract group, H' is isomorphic to $S_{p-2} \times C_2$.

We then take $E' := \mathrm{Jac}_{X_Y/H'}$. With respect to this choice, we prove pseudo Brauer verifiability for $\mathrm{Jac}_Y \to E \times E'$.

Proposition 6.25. *Let Y/K be a genus 2 curve which admits a generic cover $\phi : Y \to E$ of prime degree p.*

1. *$(S_{p-1} \times \{e\}) - (S_p \times \{e\}) - H'$ is a pseudo Brauer relation for X_Y that verifies an isogeny $\mathrm{Jac}_Y \to E \times E'$.*

2. *If K is a number field,*

$$\mathrm{rk}_p(\mathrm{Jac}_Y/K) = \sum_{v \text{ place of } K} \mathrm{ord}_p \Lambda_\Theta(X_Y/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. The case where $p = 2$ follows from Proposition 6.18. We now suppose that $p \geq 3$.

For brevity, write V_ℓ for $V_\ell(\mathrm{Jac}_{X_Y}) \otimes \mathbb{C}$ and $\mathbb{1}\uparrow_H$ for the permutation representations $\mathrm{Ind}_H^{S_p \times C_2}\mathbb{1}$. Let ϵ and σ be the 1-dimensional sign and $(p-1)$ dimensional standard representations lifted from the C_2 and S_p-quotients respectively. By decomposing into irreducible representations, we get

$$\mathbb{1}\uparrow_{S_p\times\{e\}} = \mathbb{1} \oplus \epsilon, \quad \mathbb{1}\uparrow_{S_{p-1}\times C_2} = \mathbb{1} \oplus \sigma, \quad \mathbb{1}\uparrow_{S_{p-1}\times\{e\}} = \mathbb{1} \oplus \epsilon \oplus \sigma \oplus (\sigma \otimes \epsilon)$$

We also see that

$$\langle \sigma\otimes\epsilon, \mathbb{1}\uparrow_{H'}\rangle = \langle \mathbb{1}\uparrow_{S_{p-1}\times\{e\}} - \mathbb{1}\uparrow_{S_{p-1}\times C_2} - \mathbb{1}\uparrow_{S_p\times\{e\}} + \mathbb{1}, \mathbb{1}\uparrow_{H'}\rangle = 3-2-1+1 = 1,$$

where the last equality follows from $\langle \mathbb{1}\uparrow_H, \mathbb{1}\uparrow_K\rangle = |H\backslash(S_p \times C_2)/K|$. We can therefore decompose $\mathbb{1}\uparrow_{H'} = (\sigma \otimes \epsilon) \oplus \chi$, for some $S_p \times C_2$-representation χ. Then, the multiplicities of $\mathbb{1}$, ϵ, σ, $\sigma \otimes \epsilon$ and χ in V_ℓ are as follows:

	$\mathbb{1}$	ϵ	σ	$\sigma \otimes \epsilon$	χ
V_ℓ	0	2	0	2	0

To find the multiplicities of $\mathbb{1}, \epsilon, \sigma, \sigma\otimes\epsilon$ in V_ℓ, combine Theorem 3.1(1) with Proposition 6.21(2). For the last entry, we instead show that $\langle V_\ell, \mathbb{1}\uparrow_{H'}\rangle = 2$. With τ_i as in Notation 6.22 and for $p \geq 3$, we deduce (using Burnside's orbit-counting lemma for example) that

$$\langle \mathbb{1}\uparrow_{\langle\tau_i\rangle}, \mathbb{1}\uparrow_{H'}\rangle = |\langle\tau_i\rangle\backslash(S_p \times C_2)/H'| = \begin{cases} \frac{1}{2}(p^2-1), & i = 1,2,3, \\ \frac{1}{2}(p^2-3), & i = 4, \\ p^2 - 3p + 3, & i = 5. \end{cases}$$

Therefore, $\langle V_\ell, \mathbb{1}\uparrow_{H'}\rangle \overset{\text{Thm. } 6.23}{=} 2 + 3(p)(p-1) - \sum_{i=1}^{5} |\langle\tau_i\rangle\backslash(S_p \times C_2)/H'| = 2,$

as required. Therefore, we have an isomorphism of G-representations

$$\chi \oplus \mathbb{1}\uparrow_{S_{p-1}\times\{e\}} \cong \mathbb{1}\uparrow_{S_p\times\{e\}} \oplus \mathbb{1}\uparrow_{H'} \oplus \sigma,$$

and so $(S_{p-1}\times\{e\}) - (S_p\times\{e\}) - H'$ is a pseudo Brauer relation for X_Y. In view of Proposition 6.21, this verifies an isogeny $\mathrm{Jac}_Y \to E \times E'$ completing the proof of (1).

We write $\mathcal{X}_p$ to denote $\mathcal{X}_p(\mathrm{Jac}_{X_Y})$. Then, the corresponding multiplicities in this case are as follows:

	$\mathbb{1}$	ϵ	σ	$\sigma\otimes\epsilon$	χ
$\mathcal{X}_p$	0	$\mathrm{rk}_p(E)$	0	$\mathrm{rk}_p(E')$	0

This follows from Theorem 3.1(2) for $\epsilon, \sigma\otimes\epsilon$ and Theorem 3.1(5) for $\mathbb{1}, \sigma, \chi$. We deduce

$$\mathcal{X}_p \cong \epsilon^{\oplus \mathrm{rk}_p(E)} \oplus (\sigma\otimes\epsilon)^{\oplus \mathrm{rk}_p(E')} \oplus \rho,$$

where ρ is a representation satisfying $\langle \rho, \mathbb{1}\uparrow_{S_{p-1}\times\{e\}}\rangle = \langle \rho, \mathbb{1}\uparrow_{H'}\rangle = 0$. By Lemma 4.16(2), we deduce that $\mathcal{C}_\Theta(\rho) = 1$ and therefore $S_{\Theta,p} \subseteq \{\epsilon, \sigma\otimes\epsilon\}$.

We now show that $\mathcal{C}_\Theta(\epsilon) = \mathcal{C}_\Theta(\sigma\otimes\epsilon) = p$. By choosing the trivial pairing on ϵ, we get $\mathcal{C}_\Theta(\epsilon) = \frac{\frac{1}{(p-1)!}}{\frac{1}{p!}} = p$, since the space of H'-invariant vectors is zero. Therefore, $\epsilon \in S_{\Theta,p}$.

For $\sigma\otimes\epsilon$, we fix a basis $\{e_1, \ldots, e_p\}$ for $\mathbb{C}^p$. Then, $\sigma\otimes\epsilon$ is given by the subspace spanned by $v_i = e_{i+1} - e_1$ for $i = 1, \ldots, p-1$ with $(\rho_1, \rho_2) \in S_p \times C_2$ acting via $(\rho_1, \rho_2)\cdot v_i = \mathrm{sgn}(\rho_2)(e_{\rho_1(i+1)} - e_{\rho_1(1)})$. A non-degenerate and $S_p\times C_2$-invariant pairing on $\sigma\otimes\epsilon$ is defined by setting the diagonal entries $\langle\!\langle v_i, v_i\rangle\!\rangle = 2$ and the off-diagonal entries $\langle\!\langle v_i, v_j\rangle\!\rangle = 1$. Suppose that the S_{p-1} factor in $S_{p-1}\times\{e\}$ stabilises 1. Then for $H \in \{S_{p-1}\times\{e\}, S_p\times\{e\}, H'\}$, the space of H-invariant vectors is one dimensional spanned by $u_1 = \sum_{i=1}^{p-1} v_i$, zero and one dimensional spanned by $u_2 = v_{p-2} - v_{p-1}$ respectively. Therefore,

$\langle\langle u_1, u_1\rangle\rangle = p(p-1)$, while $\langle\langle u_2, u_2\rangle\rangle = 2$. Putting everything together,

$$\mathcal{C}_\Theta(\sigma \otimes \epsilon) \overset{\text{Remark 4.10}}{=} \frac{\frac{1}{(p-1)!}\langle\langle u_1, u_1\rangle\rangle}{\frac{1}{2(p-2)!}\langle\langle u_2, u_2\rangle\rangle} = p.$$

It follows that $S_{\Theta,p} = \{\epsilon, \sigma \otimes \epsilon\}$. Therefore, part (2) follows from Theorem 5.7. □

Remark 6.26. We note that covers $Y \to E$ of genus 2 curves to elliptic curves occur in pairs (ϕ, ψ). In particular, if $\phi : Y \to E$ is a cover of prime degree p, then there exists a complementary cover $\psi : Y \to \tilde{E}$ of the same degree, where $\tilde{E}$ is an elliptic curve. Therefore, Proposition 6.21 and Proposition 6.25 are applicable when either ϕ or ψ is generic, interchanging ϕ with ψ and E with $\tilde{E}$ when needed.

6.7 Products of Weil-restrictions

Let Y be a geometrically connected curve defined over a field K of characteristic 0. In the following section, we consider isogenies

$$\prod_i \mathrm{Res}_K^{F^{H_i}} \mathrm{Jac}_Y \to \prod_j \mathrm{Res}_K^{F^{H_j}} \mathrm{Jac}_Y$$

induced from Brauer relations $\sum_i H_i - \sum_j H'_j$ for a Galois group $\mathrm{Gal}(F/K)$. These isogenies can be derived using the framework of [60, Lemma 2.4] and [64, §2]- see [30, Theorem 2.3] for details.

In the following result, we write Y_F for the base-change of Y to F and $Y_{F/K}$ for the corresponding curve over K as in Notation 2.5.

Proposition 6.27. *Let Y/K be a geometrically connected curve, F/K a Galois extension and $\Theta = \sum_i H_i - \sum_j H'_j$ a Brauer relation for* $\mathrm{Gal}(F/K)$.

1. *$\sum_i H_i - \sum_j H'_j$ is a pseudo Brauer relation for $Y_{F/K}$ that verifies an isogeny $\prod_i \mathrm{Res}_K^{F^{H_i}} \mathrm{Jac}_Y \to \prod_j \mathrm{Res}_K^{F^{H'_j}} \mathrm{Jac}_Y$.*

2. If K is a number field and p an arbitrary prime,

$$\sum_{\tau \in S_{\Theta,p}} \frac{\langle \mathcal{X}_p(\mathrm{Res}_K^F \mathrm{Jac}_Y), \tau \rangle}{\langle \tau, \tau \rangle} = \sum_{v \text{ place of } K} \mathrm{ord}_p \Lambda_\Theta(Y_{F/K}/K_v) \mod 2,$$

where Θ is the pseudo Brauer relation from part (1).

Proof. We let $K(Y)$ be the function field of Y, and we consider the Galois extension $F(Y)/K(Y)$. Then, the action of $G := \mathrm{Gal}(F/K)$ on $F(Y)$ is given the action of the Galois group on F, the constant functions in $F(Y)$. Using Theorem 2.2, this induces a G-action on $Y_{F/K}$ by K-automorphisms. Since $F(Y)^H = F^H(Y)$, then the Jacobian of the quotient of $Y_{F/K}$ by $H \leq G$ is $\mathrm{Res}_K^{F^H}(\mathrm{Jac}_Y)$ by Lemma 2.12. Part (1) follows by combining this observation with the fact that any Brauer relation for the group G is automatically a pseudo Brauer relation for $Y_{F/K}$. Write $\mathrm{g}(Y)$ to denote the genus of Y. By Lemma 3.5, $\Omega^1(\mathrm{Res}_K^F \mathrm{Jac}_Y) \cong \mathrm{Ind}_{\{e\}}^G \mathbb{1}^{\oplus \mathrm{g}(Y)}$. This is self-dual and therefore Theorem 5.7 is applicable. This completes the proof of part (2). □

Chapter 7

Abelian varieties with prescribed Tate–Shafarevich group orders up to squares

In the following chapter, we prove the following result.

Theorem 7.1 (=Corollary 7.14)**.** *For every square-free natural number m, there exists an abelian variety $A/\mathbb{Q}$ with finite Tate–Shafarevich group of order ms^2 for some integer $s \geq 1$.*

7.1 The square-free part of the Tate–Shafarevich group

Our proof relies on breaking down the Weil-restriction of scalars of an abelian variety up to isogeny followed by an application of a formula of Cassels–Tate (already discussed in §1.6.2). This allows us to express the size of the Tate–Shafarevich group, up to rational squares, in terms of Birch and Swinnerton-Dyer constants defined in §2.3.

7.1.1 Cassels–Tate formula

For the remainder of this chapter, we use the following notation.

Notation 7.2. Given a K-rational isogeny $\phi : A_1 \to A_2$, we write

$$\begin{aligned} Q(\phi) =&|\mathrm{coker}(\phi : A_1(K)/A_1(K)_{\mathrm{tors}} \to A_2(K)/A_2(K)_{\mathrm{tors}})| \\ &\times|\ker(\phi : Ш(A_1/K)_{\mathrm{div}} \to Ш(A_2/K)_{\mathrm{div}})|, \end{aligned}$$

where $Ш_{\mathrm{div}}$ denotes the divisible part of Ш. We write $Ш_0 = Ш/Ш_{\mathrm{div}}$.

For an abelian variety A/K with a fixed non-zero global exterior form ω, we denote the Birch–Swinnerton-Dyer periods by

$$\Omega_{\mathbb{C}}(A,\omega) = 2^{\dim A}\int_{A(\mathbb{C})} |\omega \wedge \overline{\omega}|\,, \qquad \Omega_{\mathbb{R}}(A,\omega) = \int_{A(\mathbb{R})} |\omega|\,.$$

We write $\Omega(A/K,\omega) = \prod_{v|\infty}\Omega_{K_v}(A,\omega)$ where $K_v = \mathbb{R}$ (resp., $\mathbb{C}$) if v is real (resp., complex). In addition, for a non-archimedean place v, we let $w^0_{A,v}$ be a Néron minimal exterior form on A, $c_v(A/K)$ be the Tamagawa number at v and $\tilde{C}(A/K,\omega) = \prod_{v\nmid\infty} c_v(A/K)|\omega/\omega^0_{A,v}|_v$. In particular, $C(A/K) = \tilde{C}(A/K)\Omega(A/K)$ where $C(A/K)$ is as in §2.3.1. Finally, we write $A^\vee$ to denote the dual abelian variety, $\phi^\vee$ for the dual isogeny and $\square$ for the square of a rational number.

The following is a version of the Cassels–Tate formula, expressed in terms of Selmer groups.

Theorem 7.3 (cf. [30, Theorem 4.3])**.** *Let $\phi : A_1 \to A_2$ be a K-rational isogeny. Then, for any non-zero global exterior forms ω_1 and ω_2 on A_1 and A_2,*

$$\frac{Q(\phi^\vee)}{Q(\phi)} = \frac{|A_2(K)_{\mathrm{tors}}|}{|A_1(K)_{\mathrm{tors}}|}\frac{|A_2^\vee(K)_{\mathrm{tors}}|}{|A_1^\vee(K)_{\mathrm{tors}}|}\frac{\tilde{C}(A_1/K,\omega_1)}{\tilde{C}(A_2/K,\omega_2)}\frac{\Omega(A_1/K,\omega_1)}{\Omega(A_2/K,\omega_2)}\prod_{p|\deg(\phi)}\frac{|Ш_0(A_1/K)[p^\infty]|}{|Ш_0(A_2/K)[p^\infty]|}.$$

Given a field extension L/K, we write ϕ_L for the base change of ϕ to L. The following proposition shows that for a carefully chosen L and working modulo squares, the Cassels–Tate formula simplifies.

Lemma 7.4. *Let L/K be a quadratic extension in which all bad primes of $A_1/K, A_2/K$ and all primes of K dividing* $\deg(\phi)$ *split. In addition, suppose*

that $\deg(\phi)$ *is a square. Then,*

$$\frac{Q(\phi_L^\vee)}{Q(\phi_L)} = \frac{|A_2(L)_{\mathrm{tors}}|}{|A_1(L)_{\mathrm{tors}}|}\frac{|A_2^\vee(L)_{\mathrm{tors}}|}{|A_1^\vee(L)_{\mathrm{tors}}|}\prod_{p|\deg(\phi)}\frac{|Ш_0(A_1/L)[p^\infty]|}{|Ш_0(A_2/L)[p^\infty]|} \mod \square.$$

Proof. By the product formula, the constant $\tilde{C}(A_1/L,\omega_1)\Omega(A_1/L,\omega_1)$ is independent of ω_1. We consider the expression from Theorem 7.3 with $\omega_1 = \phi^*\omega_2$. By our assumptions on L/K, the only terms in the product $\frac{C(A_1/L,\omega_1)}{C(A_2/L,\omega_2)}$ that are not obviously contributing a rational square are the complex places of L lying above real places of K and the non-archimedean places of L that do not divide $\deg(\phi)$. As in the proof of [65, Theorem 7.3], when w is complex, $\Omega_{\mathbb{C}}(A_1,\phi^*\omega_2)/\Omega_{\mathbb{C}}(A_2,\omega_2) = \deg(\phi) = \square$. In addition, by [78, pp. 12], $|(\phi^*\omega_2/\omega^0_{A_1,w})/(\omega_2/\omega^0_{A_2,w})|_w = 1$ whenever w is a place of L not dividing $\deg(\phi)$. To conclude, $\frac{\tilde{C}(A_1/L,\omega_1)}{\tilde{C}(A_2/L,\omega_2)}\frac{\Omega(A_1/L,\omega_1)}{\Omega(A_2/L,\omega_2)} = \square$ giving the required result. □

7.1.2 An isogeny decomposition for the Weil-restriction

In what follows, we let A/K be a principally polarised abelian variety defined over a number field K. We let p be an odd prime, F/K a cyclic extension of degree p and $\mathrm{Res}_K^F A$ the Weil-restriction of scalars from F to K. For brevity, we write $B = \mathrm{Res}_K^F A$. This is an F/K-twist of A^p, and the product polarisation on A^p descends to a principal polarisation on B/K. Then, there are K-morphisms

$$i : A \to B, \qquad \mathrm{Tr} : B \to A.$$

These are the inclusion and the trace map respectively.

After identifying the base change $B_F = A^p$ as principally polarised abelian varieties, the base changed morphisms i_F and Tr_F coincide with the diagonal inclusion and the summation map respectively. In addition, writing $i^\vee : B \to A$ for the dual of i (having suppressed the canonical principal polarisations on both sides), we have $i^\vee = \mathrm{Tr}$. Finally, we write Y to denote the kernel of the trace map. This is an abelian variety defined over K and is an F/K-twist of A^{p-1} (see [84, Proposition 2.4]).

Lemma 7.5. *Let $\phi : Y \times A \to B$ be given by $(x, y) \mapsto x + i(y)$. Then, ϕ is a K-rational isogeny with $\ker(\phi) \cong A[p]$.*

Proof. It suffices to show $\ker(\phi) \cong A[p]$. After base change to $\overline{K}$, we identify $Y_{\overline{K}} = A^{p-1}$ and $B_{\overline{K}} = A^p$. Then, on $\overline{K}$-points ϕ is given by $(x_1, \ldots, x_{p-1}, y) \mapsto (y + x_1, \ldots, y + x_{p-1}, y - \sum_{i=1}^{p-1} x_i)$. Thus, restricting the projection $Y \times A \to A$ to $\ker(\phi)$ allows us to deduce that $\ker(\phi) \cong A[p]$. □

7.1.3 An expression for $|Ш(Y/L)|$ modulo squares

We continue to write F/K to denote a cyclic, degree p extension.

Lemma 7.6. *Let L/K be a number field extension such that $L \otimes_K F$ is a field. Then, the following hold.*

1. *For all odd primes $q \neq p$, $|Ш_0(Y/L)[q^\infty]| = \square$.*

2. *If, in addition, A is an elliptic curve, $|Ш_0(Y/L)[2^\infty]| = \square$.*

Proof. By Lemma 7.5, $\deg(\phi) = p^{2\dim(A)}$. When $q \neq p$, this isogeny induces an isomorphism $Ш_0(A/L)[q^\infty] \times Ш_0(Y/L)[q^\infty] \xrightarrow{\sim} Ш_0(B/L)[q^\infty]$. Since both A and B are principally polarised, then $Ш_0(A/L)[q^\infty]$ and $Ш_0(B/L)[q^\infty]$ are of square order for all odd q [75, Theorem 8]. This proves (1). Further, by [20, Proposition A.5.2], $B_L \cong \mathrm{Res}_L^{L \otimes_K F} A$, and by combining [64, pp. 178(a)] with Shapiro's Lemma, $Ш_0(B/L)[2^\infty] \cong Ш_0(A/L \otimes_K F)[2^\infty]$. Therefore, if A is an elliptic curve, both $Ш_0(A/L)[2^\infty]$ and $Ш_0(B/L)[2^\infty]$ are of square order by [12]. Claim (2) follows. □

As in §1.8, we write $\mathrm{rk}_p(A/K)$ for the $\mathbb{Z}_p$-corank of the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(A/K) := \varinjlim_{n \geq 1} \mathrm{Sel}_{p^n}(A/K)$. This coincides with the Mordell–Weil rank of A plus the multiplicity of $\mathbb{Q}_p/\mathbb{Z}_p$ in its Tate–Shafarevich group.

Proposition 7.7. *Let L/K be a quadratic extension in which all bad primes of A/K and all primes dividing either $\deg(\phi) = p^{2\dim(A)}$ or the relative discriminant $\Delta(F/K)$ split. Then, the following hold.*

1. Up to rational squares,

$$|Ш_0(Y/L)[p^\infty]| \equiv \frac{Q(\phi_L)}{Q(\phi_L^\vee)} \frac{|Y(L)[p^\infty]|}{|Y^\vee(L)[p^\infty]|} \mod \square.$$

2. If, in addition, $\mathrm{rk}_p(A/L) = \mathrm{rk}_p(A/L \otimes_K F)$*, then*

$$|Ш_0(Y/L)[p^\infty]| \equiv p^{\mathrm{rk}_p(A/L)} \frac{|Y(L)[p^\infty]|}{|Y^\vee(L)[p^\infty]|} \mod \square.$$

Proof. Let v be a place of bad reduction of B/K. By [64, Proposition 1], v is either a place of bad reduction of A/K or $v|\Delta(F/K)$. Therefore, all bad primes of B/K split in L. Since A/K is principally polarised, $|A(L)_{\mathrm{tors}}| = |A^\vee(L)_{\mathrm{tors}}|$ and $|Ш_0(A/L)[p^\infty]| = \square$. The same holds for B. Since $\deg(\phi)$ is a power of p (see Lemma 7.5), part (1) follows from Lemma 7.4. For part (2), it suffices to show that if $\mathrm{rk}_p(A/L) = \mathrm{rk}_p(A/L \otimes_K F)$, then $Q(\phi_L)/Q(\phi_L^\vee) = p^{\mathrm{rk}_p(A/L)} \cdot \square$. After suppressing the principal polarisations $A = A^\vee, B = B^\vee$, we view $\phi^\vee$ as a morphism $B \to A \times Y^\vee$. Therefore, $Q(\phi_L)/Q(\phi_L^\vee) \equiv Q(\phi_L^\vee \circ \phi_L : A \times Y \to A \times Y^\vee) \mod \square$. Since the the degree of $\phi^\vee \circ \phi$ is a power of p, we have $Ш(A \times Y/L)_{\mathrm{div}}[q^\infty] \xrightarrow{\sim} Ш(A \times Y^\vee/L)_{\mathrm{div}}[q^\infty]$ when $q \neq p$. From this, we deduce $\ker(\phi_L^\vee \circ \phi_L \mid Ш_{\mathrm{div}}) = \ker(\phi_L^\vee \circ \phi_L \mid Ш_{\mathrm{div}}[p^\infty])$. Since $B_L \cong \mathrm{Res}_L^{L \otimes_K F} A$ (see [20, Proposition A.5.2]), then by combining [64, pp. 178(a)] with Shapiro's Lemma gives $\mathrm{Sel}_{p^\infty}(B/L) \cong \mathrm{Sel}_{p^\infty}(A/L \otimes_K F)$. Since $\mathrm{rk}_p(A/L) = \mathrm{rk}_p(A/L \otimes_K F)$, then $\mathrm{rk}_p(Y/L) = \mathrm{rk}_p(Y^\vee/L) = 0$. As a result, $Q(\phi_L^\vee \circ \phi_L)$ coincides with $Q(i_L^\vee \circ i_L)$, where we view $i_L^\vee \circ i_L$ as an endomorphism of A_L. Using the description of i and $i^\vee$ from §7.1.2, $i^\vee \circ i = [p]_A$. This gives the required result. □

7.2 Tate–Shafarevich group of non-square order

We retain all the notation from §7.1. In addition, we fix the following.

Notation 7.8. We write K_∞ to denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, K_n

for the n^{th} layer of this extension with $K_0 = \mathbb{Q}$. For d a positive, square-free integer, we let $L_n = K_n \cdot \mathbb{Q}(\sqrt{-d})$.

In this section, we will restrict our attention to the case where $A = E$ is an elliptic curve, and K and F are consecutive layers of the p-cyclotomic tower. Therefore, Y (defined as the kernel of the trace map as in §7.1.2), is an abelian variety defined over K of dimension $p-1$.

We first prove a lemma involving torsion on Y and $Y^\vee$.

Lemma 7.9. *Let E be an elliptic curve defined over $\mathbb{Q}$. For any $n \geq 0$ and any prime $p \geq 11$, both $Y(L_n)[p^\infty]$ and $Y^\vee(L_n)[p^\infty]$ are trivial.*

Proof. As abelian varieties over L_{n+1}, both Y and $Y^\vee$ are isomorphic to E^{p-1}. It therefore suffices to show that $E(L_{n+1})[p^\infty]$ is trivial for $p \geq 11$. Let E_{-d} be the quadratic twist of E by $-d$. Then, there exists a map $E(L_{n+1}) \to E(K_{n+1}) \times E_{-d}(K_{n+1})$ whose kernel and cokernel are 2-groups. Then, for any odd prime p, this induces an isomorphism

$$E(L_{n+1})[p^\infty] \xrightarrow{\sim} E(K_{n+1})[p^\infty] \times E_{-d}(K_{n+1})[p^\infty].$$

By [18, Theorem 1.1], $E(K_\infty)[p^\infty] = E(\mathbb{Q})[p^\infty]$ (similarly for E_{-d}) for any $p \geq 5$. If $p \geq 11$, Mazur's theorem [63, Theorem 2] asserts that $E(\mathbb{Q})[p^\infty]$ and $E_{-d}(\mathbb{Q})[p^\infty]$ are both trivial. Therefore, $E(L_{n+1})[p^\infty]$ is trivial. □

Central to our argument is a combination of an analytic result of Rohrlich with a theorem by Kato, which we now recall.

Theorem 7.10 ([77], [48])**.** *Suppose that E is an elliptic curve defined over $\mathbb{Q}$ with good reduction at p. Then, there exists an integer $n \geq 0$ such that*

1. *$L(E, \chi, 1) \neq 0$ for every non-trivial character χ of $\mathrm{Gal}(K_{n+1}/K_n)$,*
2. *$\mathrm{rk}_p(E/K_n) = \mathrm{rk}_p(E/K_{n+1})$.*

The following result is a formal consequence of this theorem.

Theorem 7.11. *Let $E/\mathbb{Q}$ be an elliptic curve which has good reduction at p. In addition, suppose that p splits in $L_0 = \mathbb{Q}(\sqrt{-d})$. Then, there exists a positive integer n such that*

1. $\mathrm{ord}_{s=1} L(E/L_n, s) = \mathrm{ord}_{s=1} L(E/L_{n+1}, s)$,

2. $Ш(Y/L_n)$ *is finite,*

3. $\mathrm{rk}_p(E/L_{n+1}) = \mathrm{rk}_p(E/L_n)$.

Proof. As E is defined over $\mathbb{Q}$, $\mathrm{Res}_{K_n}^{L_n} E$ is isogenous to $E \times E_{-d}$ giving an equality of L-functions

$$L(E/L_n, s) = L(E/K_n, s) L(E_{-d}/K_n, s).$$

Since p splits in L_0, both E and E_{-d} have good reduction at p. By Rohrlich [77, pp. 409], the sequence $\{\mathrm{ord}_{s=1} L(E/K_n, s)\}_{n \geq 1}$ stabilises (similarly for E_{-d}). It follows that for $n \geq 1$ sufficiently large, we have $\mathrm{ord}_{s=1} L(E/L_n, s) = \mathrm{ord}_{s=1} L(E/L_{n+1}, s)$. This proves (1).

Part (2) is a consequence of a result by Kato [48], as we now explain. Following the author's notation, for an abelian group G, a character $\tau \in \widehat{G}$, and a G-module M, we let $M^{(\tau)} = \{x \in M \mid I_\tau \cdot x = 0\}$ where $I_\tau \subseteq \mathbb{Z}[G]$ denotes the kernel of the map $\mathbb{Z}[G] \to \mathbb{C}^\times$ induced by τ. We apply this to $G = \mathrm{Gal}(L_{n+1}/\mathbb{Q}) \cong \mathbb{Z}/2p^{n+1}\mathbb{Z}$. For brevity, we write $H = \mathrm{Gal}(L_{n+1}/L_n) \cong \mathbb{Z}/p\mathbb{Z}$. Further, the composition $i \circ \mathrm{Tr}$ from §7.1.2 is equal to $N_H := \sum_{h \in H} h$ viewed as an L_n-endomorphism of B/L_n. It follows that the composition $Y \hookrightarrow B \overset{N_H}{\to} B$ is the zero map, which in turn gives a homomorphism $Ш(Y/L_n) \to \ker(N_H \mid Ш(E/L_{n+1}))$ with finite kernel. To see this, we look at the short exact sequence of abelian varieties

$$0 \to Y \to B \overset{\mathrm{Tr}}{\to} E \to 0.$$

Taking Galois cohomology gives an exact sequence

$$0 \to E(L_n)/\mathrm{Norm}_{L_n}^{L_{n+1}} E(L_{n+1}) \to H^1(L_n, Y) \to H^1(L_n, B).$$

Since $pE(L_n) \subseteq \mathrm{Norm}_{L_n}^{L_{n+1}} E(L_{n+1})$ and $E(L_n)/pE(L_n)$ is finite by the Mordell–Weil theorem, then $E(L_n)/\mathrm{Norm}_{L_n}^{L_{n+1}} E(L_{n+1})$ must be finite too. As a result, the induced map $Ш(Y/L_n) \to \ker(N_H \mid Ш(E/L_{n+1}))$ has finite kernel. Thus, it suffices to show that $\ker(N_H \mid Ш(E/L_{n+1}))$ is finite. Let τ (resp., ψ) be a primitive character (resp., character of order p^{n+1}) of G. In addition, we have a short exact sequence[1]

$$0 \to Ш(E/L_{n+1})^{(\tau)} \to \ker(N_H \mid Ш(E/L_{n+1})) \to Ш(E/L_{n+1})^{(\psi)} \qquad (\star)$$

Adding on, by Artin formalism,

$$L(E/L_{n+1}, s) = L(E/L_n, s) \prod_{\substack{\chi \in \widehat{H} \\ \chi \neq \mathrm{id}}} L(E/L_n, \chi, s).$$

By part (1), there exists $n \geq 1$ such that $L(E/L_n, \chi, 1) = L(E/\mathbb{Q}, \mathrm{Ind}_H^G \chi, 1) \neq 0$ where χ is a non-trivial character of H. It follows that $L(E/\mathbb{Q}, \tau, 1) \neq 0$ and $L(E/\mathbb{Q}, \psi, 1) \neq 0$. By [48, Corollary 14.3], $Ш(E/L_{n+1})^{(\tau)}$ and $Ш(E/L_{n+1})^{(\psi)}$ in $(\star)$ are both finite . This completes the proof of (2).

For part (3), the results of Kato and Rohrlich from above show that for the choice of n as in (1), then $\mathrm{rk}_p(E/K_n) = \mathrm{rk}_p(E/K_{n+1})$ and $\mathrm{rk}_p(E_{-d}/K_n) = \mathrm{rk}_p(E_{-d}/K_{n+1})$. In addition, for all $n \geq 0$, $\mathrm{rk}_p(E/L_n) = \mathrm{rk}_p(E/K_n) + \mathrm{rk}_p(E_{-d}/K_n)$. The result follows. □

Theorem 7.12. *Let $p \geq 11$ be a prime. Then, there exists an abelian extension $L/\mathbb{Q}$ and an abelian variety Y/L such that $|Ш(Y/L)| = p \cdot \square$.*

Proof. We let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ and suppose that p is a

[1] To see this, we note that as an element in $\mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^{2p^{n+1}} - 1)$, we can factorise $N_H = \sum_{i=1}^{p-1} (t^{2p^n})^i = \Phi_{2p^{n+1}}(t) \cdot \Phi_{p^{n+1}}(t)$, where $\Phi_{2p^{n+1}}(t)$ and $\Phi_{p^{n+1}}(t)$ are the corresponding cyclotomic polynomials.

prime of good reduction. We let d be a positive integer such that p and all bad primes of $E/\mathbb{Q}$ split in $\mathbb{Q}(\sqrt{-d})$. For the remainder of this proof, we fix n as in Theorem 7.11 so that $\mathrm{rk}_p(E/L_{n+1}) = \mathrm{rk}_p(E/L_n)$ and $Ш(Y/L_n)$ are both finite. In view of Lemma 7.6(1)-(2), $|Ш(Y/L_n)| = |Ш_0(Y/L_n)[p^\infty]| \cdot \square$. Combining this with Proposition 7.7(2) (applied with $K = K_n, F = K_{n+1}, L = L_n$) and Lemma 7.9, we get

$$|Ш(Y/L_n)| \equiv p^{\mathrm{rk}_p(E/L_n)} \mod \square. \qquad (*)$$

Since E is defined over $\mathbb{Q}$, its global root number $\omega(E/\mathbb{Q}(\sqrt{-d})) = -1$. This is because the only contribution in the root number computation comes from the unique archimedean place of $\mathbb{Q}(\sqrt{-d})$. Therefore,

$$(-1)^{\mathrm{rk}_p(E/\mathbb{Q}(\sqrt{-d}))} = (-1)^{\mathrm{rk}_p(E/\mathbb{Q})+\mathrm{rk}_p(E_{-d}/\mathbb{Q})} \overset{[30,\ \mathrm{Thm}\ 1.4]}{=} w(E/\mathbb{Q})w(E_{-d}/\mathbb{Q}).$$

Since $\mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{-d})}E$ is isogenous to $E\times E_{-d}$, we deduce that $w(E/\mathbb{Q})w(E_{-d}/\mathbb{Q}) = w(E/\mathbb{Q}(\sqrt{-d}))$ and therefore $\mathrm{rk}_p(E/\mathbb{Q}(\sqrt{-d})) \equiv 1 \bmod 2$. Since the parity of p^∞-Selmer ranks remains unchanged in odd degree Galois extensions [30, Corollary 4.15], $\mathrm{rk}_p(E/L_n) \equiv \mathrm{rk}_p(E/\mathbb{Q}(\sqrt{-d})) \equiv 1 \bmod 2$. Combining this with $(*)$ gives the required result. $\square$

Theorem 7.13. *Let p be a prime. Then, there exists an abelian variety $Y'/\mathbb{Q}$ such that $|Ш(Y'/\mathbb{Q})| = p \cdot \square$.*

Proof. For $p \geq 11$, we consider $Y' = \mathrm{Res}_{\mathbb{Q}}^{L}Y$ where Y/L is the abelian variety from Theorem 7.12. Since $Ш(Y'/\mathbb{Q}) \cong Ш(Y/L)$ (combine Shapiro's lemma with [64, pp. 178(a)]), the result follows. For $p \leq 7$, see [75] and [84]. $\square$

Corollary 7.14. *For every positive square-free integer m, there exists an abelian variety defined over $\mathbb{Q}$ with finite Tate–Shafarevich group of order $m\cdot\square$.*

Proof. Given abelian varieties A_1 and A_2, $Ш(A_1 \times A_2) \cong Ш(A_1) \times Ш(A_2)$. The result follows from Theorem 7.13. $\square$

Remark 7.15. This chapter extends the main result of [84], where the author considers the isogeny decomposition of a Weil-restriction $\mathrm{Res}_{\mathbb{Q}}^{F} E \to Y \times E$ of an elliptic curve $E/\mathbb{Q}$ with $F/\mathbb{Q}$ a cyclic degree p extension. The author then shows that the parities of $\mathrm{ord}_p\,|Ш(Y/\mathbb{Q})|$ and $\mathrm{rk}(E/\mathbb{Q})$ are the same under the assumption that $L(Y/\mathbb{Q}, 1) \neq 0$. This principle is also reflected in our work through Proposition 7.7(2).

This non-vanishing assertion is then verified numerically for a specific elliptic curve and odd primes below 25000. Our approach differs by considering higher-degree cyclic extensions of $\mathbb{Q}$ and applying an analytic result of Rohrlich, which establishes a similar condition unconjecturally, thus allowing us to obtain an unconditional result.

Appendix A

Homomorphisms between Jacobians from G-maps

In this appendix, we describe a method for constructing homomorphisms between products of Jacobians starting from G-equivariant maps between permutation modules. In particular, letting $H_1, \ldots, H_m$ and $H'_1, \ldots, H'_n$ be subgroups of G, we show that a G-map

$$\Phi : \bigoplus_{i=1}^{m} \mathbb{Z}[G/H_i] \to \bigoplus_{j=1}^{n} \mathbb{Z}[G/H'_j]$$

induces a homomorphism

$$f_\Phi : \prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i},$$

which satisfies a number of desired properties.

This formalism originates from the work of Kani–Rosen [46], where the authors show that certain relations between permutation characters, now known as Brauer relations (see Definition 4.1 and Remark 4.3) give rise to isogenies between Jacobians, though an exact description of this morphism is not given. Subsequently, the work of de Smit–Edixhoven [21] constructs the induced isogeny, though only in the isogeny category of abelian varieties. A similar construction can be found in the work of Chen [17, Lemma 3.3], though

the homomorphism afforded by this lemma doesn't quite satisfy the desired properties of Theorem A.1.

The following theorem, along with all subsequent results in this appendix, is due to A. Morgan and can be found in the joint work [53, §4.3].

Theorem A.1. *Let X be a curve over a field K of characteristic 0, and let G be a finite subgroup of $\mathrm{Aut}_K(X)$. Let*

$$\Phi : \bigoplus_i \mathbb{Z}[G/H_i] \to \bigoplus_j \mathbb{Z}[G/H'_j], \quad (H_i, H'_j \leq G)$$

be a G-equivariant homomorphism. Then, there exists a K-homomorphism

$$f_\Phi : \prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i}$$

which satisfies:

1. $f_{\Phi'\Phi} = f_\Phi f_{\Phi'}$,
2. $f_{\Phi^\vee} = (f_\Phi)^\vee$.

   (Here, and below, $(f_\Phi)^\vee$ denotes the dual homomorphism of f_Φ with respect to the canonical principal polarisations, while $\Phi^\vee$ denotes the dual homomrophism of Notation 4.21.)

A.1 Construction of f_Φ

In view of the natural inclusion and projection maps in and out of permutation modules, we can assume that Φ is of the form

$$\Phi : \mathbb{Z}[G/H] \to \mathbb{Z}[G/H'].$$

We let $\sum_{g\in G} m_g g$ be any lift of $\Phi(H)$ (that is, Φ evaluated at the trivial coset) to $\mathbb{Z}[G]$, $\tilde{\Phi} := \sum_{g\in G} m_g g_*$ the induced endomorphism on Jac_X and π_H and $\pi_{H'}$ the natural quotient maps $X \to X/H$, $X \to X/H'$.

In the following lemma, we write $\mathrm{Jac}_X^{H'}$ to denote the group variety given by the H'-stable points of Jac_X, and $(\mathrm{Jac}_X^{H'})^0$ for its connected component.

Lemma A.2. *The following hold:*

1. *The image of $\pi_{H'}^*$ is contained in $(\mathrm{Jac}_X^{H'})^0$.*
2. *The restriction of $\tilde{\Phi}$ to $(\mathrm{Jac}_X^{H'})^0$ is independent of the lift chosen for $\Phi(H)$ in $\mathbb{Z}[G]$.*
3. *The image of the restriction $\tilde{\Phi}$ to $(\mathrm{Jac}_X^{H'})^0$ is contained in $(\mathrm{Jac}_X^{H})^0$.*

Proof. For (1), we note that $\pi_{H'} \circ h = \pi_{H'}$ for all $h \in H'$, and therefore $\pi_{H'}^* = h^* \circ \pi_{H'}^*$. Since $h^* = (h_*)^{-1} = (h^{-1})_*$, we deduce that H' acts trivially on $\pi_{H'}^*(\mathrm{Jac}_X)$ and so $\pi_{H'}^*(\mathrm{Jac}_X) \subseteq \mathrm{Jac}_X^{H'}$. Since $\pi_{H'}^*(\mathrm{Jac}_X)$ is connected (since Jac_X is too), then the result follows. Claim (2) follows since H' acts trivially on $(\mathrm{Jac}_X^{H'})^0$. Claim (3) follows since the image of an H'-stable point under $\tilde{\Phi}$ is point which is fixed by H. Therefore, the image of the restriction of $\tilde{\Phi}$ to $(\mathrm{Jac}_X^{H'})^0$ lies in Jac_X^H. Since $(\mathrm{Jac}_X^{H'})^0$ is connected, the result follows. □

In view of Lemma A.2, we can construct a homomorphism between Jacobians $\alpha(\Phi) : \mathrm{Jac}_{X/H'} \to \mathrm{Jac}_{X/H}$ determined by the composition:

$$\alpha(\Phi) := \left(\mathrm{Jac}_{X/H'} \xrightarrow{\pi_{H'}^*} (\mathrm{Jac}_X^{H'})^0 \xrightarrow{\tilde{\Phi}} (\mathrm{Jac}_X^{H})^0 \xrightarrow{(\pi_H)_*} \mathrm{Jac}_{X/H} \right).$$

Remark A.3. Since H' acts trivially on $(\mathrm{Jac}_X^{H'})^0$, then the restriction of the endomorphism $\tilde{\Phi} = \sum_{g \in G} m_g g_*$ of Jac_X to $(\mathrm{Jac}_X^{H'})^0$ is independent of the choice of lift for $\Phi(H)$ to $\mathbb{Z}[G]$. As a result, the definition of $\alpha(\Phi)$ is independent of specific lift chosen for $\Phi(H)$.

Lemma A.4. $\mathrm{Jac}_{X/H'}[|H|] \subseteq \mathrm{Ker}(\alpha(\Phi))$.

Proof. It suffices to prove this claim after base-change to an algebraic closure $\overline{K}$, so we assume $K = \overline{K}$. Suppose that $|H|Z = \mathrm{div}(\eta)$ for some $\eta \in K(\overline{X}/H') = K(\overline{X})^{H'}$, and that $\tilde{\Phi} = \sum_{g \in G} m_g g_*$. Consider $\zeta = \prod_{g \in G} g(\eta)^{m_g}$.

Since $\eta \in K(\overline{X})^{H'}$, it follows that $\zeta \in K(\overline{X})^H = K(\overline{X}/H)$. A direct computation then shows that $\mathrm{div}(\zeta) = \alpha(\Phi)(Z)$, from which the claim follows. $\square$

In view of Lemma A.4, we deduce that $\alpha(\Phi)$ factors through the multiplication-by-$|H|$ map; that is $\alpha(\Phi) = |H| f_\Phi$. This allows us to define $f_\Phi = \frac{1}{|H|}\alpha(\Phi)$ as the associated intermediate map.

Definition A.5. Let $\Phi : \mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$ be a G-equivariant map. We define $f_\Phi : \mathrm{Jac}_{X/H'} \to \mathrm{Jac}_{X/H}$ to be the K-homomorphism $\frac{1}{|H|}\alpha(\Phi)$.

More generally, if $\Phi : \bigoplus_i \mathbb{Z}[G/H_i] \to \bigoplus_j \mathbb{Z}[G/H'_j]$ is a G-equivariant homomorphism, then composing with the inclusions and projections in and out of permutation modules give rise to a collection of G-equivariant maps $\Phi_{ij} : \mathbb{Z}[G/H_i] \to \mathbb{Z}[G/H'_j]$. We then define $f_\Phi : \prod_j \mathrm{Jac}_{X/H'_j} \to \prod_i \mathrm{Jac}_{X/H_i}$ to be the K-homomorphism associated to the collection $(f_{\Phi_{ij}})_{i,j}$.

Proof of Theorem 5.3. Existence follows by Lemma A.4. By additivity, it suffices to prove the desired properties in the case where the G-map is of the form $\Phi : \mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$. Claim (1) follows by a direct computation; Indeed, letting $\Phi' : \mathbb{Z}[G/H'] \to \mathbb{Z}[G/\tilde{H}]$, we deduce

$$\alpha(\Phi)\alpha(\Phi') = (\pi_H)_* \tilde{\Phi}(\pi^*_{H'}(\pi_{H'})_*)\tilde{\Phi}'\pi^*_{\tilde{H}}.$$

Since $\tilde{\Phi}'\pi^*_{\tilde{H}}$ lands in $(\mathrm{Jac}_X^{H'})^0$ by Lemma A.2, we deduce that $\pi^*_{H'}(\pi_{H'})_*$ (which agrees with $\sum_{h\in H'} h_*$ in view of Lemma 2.15) is the multiplication-by-$|H'|$ map in the above composition. From this, we deduce

$$\alpha(\Phi)\alpha(\Phi') = |H'|(\pi_H)_*\tilde{\Phi}\tilde{\Phi}'\pi^*_{\tilde{H}} = |H'|(\pi_H)_*\widetilde{\Phi'\Phi}\pi^*_{\tilde{H}} = |H'|\alpha(\Phi'\Phi).$$

Dividing both sides $|H| \cdot |H'|$ (which is allowed in view of Lemma A.4) gives $f_\Phi f_{\Phi'} = f_{\Phi'\Phi}$ completing the proof of (1).

To prove claim (2), we use the description $\mathrm{Hom}_G(\mathbb{Z}[G/H], \mathbb{Z}[G/H\prime]) \cong \mathbb{Z}[H\backslash G/H\prime]$ as a Hecke algebra. In particular, for a double coset HgH', we define $\Phi_{HgH'} : \mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$ to be the homomorphism determined by

$\Phi_{HgH'}(H) = \sum_{u \in H/H\cap gH'g^{-1}} ugH'$. It thus suffices to prove claim (2) in the case where $\Phi = \Phi_{HgH'}$.

A direct calculation shows that, for any $g \in G$, we have

$$\Phi_{HgH'}^\vee = \Phi_{H'g^{-1}H}. \tag{A.1}$$

Writing $N_H = \sum_{h\in H} h \in \mathbb{Z}[G]$, we note that in $\mathbb{Z}[G]$ we have the identity

$$\sum_{u\in H/H\cap gH'g^{-1}} ugN_{H'} = \sum_{t\in HgH'} t = \sum_{w\in H'/H'\cap g^{-1}Hg} N_H gw. \tag{A.2}$$

From (A.2) we see that $\sum_{t\in HgH'} t$ is a lift of $|H'|\Phi_{HgH'}(H)$ to $\mathbb{Z}[G]$. In particular, writing $\gamma = \sum_{t\in HgH'} t_*$, we have

$$|H||H'|f_{\phi_{HgH'}} = (\pi_H)_* \circ \gamma \circ \pi_{H'}^*.$$

Dualising gives

$$|H||H'|f_{\phi_{HgH'}}^\vee = (\pi_{H'})_* \circ \gamma^\vee \circ \pi_H^*.$$

Since $\gamma^\vee = \sum_{t\in HgH'}(t^{-1})_* = \sum_{t\in H'g^{-1}H} t_*$ and $\sum_{t\in H'g^{-1}H} t$ is a lift of $|H|\Phi_{H'g^{-1}H}(H')$ to $\mathbb{Z}[G]$ (see (A.2) we see that), we deduce that

$$|H||H'|f_{\phi_{HgH'}}^\vee = \alpha(|H|\Phi_{H'g^{-1}H}) = |H|\alpha(\Phi_{H'g^{-1}H}).$$

Dividing by $|H||H'|$ (which is allowed in view of Lemma A.4), we deduce that $f_{\Phi_{HgH'}}^\vee = f_{\Phi_{H'g^{-1}H}}$. The result follows from (A.1). □

Bibliography

[1] M. Artin, A. Grothendieck, J.-L. Verdier. *Théorie des topos et cohomologie étale des schémas (SGA4), Vol. 3.* Lect. Notes in Math. 305, Springer, 1973. 49, 67

[2] A. Bartel. *On Brauer–Kuroda type relations of S-class numbers in dihedral extensions.* J. Reine Angew. Math. 668 (2012), 211–244. 17, 60, 64

[3] A. Bartel, A. Page. *Torsion homology and regulators of isospectral manifolds.* Journal of Topology 9 (2016), 1237–1256. 18

[4] J. Bertin. *Algebraic stacks with a view toward moduli stacks of covers.* Arithmetic and geometry around Galois theory, volume 304 of Progr. Math. (2013), 1—148. Birkhäuser/Springer, Basel. 97

[5] M. Bhargava, A. Shankar. *Ternary Cubic Forms Having Bounded Invariants, and the Existence of a Positive Proportion of Elliptic Curves Having Rank 0.* Annals of Mathematics 181, no. 2 (2015), 587–621. 10

[6] B. J. Birch. *Conjecture Concerning Elliptic Curves.* Journal of the London Mathematical Society 35 (1960), 274–280. 22

[7] B. J. Birch, N. M. Stephens. *The Parity of the Rank of the Mordell–Weil Group.* Topology 5 (1966), 295–299. 21

[8] R. Brauer. *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers.* Mathematische Nachrichten 4 (1951), 158–174. 17

[9] N. Bruin, K. Doerksen. *The arithmetic of genus two curves with (4, 4)-split Jacobians.* Canadian Journal of Mathematics 63(5) (2011), 992–1024. 86, 87, 88

[10] N. Bruin, E. Flynn. *n-covers of hyperelliptic curves.* Math. Proc. Cambridge Philos. Soc. 134 (2003), 397—405. 18

[11] N. Bruin, E. Sertöz. *Prym varieties of genus four curves.* Transactions of the American Mathematical Society 373(1) (2020), 149–183. 89, 90, 91

[12] J. W. S. Cassels. *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung.* Journal für die reine und angewandte Mathematik 211 (1962), 95–112. 16, 23, 107

[13] J. W. S. Cassels. *Arithmetic on Curves of Genus 1. III. The Tate–Shafarevich and Selmer Groups.* Proceedings of the London Mathematical Society 12 (1962), 259–296.

[14] J. W. S. Cassels. *Arithmetic on Curves of Genus 1. VIII. On Conjectures of Birch and Swinnerton-Dyer.* Journal für die reine und angewandte Mathematik 217 (1965), 180–199. 22, 23, 26

[15] K. Česnavičius. *The p-parity conjecture for elliptic curves with a p-isogeny.* Journal für die reine und angewandte Mathematik (Crelle's Journal) 719 (2016), 45–73. 21

[16] I. Chen. *The Jacobians of Non-Split Cartan Modular Curves.* Proceedings of the London Mathematical Society, 77(1) (1998), 1–38. 19

[17] I. Chen. *On relations between Jacobians of certain modular curves.* Journal of Algebra 231 (2000), 414–448. 18, 114

[18] M. Chou, H. B. Daniels, I. Krijan, F. Najman. *Torsion groups of elliptic curves over the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$.* New York Journal of Mathematics 27 (2021), 99–123. 109

[19] J. Coates, T. Fukaya, K. Kato, R. Sujatha. *Root numbers, Selmer groups, and non-commutative Iwasawa theory.* J. Algebraic Geom. 19 (2010), 19–97. 22, 25, 26

[20] B. Conrad, O. Gabber, G. Prasad. *Pseudo-reductive groups*, 2nd ed. Cambridge University Press (2015). 107, 108

[21] B. de Smit, B. Edixhoven. *Sur un résultat d'Imin Chen.* Mathematical Research Letters 7 (2000), 147–153. 19, 82, 114

[22] B. de Smit. *Brauer-Kuroda relations for S-class numbers.* Acta Arithmetica 98 (2001), 133–146. 17

[23] F. Diamond, J. Shurman. *A First Course in Modular Forms.* Graduate Texts in Mathematics, vol. 228. Springer (2005). 93

[24] C. Diem, N. Naumann. *On the structure of Weil restrictions of abelian varieties.* J. Ramanujan Math. Soc. 18 (2003), 153–174. 37

[25] J. Docking. 2^∞-*Selmer rank parities via the Prym construction.* Preprint, arXiv:2108.09564v2 (2023). 26

[26] R. Donagi. *The fibers of the Prym map.* Contemp. Math. 136 (1992), 55–125. 87, 88, 89, 90

[27] T. Dokchitser, V. Dokchitser. *Parity of ranks for elliptic curves with a cyclic isogeny.* J. Number Theory 128, no. 3 (2008), 662–679. 21, 23, 26

[28] T. Dokchitser, V. Dokchitser. *Regulator constants and the parity conjecture.* Invent. Math. 178, no. 1 (2009), 23–71. 18, 28, 52, 53, 54, 57, 58, 59

[29] T. Dokchitser, V. Dokchitser. *Self-duality of Selmer groups.* Math. Proc. Cam. Phil. Soc. 146, no. 2 (2009), 257–267. 50, 60, 63, 73

[30] T. Dokchitser, V. Dokchitser. *On the Birch–Swinnerton-Dyer quotients modulo squares*. Annals of Math. 172, no. 1 (2010), 567–596. 11, 18, 21, 22, 26, 50, 51, 74, 102, 105, 112

[31] T. Dokchitser, V. Dokchitser. *Root Numbers and Parity of Ranks of Elliptic Curves*. Journal für die reine und angewandte Mathematik 658 (2011), 39–64. 12, 15, 21, 22, 27

[32] V. Dokchitser, H. Green, A. Konstantinou, A. Morgan. *Parity of ranks of Jacobians of curves*. Preprint, arXiv:2211.06357v2 (2024). 27, 59

[33] V. Dokchitser, C. Maistret. *On the parity conjecture for abelian surfaces*. Proceedings of the London Mathematical Society 127(2) (2019), 295–365. 12, 22, 26, 86

[34] B. Edixhoven, G. van der Geer, B. Moonen. *Abelian Varieties*. Available at: `http://van-der-geer.nl/~gerard/AV.pdf`.

[35] J. S. Ellenberg. *Endomorphism algebras of Jacobians*. Advances in Mathematics 162, no. 2 (2001), 243–271. 45, 47, 99

[36] M. Flach. *A generalisation of the Cassel-Tate pairing*. Journal für die reine und angewandte Mathematik 412 (1990), 113–127. 16

[37] E. V. Flynn, A. Shnidman (with an appendix by T. Fisher). *Arbitrarily large p-torsion in Tate–Shafarevich groups*. Journal of the Institute of Mathematics of Jussieu (2024), 1–22. 17

[38] T. Fisher. Appendix to *Root numbers of non-abelian twists of elliptic curves* by V. Dokchitser. Proc. London Math. Soc., no. 2 (2005), 300–324. 22

[39] G. Frey, E. Kani. *Curves of Genus 2 Covering Elliptic Curves and an Arithmetical Application*. In Arithmetic Algebraic Geometry. Birkhäuser Boston (1991), 153–176. 94

[40] G. Frey, E. Kani. *Curves of genus 2 with elliptic differentials and associated Hurwitz spaces*. Contemporary Mathematics (2009), 14. 96

[41] A. Gallese. *How to split two-dimensional Jacobians: a geometric construction*. Preprint, arXiv:2412.07414v1 (2024). 99

[42] H. Green, C. Maistret. *The 2-parity conjecture for elliptic curves with isomorphic 2-torsion*. Proc. of the Royal Soc. A 478, no. 2265 (2022). 21, 22, 26

[43] R. Greenberg. *On the Birch and Swinnerton-Dyer Conjecture*. Inventiones Mathematicae 72 (1983), 241–265. 21

[44] L. Guo. *General Selmer Groups and Critical Values of Hecke L-functions*. Mathematische Annalen 297 (1993), 221–233. MR 95b:11064 Zbl 0789.14018. 21

[45] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, Berlin (1967). 97

[46] E. Kani, M. Rosen. *Idempotent relations and factors of Jacobians*. Math. Ann. 284, no. 2 (1989), 307–327. 18, 82, 114

[47] K. Kato, F. Trihan. *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*. Inventiones mathematicae 153 (2003), 537–592. 15

[48] K. Kato. *p-adic Hodge theory and values of zeta functions of modular forms*. Astérisque 295 (2004), 117–290. 15, 109, 110, 111

[49] S. Keil. *Examples of non-simple abelian surfaces over the rationals with non-square order Tate–Shafarevich group*. Journal of Number Theory 144 (2014), 25–69. 17

[50] B. Du Kim. *The parity conjecture for elliptic curves at supersingular reduction primes*. Compos. Math. 143, no. 1 (2007), 47–72. 21

[51] S. L. Kleiman. *The Picard scheme*. Fundamental algebraic geometry (2005), 235–321. 36

[52] V. A. Kolyvagin. *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil Curves*. In: Mathematics of the USSR-Izvestiya 32.3 (1989), 523–541. Available at `http://stacks.iop.org/0025-5726/32/i=3/a=A04`. 15

[53] A. Konstantinou, A. Morgan. *On Galois covers of curves and arithmetic of Jacobians*. Preprint, arXiv:2407.18258 (2024). 30, 35, 36, 37, 38, 39, 41, 47, 70, 72, 73, 74, 77, 85, 87, 93, 97, 115

[54] K. Kramer. *Arithmetic of elliptic curves upon quadratic extension*. Trans. Amer. Math. Soc. 264, no. 1 (1981), 121–135. 21, 22, 26

[55] K. Kramer, J. Tunnell. *Elliptic curves and local ϵ-factors*. Compos. Math. 46 (1982), 307–352. 12, 21

[56] S. Kuroda. *Über die Klassenzahlen algebraischer Zahlkörper*. Nagoya Mathematical Journal 1 (1950), 1–10. 17

[57] R. M. Kuhn. *Curves of genus 2 with split Jacobian*. Transactions of the American Mathematical Society 307, no. 1 (1988), 41–49. 20, 95, 96, 98

[58] Q. Liu. *Algebraic geometry and arithmetic curves*. Volume 6 of Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford (2002). 31

[59] D. Lombardo, E. Lorenzo García, C. Ritzenthaler, J. Sijsling. *Decomposing Jacobians via Galois covers*. Experimental Mathematics 32(1) (2023), 218–240. 97, 99

[60] B. Mazur, K. Rubin, A. Silverberg. *Twisting Commutative Algebraic Groups*. Journal of Algebra 314 (2007), 419–438. 20, 102

[61] B. Mazur, K. Rubin. *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Inventiones mathematicae 181 (2010), 541–575. 10

[62] B. Mazur, K. Rubin. *Finding large Selmer rank via an arithmetic theory of local constants*. Ann. of Math. 166 (2007), 579–612. 22, 26

[63] B. Mazur (with an appendix by D. Goldfeld). *Rational isogenies of prime degree.* Inventiones mathematicae 44 (1978), 129–162. 109

[64] J. S. Milne. *On the arithmetic of abelian varieties.* Inventiones mathematicae 17 (1972), 177–190. 102, 107, 108, 112

[65] J. S. Milne. *Arithmetic Duality Theorems.* Academic Press, Inc., Boston, Mass. (1986). 73, 106

[66] J. S. Milne. *Abelian varieties.* In Arithmetic geometry, Springer, New York, NY (1986), 103–150. 49, 70

[67] J. S. Milne. *Jacobian varieties.* In Arithmetic geometry, Springer, New York, NY (1986), 167–212. 36, 37, 38

[68] R. Miranda. *Algebraic curves and Riemann surfaces.* Vol. 5. American Mathematical Soc. (1995). 96

[69] P. Monsky. *Generalizing the Birch-Stephens Theorem. I. Modular Curves.* Mathematische Zeitschrift 221 (1996), 415–420. 21, 22

[70] A. Morgan. *2-Selmer parity for hyperelliptic curves in quadratic extensions.* Proceedings of the London Mathematical Society (2022). 12, 22, 26

[71] J. Nekovář. *Selmer complexes.* Astérisque 310 (2006). 21

[72] J. Nekovář. *Some consequences of a formula of Mazur and Rubin for arithmetic local constants.* Algebra Number Theory 7, no. 5 (2013), 1101–1120. 21

[73] J. Nekovář. *Compatibility of arithmetic and algebraic local constants (the case $l \neq p$).* Compos. Math. 151, no. 9 (2015), 1626–1646. 21

[74] J. Nekovář. *Compatibility of arithmetic and algebraic local constants II. The tame abelian potentially Barsotti-Tate case.* Preprint (2016).

Available at `https://webusers.imj-prg.fr/~jan.nekovar/pu/tame.pdf`. 21

[75] B. Poonen, M. Stoll. *The Cassels-Tate pairing on polarized abelian varieties*. Annals of Mathematics (1999), 1109–1149. 16, 41, 42, 107, 112

[76] I. Reiner. *Maximal Orders*. Academic Press, New York, 1975. 70

[77] D. Rohrlich. *On L-functions of elliptic curves and cyclotomic towers*. Inventiones mathematicae 75, no. 3 (1984), 409–423. 109, 110

[78] E. F. Schaefer. *Class groups and Selmer groups*. Journal of Number Theory 56, no. 1 (1996), 79–114. 25, 26, 106

[79] J. P. Serre. *Linear representations of finite groups*. Vol. 42. New York: Springer (1977). 49, 54, 70

[80] T. Shioda. *Some remarks on abelian varieties*. Journal of the Faculty of Science, University of Tokyo, Section IA 24 (1977), 11–21. 94

[81] A. Shnidman, A. Weiss. *Elements of prime order in Tate–Shafarevich groups of abelian varieties over* $\mathbb{Q}$. Forum of Mathematics, Sigma, 10 (2022), e98. 17

[82] B. A. Smith. *Explicit endomorphisms and correspondences*. PhD Thesis, University of Cambridge (2005). 86

[83] The stacks project authors. Stacks project. Available at `https://stacks.math.columbia.edu`, (2018). 31

[84] W. A. Stein. *Shafarevich–Tate groups of nonsquare order*. In Modular Curves and Abelian Varieties 2002 Barcelona Conference Proceedings, Birkhäuser Progress in Mathematics 224 (2004), 277–289. 16, 106, 112, 113

[85] H. Stichtenoth. *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media (2009). 98

[86] J. Tate. *Duality theorems in Galois cohomology over number fields.* Proceedings of the International Congress of Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm (1963), 288–295. 16

[87] J. Tate. *On the Conjectures of Birch and Swinnerton-Dyer and a Geometric Analog.* In Séminaire Bourbaki, Vol. 9. Soc. Math. France, Paris (1995), 415–440. 23