

# The Parity Conjecture for Hyperelliptic Curves

*Holly Green*

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

November 29, 2023

I, Holly Green, 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 3 (§3, §4, §5) and 4 are the result of joint work with Vladimir Dokchitser, Alexandros Konstantinou and Adam Morgan. Chapter 6 is the result of joint work with Céline Maistret. Chapter 8 is the result of joint work with Vladimir Dokchitser and Adam Morgan.

# Abstract

The Birch and Swinnerton-Dyer conjecture famously predicts that the rank of an elliptic curve, or more generally an abelian variety, can be computed from its  $L$ -function. A consequence of this, known as the parity conjecture, is a purely arithmetic result which bypasses the conjectural theory of  $L$ -functions and asserts that the parity of the rank is determined by the root number.

This thesis investigates the parity conjecture for Jacobians of hyperelliptic curves and collates some of the first pieces of evidence (beyond elliptic curves) for the Birch and Swinnerton-Dyer conjecture. In doing this, we exhibit formulae for the parity of the rank of certain abelian varieties which use only the local theory of curves.

# Impact Statement

The Birch and Swinnerton-Dyer conjecture is considered one of the most challenging problems in modern mathematics, marrying the two main streams of number theory. Despite being formulated in the 1960s, a proof of this result still appears out of our reach. In the setting of elliptic curves, there is plenty of theoretical and numerical evidence in support of the conjecture, however, this is lacking when we consider higher dimensional abelian varieties. This thesis provides theoretical evidence in the context of Jacobians of hyperelliptic curves. This is achieved by considering the parity of their ranks, for which we provide recipes that serve as useful computational tools.

Outside of academia, number theory plays a fundamental role in the development of cryptographic algorithms. Many of these rely on objects studied in this thesis, namely, elliptic curves, hyperelliptic curves, and isogenies. Whilst this is not the purpose of the thesis, and such applications are not discussed here, some of the ideas we present could be of interest to cryptographers.

# Acknowledgements

My most sincere gratitude goes to my supervisor, Vladimir Dokchitser, not only for suggesting the problems discussed in this thesis but also for dedicating uncountably many hours to (very patiently) discussing mathematics with me.

This thesis would look very different were it not for my brilliant collaborators: Alexandros Konstantinou, Céline Maistret and Adam Morgan, to whom I would like to express my thanks. I would also like to acknowledge Tim Dokchitser, Omri Faraggi, and Sarah Millard, for the insightful discussions we shared, and my examiners Richard Hill and Ariel Pacetti, for their useful comments.

To my wonderful friends: Calum, Ellie, Erik, Sarah, Lilybelle, Alex, Reva and Bea – your support, company and sense of humour have made the last four years so much more enjoyable. I am deeply indebted to you all.

Last but not least, I am always thankful for the continuous support and encouragement given to me by my mum, my dad and my (favourite) sister Chloe.

This work was supported by University College London and the Engineering and Physical Sciences Research Council [EP/R513143/1].

# UCL Research Paper Declaration Form

1. **For a research manuscript that has already been published** (if not yet published, please skip to section 2):
  - (a) **What is the title of the manuscript?** The 2-parity conjecture for elliptic curves with isomorphic 2-torsion
  - (b) **Please include a link to or doi for the work:**  
<https://doi.org/10.1098/rspa.2022.0112>
  - (c) **Where was the work published?** Proceedings of the Royal Society A
  - (d) **Who published the work?** The Royal Society
  - (e) **When was the work published?** 07/09/2022
  - (f) **List the manuscript's authors in the order they appear on the publication:** Holly Green and Céline Maistret
  - (g) **Was the work peer reviewed?** Yes
  - (h) **Have you retained the copyright?** No
  - (i) **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** Yes,  
<https://doi.org/10.48550/arXiv.2110.06718>
  
2. **For a research manuscript prepared for publication but that has not yet been published** (if already published, please skip to section 3):

- (a) **What is the current title of the manuscript?**
- (b) **Has the manuscript been uploaded to a preprint server ‘e.g. medRxiv’?**

If ‘Yes’, please please give a link or doi:

- (c) **Where is the work intended to be published?**
- (d) **List the manuscript’s authors in the intended authorship order:**
- (e) **Stage of publication:**

3. **For multi-authored work, please give a statement of contribution covering all authors** (if single-author, please skip to section 4): Each author contributed an equal share. The research was carried out jointly (as is typical in pure mathematics) and therefore cannot be separated between the authors by section or by theme

4. **In which chapter(s) of your thesis can this material be found?** Chapters 6 and 7

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

**Candidate:** Holly Green

**Date:** 20/09/2023

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

**Date:**

# Contents

<b>1</b>	<b>Introduction</b>	<b>10</b>
1.1	The Birch and Swinnerton-Dyer and parity conjectures . . . . .	11
1.2	Local formulae . . . . .	14
1.3	Results of thesis . . . . .	16
1.4	Structure of thesis . . . . .	25
1.5	Notation . . . . .	26
<b>2</b>	<b>Preliminaries</b>	<b>28</b>
2.1	Curves and their Jacobians . . . . .	28
2.2	Weil restriction of abelian varieties . . . . .	35
2.3	Birch and Swinnerton-Dyer invariants . . . . .	36
2.4	Cluster pictures for hyperelliptic and bihyperelliptic curves . . . . .	40
2.5	Brauer relations . . . . .	46
2.6	Regulator constants . . . . .	48
2.7	Hilbert symbols . . . . .	49
<b>3</b>	<b>Automorphisms, Brauer Relations and Isogenies</b>	<b>51</b>
3.1	Counting points . . . . .	51
3.2	Exhibiting isogenies from Brauer relations . . . . .	54
3.3	Explicit construction of isogenies for $C_2 \times C_2$ . . . . .	58
3.4	Explicit construction of isogenies for $S_3$ . . . . .	62
3.5	The general construction . . . . .	65



<b>4</b>	<b>Determining Parities of Ranks of Jacobians of Curves</b>	<b>69</b>
4.1	Parities of ranks of isogenous elliptic curves . . . . .	70
4.2	Rank parity formulae . . . . .	71
4.3	Rank parity formulae for $C_2 \times C_2$ . . . . .	76
4.4	Rank parity formulae for $S_3$ . . . . .	78
4.5	Selmer group analogue . . . . .	82
<b>5</b>	<b>The Parity Conjecture for Elliptic Curves</b>	<b>84</b>
5.1	Global results . . . . .	85
5.2	Proof of Local Theorem I . . . . .	87
<b>6</b>	<b>The <math>p</math>-Parity Conjecture for Elliptic Curves over Totally Real Fields</b>	<b>93</b>
6.1	Strategy . . . . .	94
6.2	Proof of Local Theorem II . . . . .	96
6.3	The 2-parity conjecture for elliptic curves with isomorphic 2-torsion . . . . .	105
6.4	The $p$ -parity conjecture for elliptic curves over totally real fields . . . . .	107
<b>7</b>	<b>A Conjecture Concerning Hyperelliptic Curves</b>	<b>109</b>
7.1	Sturm polynomials . . . . .	110
7.2	Conjecture based on experimental data . . . . .	111
<b>8</b>	<b>The Parity Conjecture for Hyperelliptic Curves</b>	<b>121</b>
8.1	Reducing the problem to curves with nice automorphisms . . . . .	123
8.2	Controlling the parity of the rank . . . . .	124
8.3	Exhibiting an error term . . . . .	129
8.4	Proof of Local Theorem III . . . . .	135
8.5	Proof of Local Theorem IV . . . . .	149
8.6	Global consequences . . . . .	162
	<b>Bibliography</b>	<b>170</b>

# Chapter 1

## Introduction

Understanding the rational points on varieties defined over the rational numbers is the modern perspective on the theory of Diophantine equations which dates back to the 3rd century. More recently, this study has been extended to varieties over number fields. Around the 1900s, it was observed that a group law can be defined on the points of an elliptic curve and in the 1920s, Mordell and Weil proved the following breakthrough result concerning the group structure (which can also be stated for the Jacobian associated to a curve, or more generally, an abelian variety).

**Theorem** (Mordell–Weil). *Let  $E$  be an elliptic curve over a number field  $K$ . The  $K$ -rational points of  $E$  form a finitely generated abelian group, i.e.*

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

for some  $\text{rk}(E) \in \mathbb{N}$  called the rank of  $E$ , and some finite group  $E(K)_{\text{tors}}$  called the torsion subgroup of  $E(K)$ .

In light of this theorem, whether an elliptic curve has finitely many or infinitely many points is determined by its rank. However, very little is known about this global invariant, and currently, there is no effective method for its calculation. Number theorists have often observed that global information about varieties can be deduced from ‘piecing together’ local information, which involves studying varieties over local fields such as  $\mathbb{C}$ ,  $\mathbb{R}$  and  $\mathbb{Q}_p$ . The Hasse–Minkowski Theorem is a classical example of this technique, stating that two quadratic forms over a number field are equivalent

if and only if they are equivalent over every local completion of the field. In this thesis, we will demonstrate that the parity of the rank of various abelian varieties can be determined from local information. While the formulae we provide serve as useful computational tools, they also offer some of the first pieces of evidence (beyond elliptic curves) for the renowned Birch and Swinnerton–Dyer conjecture.

## 1.1 The Birch and Swinnerton-Dyer and parity conjectures

In the 1960s, Birch and Swinnerton-Dyer proposed a local description of the rank of an elliptic curve by relating it to the number of points on the reduction of the curve over finite fields. This local data is encoded in the associated  $L$ -function (a meromorphic function on the complex plane).

**Conjecture** (Birch and Swinnerton-Dyer [4, 5], Tate [66]). *Let  $A$  be an abelian variety over a number field  $K$ . Assuming that  $L(A, s)$  has an analytic continuation to  $\mathbb{C}$ ,*

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

This conjecture is regarded as one of the most challenging mathematical problems and has currently only been proved in special cases. In particular, it is known to hold for modular elliptic curves (those whose  $L$ -functions are known to have an analytic continuation) such that the order of vanishing of their  $L$ -function at  $s = 1$  is at most 1 ([30], [35]). Virtually nothing is known for abelian varieties of dimension greater than 1, and the numerical evidence is much more limited. In this thesis, we consider the Birch and Swinnerton-Dyer conjecture for Jacobians of hyperelliptic curves, the first natural family of curves to look at after elliptic curves.

As indicated by the Birch and Swinnerton-Dyer conjecture, the  $L$ -function of an abelian variety is conjectured to have an analytic continuation and to satisfy a functional equation.

**Conjecture** (Hasse–Weil, see [58]). *Let  $A$  be an abelian variety of dimension  $n$  over a number field  $K$  of degree  $d$ . The  $L$ -function  $L(A, s)$  has an analytic continuation*

to the whole of  $\mathbb{C}$ , and

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

where  $w(A) \in \{\pm 1\}$  is the global root number of  $A$ , and

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

with  $N_A$  the conductor of  $A$  and  $\Delta_K$  the discriminant of  $K$ .

Since this essentially says that  $L(A, 2 - s) = w(A)L(A, s)$ , we can observe that the root number controls the parity of the order of vanishing of  $L(A, s)$  at  $s = 1$ . Combining this with the Birch and Swinnerton-Dyer conjecture yields the ‘Birch and Swinnerton-Dyer conjecture modulo 2’, more commonly referred to as the parity conjecture.

**Conjecture** (The parity conjecture). *Let  $A$  be an abelian variety over a number field  $K$ . Then*

$$(-1)^{\text{rk}(A)} = w(A).$$

The appeal of the parity conjecture is that it is a purely arithmetic statement which does not involve the conjectural theory of  $L$ -functions. It provides an effective, local method to compute the parity of the rank because the global root number is defined as a product of local root numbers and these can be computed via the local Galois representations of  $A$ . We note that knowing the parity of the rank is sometimes enough to assert that an abelian variety has infinitely many points; for instance, if the rank is odd, then it is non-zero.

While the parity conjecture may seem like a straightforward statement, there is currently no known successful approach to resolve it unconditionally. The challenge arises from our limited understanding of the rank of an abelian variety. In particular, distinguishing the points on an abelian variety from the elements of a (potentially infinite) group known as the Shafarevich–Tate group, denoted  $\text{III}(A)$ , poses significant difficulties. With this in mind, a weaker version of the parity conjecture concerning

the  $p^\infty$ -Selmer rank of an abelian variety, denoted  $\mathrm{rk}_p(A)$ , has been formulated.

**Conjecture** (The  $p$ -parity conjecture). *Let  $p \in \mathbb{Z}$  be a prime and  $A$  be an abelian variety over a number field  $K$ . Then*

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

In certain settings, the parity of the  $p^\infty$ -Selmer rank is computable and this can lead to a proof of the  $p$ -parity conjecture. Most notably, the  $p$ -parity conjecture is known for elliptic curves over the rationals ([19]), for elliptic curves over number fields admitting a  $p$ -isogeny ([20], [8]), for elliptic curves over totally real number fields when  $p \neq 2$  (and in all non-complex multiplication cases and some complex multiplication cases when  $p = 2$ ) ([20],[48],[49],[50],[51]) and for quadratic twists of elliptic curves ([37]). However, the  $p$ -parity conjecture remains an open problem for elliptic curves over general number fields. In higher dimensions, the 2-parity conjecture is known for Jacobians of hyperelliptic curves that are base-changed from a subfield of index 2 ([47]), and for odd  $p$ , the  $p$ -parity conjecture is known for abelian varieties admitting a suitable isogeny ([9]).

When  $\#\mathrm{III}(A)$  (or more specifically  $\#\mathrm{III}(A)[p^\infty]$ ) is finite, then  $\mathrm{rk}_p(A) = \mathrm{rk}(A)$ , and thus the  $p$ -parity conjecture implies the parity conjecture. Therefore, as consequences of the aforementioned cases of the  $p$ -parity conjecture, corresponding cases of the parity conjecture have been proven, assuming the finiteness of relevant parts of the Shafarevich–Tate group. Furthermore, assuming finiteness of the  $p$ -primary part of the Shafarevich–Tate group for several primes  $p$ , the parity conjecture is known to hold over general number fields for elliptic curves ([20]) and for principally polarized abelian surfaces subject to certain local conditions ([24]).

Without knowing that  $L$ -functions have an analytic continuation, this is the only theoretical evidence we have for the Birch and Swinnerton-Dyer conjecture for abelian varieties of dimension greater than 1. The motivation behind the work presented in this thesis is to offer additional supporting evidence, specifically in the form of the parity conjecture for Jacobians of hyperelliptic curves of arbitrary genus.

## 1.2 Local formulae

Developing methods to describe the global behaviour of varieties locally (varieties are better understood over local fields) has received a lot of attention since the early 20th century. The parity conjecture provides such a method, predicting that

$$(-1)^{\text{rk}(A)} = w(A) := \prod_{v \text{ place of } K} w_v(A)$$

for an abelian variety  $A$  over a number field  $K$ , where the local root numbers  $w_v(A)$  can be determined from viewing  $A$  over the local field  $K_v$ . We refer to this as a *local formula for the parity of the rank*.

**Example 1.2.1.** Let  $C : y^2 = x^6 - 2x^2 + 5$ . Using Sage [63], we compute that

$$w_p(\text{Jac}_C) = w_\infty(\text{Jac}_C) = +1 \quad \text{for each prime } p \in \mathbb{Z}.$$

Therefore,  $w(\text{Jac}_C/\mathbb{Q}) = +1$  and the parity conjecture predicts that  $\text{rk}(\text{Jac}_C/\mathbb{Q})$  is even.

Now consider the variety over  $\mathbb{Q}(\sqrt{17})$ . Then

$$w_v(\text{Jac}_C) = +1 \quad \text{for each place } v \neq 5, \quad \text{and} \quad w_5(\text{Jac}_C) = -1$$

(note that 5 is inert). In this case,  $w(\text{Jac}_C/\mathbb{Q}(\sqrt{17})) = -1$  and the parity conjecture instead predicts that  $\text{rk}(\text{Jac}_C/\mathbb{Q}(\sqrt{17}))$  is odd, i.e.  $\text{Jac}_C$  has infinitely many  $\mathbb{Q}(\sqrt{17})$ -points.

In particular, assuming the parity conjecture, we're able to conclude that  $\text{Jac}_C$  has points of infinite order which are defined over  $\mathbb{Q}(\sqrt{17})$  but not over  $\mathbb{Q}$ .

One of the goals of this thesis is to construct analogous local formulae which hold independently of the Birch and Swinnerton-Dyer conjecture.

Soon after the formulation of the Birch and Swinnerton-Dyer conjecture, Birch commented (and Cassels formalised) that the parity of the rank of an elliptic curve admitting an isogeny can be controlled via local arithmetic ([3]). In light of this,

isogenies have since been extensively used to derive local formulae for the parity of various ranks ([36], [47], [24], [14], [19], [40]). In this thesis, we construct isogenies involving Jacobians of hyperelliptic curves of arbitrary genus and explain how, in a similar vein to the aforementioned works, we can control the parity of the rank locally.

To give the reader a flavour, let  $K$  be a number field,  $f(x) \in K[x]$  be a separable cubic with  $f(0) \neq 0$  and consider the genus 2 curve  $C : y^2 = f(x^2)$ . We will see (Theorem 6.1.3 & Remark 6.1.4) that

$$\mathrm{rk}_2(\mathrm{Jac}_C) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2 \lambda_v(f, x) \pmod{2}$$

where for  $v \nmid 2\infty$

$$\mathrm{ord}_2 \lambda_v(f, x) = \mathrm{ord}_2 c_v(E) + \mathrm{ord}_2 c_v(\mathrm{Jac}_{E'}) - \mathrm{ord}_2 c_v(\mathrm{Jac}_C) - \mathrm{ord}_2 \mu_v(C)$$

with  $E : y^2 = f(x)$ ,  $E' : y^2 = xf(x)$  and  $c_v, \mu_v$  the local Tamagawa number and deficiency term (Definition 2.3.9) at  $v$ .

### 1.2.1 Comparing local formulae

We are able to observe that the local recipe for the parity of the  $2^\infty$ -Selmer rank of  $\mathrm{Jac}_C$  given above differs from the one provided by the 2-parity conjecture.

**Example 1.2.2.** Let  $f(x) = x^3 - 2x + 5 \in \mathbb{Q}[x]$  so that  $C : y^2 = x^6 - 2x^2 + 5$ . Using Sage [63] and that  $(1, 2) \in C(\mathbb{Q})$ ,

$$c_5(E) = 1, \quad c_5(\mathrm{Jac}_{E'}) = 2, \quad c_5(\mathrm{Jac}_C) = 1, \quad \mu_5(C) = 1.$$

Therefore,

$$(-1)^{\mathrm{ord}_2 \lambda_5(f, x)} = -1 \neq w_5(\mathrm{Jac}_C) = +1.$$

It turns out that  $\mathrm{ord}_2 \lambda_v(f, x)$  is odd precisely when  $v = 5$  or  $\infty$ , resulting in  $\mathrm{rk}(\mathrm{Jac}_C/\mathbb{Q})$  being even. Miraculously, despite the constructions being different on a local level, this global prediction aligns with the one given by the parity conjecture

(see Example 1.2.1).

We can show that the local term  $(-1)^{\text{ord}_2 \lambda_v(f,x)}$  only ever differs from  $w_v(\text{Jac}_C)$  at an even number of places  $v$  of  $K$ . Using this fact, we can then deduce the 2-parity conjecture for  $\text{Jac}_C$  from our local formula. In particular,

$$(-1)^{\text{rk}_2(\text{Jac}_C)} = \prod_{v \text{ place of } K} (-1)^{\text{ord}_2 \lambda_v(f,x)} = (-1)^{\text{even}} \prod_{v \text{ place of } K} w_v(\text{Jac}_C) = w(\text{Jac}_C).$$

More generally, the bulk of any argument deducing the parity conjecture from an arbitrary local formula for the parity of the rank is in finding a suitable ‘local error term’  $H_v \in \{\pm 1\}$ . The error term should describe the difference between the local terms appearing in these two constructions at each place  $v$ ; for instance, in the context of the discussion above, we mean finding  $H_v$  satisfying

$$(-1)^{\text{ord}_2 \lambda_v(f,x)} = H_v w_v(\text{Jac}_C) \quad \text{for each } v \quad \text{and} \quad \prod_{v \text{ place of } K} H_v = +1.$$

This strategy has been used in proving most known instances of the parity conjecture, but finding the local error term is a common challenge. Each proof to date has exhibited a different ad hoc expression which we don’t know how to interpret geometrically. Furthermore, these expressions have no obvious link to one another. In the future, we hope to identify such a pattern in order to formulate a construction which works more generally, rather than case-by-case.

In this thesis we exhibit a variety of local error terms which lead to proofs of the parity conjecture in various cases. Most notably, we present two different constructions that generalise the error term found in [17, Theorem 4].

## 1.3 Results of thesis

The key results proved in this thesis are summarised below.

### 1.3.1 Elliptic curves

As mentioned previously, isogenies provide the foundation for many local formulae. With this in mind, we fix an arbitrary elliptic curve and construct an isogeny in



order to deduce the following theorem.

**Theorem 1.3.1** (=Theorem 4.4.4). *Let  $K$  be a number field and  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) be an elliptic curve over  $K$ . Let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ .*

*Assuming that  $\text{III}(E)$ ,  $\text{III}(\text{Jac}_D)$  are finite,*

$$\text{rk}(E) + \text{rk}(\text{Jac}_D) \equiv \sum_{v \text{ place of } K} \text{ord}_3 \lambda_v(E) \pmod{2}$$

where  $\lambda_v(E)$  is a local invariant (see Definition 4.4.2).

**Remark 1.3.2.** Here, and in all other local formulae presented in this thesis,  $\lambda_v$  is essentially a ratio of Tamagawa numbers/real periods of Jacobians of appropriate curves. In particular, it can be computed via studying curves over the local field  $K_v$ .

Through numerical computations, we observe that the local term appearing here is equivalent to the product of root numbers  $w_v(E)w_v(\text{Jac}_D)$  whenever  $v \nmid 3\infty$ . In particular, we exhibit the following local error term.

**Theorem 1.3.3** (=Theorem 5.1.2). *Let  $K$  be a number field and  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) be an elliptic curve over  $K$ . Whenever*

- (i)  $K_v \cong \mathbb{C}$ ,
- (ii)  $K_v/\mathbb{Q}_p$  is finite, or
- (iii)  $K_v \cong \mathbb{R}$  and  $E/\mathbb{Q}(a, b)$  does not admit a 3-isogeny,

we have that

$$(-1)^{\text{ord}_3 \lambda_v(E) + \text{ord}_3 |3|_v} = w_v(E)w_v(\text{Jac}_D)$$

where  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$  and  $\lambda_v(E)$  is the local invariant given in Definition 4.4.2.

In fact, dropping the assumptions on the Shafarevich–Tate group, Theorem 1.3.1 gives a local formula for the  $3^\infty$ -Selmer rank of  $E \times \text{Jac}_D$  (=Theorem 4.5.3). By combining this with the previous theorem and utilising known instances of the 2-parity conjecture, we obtain the following consequences.

**Theorem 1.3.4** (=Theorems 5.1.3 & 5.1.5). *Let  $E : y^2 = x^3 + ax + b$  be an elliptic curve over a number field  $K$  and let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ .*

- *The 3-parity conjecture holds for  $E \times \text{Jac}_D$ .*
- *Assuming that  $\text{III}(E)$  has finite 3-primary part and  $\text{III}(\text{Jac}_D)$  has finite 2- and 3-primary parts, the parity conjecture holds for  $E$ .*

Another instance of a local formula for the parity of the rank, again deduced from a suitable isogeny, allows us to prove further new results concerning elliptic curves (and, ultimately, hyperelliptic curves).

**Theorem 1.3.5** (=Theorem 4.3.3). *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  is separable.*

*Assuming that  $\text{III}(\text{Jac}_{X_1}), \text{III}(\text{Jac}_{X_2}), \text{III}(\text{Jac}_{X_0})$  are finite,*

$$\text{rk}(\text{Jac}_{X_1}) + \text{rk}(\text{Jac}_{X_2}) + \text{rk}(\text{Jac}_{X_0}) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f_1, f_2) \pmod{2}$$

*where  $\lambda_v(f_1, f_2)$  is a local invariant (see Definition 4.3.2).*

To recover ranks of elliptic curves, we first restrict to  $f_1(x)$  being a monic cubic and  $f_2(x) = x$ . In this case, the places of  $K$  at which the local term differs from the relevant product of local root numbers depends on the coefficients of  $f_1(x)$ .

**Theorem 1.3.6** (=Theorem 6.1.8). *Let  $K$  be a number field and  $E : y^2 = f(x)$ ,  $E' : w^2 = xf(x)$  for  $f(x) = x^3 + ax^2 + bx + c \in K[x]$  a separable monic cubic with  $c \neq 0$ . At each place  $v$  of  $K$ ,*

$$(-1)^{\text{ord}_2 \lambda_v(f, x)} \cdot \begin{cases} (b, -c)_v(-2L, \Delta_f)_v(L, -b)_v & b, L \neq 0 \\ (-c, -1)_v(2c, \Delta_f)_v & bL = 0 \end{cases} = w_v(E)w_v(\text{Jac}_{E'})$$

*where  $L = ab - 9c$ ,  $\Delta_f$  denotes the discriminant of  $f$  and  $\lambda_v(f, x)$  is the local invariant given in Definition 4.3.2.*

We formulated this result by initially visualising the curves over  $\mathbb{R}$ . Our strategy involved compiling a list of invariants  $I_i$  in the coefficients of  $f(x)$ , alongside an extensive list of cubics  $f(x) \in \mathbb{R}[x]$ . We computed  $(-1)^{\text{ord}_2 \lambda_{\mathbb{R}}(f,x)}$ ,  $w_{\mathbb{R}}(E)w_{\mathbb{R}}(\text{Jac}_{E'})$  and the Hilbert symbols  $(I_i, I_j)_{\mathbb{R}}$  for each cubic and then, using linear algebra, were able to find a suitable product of the  $(I_i, I_j)_{\mathbb{R}}$ . Taking our list of invariants to be  $-1$ , the coefficients of  $f(x)$  and its discriminant was not good enough. To cook up a more exotic invariant, we fixed certain values of  $a$  and determined for which  $b, c$  the product of Hilbert symbols should evaluate to  $-1$ . When  $a = 1$ , such values are indicated by the shaded region in Figure 1.1. This pictorial description suggested that the line  $b = 9c$  would be a good candidate, since the shaded region is the disjoint union of  $\{b > 9c\} \cap \{\Delta_f < 0\}$  and  $\{b < 9c\} \cap \{c > 0\}$  which are picked out by  $(9c - b, \Delta_f)_{\mathbb{R}}$  and  $(b - 9c, -c)_{\mathbb{R}}$  respectively. Varying  $a$ , it became clear that the correct generalisation of this line was  $L = 0$  where  $L := ab - 9c$ , and so this was appended to our list. Running the argument described above then returned an error term which worked over  $\mathbb{R}$ . Experimentation over non-Archimedean fields showed that the only correction needed was the Hilbert symbol  $(2, \Delta_f)_v$  (which is trivial over  $\mathbb{R}$ ).

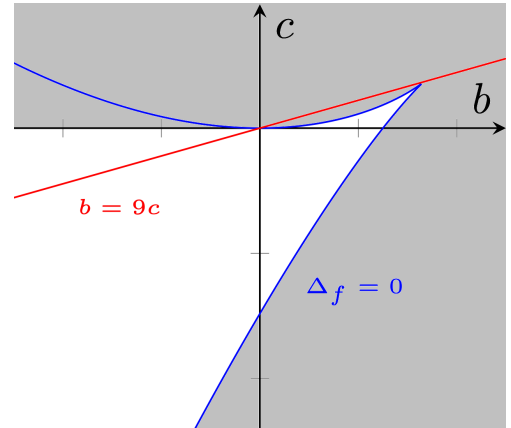


Figure 1.1

As a consequence to this comparison, and using that Theorem 1.3.5 can be rephrased to describe the parity of the  $2^\infty$ -Selmer rank (=Theorem 4.5.2), we obtain the 2-parity conjecture for certain genus 2 curves and for elliptic curves whose 2-torsion groups are isomorphic as Galois modules.

**Theorem 1.3.7** (=Theorems 6.3.2 & 6.3.4). *Let  $K$  be a number field. The 2-parity conjecture holds for*

- the Jacobian of  $C : y^2 = f(x^2)$  where  $f(x) \in K[x]$  is a separable cubic such that  $f(0) \neq 0$ , and

- $E_1$  if and only if it holds for  $E_2$ , where  $E_1, E_2$  are elliptic curves over  $K$  such that  $E_1[2] \cong E_2[2]$  as  $G_K$ -modules.

These results allow us to complete the proof of the  $p$ -parity conjecture for elliptic curves over totally real fields.

**Theorem 1.3.8** (=Theorem 6.4.1 & Corollary 6.4.2). *Let  $K$  be a totally real number field. The 2-parity conjecture holds for elliptic curves over  $K$  with complex multiplication, and consequently, the  $p$ -parity conjecture holds for all elliptic curves over  $K$ .*

### 1.3.2 Hyperelliptic curves $y^2 = xf(x)$

The generality of the local formula given in Theorem 1.3.5 allows us to ask whether the error term given in Theorem 1.3.6 has a natural generalisation? With this in mind, we state the following conjecture concerning an error term  $H_v(f)$  which we discuss below.

**Conjecture 1.3.9** (=Conjecture 7.2.5). *Let  $K$  be a number field and  $X_1 : y^2 = f(x)$ ,  $X_0 : w^2 = xf(x)$  for  $f(x) \in K[x]$  separable, monic, non-constant and such that  $f(0) \neq 0$ . At each place  $v$  of  $K$ ,*

$$(-1)^{\text{ord}_2 \lambda_v(f,x)} H_v(f) = w_v(\text{Jac}_{X_1}) w_v(\text{Jac}_{X_0})$$

where  $\lambda_v(f, x)$  is the local invariant given in Definition 4.3.2.

When  $f(x)$  is linear,  $H_v(f) = +1$ . When  $f(x) = x^2 + ax + b$ , this conjecture is [17, Theorem 4] and so we set  $H_v(f) = (a, -b)_v (-2a, a^2 - 4b)_v$ . When  $f(x)$  is a cubic, we take  $H_v(f)$  to be the product of Hilbert symbols described in Theorem 1.3.6.

Now suppose that  $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ . To find a candidate for  $H_v(f)$ , we use the strategy employed when  $f(x)$  was a cubic. Beginning with a certain list of invariants, this returns

$$H_v(f) = (J_1, -J_2)_v (J_2, -\Delta_f)_v (-d, c)_v (-c, J_3)_v (-J_3, J_4)_v (-J_4, \Delta_f)_v$$

where  $J_1, J_2, J_3, J_4$  are as in Notation 7.2.10 and, again,  $\Delta_f$  denotes the discriminant of  $f(x)$ . When all entries are non-zero, we prove the conjecture with respect to this definition of  $H_v(f)$  in most cases (namely, when  $K_v \cong \mathbb{C}$ ,  $K_v \cong \mathbb{R}$  and when  $K_v/\mathbb{Q}_p$  odd,  $f(x) \in \mathcal{O}_{K_v}[x]$  and the reduction of  $xf(x)$  has at worst two double roots).

By comparing these expressions for  $H_v(f)$  when  $\deg f \leq 4$ , we're able to observe that the entries of the Hilbert symbols all appear as coefficients in a sequence of polynomials associated to  $f(x)$ , called the *Sturm sequence*. In particular, if  $P_0, P_1, \dots, P_{\deg f}$  denotes this sequence of polynomials and all of them are non-zero with  $P_i(0)$  non-zero, then writing  $c_i$  for the lead coefficient of  $P_i$  and setting

$$H_v(f) = \prod_{i=0}^{\deg f - 1} (c_i, -c_{i+1})_v (-P_i(0), P_{i+1}(0))_v$$

uniformly recovers the expressions found in low degree. We're able to prove Conjecture 1.3.9 with respect to this general expression whenever  $K_v$  is Archimedean (=Theorems 7.2.8 & 7.2.9). Unfortunately, it is not clear how the entries of these Hilbert symbols encode information about the reduction types of the relevant curves, and so we are unable to provide a general proof when  $K_v$  is non-Archimedean.

**Corollary 1.3.10** (see Corollary 7.2.7). *Let  $K$  be a number field and  $f(x) \in K[x]$  be separable and completely reducible over  $K$ . Taking  $H_v$  to be as described above and assuming Conjecture 1.3.9, the 2-parity conjecture holds for the Jacobian of  $C : y^2 = f(x)$ .*

### 1.3.3 More general hyperelliptic curves

The approach discussed above for finding an error term  $H_v(f)$  involved considering Conjecture 1.3.9 when  $K_v \cong \mathbb{R}$  and then lifting this to the other completions of  $K$ .

If instead we initially consider completions  $K_v/\mathbb{Q}_p$ , i.e. we look for invariants that encode the  $v$ -adic distances between the roots of  $xf(x)$ , then there is an alternative way in which we can generalise the error term found in [17, Theorem 4]. This is discussed in detail in §8.3.

**Example 1.3.11.** Let  $K$  be a number field and  $f(x) \in K[x]$  be separable, monic,

have degree  $\geq 2$  and be such that  $f(0) \neq 0$ . Write  $\{\alpha_1, \dots, \alpha_n\}$  for the roots of  $f$  and assume that they are all defined over  $K_v$ , for  $v$  a place of  $K$ . Then (assuming the Hilbert symbol entries are all non-zero),

$$H_v(f) = H_v(f, x) := \prod_{1 \leq i < j \leq n} \left( -(\alpha_i + \alpha_j), -\alpha_i \alpha_j \right)_v \left( \frac{1}{2}(\alpha_i + \alpha_j), (\alpha_i - \alpha_j)^2 \right)_v.$$

In particular, if  $f(x) = x^2 + ax + b$  is such a polynomial then this becomes  $(a, -b)_v \left(-\frac{1}{2}a, a^2 - 4b\right)_v$ .

So far, we have considered Theorem 1.3.5 when  $f_2(x) = x$ . However, we can drop this assumption and define an error term  $H_v(f_1, f_2)$ , analogously to the one mentioned above, which works in full generality (=Conjecture 8.3.8). When  $f_1, f_2$  are monic, this conjecture says the following.

**Conjecture 1.3.12.** *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  where  $f_1(x), f_2(x) \in K[x]$  are monic and such that  $f_1(x)f_2(x)$  is separable. At each place  $v$  of  $K$  for which the error term  $H_v(f_1, f_2)$  given in Definition 8.3.4 is well-defined,*

$$(-1)^{\text{ord}_2 \lambda_v(f_1, f_2)} (-1, -1)_v \left[ \frac{(\deg f_1 - 1)(\deg f_2 - 1)}{2} \right] H_v(f_1, f_2) = w_v(\text{Jac}_{X_1}) w_v(\text{Jac}_{X_2}) w_v(\text{Jac}_{X_0})$$

where  $\lambda_v(f_1, f_2)$  is the local invariant given in Definition 4.3.2.

We prove this conjecture whenever  $v \mid \infty$ ,  $v \nmid 2\infty$  and the reduction of  $f_1(x)f_2(x)$  has at worst one double root, and  $v \mid 2$  and  $X_1, X_2, X_0$  all have good ordinary reduction with the roots of  $f_1(x)f_2(x)$  satisfying certain conditions (=Theorem 8.3.10).

Assuming this conjecture and the finiteness of the Shafarevich–Tate group, the parity conjecture for the Jacobian of a hyperelliptic curve whose defining polynomial is monic and reducible becomes equivalent to the parity conjecture for the product of two Jacobians of lower genus hyperelliptic curves (=Theorem 8.6.1).

The same error term allows us to formulate similar results concerning Jacobians of certain hyperelliptic curves whose defining polynomials are irreducible.

**Theorem 1.3.13** (=Theorem 8.2.6). *Let  $K$  be a number field,  $K(\sqrt{\xi})/K$  a quadratic extension and  $C : v^2 = f_0(x)\bar{f}_0(x)$ ,  $C_0 : y^2 = f_0(x)$  where  $f_0(x), \bar{f}_0(x) \in K(\sqrt{\xi})[x]$  are  $\text{Gal}_{K(\sqrt{\xi})/K}$ -conjugate and  $f_0(x)\bar{f}_0(x)$  is separable.*

*Assuming that  $\text{III}(\text{Jac}_C/K)$ ,  $\text{III}(\text{Jac}_{C_0}/K(\sqrt{\xi}))$  are finite,*

$$\text{rk}(\text{Jac}_C/K) + \text{rk}(\text{Jac}_{C_0}/K(\sqrt{\xi})) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f_0; \sqrt{\xi}) \pmod{2}$$

*where  $\lambda_v(f_0; \sqrt{\xi})$  is a local invariant.*

For now, we again only state our comparison of the local term  $\lambda_v(f_0; \sqrt{\xi})$  with local root numbers when  $f_0(x)$  is monic.

**Conjecture 1.3.14** (=Conjecture 8.3.11). *Let  $K$  be a number field,  $K(\sqrt{\xi})/K$  be a quadratic extension and  $C : v^2 = f_0(x)\bar{f}_0(x)$ ,  $C_0 : y^2 = f_0(x)$  where  $f_0(x), \bar{f}_0(x) \in K(\sqrt{\xi})[x]$  are monic,  $\text{Gal}_{K(\sqrt{\xi})/K}$ -conjugate, of degree  $2^m > 1$  and such that  $f_0(x)\bar{f}_0(x)$  is separable. At each place  $v$  of  $K$  for which the error term  $H_v(f_1, f_2)$  given in Definition 8.3.4 is well-defined,*

$$(-1)^{\text{ord}_2 \lambda_v(f_0; \sqrt{\xi})} (-1, -1)_v H_v(f_0, \bar{f}_0) = w_v(\text{Jac}_C) \prod_{\substack{\text{place } u \mid v \\ \text{of } K(\sqrt{\xi})}} w_u(\text{Jac}_{C_0})$$

*where  $\lambda_v(f_0; \sqrt{\xi})$  is a local invariant.*

We prove this conjecture under the assumption that  $\deg f_0 \geq 4$  whenever  $v \mid \infty$ ,  $v \nmid 2\infty$  and the reduction of  $f_0(x)\bar{f}_0(x)$  has at worst two double roots, and  $v \mid 2$  and  $C_0, C$  both have good ordinary reduction with the roots of  $f_0(x)\bar{f}_0(x)$  satisfying certain conditions (=Theorem 8.3.12).

Once again, assuming this conjecture and the finiteness of the Shafarevich–Tate group, the parity conjecture for the Jacobian of a hyperelliptic curve whose defining polynomial is irreducible, having degree  $2^m > 1$  and admits a factorisation over a quadratic extension becomes equivalent to the parity conjecture for the Jacobians of lower genus hyperelliptic curves (=Theorem 8.6.2).

By combining the global implications of the  $2^\infty$ -Selmer rank analogues of the scenarios discussed in this section, we deduce the following.

**Theorem 1.3.15** (=Theorem 8.6.3). *Assuming Conjectures 8.3.8 and 8.3.11, the 2-parity conjecture holds for the Jacobians of all hyperelliptic curves  $y^2 = f(x)$  such that  $\text{Gal}(f)$  is a 2-group.*

We detail in Chapter 8 how this allows us to deduce a result concerning general semistable hyperelliptic curves.

**Corollary 1.3.16** (=Corollary 8.6.4). *Let  $C : y^2 = f(x)$  be a semistable hyperelliptic curve over a number field  $K$  and write  $\mathcal{R} \subset \overline{K}$  for the set of roots of  $f(x)$ . Assuming Conjectures 8.3.8 and 8.3.11, and that  $\#\text{III}(\text{Jac}_C/K(\mathcal{R}))[p^\infty]$  is finite for each prime  $p \leq \deg f$ , the parity conjecture holds for the Jacobian of  $C$  over  $K$ .*

Moreover, using just the cases of the error term conjectures that we are able to prove, we prove the following theorem which is only conditional on the finiteness of the Shafarevich–Tate group.

**Corollary 1.3.17** (=Corollary 8.6.7). *Let  $K$  be a number field. Let  $f(x) \in \mathcal{O}_K[x]$  be separable, monic, such that  $\text{Gal}_{K(\mathcal{R})/K}$  is a 2-group and  $\text{Gal}_{\overline{K}/K}$  preserves a partition  $\{\alpha_1, \beta_1\}, \dots, \{\alpha_n, \beta_n\}$  of  $\mathcal{R}$  (the roots of  $f$ ). Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$  and suppose that the reduction of  $f(x)$  modulo  $\mathfrak{p}$  has at worst one double root whenever  $\mathfrak{p} \nmid 2$ , and that*

- $(x - \alpha_i)(x - \beta_i) \in K_{\mathfrak{p}}^{nr}[x]$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \beta_i) = \text{ord}_{\mathfrak{p}}(4)$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \alpha_j) = \text{ord}_{\mathfrak{p}}(\beta_i - \beta_j) = \text{ord}_{\mathfrak{p}}(\alpha_i - \beta_j) = 0$  for all  $i \neq j$ ,

whenever  $\mathfrak{p} \mid 2$ . Write  $C : y^2 = f(x)$ . Assuming that  $\#\text{III}(\text{Jac}_C/K(\mathcal{R}))[p^\infty]$  is finite for each prime  $p \leq \deg f$ , the parity conjecture holds for the Jacobian of  $C$ .



## 1.4 Structure of thesis

In Chapter 2, we detail the background material that will be assumed throughout this thesis, beginning with the construction of the Jacobian of a curve and a discussion of the types of curves that will be of interest. We then state results that will be used when computing (the Birch and Swinnerton-Dyer) invariants associated to the Jacobian of a curve. Several such invariants can be computed by studying the curve over a non-Archimedean local field, therefore we introduce cluster pictures for hyperelliptic and bihyperelliptic curves and present results which simplify these computations. We conclude the chapter by giving the standard definitions of Brauer relations, regulator constants and Hilbert symbols, and by stating relevant results concerning them.

We discuss a uniform method for constructing isogenies involving Jacobians in Chapter 3. This motivates Chapter 4, where we explain that an isogeny allows us to relate the local data present in the Birch and Swinnerton-Dyer conjecture to the parity of certain ranks. In particular, we derive formulae to compute the parity of the rank of (i) the Jacobian of a hyperelliptic curve whose defining polynomial is reducible, from that of lower genus curves and local data, and (ii) an elliptic curve, again from local data.

The remainder of the thesis focuses on the parity conjecture. In Chapter 5, we provide a proof for elliptic curves (under new assumptions of the Shafarevich–Tate group). We continue our study of elliptic curves in Chapter 6, proving that the 2-parity conjecture holds for elliptic curves with isomorphic 2-torsion and completing the proof of the  $p$ -parity conjecture for elliptic curves over totally real fields. In Chapter 7, we present a conjecture concerning hyperelliptic curves whose defining polynomials have a linear factor. We prove this conjecture in several cases and discuss how, as a consequence, we could deduce the 2-parity conjecture for Jacobians of hyperelliptic curves whose defining polynomials factor completely. Chapter 8 concludes the thesis by considering hyperelliptic curves. We deduce that the 2-parity conjecture holds for Jacobians of hyperelliptic curves whose Galois group is a 2-group and which satisfy certain conditions. We explain how we expect to be

able to relax these conditions and extend this result to Jacobians of all hyperelliptic curves (under relevant assumptions on the Shafarevich–Tate group).

## 1.5 Notation

Throughout this thesis we adhere to the following notation associated to a field  $K$ .

$\mathcal{K}$	a local field
$\overline{K}$	the algebraic closure of $K$
$G_K$	the absolute Galois group $\text{Gal}(\overline{K}/K)$
$\mathcal{O}_K$	the ring of integers of $K$
$k$	the residue field, when $K/\mathbb{Q}_p$ is finite
$K^{nr}$	the maximal unramified extension of $K$ , when $K/\mathbb{Q}_p$ is finite
$\text{Frob}_K$	a fixed choice of Frobenius automorphism in $G_K$ , when $K/\mathbb{Q}_p$ is finite
$ \cdot _K,  \cdot _v$	the unique extension of the the normalised absolute value on a local field $K$ (resp. $K_v$ ) to $\overline{K}$ (resp. $\overline{K}_v$ )

**Convention.** All curves are assumed to be smooth, proper, connected and geometrically connected (unless stated otherwise).

**Convention.** By  $X/K : \{f_1(x_1, \dots, x_m) = 0, \dots, f_n(x_1, \dots, x_m) = 0\}$ , we mean that  $X$  is the unique smooth projective curve over  $K$  birationally equivalent to this affine curve.

Let  $X$  be a curve over  $K$ ,  $A$  an abelian variety over  $K$ , and  $v$  a place of  $K$  (when  $K$  is a number field). The following table records the notation associated to  $X$  and  $A$ .

$A(K)_{\text{tors}}$	the torsion subgroup of $A(K)$
$\mathcal{X}_p(A)$	$\text{Hom}_{\mathbb{Z}_p}(\varinjlim \text{Sel}_{p^n}(A), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$ , the dual $p^\infty$ -Selmer group of $A$ for a prime $p \in \mathbb{Z}$
$\text{rk}_p(A)$	the $p^\infty$ -Selmer rank of $A$
$\text{III}(A)$	the Shafarevich–Tate group of $A$
$\text{Reg}(A)$	the regulator of $A$
$\Omega^1(A)$	the $K$ -vector space of regular differentials on $A$

$n_A, n_X$	the number of connected components of $A$ or $X$ when $K = \mathbb{R}$
$c_v(A), c_{\mathcal{K}}(A)$	the local Tamagawa number of $A$ at $v \nmid \infty$ , or over a finite extension $\mathcal{K}/\mathbb{Q}_p$
$C_v(A, \omega)$	$c_v(A) \cdot  \omega/\omega^0 _v$ when $v \nmid \infty$ , where $\omega^0$ is a Néron exterior form on $A$ ; $\int_{A(K_v)}  \omega $ when $K_v \cong \mathbb{R}$ ; $2^{\dim(A)} \int_{A(K_v)}  \omega \wedge \bar{\omega} $ when $K_v \cong \mathbb{C}$ ; where $\omega$ is a basis element of $\bigwedge^{\dim A} \Omega^1(A/K_v)$
$C(A)$	$\prod_{v \text{ place of } K} C_v(A, \omega)$ for a basis element $\omega$ of $\bigwedge^{\dim A} \Omega^1(A)$
$\mu_v(X), \mu_{\mathcal{K}}(X)$	the deficiency term of $X$ at $v$ , or over a local field $\mathcal{K}$ of characteristic 0, which encodes whether $X$ is deficient (see Definition 2.3.9)
$w_v(A), w_{\mathcal{K}}(A)$	the local root number of $A$ at $v$ , or over a local field $\mathcal{K}$ of characteristic 0
$w(A)$	$\prod_{v \text{ place of } K} w_v(A)$ , the global root number of $A$
$\Upsilon_X$	the dual graph of the special fibre of the minimal regular model of $X$ over $\mathcal{O}_{\mathcal{K}^{nr}}$ when $\mathcal{K}/\mathbb{Q}_p$ is finite and $X/\mathcal{K}$ is semistable (see [39, Chapter 10] for more details)

Finally, we provide a directory of other notation/terminology that we will use.

the divisor $D_S$	Notation 2.1.11
a Brauer relation	Definition 2.5.1
the regulator constant $\mathcal{C}_{\Theta}$	Definition 2.6.1
the local terms $\lambda_{\mathcal{K}}(f_1, f_2), \lambda_v(f_1, f_2)$	Definition 4.3.2
the local terms $\lambda_{\mathcal{K}}(E), \lambda_v(E)$	Definition 4.4.2
the local terms $\lambda_{\mathcal{K}}(f_0; \sqrt{\xi}), \lambda_v(f_0; \sqrt{\xi})$	Definition 8.2.5
$C_2 \times C_2$ and $D_8$ -hyperelliptic curves	Definition 8.0.1
the Hilbert symbols $H_1(T), H_2(T)$	Definition 8.3.3
the error term $H_{\mathcal{K}}(f, g)$	Definition 8.3.4

## Chapter 2

# Preliminaries

## 2.1 Curves and their Jacobians

### 2.1.1 The Jacobian of a curve

Elliptic curves are objects of interest to number theorists due to their natural group structure. An abelian variety, called the *Jacobian*, can be constructed from a curve of arbitrary genus. We describe their points and group structure here and refer the reader to [43] for further details.

Let  $X$  be a curve over a field  $K$ .

**Definition 2.1.1.** A *divisor*  $D$  on  $X$  is a formal sum

$$D = \sum_{P \in X(\bar{K})} n_P [P]$$

where  $n_P \in \mathbb{Z}$  and  $n_P = 0$  for all but finitely many  $P \in X(\bar{K})$ . The *degree* of  $D$  is  $\sum_P n_P$ . The set of all divisors on  $X$  is written  $\text{Div}(X)$  and those of degree 0 are denoted by  $\text{Div}^0(X)$ .

We note that  $\text{Div}(X)$  forms a group under addition, of which  $\text{Div}^0(X)$  is a subgroup.

**Definition 2.1.2.** A divisor  $D$  is called *principal* if there exists a non-zero rational

function on  $X$ ,  $f \in K(X)^\times$ , such that

$$D = \sum_{P \in X(\bar{K})} \text{ord}_P(f)[P]$$

where  $\text{ord}_P(f)$  denotes the order of vanishing of  $f$  at  $P$ . The set of principal divisors is written  $\text{Prin}(X)$ .

Further,  $\text{Prin}(X)$  is a subgroup of  $\text{Div}^0(X)$  since any non-zero rational function has as many zeroes as it has poles (counting multiplicities).

**Definition 2.1.3.** The Jacobian of a curve  $X$  over a field  $K$  is

$$\text{Jac}_X = \text{Pic}^0(X) := \text{Div}^0(X)/\text{Prin}(X).$$

The points on  $\text{Jac}_X$  are classes of divisors of degree 0 on  $X$ . Moreover, since  $\text{Div}^0(X)$  carries an action of the absolute Galois group  $G_K$ , the points in  $\text{Jac}_X(K)$  are classes of divisors of degree 0 that are invariant under this action.

**Theorem 2.1.4** ([43], Theorems 1.1 & 6.6, Proposition 2.1). *The Jacobian of a curve  $X$  of genus  $g$  over a field  $K$  is a principally polarised abelian variety of dimension  $g$ .*

We will sometimes need to consider the Jacobian of a curve which is not connected, in which case we refer the reader to [23, §A.6] for more details.

**Remark 2.1.5.** The Jacobian of a genus 0 curve is 0. The Jacobian of a genus 1 curve is an elliptic curve.

**Lemma 2.1.6** ([11], §4). *Let  $K$  be a field of characteristic not equal to 2 or 3. Let  $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in K[x]$  and  $C : y^2 = f(x)$ , then*

$$\text{Jac}_C : Y^2 = X^3 - 27IX - 27J,$$

where  $I = 12ae - 3bd + c^2$  and  $J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$ .

**Remark 2.1.7.** Suppose that  $f(x) = c(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$  for  $c \in K^\times$ ,  $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \overline{K}$ . Then  $\text{Jac}_C : Y^2 = (X - r_1)(X - r_2)(X - r_3)$  where

$$r_1 = 3c(\alpha_1\alpha_2 - 2\alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 - 2\alpha_2\alpha_4 + \alpha_3\alpha_4),$$

$$r_2 = 3c(\alpha_1\alpha_2 + \alpha_1\alpha_3 - 2\alpha_2\alpha_3 - 2\alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4),$$

$$r_3 = -3c(2\alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 - \alpha_1\alpha_4 - \alpha_2\alpha_4 + 2\alpha_3\alpha_4).$$

In particular,  $r_2 - r_1 = 9c(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$ ,  $r_1 - r_3 = 9c(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_4)$  and  $r_2 - r_3 = 9c(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$ .

It will sometimes be necessary to study Jacobians of curves over the reals. When doing this, we will make use of the following lemma.

**Lemma 2.1.8** ([29], Propositions 3.2 & 3.3). *Let  $X$  be a curve of genus  $g$  over  $\mathbb{R}$ . The number of connected components of  $\text{Jac}_X(\mathbb{R})$  is*

$$n_{\text{Jac}_X/\mathbb{R}} = \begin{cases} 2^{n_{X/\mathbb{R}}-1} & \text{if } n_{X/\mathbb{R}} > 0, \\ 1 & \text{if } n_{X/\mathbb{R}} = 0 \text{ and } g \text{ is even,} \\ 2 & \text{if } n_{X/\mathbb{R}} = 0 \text{ and } g \text{ is odd,} \end{cases}$$

where  $n_{X/\mathbb{R}}$  denotes the number of connected components of  $X(\mathbb{R})$ .

## 2.1.2 Induced homomorphisms between Jacobians

Given a non-constant morphism  $\pi : X \rightarrow Y$  of curves defined over a field  $K$ , we have an induced  $K$ -homomorphism  $\pi_* : \text{Jac}_X \rightarrow \text{Jac}_Y$ , given by

$$\pi_* : \sum_{P \in X(\overline{K})} n_P [P] \longmapsto \sum_{P \in X(\overline{K})} n_P [\pi(P)]$$

(on the level of divisors).

Additionally, there is an induced  $K$ -homomorphism in the reverse direction

$\pi^* : \text{Jac}_Y \rightarrow \text{Jac}_X$ , given by

$$\pi^* : \sum_{Q \in Y(\bar{K})} n_Q [Q] \longmapsto \sum_{Q \in Y(\bar{K})} n_Q \left( \sum_{P \in \pi^{-1}(Q)} e_\pi(P) [P] \right)$$

(on the level of divisors), where  $e_\pi(P)$  denotes the ramification degree of  $\pi$  at  $P$ .

Denote by  $\lambda_X$  and  $\lambda_Y$  the canonical principal polarisations on  $\text{Jac}_X$  and  $\text{Jac}_Y$ .

**Lemma 2.1.9** ([23], Lemma A.17). *We have that  $\pi^* = \lambda_X^{-1} \circ \pi_*^\vee \circ \lambda_Y$ , where  $\pi_*^\vee$  denotes the dual of  $\pi_*$ .*

### 2.1.3 Hyperelliptic curves

Let  $K$  be a field. By a *hyperelliptic curve*  $C$  over a field  $K$ , we mean a curve defined over  $K$  of genus  $g \geq 2$  which admits a finite separable morphism  $C \rightarrow \mathbb{P}_K^1$  of degree 2. When the characteristic of  $K$  is not equal to 2, we can always find a separable  $f(x) \in K[x]$  of degree  $2g + 1$  or  $2g + 2$  such that

$$C : y^2 = f(x),$$

i.e.  $C$  is the projective curve given by glueing the pair of affine patches

$$U_x : y^2 = f(x) \quad \text{and} \quad U_t : v^2 = t^{2g+2} f\left(\frac{1}{t}\right)$$

along  $x = \frac{1}{t}$  and  $y = \frac{v}{t^{g+1}}$ .

By the points at infinity on  $C$  we mean the points of  $C \setminus U_x$ , i.e. the points of  $U_t$  with  $t = 0$ . If  $\deg f = 2g + 1$  there is a unique such point  $P_\infty = (0, 0)$  and if  $\deg f = 2g + 2$  there are two distinct such points  $P_\infty = (0, \sqrt{c_f})$  and  $\iota(P_\infty) = (0, -\sqrt{c_f})$  (here  $c_f$  is the lead coefficient of  $f$  and  $\iota$  denotes the hyperelliptic involution).

**Remark 2.1.10.** All curves of genus 2 are hyperelliptic [7, Chapter 1, §1].

### 2.1.4 The Jacobian of a genus 2 curve

Let  $C$  be a curve of genus 2 defined over a field  $K$  of characteristic not equal to 2. Since such curves are hyperelliptic, we can write

$$C : y^2 = f(x)$$

where  $f(x) \in K[x]$  is a polynomial of degree 6 with no repeated roots. We describe the addition law on  $\text{Jac}_C$ , as given in [7, Chapter 2].

A point  $P \in \text{Jac}_C(\overline{K})$  can be given as a divisor on  $C$  of the form

$$P = [P_1, P_2] := P_1 + P_2 - P_\infty - \iota(P_\infty)$$

for some  $P_1, P_2 \in C(\overline{K})$ .

Let  $[P_1, P_2], [Q_1, Q_2] \in \text{Jac}_C(\overline{K})$ . There exists a cubic polynomial  $g(x) \in K[x]$  such that  $P_1, P_2, Q_1, Q_2$  are points on  $y = g(x)$ . The principal divisor on  $C$  arising from the function  $y - g(x)$  is

$$P_1 + P_2 + Q_1 + Q_2 + S_1 + S_2 - 3P_\infty - 3\iota(P_\infty) = 0 \in \text{Jac}_C(\overline{K})$$

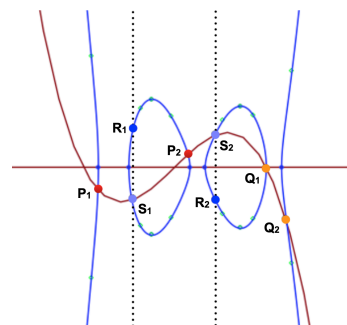
where  $S_1, S_2$  are the additional intersection points of  $C$  with  $y = g(x)$ .

Therefore,

$$[P_1, P_2] + [Q_1, Q_2] = -[S_1, S_2]$$

and so letting  $R_1 = \iota(S_1)$ ,  $R_2 = \iota(S_2)$  and noting that  $[R_1, S_1] = [R_2, S_2] = 0$  gives

$$[P_1, P_2] + [Q_1, Q_2] = [R_1, R_2].$$



**Figure 2.1:** Addition on the Jacobian of a genus 2 curve

### 2.1.5 The Jacobian of a hyperelliptic curve

Now let  $C : y^2 = f(x)$  be a hyperelliptic curve of genus  $g$  defined over a field  $K$  of characteristic not equal to 2. Roughly speaking, points in  $\text{Jac}_C(\overline{K})$  look like  $g$ -tuples



of points in  $C(\overline{K})$ . However, a geometric addition law is harder to describe.

We will only need to understand the 2-torsion points of the Jacobians of such curves.

**Notation 2.1.11.** Let  $S \subseteq \mathcal{R}$  be an even sized subset of the roots of  $f$ . Write

$$D_S := \sum_{r \in S} (r, 0) - \frac{\#S}{2} ((\infty) + \iota(\infty)) \in \text{Div}^0(C)$$

where  $\infty$  is any choice of point at infinity on  $C$  and  $\iota$  denotes the hyperelliptic involution.

**Lemma 2.1.12.** *The (class of the) divisor  $D_S$  belongs to  $\text{Jac}_C[2]$  and  $D_S, D_{S'}$  are divisors in the same class precisely when  $S = S'$  or when  $\deg f$  is even and  $S' = \mathcal{R} - S$ .*

*Proof.* See [10, Lemma 2.1]. □

This lemma describes all of the 2-torsion points on Jacobians of hyperelliptic curves.

### 2.1.6 Bihyperelliptic curves

Let  $K$  be a field of characteristic not equal to 2. A *bihyperelliptic curve* over  $K$  has an affine model  $B : \{y^2 = f_1(x), z^2 = f_2(x)\}$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  has no repeated roots. Sometimes we call  $B$  the bihyperelliptic curve arising from the hyperelliptic curves  $C_1 : y^2 = f_1(x), C_2 : z^2 = f_2(x)$  of genus  $g_1, g_2$  respectively. More explicitly,  $B$  is given by glueing

$$U_x : \begin{cases} y^2 = f_1(x) \\ z^2 = f_2(x) \end{cases} \quad \text{and} \quad U_t : \begin{cases} v^2 = t^{2g_1+2} f_1\left(\frac{1}{t}\right) \\ u^2 = t^{2g_1+2} f_2\left(\frac{1}{t}\right) \end{cases}$$

along  $x = \frac{1}{t}, y = \frac{v}{t^{g_1+1}}, z = \frac{u}{t^{g_2+1}}$  when  $\deg f_1 \deg f_2$  is even, and

$$U_x : \begin{cases} y^2 = f_1(x) \\ z^2 = f_2(x) \end{cases} \quad \text{and} \quad U_t : \begin{cases} v^2 = t^{2g_1+2} f_1\left(\frac{1}{t}\right) \\ u^2 = t^{2(g_1+g_2)+2} f_1\left(\frac{1}{t}\right) f_2\left(\frac{1}{t}\right) \end{cases}$$

along  $x = \frac{1}{t}$ ,  $y = \frac{v}{t^{g_1+1}}$ ,  $z = \frac{u}{t^{g_2v}}$  when  $\deg f_1 \deg f_2$  is odd.

By the points at infinity on  $B$  we mean the points of  $B \setminus U_x$ , i.e. the points on  $U_t$  with  $t = 0$ . If both  $\deg f_1$ ,  $\deg f_2$  are even then there are 4 such points, otherwise there are just 2.

### 2.1.7 Quotient curves

Let  $X$  be a curve over a field  $K$  and let  $G$  be a finite group of  $K$ -automorphisms of  $X$ .

By the *quotient curve of  $X$  by  $G$*  we mean the algebraic curve  $X_G$  obtained by identifying points of  $X$  that lie in the same  $G$ -orbit (equations defining  $X_G$  can be constructed from the equations defining  $X$  and the automorphisms in  $G$ ).

Since there is an equivalence between the category of regular curves over  $K$  with non-constant morphisms and the category of finitely generated field extensions of  $K$  with transcendence degree one (see [62, Tag 0BY1]), the quotient curve  $X_G$  is the curve with function field  $K(X)^G$ .

**Example 2.1.13.** Let  $K$  be a field of characteristic not equal to 2 and let  $X : \{y^2 = f_1(x), z^2 = f_2(x)\}$  be a bihyperelliptic curve over  $K$ .

Consider the  $K$ -automorphisms of  $X$  given by

$$\tau_1 : (x, y, z) \mapsto (x, y, -z) \quad \text{and} \quad \tau_2 : (x, y, z) \mapsto (x, -y, z).$$

These give rise to the quotient curves

$$X_{\langle \tau_1 \rangle} : y^2 = f_1(x), \quad X_{\langle \tau_2 \rangle} : z^2 = f_2(x),$$

$$X_{\langle \tau_1 \tau_2 \rangle} : (yz)^2 = f_1(x)f_2(x), \quad X_{\langle \tau_1, \tau_2 \rangle} = \mathbb{P}^1 \quad (\text{with parameter } x)$$

with corresponding quotient maps

$$\begin{array}{lll} \pi_1 : X \rightarrow X_{\langle \tau_1 \rangle} & \pi_2 : X \rightarrow X_{\langle \tau_2 \rangle} & \pi_0 : X \rightarrow X_{\langle \tau_1 \tau_2 \rangle} \\ (x, y, z) \mapsto (x, y), & (x, y, z) \mapsto (x, z), & (x, y, z) \mapsto (x, yz). \end{array}$$

The following result concerning the  $K$ -points on Jacobians of quotient curves

will be used in Chapter 4.

**Lemma 2.1.14** ([23], Theorem 1.3). *Let  $X$  be a curve over a number field  $K$ . Let  $H$  be a finite group of  $K$ -automorphisms of  $X$ . Then,*

$$(\mathrm{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q})^H = \mathrm{Jac}_{X_H}(K) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

## 2.2 Weil restriction of abelian varieties

Let  $K$  be a field,  $K(\sqrt{d})/K$  be a quadratic extension and  $A$  an abelian variety over  $K(\sqrt{d})$ . The *Weil restriction of scalars of  $A$  from  $K(\sqrt{d})$  to  $K$* , denoted  $\mathrm{Res}_{K(\sqrt{d})/K}A$ , is an abelian variety over  $K$  of dimension  $2 \dim A$ . It is discussed in [47, §3].

When viewed as an abelian variety over  $K(\sqrt{d})$ , we have that

$$\mathrm{Res}_{K(\sqrt{d})/K}A \cong A \times A. \tag{2.1}$$

In particular,

$$\mathrm{Res}_{K(\sqrt{d})/K}A(K) = \{(P, P) \in A(K(\sqrt{d})) \times A(K(\sqrt{d}))\},$$

because if  $(P, Q) \in \mathrm{Res}_{K(\sqrt{d})/K}A(\overline{K})$  and  $\sigma \in G_K$ , then  $\sigma(P, Q) = (\sigma(P), \sigma(Q))$  when  $\sigma(\sqrt{d}) = \sqrt{d}$  and  $\sigma(P, Q) = (\sigma(Q), \sigma(P))$  otherwise.

Now let  $K$  be a number field and  $v$  be a place of  $K$ . If  $v$  splits in  $K(\sqrt{d})$ , then viewed as an abelian variety over  $K_v$  we have the same isomorphism as detailed in (2.1). If instead there is a unique place  $w$  of  $K(\sqrt{d})$  above  $v$ , then viewed as an abelian variety over  $K_v$  we have that

$$\mathrm{Res}_{K(\sqrt{d})/K}A \cong \mathrm{Res}_{K(\sqrt{d})_w/K_v}A.$$

## 2.3 Birch and Swinnerton-Dyer invariants

We recall the statement of the Birch and Swinnerton-Dyer conjecture for principally polarised abelian varieties.

**Conjecture 2.3.1** (Birch and Swinnerton-Dyer [4, 5], Tate [66]). *Let  $A$  be a principally polarised abelian variety over a number field  $K$  of discriminant  $\Delta_K$ . Assuming that  $L(A, s)$  has an analytic continuation to  $\mathbb{C}$ ,*

$$(i) \text{ rk}(A) = \text{ord}_{s=1} L(A, s),$$

(ii) *if  $\#\text{III}(A)$  is finite, then the leading term in the Taylor expansion of  $L(A, s)$  at  $s = 1$  is*

$$\text{BSD}(A) := \frac{\#\text{III}(A)\text{Reg}(A)C(A)}{\#A(K)_{\text{tors}}^2 \sqrt{|\Delta_K|^{\dim A}}}.$$

We will be interested in computing the invariants appearing here, along with the root number which appears in the parity conjecture, when  $A$  is the Jacobian of a curve. In several instances, this data can be determined from the underlying curve.

### 2.3.1 Heights

The following result will be used when we compute regulators for Jacobians of quotient curves.

**Lemma 2.3.2** (To appear in [46]). *Let  $X$  be a curve over a number field  $K$ . Let  $H$  be a finite group of  $K$ -automorphisms of  $X$  and  $\pi_H : X \rightarrow X_H$  the quotient map. For each  $P, Q \in \text{Jac}_{X_H}(K)$ ,*

$$\langle (\pi_H)^*P, (\pi_H)^*Q \rangle = \#H \langle P, Q \rangle_H$$

where  $\langle, \rangle$  and  $\langle, \rangle_H$  denote the Néron–Tate height pairings on  $\text{Jac}_X(K)$  and  $\text{Jac}_{X_H}(K)$  respectively.

### 2.3.2 Tamagawa numbers

At various points in this thesis, we will need to calculate Tamagawa numbers for Jacobians of curves. We will often do this via the following lemma.

**Theorem 2.3.3** ([22], Lemma 2.22 & Remark 2.23). *Let  $\mathcal{K}$  be a non-Archimedean local field of characteristic 0 with residue field  $k$ . For a semistable curve  $C/\mathcal{K}$ ,  $c_{\mathcal{K}}(\text{Jac}_C)$  is given by the size of the  $G_k$ -invariants of the cokernel of*

$$H_1(\Upsilon_C, \mathbb{Z}) \rightarrow \text{Hom}(H_1(\Upsilon_C, \mathbb{Z}), \mathbb{Z}), \quad \ell \mapsto \langle \ell, \cdot \rangle.$$

### 2.3.3 Root numbers

Root numbers of abelian varieties over Archimedean fields are particularly easy to describe.

**Lemma 2.3.4** ([55], Proposition 1 or [57], Lemma 2.1). *Let  $A$  be an abelian variety over an Archimedean local field  $\mathcal{K}$ . Then,*

$$w_{\mathcal{K}}(A) = (-1)^{\dim A}.$$

When computing root numbers over non-Archimedean fields for Jacobians of semistable curves we can again turn our attention to the dual graph.

**Theorem 2.3.5** ([22], Theorem 2.20). *Let  $\mathcal{K}$  be a non-Archimedean local field of characteristic 0 with residue field  $k$ . For a semistable curve  $C/\mathcal{K}$ ,*

$$w_{\mathcal{K}}(\text{Jac}_C) = (-1)^a$$

*where  $a$  is the multiplicity of the trivial representation of  $G_k$  in the homology of the dual graph  $H_1(\Upsilon_C, \mathbb{Q})$ .*

**Theorem 2.3.6** ([12]). *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension and let  $E$  be a semistable elliptic curve over  $\mathcal{K}$ . Then  $w_{\mathcal{K}}(E) = -1$  precisely when  $E$  has split multiplicative reduction.*

### 2.3.4 Deficiency and the Shafarevich–Tate group

We conclude our discussion of Birch and Swinnerton-Dyer invariants for Jacobians of general curves by describing how we are able to control the size of the Shafarevich–

Tate group up to squares. This is achieved by studying the local arithmetic of the underlying curve.

In the 1960s, when considering elliptic curves, Cassels proved the following.

**Theorem 2.3.7** (Cassels [6]). *Let  $E$  be an elliptic curve defined over a number field  $K$ . Assuming that  $\#\text{III}(E)$  is finite, it is a square.*

Unfortunately, the same does not hold upon replacing  $E$  with a general abelian variety. Instead, in the case of principally polarised abelian varieties, we have the following.

**Theorem 2.3.8** (Poonen–Stoll [53], Theorem 8). *Let  $A$  be a principally polarised abelian variety over a number field  $K$ . Write  $\text{III}_0(A)$  for the quotient of  $\text{III}(A)$  by its maximal divisible subgroup and let  $p \in \mathbb{Z}$  be a prime. Then,  $\#\text{III}_0(A)[p^\infty]$  is a square when  $p \neq 2$ , and a square or twice a square otherwise.*

Moreover, when  $A$  is the Jacobian of a curve, we can explicitly describe  $\#\text{III}_0(A)[2^\infty]$  up to squares.

**Definition 2.3.9.** Let  $X$  be a curve of genus  $g$  over a local field  $\mathcal{K}$ . We say that  $X$  is *deficient* if it has no  $\mathcal{K}$ -rational divisor of degree  $g - 1$  and we define the *deficiency term* by

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

When  $X$  is a curve over a number field  $K$ , we say that  $X$  is deficient at a place  $v$  of  $K$  if it is deficient over  $K_v$  and write  $\mu_v(X)$  for the deficiency term.

**Example 2.3.10.** Let  $X/\mathbb{Q} : y^2 = (x^2 - 6)(x^4 + 1)$  be a genus 2 curve. Since  $(\sqrt{6}, 0) \in X(\mathbb{Q}_5)$  gives rise to a degree 1 divisor,  $X$  is not deficient over  $\mathbb{Q}_5$  and  $\mu_5(X) = 1$ .

**Theorem 2.3.11** (Poonen–Stoll [53], Theorem 8 & Corollary 12). *Let  $X$  be a curve over a number field  $K$ . Write  $\text{III}_0(\text{Jac}_X)$  for the quotient of  $\text{III}(\text{Jac}_X)$  by its maximal*

divisible subgroup. Then,

$$\#\text{III}_0(\text{Jac}_X)[2^\infty] \equiv \prod_{v \text{ place of } K} \mu_v(X) \pmod{\mathbb{Q}^{\times 2}}.$$

There is currently no analogue of this result for general principally polarised abelian varieties.

**Remark 2.3.12.** If  $X$  has genus 0, then  $\text{Jac}_X = 0$  and so  $\text{III}(\text{Jac}_X) = 1 \Rightarrow \prod_v \mu_v(X) = \square$ . In particular,  $X$  is deficient at an even number of places of  $K$ .

**Remark 2.3.13.** A genus 1 curve  $E$  over a local field  $\mathcal{K}$  is never deficient and so we recover Cassels' result on elliptic curves.

We now make some further comments regarding deficiency over Archimedean local fields.

**Remark 2.3.14.** Curves over  $\mathbb{C}$  are never deficient.

**Lemma 2.3.15.** A curve  $X$  of genus  $g$  over  $\mathbb{R}$  is deficient if and only if  $g$  is even and  $X(\mathbb{R}) = \emptyset$ .

*Proof.* Any  $\mathbb{R}$ -rational divisor on  $X$  looks like

$$\sum_{P \in X(\mathbb{C}) \setminus X(\mathbb{R})} n_P([P] + [\bar{P}]) + \sum_{P \in X(\mathbb{R})} n_P[P].$$

From this, it is clear that no such divisor of degree  $g - 1$  exists precisely when  $g$  is even and  $X(\mathbb{R}) = \emptyset$ .  $\square$

**Remark 2.3.16.** We will use this characterisation of deficiency over  $\mathbb{R}$  for hyperelliptic and bihyperelliptic curves. With this in mind, we note that

- $y^2 = f(x)$  has even genus if and only if  $\deg f \equiv 1$  or  $2 \pmod{4}$ ,
- $\{y^2 = f_1(x), z^2 = f_2(x)\}$  has even genus if and only if both  $\deg f_1, \deg f_2$  are odd (since, by Theorem 3.3.2, the genus of this bihyperelliptic curve is the sum of the genera of  $y^2 = f_1(x), z^2 = f_2(x), w^2 = f_1(x)f_2(x)$ ).

## 2.4 Cluster pictures for hyperelliptic and bihyperelliptic curves

The central theme of this thesis involves using the arithmetic of curves over local fields ( $\mathbb{R}$ ,  $\mathbb{C}$ , or finite extensions of  $\mathbb{Q}_p$ ) to make global assertions, more specifically, concerning the ranks of Jacobians.

In the setting of semistable hyperelliptic curves, the machinery of *cluster pictures* developed in [22] offers a convenient way to compute this local data. Similarly, the local data for semistable bihyperelliptic curves can be computed from their *chromatic cluster pictures* as in [27].

Here we recall the key definitions and results of these theories which are required for this thesis.

### 2.4.1 Clusters

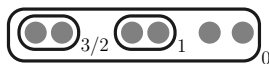
**Definition 2.4.1.** Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $C : y^2 = f(x)$  be a hyperelliptic curve of genus  $g$  over  $\mathcal{K}$ , i.e.  $\deg f = 2g + 1$  or  $2g + 2$ , with  $\mathcal{R}$  denoting the set of roots of  $f$ . A *cluster* is a non-empty subset  $\mathfrak{s} \subseteq \mathcal{R}$  of the form  $\mathfrak{s} = D \cap \mathcal{R}$  for some disc  $D = \{x \in \overline{\mathcal{K}} : v(x - z) \geq d\}$  and some  $z \in \mathcal{K}$ ,  $d \in \mathbb{Q}$ . Any such  $z = z_{\mathfrak{s}}$  is called a *centre* of  $\mathfrak{s}$ . If  $|\mathfrak{s}| > 1$ , we say that  $\mathfrak{s}$  is a *proper* cluster and we define its *depth* to be

$$d_{\mathfrak{s}} = \min_{r, r' \in \mathfrak{s}} v(r - r').$$

The *cluster picture*  $\Sigma$  of  $C$  is the collection of all clusters of the roots of  $f$ .

The cluster picture of  $C$  is a purely combinatorial object which allows us to visualise how close the roots of  $f$  are  $\mathcal{K}$ -adically. We draw cluster pictures by drawing roots of  $f$  as  $\bullet$  and drawing ovals around roots in a proper cluster.

**Example 2.4.2.** Let  $C/\mathbb{Q}_7 : y^2 = (x^2 + 7^3)((x + 1)^2 - 7^2)(x - 1)(x - 2)$ . The cluster picture for  $C$  is



where, from left to right, the roots are  $\sqrt{-7^3}$ ,  $-\sqrt{-7^3}$ ,  $6$ ,  $-8$ ,  $1$  and  $2$ .

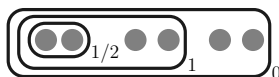


In order to work with clusters, we introduce some additional terminology.

**Definition 2.4.3.** Let  $\Sigma$  be a cluster picture and  $\mathfrak{s} \in \Sigma$  a cluster. If  $\mathfrak{s}' \subsetneq \mathfrak{s}$  is a maximal subcluster of  $\mathfrak{s}$  then we say that  $\mathfrak{s}'$  is a *child* of  $\mathfrak{s}$  and  $\mathfrak{s}$  is a *parent* of  $\mathfrak{s}'$ , written  $\mathfrak{s}' < \mathfrak{s}$  and  $\mathfrak{s} = P(\mathfrak{s}')$  respectively. The *relative depth* of  $\mathfrak{s}$  is  $\delta_{\mathfrak{s}} = d_{\mathfrak{s}} - d_{P(\mathfrak{s})}$ .

Traditionally, we decorate the bottom right corner of a cluster with its relative depth when drawing cluster pictures.

**Example 2.4.4.** Let  $C/\mathbb{Q}_7 : y^2 = (x^2 + 7^3)(x^2 - 7^2)(x - 1)(x - 2)$ . The cluster picture for  $C$  is



where, from left to right, the roots are  $\sqrt{-7^3}$ ,  $-\sqrt{-7^3}$ ,  $7$ ,  $-7$ ,  $1$  and  $2$ .

**Definition 2.4.5.** A cluster  $\mathfrak{s}$  is *even* (*odd* respectively) if  $|\mathfrak{s}|$  is even (odd respectively) and *übereven* if it's an even cluster with only even children. Furthermore,  $\mathfrak{s}$  is a *twin* if  $|\mathfrak{s}| = 2$  and a *cotwin* if it is non-übereven with a child of size  $2g$ . A cluster  $\mathfrak{s}$  is *principal* if  $|\mathfrak{s}| \geq 3$  except if either  $\mathfrak{s} = \mathcal{R}$  is even with exactly two children, or if  $\mathfrak{s} = \mathcal{R}$  is a cotwin.

The Galois group  $G_{\mathcal{K}}$ , in particular a choice of Frobenius element in  $G_{\mathcal{K}}$ , acts on clusters via its action on the roots of  $f$ . This action preserves depths and containments of clusters. When drawing cluster pictures, we link clusters that are in the same Frobenius orbit by lines; for instance,  $\textcircled{\bullet\bullet} \textcircled{\bullet\bullet}$ .

We provide the following definition in more generality than is necessary for this thesis in the interest of completeness. The construction simplifies in most cases we consider (see Remark 2.4.7).

**Definition 2.4.6.** For a cluster  $\mathfrak{s}$ , we write  $\mathfrak{s}^*$  for the smallest cluster  $\mathfrak{s}^* \supseteq \mathfrak{s}$  whose parent is not übereven (and  $\mathfrak{s}^* = \mathcal{R}$  if no such cluster exists). If  $\mathfrak{s}$  is a cotwin, we write  $\mathfrak{s}^*$  for its child of size  $2g$ .

For an even cluster  $\mathfrak{s}$  we fix a choice of  $\theta_{\mathfrak{s}} = \sqrt{c_f \prod_{r \notin \mathfrak{s}} (z_{\mathfrak{s}} - r)}$ , where  $c_f$  is the lead coefficient of  $f$  and  $z_{\mathfrak{s}}$  is a centre for  $\mathfrak{s}$ . If  $\mathfrak{s}$  is either even or a cotwin, we define

$\epsilon_{\mathfrak{s}} : G_{\mathcal{K}} \rightarrow \{\pm 1\}$  by

$$\epsilon_{\mathfrak{s}}(\sigma) \equiv \frac{\sigma(\theta_{\mathfrak{s}^*})}{\theta_{(\sigma\mathfrak{s})^*}} \pmod{\mathfrak{m}},$$

where  $\text{mod } \mathfrak{m}$  denotes reduction to the residue field of  $\mathcal{K}$ .

For all other clusters  $\mathfrak{s}$ , we set  $\epsilon_{\mathfrak{s}}(\sigma) = 0$ .

We decorate the top right corner of an even cluster  $\mathfrak{s}$  satisfying  $\mathfrak{s}^* = \mathfrak{s}$  with a  $+$  or  $-$  to indicate the value of  $\epsilon_{\mathfrak{s}}(\text{Frob}_{\mathcal{K}})$ .

**Remark 2.4.7.** Let  $C : y^2 = f(x)$  and assume that  $\mathcal{R}$  is not  $\bar{u}$ bereven. Whenever  $\mathfrak{t} < \mathcal{R}$  is a twin,

$$\epsilon_{\mathfrak{t}}(\sigma) \equiv \frac{\sigma(\theta_{\mathfrak{t}})}{\theta_{\sigma\mathfrak{t}}}.$$

Furthermore, if  $\mathfrak{t} = \{r, s\}$  is fixed by  $\sigma \in G_{\mathcal{K}}$ , then

$$\epsilon_{\mathfrak{t}}(\sigma) = +1 \iff c_f \frac{f(x)}{(x-r)(x-s)} \Big|_{x=\frac{1}{2}(r+s)} = \square.$$

## 2.4.2 Computing data for semistable hyperelliptic curves

When a hyperelliptic curve is semistable, many of its local arithmetic invariants can be computed from its cluster picture. The following result classifies semistable hyperelliptic curves.

**Theorem 2.4.8** ([22], Theorem 7.1). *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$ . Let  $C : y^2 = f(x)$  be a semistable hyperelliptic curve over  $\mathcal{K}$  of genus  $\geq 2$  and write  $\mathcal{R} \subset \bar{\mathcal{K}}$  for the set of roots of  $f$ . Then,  $C/\mathcal{K}$  has semistable reduction if and only if*

- (i) *the extension  $\mathcal{K}(\mathcal{R})/\mathcal{K}$  has ramification degree at most 2,*
- (ii) *every proper cluster of  $\Sigma_C$  is  $I_{\mathcal{K}}$ -invariant, and*
- (iii) *every principal cluster  $\mathfrak{s} \in \Sigma_C$  has  $d_{\mathfrak{s}} \in \mathbb{Z}$  and*

$$\nu_{\mathfrak{s}} := v(c_f) + \sum_{r \in \mathcal{R}} d_{r \wedge \mathfrak{s}} \in 2\mathbb{Z}$$

*where  $r \wedge \mathfrak{s}$  denotes the smallest cluster containing both  $r$  and  $\mathfrak{s}$ .*

When the cluster picture is particularly simple, the following results provide convenient methods for computing local data. These are special cases of [2, Theorem 10.1], [2, Theorem 13.2 & Proposition 13.3] and [22, Theorem 12.4] respectively

**Theorem 2.4.9.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $C$  be a hyperelliptic curve over  $\mathcal{K}$  of genus  $\geq 2$ . Assume that all proper clusters of  $\Sigma_C$  are twins or  $\mathcal{R}$ , and that  $\mathcal{R}$  is not *übereven*. For each twin  $\mathfrak{t} > \mathcal{R}$ , write*

$$c_{\mathfrak{t}} = \begin{cases} 2\delta_{\mathfrak{t}} & \text{if } \epsilon_{\mathfrak{t}}(\text{Frob}_{\mathcal{K}}^{q_{\mathfrak{t}}}) = +1 \\ \gcd(2\delta_{\mathfrak{t}}, 2) & \text{if } \epsilon_{\mathfrak{t}}(\text{Frob}_{\mathcal{K}}^{q_{\mathfrak{t}}}) = -1 \end{cases}$$

where  $q_{\mathfrak{t}}$  is the size of the  $\text{Frob}_{\mathcal{K}}$ -orbit of  $\mathfrak{t}$ . The Tamagawa number of  $\text{Jac}_C$  is then

$$c_{\mathcal{K}}(\text{Jac}_C) = \prod_{\mathfrak{t}} c_{\mathfrak{t}}$$

where the product is taken over representatives of  $\text{Frob}_{\mathcal{K}}$ -orbits of twins.

**Theorem 2.4.10.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and  $C : y^2 = f(x)$  be a semistable hyperelliptic curve over  $\mathcal{K}$  of genus  $\geq 2$ . Assume that all proper clusters of  $\Sigma_C$  are twins or  $\mathcal{R}$ , and that  $\mathcal{R}$  is not *übereven*. Then*

$$w_{\mathcal{K}}(\text{Jac}_C) = (-1)^{\#\{\mathfrak{t} < \mathcal{R}/G_{\mathcal{K}} : \epsilon_{\mathfrak{t}}(\text{Frob}_{\mathcal{K}}^{q_{\mathfrak{t}}}) = +1\}}$$

where  $q_{\mathfrak{t}}$  is the size of the  $\text{Frob}_{\mathcal{K}}$ -orbit of  $\mathfrak{t}$ .

**Theorem 2.4.11.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $C$  be a semistable hyperelliptic curve over  $\mathcal{K}$  of genus  $g \geq 2$ . Assume that all proper clusters of  $\Sigma_C$  are twins or  $\mathcal{R}$ , and that  $\mathcal{R}$  is not *übereven*. Then  $C/\mathcal{K}$  is not deficient.*

### 2.4.3 Chromatic clusters

When studying bihyperelliptic curves we have an analogue of the cluster picture defined in §2.4.1.

**Definition 2.4.12.** Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $B : \{y^2 = f_1(x), z^2 = f_2(x)\}$  be a bihyperelliptic curve over  $\mathcal{K}$ . The *chromatic cluster*

picture  $\Sigma^{\text{chr}}$  of  $B$  is the cluster picture  $\Sigma$  of the hyperelliptic curve  $C : w^2 = f_1(x)f_2(x)$  with a colouring function  $\Sigma \rightarrow \{\text{red, blue, black, purple}\}$ , assigning a colour to each cluster according to the rules:

- (i) clusters of size 1 consisting of a root of  $f_1$  ( $f_2$  respectively) are coloured red  $\bullet$  (blue  $\blacklozenge$  respectively),
- (ii) clusters with an odd number of blue children and an even number of red children (an odd number of red children and an even number of blue children respectively) are coloured blue (red respectively),
- (iii) clusters with an odd number of blue children and an odd number of red children are coloured purple,
- (iv) all other clusters are coloured black,

where purple children are counted as *both* red *and* blue. Blue, red and purple clusters are called *chromatic clusters*. Clusters with purple children, or clusters with both blue and red children have *polychromatic children*, whereas clusters whose only chromatic children are red or blue have *monochromatic children*.

**Example 2.4.13.** Let  $B/\mathbb{Q}_7 : \{y^2 = (x^2 + 7^3)(x - 6), z^2 = (x + 8)(x - 1)(x - 2)\}$ . The chromatic cluster picture of  $B$  is



where, from left to right, the roots are  $\sqrt{-7^3}$ ,  $-\sqrt{-7^3}$ , 6,  $-8$ , 1 and 2.

Note that, without the colouring, this is the cluster picture of  $C$  given in Example 2.4.2.

### 2.4.4 Computing data for semistable bihyperelliptic curves

In order to calculate Tamagawa numbers and root numbers of the Jacobian of a semistable bihyperelliptic curve via Theorems 2.3.3 and 2.3.5, we need to be able to

construct its dual graph. To do this we will use the following special case of [27, Theorems 3.1 & 3.3].

**Theorem 2.4.14.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $B$  be the bihyperelliptic curve arising from distinct hyperelliptic curves  $C_1, C_2$  over  $\mathcal{K}$  such that  $B$  is semistable. Let  $\Sigma^{\text{chr}}$  be the chromatic cluster picture of  $B$  and assume that  $\delta_{\mathcal{R}} \in \mathbb{Z}$ ,  $\mathcal{R}$  is not *übereven* and that all proper clusters are twins or  $\mathcal{R}$ . The dual graph,  $\Upsilon_B$ , consists of one vertex  $v$  when  $\mathcal{R}$  has polychromatic children, and two vertices  $v^+, v^-$  when  $\mathcal{R}$  has monochromatic children. These vertices are connected by chains as follows*

Name	From	To	Length	Condition
$L_{\mathfrak{t}}$	$v^+$	$v^-$	$\delta_{\mathfrak{t}}$	$\mathfrak{t}$ chromatic twin
$L_{\mathfrak{t}}^+$	$v^+$	$v^{\varsigma(\mathfrak{t}, \mathcal{R}), -\varsigma(\mathfrak{t}, \mathcal{R})}$	$2\delta_{\mathfrak{t}}$	$\mathfrak{t}$ black twin
$L_{\mathfrak{t}}^-$	$v^-$	$v^{-\varsigma(\mathfrak{t}, \mathcal{R}), \varsigma(\mathfrak{t}, \mathcal{R})}$		

where  $\varsigma(\mathfrak{t}, \mathcal{R}) = -1$  if  $\mathfrak{t}, \mathcal{R}$  have monochromatic children of opposite colours and 1 otherwise (and  $v^{\pm,+} = v^{\pm,-} = v^{\pm}$  if  $\mathcal{R}$  has monochromatic red children;  $v^{+,\pm} = v^{-,\pm} = v^{\pm}$  if  $\mathcal{R}$  has monochromatic blue children; and  $v^+ = v^- = v$  if  $\mathcal{R}$  has polychromatic children).

Moreover, Frobenius acts on  $\Upsilon_B$  by

(i)  $\text{Frob}_{\mathcal{K}}(v^{\pm}) = v^{\pm \epsilon_{\mathcal{R}_{C_i}, C_i}(\text{Frob}_{\mathcal{K}})}$  when  $\mathcal{R}$  has monochromatic children and  $\mathcal{R}_{C_i}$  is *übereven*,

(ii)  $\text{Frob}_{\mathcal{K}}(L_{\mathfrak{t}}) = \epsilon_{\mathfrak{t}, B} L_{\text{Frob}_{\mathcal{K}}(\mathfrak{t})}$  for each chromatic twin  $\mathfrak{t}$ , and

(iii)  $\text{Frob}_{\mathcal{K}}(L_{\mathfrak{t}}^{\pm}) = \epsilon_{\mathfrak{t}, C_i} L_{\text{Frob}_{\mathcal{K}}(\mathfrak{t})}^{\pm \epsilon_{\mathfrak{t}, C_j}}$  where  $\{i, j\} = \{1, 2\}$  if  $\mathfrak{t}$  has red children and  $\{i, j\} = \{2, 1\}$  if  $\mathfrak{t}$  has blue children, for each black twin  $\mathfrak{t}$

(where  $-L$  is the same loop but inverted).

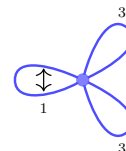
**Remark 2.4.15.** To compute  $\epsilon_{\mathfrak{t}, C_1}$  when  $\mathfrak{t}$  has blue children (or  $\epsilon_{\mathfrak{t}, C_2}$  when  $\mathfrak{t}$  has red children) we view  $\mathfrak{t}$  as a  $\mathcal{K}$ -adic disk containing no roots.

**Remark 2.4.16.** To determine whether or not a bihyperelliptic curve  $B$  is semistable, we use Corollary 3.3.4 (which phrases this in terms of the hyperelliptic curves  $B$  projects onto) and Theorem 2.4.8.

**Example 2.4.17.** Let  $B/\mathbb{Q}_7$  be as in Example 2.4.13, arising from the hyperelliptic curves  $C_1/\mathbb{Q}_7 : y^2 = (x^2 + 7^3)(x - 6)$ ,  $C_2/\mathbb{Q}_7 : z^2 = (x + 8)(x - 1)(x - 2)$ . Then

$$\Sigma_B^{\text{chr}} = \boxed{\textcircled{+}_{3/2} \textcircled{-}_1 \blacklozenge \blacklozenge}_0, \quad \Sigma_{C_1} = \boxed{\textcircled{+}_{3/2} \textcircled{\phantom{+}}}_0, \quad \Sigma_{C_2} = \boxed{\blacklozenge \blacklozenge}_0.$$

By Theorem 2.4.14, the dual graph  $\Upsilon_B$  has one vertex with one loop of length 1 (inverted by Frobenius) and two loops of length 3 (fixed by Frobenius).



## 2.5 Brauer relations

Isogenies between Jacobians of curves serve as crucial ingredients in many constructions presented in this thesis. A rich source of such maps are representation theoretic objects called ‘Brauer relations’.

**Definition 2.5.1.** Let  $G$  be a finite group and  $\mathcal{H}$  a set of representatives of the subgroups of  $G$  up to conjugacy. We call an expression

$$\sum_i H_i - \sum_j H'_j \quad (H_i, H'_j \in \mathcal{H})$$

a *Brauer relation* for  $G$  if  $\bigoplus_i \mathbb{C}[G/H_i] \cong \bigoplus_j \mathbb{C}[G/H'_j]$  (or equivalently, the character  $\sum_i \text{Ind}_{H_i}^G \mathbf{1} - \sum_j \text{Ind}_{H'_j}^G \mathbf{1} = 0$ ).

We recall that the induced character of  $\mathbf{1}$  has a particularly nice description.

**Lemma 2.5.2.** *Let  $G$  be a finite group with subgroup  $H$ . For  $g \in G$ ,*

$$\text{Ind}_H^G \mathbf{1}(g) = \#\text{fix}_{G/H}(g)$$

*i.e. the number of left cosets  $G/H$  fixed under left multiplication by  $g$ .*

**Example 2.5.3.** Let  $G = C_2 \times C_2 := \langle \tau_1, \tau_2 \rangle$  and write  $\chi_{+,+}$ ,  $\chi_{+,-}$ ,  $\chi_{-,+}$ ,  $\chi_{-,-}$  for the irreducible representations, where the subscripts denote the images of  $\tau_1$ ,  $\tau_2$  respectively.

The permutation representations of  $G$  are displayed in the table below.

$H$	$\mathbb{C}[G/H]$
$1$	$\chi_{+,+} \oplus \chi_{+,-} \oplus \chi_{-,+} \oplus \chi_{-,-}$
$\langle \tau_1 \rangle$	$\chi_{+,+} \oplus \chi_{+,-}$
$\langle \tau_2 \rangle$	$\chi_{+,+} \oplus \chi_{-,+}$
$\langle \tau_1 \tau_2 \rangle$	$\chi_{+,+} \oplus \chi_{-,-}$
$\langle \tau_1, \tau_2 \rangle$	$\chi_{+,+}$

From this, we see that  $G$  has a unique Brauer relation (up to scaling by  $\mathbb{Z}$ ), given by:

$$\langle \tau_1 \rangle + \langle \tau_2 \rangle + \langle \tau_1 \tau_2 \rangle - 2(C_2 \times C_2) - 1.$$

**Example 2.5.4.** Let  $G = S_3 := \langle \sigma, \tau \rangle$ , where  $\sigma^3 = \tau^2 = 1$ . Write  $\mathbf{1}$ ,  $\epsilon$ ,  $\rho$  for the irreducible representations of  $S_3$ , where  $\epsilon$  has dimension 1 and  $\rho$  has dimension 2.

The permutation representations of  $G$  are displayed in the table below.

$H$	$\mathbb{C}[G/H]$
$1$	$\mathbf{1} \oplus \epsilon \oplus \rho^{\oplus 2}$
$\langle \tau \rangle$	$\mathbf{1} \oplus \rho$
$\langle \sigma \rangle$	$\mathbf{1} \oplus \epsilon$
$\langle \sigma, \tau \rangle$	$\mathbf{1}$

From this, we see that  $G$  has a unique Brauer relation (up to scaling by  $\mathbb{Z}$ ), given by:

$$2\langle \tau \rangle + \langle \sigma \rangle - 2S_3 - 1.$$

**Example 2.5.5.** Let  $G = D_8 := \langle \sigma, \tau \rangle$ , where  $\sigma^4 = \tau^2 = 1$  and  $\sigma\tau\sigma = \tau^{-1}$ .

It can be checked that  $G$  has the following 3 (linearly independent) Brauer

relations:

$$\begin{aligned} \langle \tau \rangle + \langle \sigma^2, \sigma\tau \rangle - \langle \sigma^2, \tau \rangle - \langle \tau\sigma \rangle, \\ \langle \sigma \rangle + \langle \sigma^2, \sigma\tau \rangle + \langle \sigma^2, \tau \rangle - \langle \sigma^2 \rangle - 2D_8, \\ \langle \sigma^2 \rangle + 2\langle \tau\sigma \rangle - 2\langle \sigma^2, \sigma\tau \rangle - 1. \end{aligned}$$

## 2.6 Regulator constants

Here we introduce the concept of regulator constants, an extended discussion of which can be found in [18]. We record some of their key properties. This theory will be implemented in Chapter 4, where we will extract information about ranks from regulators.

**Definition 2.6.1.** Let  $K$  be a field of characteristic 0. Let  $G$  be a finite group,  $\rho$  a self-dual  $KG$ -representation and  $\Theta = \sum_i H_i - \sum_j H'_j$  a Brauer relation for  $G$ . Fix a  $G$ -invariant, non-degenerate,  $K$ -bilinear pairing  $\langle, \rangle$  on  $\rho$  with values in some extension  $L$  of  $K$  and define the *regulator constant* to be

$$\mathcal{C}_\Theta(\rho) = \frac{\prod_i \det\left(\frac{1}{\#H_i} \langle, \rangle \mid \rho^{H_i}\right)}{\prod_j \det\left(\frac{1}{\#H'_j} \langle, \rangle \mid \rho^{H'_j}\right)} \in K^\times / K^{\times 2},$$

where (for  $H \leq G$ )  $\rho^H$  is the space of  $H$ -invariant vectors of  $\rho$  and  $\det\left(\frac{1}{\#H} \langle, \rangle \mid V\right)$  is the determinant of the matrix with  $(i, j)$ -th entry  $\frac{1}{\#H} \langle e_i, e_j \rangle$  for any  $K$ -basis  $\{e_i\}$  of  $V$ .

That  $\mathcal{C}_\Theta(\rho)$  lies in  $K^\times / K^{\times 2}$ , rather than  $L^\times / K^{\times 2}$ , is true since the pairing can be chosen to be  $K$ -valued.

**Remark 2.6.2.** It is important to note that that  $\mathcal{C}_\Theta(\rho)$  is well-defined, non-zero and independent of the choice of pairing  $\langle, \rangle$  (see [18, Lemma 2.15, Theorem 2.17]).

**Example 2.6.3.** Let  $G = C_2 \times C_2 := \langle \tau_1, \tau_2 \rangle$  and  $\Theta = \langle \tau_1 \rangle + \langle \tau_2 \rangle + \langle \tau_1\tau_2 \rangle - 2G - 1$ .

Write  $\chi_{+,+}$ ,  $\chi_{+,-}$ ,  $\chi_{-,+}$ ,  $\chi_{-,-}$  for the irreducible characters, where the subscripts denote the images of  $\tau_1$ ,  $\tau_2$  respectively.



We note that  $\chi_{+,+}^H = \mathbb{C}$  for each  $H \leq G$ , therefore

$$\mathcal{C}_\Theta(\chi_{+,+}) = \frac{(\frac{1}{2})^3}{1 \cdot (\frac{1}{4})^2} = 2.$$

For the other characters,  $\chi^H = \mathbb{C}$  for  $H \in \{1, H'\}$  (where  $H'$  has order 2) and 0 otherwise, and so

$$\mathcal{C}_\Theta(\chi_{+,-}) = \mathcal{C}_\Theta(\chi_{-,+}) = \mathcal{C}_\Theta(\chi_{-,-}) = \frac{1^2 \cdot \frac{1}{2}}{1^3} = 2 \pmod{\mathbb{Q}^{\times 2}}.$$

**Lemma 2.6.4** ([18], Corollary 2.18). *Let  $K$  be a field of characteristic 0. Let  $G$  be a finite group,  $\rho_1, \rho_2$  be self-dual  $KG$ -representations and  $\Theta$  be a Brauer relation for  $G$ . Then,*

$$\mathcal{C}_\Theta(\rho_1 \oplus \rho_2) = \mathcal{C}_\Theta(\rho_1)\mathcal{C}_\Theta(\rho_2).$$

## 2.7 Hilbert symbols

Here we remind the reader of the definition of the Hilbert symbol and of its global behaviour. More details can be found in [45].

**Definition 2.7.1.** Let  $\mathcal{K}$  be a local field of characteristic 0 and let  $a, b \in \mathcal{K}^\times$ . The *Hilbert symbol of  $a, b$  relative to  $\mathcal{K}$*  is

$$(a, b)_\mathcal{K} = \begin{cases} +1 & z^2 - ax^2 - by^2 = 0 \text{ has a solution } (z, x, y) \neq (0, 0, 0) \text{ in } \mathcal{K}^3, \\ -1 & \text{otherwise.} \end{cases}$$

If  $\mathcal{K} = K_v$  where  $K$  is a number field and  $v$  is a place of  $K$ , we write  $(a, b)_v$ .

**Remark 2.7.2.** The Hilbert symbol is symmetric, bimultiplicative and non-degenerate [45, Theorem 4.4].

**Theorem 2.7.3** (E.g. [45], 5.4). *Let  $K$  be a number field and  $a, b \in K^\times$ . Then*

$$\prod_{v \text{ place of } K} (a, b)_v = +1.$$

We now record some identities concerning Hilbert symbols which simplify their computation.

**Lemma 2.7.4.** (i) *If  $\mathcal{K} \cong \mathbb{C}$  then  $(a, b)_{\mathcal{K}} = +1$ .*

(ii) *If  $\mathcal{K} \cong \mathbb{R}$  then  $(a, b)_{\mathcal{K}} = -1$  if and only if  $a, b < 0$ .*

**Lemma 2.7.5** ([24], Lemma 9.8 and [1]). *Let  $\mathcal{K}$  be a local field of characteristic 0 and let  $a, b \in \mathcal{K}^{\times}$ . Then*

(i)  *$(a, b)_{\mathcal{K}} = (a + b, -ab)_{\mathcal{K}}$  whenever  $a + b \in \mathcal{K}^{\times}$ , and*

(ii)  *$(a, b)_{\mathcal{K}} = (a_0, b)_{\mathcal{L}}$  whenever  $a = N_{\mathcal{L}/\mathcal{K}}a_0$  for  $a_0 \in \mathcal{L}^{\times}$  and  $\mathcal{L}/\mathcal{K}$  a finite extension.*

**Lemma 2.7.6** ([24], Lemma 10.1). *Let  $\mathcal{K}/\mathbb{Q}_2$  be a finite extension. If  $a = \square \cdot (1 + 4t) \in \mathcal{K}^{\times}$  for some  $t \in \mathcal{O}_{\mathcal{K}}$ , then  $(a, u)_{\mathcal{K}} = +1$  for all  $u \in \mathcal{O}_{\mathcal{K}}^{\times}$ .*

## Chapter 3

# Automorphisms, Brauer Relations and Isogenies

Historically, isogenies between abelian varieties have proven to be valuable tools for deducing information about ranks ([3], [36], [47], [24], [14], [19], [40]). In this chapter, we describe the manner in which the automorphism group of a curve encodes isogenies between Jacobians. In particular, we present a new proof of a theorem of Kani and Rosen [32, Theorem 3] (=Theorem 3.2.2), which asserts that each Brauer relation for the automorphism group of a curve gives rise to such an isogeny. This new strategy involves comparing the Zeta functions of relevant quotient curves.

We provide two examples of isogenies which arise in this way and will be important in later parts of this thesis.

The final section of this chapter provides an explicit description of the isogeny arising from a Brauer relation (due to Morgan, [23]). We include this for the interested reader, but it will not be used in developing the theory of the rest of the thesis. This construction is important in proving of a result (of Konstantinou and Morgan) concerning parities of ranks of Selmer groups, which we state in the next chapter.

### 3.1 Counting points

To illustrate our approach, let  $K$  be a field and  $f(x) \in K[x]$  be a separable quadratic with  $f(0) \neq 0$ . Define genus 1 curves  $E : y^2 = xf(x)$  and  $E' : y^2 = f(x^2)$  which are

related by the double cover

$$E' \rightarrow E, \quad (x, y) \mapsto (x^2, xy).$$

When we consider the elliptic curves  $E$  and  $\text{Jac}_{E'}$ , this cover translates into the 2-isogeny used in [17] to prove that the 2-parity conjecture holds for  $E$  (see Example 3.3.5).

The existence of an isogeny  $E \rightarrow \text{Jac}_{E'}$  can be seen from the equality of the  $L$ -functions of the elliptic curves, which can be observed by comparing the number of points they have over finite fields. We illustrate this point count in a more general setting.

Let  $K$  be a field and  $f_1(x), f_2(x) \in K[x]$  be such that  $f_1(x)f_2(x)$  is separable. Consider the diagram:

$$\begin{array}{ccccc}
 & & X : \{y^2 = f_1(x), z^2 = f_2(x)\} & & \\
 & \swarrow & \downarrow & \searrow & \\
 X_1 : y^2 = f_1(x) & & X_0 : w^2 = f_1(x)f_2(x) & & X_2 : z^2 = f_2(x) \\
 & \searrow & \downarrow & \swarrow & \\
 & & \mathbb{P}^1 & & 
 \end{array}$$

**Figure 3.1:**  $C_2 \times C_2$  diagram of covers of curves

where  $\mathbb{P}^1$  has coordinate  $x$ .

**Remark 3.1.1.** If  $f_1(x) = f(x)$  is a quadratic and  $f_2(x) = x$ , then  $X_1, X_2$  have genus 0 and  $X_0 = E, X = E'$  (where  $E, E'$  are as in the discussion above).

Recall that, for a curve  $C$  defined over a number field  $K$  and  $\mathfrak{p}$  a prime of  $K$  of good reduction, the Zeta function is

$$Z_{\mathfrak{p}}(C, T) = \exp \left( \sum_{n \geq 1} \frac{\#C_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^n})}{n} T^n \right)$$

where  $C_{\mathfrak{p}}$  denotes the reduction of  $C$  to the residue field  $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ .

**Proposition 3.1.2.** *Let  $K$  be a number field and  $\mathfrak{p}$  be a prime of  $K$  of good reduction for  $X_1, X_2, X_0$  and  $X$ . Then,*

$$Z_{\mathfrak{p}}(X_1, T)Z_{\mathfrak{p}}(X_2, T)Z_{\mathfrak{p}}(X_0, T) = Z_{\mathfrak{p}}(X, T)Z_{\mathfrak{p}}(\mathbb{P}^1, T)^2.$$

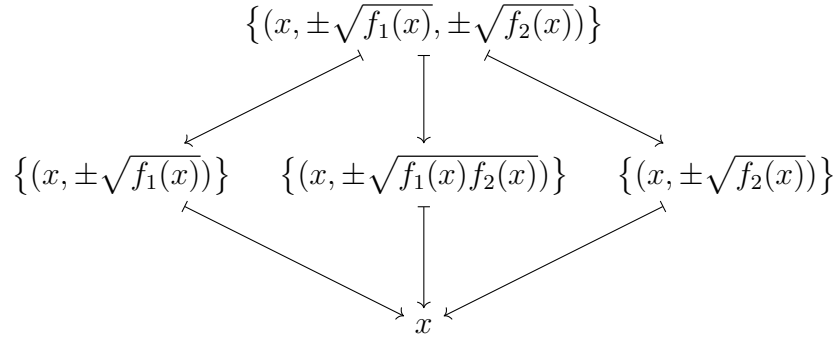
*Proof.* By definition of  $Z_{\mathfrak{p}}$ , the result follows upon showing that for each  $n \geq 1$ ,

$$\#(X_1)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^n}) + \#(X_2)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^n}) + \#(X_0)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^n}) = \#X_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^n}) + 2\#\mathbb{P}_{\mathfrak{p}}^1(\mathbb{F}_{\mathfrak{p}^n}).$$

Write  $\pi_{X_1} : (X_1)_{\mathfrak{p}} \rightarrow \mathbb{P}_{\mathfrak{p}}^1$ ,  $(x, y) \mapsto x$  and similarly for  $\pi_{X_2}, \pi_{X_0}, \pi_X$ . We instead show that for each  $n \geq 1$  and each  $x \in \mathbb{P}_{\mathfrak{p}}^1(\mathbb{F}_{\mathfrak{p}^n})$ ,

$$\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) + \#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) + \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) + 2. \quad (3.1)$$

Suppose first that  $x \in \mathbb{A}_{\mathfrak{p}}^1(\mathbb{F}_{\mathfrak{p}^n})$ , then  $\pi_{X_1}^{-1}(x), \pi_{X_2}^{-1}(x), \pi_{X_0}^{-1}(x)$ , and  $\pi_X^{-1}(x)$  are as displayed below.



**Case I:** Suppose that  $f_1(x), f_2(x) \neq 0$  in  $\mathbb{F}_{\mathfrak{p}^n}$ . If both  $f_1(x), f_2(x)$  are squares in  $\mathbb{F}_{\mathfrak{p}^n}$ , then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$  and  $\#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 4$ . If  $f_1(x)$  is a square in  $\mathbb{F}_{\mathfrak{p}^n}$  and  $f_2(x)$  is not, then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$  and  $\#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 0$  (similarly when  $f_2(x)$  is a square and  $f_1(x)$  is not). Finally, if neither  $f_1(x)$  nor  $f_2(x)$  are squares in  $\mathbb{F}_{\mathfrak{p}^n}$ , then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 0$  and  $\#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$ . In each case, (3.1) is satisfied.

**Case II:** Suppose that  $f_1(x) = 0$  and  $f_2(x) \neq 0$  in  $\mathbb{F}_{\mathfrak{p}^n}$  (or  $f_1(x) \neq 0$  and  $f_2(x) = 0$ ). If  $f_2(x)$  is a square in  $\mathbb{F}_{\mathfrak{p}^n}$ , then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 1$  and

$\#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$ . Conversely, if  $f_2(x)$  is not a square in  $\mathbb{F}_{\mathfrak{p}^n}$ , then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 1$  and  $\#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 0$ . Again, in both cases, (3.1) is satisfied.

Now suppose that  $x \in (\mathbb{F}_{\mathfrak{p}}^1 - \mathbb{A}_{\mathfrak{p}}^1)(\mathbb{F}_{\mathfrak{p}^n})$ . If  $\deg f_1, \deg f_2$  are both even, then  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$  and  $\#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 4$ . Otherwise, two of  $\#\pi_{X_1}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}), \#\pi_{X_2}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}), \#\pi_{X_0}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n})$  equal 1 with the other equalling 2 and  $\#\pi_X^{-1}(x)(\mathbb{F}_{\mathfrak{p}^n}) = 2$ . In both cases, (3.1) is satisfied.  $\square$

This identity of Zeta functions of curves can be converted into one of  $L$ -functions of Jacobians. Via a result of Faltings, this then guarantees the existence of an isogeny (this argument appears in more detail within the proof of Theorem 3.2.2).

**Theorem 3.1.3.** *When  $K$  is a number field, there exists an isogeny  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_X$ .*

We will study this isogeny in more detail in §3.3 since it will play an important role in later chapters. In particular, we will eventually use it to obtain results concerning the 2-parity conjecture for certain hyperelliptic curves.

## 3.2 Exhibiting isogenies from Brauer relations

Here we present the analogue of the Zeta function identity given in Proposition 3.1.2 for general curves and explain why such a relationship guarantees the existence of an isogeny. The description of the isogeny is not given here, for this we refer the reader to §3.5.

**Proposition 3.2.1.** *Let  $K$  be a number field and  $X$  a curve over  $K$ . Let  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . If  $\mathfrak{p}$  is a prime of  $K$  of good reduction for each quotient curve  $X_{H_i}, X_{H'_j}$  then*

$$\prod_i Z_{\mathfrak{p}}(X_{H_i}, T) = \prod_j Z_{\mathfrak{p}}(X_{H'_j}, T).$$

Before proving this result we highlight the consequences of interest to us, in particular, how it can be converted into a statement concerning Jacobians of curves.

For  $A$  an abelian variety over a number field  $K$ , its  $L$ -function is

$$L(A, s) := \prod_{\mathfrak{p} \text{ prime of } K} L_{\mathfrak{p}}(A, |\mathfrak{p}|^{-s})^{-1},$$

where  $L_{\mathfrak{p}}(A, T) \in \mathbb{Z}[T]$  has degree at most  $2 \dim A$  and is known as the  $L$ -factor of  $A$  at  $\mathfrak{p}$ .

Suppose that  $A = \text{Jac}_X$  where  $X$  is a curve over  $K$ . For primes  $\mathfrak{p}$  at which  $X$  has good reduction (all but finitely many), the  $L$ -factor can be computed directly from the Zeta function. In particular, there are polynomials  $P_0(X, T), P_2(X, T) \in \mathbb{Z}[T]$  such that

$$L_{\mathfrak{p}}(\text{Jac}_X, T) = Z_{\mathfrak{p}}(X, T)P_0(X, T)P_2(X, T).$$

This equality allows us to convert results concerning Zeta functions of curves into results concerning the  $L$ -functions of their Jacobians.

**Theorem 3.2.2.** *Let  $K$  be a number field and  $X$  a curve over  $K$ . Let  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . Then,*

$$(i) \prod_i L(\text{Jac}_{X_{H_i}}, s) = \prod_j L(\text{Jac}_{X_{H'_j}}, s),$$

(ii) *there's a  $K$ -isogeny*

$$\prod_i \text{Jac}_{X_{H_i}} \rightarrow \prod_j \text{Jac}_{X_{H'_j}},$$

$$(iii) \sum_i \text{rk}(\text{Jac}_{X_{H_i}}) = \sum_j \text{rk}(\text{Jac}_{X_{H'_j}}).$$

*Proof.* We need only prove (i) since (ii) follows immediately using the multiplicativity of  $L$  and a result of Faltings ([26, §5, Corollary 2]), and (iii) follows from (ii) using that the rank is invariant under isogeny.

Let  $\mathfrak{p}$  be a prime as in Proposition 3.2.1, then

$$\begin{aligned}
\prod_i L_{\mathfrak{p}}(\text{Jac}_{X_{H_i}}, T) &= \prod_i Z_{\mathfrak{p}}(X_{H_i}, T) \cdot \prod_i P_0(X_{H_i}, T) \cdot \prod_i P_2(X_{H_i}, T) \\
&= \prod_j Z_{\mathfrak{p}}(X_{H'_j}, T) \cdot \prod_i P_0(X_{H_i}, T) \cdot \prod_i P_2(X_{H_i}, T) \\
&= \prod_j L_{\mathfrak{p}}(\text{Jac}_{X_{H'_j}}, T) \cdot \frac{\prod_i P_0(X_{H_i}, T) \cdot \prod_i P_2(X_{H_i}, T)}{\prod_j P_0(X_{H'_j}, T) \cdot \prod_j P_2(X_{H'_j}, T)} \\
&= \prod_j L_{\mathfrak{p}}(\text{Jac}_{X_{H'_j}}, T)
\end{aligned}$$

having deduced the final equality using that the roots of  $L_{\mathfrak{p}}$ ,  $P_0$  and  $P_2$  have absolute value  $(\sqrt{\#\mathbb{F}_{\mathfrak{p}}})^{-1}$ , 1 and  $(\#\mathbb{F}_{\mathfrak{p}})^{-1}$  respectively (by the Riemann hypothesis part of the Weil conjectures, [13]) and the constant terms of  $\prod_i L_{\mathfrak{p}}(\text{Jac}_{X_{H_i}}, T)$ ,  $\prod_j L_{\mathfrak{p}}(\text{Jac}_{X_{H'_j}}, T)$  are equal.

Since this equality of  $L$ -factors holds for almost all primes  $\mathfrak{p}$ , it must in fact hold at every prime ([26, §5, Corollary 2]) which gives the required identity concerning  $L$ -functions.  $\square$

**Remark 3.2.3.** We note that Theorem 3.2.2 applies when  $X$  is not geometrically connected, using the notion of the Jacobian as given in [23, §A.6].

The remainder of this section is dedicated to proving Proposition 3.2.1.

**Notation 3.2.4.** Fix  $n \in \mathbb{N}$  and write  $C_n = \langle h \rangle$ . For each  $m \in \mathbb{N}$ ,

$$\rho_m(h) = \begin{cases} \exp(2\pi i/m) & m \mid n \\ 0 & m \nmid n \end{cases}$$

defines a (1-dimensional) representation of  $C_n$ . Let  $G$  be a finite group, then  $\tilde{\rho}_m((g, h)) = \rho_m(h)$  for each  $g \in G$  defines a (1-dimensional) representation of  $G \times C_n$ .

**Lemma 3.2.5.** *Let  $S$  be a set acted on by  $C_n$ . The number of orbits of  $S$  of length divisible by  $m \in \mathbb{N}$  is  $\langle \rho_m, \mathbb{C}[S] \rangle_{C_n}$ .*



*Proof.* Suppose that  $m \mid n$ , otherwise the result is clear. Fix  $O$  to be an orbit of the action. Since  $C_n$  acts transitively on  $O$ , there's a subgroup  $H \leq C_n$  such that  $O \cong C_n/H$  (as sets with  $C_n$ -actions). Therefore,

$$\langle \rho_m, \mathbb{C}[O] \rangle_{C_n} = \langle \rho_m, \text{Ind}_H^{C_n} \mathbb{1} \rangle_{C_n} = \begin{cases} 1 & m \mid \#O \\ 0 & m \nmid \#O \end{cases}$$

and the result follows using that  $\langle \rho_m, \mathbb{C}[S] \rangle_{C_n} = \sum \langle \rho_m, \mathbb{C}[O] \rangle_{C_n}$  where the sum is taken over the orbits of  $S$ .  $\square$

**Lemma 3.2.6.** *Let  $G$  be a finite group. Let  $S'$  be a set acted on by  $G \times C_n$ . The number of  $G$ -orbits of  $S'$  in a  $C_n$ -orbit of length divisible by  $m \in \mathbb{N}$  is  $\langle \tilde{\rho}_m, \mathbb{C}[S'] \rangle_{G \times C_n}$ .*

*Proof.* Let  $S$  be the set of  $G$ -orbits of  $S'$ . Since  $\mathbb{C}[S] \cong \mathbb{C}[S']^G$  as  $C_n$ -representations, Lemma 3.2.5 says that the number of  $G$ -orbits of  $S'$  in a  $C_n$ -orbit with length divisible by  $m \in \mathbb{N}$  is  $\langle \rho_m, \mathbb{C}[S']^G \rangle_{C_n}$ . Since  $\tilde{\rho}_m$  acts trivially on  $G$ , this is equal to  $\langle \tilde{\rho}_m, \mathbb{C}[S'] \rangle_{G \times C_n}$ .  $\square$

**Lemma 3.2.7.** *Let  $G$  be a finite group and  $\sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . Let  $S'$  be a set acted on by  $G \times C_n$ . For each  $m \in \mathbb{N}$*

$$\sum_i \theta_m(H_i) - \sum_j \theta_m(H'_j) = 0$$

where (for  $H \leq G$ )  $\theta_m(H)$  denotes the number of  $H$ -orbits of  $S'$  in a  $C_n$ -orbit with length divisible by  $m \in \mathbb{N}$ .

*Proof.* Fix  $m \in \mathbb{N}$  and  $H \leq G$ , then

$$\begin{aligned} \theta_m(H) &\stackrel{\text{Lemma 3.2.6}}{=} \langle \text{Res}_{H \times C_n}^{G \times C_n} \tilde{\rho}_m, \text{Res}_{H \times C_n}^{G \times C_n} \mathbb{C}[S'] \rangle_{H \times C_n} \\ &\stackrel{\text{Frobenius Reciprocity}}{=} \langle \tilde{\rho}_m \otimes \mathbb{C}[(G \times C_n)/(H \times C_n)], \mathbb{C}[S'] \rangle_{G \times C_n}. \end{aligned}$$

The Brauer relation  $\sum_i H_i - \sum_j H'_j$  for  $G$  lifts to the Brauer relation  $\sum_i (H_i \times C_n) - \sum_j (H'_j \times C_n)$  for  $G \times C_n$  and so the result holds using the expression for  $\theta_m(H)$  above.  $\square$

*Proof of Proposition 3.2.1.* For each  $H \leq G$  write  $\bar{\pi}_H : (X_H)_{\mathfrak{p}} \rightarrow (X_G)_{\mathfrak{p}}$  for the projection map on the reduced curves. As in the proof of Proposition 3.1.2, to deduce the result it is enough to show that for each  $m \geq 1$  and each  $x \in (X_G)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^m})$ ,

$$\sum_i \#\bar{\pi}_{H_i}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^m}) - \sum_j \#\bar{\pi}_{H'_j}^{-1}(x)(\mathbb{F}_{\mathfrak{p}^m}) = 0.$$

Write  $C_n := \langle \text{Frob}_{\mathfrak{p}} \rangle$  and  $S' := \bar{\pi}_1^{-1}(x)(\overline{\mathbb{F}_{\mathfrak{p}}})$  (acted on by  $G \times C_n$ ). We observe that for  $H \leq G$ ,

$$\pi_H^{-1}(x)(\mathbb{F}_{\mathfrak{p}^m}) \cong \{H\text{-orbits of } S' \text{ in a } C_n\text{-orbit of length divisible by } m\}$$

and so the above identity holds by Lemma 3.2.7.  $\square$

### 3.3 Explicit construction of isogenies for $C_2 \times C_2$

We now explain how the isogeny detailed in Theorem 3.1.3 can be observed from Theorem 3.2.2. We explicitly describe the isogeny and discuss its properties which will be important in later chapters.

**Notation 3.3.1.** Let  $K$  be a field of characteristic 0 and  $f_1(x), f_2(x) \in K[x]$  be such that  $f_1(x)f_2(x)$  is separable. Define a bihyperelliptic curve over  $K$  by

$$X : \{y^2 = f_1(x), z^2 = f_2(x)\}.$$

The group  $G = C_2 \times C_2 := \langle \tau_1, \tau_2 \rangle$  acts on  $X$  where  $\tau_1 : (x, y, z) \mapsto (x, y, -z)$ ,  $\tau_2 : (x, y, z) \mapsto (x, -y, z)$ . The unique Brauer relation for  $G$ , up to multiplication by integers, is given by

$$\langle \tau_1 \rangle + \langle \tau_2 \rangle + \langle \tau_1 \tau_2 \rangle - 2G - \{1\}$$

(see Example 2.5.3). When  $K$  is a number field, applying Theorem 3.2.2(ii) with respect to this gives the existence of an isogeny  $\text{Jac}_{X_{\langle \tau_1 \rangle}} \times \text{Jac}_{X_{\langle \tau_2 \rangle}} \times \text{Jac}_{X_{\langle \tau_1 \tau_2 \rangle}} \rightarrow \text{Jac}_X$ , since  $X_G = \mathbb{P}^1$  with parameter  $x$ , realised by the map  $\pi_x : (x, y, z) \mapsto x$ . We now

describe this explicitly using the models for the quotient curves given in Example 2.1.13 and the induced maps between Jacobians described in §2.1.2. We refer the reader to Figure 3.1 for a pictorial summary.

**Theorem 3.3.2.** *Let  $K$  be a field of characteristic 0 and  $f_1(x), f_2(x) \in K[x]$  be such that  $f_1(x)f_2(x)$  is separable. Define  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  and  $X : \{y^2 = f_1(x), X_2 : z^2 = f_2(x)\}$ . Then*

$$\psi := ((\pi_1)_*, (\pi_2)_*, (\pi_0)_*) : \text{Jac}_X \rightarrow \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0},$$

$$\phi := (\pi_1)^* + (\pi_2)^* + (\pi_0)^* : \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_X.$$

are mutually-dual isogenies, where  $\pi_1 : (x, y, z) \mapsto (x, y) \in X_1$ ,  $\pi_2 : (x, y, z) \mapsto (x, z) \in X_2$  and  $\pi_0 : (x, y, z) \mapsto (x, yz) \in X_0$  whenever  $(x, y, z) \in X$ . Moreover, they satisfy  $\psi \circ \phi = [2] = \phi \circ \psi$ .

*Proof.* That  $\psi$  and  $\phi$  are isogenies follows from their compositions being the multiplication-by-two maps, which is argued below. Their mutual duality is noted in Example 3.5.4, by applying Theorem 3.5.2 (this is essentially due to the mutual-duality of  $\pi_*$  and  $\pi^*$ , see Lemma 2.1.9).

Let  $P \in X(\overline{K})$ , then  $\phi \circ \psi$  maps the divisor  $[P]$  to

$$3[P] + [\tau_1 P] + [\tau_2 P] + [\tau_1 \tau_2 P] = 2[P] + (\pi_x)^*((\pi_x)_*(P)).$$

Therefore  $(\phi \circ \psi)(D) = 2D + (\pi_x)^*((\pi_x)_*(D))$  when  $D \in \text{Div}(X)$ . When the degree of  $D$  is 0, noting that  $(\pi_x)_*(D) \in \text{Div}^0(\mathbb{P}^1)$  and hence  $(\pi_x)^*((\pi_x)_*(D)) \in \text{Div}^0(X)$  are principal, gives that  $\phi \circ \psi$  is multiplication by 2 on  $\text{Jac}_X$ .

Now consider the composition  $\psi \circ \phi$ . Let  $P \in X_1(\overline{K})$ , then  $\psi \circ \phi$  maps  $([P], 0, 0)$  to

$$(2[P], (\pi_2)_* \circ (\pi_1)^*(P), (\pi_0)_* \circ (\pi_1)^*(P))$$

where  $(\pi_2)_* \circ (\pi_1)^*(P)$  and  $(\pi_0)_* \circ (\pi_1)^*(P)$  are the pullbacks to  $\text{Div}(X_2)$  and  $\text{Div}(X_0)$  of a point on  $\mathbb{P}^1$ . If  $D \in \text{Div}^0(X_1)$  then  $(\pi_2)_* \circ (\pi_1)^*(D)$  and  $(\pi_0)_* \circ (\pi_1)^*(D)$  are principal (since  $(\pi_1)^*(D)$  is) and so  $\psi \circ \phi$  sends points of  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$

of the form  $(D, 0, 0)$  to  $(2D, 0, 0)$ . Arguing similarly gives the result for points of the form  $(0, D, 0)$  and  $(0, 0, D)$  and therefore that  $\psi \circ \phi$  is multiplication by 2 on  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$ .  $\square$

**Corollary 3.3.3.** *The degree of  $\phi$  and  $\psi$  is  $2^{\deg f_1 + \deg f_2 - 3}$  when both  $\deg f_1, \deg f_2$  are even, and  $2^{\deg f_1 + \deg f_2 - 2}$  otherwise.*

*Proof.* Since  $\psi \circ \phi = [2]$  on  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$ ,

$$\begin{aligned} \deg \psi \circ \phi &= 2^{2 \dim(\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0})} \\ &= 2^2 \left( \left\lfloor \frac{\deg f_1 - 1}{2} \right\rfloor + \left\lfloor \frac{\deg f_2 - 1}{2} \right\rfloor + \left\lfloor \frac{\deg f_1 + \deg f_2 - 1}{2} \right\rfloor \right). \end{aligned}$$

The result then follows from the mutual duality of  $\phi$  and  $\psi$ , i.e. that  $\deg \phi = \deg \psi$ .  $\square$

**Corollary 3.3.4.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$ . The bihyperelliptic curve  $X/\mathcal{K}$  is semistable if and only if the hyperelliptic curves  $X_1, X_2, X_0/\mathcal{K}$  are all semistable.*

*Proof.* Since  $\text{Jac}_X$  is isogenous to  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$ , their Tate modules are isomorphic ([64]). By [31, Proposition 3.5], semistability can be determined from the Tate module.  $\square$

**Example 3.3.5.** Let  $f_1(x) = ax^2 + bx + c \in K[x]$ ,  $f_2(x) = x$  so that  $X_0 : w^2 = ax^3 + bx^2 + cx$  and  $X : z^2 = ay^4 + by^2 + c$ .

Theorem 3.3.2 gives a 2-isogeny  $\phi : X_0 \rightarrow \text{Jac}_X$  between elliptic curves. Applying Lemma 2.1.6, we see that

$$\begin{aligned} \text{Jac}_X : Z^2 &= Y^3 - 27(b^2 + 12ac)Y + 54b(b^2 - 36ac) \\ &\cong E : Z^2 = Y^3 - 2bY^2 + (b^2 - 4ac)Y, \end{aligned}$$

where the isomorphism comes from shifting the 2-torsion point  $(-6b, 0)$  to  $(0, 0)$ . In

the case when  $a = 1$ ,  $\phi$  must therefore be the classical 2-isogeny

$$X_0 \ni (x, w) \mapsto (x + b + cx^{-1}, w - cx^{-2}w) \in E$$

(for example, see [17]).

**Example 3.3.6.** Let  $f_1(x) = d \in K^\times$  and  $f_2(x)$  be a cubic.

Theorem 3.3.2 gives a 2-isogeny

$$\phi : E \times E_d \rightarrow \text{Jac}_X \cong \text{Res}_{K(\sqrt{d})/K} E$$

where  $E = X_2 : z^2 = f_2(x)$ ,  $E_d = X_0 : w^2 = df_2(x)$  is the quadratic twist of  $E$  by  $d$  and, since  $X : \{y^2 = dz^2 = f_2(x)\}$ , the isomorphism on the right-hand-side holds by [23, Lemma A.22]. This is another classical isogeny (for example, see [37]). The analogous one obtained by letting  $f_2(x)$  have arbitrary degree is studied in [47].

It will often be important to have an understanding of the kernel of the isogeny  $\phi$ . Since  $\psi \circ \phi = [2]$ , we observe that  $\ker \phi \leq \text{Jac}_{X_1}[2] \times \text{Jac}_{X_2}[2] \times \text{Jac}_{X_0}[2]$ .

Recall that, given a hyperelliptic curve  $C : y^2 = f(x)$  over a field  $K$  and  $\mathcal{R} \subset \overline{K}$  the roots of  $f(x)$ , there is a correspondence between points in  $\text{Jac}_C[2]$  and even sized subsets of  $\mathcal{R}$  (c.f. Notation 2.1.11 and Lemma 2.1.12). This correspondence is one-to-one when  $\deg f$  is odd and two-to-one when  $\deg f$  is even.

**Lemma 3.3.7.** *Let  $K$  be a field of characteristic 0,  $f_1(x), f_2(x) \in K[x]$  be such that  $f_1(x)f_2(x)$  is separable and write  $\mathcal{R}_1, \mathcal{R}_2 \subset \overline{K}$  for the roots of  $f_1(x), f_2(x)$ , respectively. Then,*

$$\ker \phi = \left\{ (D_S, D_T, D_{S \cup T}) : S \subseteq \mathcal{R}_1, T \subseteq \mathcal{R}_2 \text{ have even size} \right\}$$

where  $\phi$  is the isogeny constructed in Theorem 3.3.2 and  $D_S, D_T, D_{S \cup T}$  are as in Notation 2.1.11.

*Proof.* The given kernel can be seen to satisfy the size constraint imposed by Corollary 3.3.3. In particular, the points  $(D_S, D_T, D_{S \cup T})$  are distinct as  $S,$

$T$  vary unless  $\deg f_1, \deg f_2$  are both even, in which case  $(D_S, D_T, D_{S \cup T}) = (D_{\mathcal{R}_1 - S}, D_{\mathcal{R}_2 - T}, D_{(\mathcal{R}_1 - S) \cup (\mathcal{R}_2 - T)})$ .

It remains to check that  $\phi((D_S, D_T, D_{S \cup T})) = 0$ . Let  $\infty_0$  denote the point at infinity on  $\mathbb{P}^1$  and  $\pi_x : X \rightarrow \mathbb{P}^1, (x, y, z) \mapsto x$ , then

$$\begin{aligned} (\pi_1)^*(D_S) &= \sum_{r \in S} \left( (r, 0, \sqrt{f_2(r)}) + (r, 0, -\sqrt{f_2(r)}) \right) - \frac{\#S}{2} \pi_x^*(\infty_0), \\ (\pi_2)^*(D_T) &= \sum_{r \in T} \left( (r, \sqrt{f_1(r)}, 0) + (r, -\sqrt{f_1(r)}, 0) \right) - \frac{\#T}{2} \pi_x^*(\infty_0). \end{aligned}$$

Since

$$(\pi_0)^*(D_{S \cup T}) = (\pi_1)^*(D_S) + (\pi_2)^*(D_T),$$

and the class of each of these divisors is 2-torsion (for example,  $2 \cdot (\pi_1)^*(D_S)$  is the principal divisor coming from  $\prod_{\alpha \in S} (x - \alpha) \in \overline{K}(X)^\times$ ), we have shown that  $(D_S, D_T, D_{S \cup T}) \in \ker \phi$ .  $\square$

**Example 3.3.8.** Let  $f_1(x) = (x^2 - 2)(x + 5)$  and  $f_2(x) = (x - 1)^2 - 3$ .

By Lemma 3.3.7, the kernel of  $\phi$  is precisely

$$\left\{ (D_S, 0, D_S), (D_S, 0, D_{S \cup \mathcal{R}_2}) : S = \emptyset, \{-\sqrt{2}, \sqrt{2}\}, \{\sqrt{2}, -5\}, \{-\sqrt{2}, -5\} \right\},$$

having used that  $D_\emptyset = D_{\mathcal{R}_2} = 0 \in \text{Jac}_{X_2}$ .

### 3.4 Explicit construction of isogenies for $S_3$

We now describe and study another isogeny which we exhibit via Theorem 3.1.3. This will be used in a later chapter when we discuss the parity conjecture for elliptic curves.

**Notation 3.4.1.** Let  $K$  be a field of characteristic 0 and  $f(x) = x^3 + ax + b \in K[x]$  be a separable cubic. Let  $g(y^2) = -27y^4 + 54by^2 - (4a^3 + 27b^2) \in K[y]$  be the discriminant of  $f(x) - y^2$  (viewed as a polynomial in  $x$ ). Define a curve over  $K$  by

$$X : \{y^2 = f(x), \Delta^2 = g(y^2)\}.$$

**Lemma 3.4.2.** *When  $a \neq 0$ ,  $X$  is a genus 3 bihyperelliptic curve. It is isogenous to  $E \times \text{Jac}_C$  where  $C : W^2 = -(3x^2 + 4a)f(x)$  has genus 2.*

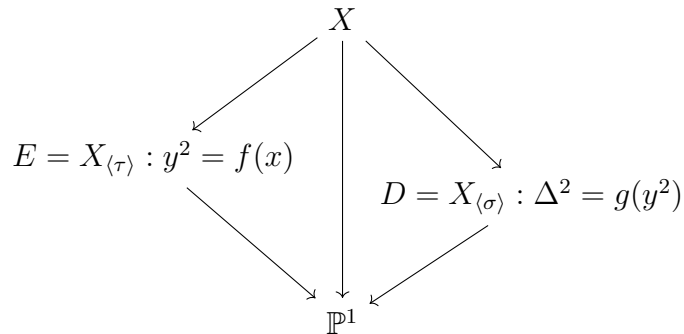
*Proof.* By definition,

$$X : \{y^2 = f(x), \Delta^2 = g(f(x)) = -(3x^2 + a)^2(3x^2 + 4a)\}.$$

Letting  $z = \Delta/(3x^2 + a)$  gives  $X : \{y^2 = f(x), z^2 = -(3x^2 + 4a)\}$ . This is a bihyperelliptic curve which, by Theorem 3.3.2 with  $f_1(x) = f(x)$ ,  $f_2(x) = -(3x^2 + 4a)$ , is isogenous to  $E \times \text{Jac}_C$  and so has genus 3.  $\square$

Write  $x' = -\frac{x}{2} + \frac{6ax^2 + 9(y^2 - b)x + 4a^2}{2\Delta}$ . The group  $G = S_3 := \langle \sigma, \tau \rangle$  acts on  $X$  where  $\sigma : (x, y, \Delta) \mapsto (x', y, \Delta)$  and  $\tau : (x, y, \Delta) \mapsto (x, y, -\Delta)$ . We note that  $\sigma$  has order 3 and that  $\sigma^2 : (x, y, \Delta) \mapsto (-x - x', y, \Delta)$ .

The quotients of  $X$  by the subgroups of  $S_3$ , up to conjugacy, are displayed in Figure 3.2, where  $\mathbb{P}^1$  has coordinate  $y$ .



**Figure 3.2:**  $S_3$  diagram of covers of curves

We note that  $D$  has genus 1 when  $a \neq 0$ .

The unique Brauer relation for  $G$ , up to multiplication by integers, is given by

$$2\langle \tau \rangle + \langle \sigma \rangle - 2G - \{1\}$$

(see Example 2.5.4). When  $K$  is a number field, applying Theorem 3.2.2(ii) with respect to this gives the existence of an isogeny  $E \times E \times \text{Jac}_D \rightarrow \text{Jac}_X$ , since  $\text{Jac}_{X_G} = 0$ .

We observe that the quotient maps for  $E$  and  $D$  are

$$\begin{aligned}\pi_E : X &\rightarrow E & \pi_D : X &\rightarrow D \\ (x, y, \Delta) &\mapsto (x, y), & (x, y, \Delta) &\mapsto (y, \Delta).\end{aligned}$$

As in Theorem 3.3.2, they allow us to explicitly construct our isogeny.

**Theorem 3.4.3.** *Let  $K$  be a field of characteristic 0,  $f(x) = x^3 + ax + b \in K[x]$  a separable cubic and  $g(y^2) = -27y^4 + 54by^2 - (4a^3 + 27b^2) \in K[y]$ . Define  $E : y^2 = f(x)$ ,  $D : \Delta^2 = g(y^2)$  and  $X : \{y^2 = f(x), \Delta^2 = g(y^2)\}$ . Then*

$$\begin{aligned}\psi &:= ((\pi_E)_*, (\pi_E)_* \circ \sigma_*, (\pi_D)_*) : \text{Jac}_X \rightarrow E \times E \times \text{Jac}_D, \\ \phi &:= (\pi_E)^* + \sigma^* \circ (\pi_E)^* + (\pi_D)^* : E \times E \times \text{Jac}_D \rightarrow \text{Jac}_X,\end{aligned}$$

are mutually-dual isogenies of degree 9, where  $\pi_E : (x, y, \Delta) \mapsto (x, y) \in E$ ,  $\pi_D : (x, y, \Delta) \mapsto (y, \Delta) \in X_2$ ,  $\sigma : (x, y, \Delta) \mapsto (-\frac{x}{2} + \frac{6ax^2 + 9(y^2 - b)x + 4a^2}{2\Delta}, y, \Delta) \in X$  whenever  $(x, y, z) \in X$  and  $\phi(P, Q, R) = (\pi_E)^*P + \sigma^* \circ (\pi_E)^*Q + (\pi_D)^*R$ .

*Proof.* That  $\psi$  and  $\phi$  are isogenies follows upon showing that  $\psi \circ \phi \in \text{End}(E \times E \times \text{Jac}_D)$ , which is argued below. Their mutual duality is noted in Example 3.5.6, by applying Theorem 3.5.2 (this is essentially due to the mutually-duality of  $\pi_*$  and  $\pi^*$ , see Lemma 2.1.9).

First observe that  $(\pi_E)_* \circ (\pi_E)^* = (\pi_E)_* \circ \sigma_* \circ \sigma^* \circ (\pi_E)^* = [2]_E$  and  $(\pi_D)_* \circ (\pi_D)^* = [3]_{\text{Jac}_D}$ . Additionally,

$$(\pi_E)_* \circ \sigma^* \circ (\pi_E)^* = (\pi_E)_* \circ \sigma_* \circ (\pi_E)^* = [-1]_E$$

since  $(x, y) + (x', y) + (-x - x', y) = 0$  for any  $(x, y) \in E$ . Using this, alongside the fact that  $(y, \Delta) + (y, -\Delta) = 0$  for any  $(y, \Delta) \in D$ , we see that all other compositions are 0 and so

$$(\psi \circ \phi)(P, Q, R) = (2P - Q, 2Q - P, 3R) \implies \psi \circ \phi \in \text{End}(E \times E \times \text{Jac}_D).$$



From this we deduce that  $\ker \psi \circ \phi = \{(P, -P, R) : P \in E[3], R \in \text{Jac}_D[3]\}$ . In particular,  $\deg \psi \circ \phi = 81$  and (using that  $\psi, \phi$  are duals)  $\deg \phi = \deg \psi = 9$ .  $\square$

### 3.5 The general construction

Theorem 3.2.2 asserts the existence of an isogeny between the Jacobians of quotients of a curve  $X$  defined over a number field, given a Brauer relation for a finite group of its automorphisms. We exhibited such isogenies in the previous two sections.

For completeness, we now provide an explicit description of the isogeny in general (as given in [23, §3]) where  $K$  can be any field of characteristic 0. The content of this section is not required for the rest of this thesis.

**Construction 3.5.1.** Let  $K$  be a field of characteristic 0 and  $X$  a curve over  $K$ . Let  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ .

(1). Let  $\Phi : \bigoplus_j \mathbb{Z}[G/H'_j] \rightarrow \bigoplus_i \mathbb{Z}[G/H_i]$  be a  $G$ -module homomorphism and write

$$\Phi_{j,i} : \mathbb{Z}[G/H'_j] \rightarrow \mathbb{Z}[G/H_i]$$

for the corresponding  $G$ -module homomorphisms of the summands for each  $i, j$ .

(2). For each  $i, j$ , fix some  $\sum_{g \in G} a_g g \in \mathbb{Z}[G]$  to be such that  $\sum_{g \in G} a_g g H_i = \Phi_{j,i}(H'_j) \in \mathbb{Z}[G/H_i]$  and define the endomorphism

$$\tilde{\Phi}_{j,i} := \sum_{g \in G} a_g g_* : \text{Jac}_X \rightarrow \text{Jac}_X$$

(where  $g_* : P \mapsto g \cdot P$  for  $P \in X(\overline{K})$ ). We note that  $\tilde{\Phi}_{j,i}$  restricted to  $\text{Jac}_X^{H_i}$  is independent of the choice of  $\sum_{g \in G} a_g g$ .

(3). For each  $i, j$ , define the homomorphism

$$f_{\Phi_{j,i}} := \frac{1}{\#H'_j} ((\pi_{H'_j})_* \circ \tilde{\Phi}_{j,i} \circ (\pi_{H_i})^*) : \text{Jac}_{X_{H_i}} \rightarrow \text{Jac}_{X_{H'_j}}$$

where (for  $H \leq g$ )  $(\pi_H)_*$ ,  $(\pi_H)^*$  are the induced homomorphisms for the quotient maps  $\pi_H : X \rightarrow X_H$  (see §2.1.2). Since  $(\pi_{H_i})^*$  in fact maps  $\text{Jac}_{X_{H_i}}$  into  $\text{Jac}_X^{H_i}$ ,  $f_{\Phi_{j,i}}$

is independent of the choice of  $\tilde{\Phi}_{j,i}$  made in (2).

(4). Define

$$f_{\Phi} := \left( \sum_i f_{\Phi_{j,i}} \right)_j : \prod_i \text{Jac}_{X_{H_i}} \rightarrow \prod_j \text{Jac}_{X_{H'_j}}.$$

**Theorem 3.5.2.** *Let  $K$  be a field of characteristic 0 and  $X$  a curve over  $K$ . Let  $G$  be a finite group of  $K$ -automorphisms of  $X$  with Brauer relation  $\sum_i H_i - \sum_j H'_j$  and  $\Phi : \bigoplus_j \mathbb{Z}[G/H'_j] \rightarrow \bigoplus_i \mathbb{Z}[G/H_i]$  an injective  $G$ -module homomorphism. Then*

$$f_{\Phi} : \prod_i \text{Jac}_{X_{H_i}} \rightarrow \prod_j \text{Jac}_{X_{H'_j}}$$

as in Construction 3.5.1 is a  $K$ -isogeny and  $(f_{\Phi})^{\vee} = f_{\Phi^{\vee}}$ .

*Proof.* Omitted. See [23, Theorem 3.2]. □

**Remark 3.5.3.** In light of this construction, we could have asserted the existence of the isogeny in Theorem 3.2.2(ii) independently of Faltings theorem ([26, §5, Corollary 2]).

**Example 3.5.4.** Let  $G = C_2 \times C_2 := \langle \tau_1, \tau_2 \rangle$  act on  $X : \{y^2 = f_1(x), z^2 = f_2(x)\}$  as in §3.3. Applying Theorem 3.5.2, we can recover the isogeny  $\phi$  described in Theorem 3.3.2.

There is an injective  $C_2 \times C_2$ -module homomorphism given by

$$\Phi : \mathbb{Z}[G/G] \oplus \mathbb{Z}[G/G] \oplus \mathbb{Z}[G/\{1\}] \rightarrow \mathbb{Z}[G/\langle \tau_1 \rangle] \oplus \mathbb{Z}[G/\langle \tau_2 \rangle] \oplus \mathbb{Z}[G/\langle \tau_1 \tau_2 \rangle]$$

$$x_1 \mapsto (1 + \tau_2)y_1,$$

$$x_2 \mapsto (1 + \tau_1)y_2,$$

$$x_3 \mapsto y_1 + y_2 + y_3,$$

where  $x_j$  denotes the trivial coset in  $\mathbb{Z}[G/H'_j]$  ( $H'_1 = H'_2 = G$ ,  $H'_3 = \{1\}$ ) and  $y_i$  denotes the trivial coset in  $\mathbb{Z}[G/H_i]$  ( $H_1 = \langle \tau_1 \rangle$ ,  $H_2 = \langle \tau_2 \rangle$ ,  $H_3 = \langle \tau_1 \tau_2 \rangle$ ).

Since  $\text{Jac}_{X_{H'_j}} = 0$  for  $j = 1, 2$ , the isogeny is

$$f_\Phi = f_{\Phi_{3,1}} + f_{\Phi_{3,2}} + f_{\Phi_{3,3}} : \text{Jac}_{X_{H_1}} \times \text{Jac}_{X_{H_2}} \times \text{Jac}_{X_{H_3}} \rightarrow \text{Jac}_X.$$

We observe that  $\Phi_{3,i}(H'_3) = H_i$  for  $i = 1, 2, 3$  and so take  $\tilde{\Phi}_{3,i} = 1$  be the identity endomorphism on  $\text{Jac}_X$ . Since  $(\pi_{H'_3})_*$  is also the identity endomorphism on  $\text{Jac}_X$ , it follows that

$$f_{\Phi_{3,i}} = (\pi_{H_i})^* \quad \text{for } i = 1, 2, 3.$$

Therefore  $f_\Phi = \phi$ .

By Theorem 3.5.2, Construction 3.5.1 also gives the dual of this isogeny, i.e.

$$(f_\Phi)^\vee = f_{\Phi^\vee} = (f_{\Phi_{1,3}^\vee}, f_{\Phi_{2,3}^\vee}, f_{\Phi_{3,3}^\vee}) : \text{Jac}_X \rightarrow \text{Jac}_{X_{H_1}} \times \text{Jac}_{X_{H_2}} \times \text{Jac}_{X_{H_0}}.$$

First observe that  $\Phi_{1,3}^\vee(H_1) = (1 + \tau_1)H'_3$ , therefore we can take  $f_{\Phi_{1,3}^\vee} = \frac{1}{2}((\pi_{H_1})_* \circ (1_* + \tau_{1*})) = (\pi_{H_1})_*$ . Similarly,  $f_{\Phi_{2,3}^\vee} = \frac{1}{2}((\pi_{H_2})_* \circ (1_* + \tau_{2*})) = (\pi_{H_2})_*$  and  $f_{\Phi_{3,3}^\vee} = \frac{1}{2}((\pi_{H_3})_* \circ (1_* + \tau_1\tau_{2*})) = (\pi_{H_3})_*$ .

Therefore,  $(f_\Phi)^\vee = \phi^\vee = \psi$  (as in Theorem 3.3.2).

**Example 3.5.5.** Continuing with the notation in Example 3.5.4, define an injective  $C_2 \times C_2$ -module homomorphism  $\Phi'$  by  $\Phi'(x_i) = \Phi(x_i)$  for  $i = 1, 2$  and  $\Phi'(x_3) = 3\Phi(x_3)$ .

Applying Construction 3.5.1 with respect to  $\Phi'$  gives another isogeny

$$f_{\Phi'} = [3] \circ f_\Phi : \text{Jac}_{X_{H_1}} \times \text{Jac}_{X_{H_2}} \times \text{Jac}_{X_{H_3}} \rightarrow \text{Jac}_X.$$

**Example 3.5.6.** Let  $G = S_3 := \langle \sigma, \tau \rangle$  act on  $X : \{y^2 = f(x), \Delta^2 = g(y^2)\}$  as in §3.4. Again we apply Theorem 3.5.2 to recover the isogeny  $\phi$  described in Theorem 3.4.3.

There is an injective  $S_3$ -module homomorphism given by

$$\begin{aligned} \Phi : \mathbb{Z}[G/G] \oplus \mathbb{Z}[G/G] \oplus \mathbb{Z}[G/\{1\}] &\rightarrow \mathbb{Z}[G/\langle\tau\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle] \oplus \mathbb{Z}[G/\langle\sigma\rangle] \\ x_1 &\mapsto (1 + \sigma + \sigma^2)y_1 + (1 + \sigma + \sigma^2)y_2 + (1 + \tau)y_3, \\ x_2 &\mapsto (1 + \sigma + \sigma^2)y_2 + (1 + \tau)y_3, \\ x_3 &\mapsto y_1 + \sigma^2y_2 + y_3, \end{aligned}$$

where  $x_j$  denotes the trivial coset in  $\mathbb{Z}[G/H'_j]$  ( $H'_1 = H'_2 = G$ ,  $H'_3 = \{1\}$ ) and  $y_i$  denotes the trivial coset in  $\mathbb{Z}[G/H_i]$  ( $H_1 = H_2 = \langle\tau\rangle$ ,  $H_3 = \langle\sigma\rangle$ ).

Since  $\text{Jac}_{X_{H'_j}} = 0$  for  $j = 1, 2$ , the isogeny is

$$f_\Phi = f_{\Phi_{3,1}} + f_{\Phi_{3,2}} + f_{\Phi_{3,3}} : \text{Jac}_{X_{H_1}} \times \text{Jac}_{X_{H_2}} \times \text{Jac}_{X_{H_3}} \rightarrow \text{Jac}_X.$$

Upon observing that  $\Phi_{3,1}(H'_3) = H_1$ ,  $\Phi_{3,2}(H'_3) = \sigma^2H_2$  and  $\Phi_{3,3}(H'_3) = H_3$ , we may fix  $\tilde{\Phi}_{3,1} = \tilde{\Phi}_{3,3} = 1$  to be the identity endomorphism on  $\text{Jac}_X$  and  $\tilde{\Phi}_{3,2} = (\sigma^2)_* = \sigma^*$ . Plugging these into the expression for  $f_\Phi$ , we see that this is precisely the isogeny  $\phi$ . Namely,

$$\text{Jac}_{X_{\langle\tau\rangle}} \times \text{Jac}_{X_{\langle\tau\rangle}} \times \text{Jac}_{X_{\langle\sigma\rangle}} \ni (P, Q, R) \mapsto \pi_{\langle\tau\rangle}^*P + \sigma^* \circ \pi_{\langle\tau\rangle}^*Q + \pi_{\langle\sigma\rangle}^*R \in \text{Jac}_X.$$

As in Example 3.5.4,  $f_\Phi^\vee = (f_{\Phi_{1,3}^\vee}, f_{\Phi_{2,3}^\vee}, f_{\Phi_{3,3}^\vee})$ . We note that  $\Phi_{1,3}^\vee(H_1) = (1 + \tau)H'_3$ ,  $\Phi_{2,3}^\vee(H_2) = (1 + \tau)\sigma H'_3$  and  $\Phi_{3,3}^\vee(H_3) = (1 + \sigma + \sigma^2)H'_3$ . Therefore, we can take  $f_{\Phi_{1,3}^\vee} = \frac{1}{2}((\pi_{H_1})_* \circ (1_* + \tau_*)) = (\pi_{H_1})_*$ ,  $f_{\Phi_{2,3}^\vee} = \frac{1}{2}((\pi_{H_2})_* \circ (\sigma_* + \tau\sigma_*)) = (\pi_{H_2})_* \circ \sigma_*$ ,  $f_{\Phi_{3,3}^\vee} = \frac{1}{3}((\pi_{H_3})_* \circ (1_*\sigma_* + \sigma^2_*)) = (\pi_{H_3})_*$  to see that  $(f_\Phi)^\vee = \phi^\vee = \psi$  (as in Theorem 3.4.3).

## Chapter 4

# Determining Parities of Ranks of Jacobians of Curves

Combining the conjectural framework of  $L$ -functions with the Birch and Swinnerton-Dyer conjecture yields the parity conjecture. This conjecture asserts that the parity of the rank of an abelian variety is determined by its local root numbers. Since the local arithmetic of abelian varieties (specifically, Jacobians of curves) is better understood than the global arithmetic, having such a local-global tool which can be used unconditionally is desirable.

In this chapter, we exploit the isogenies constructed from automorphisms in the previous chapter by applying the isogeny invariance of the Birch and Swinnerton-Dyer conjecture to them. By doing this, we are able to construct an arithmetic analogue of the local root number. We will see that, assuming the Shafarevich–Tate conjecture (this is a weaker assumption than what is currently needed for the parity conjecture to hold), this controls the parity of the rank in certain situations.

The final section discusses the analogous results (from [23], included without proof) that we obtain when replacing ranks with  $p^\infty$ -Selmer ranks.

We will not attempt to compare local root numbers with their arithmetic analogues here; this will be the focus of the remaining chapters.

## 4.1 Parities of ranks of isogenous elliptic curves

As noted in §1.2, Birch once commented that the parity of the rank of an elliptic curve admitting an isogeny is controlled by local data, specifically Tamagawa numbers and periods [3]. This is a consequence of the conjectured lead term of the  $L$ -function being invariant under isogeny.

**Theorem 4.1.1** (Cassels–Tate [6, 66]). *Let  $A, A'$  be isogenous abelian varieties defined over a number field  $K$ . Assuming that  $\text{III}(A), \text{III}(A')$  are finite,*

$$\text{BSD}(A/K) = \text{BSD}(A'/K).$$

In particular, let  $E, E'$  be isogenous elliptic curves defined over a number field  $K$ . Under the finiteness assumption on their Shafarevich–Tate groups, and noting Theorem 2.3.7, we see that

$$\frac{\text{Reg}(E)}{\text{Reg}(E')} = \frac{C(E')}{C(E)} \cdot \frac{\#\text{III}(E')}{\#\text{III}(E)} \cdot \frac{\#E(K)_{\text{tors}}^2}{\#E'(K)_{\text{tors}}^2} = \frac{C(E')}{C(E)} \cdot \square \quad (4.1)$$

where  $\square \in \mathbb{Q}^\times$  is a square.

**Example 4.1.2.** Let  $E/\mathbb{Q} : y^2 + xy = x^3 - x$  (65.a1),  $E'/\mathbb{Q} : y^2 + xy = x^3 + 4x + 1$  (65.a2).

We evaluate the right-hand-side of (4.1). Taking  $\omega$  and  $\omega'$  to be the global minimal differentials on  $E$  and  $E'$  respectively,  $C_p(E, \omega) = c_p(E)$  and  $C_p(E', \omega') = c_p(E')$  for all primes  $p \in \mathbb{Z}$ . We then note that

$$c_5(E') = c_{13}(E') = 2, \quad C_\infty(E, \omega) = 5.382\dots, \quad C_\infty(E', \omega') = 2.691\dots,$$

and  $c_p(E), c_p(E') = 1$  otherwise. Therefore,

$$\frac{\text{Reg}(E)}{\text{Reg}(E')} = c_5(E') \cdot c_{13}(E') \cdot \frac{C_\infty(E', \omega')}{C_\infty(E, \omega)} \cdot \square = 2 \cdot \square \neq 1$$

and so  $\text{rk}(E) = \text{rk}(E') > 0$  (otherwise  $\text{Reg}(E) = \text{Reg}(E') = 1$ ). In particular, we have observed the existence of infinitely many rational points on  $E$  and  $E'$  by looking

only at their local behaviour.

A stronger conclusion can in fact be made about the ranks of isogenous elliptic curves via the following lemma.

**Lemma 4.1.3** ([16], Lemma 1.3). *Let  $E, E'$  be elliptic curves defined over a number field  $K$  and  $\phi : E \rightarrow E'$  a  $K$ -rational isogeny of degree  $d$ . Then*

$$\frac{\text{Reg}(E/K)}{\text{Reg}(E'/K)} \equiv d^{\text{rk}(E/K)} \pmod{\mathbb{Q}^{\times 2}}.$$

Combining this with (4.1) gives the following formula for the parity of the ranks of elliptic curves admitting  $d$ -isogenies:

$$\text{rk}(E) = \text{rk}(E') \equiv \sum_{v \text{ place of } K} \text{ord}_d\left(\frac{C_v(E', \omega')}{C_v(E, \omega)}\right) \pmod{2}. \quad (4.2)$$

Upon fixing choices of global differentials  $\omega$  and  $\omega'$ , the right-hand-side of this expression only concerns  $E$  and  $E'$  over local fields and so we call this a *local formula*. Such formulae are desirable since we understand the local arithmetic of curves much better than the global arithmetic.

**Example 4.1.4.** Applying (4.2) with  $d = 2$  to the 2-isogenous elliptic curves  $E/\mathbb{Q} : y^2 + xy = x^3 - x$ ,  $E'/\mathbb{Q} : y^2 + xy = x^3 + 4x + 1$  (as in Example 4.1.2), we determine that their ranks are odd (and not just non-zero).

## 4.2 Rank parity formulae

Our goal here is to develop the argument presented in the previous section so that it is applicable to isogenies arising from Brauer relations, which involve the Jacobians of higher genus curves. In previous works, regulator constants (see §2.6) have been used to manipulate expressions concerning regulators of elliptic curves over field extensions into ones encoding the parity of a suitable rank (see [18, §1.iv.]). The new technique we employ here involves replacing extensions of number fields by covers of curves.

We begin with an analogue of Lemma 4.1.3.

**Lemma 4.2.1.** *Let  $X$  be a curve defined over a number field  $K$ ,  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\Theta = \sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . Then*

$$\frac{\prod_j \text{Reg}(\text{Jac}_{X_{H'_j}})}{\prod_i \text{Reg}(\text{Jac}_{X_{H_i}})} \equiv \mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \pmod{\mathbb{Q}^{\times 2}}.$$

*Proof.* Let  $H \leq G$ , write  $\{P_1, \dots, P_N\}$  for a basis of  $\text{Jac}_{X_H}(K)/\text{Jac}_{X_H}(K)_{\text{tors}}$  and  $\langle, \rangle, \langle, \rangle_H$  for the Néron–Tate height pairings on  $\text{Jac}_X(K), \text{Jac}_{X_H}(K)$  respectively. Then

$$\begin{aligned} \text{Reg}(\text{Jac}_{X_H}) &:= \left| \det \left( \langle P_i, P_j \rangle_H \right) \right| \\ &\stackrel{\text{Lemma 2.3.2}}{=} \left| \det \left( \frac{1}{\#H} \langle (\pi_H)^* P_i, (\pi_H)^* P_j \rangle \right) \right| \\ &\stackrel{\text{Lemma 2.1.14}}{=} \left| \det \left( \frac{1}{\#H} \langle, \rangle \mid (\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q})^H \right) \right| \pmod{\mathbb{Q}^{\times 2}}. \end{aligned}$$

The result now follows readily by taking the specified quotient of regulators.  $\square$

This lemma is of interest to us because, as we'll see later (Lemmata 4.3.1, 4.4.1 & 8.2.7), this regulator constant encodes information about parities of ranks of Jacobians. With this in mind, the following closely resembles the local formula given in (4.2).

**Theorem 4.2.2.** *Let  $X$  be a curve defined over a number field  $K$ ,  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\Theta = \sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ .*

*Assuming that  $\text{III}(\text{Jac}_X)$  is finite,*

$$\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \equiv \prod_{v \text{ place of } K} \left( \frac{C_v(\prod_i \text{Jac}_{X_{H_i}}, \omega') \cdot \prod_i \mu_v(X_{H_i})}{C_v(\prod_j \text{Jac}_{X_{H'_j}}, \omega) \cdot \prod_j \mu_v(X_{H'_j})} \right) \pmod{\mathbb{Q}^{\times 2}}$$

*where  $\omega', \omega$  denote fixed choices of non-zero global exterior forms for  $\prod_i \text{Jac}_{X_{H_i}}, \prod_j \text{Jac}_{X_{H'_j}}$  respectively.*

*Proof.* Applying Theorem 4.1.1 to the  $K$ -isogeny  $\prod_i \text{Jac}_{X_{H_i}} \rightarrow \prod_j \text{Jac}_{X_{H'_j}}$  guaranteed by Theorem 3.2.2(ii) gives the following equality of Birch and Swinnerton-Dyer



invariants

$$\frac{\text{Reg}(\prod_j \text{Jac}_{X_{H'_j}})}{\text{Reg}(\prod_i \text{Jac}_{X_{H_i}})} = \frac{C(\prod_i \text{Jac}_{X_{H_i}})}{C(\prod_j \text{Jac}_{X_{H'_j}})} \cdot \frac{\#\text{III}(\prod_i \text{Jac}_{X_{H_i}})}{\#\text{III}(\prod_j \text{Jac}_{X_{H'_j}})} \cdot \frac{\#\prod_j \text{Jac}_{X_{H'_j}}(K)_{\text{tors}}^2}{\#\prod_i \text{Jac}_{X_{H_i}}(K)_{\text{tors}}^2}.$$

Since the regulator and Shafarevich–Tate groups are known to be multiplicative [66], combining this expression with Lemma 4.2.1 and Theorem 2.3.11 yields the required identity.  $\square$

Upon having fixed the global exterior forms  $\omega, \omega'$ , this becomes a local formula for  $\mathcal{C}_{\Theta}(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \bmod \mathbb{Q}^{\times 2}$ . The dependence of the local terms on this initial choice could in fact be removed (see [23, Definition 6.16]), but this is not necessary for this thesis.

**Remark 4.2.3.** The local terms appearing in Theorem 4.2.2 involve abelian varieties whose dimensions are (potentially) large. In view of computing these, it is useful to note that if  $\omega_i$  is a non-zero global exterior form for  $\text{Jac}_{X_{H_i}}$  then

$$C_v(\prod_i \text{Jac}_{X_{H_i}}, \bigwedge_i \omega_i) = \prod_i C_v(\text{Jac}_{X_{H_i}}, \omega_i),$$

see [23, Remark 6.3].

An isogeny  $\phi : A \rightarrow B$  of abelian varieties over a field  $K$  naturally induces a  $K$ -linear map  $\phi^* : \bigwedge^{\dim B} \Omega^1(B) \rightarrow \bigwedge^{\dim A} \Omega^1(A)$  (see [59, §6.1]).

**Example 4.2.4.** Let  $\psi : \text{Jac}_X \rightarrow \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$  be the isogeny defined in Theorem 3.3.2, arising from a Brauer relation for  $C_2 \times C_2$ .

We demonstrate how to compute  $\psi^*\omega$  when  $\omega = P_1^*(\omega_1) \wedge P_2^*(\omega_2) \wedge P_0^*(\omega_0)$  and  $\omega_i$  is a global exterior form for  $\text{Jac}_{X_i}$  with  $P_i : \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_{X_i}$  the projection map. This will be used later on, within the proof of Lemma 5.2.6.

Since, by definition,  $\psi^*$  distributes over wedge products

$$\begin{aligned}\psi^*\omega &= \psi^*P_1^*(\omega_1) \wedge \psi^*P_2^*(\omega_2) \wedge \psi^*P_0^*(\omega_0) \\ &= (P_1 \circ \psi)^*\omega_1 \wedge (P_2 \circ \psi)^*\omega_2 \wedge (P_0 \circ \psi)^*\omega_0 \\ &= ((\pi_1)_*)^*\omega_1 \wedge ((\pi_2)_*)^*\omega_2 \wedge ((\pi_0)_*)^*\omega_0.\end{aligned}$$

In practice, it is often useful to note the following lemmata when computing the local terms in Theorem 4.2.2.

**Lemma 4.2.5.** *Let  $\phi : A \rightarrow B$  be an isogeny of abelian varieties defined over a number field  $K$ . Let  $v$  be a place of  $K$  and let  $\omega$  be a basis element of  $\bigwedge^{\dim B} \Omega^1(B/K_v)$ .*

*Then,*

$$\frac{C_v(A, \phi^*\omega)}{C_v(B, \omega)} = \frac{\#\ker \phi(K_v)}{\#\operatorname{coker} \phi(K_v)}.$$

*Proof.* This is standard, see for example [42, Theorem 7.3].  $\square$

**Lemma 4.2.6.** *Let  $A$  be an abelian variety defined over a number field  $K$  and  $S$  a finite set of non-Archimedean places of  $K$ . There exists a non-zero global exterior form  $\omega$  on  $A$  such that  $|\omega/\omega_{A/K_v}^0|_v = 1$  for each  $v \in S$ .*

*Proof.* Let  $\omega' \in \bigwedge^{\dim A} \Omega^1(A/K)$  be a basis element. For each place  $v \in S$ , write  $m_v = \omega'/\omega_{A/K_v}^0 \in K_v$ . By the Chinese Remainder Theorem, there exists  $m \in K^\times$  such that  $m \cdot m_v \in \mathcal{O}_{K_v}^\times$  for all  $v \in S$ . Therefore  $\omega = m \cdot \omega'$  satisfies the lemma.  $\square$

In all of the examples considered in this thesis, the following version of Theorem 4.2.2 will be applicable and more convenient.

**Corollary 4.2.7.** *Let  $X$  be a curve defined over a number field  $K$ ,  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\Theta = \sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . Suppose that there is a unique  $H'_j$  with  $\operatorname{Jac}_{X_{H'_j}} \neq 0$ , so that Theorem 3.2.2(ii) gives rise to an isogeny  $\phi : \prod_i \operatorname{Jac}_{X_{H_i}} \rightarrow \operatorname{Jac}_{X'}$ .*

Assuming that  $\text{III}(\text{Jac}_X)$  is finite, then for  $p \in \mathbb{Z}$  a prime,

$$\begin{aligned} \text{ord}_p \mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) &\equiv \sum_{v|\infty} \text{ord}_p \left( \frac{\#\ker \phi(K_v)}{\#\text{coker } \phi(K_v)} \cdot \frac{\prod_i \mu_v(X_{H_i})}{\mu_v(X')} \right) \\ &+ \sum_{v \nmid \infty} \text{ord}_p \left( \frac{\prod_i c_v(\text{Jac}_{X_{H_i}}) \mu_v(X_{H_i})}{c_v(\text{Jac}_{X'}) \mu_v(X')} \cdot \left| \frac{\phi^* \omega_{\text{Jac}_{X'}/K_v}^0}{\omega_{\prod_i \text{Jac}_{X_{H_i}}/K_v}^0} \right|_v \right) \pmod{2}. \end{aligned}$$

*Proof.* Let  $\omega$  be a non-zero global exterior form for  $\text{Jac}_{X'}$  which is minimal at all places  $v$  of  $K$  such that  $v \mid p$  (such a choice is possible by Lemma 4.2.6) and let  $\omega' = \phi^* \omega$ . The stated formula is then deduced from Theorem 4.2.2 as follows.

By Lemma 4.2.5,

$$\begin{aligned} \text{ord}_p \left( \prod_{v|\infty} \frac{C_v(\prod_i \text{Jac}_{X_{H_i}}, \phi^* \omega) \cdot \prod_i \mu_v(X_{H_i})}{C_v(\text{Jac}_{X'}, \omega) \cdot \mu_v(X')} \right) \\ = \sum_{v|\infty} \text{ord}_p \left( \frac{\#\ker \phi(K_v)}{\#\text{coker } \phi(K_v)} \cdot \frac{\prod_i \mu_v(X_{H_i})}{\mu_v(X')} \right). \end{aligned}$$

By the multiplicativity of the Tamagawa number (see [66]),

$$\begin{aligned} \text{ord}_p \left( \prod_{v \nmid \infty} \frac{C_v(\prod_i \text{Jac}_{X_{H_i}}, \phi^* \omega) \cdot \prod_i \mu_v(X_{H_i})}{C_v(\text{Jac}_{X'}, \omega) \cdot \mu_v(X')} \right) \\ = \sum_{v \nmid \infty} \text{ord}_p \left( \frac{\prod_i c_v(\text{Jac}_{X_{H_i}}) \mu_v(X_{H_i})}{c_v(\text{Jac}_{X'}) \mu_v(X')} \cdot \left| \frac{\phi^* \omega}{\omega_{\prod_i \text{Jac}_{X_{H_i}}/K_v}^0} \right|_v \cdot \left| \frac{\omega_{\text{Jac}_{X'}/K_v}^0}{\omega} \right|_v \right). \end{aligned}$$

Finally, if  $v \nmid p\infty$  then  $\text{ord}_p(|\cdot|_v) = 0$ , and if  $v \mid p$  then by the assumptions on  $\omega$  we see that  $|\omega_{\text{Jac}_{X'}/K_v}^0 / \omega|_v = 1$  and

$$\begin{aligned} \left| \frac{\phi^* \omega}{\omega_{\prod_i \text{Jac}_{X_{H_i}}/K_v}^0} \right|_v &= \left| \frac{\phi^* \omega}{\phi^* \omega_{\text{Jac}_{X'}/K_v}^0} \cdot \frac{\phi^* \omega_{\text{Jac}_{X'}/K_v}^0}{\omega_{\prod_i \text{Jac}_{X_{H_i}}/K_v}^0} \right|_v \\ &= \left| \frac{\phi^* \omega_{\text{Jac}_{X'}/K_v}^0}{\omega_{\prod_i \text{Jac}_{X_{H_i}}/K_v}^0} \right|_v. \end{aligned} \quad \square$$

We now explain how we obtain a local formula for the parity of the rank from Corollary 4.2.7 in the settings discussed in §3.3 and §3.4.

### 4.3 Rank parity formulae for $C_2 \times C_2$

Recall the set up of §3.3. In particular,  $K$  is a field of characteristic 0 and

$$X : \{y^2 = f_1(x), z^2 = f_2(x)\}$$

admits an action of  $C_2 \times C_2 = \langle \tau_1, \tau_2 \rangle$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  is separable. We additionally define

$$X_1 : y^2 = f_1(x), \quad X_2 : z^2 = f_2(x), \quad X_0 : w^2 = f_1(x)f_2(x).$$

**Lemma 4.3.1.** *Let  $K$  be a number field and  $\Theta = \langle \tau_1 \rangle + \langle \tau_2 \rangle + \langle \tau_1 \tau_2 \rangle - 2C_2 \times C_2 - \{1\}$ .*

*Then,*

$$\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = 2^{\text{rk}(\text{Jac}_X)} = 2^{\text{rk}(\text{Jac}_{X_1}) + \text{rk}(\text{Jac}_{X_2}) + \text{rk}(\text{Jac}_{X_0})}.$$

*Proof.* Write  $\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q} = \chi_{+,+}^{\oplus n_1} \oplus \chi_{+,-}^{\oplus n_2} \oplus \chi_{-,+}^{\oplus n_3} \oplus \chi_{-,-}^{\oplus n_4}$  for the decomposition into irreducible characters of  $C_2 \times C_2$ , where the subscripts denote the images of  $\tau_1, \tau_2$  respectively. Taking dimensions gives that  $n_1 + n_2 + n_3 + n_4 = \text{rk}(\text{Jac}_X)$ . Using that the rank is invariant under isogeny, this is equal to  $\text{rk}(\text{Jac}_{X_1}) + \text{rk}(\text{Jac}_{X_2}) + \text{rk}(\text{Jac}_{X_0})$ . The result then follows by Lemma 2.6.4 and Example 2.6.3.  $\square$

**Definition 4.3.2.** Let  $\mathcal{K}$  be a local field of characteristic 0 and  $\phi : \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_X$  be the  $\mathcal{K}$ -isogeny constructed in Theorem 3.3.2. We define the local invariant  $\lambda_{\mathcal{K}}(f_1, f_2)$  to be

$$\left\{ \begin{array}{ll} 2^{\deg f_1 \deg f_2 + 1} & \mathcal{K} \simeq \mathbb{C}, \\ \# \ker \phi \Big|_{(\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0})(\mathcal{K})} \circ \frac{n_{\text{Jac}_{X_1}} n_{\text{Jac}_{X_2}} n_{\text{Jac}_{X_0}} \mu(X_1) \mu(X_2) \mu(X_0)}{n_{\text{Jac}_X} \mu(X)} & \mathcal{K} \simeq \mathbb{R}, \\ \frac{c(\text{Jac}_{X_1}) c(\text{Jac}_{X_2}) c(\text{Jac}_{X_0}) \mu(X_1) \mu(X_2) \mu(X_0)}{c(\text{Jac}_X) \mu(X)} & \mathcal{K}/\mathbb{Q}_p \text{ finite, } p \neq 2, \\ \frac{c(\text{Jac}_{X_1}) c(\text{Jac}_{X_2}) c(\text{Jac}_{X_0}) \mu(X_1) \mu(X_2) \mu(X_0)}{c(\text{Jac}_X) \mu(X)} \Big|_{\omega_{\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}/\mathcal{K}}^0} \Big|_{\omega_{\text{Jac}_X/\mathcal{K}}^0} & \mathcal{K}/\mathbb{Q}_2 \text{ finite.} \end{array} \right.$$

**Theorem 4.3.3.** *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  is separable.*

*Assuming that  $\text{III}(\text{Jac}_{X_1}), \text{III}(\text{Jac}_{X_2}), \text{III}(\text{Jac}_{X_0})$  are finite,*

$$\text{rk}(\text{Jac}_{X_1}) + \text{rk}(\text{Jac}_{X_2}) + \text{rk}(\text{Jac}_{X_0}) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f_1, f_2) \pmod{2}$$

where  $\lambda_v(f_1, f_2)$  is as in Definition 4.3.2.

*Proof.* Let  $G = C_2 \times C_2$ ,  $\Theta = \langle \tau_1 \rangle + \langle \tau_2 \rangle + \langle \tau_1 \tau_2 \rangle - 2G - \{1\}$  and  $p = 2$ . Combining Corollary 4.2.7 and Lemma 4.3.1 gives a modulo 2 formula for  $\text{rk}(\text{Jac}_{X_1}) + \text{rk}(\text{Jac}_{X_2}) + \text{rk}(\text{Jac}_{X_0})$ . That the terms on the right-hand-side of this formula are congruent to  $\text{ord}_2 \lambda_v(f_1, f_2)$  is argued case-by-case.

When  $K_v \cong \mathbb{C}$ , this holds since  $\# \text{coker } \phi(\mathbb{C}) = 1$ ,  $\# \text{ker } \phi(\mathbb{C}) = 2^{\deg f_1 \deg f_2 + 1}$ .  $\square$  by Corollary 3.3.3 and  $\mu = 1$  (see Remark 2.3.14).

When  $K_v \cong \mathbb{R}$ , [24, Lemma 3.4] converts the kernel/cokernel contribution into the required form.

Finally, when  $K_v/\mathbb{Q}_p$  we use that  $\text{ord}_2(|\cdot|_v) = 0$  for odd  $p$ .  $\square$

**Example 4.3.4.** Let  $K = \mathbb{Q}(\sqrt{-19})$ ,  $f_1(x) = x$  and  $f_2(x) = -27x^2 + \frac{35}{2}x - \frac{43}{16}$ . Then  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$  have genus 0 and

$$X_0 : w^2 = -27x^3 + \frac{35}{2}x^2 - \frac{43}{16}x, \quad X : z^2 = -27y^4 + \frac{35}{2}y^2 - \frac{43}{16}$$

and have genus 1 with  $\text{Jac}_X : Z^2 = Y^3 - 31779Y - 2179170$  (by Lemma 2.1.6).

First note that,  $\mu_v(X_0) = \mu_v(X) = 1$  (by Remark 2.3.13) and  $\mu_v(X_1) = \mu_v(X_2) = 1$  ( $X_1, X_2$  have a  $K$ -point  $\Rightarrow$  a  $K_v$  rational divisor of any degree) at each place  $v$  of  $K$ . Using that  $X_0, \text{Jac}_X$  have good reduction away from  $v \mid 3 \cdot 43$ , Theorem 4.3.3 reduces to

$$\text{rk}(X_0) = \text{rk}(\text{Jac}_X) \equiv \text{ord}_2 \lambda_\infty(x, f_2) + \sum_{v \mid 2, 3, 43} \text{ord}_2 \lambda_v(x, f_2) \pmod{2}$$

where  $\infty$  denotes the unique place of  $K$  whose completion is  $\mathbb{C}$ . We proceed by

computing the terms on the right-hand side.

Since  $\deg f_1 \deg f_2 = 2$ ,  $\text{ord}_2 \lambda_\infty(x, f_2) \equiv 1 \pmod{2}$ .

Let  $v$  be the unique place above 2 (this is inert in  $K$ ). Using that  $X_0$  and  $\text{Jac}_X$  have good reduction at  $v$  and that the residue field of  $K_v$  has size 4,

$$\text{ord}_2 \lambda_v(x, f_2) = \text{ord}_2(|\phi^* \omega_{\text{Jac}_X}^0 / \omega_{X_0}^0|_v) \equiv 0 \pmod{2}.$$

Now let  $v$  be the unique place above 3 (this is also inert in  $K$ ). Since  $c_v(X_0) = 6$  and  $c_v(\text{Jac}_X) = 3$  (as computed in Sage [63]),  $\text{ord}_2 \lambda_v(x, f_2) \equiv 1 \pmod{2}$ .

Finally, let  $v_1, v_2 \mid 43$  (this splits in  $K$ ) be distinct. Then  $K_{v_1} \cong K_{v_2}$  and so  $\text{ord}_2 \lambda_{v_1}(x, f_2) + \text{ord}_2 \lambda_{v_2}(x, f_2) \equiv 0 \pmod{2}$ .

In summary, if  $\text{III}(X_0)$  is finite then by Theorem 4.3.3,

$$\text{rk}(X_0) = \text{rk}(\text{Jac}_X) \equiv 1 + 1 \equiv 0 \pmod{2}.$$

**Remark 4.3.5.** In general, such a computation would require the local data attached to hyperelliptic and bihyperelliptic curves, not just elliptic curves. In many cases we can compute the Tamagawa numbers for these using Theorem 2.3.3 and Theorems 2.4.9 and 2.4.14.

## 4.4 Rank parity formulae for $S_3$

Recall the set up of §3.4. In particular,  $K$  is a field of characteristic 0 and

$$X : \{y^2 = f(x), \Delta^2 = g(y^2)\}$$

admits an action of  $S_3 = \langle \sigma, \tau \rangle$  where  $f(x) = x^3 + ax + b \in K[x]$  is a separable cubic and  $g(y^2) = -27y^4 + 54by^2 - (4a^3 + 27b^2) \in K[y]$ . We assume that  $a \neq 0$  to additionally define genus 1 curves

$$E : y^2 = f(x), \quad D : \Delta^2 = g(y^2).$$

**Lemma 4.4.1.** *Let  $K$  be a number field and  $\Theta = 2\langle\tau\rangle + \langle\sigma\rangle - 2S_3 - \{1\}$ . Then,*

$$\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = 3^{\text{rk}(E) + \text{rk}(\text{Jac}_D)}.$$

*Proof.* Write  $\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbf{1}^{\oplus n_1} \oplus \epsilon^{\oplus n_2} \oplus \rho^{\oplus n_3}$  for the decomposition into irreducible representations of  $S_3$ , where  $\epsilon$  has dimension 1 and  $\rho$  has dimension 2. By [18, Example 1.5],

$$\mathcal{C}_\Theta(\mathbf{1}) = \mathcal{C}_\Theta(\epsilon) = \mathcal{C}_\Theta(\rho) = 3$$

and so Lemma 2.6.4 yields that  $\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = 3^{n_1 + n_2 + n_3}$ . Applying Lemma 2.1.14 with  $H = \langle\tau\rangle$  and taking dimensions immediately gives that  $\text{rk}(E) = n_1 + n_3$  (since  $H$  fixes a 1 dimensional subspace of  $\rho$ ). Similarly, letting  $H = \langle\sigma\rangle$  gives that  $\text{rk}(\text{Jac}_D) = n_1 + n_2$  and letting  $H = S_3$  gives that  $0 = \text{rk}(\text{Jac}_{\mathbb{P}^1}) = n_1$ . The result then follows.  $\square$

**Definition 4.4.2.** Let  $\mathcal{K}$  be a local field of characteristic 0 and  $\phi : E \times E \times \text{Jac}_D \rightarrow \text{Jac}_X$  be the  $\mathcal{K}$ -isogeny constructed in Theorem 3.4.3. We define the local invariant  $\lambda_{\mathcal{K}}(E)$  to be

$$\left\{ \begin{array}{ll} 1 & \mathcal{K} \simeq \mathbb{C}, \\ \#\ker \phi(\mathcal{K}) & \mathcal{K} \simeq \mathbb{R}, \\ \frac{c(\text{Jac}_D)}{c(\text{Jac}_X)} & \mathcal{K}/\mathbb{Q}_p \text{ finite, } p \neq 3, \\ \frac{c(\text{Jac}_D)}{c(\text{Jac}_X)} \Big|_{\omega_{E \times E \times \text{Jac}_D/\mathcal{K}}^0}^{\phi^* \omega_{\text{Jac}_X/\mathcal{K}}^0} \Big|_{\mathcal{K}} & \mathcal{K}/\mathbb{Q}_3 \text{ finite.} \end{array} \right.$$

**Remark 4.4.3.** Let  $\phi' : E \times E \times \text{Jac}_D \rightarrow \text{Jac}_X$  be any  $\mathcal{K}$ -isogeny. We could instead define an invariant  $\lambda_{\mathcal{K}}(E, \phi')$  to be as above when  $\mathcal{K} \cong \mathbb{R}$  or  $\mathcal{K}/\mathbb{Q}_p$  finite (replacing  $\phi$  by  $\phi'$ ) and equal to  $\deg \phi'$  when  $\mathcal{K} \cong \mathbb{C}$ . The following theorem would still hold upon replacing  $\lambda_{\mathcal{K}}(E)$  by  $\lambda_{\mathcal{K}}(E, \phi')$ .

**Theorem 4.4.4.** *Let  $K$  be a number field and  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) an elliptic curve over  $K$ . Let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ .*

*Assuming that  $\text{III}(E)$ ,  $\text{III}(\text{Jac}_D)$  are finite,*

$$\text{rk}(E) + \text{rk}(\text{Jac}_D) \equiv \sum_{v \text{ place of } K} \text{ord}_3 \lambda_v(E) \pmod{2}$$

where  $\lambda_v(E)$  is as in Definition 4.4.2.

*Proof.* Let  $G = S_3$ ,  $\Theta = 2\langle\tau\rangle + \langle\sigma\rangle - 2G - \{1\}$  and  $p = 3$ . Combining Corollary 4.2.7 and Lemma 4.4.1 gives a modulo 2 formula for  $\text{rk}(E) + \text{rk}(\text{Jac}_D)$ . We now argue that the terms on the right-hand-side of this formula are congruent to  $\text{ord}_3 \lambda_v(E)$ . First note that  $\text{ord}_3(\mu_v) = 0$  since  $\mu_v = 1$  or  $2$ .

When  $K_v \cong \mathbb{C}$ , this holds since  $\#\text{coker } \phi(\mathbb{C}) = 1$  and  $\#\ker \phi(\mathbb{C}) = 9$  by Theorem 3.4.3.

When  $K_v \cong \mathbb{R}$ , apply [24, Lemma 3.4] and use that  $\text{ord}_3(n_A) = 0$  for any abelian variety  $A/K_v$  to see that  $\text{ord}_3\left(\frac{\#\ker \phi(K_v)}{\#\text{coker } \phi(K_v)}\right) = \text{ord}_3(\#\ker \phi|_{(E \times E \times \text{Jac}_D)(K_v)^\circ}) = \text{ord}_3(\#\ker \phi(K_v))$ .

Finally, when  $K_v/\mathbb{Q}_p$  we use that  $\text{ord}_3(c(E)^2) \equiv 0 \pmod{2}$  and  $\text{ord}_3(|\cdot|_v) = 0$  when  $p \neq 3$ .  $\square$

By Lemma 3.4.2,  $X$  has genus 3 whenever  $a \neq 0$ . At present, the theory of non-hyperelliptic genus 3 curves over  $p$ -adic fields is limited and so determining their local invariants, such as Tamagawa numbers, can pose a challenge. Recall that we exhibited a bihyperelliptic model for  $X$ , allowing us to study the curve locally via [27]. Since we are only interested in the 3-part of its Tamagawa number (c.f. Theorem 4.4.4), we note the following.

**Lemma 4.4.5.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension,  $E : y^2 = f(x) := x^3 + ax + b \in \mathcal{K}[x]$  (with  $a \neq 0$ ),  $C : W^2 = -(3x^2 + 4a)f(x)$  and  $X : \{y^2 = f(x), \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)\}$ . Then*

$$\text{ord}_3 c(\text{Jac}_X) = \text{ord}_3 c(E)c(\text{Jac}_C).$$

*Proof.* As observed in Lemma 3.4.2, there's an isogeny  $E \times \text{Jac}_C \rightarrow \text{Jac}_X$  of degree 8 (by Corollary 3.3.3). A straightforward generalisation of [21, Lemma 6.2] gives that  $c(\text{Jac}_X) = 2^n \cdot c(E)c(\text{Jac}_C)$  for some  $n \in \mathbb{Z}$ .  $\square$

**Example 4.4.6.** Let  $K = \mathbb{Q}(\sqrt{-19})$  and fix  $f(x) = x^3 - \frac{1}{3}x + \frac{35}{108}$ . Then

$$E : y^2 = x^3 - \frac{1}{3}x + \frac{35}{108}, \quad D : \Delta^2 = -27y^4 + \frac{35}{2}y^2 - \frac{43}{16},$$



and  $\text{Jac}_D : Z^2 = Y^3 - 31779Y - 2179170$  (by Lemma 2.1.6).

Noting that  $E$ ,  $\text{Jac}_D$ ,  $\text{Jac}_X$  have good reduction when  $v \nmid 3 \cdot 43$ , Theorem 4.4.4 says that

$$\text{rk}(E) + \text{rk}(\text{Jac}_D) \equiv \sum_{v|3,43} \text{ord}_3 \lambda_v(E) \pmod{2}$$

since  $\text{ord}_3 \lambda_\infty(E) = 0$  (where  $\infty$  denotes the unique place of  $K$  whose completion is  $\mathbb{C}$ ). We proceed by computing the terms on the right-hand side.

Let  $v$  be the unique place above 3 (this is inert in  $K$ ). Since  $c_v(\text{Jac}_D) = 3$  it remains to compute  $\text{ord}_3 c_v(\text{Jac}_X) = \text{ord}_3 c_v(E)c_v(\text{Jac}_C)$  (as in Lemma 4.4.5). We have  $c_v(E) = 1$  and  $c_v(\text{Jac}_C) = 2$ , where the Tamagawa number for  $C$  has been computed using [22, Theorem 8.5] with  $\Sigma_{C/K_v} = \langle \langle \langle \langle \langle \cdot \rangle \rangle \rangle \rangle \rangle_{-1}$ . Therefore  $\text{ord}_3 \lambda_v(E) \equiv 1 \pmod{2}$ .

As in Example 4.3.4, 43 splits in  $K$  and so  $\text{ord}_3 \lambda_{v_1}(E) + \text{ord}_3 \lambda_{v_2}(E) \equiv 0 \pmod{2}$  where  $v_1, v_2 \mid 43$  are distinct.

To summarise, if  $\text{III}(E)$  and  $\text{III}(\text{Jac}_D)$  are finite then by Theorem 4.4.4,

$$\text{rk}(E) + \text{rk}(\text{Jac}_D) \equiv 1 \pmod{2}.$$

In light of Example 4.3.4, where we showed that  $\text{rk}(\text{Jac}_D) \equiv 0 \pmod{2}$ , we can in fact assert that  $\text{rk}(E)$  is odd (conditional on the finiteness of  $\text{III}(E)$  and  $\text{III}(\text{Jac}_D)$ ) and that  $E$  has infinitely many  $K$ -points.

This isn't an isolated example, we can always apply both Theorem 4.3.3 and Theorem 4.4.4 to compute the parity of the rank of a general elliptic curve.

**Remark 4.4.7.** Recall that  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ . By Example 3.3.5,

$$\text{Jac}_D : Z^2 = Y^3 - 34992(a^3 + 9b^2)Y - 11337408(a^3 + 6b^2)$$

admits a 2-isogeny. Mapping the 2-torsion point  $(-324b, 0)$  to  $(0, 0)$  and replacing  $Y, Z$  by  $6^2Y, 6^3Z$  we see that

$$\text{Jac}_D : Z^2 = Y^3 - 27bY^2 - 27a^3Y.$$

**Corollary 4.4.8.** *Let  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) be an elliptic curve over a number field  $K$ . Let  $g(x) = -27x^2 + 54bx - (4a^3 + 27b^2)$ . Assuming that  $\text{III}(E)$ ,  $\text{III}(\text{Jac}_{\Delta^2=g(y^2)})$  are finite,*

$$\text{rk}(E) \equiv \sum_{v \text{ place of } K} \text{ord}_3 \lambda_v(E) + \text{ord}_2 \lambda_v(g(x), x) \pmod{2}$$

where  $\lambda_v(E)$  is as in Definition 4.4.2 and  $\lambda_v(g(x), x)$  is as in Definition 4.3.2.

*Proof.* By Theorem 4.4.4,

$$\text{rk}(E) + \text{rk}(\text{Jac}_{\Delta^2=g(y^2)}) \equiv \sum_{v \text{ place of } K} \text{ord}_3 \lambda_v(E) \pmod{2}.$$

Applying Theorem 4.3.3 with  $f_1(x) = g(x)$  and  $f_2(x) = x$  gives that

$$\text{rk}(\text{Jac}_{\Delta^2=g(y^2)}) \equiv \text{rk}(\text{Jac}_{w^2=xg(x)}) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(g(x), x) \pmod{2}$$

since  $\text{Jac}_{\Delta^2=g(y^2)}$  is isogenous to  $\text{Jac}_{w^2=xg(x)}$ . Summing these two expressions gives the desired formula.  $\square$

## 4.5 Selmer group analogue

The formulae exhibited in the previous sections all rely on the finiteness of the Shafarevich–Tate group. Here we state an analogue for Selmer groups (whose proof will be omitted), where this assumption can be dropped.

**Theorem 4.5.1** ([23], Theorem 7.4). *Let  $X$  be a curve defined over a number field  $K$ ,  $G$  be a finite group of  $K$ -automorphisms of  $X$  and  $\Theta = \sum_i H_i - \sum_j H'_j$  be a Brauer relation for  $G$ . For  $p \in \mathbb{Z}$  a prime,*

$$\text{ord}_p \mathcal{C}_\Theta(\mathcal{X}_p(\text{Jac}_X)) \equiv \sum_{v \text{ place of } K} \text{ord}_p \left( \frac{C_v(\prod_i \text{Jac}_{X_{H_i}}, \omega) \cdot \prod_i \mu_v(X_{H_i})}{C_v(\prod_j \text{Jac}_{X_{H'_j}}, \omega') \cdot \prod_j \mu_v(X_{H'_j})} \right) \pmod{2}$$

where  $\omega, \omega'$  denote fixed choices of non-zero global exterior forms for  $\prod_i \text{Jac}_{X_{H_i}}, \prod_j \text{Jac}_{X_{H'_j}}$  respectively.

Of particular interest to us are the analogues this provides of the explicit local formulae given in §4.3 and §4.4.

**Theorem 4.5.2.** *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  is separable. Then*

$$\mathrm{rk}_2(\mathrm{Jac}_{X_1}) + \mathrm{rk}_2(\mathrm{Jac}_{X_2}) + \mathrm{rk}_2(\mathrm{Jac}_{X_0}) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2 \lambda_v(f_1, f_2) \pmod{2}$$

where  $\lambda_v(f_1, f_2)$  is as in Definition 4.3.2.

**Theorem 4.5.3.** *Let  $K$  be a number field and  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) an elliptic curve over  $K$ . Let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ . Then*

$$\mathrm{rk}_3(E) + \mathrm{rk}_3(\mathrm{Jac}_D) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_3 \lambda_v(E) \pmod{2}$$

where  $\lambda_v(E)$  is as in Definition 4.4.2.

As before, these instances of Theorem 4.5.1 are deduced by looking at Brauer relations in the groups  $C_2 \times C_2$  and  $S_3$ . As in Corollary 4.4.8, we can apply them both with relevant assumptions on the Shafarevich–Tate group to formulate an arithmetic analogue of the parity conjecture for elliptic curves, i.e. an expression in local data for the parity of the rank.

Using Brauer relations in  $C_2 \times C_2$ ,  $D_{2p}$  (for  $p$  a prime) and  $D_8$ , this same procedure allows us to formulate an arithmetic analogue of the parity conjecture for arbitrary Jacobians. Once again, the proof of this relies on the finiteness of the Shafarevich–Tate group, but bypasses the conjectured analytic continuation of  $L$ -functions, their conjectured functional equations and the Birch–Swinnerton-Dyer conjecture (all of which are currently required for the parity conjecture to hold). We will not discuss the proof here and instead refer the reader to [23, Theorem 8.16(i)].

These formulae provide starting points for proving new cases of the parity conjecture, the focus of the remainder of this thesis.

## Chapter 5

# The Parity Conjecture for Elliptic Curves

In the previous chapter, Corollary 4.4.8 detailed a local formula for the parity of the rank of an arbitrary elliptic curve (assuming the finiteness of the Shafarevich–Tate group) which resembles the parity conjecture. Recall,

**Conjecture** (The parity conjecture). *Let  $E$  be an elliptic curve over a number field  $K$ . Then*

$$(-1)^{\mathrm{rk}(E)} = \prod_{v \text{ place of } K} w_v(E).$$

At present, there is no unconditional proof of this conjecture. For an arbitrary elliptic curve, it is known to be true under the assumption that  $\mathrm{III}(E/K(E[2]))$  has finite 2- and 3-primary parts [20, Theorem 1.2]. In this chapter we provide a new proof, under different assumptions on the Shafarevich–Tate group.

Specifically, we compare the local terms  $\lambda_v(E)$  appearing in Theorem 4.5.3, which control the parity of the  $3^\infty$ -Selmer rank of  $E \times \mathrm{Jac}_D$  ( $D$  is a genus 1 curve closely related to  $E$ ), to the product of local root numbers  $w_v(E)w_v(\mathrm{Jac}_D)$ . It turns out that these terms are not equal place-by-place and we provide a description of their difference (in most cases) in Theorem 5.1.2. An immediate consequence of this comparison is that the terms match globally (i.e. when summing/taking the product over all places of  $K$ ). We therefore deduce that the 3-parity conjecture holds for  $E \times \mathrm{Jac}_D$  (=Theorem 5.1.3). The parity conjecture for  $E$  then follows from

known cases of the 2-parity conjecture and imposing relevant assumptions on  $\text{III}(E)$ ,  $\text{III}(\text{Jac}_D)$  (=Theorem 5.1.5).

## 5.1 Global results

We adopt the notation of §3.4 and §4.4, which we recall below.

**Notation 5.1.1.** Let  $K$  be a field of characteristic 0 and  $f(x) = x^3 + ax + b \in K[x]$  be a separable cubic. Let  $g(y^2) = -27y^4 + 54by^2 - (4a^3 + 27b^2) \in K[y]$  be the discriminant of  $f(x) - y^2$  (viewed as a polynomial in  $x$ ). Assume that  $a \neq 0$  and define curves over  $K$  by

$$E : y^2 = f(x), \quad D : \Delta^2 = g(y^2), \quad X : \{y^2 = f(x), \Delta^2 = g(y^2)\}.$$

Let  $\phi : E \times E \times \text{Jac}_D \rightarrow \text{Jac}_X$  be the  $K$ -isogeny constructed in §3.4.

Recall that  $E$  and  $\text{Jac}_D$  are elliptic curves and  $X$  is a genus 3 curve (see Lemma 3.4.2). When  $K$  is a number field, Theorem 4.5.3 gives a formula for the parity of the  $3^\infty$ -Selmer rank of  $E \times \text{Jac}_D$ . From this, we are able to deduce the 3-parity conjecture via the following result.

**Theorem 5.1.2** (Local Theorem I). *Let  $E : y^2 = x^3 + ax + b$  (with  $a \neq 0$ ) be an elliptic curve over a local field  $\mathcal{K}$ . Whenever*

- (i)  $\mathcal{K} \cong \mathbb{C}$ ,
- (ii)  $\mathcal{K}/\mathbb{Q}_p$  is finite, or
- (iii)  $\mathcal{K} \cong \mathbb{R}$  and  $a, b \in \overline{\mathbb{Q}}$  are such that  $E/\mathbb{Q}(a, b)$  does not admit a 3-isogeny,

we have that

$$(-1)^{\text{ord}_3 \lambda_{\mathcal{K}}(E) + \text{ord}_3 |3|_{\mathcal{K}}} = w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_D)$$

where  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$  and  $\lambda_{\mathcal{K}}(E)$  is as in Definition 4.4.2.

We postpone the proof of this theorem to the subsequent section and first present its global consequences.

**Theorem 5.1.3.** *Let  $E : y^2 = x^3 + ax + b$  be an elliptic curve over a number field  $K$  and let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ . The 3-parity conjecture holds for  $E \times \text{Jac}_D$ .*

*Proof.* If  $a = 0$  then  $E$  admits a 3-isogeny and  $D$  has genus 0. The 3-parity conjecture is known to hold for such elliptic curves by [20, Theorem 1.8] and so we're done (since  $\text{Jac}_D = 0$ ).

If  $a \neq 0$  and  $E$  admits a 3-isogeny then  $3x^4 + 6ax^2 - 12bx - a^2$  (the 3rd division polynomial for  $E$ ) has a root  $r \in K^\times$ . Since  $\text{Jac}_D : Z^2 = Y^3 - 27bY^2 - 27a^3Y$  (by Remark 4.4.7) has 3rd division polynomial  $x^4 - 36bx^3 - 54a^3x^2 - 243a^6$  with root  $-3a^2/r \in K$ , we see that  $\text{Jac}_D$  also admits a 3-isogeny. Again, the 3-parity conjecture is then known to hold for both  $E$  and  $\text{Jac}_D$ .

If  $a \neq 0$  and  $E$  does not admit a 3-isogeny then Theorem 5.1.2 says that, for each place  $v$  of  $K$ ,  $(-1)^{\text{ord}_3 \lambda_v(E) + \text{ord}_3 |3|_v} = w_v(E)w_v(\text{Jac}_D)$ . The result then follows upon taking the product over all such  $v$  and then invoking Theorem 4.5.3 and the fact that  $\prod_v |3|_v = 1$  (the product formula for absolute values on  $K$ ).  $\square$

**Corollary 5.1.4.** *Let  $E : y^2 = x^3 + ax + b$  be an elliptic curve over a number field  $K$  and let  $D : \Delta^2 = -27y^4 + 54by^2 - (4a^3 + 27b^2)$ . Then*

$$(-1)^{\text{rk}_3(E) + \text{rk}_3(\text{Jac}_D) + \text{rk}_2(\text{Jac}_D)} = w(E).$$

*Proof.* By Remark 4.4.7,  $\text{Jac}_D$  admits a 2-isogeny and so it is known to satisfy the 2-parity conjecture ([20, Theorem 1.8]).  $\square$

Imposing certain assumptions on the Shafarevich–Tate group we are now able to deduce that the parity conjecture holds for elliptic curves.

**Theorem 5.1.5.** *Let  $E : y^2 = f(x)$  be an elliptic curve over a number field  $K$ . Let  $D : \Delta^2 = g(y^2)$  where  $g(y^2) \in K[y]$  is the discriminant of  $f(x) - y^2$ . Assuming that  $\text{III}(E)$  has finite 3-primary part and  $\text{III}(\text{Jac}_D)$  has finite 2- and 3-primary parts, the parity conjecture holds for  $E$ .*

**Remark 5.1.6.** The assumption that the 2- and 3-primary parts of  $\text{III}(\text{Jac}_D)$  are finite could in fact be replaced by the weaker assumption that  $\text{rk}_3(\text{Jac}_D) \equiv \text{rk}_2(\text{Jac}_D) \pmod{2}$ .

## 5.2 Proof of Local Theorem I

We now turn our attention to proving Theorem 5.1.2.

**Proposition 5.2.1.** *Theorem 5.1.2 holds when  $\mathcal{K} \cong \mathbb{C}$ .*

*Proof.* Clearly  $(-1)^{\text{ord}_3 \lambda_{\mathcal{K}}(E)} = (-1)^{\text{ord}_3 |3|_{\mathcal{K}}} = +1$  and since  $E$  and  $\text{Jac}_D$  are elliptic curves,  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = -1$  (Lemma 2.3.4).  $\square$

**Lemma 5.2.2.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be finite. It is sufficient to prove Theorem 5.1.2 when  $a, b \in \mathcal{O}_{\mathcal{K}}$ .*

*Proof.* Let  $E$  be as in the statement of Theorem 5.1.2 and let  $u \in \mathcal{K}^{\times}$  be such that  $u^4 a, u^6 b \in \mathcal{O}_{\mathcal{K}}$ . Let  $E' : y^2 = x^3 + u^4 a x + u^6 b \in \mathcal{O}_{\mathcal{K}}[x]$  and define  $D', X'$  as usual. Then  $X \ni (x, y, \Delta) \mapsto (u^{-2}x, u^{-3}y, u^{-6}\Delta) \in X'$  is an isomorphism, giving that  $E \cong E'$ ,  $D \cong D'$  too. Therefore, proving Theorem 5.1.2 for  $E$  is equivalent to proving it for  $E'$ .  $\square$

**Proposition 5.2.3.** *Theorem 5.1.2 holds when  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p \neq 2, 3$  and  $E \times \text{Jac}_D/\mathcal{K}$  is semistable.*

*Proof.* Below, all equivalences are taken modulo  $\pi$ , where  $\pi$  is a uniformiser of  $\mathcal{K}$ . We write  $v$  for a normalised valuation on  $\overline{\mathcal{K}}$ , i.e.  $v(\pi) = 1$ . We may assume by Lemma 5.2.2 that  $a, b \in \mathcal{O}_{\mathcal{K}}$ . Consider the model  $\text{Jac}_D : Z^2 = Y^3 - 27bY^2 - 27a^3Y$  (given in Remark 4.4.7) and let  $C : W^2 = -(3x^2 + 4a)(x^3 + ax + b)$ . By Lemma 4.4.5, it suffices to show that

$$(-1)^{\text{ord}_3(c_{\mathcal{K}}(\text{Jac}_D)c_{\mathcal{K}}(E)c_{\mathcal{K}}(\text{Jac}_C))} = w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_D).$$

Let  $d := 4a^3 + 27b^2$  and note that  $\Delta_E = -16d$ ,  $\Delta_{\text{Jac}_D} = -314928a^6d$  and  $\Delta_C = 12288ad^3$ . Since  $E$  is semistable, we can assume that  $a \equiv 0 \Rightarrow b \not\equiv 0$  (if not, we can perform a change of variables so that this is satisfied).

We use Tate's algorithm ([65] or [61, Chapter IV, §9]) to compute  $c_{\mathcal{K}}(E)$ ,  $c_{\mathcal{K}}(\text{Jac}_D)$ , Theorem 2.4.9 to compute  $c_{\mathcal{K}}(\text{Jac}_C)$  from  $\Sigma_{C/\mathcal{K}}$  and Theorem 2.3.6 for  $w_{\mathcal{K}}(E)$ ,  $w_{\mathcal{K}}(\text{Jac}_D)$ .

**Suppose  $a, d$  are units.**  $E$ ,  $\text{Jac}_D$  and  $\text{Jac}_C$  have good reduction, so  $c_{\mathcal{K}}(\text{Jac}_D) = c_{\mathcal{K}}(E) = c_{\mathcal{K}}(\text{Jac}_C) = 1$  and  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = +1$ .

**Suppose  $a \equiv 0$ .** Then  $b, d$  are units and so  $c_{\mathcal{K}}(E) = 1$ ,  $w_{\mathcal{K}}(E) = +1$ . Observe that the reductions of  $\text{Jac}_D$  and  $C$  are  $Z^2 = Y^2(Y - 27b)$  and  $W^2 = -3x^2(x^3 + b)$  respectively with  $\Sigma_{C/\mathcal{K}} = \overline{\text{O} \circledast_{v(a)} \text{O} \circledast \text{O}}_0$ . If  $-3b$  is a square modulo  $\pi$  then  $c_{\mathcal{K}}(\text{Jac}_D) = 6v(a)$ ,  $c_{\mathcal{K}}(\text{Jac}_C) = v(a)$  (since  $\epsilon = +$ ) and  $w_{\mathcal{K}}(\text{Jac}_D) = -1$ . If  $-3b$  is not a square modulo  $\pi$  then  $c_{\mathcal{K}}(\text{Jac}_D) = 2$ ,  $w_{\mathcal{K}}(\text{Jac}_D) = +1$  and  $c_{\mathcal{K}}(\text{Jac}_C) = \gcd(v(a), 2)$  (since  $\epsilon = -$ ).

**Suppose  $d \equiv 0$ .** Then  $a, b$  are units. Observe that the reductions of  $E$ ,  $\text{Jac}_D$  and  $C$  are  $y^2 = (x - \frac{3b}{a})(x + \frac{3b}{2a})^2$ ,  $Z^2 = Y(Y - \frac{27b}{2})^2$  and  $W^2 = -3(x - \frac{3b}{a})^2(x + \frac{3b}{2a})^2(x + \frac{3b}{a})$  respectively with  $\Sigma_{C/\mathcal{K}} = \overline{\text{O} \circledast_{v(d)} \text{O} \circledast_{2v(d)} \text{O}}_0$ . If  $6b$  is a square modulo  $\pi$  then  $c_{\mathcal{K}}(E) = c_{\mathcal{K}}(\text{Jac}_D) = v(d)$ ,  $c_{\mathcal{K}}(\text{Jac}_C) = 2v(d)^2$  (since  $\epsilon = +$ ) and  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = -1$ . If  $6b$  is not a square modulo  $\pi$  then  $c_{\mathcal{K}}(E) = c_{\mathcal{K}}(\text{Jac}_D) = \gcd(v(d), 2)$  (since  $\epsilon = -$ ),  $c_{\mathcal{K}}(\text{Jac}_C) = 2\gcd(v(d), 2)$  and  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = +1$ .  $\square$

**Proposition 5.2.4.** *Theorem 5.1.2 holds when  $\mathcal{K} \cong \mathbb{R}$ ,  $a, b \in \overline{\mathbb{Q}}$  and  $E/\mathbb{Q}(a, b)$  does not admit a 3-isogeny.*

*Proof.* Note that  $\text{ord}_3|3|_{\mathcal{K}} = 1$ . Since  $E$  and  $\text{Jac}_D$  are elliptic curves,  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = -1$  (see Lemma 2.3.4). By definition of  $\lambda_{\mathcal{K}}(E)$ , it remains to compute  $(-1)^{\text{ord}_3 \# \ker \phi(\mathcal{K})}$ .

It follows from the proof of Theorem 3.4.3 that  $\ker \phi \leq \{(P, -P, R) : P \in E[3], R \in \text{Jac}_D[3]\}$  and  $\# \ker \phi = 9$ . Consider the projection  $f : \ker \phi \rightarrow E[3]$  onto the first coordinate. Since  $E$  does not admit a  $\mathbb{Q}(a, b)$ -rational 3-isogeny,  $E[3]$  has no non-trivial subgroup which is stable under  $G_{\mathbb{Q}(a, b)}$ , therefore  $f(\ker \phi) = 0$  or  $E[3]$ . By this observation, either  $\ker \phi = \{(0, 0, R) : R \in \text{Jac}_D[3]\}$  or  $\ker \phi \cong E[3]$  and in both cases  $\# \ker \phi(\mathcal{K}) = 3$ . In particular,  $(-1)^{\text{ord}_3 \# \ker \phi(\mathcal{K})} = -1$ .  $\square$

**Lemma 5.2.5.** *Theorem 5.1.2 holds when  $\mathcal{K}/\mathbb{Q}_2$  is finite and  $E : y^2 = x^3 - \frac{1}{3}x + \frac{35}{108}$ .*



*Proof.* Note that  $\text{ord}_3|3|_{\mathcal{K}} = 0$ .  $E$ ,  $\text{Jac}_D$  and  $\text{Jac}_X$  all have good reduction over  $\mathcal{K}$ , so  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_D) = +1$  and  $\lambda_{\mathcal{K}}(E) = 1$ .  $\square$

Let  $Y/\mathcal{K}$  be a curve over a local field. Write  $\omega_Y^0$  for the wedge product of a basis of integral differentials of  $Y$ , i.e. an  $\mathcal{O}_{\mathcal{K}}$ -basis of the global sections of the relative dualising sheaf of a regular model of  $Y$ , as an  $\mathcal{O}_{\mathcal{K}}$  lattice in  $\Omega^1(Y)$  (see [38]).

**Lemma 5.2.6.** *Let  $\mathcal{K}/\mathbb{Q}_3$  be finite. Then*

$$\left| \frac{\phi^* \omega_{\text{Jac}_X/\mathcal{K}}^0}{\omega_{E \times E \times \text{Jac}_D/\mathcal{K}}^0} \right|_{\mathcal{K}} = \left| \frac{3\gamma}{\alpha\beta} \right|_{\mathcal{K}}$$

where  $\alpha, \beta, \gamma \in \mathcal{K}$  are such that  $\omega_E^0 = \alpha \frac{dx}{y}$ ,  $\omega_D^0 = \beta \frac{dy}{\Delta}$  and  $\omega_C^0 = \gamma \left( \frac{dx}{W} \wedge x \frac{dx}{W} \right)$  for  $C : W^2 = -(3x^2 + 4a)(x^3 + ax + b)$ .

*Proof.* We first observe that

$$\left| \frac{\phi^* \omega_{\text{Jac}_X/\mathcal{K}}^0}{\omega_{E \times E \times \text{Jac}_D/\mathcal{K}}^0} \right|_{\mathcal{K}} = 9 \left| \frac{\omega_{\text{Jac}_X/\mathcal{K}}^0}{(\phi^{\vee})^* \omega_{E \times E \times \text{Jac}_D/\mathcal{K}}^0} \right|_{\mathcal{K}}$$

using the description of  $\phi^{\vee} \circ \phi$  given in Theorem 3.4.3. Let  $\psi = ((\pi_2)_*, (\pi_0)_*) : \text{Jac}_X \rightarrow E \times \text{Jac}_C$  denote the isogeny of degree 8 identified in Theorem 3.3.2 (where we let  $f_1(x) = -(3x^2 + 4a)$ ,  $f_2(x) = x^3 + ax + b$  so that  $X_1 = \mathbb{P}^1$ ,  $X_2 = E$  and  $X_0 = C$ ). Then

$$\left| \frac{\omega_{\text{Jac}_X/\mathcal{K}}^0}{(\phi^{\vee})^* \omega_{E \times E \times \text{Jac}_D/\mathcal{K}}^0} \right|_{\mathcal{K}} = \left| \frac{\omega_{\text{Jac}_X}^0}{\psi^* \omega_{E \times \text{Jac}_C}^0} \cdot \frac{\psi^* \omega_{E \times \text{Jac}_C}^0}{(\phi^{\vee})^* \omega_{E \times E \times \text{Jac}_D}^0} \right|_{\mathcal{K}}$$

where we observe that, by [21, Lemma 4.3], the first term is a unit. We compute

$$\begin{aligned} \psi^* \omega_{E \times \text{Jac}_C}^0 &= \psi^*(\omega_E^0 \wedge \omega_C^0) \\ &= ((\pi_2)_*)^* \omega_E^0 \wedge ((\pi_0)_*)^* \omega_C^0 \\ &= \alpha\gamma \left( \frac{dx}{y} \wedge \frac{dx}{W} \wedge x \frac{dx}{W} \right) \\ &= \alpha\gamma \left( \frac{dx}{y} \wedge \frac{(3x^2 + a)dx}{y\Delta} \wedge x \frac{(3x^2 + a)dx}{y\Delta} \right) \end{aligned}$$

where the first equality uses that the Néron model respects products [54, Proposition 9.6.8] and that  $\omega_{\text{Jac}_C}^0 = \omega_C^0$  [67, Lemma 9], and the second uses Example 4.2.4. Similarly,  $(\phi^\vee)^*(\omega_{E \times E \times \text{Jac}_D}^0) = ((\pi_E)_*)^*\omega_E^0 \wedge ((\pi_E)_* \circ \sigma_*)^*\omega_E^0 \wedge ((\pi_E)_*)^*\omega_D^0 = \alpha^2\beta\left(\frac{dx}{y} \wedge \frac{dx'}{y} \wedge \frac{dy}{\Delta}\right)$  where  $x' = -\frac{x}{2} + \frac{6ax^2+9(y^2-b)x+4a^2}{2\Delta}$  (as in the definition of  $\sigma$ ).

Now using the identities  $2ydy = (3x^2 + a)dx$  and  $\Delta d\Delta = -54y(y^2 - b)dy$ , we see that

$$\frac{dx'}{y} = -\frac{dx}{2y} + \frac{3x(3x^2 + a)dx}{2y\Delta} \quad \text{and} \quad \frac{dy}{\Delta} = \frac{(3x^2 + a)dx}{2y\Delta}.$$

Therefore  $\frac{dx}{y} \wedge \frac{dx'}{y} \wedge \frac{dy}{\Delta} = -\frac{3}{4} \cdot \frac{dx}{y} \wedge \frac{(3x^2+a)dx}{y\Delta} \wedge x \frac{(3x^2+a)dx}{y\Delta}$  and the result follows.  $\square$

**Lemma 5.2.7.** *Let  $E : y^2 = x^3 + ax + b$  an elliptic curve over a finite extension  $\mathcal{K}/\mathbb{Q}_p$  with  $a \neq 0$ . There is an  $\epsilon > 0$  such that changing  $a, b$  to any  $a' \neq 0, b'$  with  $|a - a'|_{\mathcal{K}}, |b - b'|_{\mathcal{K}} < \epsilon$  does not change  $w_{\mathcal{K}}(E)$ ,  $w_{\mathcal{K}}(\text{Jac}_D)$  and  $\text{ord}_3 \lambda_{\mathcal{K}}(E) \pmod{2}$ .*

*Proof.* Root numbers are functions of  $V_\ell E = T_\ell E \otimes \mathbb{Q}_\ell$ , so their local constancy can be seen from that of the Tate module [34, p. 569]. The same argument applies to the 3-part of the Tamagawa number when  $p \neq 3$  since, for  $A/\mathcal{K}$  an abelian variety,  $\text{ord}_3 c_{\mathcal{K}}(A) = \text{ord}_3 \#\Phi(A)[3^\infty]$  and by [31] (or see [33, §2])  $\Phi(A)[3^\infty] \cong H^1(I_{\mathcal{K}}, T_3(A))_{\text{tors}}$  ( $\Phi$  denotes the group of connected components of the special fibre of the Néron model of  $A$  over  $\mathcal{O}_{\mathcal{K}}$ ).

Now consider  $\lambda_{\mathcal{K}}(E)$  when  $p = 3$ . By Lemmata 4.4.5 and 5.2.6 (and using their notation) we need to show that  $\text{ord}_3 c_{\mathcal{K}}(E)$ ,  $\text{ord}_3 c_{\mathcal{K}}(\text{Jac}_D)$ ,  $\text{ord}_3 c_{\mathcal{K}}(\text{Jac}_C)$  and  $\text{ord}_3 |3\gamma/\alpha\beta|_{\mathcal{K}}$  are locally constant. For the terms concerning  $E$  and  $\text{Jac}_D$  this follows from Tate's algorithm [65] (or [61, Chapter IV, §9]). For the terms concerning  $\text{Jac}_C$  this follows from the proof of [24, Lemma 11.2].  $\square$

With this in mind, we are now able to prove the remaining cases of Theorem 5.1.2.

**Proposition 5.2.8.** *Theorem 5.1.2 holds when*

1.  $\mathcal{K}/\mathbb{Q}_3$  is finite,
2.  $\mathcal{K}/\mathbb{Q}_2$  is finite,

3.  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p \neq 2, 3$  and  $E \times \text{Jac}_D/\mathcal{K}$  is not semistable.

*Proof.* We deduce these cases from known instances of the 3-parity conjecture. In particular, we approximate  $f(x) = x^3 + ax + b \in \mathcal{K}[x]$  by a separable cubic  $f_0(x) = x^3 + a_0x + b_0 \in \mathcal{O}_L[x]$  with  $a_0 \neq 0$  where  $L$  is a totally real field, subject to certain conditions. Let  $E_0 : y^2 = f_0(x)$  and define  $D_0, \phi_0$  for this elliptic curve as usual.

(1). Let  $L$  be a totally real number field with a unique prime  $\mathfrak{q} \mid 3$  and with  $L_{\mathfrak{q}} \cong \mathcal{K}$  (to see that such a field exists, if  $\mathcal{K} = \mathbb{Q}_3[x]/(h(x))$  for some monic  $h(x) \in \mathbb{Q}_3[x]$  then approximate  $h(x)$  by  $\tilde{h}(x) \in \mathbb{Q}[x]$  which has all real roots; take  $L = \mathbb{Q}[x]/(\tilde{h}(x))$ ). Fix a prime  $\mathfrak{p}' \nmid 2, 3$ . Choose  $a_0, b_0 \in \mathcal{O}_L$  to be  $\mathfrak{q}$ -adically close to  $a, b$  respectively and  $\mathfrak{r}$ -adically close to  $-\frac{1}{3}, \frac{35}{108}$  respectively whenever  $\mathfrak{r} \mid 2$ . Ensure that  $\mathfrak{p}' \nmid 4a_0^3 + 27b_0^2$  and  $3 \nmid \#E_0(\mathbb{F}_{\mathfrak{p}'^2})$  so that  $E_0$  does not admit a 3-isogeny (this is possible since there exists an  $E_0/\mathbb{F}_{\mathfrak{p}'}$  with  $\#E_0(\mathbb{F}_{\mathfrak{p}'}) \equiv 2 \pmod{3}$  by [56, Theorem 1a], [68]). For primes  $\mathfrak{p} \nmid 2, 3$ , ensure that  $\mathfrak{p} \nmid b_0$  whenever  $\mathfrak{p} \mid a_0$ . Theorem 5.1.2 holds for  $E_0/L_v$  whenever  $L_v/\mathbb{Q}_p$  is finite and  $p \neq 3$  (when  $p \neq 2, 3$  this is Proposition 5.2.3, when  $p = 2$  this is Lemmata 5.2.5 and 5.2.7), or  $L_v \cong \mathbb{R}$  (by Proposition 5.2.4). Since the 3-parity conjecture is known to hold for  $E_0/L$  and  $\text{Jac}_{D_0}/L$  (by [51, Theorem E]),

$$\begin{aligned}
1 &= (-1)^{\text{rk}_3(E_0/L) + \text{rk}_3(\text{Jac}_{D_0}/L)} w(E_0/L) w(\text{Jac}_{D_0}/L) \\
&\stackrel{\text{Thm. 4.5.3}}{=} \prod_{v \text{ place of } L} (-1)^{\text{ord}_3 \lambda_v(E_0)} w_v(E_0) w_v(\text{Jac}_{D_0}) \\
&= (-1)^{\text{ord}_3 \lambda_{\mathfrak{q}}(E_0)} w_{\mathfrak{q}}(E_0) w_{\mathfrak{q}}(\text{Jac}_{D_0}) \cdot \prod_{v \neq \mathfrak{q} \text{ place of } L} (-1)^{\text{ord}_3 |3|_v} \\
&\stackrel{\text{Lemma 5.2.7}}{=} (-1)^{\text{ord}_3 \lambda_{\mathcal{K}}(E) + \text{ord}_3 |3|_{\mathcal{K}}} w_{\mathcal{K}}(E) w_{\mathcal{K}}(\text{Jac}_D).
\end{aligned}$$

(2). Let  $L$  be a totally real number field with a unique prime  $\mathfrak{q} \mid 2$  and with  $L_{\mathfrak{q}} \cong \mathcal{K}$ . Fix a prime  $\mathfrak{p}' \nmid 2, 3$ . Choose  $a_0, b_0 \in \mathcal{O}_L$  to be  $\mathfrak{q}$ -adically close to  $a, b$  respectively. Ensure that  $\mathfrak{p}' \nmid 4a_0^3 + 27b_0^2$  and  $3 \nmid \#E(\mathbb{F}_{\mathfrak{p}'^2})$ . For primes  $\mathfrak{p} \nmid 2, 3$ , ensure that  $\mathfrak{p} \nmid b_0$  whenever  $\mathfrak{p} \mid a_0$ . Theorem 5.1.2 holds for  $E_0/L_v$  whenever  $L_v/\mathbb{Q}_p$  is finite and  $p \neq 2$  (when  $p \neq 2, 3$  this is Proposition 5.2.3, when  $p = 3$  this is (1)), or  $L_v \cong \mathbb{R}$

(by Proposition 5.2.4). Arguing as above proves that Theorem 5.1.2 must also hold for  $E_0/L_q$  and hence  $E/\mathcal{K}$ .

(3). Argue as in (2), replacing 2 by  $p$  and the condition  $\mathfrak{p} \nmid 2, 3$  by  $\mathfrak{p} \nmid 2, 3, p$ .  $\square$

*Proof of Theorem 5.1.2.* This is Proposition 5.2.1 when  $\mathcal{K} \cong \mathbb{C}$ , 5.2.8(2) when  $\mathcal{K}/\mathbb{Q}_2$ , 5.2.8(1) when  $\mathcal{K}/\mathbb{Q}_3$ , Propositions 5.2.3 and 5.2.8(3) when  $\mathcal{K}/\mathbb{Q}_p$  for  $p \neq 2, 3$  and Proposition 5.2.4 when  $\mathcal{K} \cong \mathbb{R}$ .  $\square$

## Chapter 6

# The $p$ -Parity Conjecture for Elliptic Curves over Totally Real Fields

In Chapter 5, we saw an instance in which the formulae developed in Chapter 4 can be used to prove the parity conjecture. In particular, we proved that the parity conjecture holds for elliptic curves over number fields under certain assumptions on the Shafarevich–Tate group (=Theorem 5.1.5).

Here we demonstrate that these assumptions can be weakened when the underlying number field is totally real, by completing the proof of the  $p$ -parity conjecture over such fields. We address the case when  $p = 2$  and the elliptic curve has complex multiplication (=Theorem 6.4.1), with the other cases being dealt with in [19], [20], [48], [49], [50], [51].

To achieve this result we first prove new cases of the 2-parity conjecture over general number fields for abelian surfaces isomorphic to a product of certain elliptic curves, and for elliptic curves whose 2-torsion groups are isomorphic as Galois modules (=Theorems 6.3.1, 6.3.2, 6.3.4). As in the previous chapter, these global results are deduced from a comparison of local invariants (=Theorem 6.1.8), specifically root numbers and the terms appearing in Theorem 4.5.2 when  $f_1(x)$  is a monic cubic and  $f_2(x) = x$ .

The results of this chapter can also be found in [28].

## 6.1 Strategy

**Notation 6.1.1.** Let  $K$  be a field of characteristic 0 and  $f(x) \in K[x]$  be a separable monic cubic with roots  $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}^\times$ . Define curves over  $K$  by

$$E : y^2 = f(x), \quad E' : w^2 = xf(x), \quad X : y^2 = f(x^2)$$

and let  $\phi : E \times \text{Jac}_{E'} \rightarrow \text{Jac}_X$  be the  $K$ -isogeny constructed in Theorem 3.3.2 (by letting  $f_1(x) = f(x)$  and  $f_2(x) = x$ ).

Observe that  $E$  and  $\text{Jac}_{E'}$  are elliptic curves and  $X$  is a genus 2 curve. Moreover,  $\text{Jac}_{E'}$  has the following nice model.

**Remark 6.1.2.** The map  $x_0 = -\frac{\alpha_1\alpha_2\alpha_3}{x}$ ,  $w_0 = \frac{\alpha_1\alpha_2\alpha_3w}{x^2}$  gives

$$\text{Jac}_{E'} : w_0^2 = (x_0 + \alpha_2\alpha_3)(x_0 + \alpha_1\alpha_3)(x_0 + \alpha_1\alpha_2).$$

Theorem 4.5.2 (again with  $f_1(x) = f(x)$  and  $f_2(x) = x$ ) gives the following formula for the parity of the  $2^\infty$ -Selmer rank of  $E \times \text{Jac}_{E'}$ .

**Theorem 6.1.3.** *Let  $K$  be a number field and  $E : y^2 = f(x)$ ,  $E' : w^2 = xf(x)$  for  $f(x) \in K[x]$  a separable cubic with  $f(0) \neq 0$ . Then,*

$$\text{rk}_2(E) + \text{rk}_2(\text{Jac}_{E'}) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f, x) \pmod{2}$$

where  $\lambda_v(f, x)$  is as in Definition 4.3.2. Namely, for  $\mathcal{K}$  a local field and  $f(x) \in \mathcal{K}[x]$  a separable monic cubic such that  $f(0) \neq 0$ ,

$$\lambda_{\mathcal{K}}(f, x) = \begin{cases} 2^4 & \mathcal{K} \simeq \mathbb{C}, \\ \# \ker \phi|_{(E \times \text{Jac}_{E'}) (\mathcal{K})^\circ} \frac{n_{E \times \text{Jac}_{E'}}}{n_{\text{Jac}_X \mu(X)}} & \mathcal{K} \simeq \mathbb{R}, \\ \frac{c(E)c(\text{Jac}_{E'})}{c(\text{Jac}_X)\mu(X)} & \mathcal{K}/\mathbb{Q}_p \text{ finite, } p \neq 2, \\ \frac{c(E)c(\text{Jac}_{E'})}{c(\text{Jac}_X)\mu(X)} \Big|_{\frac{\phi^* \omega_{\text{Jac}_X}^0}{\omega_{E \times \text{Jac}_{E'}}^0}} \Big|_{\mathcal{K}} & \mathcal{K}/\mathbb{Q}_2 \text{ finite.} \end{cases}$$

**Remark 6.1.4.** Noting that  $\text{rk}_2(E) + \text{rk}_2(\text{Jac}_{E'}) = \text{rk}_2(\text{Jac}_X)$  ( $E \times \text{Jac}_{E'}$  and  $\text{Jac}_X$  are isogenous), this theorem also provides a local formula for the parity of the  $2^\infty$ -Selmer rank of (Jacobians of) genus 2 curves of the form  $y^2 = f(x^2)$ .

With this in mind, we compare  $(-1)^{\text{ord}_2 \lambda_v(f,x)}$  place-by-place to the product of root numbers  $w_v(E)w_v(\text{Jac}_{E'})$  appearing in the analogous statement of the 2-parity conjecture. As in the previous chapter (c.f. Theorem 5.1.2), it turns out that these terms are not always equal and we are able to show that they must differ at exactly an even number of places.

**Definition 6.1.5.** Let  $\mathcal{K}$  be a local field of characteristic 0 and let  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{K}[x]$  be such that  $c \neq 0$ . Write  $\Delta_f := 18abc - 4a^3c + a^2b^2 - 4b^3 - 27c^2 \neq 0$  for the discriminant of  $f$ ,  $L := ab - 9c$  and define  $H_{\mathcal{K}}(f)$  to be the following product of Hilbert symbols

$$H_{\mathcal{K}}(f) = \begin{cases} (b, -c)_{\mathcal{K}} \cdot (-2L, \Delta_f)_{\mathcal{K}} \cdot (L, -b)_{\mathcal{K}} & b, L \neq 0, \\ (-c, -1)_{\mathcal{K}} \cdot (2c, \Delta_f)_{\mathcal{K}} & \text{otherwise.} \end{cases}$$

**Remark 6.1.6.** As  $b$  or  $L$  approach 0, both expressions for  $H_{\mathcal{K}}(f)$  agree. This can be seen in the proof of Lemma 6.2.7.

**Remark 6.1.7.** The invariant  $L$  can be written in terms of the roots of  $f$  as

$$L = 8\alpha_1\alpha_2\alpha_3 - (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_3).$$

**Theorem 6.1.8** (Local Theorem II). *Let  $\mathcal{K}$  be a local field of characteristic 0 and and  $E : y^2 = f(x)$ ,  $E' : w^2 = xf(x)$  for  $f(x) \in \mathcal{K}[x]$  a separable monic cubic with  $f(0) \neq 0$ . Then*

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)} H_{\mathcal{K}}(f) = w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_{E'})$$

where  $\lambda_{\mathcal{K}}(f, x)$  is as in Definition 4.3.2 and  $H_{\mathcal{K}}(f)$  is as in Definition 6.1.5.

The key, global, consequences of this Theorem are discussed in §6.3 and §6.4.

## 6.2 Proof of Local Theorem II

### 6.2.1 Proof over Archimedean fields

We begin by proving that Theorem 6.1.8 holds when  $\mathcal{K}$  is an Archimedean local field, the cases in which we can best visualise  $\lambda_{\mathcal{K}}(f, x)$ .

**Proposition 6.2.1.** *Theorem 6.1.8 holds when  $\mathcal{K} \cong \mathbb{C}$ .*

*Proof.* Clearly  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f, x)} = H_{\mathcal{K}}(f) = +1$  and since  $E$  and  $\text{Jac}_{E'}$  are elliptic curves,  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_{E'}) = -1$  (see Lemma 2.3.4).  $\square$

**Proposition 6.2.2.** *Theorem 6.1.8 holds when  $\mathcal{K} \cong \mathbb{R}$ .*

*Proof.* As in the proof of 6.2.1,  $w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_{E'}) = +1$ . Therefore, we need only verify that  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f, x)} = H_{\mathcal{K}}(f)$ . Table 6.1 gives the values of  $n_E$ ,  $n_{\text{Jac}_{E'}}$ ,  $n_{\text{Jac}_X}$ ,  $\#\ker \phi|_{(E \times \text{Jac}_{E'})_{(\mathcal{K})^\circ}}$ ,  $\mu(X)$ ,  $\lambda_{\mathcal{K}}(f, x)$  and  $H_{\mathcal{K}}(f)$  for each possible arrangement of the real roots of  $xf(x)$ . In particular, column 2 lists the real roots of  $xf(x)$  from smallest to largest where the roots of  $f$  are denoted by red circles ( $\bullet$ ) and the root 0 (of  $x$ ) is denoted by a blue diamond ( $\blacklozenge$ ).

Case	Real roots	$n_E$	$n_{\text{Jac}_{E'}}$	$n_{\text{Jac}_X}$	$\#\ker \phi _{(E \times \text{Jac}_{E'})_{(\mathcal{K})^\circ}}$	$\mu(X)$	$\lambda_{\mathcal{K}}(f, x)$	$H_{\mathcal{K}}(f)$
1	$\blacklozenge \bullet \bullet \bullet$	2	2	4	2	1	2	-1
2	$\bullet \blacklozenge \bullet \bullet$	2	2	2	1	1	2	-1
3	$\bullet \bullet \blacklozenge \bullet$	2	2	1	1	1	4	+1
4	$\bullet \bullet \bullet \blacklozenge$	2	2	1	1	1	4	+1
5	$\blacklozenge \bullet$	1	1	1	2	1	2	-1
6	$\bullet \blacklozenge$	1	1	1	2	1	2	-1

**Table 6.1:** Data for Proposition 6.2.2

The contents of columns 3, 4 and 5 are determined using Lemma 2.1.8 and from observing that  $n_E = n_{E'} = 2$  when  $f$  has 3 real roots and 1 otherwise, and that  $n_X = 3$  when  $f$  has 3 positive real roots, 2 when  $f$  has 2 positive real roots and 1 otherwise.

For column 6 we use the description of  $\ker \phi$  as given in Lemma 3.3.7, to deduce that

$$\ker \phi = \left\{ O, \left( (\alpha_i, 0), \left( -\frac{\alpha_1 \alpha_2 \alpha_3}{\alpha_i}, 0 \right) \right) \text{ for } i = 1, 2, 3 \right\}$$



(for example,  $T = \emptyset \subseteq \mathcal{R}_x$ ,  $S = \{\alpha_1, \alpha_2\} \subseteq \mathcal{R}_f$  gives  $(D_S, D_S)$  where  $\text{Jac}_E \ni D_S = (\alpha_1, 0) + (\alpha_2, 0) - 2\infty = (\alpha_3, 0) - \infty$  and  $\text{Jac}_{E'} \ni D_S = (\alpha_1, 0) + (\alpha_2, 0) - \infty - \iota(\infty) = (\alpha_3, 0) + (0, 0) - \infty - \iota(\infty) \mapsto (-\alpha_1\alpha_2, 0) - \infty_{\text{Jac}_{E'}}$  by Remark 6.1.2).

We count how many elements lie on the identity component of  $(E \times \text{Jac}_{E'}) (\mathcal{K})$  (i.e. each entry of the pair of points lies on the identity component of the corresponding curve). Clearly the point  $O$  on  $E \times \text{Jac}_{E'}$  always satisfies this condition. Let  $\alpha_3$  be the largest real root of  $f$ , so that  $(\alpha_3, 0) \in E(\mathcal{K})^\circ$  and  $(\alpha_1, 0), (\alpha_2, 0) \notin E(\mathcal{K})^\circ$ . Now  $\#\ker \phi|_{(E \times \text{Jac}_{E'}) (\mathcal{K})^\circ}$  is 2 precisely when  $(-\alpha_1\alpha_2, 0) \in \text{Jac}_{E'}(\mathcal{K})^\circ$ , i.e. when  $-\alpha_1\alpha_2$  is the largest real element of  $T = \{-\alpha_1\alpha_2, -\alpha_2\alpha_3, -\alpha_1\alpha_3\}$ , and 1 otherwise. In cases (1) to (4),  $T \subseteq \mathbb{R}$  and it can be observed that  $-\alpha_1\alpha_2$  is the largest precisely when  $\alpha_1, \alpha_2 > 0$ . In cases (5) and (6),  $\alpha_1 = \bar{\alpha}_2$  and so  $-\alpha_1\alpha_2$  is the only real element of  $T$ , in particular it is the largest real element.

Column 7 keeps track of the deficiency contribution from  $X$ , which is 1 since  $X(\mathbb{R})$  is always non-empty.

Column 8 gives the value of  $\lambda_{\mathcal{K}}(f, x)$ .

We now justify the value of  $H_{\mathcal{K}}(f)$ , as given in column 9, via a case-by-case analysis of the signs of the Hilbert symbol entries.

First observe that when  $b, L \neq 0$ ,  $(L, -b) = (L, -ac) \cdot (ab, -c)$  since  $(L, abc) = (ab, -c)$  by Lemma 2.7.5(i). Therefore,

$$H_{\mathcal{K}}(f) = (-2L, \Delta_f) \cdot (L, -ac) \cdot (a, -c).$$

Since the sign of  $a$  is easier to control than that of  $b$ , we will use this equivalent expression whenever  $b, L \neq 0$ .

(1) and (4).  $\Delta_f, b, ac > 0$ . Applying the AM-GM inequality gives that for  $i \neq j$ ,  $\alpha_i + \alpha_j > 2\sqrt{\alpha_i\alpha_j}$  in case (1) and  $\alpha_i + \alpha_j > -2\sqrt{\alpha_i\alpha_j}$  in case (4). In particular, in case (1) we have  $L < 0$  and  $H_{\mathcal{K}}(f) = -1$  and in case (4) we have  $L > 0$  and  $H_{\mathcal{K}}(f) = +1$ .

(2).  $\Delta_f, c > 0$ . If  $b, L \neq 0$  then  $H_{\mathcal{K}}(f) = (L, -a) \cdot (a, -1)$  which is  $-1$  unless  $a, L > 0$ . Suppose  $\alpha_1 < 0$ . If  $a > 0$  then  $\alpha_1 + \alpha_2, \alpha_1 + \alpha_3 < 0$ ,  $\alpha_2 + \alpha_3 > 0$  and so  $L < 0$  by Remark 6.1.7. If  $bL = 0$  then clearly  $H_{\mathcal{K}}(f)$  again evaluates to  $-1$ .

(3).  $\Delta_f > 0, c < 0$ . If  $b, L \neq 0$  then  $H_{\mathcal{K}}(f) = (L, a)$  which is  $+1$  unless  $a, L < 0$ . Suppose  $\alpha_1, \alpha_2 < 0$ . If  $a < 0$  then  $\alpha_1 + \alpha_3, \alpha_2 + \alpha_3 > 0, \alpha_1 + \alpha_2 < 0$  and so  $L > 0$  by Remark 6.1.7. If  $bL = 0$  then clearly  $H_{\mathcal{K}}(f)$  again evaluates to  $+1$ .

(5).  $\Delta_f, c < 0$ . If  $b, L \neq 0$  then  $H_{\mathcal{K}}(f) = -(L, -a)$  which is  $-1$  unless  $a > 0, L < 0$ . Suppose  $\alpha_2 = \bar{\alpha}_1$ . If  $a > 0$  then  $\alpha_1 + \alpha_2 < 0$  and so  $L > 0$  by Remark 6.1.7. If  $bL = 0$  then clearly  $H_{\mathcal{K}}(f)$  again evaluates to  $-1$ .

(6).  $\Delta_f < 0, c > 0$ . If  $b, L \neq 0$  then  $H_{\mathcal{K}}(f) = -(-L, a)$  which is  $-1$  unless  $a < 0, L > 0$ . Suppose  $\alpha_2 = \bar{\alpha}_1$ . If  $a < 0$  then  $\alpha_1 + \alpha_2 > 0$  and so  $L < 0$  by Remark 6.1.7. If  $bL = 0$  then clearly  $H_{\mathcal{K}}(f)$  again evaluates to  $-1$ .  $\square$

## 6.2.2 Proof over non-Archimedean fields for nice reduction types

We now focus on proving that Theorem 6.1.8 holds when  $\mathcal{K}/\mathbb{Q}_p$  is a finite extension,  $p \neq 2$ , and the reduction of  $xf(x)$  has at worst one double root.

**Lemma 6.2.3.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension. It is sufficient to prove Theorem 6.1.8 when  $f(x) \in \mathcal{O}_{\mathcal{K}}[x]$ .*

*Proof.* Let  $f_0(x) = x^3 + ax^2 + bx + c \in \mathcal{K}[x]$  and choose  $u \in \mathcal{K}^\times$  such that  $u^2a, u^4b, u^6c \in \mathcal{O}_{\mathcal{K}}$ . Define  $f(x) = x^3 + u^2ax^2 + u^4bx + u^6c \in \mathcal{O}_{\mathcal{K}}[x]$ . Since  $y^2 = f_0(x) \cong y^2 = f(x), w^2 = xf_0(x) \cong w^2 = xf(x)$  and  $H_{\mathcal{K}}(f_0) = H_{\mathcal{K}}(f)$  (the Hilbert symbol entries have been scaled by squares), Theorem 6.1.8 holds for  $f_0(x)$  if and only if it holds for  $f(x)$ .  $\square$

**Proposition 6.2.4.** *Theorem 6.1.8 holds when  $\mathcal{K}/\mathbb{Q}_p$  is a finite extension,  $p \neq 2$ , and both  $E, E'$  are semistable with  $\Sigma_{E'} = \textcircled{\bullet\bullet\bullet\bullet}_0$  or  $\textcircled{\bullet\bullet\bullet}_0$ .*

*Proof.* By Lemma 6.2.3, we may assume that  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{O}_{\mathcal{K}}[x]$ .

The inputs of Table 6.2 (columns 2 and 3) are the cluster pictures of  $E$  and  $E'$ , where the roots of  $f$  are denoted by red circles ( $\bullet$ ) and the root 0 (of  $x$ ) is denoted by a blue diamond ( $\blacklozenge$ ). Column 1 indexes the various cases using the reduction types of  $X/\mathcal{K}$  as defined in [22, Table 1.1].

Type	$\Sigma_E$	$\Sigma_{E'}$	$\Sigma_{\text{Jac}_{E'}}$	$\Upsilon_X$	$c(E)$	$c(\text{Jac}_{E'})$	$c(\text{Jac}_X)$	$\mu(X)$	$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)}$	$w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_{E'})$	$H_{\mathcal{K}}(f)$
2					1	1	1	1	+1	+1	+1
$1_n^+$					1	2n	n	1	-1	-1	+1
$1_n^-$					1	2	$\tilde{n}$	1	$(-1)^n$	+1	$(-1)^n$
$I_{n,n}^{+,+}$					n	n	$n^2$	1	+1	+1	+1
$I_{n \sim n}^+(a)$					n	$\tilde{n}$	n	1	$(-1)^{n+1}$	-1	$(-1)^n$
$I_{n \sim n}^+(b)$					$\tilde{n}$	n	n	1	$(-1)^{n+1}$	-1	$(-1)^n$
$I_{n,n}^{-,-}$					$\tilde{n}$	$\tilde{n}$	$\tilde{n}^2$	1	+1	+1	+1

Notation:  $\tilde{n} = \text{gcd}(2, n)$ .

**Table 6.2:** Data for Proposition 6.2.4

Column 4 gives the cluster picture for  $\text{Jac}_{E'}$ , which is easily determined from that of  $E'$  via Remark 6.1.2.

Column 5 gives the dual graph of the minimal regular model of  $X/\mathcal{K}$ , denoted  $\Upsilon_X$ , where an arrow is used to indicate the action of Frobenius. This is determined using Theorem 2.4.14 (with  $f_1(x) = f(x)$ ,  $f_2(x) = x$  so that  $B = X$ ).

Columns 6 and 7 list the Tamagawa numbers for  $E$  and  $\text{Jac}_{E'}$ , calculated from their respective cluster pictures using [60, Table 15.1].

Similarly, column 8 contains the Tamagawa number for  $\text{Jac}_X$  but calculated from  $\Upsilon_X$  using Theorem 2.3.3.

Column 9 keeps track of the deficiency contribution from  $X/\mathcal{K}$ , using Theorem 2.4.11.

Column 10 gives the value of  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)}$ .

Column 11 gives  $w_{\mathcal{K}}(E)w_{\mathcal{K}}(\text{Jac}_{E'})$  using Theorem 2.3.6.

It remains to compute the value of  $H_{\mathcal{K}}(f)$  via a case-by-case analysis of the valuations of  $b$ ,  $c$ ,  $L$ ,  $\Delta_f$ . Recall that  $\alpha_1, \alpha_2, \alpha_3$  denote the roots of  $f$ . Below, all equivalences are taken modulo  $\pi$ , where  $\pi$  is a uniformiser of  $\mathcal{K}$ . We write  $v$  for a normalised valuation on  $\overline{\mathcal{K}}$ , i.e.  $v(\pi) = 1$ .

**Type 2.** We must show that  $H_{\mathcal{K}}(f) = +1$ . We have that  $v(c) = v(\Delta_f) = 0$ .

Suppose  $b, L \neq 0$ . Then  $H_{\mathcal{K}}(f) = (b, -c)(L, -b\Delta_f)$ . If  $v(b) = v(L) = 0$ , we are done. Suppose that  $\mathcal{K}/\mathbb{Q}_p$  and  $p \neq 3$ . If  $b \equiv 0$  then  $L \equiv -9c$ , and so  $H_{\mathcal{K}}(f) = +1$ . If  $L \equiv 0$  then  $v(a) = v(b) = 0$  and  $-b\Delta_f \equiv \frac{4}{b^2}(b^3 - 27c^2)^2$ , and so again  $H_{\mathcal{K}}(f) = +1$ .

Now suppose that  $\mathcal{K}/\mathbb{Q}_3$  and  $L \equiv 0$ . Write  $b = \pi^{v(b)}u_1$ ,  $3 = \pi^{v(3)}u_2$  for units  $u_1, u_2$  and assume that  $v(b) > 0$  (if  $v(b) = 0$  then we again observe that  $-b\Delta_f$  is a square). Note that  $\Delta_f \equiv -a^3c$ , so  $v(a) = 0$ .

- If  $v(b) < 2v(3)$ , then  $L = \pi^{v(b)}(au_1 - \pi^{2v(3)-v(b)}cu_2^2)$  where  $au_1 - \pi^{2v(3)-v(b)}cu_2^2 \equiv au_1$ . So  $H_{\mathcal{K}}(f) = +1$  having used the standard identity  $(\pi, -\pi) = 1$ .
- If  $v(b) = 2v(3)$ , then  $L = \pi^{v(b)}(au_1 - cu_2^2)$  and  $H_{\mathcal{K}}(f) = (au_1 - cu_2^2, -u_1\Delta_f)$ , having used that  $v(b)$  is even. If  $v(au_1 - cu_2^2) = 0$  then we are done, else  $-u_1\Delta_f \equiv u_2^2a^2c^2$  and so  $H_{\mathcal{K}}(f) = +1$ .

- If  $v(b) > 2v(3)$ , then  $L = \pi^{2v(3)}(\pi^{v(b)-2v(3)}au_1 - cu_2^2)$  where  $\pi^{v(b)-2v(3)}au_1 - cu_2^2 \equiv -cu_2^2$  and so  $H_{\mathcal{K}}(f) = +1$ .

Suppose  $bL = 0$ . Clearly  $H_{\mathcal{K}}(f) = +1$ .

**Types  $1_n^+$  or  $1_n^-$ .** Suppose that  $\alpha_1 \equiv 0$  with  $v(\alpha_1) = n$ . Since  $\theta_{t,E'} = \sqrt{\frac{1}{4}(\alpha_1 - 2\alpha_2)(\alpha_1 - 2\alpha_3)}$ , it can be observed that we are in type  $1_n^+$  when  $\alpha_2\alpha_3 \in (\mathcal{K}^\times)^2$  (when  $\theta_{t,E'} \in \mathcal{K}^\times$ ), and type  $1_n^-$  otherwise. It is required to show that  $H_{\mathcal{K}}(f) = -1$  precisely when  $n$  is odd and  $\alpha_2\alpha_3 \notin (\mathcal{K}^\times)^2$ , i.e. that  $H_{\mathcal{K}}(f) = (\pi^n, \alpha_2\alpha_3)$ . We have that  $v(b) = v(\Delta_f) = 0$  and  $v(c) = n$ .

Suppose  $L \neq 0$ . Then  $H_{\mathcal{K}}(f) = (b, \pi^n)(L, -b\Delta_f)$  and since  $b \equiv \alpha_2\alpha_3$  it remains to show that  $(L, -b\Delta_f) = +1$ . If  $v(L) = 0$  we are done. If not, then  $L \equiv -\alpha_2\alpha_2(\alpha_2 + \alpha_3)$  and so  $\alpha_2 \equiv -\alpha_3$  and  $-b\Delta_f \equiv 4\alpha_3^8$ .

Suppose  $L = 0$ . Then  $H_{\mathcal{K}}(f) = (\pi^n, -\Delta_f)$  where  $\Delta_f = -\frac{4}{b^3}(b^3 - 27c^2)^2$  and  $b \equiv \alpha_2\alpha_3$ .

**Types  $I_{n,n}^{+,+}$ ,  $I_{n\sim n}^+(a)$ ,  $I_{n\sim n}^+(b)$ , or  $I_{n,n}^{-,-}$ .** Suppose that  $v(\alpha_1) = 0$  and  $\alpha_2 \equiv \alpha_3$  with  $v(\alpha_2 - \alpha_3) = \frac{n}{2}$ . Since  $\theta_{t,E} = \sqrt{\frac{1}{2}(\alpha_2 + \alpha_3) - \alpha_1}$  and  $\theta_{t,E'} = \sqrt{\frac{1}{2}(\alpha_2 + \alpha_3)(\frac{1}{2}(\alpha_2 + \alpha_3) - \alpha_1)}$ , it can be observed that we are in type  $I_{n,n}^{+,+}$  or  $I_{n,n}^{-,-}$  when  $\frac{1}{2}(\alpha_2 + \alpha_3) \in (\mathcal{K}^\times)^2$  (when  $\theta_{t,E}, \theta_{t,E'} \in \mathcal{K}^\times$ , or  $\theta_{t,E}, \theta_{t,E'} \notin \mathcal{K}^\times$ ), and type  $I_{n,n}^{+,-}$  or  $I_{n,n}^{-,+}$  otherwise. It is required to show that  $H_{\mathcal{K}}(f) = -1$  precisely when  $n$  is odd and  $\frac{1}{2}(\alpha_2 + \alpha_3) \notin (\mathcal{K}^\times)^2$ , i.e. that  $H_{\mathcal{K}}(f) = (\pi^n, \frac{1}{2}(\alpha_2 + \alpha_3))$ . We have that  $v(c) = v(L) = 0$  and  $v(\Delta_f) = n$ .

Suppose  $b \neq 0$ . Then  $H_{\mathcal{K}}(f) = (b, -cL)(-2L, \pi^n)$  and as  $L \equiv -(\alpha_2 + \alpha_3)(\alpha_1 - \frac{1}{2}(\alpha_2 + \alpha_3))^2$  it remains to show that  $(b, -cL) = +1$ . If  $v(b) = 0$  we are done. If not, since  $b \equiv \frac{1}{2}(\alpha_2 + \alpha_3)(2\alpha_1 + \frac{1}{2}(\alpha_2 + \alpha_3))$  we have that  $\alpha_1 \equiv -\frac{1}{4}(\alpha_2 + \alpha_3)$  and  $-cL \equiv \frac{9}{256}(\alpha_2 + \alpha_3)^6$ .

Suppose  $b = 0$ . Then  $H_{\mathcal{K}}(f) = (2c, \pi^n)$  where  $2c = 2\alpha_1^2(\alpha_2 + \alpha_3)$ . □

### 6.2.3 Proof in the remaining cases

Here we prove that Theorem 6.1.8 holds in all remaining cases using a global–local argument. Namely, when  $\mathcal{K}/\mathbb{Q}_p$  is finite and  $p = 2$ , or  $p$  is odd and the reduction of  $xf(x)$  has worse than one double root.

### Continuity of local invariants

**Lemma 6.2.5** ([20], Lemma 3.2). *Let  $\mathcal{K}$  be a local field of characteristic 0. The Hilbert symbol  $(A, B)$  is a continuous function of  $A, B \in \mathcal{K}^\times$ .*

**Lemma 6.2.6.** *Let  $\mathcal{K}$  be a local field of characteristic 0 and  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{K}[x]$  a separable cubic. Define  $E : y^2 = f(x)$ ,  $E' : w^2 = xf(x)$ . The invariants  $b$ ,  $c$ ,  $L := ab - 9c$ ,  $\Delta_f$  (the discriminant of  $f$ ),  $w_{\mathcal{K}}(E)$ ,  $w_{\mathcal{K}}(\text{Jac}_{E'})$  and  $\lambda_{\mathcal{K}}(f, x)$  (as in Definition 4.3.2) are continuous in the coefficients of  $f(x)$ .*

*Proof.* This can be seen from [24, Lemma 11.2]. □

**Lemma 6.2.7.** *Let  $\mathcal{K}$  be a local field of characteristic 0 and  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{O}_{\mathcal{K}}[x]$  be separable. There is an  $\epsilon > 0$  such that if  $\tilde{f}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c} \in \mathcal{O}_{\mathcal{K}}[x]$  is separable and  $|a - \tilde{a}|_{\mathcal{K}}, |b - \tilde{b}|_{\mathcal{K}}, |c - \tilde{c}|_{\mathcal{K}} < \epsilon$ , then Theorem 6.1.8 holds for  $f(x)$  if and only if it holds for  $\tilde{f}(x)$ .*

*Proof.* If  $b, L \neq 0$  then, ensuring that  $\tilde{b}, \tilde{L} \neq 0$ , this is clear from Lemmata 6.2.5 and 6.2.6. If  $b = \tilde{b} = 0$  or  $L = \tilde{L} = 0$  then, again, this is clear. When we are not in either of these cases, Lemma 6.2.6 still asserts that the root numbers are unchanged and that  $\lambda_{\mathcal{K}}(f, x) = \lambda_{\mathcal{K}}(\tilde{f}, x)$ , but showing that  $H_{\mathcal{K}}(f) = H_{\mathcal{K}}(\tilde{f})$  is more delicate.

Suppose that  $\mathcal{K}$  is non-Archimedean. Let  $\pi$  denote a fixed choice of uniformiser and  $v$  a normalised valuation. We write  $\square$  for a non-zero square element in  $\mathcal{K}$ .

Suppose that  $b = 0$  and  $\tilde{b} \neq 0$ . Let  $N = v(c) + v(36) + 1$  and pick  $a \equiv \tilde{a}$ ,  $b \equiv \tilde{b}$ ,  $c \equiv \tilde{c} \pmod{\pi^N}$ . Then  $\tilde{L} = \tilde{a}\tilde{b} - 9\tilde{c} \equiv -9\tilde{c} \not\equiv 0 \pmod{\pi_{\mathcal{K}}^N}$  and so  $\tilde{L} = -\tilde{c} \cdot \square$ . Therefore  $H_{\mathcal{K}}(\tilde{f}) = (\tilde{b}, -\tilde{c})(2\tilde{c}, \Delta_{\tilde{f}})(-\tilde{c}, -\tilde{b}) = (2\tilde{c}, \Delta_{\tilde{f}})(-\tilde{c}, -1)$  which by Lemma 6.2.5 is equal to  $H_{\mathcal{K}}(f)$ .

Now suppose that  $L = 0$  and  $\tilde{L} \neq 0$ . Let  $N = v(b) + 2v(a^2 - 3b) + v(16) + 1$  and pick  $a \equiv \tilde{a}$ ,  $b \equiv \tilde{b}$ ,  $c \equiv \tilde{c} \pmod{\pi^N}$ . We have that  $\tilde{a}\tilde{b} \equiv 9\tilde{c} \pmod{\pi^N}$ , therefore  $9\Delta_{\tilde{f}} \equiv -4\tilde{b}(\tilde{a}^2 - 3\tilde{b})^2 \not\equiv 0 \pmod{\pi^N}$  and  $\Delta_{\tilde{f}} = -\tilde{b} \cdot \square$ . So,  $H_{\mathcal{K}}(\tilde{f}) = (\tilde{b}, -\tilde{c})(-2\tilde{L}, -\tilde{b})(\tilde{L}, -\tilde{b}) = (\tilde{b}, -\tilde{c})(-2, -\tilde{b})$  and by Lemma 6.2.5 this is equal to  $H_{\mathcal{K}}(f)$  since  $\Delta_f = -b \cdot \square$ .

The case when  $\mathcal{K}$  is Archimedean and  $bL = 0$  follows from Table 6.1 since  $f$  and  $\tilde{f}$  will have the same number of positive and negative real roots. □

**Reduction steps**

**Lemma 6.2.8.** *Let  $K$  be a number field and  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{O}_K[x]$  be a separable cubic such that  $a^2 - 3b, b, a^2 - 4b, ab - 9c, c \neq 0$ . Fix a prime  $\mathfrak{p} \nmid 2, 3$  and suppose that the following conditions are satisfied:*

$$(i) \quad \mathfrak{p} \mid a^2 - 3b \Rightarrow \mathfrak{p} \nmid ab - 9c,$$

$$(ii) \quad \mathfrak{p} \mid b(a^2 - 4b) \Rightarrow \mathfrak{p} \nmid c.$$

*Then  $xf(x)$  either has distinct roots, or no worse than 1 double root modulo  $\mathfrak{p}$ .*

*Proof.* We must prove that (i) and (ii) guarantee that  $xf(x)$  has at least 3 distinct roots mod  $\mathfrak{p}$ .

Suppose that three roots of  $xf(x)$  are congruent mod  $\mathfrak{p}$ . This happens when either (1) all three roots of  $f(x)$  are congruent, or (2) two roots of  $f(x)$  are congruent to 0. Situation (1) occurs if  $f(x), f'(x) = 3x^2 + 2ax + b, f''(x) = 6x + 2a$  share a root mod  $\mathfrak{p}$ , i.e. when  $f(-\frac{a}{3}) \equiv f'(-\frac{a}{3}) \equiv 0 \pmod{\mathfrak{p}}$ . Condition (i) ensures that this does not happen. We are in situation (2) whenever  $f(0) \equiv f'(0) \equiv 0 \pmod{\mathfrak{p}}$ . Condition (ii) ensures that this does not happen.

Now suppose that  $xf(x)$  has two double roots mod  $\mathfrak{p}$ , so that two roots of  $f(x)$  are (non-zero and) congruent mod  $\mathfrak{p}$  with the remaining root congruent to zero. Here  $f(0) \equiv 0$  and  $\Delta_f \equiv 0$ . By definition of  $\Delta_f$ , these happen simultaneously when  $c \equiv 0$  and  $a^2b^2 - 4b^3 \equiv 0$ , so again condition (ii) ensures that this does not happen.  $\square$

**Remark 6.2.9.** Using cluster pictures, Lemma 6.2.8 says that  $\Sigma_{E'/K_{\mathfrak{p}}}$  is either  $\textcircled{\bullet\bullet\bullet}_0$  or  $\textcircled{\bullet\bullet}_0$ . In particular, Proposition 6.2.4 holds for such a choice of  $f(x)$ .

**Lemma 6.2.10.** *Let  $\mathcal{K}/\mathbb{Q}_3$  be a finite extension and let  $f(x) = x^3 + x + 1 \in \mathcal{K}[x]$  then Theorem 6.1.8 holds.*

*Proof.*  $E$  and  $\text{Jac}_{E'}$  have good reduction over  $\mathcal{K}$  so  $w_{\mathcal{K}}(E) = w_{\mathcal{K}}(\text{Jac}_{E'}) = 1$  and  $\lambda_{\mathcal{K}}(f, x) = 1$ . Additionally,  $H_{\mathcal{K}}(f) = (1, -1)(18, -31)(-9, -1) = +1$ .  $\square$

As in the proof of Proposition 5.2.8, we deduce the remaining cases of Theorem 6.1.8 from known instances of the 2-parity conjecture.

**Proposition 6.2.11.** *Theorem 6.1.8 holds when*

1.  $\mathcal{K}/\mathbb{Q}_2$  is finite,
2.  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p$  odd.

*Proof.* (1). Let  $\mathcal{K}/\mathbb{Q}_2$  be a finite extension. Pick a totally real number field  $F$  with a unique prime  $\mathfrak{p} \mid 2$  so that  $F_{\mathfrak{p}} \cong \mathcal{K}$ . Fix another prime  $\mathfrak{p} \neq \mathfrak{p}' \nmid 2, 3$ . By Lemma 6.2.3, we may assume that  $f(x) = x^3 + ax^2 + bx + c \in \mathcal{O}_{\mathcal{K}}[x]$ . We will approximate  $f(x)$  by  $\tilde{f}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c} \in \mathcal{O}_F[x]$  (with non-zero discriminant) subject to the following:

- (i) pick  $\tilde{a}$  to be  $\mathfrak{p}$ -adically close to  $a$ ,  $\mathfrak{p}'$ -adically close to  $-1$  and  $\mathfrak{q}$ -adically close to  $0$  for all  $\mathfrak{q} \mid 3$ ,
- (ii) pick  $\tilde{b} \neq 0, \frac{1}{4}\tilde{a}^2, \frac{1}{3}\tilde{a}^2$  so that  $\tilde{b}$  is  $\mathfrak{p}$ -adically close to  $b$ ,  $\mathfrak{p}'$ -adically close to  $-1$  and  $\mathfrak{q}$ -adically close to  $1$  for all  $\mathfrak{q} \mid 3$ ,
- (iii) pick  $\tilde{c} \neq 0, \frac{1}{9}\tilde{a}\tilde{b}$  so that  $\tilde{c}$  is  $\mathfrak{p}$ -adically close to  $c$ ,  $\mathfrak{p}'$ -adically close to  $1$ ,  $\mathfrak{q}$ -adically close to  $1$  for all  $\mathfrak{q} \mid 3$ , and such that if  $\mathfrak{q} \nmid 2, 3, \mathfrak{p}'$  then conditions (1) and (2) of Lemma 6.2.8 are satisfied (namely:  $9\tilde{c} \not\equiv \tilde{a}\tilde{b} \pmod{\mathfrak{q}}$  for all  $\mathfrak{q} \mid \tilde{a}^2 - 3\tilde{b}$ , and  $\tilde{c} \not\equiv 0 \pmod{\mathfrak{q}}$  for all  $\mathfrak{q} \mid \tilde{b}(\tilde{a}^2 - 4\tilde{b})$ ).

Let  $\tilde{E} : y^2 = \tilde{f}(x)$  and  $\tilde{E}' : w^2 = x\tilde{f}(x)$ . By construction,  $\tilde{f}(x)$  is  $\mathfrak{p}$ -adically close to  $f(x)$ ,  $\mathfrak{p}'$ -adically close to  $x^3 - x^2 - x + 1$ ,  $\mathfrak{q}$ -adically close to  $x^3 + x + 1$  when  $\mathfrak{q} \mid 3$ , and  $\mathfrak{q}$ -adically close to a monic cubic for which Proposition 6.2.4 holds when  $\mathfrak{q} \nmid 2, 3, \mathfrak{p}'$ . Invoking Lemma 6.2.7, this means that Theorem 6.1.8 holds for  $\tilde{f} \in F_v[x]$  whenever  $v \neq \mathfrak{p}$ , and proving it for  $\tilde{f} \in F_{\mathfrak{p}}[x]$  is equivalent to proving it for  $f \in \mathcal{K}[x]$ .

Noting that  $\tilde{E}$  and  $\text{Jac}_{\tilde{E}'}$  have multiplicative reduction over  $F_{\mathfrak{p}'}$  enforces that  $\text{ord}_{\mathfrak{p}'} j(\tilde{E}), \text{ord}_{\mathfrak{p}'} j(\text{Jac}_{\tilde{E}'}) < 0$ . In particular, the 2-parity conjecture holds for  $\tilde{E}$  and  $\text{Jac}_{\tilde{E}'}$  (it is known to hold for elliptic curves over totally real number fields with



non-integral  $j$ -invariant by [20, Theorem 2.4]). Therefore,

$$\begin{aligned}
 1 &= (-1)^{\mathrm{rk}_2(\tilde{E}/F) + \mathrm{rk}_2(\mathrm{Jac}_{\tilde{E}'}/F)} w(\tilde{E}/F) w(\mathrm{Jac}_{\tilde{E}'}/F) \\
 &\stackrel{\text{Thm. 6.1.3}}{=} \prod_{v \text{ place of } F} (-1)^{\mathrm{ord}_2 \lambda_v(\tilde{f}, x)} w_v(\tilde{E}) w_v(\mathrm{Jac}_{\tilde{E}'}) \\
 &= (-1)^{\mathrm{ord}_2 \lambda_{\mathfrak{p}}(\tilde{f}, x)} w_{\mathfrak{p}}(\tilde{E}) w_{\mathfrak{p}}(\mathrm{Jac}_{\tilde{E}'}) \cdot \prod_{v \neq \mathfrak{p}} H_{F_v}(\tilde{f}) \\
 &= (-1)^{\mathrm{ord}_2 \lambda_{\mathfrak{p}}(\tilde{f}, x)} w_{\mathfrak{p}}(\tilde{E}) w_{\mathfrak{p}}(\mathrm{Jac}_{\tilde{E}'}) \cdot H_{F_{\mathfrak{p}}}(\tilde{f})
 \end{aligned}$$

where the last equality follows from the product law for Hilbert symbols. In conclusion, we now know that Theorem 6.1.8 holds for  $\tilde{f}(x) \in F_{\mathfrak{p}}[x]$  and so it must also hold for  $f(x) \in F_{\mathfrak{p}}[x]$  where  $F_{\mathfrak{p}} \cong \mathcal{K}$ .

(2). Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension and  $p$  odd. We repeat the above argument, replacing 2 by  $p$  (when  $p = 3$  we also replace the condition “ $\mathfrak{q} \mid 3$ ” by “ $\mathfrak{q} \mid 3$  and  $\mathfrak{q} \neq \mathfrak{p}$ ”).  $\square$

*Proof of Theorem 6.1.8.* This is Proposition 6.2.1 when  $\mathcal{K} \cong \mathbb{C}$ , Proposition 6.2.2 when  $\mathcal{K} \cong \mathbb{R}$  and Proposition 6.2.11 when  $\mathcal{K}/\mathbb{Q}_p$  is finite.  $\square$

### 6.3 The 2-parity conjecture for elliptic curves with isomorphic 2-torsion

We now present the 2-parity results which we deduce from Theorem 6.1.8.

**Theorem 6.3.1.** *Let  $K$  be a number field and  $E : y^2 = f(x)$ ,  $E' : w^2 = xf(x)$  for  $f(x) \in K[x]$  a separable monic cubic with  $f(0) \neq 0$ . The 2-parity conjecture holds for  $E$  if and only if it holds for  $\mathrm{Jac}_{E'}$ .*

*Proof.* By Theorem 6.1.8,  $(-1)^{\mathrm{ord}_2 \lambda_v(f, x)} H_v(f) = w_v(E) w_v(\mathrm{Jac}_{E'})$  at each place  $v$  of  $K$ . Taking the product over all such  $v$  and then invoking Theorem 6.1.3 and the product formula for Hilbert symbols, gives that

$$(-1)^{\mathrm{rk}_2(E) + \mathrm{rk}_2(\mathrm{Jac}_{E'})} = w(E) w(\mathrm{Jac}_{E'}). \quad \square$$

**Theorem 6.3.2.** *Let  $K$  be a number field and  $X : y^2 = cf(x^2)$  for  $f(x) \in K[x]$  a separable monic cubic with  $f(0) \neq 0$  and  $c \in K^\times$ . The 2-parity conjecture holds for the Jacobian of the genus 2 curve  $X$ .*

*Proof.* Let  $E : y^2 = f(x)$ ,  $E' : y^2 = xf(x)$  and  $E_c : y^2 = cf(x)$ ,  $E'_c : w^2 = cx f(x)$ . By Theorem 3.3.2 (with  $f_1(x) = cf(x)$ ,  $f_2(x) = x$ ), there is an isogeny  $E_c \times \text{Jac}_{E'_c} \rightarrow \text{Jac}_X$ . Proving the 2-parity conjecture for  $\text{Jac}_X$  is therefore equivalent to proving it for  $E_c \times \text{Jac}_{E'_c}$ . We observe that the 2-parity conjecture for quadratic twists [20, Corollary 1.6] says that the 2-parity conjecture holds for  $E_c$  and  $\text{Jac}_{E'_c}$  if and only if it holds for  $E$  and  $\text{Jac}_{E'}$  respectively. This further reduces proving the 2-parity conjecture for  $\text{Jac}_X$  to proving it for  $E \times \text{Jac}_{E'}$ , which holds by Theorem 6.3.1.  $\square$

**Lemma 6.3.3.** *Let  $K$  be a number field and  $E_1, E_2$  be elliptic curves over  $K$ . If  $E_1[2] \cong E_2[2]$  as  $G_K$ -modules, then either  $E_2$  is a quadratic twist of  $E_1$  or there exists a separable monic cubic  $f(x) \in K[x]$  with  $f(0) \neq 0$  and some  $d \in K^\times$  such that*

$$E_1 : y^2 = f(x), \quad E_2 : dw^2 = xf(x).$$

*Proof.* Write  $E_1 : y^2 = g_1(x)$ ,  $E_2 : w^2 = g_2(x)$  for monic cubics  $g_1, g_2 \in K[x]$  and  $\Phi : E_1[2] \rightarrow E_2[2]$  for a  $G_K$ -module isomorphism. Let  $\alpha_1, \alpha_2, \alpha_3$  and  $\beta_1, \beta_2, \beta_3$  denote the roots of  $g_1(x)$  and  $g_2(x)$  respectively, labelled so that  $\Phi((\alpha_i, 0)) = (\beta_i, 0)$ . Define

$$A = \alpha_1\alpha_2(\beta_1 - \beta_2) + \alpha_3\alpha_1(\beta_3 - \beta_1) + \alpha_2\alpha_3(\beta_2 - \beta_3),$$

$$B = \alpha_1\alpha_2\beta_3(\beta_2 - \beta_1) + \alpha_3\alpha_1\beta_2(\beta_1 - \beta_3) + \alpha_2\alpha_3\beta_1(\beta_3 - \beta_2),$$

$$C = \beta_1(\alpha_2 - \alpha_3) + \beta_2(\alpha_3 - \alpha_1) + \beta_3(\alpha_1 - \alpha_2),$$

$$D = \beta_1\beta_2(\alpha_1 - \alpha_2) + \beta_2\beta_3(\alpha_2 - \alpha_3) + \beta_3\beta_1(\alpha_3 - \alpha_1),$$

then  $h(z) := \frac{Dz-B}{A-Cz}$  is the Möbius transformation mapping  $\alpha_i$  to  $\beta_i$ . Using that  $G_K$  permutes the roots of  $g_1$  and the roots of  $g_2$  in the same way, one can readily check that  $h(z)$  is defined over  $K$ . Observing that  $h(x) - h(\alpha_i) = \frac{AD-BC}{(A-Cx)(A-C\alpha_i)}(x - \alpha_i)$

gives

$$g_2(h(x)) = \frac{(AD - BC)^3}{(A - Cx)^3(A - C\alpha_1)(A - C\alpha_2)(A - C\alpha_3)}g_1(x).$$

Clearly,  $E_2 : w^2 = g_2(h(x))$  and hence also,

$$E_2 : w^2 = \begin{cases} \frac{A(A-C\alpha_1)(A-C\alpha_2)(A-C\alpha_3)}{AD-BC}(1 - \frac{C}{A}x)g_1(x) & A \neq 0, \\ -\frac{C\alpha_1\alpha_2\alpha_3}{B}xg_1(x) & A = 0. \end{cases}$$

If  $A, C \neq 0$ , we set  $x_0 = 1 - \frac{C}{A}x$  so that  $E_1 : y^2 = f(x_0)$  and  $E_2 : w^2 = dx_0f(x_0)$  where  $f(x_0) = g_1(\frac{A}{C}(1 - x_0))$  and  $d \in K^\times$ . If  $A \neq 0$  and  $C = 0$ , then  $E_2$  is just a quadratic twist of  $E_1$ . Finally, if  $A = 0$  then the result is clear.  $\square$

**Theorem 6.3.4.** *Let  $K$  be a number field and  $E_1, E_2$  be elliptic curves over  $K$ . If  $E_1[2] \cong E_2[2]$  as  $G_K$ -modules, then the 2-parity conjecture holds for  $E_1$  if and only if it holds for  $E_2$ .*

*Proof.* By Lemma 6.3.3, either  $E_2$  is a quadratic twist of  $E_1$  and this is just [20, Corollary 1.6], or  $E_1 : y^2 = f(x)$  and  $E_2 : dw^2 = xf(x)$  for some separable monic cubic  $f(x) \in K[x]$  with  $f(0) \neq 0$  and some  $d \in K^\times$ . Since  $E_2 \cong \text{Jac}_{dw^2=xf(x)}$ , the 2-parity conjecture holds for  $E_2$  if and only if it holds for  $\text{Jac}_{w^2=xf(x)}$  by [20, Corollary 1.6]. In turn, Theorem 6.3.1 says that the 2-parity conjecture holds for  $\text{Jac}_{w^2=xf(x)}$  if and only if it holds for  $E_1$ .  $\square$

## 6.4 The $p$ -parity conjecture for elliptic curves over totally real fields

We conclude this chapter by explaining how we are able to deduce the missing case of the  $p$ -parity conjecture for elliptic curves over totally real number fields from the 2-parity results presented in the previous section.

**Theorem 6.4.1.** *Let  $E$  be an elliptic curve with complex multiplication over a totally real number field  $K$ . The 2-parity conjecture holds for  $E$ .*

*Proof.* Write  $E : y^2 = f(x)$  where  $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ . For  $\gamma \in K$ , set

$f_\gamma(x) = f(x - \gamma)$  and define  $E(\gamma) = \text{Jac}_{y^2 = xf_\gamma(x)}$ . By Remark 6.1.2,

$$E(\gamma) : y^2 = (x + (\alpha_1 + \gamma)(\alpha_2 + \gamma))(x + (\alpha_1 + \gamma)(\alpha_3 + \gamma))(x + (\alpha_2 + \gamma)(\alpha_3 + \gamma))$$

from which it is clear that  $E[2] \cong E(\gamma)[2]$  as  $G_K$ -modules. Since  $j(E(\gamma))$  is a non-constant rational function in  $\gamma$ , there exists some  $\gamma_0 \in K$  such that  $j(E(\gamma_0)) \notin \mathcal{O}_K$  and so  $E(\gamma_0)$  does not have complex multiplication. In particular, the 2-parity conjecture holds for  $E(\gamma_0)$  by [20, Theorem 2.4]. Applying Theorem 6.3.4 gives that the 2-parity conjecture also holds for  $E$ .  $\square$

**Corollary 6.4.2.** *Let  $p \in \mathbb{Z}$  be a prime. The  $p$ -parity conjecture holds for all elliptic curves over totally real number fields.*

*Proof.* When  $p$  is odd, this is [51, Theorem E] and [49, Theorem A]. When  $p = 2$  and the elliptic curve does not have complex multiplication, this is [20, Theorem 2.4]. When  $p = 2$  and the elliptic curve has complex multiplication, this is Theorem 6.4.1.  $\square$

## Chapter 7

# A Conjecture Concerning Hyperelliptic Curves

In the previous chapter, we saw that a product of Hilbert symbols (=Definition 6.1.5) correctly describes the difference between local root numbers and the local invariants appearing in Theorem 4.5.2 when  $f_1(x)$  is a monic cubic and  $f_2(x) = x$  (=Theorem 6.1.8). The entires of these Hilbert symbols depend only on the coefficients of the cubic, resembling the construction of Dokchitser and Dokchitser ([17, Theorem 4]) which addresses the case when  $f_1(x)$  is a monic quadratic.

With this in mind, we now present a conjectural generalisation of these two results (=Definition 7.2.3 & Conjecture 7.2.5), i.e. when we allow  $f_1(x)$  to be a monic polynomial of arbitrary degree. (The next, and final, chapter aims to deal with the comparison in full generality, when  $f_1(x), f_2(x)$  are arbitrary coprime polynomials.) We again describe the local difference as a product of Hilbert symbols whose entries depend on the coefficients of  $f_1(x)$ ; specifically, they arise as coefficients of polynomials in the Sturm sequence for  $f_1(x)$ .

We provide a proof of this conjecture over Archimedean local fields (=Propositions 7.2.8 & 7.2.9) and in certain nice cases when the field is non-Archimedean and  $f_1(x)$  is a quartic (=Proposition 7.2.11). More generally, when the underlying field is non-Archimedean, the conjecture is supported by numerical evidence.

As before, we highlight the global consequences of this local statement. For instance, the 2-parity conjecture for Jacobians of hyperelliptic curves whose defining

polynomial is completely reducible (=Corollary 7.2.7).

The statements of some of the results of this chapter can also be found in [28].

## 7.1 Sturm polynomials

We recall the definition of the Sturm sequence for a real polynomial.

**Definition 7.1.1.** Let  $f(x) \in \mathbb{R}[x]$ . The *Sturm sequence* for  $f$  is a sequence of polynomials  $P_0, P_1, \dots$  defined via

$$P_0 = f(x), \quad P_1 = f'(x), \quad P_{i+1} \equiv -P_{i-1} \pmod{P_i} \text{ for } i \geq 1,$$

where either  $\deg P_{i+1} < \deg P_i$  or  $P_{i+1} = 0$ . The sequence terminates once one of the  $P_i$  is zero.

**Example 7.1.2.** The Sturm sequence for  $f(x) = x^2 + ax + b \in \mathbb{R}[x]$  is

$$P_0 = f(x), \quad P_1(x) = 2x + a, \quad P_2(x) = \frac{1}{4}(a^2 - 4b).$$

**Example 7.1.3.** The Sturm sequence for  $f(x) = x^3 + ax^2 + bx + c \in \mathbb{R}[x]$  is

$$P_0 = f(x), \quad P_1(x) = 3x^2 + 2ax + b, \quad P_2(x) = \frac{1}{9}((2a^2 - 6b)x + (ab - 9c)),$$

$$P_3(x) = \frac{9}{4(a^2 - 3b)^2}(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2),$$

(assuming  $P_2(x) \neq 0$ , else  $P_3(x)$  is not defined).

**Definition 7.1.4.** Let  $P_0, P_1, \dots$  be the Sturm sequence for  $f(x) \in \mathbb{R}[x]$ . Let  $x_0 \in \mathbb{R}$ . Write  $\kappa(x_0)$  for the number of sign changes (ignoring zeros) in the sequence of real numbers  $P_0(x_0), P_1(x_0), \dots$ .

**Theorem 7.1.5** (Sturm's theorem). *The number of roots of  $f(x) \in \mathbb{R}[x]$  in the interval  $(a, b] \subseteq \mathbb{R}$  is  $\kappa(a) - \kappa(b)$ .*

Since the Sturm sequence for  $f(x)$  provides us with a way to compute the number of roots it has in any half-open interval, we will see that it provides good can-

didates for expressions in the coefficients of  $f(x)$  which control the behaviour of the hyperelliptic curve  $y^2 = f(x)$  (over the reals).

## 7.2 Conjecture based on experimental data

We now generalise the set up presented in §6.1 in order to formulate an analogue of Theorem 6.1.8 which works in higher genus.

**Notation 7.2.1.** Let  $K$  be a field of characteristic 0 and  $f(x) \in K[x]$  be separable, monic and such that  $f(0) \neq 0$ . Define curves over  $K$  by

$$X_1 : y^2 = f(x), \quad X_0 : w^2 = xf(x), \quad X : y^2 = f(x^2)$$

and let  $\phi : \text{Jac}_{X_1} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_X$  denote the  $K$ -isogeny constructed in Theorem 3.3.2 (by letting  $f_1(x) = f(x)$  and  $f_2(x) = x$ ).

Theorem 4.5.2 (again with  $f_1(x) = f(x)$ ,  $f_2(x) = x$ ) gives the following formula for the parity of the  $2^\infty$ -Selmer rank of  $\text{Jac}_{X_1} \times \text{Jac}_{X_0}$  (or equivalently, of  $\text{Jac}_X$ ).

**Theorem 7.2.2.** *Let  $K$  be a number field and  $X_1 : y^2 = f(x)$ ,  $X_0 : w^2 = xf(x)$  for  $f(x) \in K[x]$  separable, monic and such that  $f(0) \neq 0$ . Then*

$$\text{rk}_2(\text{Jac}_{X_1}) + \text{rk}_2(\text{Jac}_{X_0}) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f, x) \pmod{2}$$

where  $\lambda_v(f, x)$  is as in Definition 4.3.2. Namely, for  $\mathcal{K}$  a local field and  $f(x) \in \mathcal{K}[x]$  separable, monic and such that  $f(0) \neq 0$ ,

$$\lambda_{\mathcal{K}}(f, x) = \begin{cases} 2^{\deg f + 1} & \mathcal{K} \simeq \mathbb{C}, \\ \# \ker \phi \Big|_{(\text{Jac}_{X_1} \times \text{Jac}_{X_0})(\mathcal{K})^\circ} \frac{n_{\text{Jac}_{X_1}} n_{\text{Jac}_{X_0}} \mu(X_1)}{n_{\text{Jac}_X} \mu(X)} & \mathcal{K} \simeq \mathbb{R}, \\ \frac{c(\text{Jac}_{X_1}) c(\text{Jac}_{X_0}) \mu(X_1)}{c(\text{Jac}_X) \mu(X)} & \mathcal{K}/\mathbb{Q}_p \text{ finite, } p \neq 2, \\ \frac{c(\text{Jac}_{X_1}) c(\text{Jac}_{X_0}) \mu(X_1)}{c(\text{Jac}_X) \mu(X)} \Big|_{\omega_{\text{Jac}_{X_1} \times \text{Jac}_{X_0}}^0} \frac{\phi^* \omega_{\text{Jac}_X}^0}{\omega_{\text{Jac}_{X_1} \times \text{Jac}_{X_0}}^0} \Big|_{\mathcal{K}} & \mathcal{K}/\mathbb{Q}_2 \text{ finite,} \end{cases}$$

where  $X : y^2 = f(x^2)$ .

As in the preceding chapters, we compare the terms  $(-1)^{\text{ord}_2 \lambda_v(f,x)}$  (in this arithmetic analogue of the 2-parity conjecture for  $\text{Jac}_{X_1} \times \text{Jac}_{X_0}$ ) to  $w_v(\text{Jac}_{X_1})w_v(\text{Jac}_{X_0})$ .

This comparison is carried out most easily over the reals, since computing  $\lambda_{\mathbb{R}}(f,x)$  boils down to counting the connected components of the hyperelliptic curves  $X_1, X_0$  and  $X$ , which can be determined from the number of real roots of  $f(x)$  and  $f(x^2)$ . Sturm's theorem allows us to count the latter, i.e. the number of real roots of  $f(x)$  greater than 0, and so the Sturm polynomials evaluated at 0 and  $\infty$  provide good candidates for invariants describing the required difference.

**Definition 7.2.3.** Let  $\mathcal{K}$  be a local field of characteristic 0 and  $f(x) \in \mathcal{K}[x]$  be separable and monic. Let  $P_0, P_1, \dots, P_{\deg f} \neq 0$  denote the Sturm sequence for  $f(x)$ , write  $c_i$  for the lead coefficient of  $P_i$  and assume that  $\prod_{i=0}^{\deg f-1} P_i(0) \neq 0$ . Define

$$H_{\mathcal{K}}(f) = \prod_{i=0}^{\deg f-1} (c_i, -c_{i+1})_{\mathcal{K}} \cdot (-P_i(0), P_{i+1}(0))_{\mathcal{K}}.$$

**Remark 7.2.4.** When  $f$  is a quadratic, Example 3.3.5 notes that  $\phi$  becomes a 2-isogeny of elliptic curves and this construction recovers the error term given in [17, Theorem 4] (see Example 7.1.2). When  $f$  is a cubic, this is precisely  $H_{\mathcal{K}}(f)$  as in Definition 6.1.5 when  $b, L \neq 0$  (see Example 7.1.3).

**Conjecture 7.2.5.** Let  $\mathcal{K}$  be a local field of characteristic 0 and  $X_1 : y^2 = f(x)$ ,  $X_0 : w^2 = xf(x)$  for  $f(x) \in \mathcal{K}[x]$  separable, monic and such that  $f(0) \neq 0$ . Let  $P_0, P_1, \dots, P_{\deg f} \neq 0$  denote the Sturm sequence for  $f(x)$  and assume that  $\prod_{i=0}^{\deg f-1} P_i(0) \neq 0$ . Then

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)} H_{\mathcal{K}}(f) = w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_0})$$

where  $\lambda_{\mathcal{K}}(f,x)$  is as in Definition 4.3.2 and  $H_{\mathcal{K}}(f)$  is as in Definition 7.2.3.

If  $P_i(0) = 0$  or  $\deg P_{i+1} < \deg P_i - 1$  for some  $i$ , then  $H_{\mathcal{K}}(f)$  is no longer well-defined. It is expected that a different Hilbert symbol expression can be found so that the conjecture still holds (as in Definition 6.1.5, when  $bL = 0$ ).



**Corollary 7.2.6.** *Let  $K$  be a number field and  $X_1 : y^2 = f(x)$ ,  $X_0 : w^2 = xf(x)$  for  $f(x) \in \mathcal{K}[x]$  separable and monic. Assuming Conjecture 7.2.5, the 2-parity conjecture holds for  $\text{Jac}_{X_1}$  if and only if it holds for  $\text{Jac}_{X_0}$ .*

*Proof.* This is argued as in the proof of Theorem 6.3.1.  $\square$

**Corollary 7.2.7.** *Let  $K$  be a number field and  $C : y^2 = f(x)$  for  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$  separable with  $\alpha_i \in K$  for each  $i$ . For each  $1 \leq k \leq n - 2$ , write  $P_{k,0}, \dots, P_{k,n-k} \neq 0$  for the Sturm sequence of  $\prod_{j=k+1}^n (x + \alpha_k - \alpha_j)$ . Assuming  $\prod_{k,i} P_{k,i}(0) \neq 0$  and Conjecture 7.2.5 holds, the 2-parity conjecture holds for the Jacobian of  $C$ .*

*Proof.* Let  $f_1(x) = \prod_{j=2}^n (x + \alpha_1 - \alpha_j)$  and  $f_2(x) = x$ . By Corollary 7.2.6, the 2-parity conjecture holds for  $\text{Jac}_{w^2=f_1(x)f_2(x)} \cong \text{Jac}_C$  if and only if it holds for  $\text{Jac}_{y^2=f_1(x)}$ . Applying this repeatedly, we end up seeing that the 2-parity conjecture holds for  $\text{Jac}_C$  if and only if it holds for  $\text{Jac}_{y^2=(x+\alpha_{n-2}-\alpha_{n-1})(x+\alpha_{n-2}-\alpha_n)} = 0$ .  $\square$

### 7.2.1 Proof over Archimedean fields

In certain cases, we are able to prove Conjecture 7.2.5; for instance, when  $\mathcal{K}$  is Archimedean.

**Proposition 7.2.8.** *Conjecture 7.2.5 holds when  $\mathcal{K} \cong \mathbb{C}$ .*

*Proof.* We have that  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)} = (-1)^{\deg f+1}$  (by definition),  $H_{\mathcal{K}}(f) = +1$  and  $w_{\mathcal{K}}(\text{Jac}_{X_1})w_{\mathcal{K}}(\text{Jac}_{X_0}) = (-1)^{\deg f-1}$  (see Lemma 2.3.4).  $\square$

**Proposition 7.2.9.** *Conjecture 7.2.5 holds when  $\mathcal{K} \cong \mathbb{R}$ .*

*Proof.* Write  $r_1 < \dots < r_{\deg f - 2a}$  for the real roots of  $f(x)$  and let  $\mathbb{1}_{0 < r_j} = 1$  if  $0 < r_j$ , and 0 otherwise. By Lemmata 8.4.10 and 8.4.11, it is enough to prove that

$$H_{\mathcal{K}}(f) = (-1)^{a + \sum_{j \equiv \deg f + 1 \pmod{2}} \mathbb{1}_{0 < r_j}} = (-1)^{\lfloor \frac{\kappa(0) + \kappa(\infty)}{2} \rfloor} \quad (7.1)$$

since  $a \equiv 0 \pmod{2} \Leftrightarrow \Delta_f = c_{\deg f} \cdot \square > 0 \Leftrightarrow \kappa(\infty) \equiv 0 \pmod{2}$  and  $\sum_{j \equiv \deg f + 1 \pmod{2}} \mathbb{1}_{0 < r_j} \equiv \lfloor \frac{\kappa(0) - \kappa(\infty)}{2} \rfloor \pmod{2}$ .

Write  $\text{sign}(c_i) = +1$  if  $c_i > 0$ , and  $-1$  otherwise. Let  $c_0 = c'_0, c'_1, \dots, c'_{\kappa(\infty)}$  be a sublist of  $c_0, c_1, \dots, c_{\deg f}$  such that  $\text{sign}(c'_i) \neq \text{sign}(c'_{i+1})$ . Then

$$\prod_{i=0}^{\deg f-1} (c_i, -c_{i+1})_{\mathcal{K}} = \prod_{i=0}^{\kappa(\infty)-1} (c'_i, -c'_{i+1})_{\mathcal{K}} = (c'_0, -c'_1)_{\mathcal{K}}^{\kappa(\infty)} \cdot (-1)^{\lfloor \frac{\kappa(\infty)}{2} \rfloor} = (-1)^{\lfloor \frac{\kappa(\infty)}{2} \rfloor}$$

using that the list of  $c'_i$  alternates in sign and  $c'_0 > 0$  ( $f$  is monic). Doing the same to construct a list  $P_0(0) = P_0(0)', P_1(0)', \dots, P_{\kappa(0)}(0)'$  gives

$$\begin{aligned} \prod_{i=0}^{\deg f-1} (-P_i(0), P_{i+1}(0))_{\mathcal{K}} &= \prod_{i=0}^{\kappa(0)-1} (-P_i(0)', P_{i+1}(0)')_{\mathcal{K}} \\ &= (-P_0(0)', P_1(0)')_{\mathcal{K}}^{\kappa(0)} \cdot (-1)^{\lfloor \frac{\kappa(0)}{2} \rfloor} = (-1)^{\kappa(0)\kappa(\infty) + \lfloor \frac{\kappa(0)}{2} \rfloor} \end{aligned}$$

since the list of  $P_i(0)'$  alternates in sign and  $\text{sign}(P_0(0)') = (-1)^{\kappa(0) + \kappa(\infty)}$ . Therefore

$$H_{\mathcal{K}}(f) = (-1)^{\lfloor \frac{\kappa(\infty)}{2} \rfloor + \kappa(0)\kappa(\infty) + \lfloor \frac{\kappa(0)}{2} \rfloor} = (-1)^{\lfloor \frac{\kappa(0) + \kappa(\infty)}{2} \rfloor}$$

as in (7.1). □

### 7.2.2 Proof over non-Archimedean fields for nice reduction types, when $f$ is a quartic

We are currently unable to prove Conjecture 7.2.5 in complete generality since we lack an understanding of the relationship between the entries of the Hilbert symbols defining  $H_{\mathcal{K}}(f)$  and the reduction types of  $X_1, X_0$  and  $X$  over non-Archimedean fields.

Despite this, we are able to prove the simplest unsolved case: when  $\mathcal{K}$  is non-Archimedean of odd residue characteristic,  $f(x)$  is a quartic and  $X_1, X_0$  have nice reduction types (see Proposition 6.2.4 when  $\deg f = 3$  and [17, Theorem 4] when  $\deg f = 2$ ).

**Notation 7.2.10.** Let  $K$  be a field and  $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$  be

separable. Write  $\Delta_f$  for the discriminant of  $f(x)$  and define

$$\begin{aligned} J_1 &= 3a^2 - 8b, \\ J_2 &= 2a^2b^2 - 8b^3 - 6a^3c + 28abc - 36c^2 - 12a^2d + 32bd, \\ J_3 &= ac - 16d, \\ J_4 &= a^2bc - 4b^2c + 3ac^2 - 9a^3d + 32abd - 48cd. \end{aligned}$$

When  $K = \mathcal{K}$  is a local field of characteristic 0, for such a quartic  $f(x)$ ,

$$H_{\mathcal{K}}(f) = (J_1, -J_2)_{\mathcal{K}} \cdot (J_2, -\Delta_f)_{\mathcal{K}} \cdot (-d, c)_{\mathcal{K}} \cdot (-c, J_3)_{\mathcal{K}} \cdot (-J_3, J_4)_{\mathcal{K}} \cdot (-J_4, \Delta_f)_{\mathcal{K}}$$

(assuming that  $J_1, J_2, J_3, J_4, \Delta_f, d, c \neq 0$ ).

Since the entries of these Hilbert symbols come from the Sturm sequence of  $f(x)$ , which is determined recursively via Euclid's algorithm, there are various identities relating them. For example,

$$J_1^2 \Delta_f + J_1 J_4^2 + J_2^2 J_3 - 2(ab - 6c) J_2 J_4 = 0. \tag{7.2}$$

**Proposition 7.2.11.** *Conjecture 7.2.5 holds when  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p \neq 2$ ,  $f(x) \in \mathcal{O}_{\mathcal{K}}[x]$  is a quartic and both  $X_1, X_0$  are semistable with  $\Sigma_{X_0} = \textcircled{\bullet\bullet\bullet\bullet}_0, \textcircled{\bullet\bullet\bullet}_0$  or  $\textcircled{\bullet\bullet}_0$ .*

*Proof.* The inputs of Table 7.1 (columns 1 and 2) are the possible cluster pictures for  $X_1$  and  $X_0$  where the roots of  $f$  are denoted by red circles ( $\bullet$ ) and the root 0 (of  $x$ ) is denoted by a blue diamond ( $\blacklozenge$ ), under the imposed assumption. We note that  $\mu(X_1) = \mu(X) = 1$ , since  $X_1$  has genus 1 and  $X$  has genus 3 (c.f. Theorem 2.4.11), and so we don't declare these quantities.

Column 3 gives the cluster picture for  $\text{Jac}_{X_1}$ , which is determined from the cluster picture for  $X_1$  using Remark 2.1.7 (normalised so that  $d_{\mathcal{R}} = 0$ ).

Column 4 gives the dual graph of the minimal regular model for  $X$ , where an arrow is used to indicate the action of Frobenius. This is determined using Theorem

$\Sigma_{X_1}$	$\Sigma_{X_0}$	$\Sigma_{\text{Jac} X_1}$	$\mathcal{T}_X$	$c(\text{Jac} X_1)$	$c(\text{Jac} X_0)$	$c(\text{Jac} X)$	$(-1)^{\text{ord} \lambda_K(f; w)}$	$w_K(\text{Jac} X_1)$	$w_K(\text{Jac} X_0)$	$H_K(f)$
				1	1	1	+1	+1	+1	+1
				1	2m	m	-1	+1	-1	+1
				1	2	n-tilde	$(-1)^m$	+1	+1	$(-1)^m$
				n	n	n^2	+1	-1	-1	+1
				n	n-tilde	n	$(-1)^{n+1}$	-1	+1	$(-1)^n$
				n	2mn	mn^2	-1	-1	+1	+1
				n	2m-tilde n	mn	$(-1)^n$	-1	-1	$(-1)^n$
				n	2n	n-tilde mn^2	$(-1)^m$	-1	-1	$(-1)^m$
				n	2n-tilde	n-tilde mn	$(-1)^{m+n+1}$	-1	+1	$(-1)^{m+n}$
				n-tilde	n	n	$(-1)^{n+1}$	+1	-1	$(-1)^n$
				n-tilde	n-tilde	n-tilde^2	+1	+1	+1	+1
				n-tilde	2mn	mn	$(-1)^n$	+1	+1	$(-1)^n$

										$m\tilde{n}^2$	-1	+1	-1	+1
										$\tilde{m}n$	$(-1)^{m+n+1}$	+1	-1	$(-1)^{m+n}$
										$\tilde{m}\tilde{n}^2$	$(-1)^m$	+1	+1	$(-1)^m$
										$2n_1n_2$	-1	-1	+1	+1
										$n_1\tilde{n}_2$	$(-1)^{n_2}$	-1	-1	$(-1)^{n_2}$
										$2(n_1+n_2)$	$(-1)^{n_1+n_2+1}$	-1	+1	$(-1)^{n_1+n_2}$
										$4n$	-1	+1	-1	+1
										$\tilde{n}$	$(-1)^n$	+1	+1	$(-1)^n$

Notation:  $\tilde{n} = \gcd(2, n)$ .

Table 7.1: Data for Proposition 7.2.11

2.4.14 (letting  $f_1(x) = f(x)$ ,  $f_2(x) = x$  so that  $B$  becomes  $X$ , whose chromatic cluster picture is as in column 2).

Columns 5, 6 and 7 list the Tamagawa numbers for  $\text{Jac}_{X_1}$ ,  $\text{Jac}_{X_0}$  and  $\text{Jac}_X$ , where the first and second are calculated from their cluster pictures using [60, Table 15.1] and Theorem 2.4.9 respectively, and the third is calculated from  $\Upsilon_X$  using Theorem 2.3.3.

Column 8 gives the value of  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f,x)}$ .

Columns 9 and 10 give  $w_{\mathcal{K}}(\text{Jac}_{X_1})$  and  $w_{\mathcal{K}}(\text{Jac}_{X_0})$  calculated using Theorems 2.3.6 and 2.4.10 respectively.

It remains to compute the value of  $H_{\mathcal{K}}(f)$ . Unless specified otherwise, equivalences are taken modulo  $\pi$ , where  $\pi$  is a uniformiser of  $\mathcal{K}$  and we write  $v$  for a normalised valuation on  $\overline{\mathcal{K}}$ , i.e.  $v(\pi) = 1$ . By assumption,  $a, b, c, d \in \mathcal{O}_{\mathcal{K}}$  and we let  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  denote the roots of  $f$ .

**Row 1.**  $d, \Delta_f$  are units. A case-by-case analysis of the valuations of  $J_1$  and  $J_2$  gives that  $(J_1, -J_2)(J_2, -\Delta_f) = +1$ . This is clear when  $J_1$  is a unit, since either  $J_2$  is also a unit, or  $J_2 \equiv 0 \Rightarrow -J_1 \Delta_f \equiv \square$  by (7.2). Write  $J_1 = Z\pi^k$  (for  $k > 0$ ) and  $a^3 - 16c = Y\pi^l$  where  $Z, Y \not\equiv 0$ . Since  $\Delta_f \equiv -(a^4 - 256d) \cdot \square$  (where  $\square$  denotes a square unit), we have that  $a^4 - 256d$  is a unit. If  $k \neq 2l$ , then the identity follows using that  $J_2 \equiv Z(a^4 - 256d)\pi^k \cdot \square \pmod{\pi^{k+1}}$  when  $k < 2l$  and  $J_2 \equiv -\pi^{2l} \cdot \square \pmod{\pi^{2l+1}}$  when  $k > 2l$  (where  $\square$  again denotes a square unit). If  $k = 2l$ , then either  $v(J_2) = 2l$  or  $Z(a^4 - 256d) \equiv \square$  and again the identity holds. Similarly, a case-by-case analysis of the valuations of  $c, J_3$  and  $J_4$  gives that  $(-d, c)(-c, J_3)(-J_3, J_4)(-J_4, \Delta_f) = +1$ . This is clear when  $c, J_3$  and  $J_4$  are all units. When  $J_3$  is a unit, the product becomes  $(c, -dJ_3)(J_4, -J_3\Delta_f)$  which is visibly equal to  $+1$  upon observing that  $c \equiv 0 \Rightarrow -dJ_3 \equiv 16d^2$  and  $J_4 \equiv 0 \Rightarrow -J_3\Delta_f \equiv \square$  (when  $J_1 \not\equiv 0$  this follows from (7.2), else  $3 \equiv 0$  or  $a^3 \equiv 16c$ ). Now suppose that  $J_3 \equiv 0$ . If  $c, J_4$  are units then  $-cJ_4 \equiv \square$ . Otherwise, write  $J_3 = Z\pi^k$  and  $J_1 = Y\pi^l$  where  $Z, Y \not\equiv 0$  and  $k, l > 0$ . Since  $\Delta_f \equiv 3c(a^3 - 16c) \cdot \square$  (where  $\square$  denotes a square unit), we have that  $3, a^3 - 16c$  are units. It remains to show that  $(\pi^k, -cJ_4)(J_4, -3Zc(a^3 - 16c)) = +1$ . If  $k \neq 2l$ , then the identity follows using that  $J_4 \equiv -3Z(a^3 - 16c)\pi^k \cdot \square \pmod{\pi^{k+1}}$  when  $k < 2l$  and

$J_4 \equiv -c\pi^{2l} \cdot \square \pmod{\pi^{2l+1}}$  when  $k > 2l$  (where  $\square$  denotes a square unit). If  $k = 2l$ , then either  $v(J_4) = 2l$  or  $-3Zc(a^3 - 16c) \equiv \square$  and again the identity holds. In conclusion,  $H_{\mathcal{K}}(f) = +1$ .

**Rows 2, 3.**  $d \equiv 0$  and  $\Delta_f$  is a unit (therefore, so is  $c$ ). Arguing as above, again gives that  $(J_1, -J_2)(J_2, -\Delta_f) = +1$ . Additionally, a case-by-case analysis of the valuations of  $J_3$  and  $J_4$  gives that  $(-c, J_3)(-J_3, J_4)(-J_4, \Delta_f) = +1$  where we argue as before when  $J_3 \neq 0$ . Otherwise, write  $J_3 = W\pi^k$ ,  $d = Y\pi^l$ ,  $b = Z\pi^i$  where  $W, Y, Z \neq 0$  and  $k, l, i > 0$ , then  $\Delta_f \equiv -3 \cdot \square$  where  $\square$  denotes a square unit ( $3$  is a unit since  $\Delta_f \neq 0$ ). It remains to show that  $(-c, \pi^k)(3W\pi^k, J_4) = +1$ . This follows from observing that  $J_4 \equiv 3cW\pi^k - c\pi^{4l} \cdot \square \pmod{\pi^{\min\{k, 4l\}+1}}$  when  $2l < i$ ,  $J_4 \equiv 3cW\pi^k - c\pi^{2i} \cdot \square \pmod{\pi^{\min\{k, 2i\}+1}}$  when  $2l > i$  and  $J_4 \equiv 3cW\pi^k - c(c^2Z - 96Y^2)^2\pi^{4l} \cdot \square \pmod{\pi^{\min\{k, 4l\}+1}}$  when  $2l = i$  (where  $\square$  denotes a square unit). In conclusion, letting  $v(\alpha_1) = m$ ,  $H_{\mathcal{K}}(f) = (-d, c) = (-\alpha_2\alpha_3\alpha_4, \pi)^m$  which evaluates to the claimed values upon varying the sign attached to the twin.

**Rows 4, 5, 10, 11.** Suppose that  $v(\alpha_1 - \alpha_2) = \frac{n}{2}$ , then  $H_{\mathcal{K}}(f) = (J_1, -J_2)(-\alpha_3\alpha_4, c)(-c, J_3)(J_3, -(\alpha_1 + \alpha_2)(\alpha_3 - \alpha_4)^2)(\frac{\alpha_1 + \alpha_2}{2}, \pi^n)$ . Since  $J_2$  is a unit and  $J_1 \equiv 0 \Rightarrow J_2 \equiv -\frac{9}{64}(a^3 - 16c)^2$  we have that  $(J_1, -J_2) = +1$ . That  $(-\alpha_3\alpha_4, c)(-c, J_3)(J_3, -(\alpha_1 + \alpha_2)(\alpha_3 - \alpha_4)^2) = +1$  can be seen via a case-by-case analysis of the valuations of  $c$  and  $J_3$  since  $c \equiv 0 \Rightarrow J_3 \equiv -\alpha_3\alpha_4 \cdot \square \neq 0$  and  $J_3 \equiv 0 \Rightarrow c \equiv -(\alpha_1 + \alpha_2)(\alpha_3 - \alpha_4)^2 \cdot \square \neq 0$ . Therefore  $H_{\mathcal{K}}(f) = (\frac{\alpha_1 + \alpha_2}{2}, \pi)^n$  which evaluates to the claimed values upon varying the signs attached to the twins.

**Rows 6–9, 12–15.** Suppose that  $v(\alpha_1 - \alpha_2) = \frac{n}{2}$  and  $v(\alpha_3) = m$ , then  $H_{\mathcal{K}}(f) = (J_1, -J_2)(\pi^m, -\alpha_4)(-(\alpha_1 + \alpha_2)\alpha_4, J_3)(\frac{\alpha_1 + \alpha_2}{2}, \pi^n)$ . Arguing as above  $(J_1, -J_2) = +1$  and since  $J_3 \equiv 0 \Rightarrow \alpha_1 + \alpha_2 \equiv -\alpha_4$ ,  $H_{\mathcal{K}}(f) = (-\alpha_4, \pi)^m(\frac{\alpha_1 + \alpha_2}{2}, \pi)^n$  which evaluates to the claimed values upon varying the signs attached to the twins.

**Rows 16–18.** Suppose that  $v(\alpha_1 - \alpha_2) = \frac{n_1}{2}$  and  $v(\alpha_3 - \alpha_4) = \frac{n_2}{2}$ , then  $H_{\mathcal{K}}(f) = (J_2, -\Delta_f)(-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), J_4)(-J_4, \Delta_f)$ .

Suppose that  $n_1 > n_2$ . Since  $J_2 \equiv 2(\alpha_3 - \alpha_4)^2(\frac{\alpha_1 + \alpha_2}{2} - \alpha_3)^2(\frac{\alpha_1 + \alpha_2}{2} - \alpha_4)^2 \pmod{\pi^{n_1}}$  and  $J_4 \equiv -(\alpha_1 + \alpha_2)(\alpha_3 - \alpha_4)^2(\frac{\alpha_1 + \alpha_2}{2} - \alpha_3)^2(\frac{\alpha_1 + \alpha_2}{2} - \alpha_4)^2 \pmod{\pi^{n_1}}$ ,  $H_{\mathcal{K}}(f) = (2(\alpha_3 - \alpha_4)^2, -(\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2)(-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), (\alpha_3 - \alpha_4)^2)((\alpha_1 + \alpha_2)(\alpha_3 - \alpha_4)^2, (\alpha_1 -$

$\alpha_2)^2(\alpha_3 - \alpha_4)^2) = (\pi, \frac{\alpha_1 + \alpha_2}{2})^{n_1}(\pi, \frac{\alpha_3 + \alpha_4}{2})^{n_2}$ . This evaluates to the claimed values upon varying the signs attached to the twins.

Suppose that  $n_1 = n_2$ . Write  $(\alpha_1 - \alpha_2)^2 = S\pi^{n_1}$ ,  $(\alpha_3 - \alpha_4)^2 = T\pi^{n_1}$  where  $S, T \not\equiv 0$ , then  $H_{\mathcal{K}}(f) = (J_2, -ST)(J_4, -ST(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4))$ . Observe that  $J_2 \equiv 2\pi^{n_1}(\frac{\alpha_1 + \alpha_2}{2} - \frac{\alpha_3 + \alpha_4}{2})^2(S + T) \pmod{\pi^{n_1+1}}$  and  $J_4 \equiv -\pi^{n_1}(\frac{\alpha_1 + \alpha_2}{2} - \frac{\alpha_3 + \alpha_4}{2})^2((\alpha_3 + \alpha_4)S + (\alpha_1 + \alpha_2)T) \pmod{\pi^{n_1+1}}$ . Via a case-by-case analysis of the valuations of  $S + T$  and  $(\alpha_3 + \alpha_4)S + (\alpha_1 + \alpha_2)T$  it can be seen that  $H_{\mathcal{K}}(f) = ((\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \pi)^{n_1}$ . This evaluates to the claimed values upon varying the signs attached to the twins.

**Rows 19, 20.** Write  $(\alpha_1 - \alpha_2)^2 = S\pi^n$ ,  $(\alpha_3 - \alpha_4)^2 = T\pi^n$  where  $S, T \not\equiv 0$ , then  $H_{\mathcal{K}}(f) = (J_2, -ST(\frac{\alpha_1 + \alpha_2}{2} - \frac{\alpha_3 + \alpha_4}{2})^2)(J_4, -ST(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)(\frac{\alpha_1 + \alpha_2}{2} - \frac{\alpha_3 + \alpha_4}{2})^2)$ . Arguing as above, via a case-by-case analysis of the valuations of  $S + T$  and  $(\alpha_3 + \alpha_4)S + (\alpha_1 + \alpha_2)T$ , it can be seen that  $H_{\mathcal{K}}(f) = ((\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \pi)^n$  which again evaluates to the claimed values upon varying the sign attached to the orbit of twins.  $\square$



## Chapter 8

# The Parity Conjecture for Hyperelliptic Curves

We now shift our attention to arbitrary genus hyperelliptic curves, where, beyond genus 2, very little progress has been made towards proving the Birch and Swinnerton–Dyer and parity conjectures.

So far in this thesis, we have been able to deduce several instances of the parity conjecture for low genus curves (under assumptions on the Shafarevich–Tate group) through comparing the terms appearing in Theorem 4.5.1 to local root numbers. We began thinking about higher genus curves in the previous chapter (hyperelliptic curves whose defining polynomials have a linear factor), and we provided a conjectural generalisation of the method of Chapter 6. Here, we advance this further by considering all hyperelliptic curves.

Our strategy is to reduce the problem to studying hyperelliptic curves with nice models (those whose Galois group is a 2-group).

**Definition 8.0.1.** Let  $C : y^2 = f(x)$  be a hyperelliptic curve over a number field  $K$ .

If  $f(x) = f_1(x)f_2(x)$  for  $f_1(x), f_2(x) \in K[x]$  with  $\deg f_1, \deg f_2 < \deg f$ , then we call  $C$  a  $C_2 \times C_2$ -hyperelliptic curve.

If  $f(x) = f_0(x)\bar{f}_0(x)$  for  $\text{Gal}_{L/K}$ -conjugate polynomials  $f_0(x), \bar{f}_0(x) \in L[x]$  where  $L/K$  is a quadratic extension, then we call  $C$  a  $D_8$ -hyperelliptic curve.

For both kinds of hyperelliptic curve, we present an arithmetic analogue of the 2-parity conjecture i.e. a method to compute the parity of the  $2^\infty$ -Selmer rank of

their Jacobians from the local data attached to higher genus curves (=Theorems 8.2.1 & 8.2.6). In the setting of  $D_8$ -hyperelliptic curves, we use properties of the Weil restriction to achieve this.

As in previous chapters, we then compare the local data appearing in these constructions to local root numbers and provide a conjectural description of the difference (=Conjectures 8.3.8 & 8.3.11) which we call the *error term*. The main feature of the error term is a product of Hilbert symbols whose entries are defined via the roots of the hyperelliptic curve's defining polynomial, rather than its coefficients (as in Chapters 6 and 7). We observe that, when considering elliptic curves, this recovers the error term exhibited in [17, Theorem 4].

There are several cases in which we are able to prove the aforementioned conjectures (=Theorems 8.3.10 & 8.3.12); namely, at infinite places of the number field and at finite places where the reduction type of the hyperelliptic curve is nice. We expect to be able to prove the remaining cases using the following argument which we omit from this thesis (since it is work in progress). First, we show that the theorems hold over completions of (global) function fields with the reduction types specified in 8.3.10 & 8.3.12. Then, we extend this to all reduction types over completions of function fields using a global-to-local method (resembling the proofs of Propositions 5.2.8 & 6.2.11), since the parity conjecture is known to hold over function fields. The proof is complete upon observing that the truth of Conjectures 8.3.8 & 8.3.11 depend only on the cluster pictures (or similar local data) and that the function field setting covers all possibilities.

We conclude the chapter with a discussion of the global implications of our local results. In particular, we explain how the parity conjecture for semistable hyperelliptic curves follows from the error term conjectures for  $C_2 \times C_2$ - and  $D_8$ -hyperelliptic curves, and the finiteness of the Shafarevich–Tate group (=Corollary 8.6.4). We also highlight the instances of the 2-parity conjecture which follow from cases of the error term conjectures we've been able to prove, and therefore hold unconditionally (=Theorem 8.6.6).

## 8.1 Reducing the problem to curves with nice automorphisms

Our first step towards proving the parity conjecture for semistable hyperelliptic curves is to reduce the problem to a smaller family.

**Theorem 8.1.1.** *Let  $K$  be a number field. Suppose that the 2-parity conjecture holds for the Jacobians of all  $C_2 \times C_2$ -hyperelliptic curves over  $K$ , and of all  $D_8$ -hyperelliptic curves over  $K$  whose defining polynomial has degree a power of 2.*

*Let  $C : y^2 = f(x)$  be a semistable hyperelliptic curve over  $K$  and write  $\mathcal{R} \subset \overline{K}$  for the set of roots of  $f(x)$ . If  $\text{III}(\text{Jac}_C/K(\mathcal{R})) [p^\infty]$  is finite for each prime  $p \leq \deg f$ , then the parity conjecture holds for the Jacobian of  $C$ .*

*Proof.* Applying [24, Theorem B.1] with  $F = K(\mathcal{R})$  and  $A = \text{Jac}_C$  (for which there are no primes of unstable reduction), we see that it is enough to prove the parity conjecture for  $\text{Jac}_C/K(\mathcal{R})^H$  whenever  $H \leq \text{Gal}_{K(\mathcal{R})/K}$  is a 2-group. This is equivalent to the 2-parity conjecture for  $\text{Jac}_C/K(\mathcal{R})^H$ , since  $\#\text{III}(\text{Jac}_C/K(\mathcal{R})) [2^\infty]$  and hence  $\#\text{III}(\text{Jac}_C/K(\mathcal{R})^H) [2^\infty]$  are assumed to be finite. The 2-parity conjecture for such curves follows from the 2-parity conjecture for Jacobians of all hyperelliptic curves such that the Galois group of their defining polynomial is a 2-group. We now show that these are either  $C_2 \times C_2$ -hyperelliptic curves, or  $D_8$ -hyperelliptic curves whose defining polynomial has degree a power of 2.

Let  $\tilde{C} : y^2 = \tilde{f}(x)$  be such a curve, i.e.  $G := \text{Gal}_{K(\tilde{\mathcal{R}})/K}$  is a 2-group where  $\tilde{\mathcal{R}} \subset \overline{K}$  denotes the roots of  $\tilde{f}(x)$ .

If  $\tilde{f}(x)$  is reducible over  $K$ , then  $\tilde{C}$  is a  $C_2 \times C_2$ -hyperelliptic curve and the parity conjecture holds by assumption.

If  $\tilde{f}(x)$  is irreducible over  $K$ , then  $G$  acts transitively on  $\tilde{\mathcal{R}}$ . Fix  $r \in \tilde{\mathcal{R}}$ . As  $G$  is a 2-group, there is a chain of normal subgroups  $\text{Stab}_G(r) = H_0 < H_1 < H_2 < \dots < H_{n-1} < H_n = G$  with each successive quotient having size 2 (c.f. the Sylow theorems). By the orbit-stabiliser theorem,  $H_{n-1}$  permutes  $\tilde{\mathcal{R}}$  in two orbits  $\tilde{\mathcal{R}}_1, \tilde{\mathcal{R}}_2$  which are preserved by  $G$  (since  $H_{n-1}$  is normal in  $G$ ). Therefore  $\tilde{f}(x) = f_0(x)\bar{f}_0(x)$  over  $L = K(\tilde{\mathcal{R}})^{H_{n-1}}$  (where the roots of  $f_0(x), \bar{f}_0(x)$  are  $\tilde{\mathcal{R}}_1, \tilde{\mathcal{R}}_2$  respectively), i.e.  $\tilde{C}$

is a  $D_8$ -hyperelliptic curve whose defining polynomial has degree a power of 2, and again the parity conjecture holds by assumption.  $\square$

## 8.2 Controlling the parity of the rank

We now explain how we can use familiar local data and lower genus hyperelliptic curves to determine the parity of the  $2^\infty$ -Selmer rank of the Jacobian of a  $C_2 \times C_2$ - or  $D_8$ -hyperelliptic curve.

### 8.2.1 $C_2 \times C_2$ -hyperelliptic curves

**Theorem 8.2.1** (=Theorem 4.5.2). *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  where  $f_1(x), f_2(x) \in K[x]$  are such that  $f_1(x)f_2(x)$  is separable. Then*

$$\mathrm{rk}_2(\mathrm{Jac}_{X_1}) + \mathrm{rk}_2(\mathrm{Jac}_{X_2}) + \mathrm{rk}_2(\mathrm{Jac}_{X_0}) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2 \lambda_v(f_1, f_2) \pmod{2}$$

where  $\lambda_v(f_1, f_2)$  is as in Definition 4.3.2.

### 8.2.2 $D_8$ -hyperelliptic curves

Let  $K$  be a field of characteristic 0 and  $K(\sqrt{\xi})/K$  be a quadratic extension.

**Notation 8.2.2.** Let  $f_0(x) \in K(\sqrt{\xi})[x]$  be such that  $f_0(x)\bar{f}_0(x)$  is separable, where  $\bar{f}_0(x)$  denotes the  $\mathrm{Gal}_{K(\sqrt{\xi})/K}$ -conjugate of  $f_0(x)$ . Define curves over  $K$  by

$$C : v^2 = f_0(x)\bar{f}_0(x), \quad X : \{y^2 = f_0(x), z^2 = \bar{f}_0(x), w^2 = \xi\}$$

(for a model of  $X$  fixed by  $\mathrm{Gal}_{K(\sqrt{\xi})/K}$ , instead consider  $\{y^2 + z^2 = f_0(x) + \bar{f}_0(x), (yz)^2 = f_0(x)\bar{f}_0(x), w^2 = \xi\}$ ).

The group  $G = D_8 := \langle \sigma, \tau \rangle$  acts on  $X$  where  $\sigma : (x, y, z, w) \mapsto (x, z, -y, -w)$ ,  $\tau : (x, y, z, w) \mapsto (x, y, -z, w)$ . There are three linearly independent Brauer relations for  $G$ , one of which is given by

$$\langle \tau \rangle + \langle \sigma^2, \sigma\tau \rangle - \langle \sigma^2, \tau \rangle - \langle \tau\sigma \rangle.$$

Applying Theorem 3.2.2(ii) with respect to this gives the existence of an isogeny  $\text{Jac}_{X_{\langle\tau\rangle}} \times \text{Jac}_{X_{\langle\sigma^2, \sigma\tau\rangle}} \rightarrow \text{Jac}_{X_{\langle\sigma^2, \tau\rangle}} \times \text{Jac}_{X_{\langle\tau\sigma\rangle}}$ .

The quotients of  $X$  by the subgroups of  $G$ , up to conjugacy, are displayed in Figure 8.1.

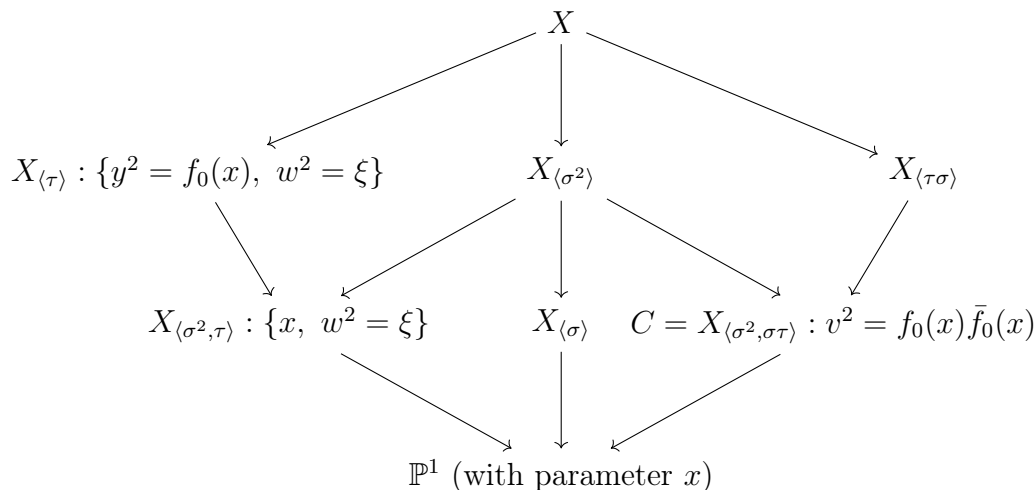


Figure 8.1:  $D_8$  diagram of covers of curves

Additionally, since the function field of  $X_{\langle\tau\sigma\rangle}$  is  $K(X)^{\langle\tau\sigma\rangle} = K(x, y + z)$  (c.f. §2.1.7) we see that

$$X' = X_{\langle\tau\sigma\rangle} : u^4 - 2(f_0(x) + \bar{f}_0(x))u^2 + (f_0(x) - \bar{f}_0(x))^2 = 0.$$

**Notation 8.2.3.** Write  $C_0 : y^2 = f_0(x)$ ,  $\bar{C}_0 : z^2 = \bar{f}_0(x)$  for hyperelliptic curves over  $K(\sqrt{\xi})$  and  $\text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0}$  for the Weil restriction of  $\text{Jac}_{C_0}$  from  $K(\sqrt{\xi})$  to  $K$  (see §2.2).

In the next lemma, we note that the  $K$ -isogeny identified above can be rewritten in terms of these explicit curves. Additionally, we show that, when viewed over the quadratic extension  $K(\sqrt{\xi})$ , the isogeny coincides with the one constructed in §3.3.

**Lemma 8.2.4.** *As abelian varieties over  $K$ ,  $\text{Jac}_{X_{\langle\tau\rangle}} \cong \text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0}$ . In particular, there exists a  $K$ -isogeny  $\phi : \text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  with*

$$\ker \phi = \left\{ ((D_S, D_T), D_{S \cup T}) : S \subseteq \mathcal{R}_{f_0}, T \subseteq \mathcal{R}_{\bar{f}_0} \text{ have even size} \right\}$$

which, via the isomorphism noted in (2.1), becomes the  $K(\sqrt{\xi})$ -isogeny  $\text{Jac}_{C_0} \times \text{Jac}_{\bar{C}_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  constructed in Theorem 3.3.2 (with  $K$  replaced by  $K(\sqrt{\xi})$ ),  $f_1(x) = f_0(x)$ ,  $f_2(x) = \bar{f}_0(x)$ .

*Proof.* The isomorphism is immediate from [23, Lemma A.22].

The proposed kernel is a finite subgroup of  $\text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0}(\bar{K}) \times \text{Jac}_C(\bar{K})$  and is stable under the action of  $G_K$ , since  $\sigma((D_S, D_T), D_{S \cup T}) = ((D_{\sigma(S)}, D_{\sigma(T)}), D_{\sigma(S) \cup \sigma(T)})$  or  $((D_{\sigma(T)}, D_{\sigma(S)}), D_{\sigma(S) \cup \sigma(T)})$  for  $\sigma \in G_K$ . Therefore, [44, Chapter 4, Lemma 2.1] guarantees the existence of a  $K$ -isogeny  $\phi : \text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0} \times \text{Jac}_C \rightarrow A$  (for some abelian variety  $A/K$ ) with such kernel.

Applying the construction in §3.3 with  $f_1(x) = f_0(x)$ ,  $f_2(x) = \bar{f}_0(x)$  gives rise to a  $K(\sqrt{\xi})$ -isogeny  $\text{Jac}_{C_0} \times \text{Jac}_{\bar{C}_0} \times \text{Jac}_C \rightarrow \text{Jac}_{\{y^2=f_0(x), z^2=\bar{f}_0(x)\}} \cong \text{Jac}_{X'}$ , with the isomorphism following from the curves viewed over  $K(\sqrt{\xi})$  having the same function fields ([62, Tag 0BY1]). By Lemma 3.3.7, this isogeny has the same kernel as the isogeny  $\phi$  (as above) and so it must in fact be defined over  $K$ , giving that  $A \cong \text{Jac}_{X'}$ .  $\square$

**Definition 8.2.5.** Let  $\mathcal{K}$  be a local field of characteristic 0,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  be a quadratic extension and  $\phi : \text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  be the  $\mathcal{K}$ -isogeny as in Lemma 8.2.4. We define the local invariant  $\lambda_{\mathcal{K}}(f_0; \sqrt{\xi})$  to be

$$\left\{ \begin{array}{ll} \# \ker \phi |_{(\text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C)(\mathcal{K})^\circ} \frac{n_{\text{Jac}_C} \mu_{\mathcal{K}}(C)}{n_{\text{Jac}_{X'}} \mu_{\mathcal{K}}(X')} & \mathcal{K} \simeq \mathbb{R}, \\ \frac{c_{\mathcal{K}}(\text{Jac}_C) c_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) \mu_{\mathcal{K}}(C) \mu_{\mathcal{K}(\sqrt{\xi})}(C_0)}{c_{\mathcal{K}}(\text{Jac}_{X'}) \mu_{\mathcal{K}}(X')} & \mathcal{K}/\mathbb{Q}_p \text{ finite, } p \neq 2, \\ \frac{c_{\mathcal{K}}(\text{Jac}_C) c_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) \mu_{\mathcal{K}}(C) \mu_{\mathcal{K}(\sqrt{\xi})}(C_0)}{c_{\mathcal{K}}(\text{Jac}_{X'}) \mu_{\mathcal{K}}(X')} \Big|_{\omega_{\text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C / \mathcal{K}}^0} \frac{\phi^* \omega_{\text{Jac}_{X'/\mathcal{K}}}^0}{\omega_{\text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C / \mathcal{K}}^0} \Big|_{\mathcal{K}} & \mathcal{K}/\mathbb{Q}_2 \text{ finite.} \end{array} \right.$$

**Theorem 8.2.6.** Let  $K$  be a number field,  $K(\sqrt{\xi})/K$  a quadratic extension and  $C : v^2 = f_0(x)\bar{f}_0(x)$ ,  $C_0 : y^2 = f_0(x)$  where  $f_0(x)$ ,  $\bar{f}_0(x) \in K(\sqrt{\xi})[x]$  are  $\text{Gal}_{K(\sqrt{\xi})/K}$ -conjugate and  $f_0(x)\bar{f}_0(x)$  is separable.

Assuming that  $\text{III}(\text{Jac}_C/K)$ ,  $\text{III}(\text{Jac}_{C_0}/K(\sqrt{\xi}))$  are finite,

$$\text{rk}(\text{Jac}_C/K) + \text{rk}(\text{Jac}_{C_0}/K(\sqrt{\xi})) \equiv \sum_{v \text{ place of } K} \text{ord}_2 \lambda_v(f_0; \sqrt{\xi}) \pmod{2}$$

where  $\lambda_v(f_0; \sqrt{\xi})$  is as in Definition 8.2.5 when  $K_v(\sqrt{\xi})/K_v$  is a quadratic extension and  $\lambda_v(f_0; \sqrt{\xi}) := \lambda_{K_v(\sqrt{\xi})}(f_0, \bar{f}_0)$  is as in Definition 4.3.2 when  $K_v(\sqrt{\xi}) \cong K_v$ .

We will prove this below by applying the isogeny invariance of the Birch and Swinnerton-Dyer conjecture to the  $K$ -isogeny  $\phi : \text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  constructed in Lemma 8.2.4. Since this isogeny involves a Weil restriction, the proof is slightly more delicate than those of Theorems 4.3.3 and 4.4.4.

**Lemma 8.2.7.** *Let  $K$  be a number field and  $\Theta = \langle \tau \rangle + \langle \sigma^2, \sigma\tau \rangle - \langle \sigma^2, \tau \rangle - \langle \tau\sigma \rangle$ . Then,*

$$\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = 2^{\text{rk}(\text{Jac}_C/K) + \text{rk}(\text{Jac}_{C_0}/K(\sqrt{\xi}))}.$$

*Proof.* Write  $\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q} = \chi_{+,+}^{\oplus n_1} \oplus \chi_{+,-}^{\oplus n_2} \oplus \chi_{-,+}^{\oplus n_3} \oplus \chi_{-,-}^{\oplus n_4} \oplus \rho^{\oplus n_5}$  for the decomposition into irreducible representations of  $D_8$ , where each  $\chi$  has dimension 1 with subscripts denoting the images of  $\sigma, \tau$  respectively, and  $\rho$  has dimension 2. By [18, Example 2.22],

$$\mathcal{C}_\Theta(\chi_{+,+}) = \mathcal{C}_\Theta(\chi_{+,-}) = 1, \quad \mathcal{C}_\Theta(\chi_{-,+}) = \mathcal{C}_\Theta(\chi_{-,-}) = \mathcal{C}_\Theta(\rho) = 2$$

and so Lemma 2.6.4 yields that  $\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) = 2^{n_3+n_4+n_5}$ . Applying Lemma 2.1.14 with  $H = \langle \sigma^2, \sigma\tau \rangle$  and taking dimensions immediately gives that  $\text{rk}(\text{Jac}_C/K) = n_1 + n_4$ . Instead letting  $H = \langle \tau \rangle$ , we see that

$$n_1 + n_3 + n_5 = \text{rk}(\text{Jac}_{X_H}/K) = \text{rk}(\text{Jac}_{C_0}/K(\sqrt{\xi}))$$

since  $H$  fixes a 1-dimensional subspace of  $\rho$  and  $\text{Jac}_{X_H} \cong \text{Res}_{K(\sqrt{\xi})/K}(\text{Jac}_{C_0})$  (Lemma 8.2.4). The result then follows.  $\square$

*Proof of Theorem 8.2.6.* Consider the  $K$ -isogeny  $\phi : \text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  as given in Lemma 8.2.4. As in the proof of Theorem 4.2.2,

$$\mathcal{C}_\Theta(\text{Jac}_X(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \equiv \frac{C(\text{Res } \text{Jac}_{C_0} \times \text{Jac}_C)}{C(\text{Jac}_{X'})} \cdot \frac{\#\text{III}(\text{Jac}_{C_0})\#\text{III}(\text{Jac}_C)}{\#\text{III}(\text{Jac}_{X'})} \pmod{\mathbb{Q}^{\times 2}}$$

having used that  $\text{III}(\text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0}) = \text{III}(\text{Jac}_{C_0})$  (see [41, Theorem 1]).

Let  $\omega$  be a non-zero global exterior form for  $\text{Jac}_{X'}$  which is minimal at all places of  $K$  above 2 (c.f. Lemma 4.2.6), and let  $\omega' = \phi^*\omega$ . Applying Lemma 4.2.5 when  $v \mid \infty$ , multiplicativity of  $c_v$  when  $v \nmid \infty$ , and Theorem 2.3.11, gives that

$$\begin{aligned} &\equiv \prod_{\substack{v \mid \infty \\ \text{place of } K}} \frac{\#\ker \phi(K_v)}{\#\text{coker } \phi(K_v)} \prod_{\substack{v \nmid \infty \\ \text{place of } K}} \frac{c_v(\text{Res Jac}_{C_0})c_v(\text{Jac}_C)}{c_v(\text{Jac}_{X'})} \left| \frac{\phi^*\omega}{\omega_{\text{Res Jac}_{C_0} \times \text{Jac}_C}^0} \frac{\omega_{\text{Jac}_{X'}}^0}{\omega} \right|_v \\ &\quad \cdot \prod_{v \text{ place of } K} \frac{\mu_v(C) \prod_{w \mid v} \mu_w(C_0)}{\mu_v(X')} \pmod{\mathbb{Q}^{\times 2}} \end{aligned}$$

where  $w$  denotes a place of  $K(\sqrt{\xi})$ .

In light of Lemma 8.2.7, it remains to show that the 2-adic valuation of the displayed term at a place  $v$  of  $K$  has the same parity as  $\text{ord}_2 \lambda_v(f_0; \sqrt{\xi})$ .

Suppose that there are two places  $w_1, w_2$  of  $K(\sqrt{\xi})$  above  $v$ . In particular,  $K_v(\sqrt{\xi})_{w_i} \cong K_v$  for  $i = 1, 2$  and  $\{C_0/K(\sqrt{\xi})_{w_1}, C_0/K(\sqrt{\xi})_{w_2}\} \cong \{C_0/K_v, \bar{C}_0/K_v\}$ . By definition,  $\lambda_v(f_0; \sqrt{\xi}) = \lambda_{K_v(\sqrt{\xi})}(f_0, \bar{f}_0)$ . When  $K_v \cong \mathbb{C}$ , this is clear since  $\#\text{coker } \phi(K_v) = 1$ ,  $\#\ker \phi(K_v) = 2^{2 \deg f_0 - 3}$  when  $\deg f_0$  is even,  $2^{2 \deg f_0 - 2}$  when  $\deg f_0$  is odd, and  $\mu = 1$ . When  $K_v \cong \mathbb{R}$ , this follows from (2.1) and [24, Lemma 3.4]. When  $K_v/\mathbb{Q}_p$  is finite, this follows from (2.1) and that  $\text{ord}_2(|\cdot|_v) = 0$  when  $p$  is odd.

Now suppose that there's a unique place  $w$  of  $K(\sqrt{\xi})$  above  $v$  so that  $K(\sqrt{\xi})_w \cong K_v(\sqrt{\xi})$  is a quadratic extension of  $K_v$  and  $\lambda_v(f_0; \sqrt{\xi})$  is as in Definition 8.2.5. When  $K_v \cong \mathbb{R}$  (and  $K(\sqrt{\xi})_w \cong \mathbb{C}$ ), this follows from [24, Lemma 3.4] and the fact that  $\text{Res Jac}_{C_0}(\mathbb{R}) \cong \text{Jac}_{C_0}(\mathbb{C})$ . When  $K_v/\mathbb{Q}_p$  is finite, this clear upon noting that  $c_v(\text{Res Jac}_{C_0}) = \prod_{w \mid v} c_w(\text{Jac}_{C_0})$  (see [41, Proposition 2(a)]) and that  $\text{ord}_2(|\cdot|_v) = 0$  when  $p$  is odd.  $\square$

Theorem 4.5.1 provides an analogous local formula for the parity of the  $2^\infty$ -Selmer rank of  $\text{Res}_{K(\sqrt{\xi})/K} \text{Jac}_{C_0} \times \text{Jac}_C$ .

**Theorem 8.2.8.** *Let  $K$  be a number field,  $K(\sqrt{\xi})/K$  a quadratic extension and  $C : v^2 = f_0(x)\bar{f}_0(x)$ ,  $C_0 : y^2 = f_0(x)$  where  $f_0(x), \bar{f}_0(x) \in K(\sqrt{\xi})[x]$  are  $\text{Gal}_{K(\sqrt{\xi})/K}$ -*



conjugate and  $f_0(x)\bar{f}_0(x)$  is separable. Then,

$$\mathrm{rk}_2(\mathrm{Jac}_C/K) + \mathrm{rk}_2(\mathrm{Jac}_{C_0}/K(\sqrt{\xi})) \equiv \sum_{v \text{ place of } K} \mathrm{ord}_2 \lambda_v(f_0; \sqrt{\xi}) \pmod{2}$$

where  $\lambda_v(f_0; \sqrt{\xi})$  is as in Definition 8.2.5 when  $K_v(\sqrt{\xi})/K_v$  is a quadratic extension and  $\lambda_v(f_0; \sqrt{\xi}) := \lambda_{K_v(\sqrt{\xi})}(f_0, \bar{f}_0)$  is as in Definition 4.3.2 when  $K_v(\sqrt{\xi}) \cong K_v$ .

### 8.3 Exhibiting an error term

Here we describe a conjectural error term for the formulae given in Theorems 8.2.1(=4.5.2) and 8.2.8. More precisely, we construct a product of Hilbert symbols which we aim to show controls the difference between the local invariants appearing in these formulae and relevant local root numbers.

Let  $K$  be a field of characteristic 0 and let  $f(x)g(x) \in K[x]$  be a separable polynomial with  $f(x), g(x) \in L[x]$  for  $L/K$  finite and such that the set  $\{f(x), g(x)\}$  is fixed by  $\mathrm{Gal}_{L/K}$ . Write  $\mathcal{R}_f, \mathcal{R}_g \subset \bar{K}$  for the roots of  $f(x), g(x)$  respectively.

**Assumption  $(\star)$ .** For each distinct pair  $r_1, r_2 \in \mathcal{R}_f$  and  $s \in \mathcal{R}_g$  assume that  $r_1 + r_2 \neq 2s$ . Similarly upon swapping the roles of  $f$  and  $g$ .

**Lemma 8.3.1.** *Let  $K$  be a field of characteristic 0 and  $f(x)g(x) \in K[x]$ . There exists a  $t \in K$  such that  $f_t(x) := f(\frac{x}{1-tx}), g_t(x) := g(\frac{x}{1-tx})$  satisfy Assumption  $(\star)$ .*

*Proof.* The roots of  $f_t(x), g_t(x)$  are  $\{\frac{r}{1+tr} : r \in \mathcal{R}_f\}, \{\frac{r}{1+tr} : r \in \mathcal{R}_g\}$  respectively.

We note that

$$\frac{r_1}{1+tr_1} + \frac{r_2}{1+tr_2} = 2\frac{s}{1+ts} \iff t = \frac{r_1 + r_2 - 2s}{s(r_1 + r_2) - 2r_1r_2}.$$

Therefore, for all but finitely many  $t \in K$ ,  $f_t(x), g_t(x)$  satisfy Assumption  $(\star)$ .  $\square$

**Notation 8.3.2.** Let

$$\mathcal{T} = \{\{r_1, r_2, s\} : r_1 \neq r_2 \in \mathcal{R}_f, s \in \mathcal{R}_g \text{ or } r_1 \neq r_2 \in \mathcal{R}_g, s \in \mathcal{R}_f\}.$$

For  $T \in \mathcal{T}$ , write  $\Gamma_T \leq G_K$  for the subgroup of elements preserving  $T$  as a set and let  $K(T) := \overline{K}^{\Gamma_T} = K(r_1 + r_2, r_1 r_2, s)$ .

**Definition 8.3.3.** Let  $T = \{r_1, r_2, s\} \in \mathcal{T}$ . When  $K = \mathcal{K}$  is a local field, we define  $H_{\mathcal{K}}(T) = H_1(T)H_2(T) \in \{\pm 1\}$  where

$$\begin{aligned} H_1(T) &= \left(- (r_1 + r_2 - 2s), -(r_1 - s)(r_2 - s)\right)_{\mathcal{K}(T)}, \\ H_2(T) &= \left(\frac{1}{2}(r_1 + r_2) - s, (r_1 - r_2)^2\right)_{\mathcal{K}(T)}. \end{aligned}$$

**Definition 8.3.4.** Let  $O$  denote a  $G_K$ -orbit of  $\mathcal{T}$  and fix an orbit representative  $T_O \in O$ . When  $K = \mathcal{K}$  is a local field, we define

$$H_{\mathcal{K}}(f, g) = \prod_{O \in \mathcal{T}/G_{\mathcal{K}}} H_{\mathcal{K}}(T_O) \in \{\pm 1\}$$

which we denote by  $H_v(f, g)$  when  $\mathcal{K} = K_v$  (for  $K$  a number field,  $v$  a place of  $K$ ).

**Example 8.3.5.** Let  $\mathcal{K}$  be a local field of characteristic 0,  $f(x) = x^2 + ax + b \in \mathcal{K}[x]$  and  $g(x) = x$ . Then  $\mathcal{T} = \{\{r_1, r_2, 0\}\}$  where  $r_1, r_2 \in \overline{\mathcal{K}}$  denote the roots of  $f(x)$ .

Let  $T = \{r_1, r_2, 0\}$ . Since  $\mathcal{K}(T) = \mathcal{K}$ , it follows that

$$H_{\mathcal{K}}(f, g) = (a, -b)_{\mathcal{K}}(-\frac{1}{2}a, a^2 - 4b)_{\mathcal{K}} = (a, -b)_{\mathcal{K}}(-2a, a^2 - 4b)_{\mathcal{K}}.$$

We note that this is the error term for elliptic curves admitting a 2-isogeny found in [17, Theorem 4].

**Lemma 8.3.6.** Let  $K$  be a number field and suppose that  $G_K$  acts transitively on  $S \subseteq \mathcal{T}$ . Fix  $T \in S$ . For each place  $v$  of  $K$ , there's a one-to-one correspondence

$$\{G_{K_v}\text{-orbits of } S\} \longleftrightarrow \{\text{places } w \mid v \text{ of } K(T)\}.$$

Explicitly, fixing a place  $z$  of  $\overline{K}$  above  $v$ ,  $\sigma^{-1} \in G_K$  induces an isomorphism of local fields

$$K_v(\sigma T) \cong K(T)_{\sigma^{-1}z},$$

where  $w$  is a place of  $K(T)$  such that  $z \mid w$ .

*Proof.* We have an isomorphism  $S \cong G_K/G_{K(T)}$  of  $G_K$ -sets and, fixing an embedding  $\overline{K} \hookrightarrow \overline{K}_v$ , or equivalently a place  $z \mid v$  of  $\overline{K}$ , an isomorphism  $G_{K_v} \cong D_z$  of groups (where  $D_z$  denotes the decomposition group of  $G_K$ ). Both the  $G_{K_v}$ -orbits of  $S$  and the places  $w$  of  $K(T)$  above  $v$  are in one-to-one correspondence with the  $D_z - G_{K(T)}$  double cosets of  $G_K$  (for the latter, see e.g. [52, Chapter 1, §9]). In particular, let  $T_O = \sigma T$  be a representative for  $O \in S/G_{K_v}$  (for some  $\sigma \in G_K$ ). Then  $O$  corresponds to the place  $w$  of  $K(T)$  such that  $\sigma^{-1}z \mid w$ .

Let  $w$  be a place of  $K(T)$  such that  $z \mid w$ . Writing  $w = \mathfrak{m}_{\overline{K}_z} \cap \mathcal{O}_{K(T)}$  we see that  $K_v(\sigma T) \cong K(\sigma T)_w$ . Applying  $\sigma^{-1}$  gives the required isomorphism.  $\square$

**Theorem 8.3.7.** *Let  $K$  be a number field and  $f(x)g(x) \in K[x]$  be a separable polynomial with  $f(x), g(x) \in L[x]$  for  $L/K$  finite and such that the set  $\{f(x), g(x)\}$  is fixed by  $\text{Gal}_{L/K}$ . Then*

$$\prod_{v \text{ place of } K} H_v(f, g) = +1$$

where  $H_v(f, g)$  is as in Definition 8.3.4.

*Proof.* Suppose that  $G_K$  acts transitively on  $S \subseteq \mathcal{T}$  and fix  $T \in S$ . Let  $O \in S/G_{K_v}$  be represented by the triple  $T_O = \sigma T$ , for some  $\sigma \in G_K$ .

Fix  $v$  a place of  $K$ . By the correspondence and isomorphism of local fields detailed in Lemma 8.3.6, the product of  $K_v(\sigma T)$ -valued Hilbert symbols  $H_v(\sigma T)$  is equal to the product of  $K(T)_w$ -valued Hilbert symbols  $H_w(T)$ , where  $w$  is the place of  $K(T)$  in correspondence with  $O$  (i.e.  $\sigma^{-1}z \mid w$ ). In particular,

$$\prod_{O \in S/G_{K_v}} H_v(T_O) = \prod_{w|v \text{ place of } K(T)} H_w(T).$$

Taking the product over places  $v$  of  $K$  gives  $+1$  (by the product law for Hilbert symbols over  $K(T)$ ) and the result follows upon applying this to each  $G_K$ -orbit of  $\mathcal{T}$ .  $\square$

We now explain the manner in which  $H_{\mathcal{K}}$  allows us to describe the difference between the local invariants  $\lambda_{\mathcal{K}}$  of Theorems 8.2.1 and 8.2.8 and local root numbers.

We begin with the construction concerning  $C_2 \times C_2$ -hyperelliptic curves (those whose defining polynomials are reducible).

**Conjecture 8.3.8.** *Let  $\mathcal{K}$  be a local field of characteristic 0 and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  for  $f_1(x), f_2(x) \in \mathcal{K}[x]$  such that  $f_1(x)f_2(x)$  is separable and Assumption  $(\star)$  holds. Then*

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)} w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_2}) w_{\mathcal{K}}(\text{Jac}_{X_0}) = (-1, -1)_{\mathcal{K}}^{\left[ \frac{(n_1-1)(n_2-1)}{2} \right]} H_{\mathcal{K}}(f_1, f_2) \cdot (-1, c_{f_1}^{\frac{1}{2}n_2(n_2+1)} c_{f_2}^{\frac{1}{2}n_1(n_1+1)})_{\mathcal{K}} (c_{f_1}, c_{f_2})_{\mathcal{K}}^{n_1 n_2} (\Delta_{f_1} R_{f_1, f_2}, c_{f_2})_{\mathcal{K}} (\Delta_{f_2} R_{f_2, f_1}, c_{f_1})_{\mathcal{K}}$$

where  $c_{f_i}, n_i$  denote the lead coefficient and degree of  $f_i$ ,  $\Delta$  denotes the discriminant,  $R$  denotes the resultant,  $H_{\mathcal{K}}(f_1, f_2)$  is as in Definition 8.3.4 and  $\lambda_{\mathcal{K}}(f_1, f_2)$  is as in Definition 4.3.2.

**Remark 8.3.9.** When  $f_1(x) \in \mathcal{K}[x]$  is a monic quadratic and  $f_2(x) = x$ , this is [17, Theorem 4] (c.f. Example 8.3.5 for  $H_{\mathcal{K}}$  in this case). An open problem is to show that this becomes Theorem 6.1.8 when  $f_1(x) \in \mathcal{K}[x]$  is a monic cubic and  $f_2(x) = x$ .

Unfortunately a complete proof of Conjecture 8.3.8 is currently out of our reach, with particularly troublesome cases being when  $\mathcal{K}/\mathbb{Q}_2$ , or when  $\mathcal{K}/\mathbb{Q}_p$  and  $\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$  is not semistable over  $\mathcal{K}$  (in these situations, the theory concerning the local invariants for hyperelliptic/bihyperelliptic curves is much less developed). However, in the next section we provide proofs in the following cases.

**Theorem 8.3.10** (Local Theorem III). *Let  $\mathcal{K}$  be a local field of characteristic 0 and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  for monic  $f_1(x), f_2(x) \in \mathcal{K}[x]$  such that  $f_1(x)f_2(x)$  is separable and Assumption  $(\star)$  holds. Conjecture 8.3.8 holds when:*

- (1)  $\mathcal{K}$  is Archimedean,
- (2)  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p \neq 2$ , and the reduction of  $f_1(x)f_2(x)$  has at worst one double root, or
- (3)  $\mathcal{K}/\mathbb{Q}_2$  is finite and  $X_1, X_2, X_0$  have good ordinary reduction with

$$\Sigma_{X_1} = \left( \begin{array}{c} \circ \circ \circ \circ \cdots \circ \circ \circ \circ \\ v(4) v(4) \cdots v(4) v(4) \end{array} \right)_0, \quad \Sigma_{X_2} = \left( \begin{array}{c} \diamond \diamond \diamond \diamond \cdots \diamond \diamond \diamond \diamond \\ v(4) v(4) \cdots v(4) v(4) \end{array} \right)_0,$$

$$\Sigma_{X_0} = \left( \begin{array}{c} \circ \circ \circ \circ \cdots \circ \circ \circ \circ \quad \diamond \diamond \diamond \diamond \cdots \diamond \diamond \diamond \diamond \\ v(4) v(4) \cdots v(4) v(4) \quad v(4) v(4) \cdots v(4) v(4) \end{array} \right)_0.$$

In particular,

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)} w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_2}) w_{\mathcal{K}}(\text{Jac}_{X_0}) = (-1, -1)_{\mathcal{K}}^{\left\lceil \frac{(n_1-1)(n_2-1)}{2} \right\rceil} H_{\mathcal{K}}(f_1, f_2)$$

where  $n_i$  denotes the degree of  $f_i$ ,  $H_{\mathcal{K}}(f_1, f_2)$  is as in Definition 8.3.4 and  $\lambda_{\mathcal{K}}(f_1, f_2)$  is as in Definition 4.3.2.

*Proof.* For (1), this is Propositions 8.4.1 and 8.4.12. For (2), this is Proposition 8.4.16. For (3), this is Proposition 8.4.21.  $\square$

We now state an analogous local conjecture and theorem for  $D_8$ -hyperelliptic curves (those whose defining polynomials are irreducible but admit a factorisation over a quadratic extension). In view of the parity conjecture, it is enough to consider such curves whose defining polynomials have degree a power of 2 (c.f. Theorem 8.1.1).

**Conjecture 8.3.11.** *Let  $\mathcal{K}$  be a local field of characteristic 0,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  be a quadratic extension and  $C_0 : y^2 = f_0(x)$ ,  $C : w^2 = f_0(x)\bar{f}_0(x)$  for  $\text{Gal}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}}$ -conjugate  $f_0(x)$ ,  $\bar{f}_0(x) \in \mathcal{K}(\sqrt{\xi})[x]$  of degree  $n = 2^m > 1$  such that  $f_0(x)\bar{f}_0(x)$  is separable and Assumption  $(\star)$  holds. Then*

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \sqrt{\xi})} w_{\mathcal{K}}(\text{Jac}_C) w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) = (-1, -1)_{\mathcal{K}} H_{\mathcal{K}}(f_0, \bar{f}_0) (-1, c_{f_0 \bar{f}_0})_{\mathcal{K}}^{\frac{n}{2}} (R_{f_0, \bar{f}_0}, c_{f_0 \bar{f}_0})_{\mathcal{K}} (\Delta_{\bar{f}_0}, c_{f_0})_{\mathcal{K}(\sqrt{\xi})}$$

where  $c_{f_0}$ ,  $c_{\bar{f}_0}$  denote the lead coefficients of  $f_0$ ,  $\bar{f}_0$  respectively,  $\Delta$  denotes the discriminant,  $R$  denotes the resultant,  $H_{\mathcal{K}}(f_0, \bar{f}_0)$  is as in Definition 8.3.4 and  $\lambda_{\mathcal{K}}(f_0; \sqrt{\xi})$  is as in Definition 8.2.5.

As in the case of  $C_2 \times C_2$ -hyperelliptic curves, at present we are only able to prove this conjecture in certain instances. This is the focus of §8.5.

**Theorem 8.3.12** (Local Theorem IV). *Let  $\mathcal{K}$  be a local field of characteristic 0,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  be a quadratic extension and  $C_0 : y^2 = f_0(x)$ ,  $C : w^2 = f_0(x)\bar{f}_0(x)$  for monic,  $\text{Gal}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}}$ -conjugate  $f_0(x), \bar{f}_0(x) \in \mathcal{K}(\sqrt{\xi})[x]$  of degree  $n = 2^m \geq 4$  such that  $f_0(x)\bar{f}_0(x)$  is separable and Assumption  $(\star)$  holds. Conjecture 8.3.11 holds when:*

- (1)  $\mathcal{K}$  is Archimedean (i.e.  $\mathcal{K} \cong \mathbb{R}$ ),
- (2)  $\mathcal{K}/\mathbb{Q}_p$  is finite,  $p \neq 2$ , and the reduction of  $f_0(x)\bar{f}_0(x)$  has at worst two double roots, or
- (3)  $\mathcal{K}/\mathbb{Q}_2$  is finite,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  is unramified, and  $C_0, C$  have good ordinary reduction with

$$\Sigma_{C_0/\mathcal{K}(\sqrt{\xi})} = \boxed{\textcircled{\text{red}}_{v(4)} \textcircled{\text{red}}_{v(4)} \cdots \textcircled{\text{red}}_{v(4)}}, \quad \Sigma_{C/\mathcal{K}} = \boxed{\textcircled{\text{red}}_{v(4)} \cdots \textcircled{\text{red}}_{v(4)} \textcircled{\text{blue}}_{v(4)} \cdots \textcircled{\text{blue}}_{v(4)}}.$$

In particular,

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \sqrt{\xi})} w_{\mathcal{K}}(\text{Jac}_C) w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) = (-1, -1)_{\mathcal{K}} H_{\mathcal{K}}(f_0, \bar{f}_0)$$

where  $H_{\mathcal{K}}(f_0, \bar{f}_0)$  is as in Definition 8.3.4 and  $\lambda_{\mathcal{K}}(f_0; \sqrt{\xi})$  is as in Definition 8.2.5.

*Proof.* For (1), this is Proposition 8.5.7. For (2), this is Proposition 8.5.13. For (3), this is Proposition 8.5.14.  $\square$

**Remark 8.3.13.** We omit a proof of Theorem 8.3.12 when  $\deg f_0 = 2$  for ease of exposition (in this case the methods used to compute the required local invariants are different). This does not impact the global results we obtain since, when  $K$  is a number field and  $f_0(x) \in K(\sqrt{\xi})[x]$  is a monic quadratic,  $\text{Jac}_C$  is an elliptic curve with a  $K$ -rational 2-torsion point (see Remark 2.1.7) for which the 2-parity conjecture is already known to hold ([20, Theorem 1.8]).

**Remark 8.3.14.** We note that when  $\mathcal{K}/\mathbb{Q}_2$  and  $X_1, X_2, X_0/\mathcal{K}$  or  $C_0/\mathcal{K}(\sqrt{\xi}), C/\mathcal{K}$  have good ordinary reduction, [25, Theorem 1.2] guarantees that the curves admit models with the cluster pictures specified in Theorems 8.3.10 and 8.3.12 whenever the size of the residue field of  $\mathcal{K}$  exceeds the genus of  $X_0$  or  $C$ .

**Remark 8.3.15.** When  $\mathcal{K}/\mathbb{Q}_p$  and  $p \neq 2$ , we expect to be able to generalise the proofs of Propositions 8.4.16 and 8.5.13 to prove Conjectures 8.3.8 and 8.3.11 whenever the hyperelliptic curves are all semistable with nice cluster pictures; for instance, their top clusters are principal and not *übereven*.

Given this generalisation, we then expect to be able to use deformation arguments to extend the proof to the cases when

- $p \neq 2$  and  $X_0, C$  are tame, and
- $p = 2$  and  $X_0, C$  have good ordinary reduction.

This is work in progress.

## 8.4 Proof of Local Theorem III

Throughout this section we assume the set up of Theorem 8.3.10. In particular,  $\mathcal{K}$  is a local field of characteristic 0 and  $f_1(x), f_2(x) \in \mathcal{K}[x]$  are monic, such that  $f_1(x)f_2(x)$  is separable and Assumption  $(\star)$  holds. We define hyperelliptic curves over  $\mathcal{K}$  by

$$X_1 : y^2 = f_1(x), \quad X_2 : z^2 = f_2(x), \quad X_0 : w^2 = f_1(x)f_2(x),$$

and a bihyperelliptic curve over  $\mathcal{K}$  by

$$X : \{y^2 = f_1(x), z^2 = f_2(x)\}.$$

### 8.4.1 Proof over Archimedean fields

We first prove that Theorem 8.3.10 holds when  $\mathcal{K}$  is an Archimedean local field.

This is straightforward when  $\mathcal{K} \cong \mathbb{C}$ , in which case we recall that

$$\lambda_{\mathcal{K}}(f_1, f_2) = 2^{\deg f_1 \deg f_2 + 1}.$$

**Proposition 8.4.1.** *Theorem 8.3.10 holds when  $\mathcal{K} \cong \mathbb{C}$ .*

*Proof.* Using that  $(-, -)_{\mathcal{K}} = +1$ , we need only show that

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)} w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_2}) w_{\mathcal{K}}(\text{Jac}_{X_0}) = +1.$$

This follows from the definition of  $\lambda_{\mathcal{K}}$  and noting that  $w_{\mathcal{K}}(\text{Jac}_{X_1}) = (-1)^{\lfloor \frac{\deg f_1 - 1}{2} \rfloor}$ ,  $w_{\mathcal{K}}(\text{Jac}_{X_2}) = (-1)^{\lfloor \frac{\deg f_2 - 1}{2} \rfloor}$ ,  $w_{\mathcal{K}}(\text{Jac}_{X_0}) = (-1)^{\lfloor \frac{\deg f_1 + \deg f_2 - 1}{2} \rfloor}$  (by Lemma 2.3.4).  $\square$

When  $\mathcal{K} \cong \mathbb{R}$ , we begin by determining  $H_{\mathcal{K}}(f_1, f_2)$ .

**Lemma 8.4.2.** *Let  $\mathcal{K} \cong \mathbb{R}$  and  $T = \{r_1, r_2, s\} \in \mathcal{T}$ . Then  $H_1(T)H_2(T) = -1$  precisely when  $s \in \mathbb{R}$  and either*

(1)  $r_1, r_2 \in \mathbb{R}$  with  $r_1, r_2 > s$ , or

(2)  $r_1, r_2$  are complex conjugates.

*Proof.* If  $\mathcal{K}(T) \cong \mathbb{C}$  then  $H_1(T) = H_2(T) = +1$  by definition. Therefore, suppose that  $\mathcal{K}(T) \cong \mathbb{R}$ , i.e.  $s \in \mathbb{R}$  and  $\{r_1, r_2\}$  is fixed under the action of complex conjugation.

If  $r_1, r_2 \in \mathbb{R}$  then  $(r_1 - r_2)^2 > 0$  and so  $H_2(T) = +1$ . It's then easy to check that both entries of  $H_1(T)$  are  $< 0$  only when  $r_1, r_2 > s$ .

If  $r_1, r_2$  are complex conjugates then  $(r_1 - r_2)^2 < 0$  and  $(r_1 - s)(r_2 - s) > 0$ . Therefore,  $H_1(T)H_2(T) = (-(r_1 + r_2 - 2s), -1)_{\mathcal{K}}(\frac{1}{2}(r_1 + r_2) - s, -1)_{\mathcal{K}} = -1$ .  $\square$

**Notation 8.4.3.** Write  $n_1, n_2$  for the degrees of  $f_1, f_2$  respectively and

$$\mathcal{R}_{f_1} \cap \mathbb{R} = \{\alpha_1, \dots, \alpha_{n_1 - 2a_1} : \alpha_i < \alpha_{i+1}\},$$

$$\mathcal{R}_{f_2} \cap \mathbb{R} = \{\beta_1, \dots, \beta_{n_2 - 2a_2} : \beta_i < \beta_{i+1}\},$$

where  $\mathcal{R}_{f_1}, \mathcal{R}_{f_2} \subset \overline{\mathcal{K}}$  denote the roots of  $f_1, f_2$  respectively.

For  $t_1, t_2 \in \mathbb{R}$ , write

$$\mathbb{1}_{t_1 < t_2} = \begin{cases} 1 & t_1 < t_2, \\ 0 & \text{otherwise.} \end{cases}$$



**Corollary 8.4.4.** *Let  $\mathcal{K} \cong \mathbb{R}$ . Then,*

$$H_{\mathcal{K}}(f_1, f_2) = (-1)^{\frac{1}{2}n_1(n_2(1-n_1)+2a_2)+\sum_{i+j \equiv n_1+n_2+1 \pmod{2}} \mathbb{1}_{\alpha_i < \beta_j}}$$

*Proof.* This follows, as below, from counting the triples detailed in Lemma 8.4.2.

Let  $t \in \mathbb{R}$ . The number of triples  $\{t, \beta_j, \beta_k\}$  with  $\beta_j, \beta_k > t$  is

$$\begin{aligned} \binom{\sum_j \mathbb{1}_{t < \beta_j}}{2} &= \frac{1}{2} \left( \left( \sum_j \mathbb{1}_{t < \beta_j} \right)^2 - \sum_j \mathbb{1}_{t < \beta_j} \right) \\ &= \sum_{j < i} \mathbb{1}_{t < \beta_j} \mathbb{1}_{t < \beta_i} \\ &= \sum_j (n_2 - 2a_2 - j) \mathbb{1}_{t < \beta_j} \\ &\equiv \sum_{j \equiv n_2+1 \pmod{2}} \mathbb{1}_{t < \beta_j} \pmod{2}. \end{aligned}$$

Thus, the number of triples  $\{\alpha_i, \beta_j, \beta_k\}$  of the first type is congruent to  $\sum_i \sum_{j \equiv n_2+1 \pmod{2}} \mathbb{1}_{\alpha_i < \beta_j}$  modulo 2. By symmetry, and using that  $\mathbb{1}_{t < \alpha_i} = 1 - \mathbb{1}_{\alpha_i < t}$ , the number of triples  $\{\alpha_i, \alpha_k, \beta_j\}$  of the first type is congruent to  $\frac{1}{2}n_2(n_1(1-n_1) - 2a_1) + \sum_{i \equiv n_1+1 \pmod{2}} \sum_j \mathbb{1}_{\alpha_i < \beta_j}$  modulo 2.

Since the number of triples of the second type is  $(n_1 - 2a_1)a_2 + (n_2 - 2a_2)a_1$ , we obtain the required expression for  $H_{\mathcal{K}}(f_1, f_2)$ .  $\square$

Having described  $H_{\mathcal{K}}$ , it remains to compute the right-hand-side of Theorem 8.3.10. This could be computed directly, however we will use the following result to make an immediate simplification.

**Lemma 8.4.5** (To appear in [46]). *Suppose that  $A, B$  are principally polarised abelian varieties over  $\mathbb{R}$  and that  $\phi : A \rightarrow B$  is an isogeny with  $\phi \circ \hat{\phi} = [2] = \hat{\phi} \circ \phi$ . Then*

$$(-1)^{\text{ord}_2 \left( \frac{\#\ker \phi(\mathbb{R})}{\#\text{coker } \phi(\mathbb{R})} \right)} \cdot w(A) = (-1)^{\text{ord}_2 \#\ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ}}$$

where  $\phi_{-1}$  is the induced isogeny on the quadratic twists by  $-1$ , i.e.  $\phi_{-1} := \psi_B \circ \phi \circ \psi_A^{-1}$  and  $\psi_A : A \rightarrow A_{-1}$ ,  $\psi_B : B \rightarrow B_{-1}$  are isomorphisms over  $\mathbb{C}$  such

that  $\overline{\psi_A(-P)} = \psi_A(\overline{P})$  for each  $P \in A(\mathbb{C})$ , and similarly for  $\psi_B$ .

In particular, in line with Corollary 4.2.7, when  $\mathcal{K} \cong \mathbb{R}$

$$\begin{aligned} (-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)} w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_2}) w_{\mathcal{K}}(\text{Jac}_{X_0}) \\ = (-1)^{\text{ord}_2 \# \ker \phi_{-1} |_{(\text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0})_{-1}(\mathcal{K})^\circ}}. \end{aligned}$$

We now state two lemmata which will allow us to compute this quantity.

**Lemma 8.4.6.** *Let  $\phi : \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0} \rightarrow \text{Jac}_X$  be the  $\mathcal{K}$ -isogeny defined in Theorem 3.3.2 and let  $\phi_{-1}$  be as in Lemma 8.4.5. Then*

$$\ker \phi_{-1} = \left\{ (D_S, D_T, D_{S \cup T}) : S \subseteq \mathcal{R}_{f_1}, T \subseteq \mathcal{R}_{f_2} \text{ have even size} \right\}$$

where  $\mathcal{R}_{f_1}, \mathcal{R}_{f_2} \subset \mathbb{C}$  denote the roots of  $f_1(x), f_2(x)$  respectively.

*Proof.* Write  $A = \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$  then  $A_{-1} = \text{Jac}_{(X_1)_{-1}} \times \text{Jac}_{(X_2)_{-1}} \times \text{Jac}_{(X_0)_{-1}}$  (since the hyperelliptic involution on a hyperelliptic curve induces multiplication by  $-1$  on its Jacobian [47, §1.5.2]). The result then follows from Lemma 3.3.7 since  $\ker \phi_{-1} = \psi_A(\ker \phi)$ .  $\square$

**Lemma 8.4.7.** *Let  $f(x) \in \mathbb{R}[x]$  be monic and separable. Define  $C : y^2 = -f(x)$  and let  $S \subseteq \mathcal{R}_f$  have even size. Then  $D_S \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if  $S$  is closed under conjugation and  $\deg(D_S \cap \mathfrak{c})$  is even for each connected component  $\mathfrak{c}$  of  $C(\mathbb{R})$ .*

*Proof.* This is [29, Proposition 4.2] when  $C(\mathbb{R}) \neq \emptyset$  or when  $C(\mathbb{R}) = \emptyset$  and  $\frac{1}{2}(\deg f - 2)$  is even, and [15, Lemma 2.2.3] otherwise.  $\square$

To be able to count the required points in the kernel it is convenient to construct the following graph. We write  $(X_1)_{-1}, (X_2)_{-1}, (X_0)_{-1}$  for the quadratic twists of  $X_1, X_2, X_0$  by  $-1$  respectively.

**Definition 8.4.8.** Let  $\mathcal{G} = (V, E)$  be a coloured graphed where:  $V = \mathcal{R}_{f_1 f_2} \cap \mathbb{R}$  with roots of  $f_1, f_2$  coloured red, blue respectively, and edges in  $E$  determined by the following rules

- there is a red edge between two red roots precisely when they correspond to points on the same connected component of  $(X_1)_{-1}$ ,
- there is a blue edge between two blue roots precisely when they correspond to points on the same connected component of  $(X_2)_{-1}$ ,
- there is a black edge between any two roots corresponding to points on the same connected component of  $(X_0)_{-1}$ .

Write  $\mathcal{Y}$  for the collection of connected subsets of  $\mathcal{G}$  (i.e.  $\Gamma \subseteq V$  such that  $x \in \Gamma \Rightarrow$  all neighbours of  $x \in \Gamma$ ) and  $n_{\mathcal{G}}$  for the number of connected components of  $\mathcal{G}$ .

Suppose that  $\mathcal{R}_{f_1 f_2} \subset \mathbb{R}$ . Then there's a one-to-one correspondence

$$\mathcal{Y}/\text{complements} \longleftrightarrow \ker \phi_{-1}|_{\text{Jac}_{(X_1)_{-1}} \times \text{Jac}_{(X_2)_{-1}} \times \text{Jac}_{(X_0)_{-1}}(\mathbb{R})^\circ}$$

where for  $\Gamma \subseteq V$  a connected subset of  $\mathcal{G}$ , we write  $\Gamma \sim V \setminus \Gamma$  and  $\mathcal{Y}/\text{complements} := \mathcal{Y}/\sim$ .

In particular, let  $\Gamma = S \cup T \in \mathcal{Y}/\text{complements}$  where  $S \subseteq \mathcal{R}_{f_1}$ ,  $T \subseteq \mathcal{R}_{f_2}$ . Without loss of generality we may assume that  $S, T$  have even size ( $\#S \cup T$  is even when  $\deg f_1 f_2$  is even, and so if  $\#S, \#T$  are odd then replace  $\Gamma$  by  $V \setminus \Gamma$ ; when  $\deg f_1$  is even and  $\deg f_2$  is odd then  $\#S$  is even, if  $\#T$  is odd then replace  $\Gamma$  by  $V \setminus \Gamma$ ). Then

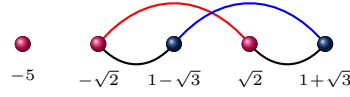
$$\Gamma \longmapsto (D_S, D_T, D_{S \cup T}), \quad \emptyset \longmapsto 0.$$

Conversely, let  $P = (D_S, D_T, D_{S \cup T}) \in \ker \phi_{-1}|_{\text{Jac}_{(X_1)_{-1}} \times \text{Jac}_{(X_2)_{-1}} \times \text{Jac}_{(X_0)_{-1}}(\mathbb{R})^\circ}$  for even sized subsets  $S \subseteq \mathcal{R}_{f_1}$ ,  $T \subseteq \mathcal{R}_{f_2}$ . Then

$$P \longmapsto S \cup T.$$

**Example 8.4.9.** Let  $f_1(x) = (x^2 - 2)(x + 5)$  and  $f_2(x) = (x - 1)^2 - 3$ , then we can construct the graph  $\mathcal{G}$  (Figure 8.2).

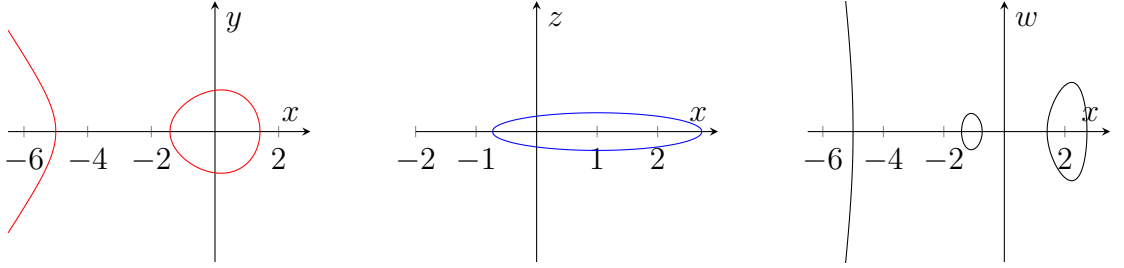
Using the correspondence detailed above, we observe that there are only two points in  $\ker \phi_{-1}$  belonging to  $\text{Jac}_{(X_1)_{-1}} \times \text{Jac}_{(X_2)_{-1}} \times \text{Jac}_{(X_0)_{-1}}(\mathbb{R})^\circ$ . In particu-



**Figure 8.2:** The graph  $\mathcal{G}$  when  $f_1(x) = (x^2 - 2)(x + 5)$ ,  $f_2(x) = (x - 1)^2 - 3$ .

lar, writing  $\mathcal{Y}/\text{complements} = \{\emptyset, \Gamma\}$  where  $\Gamma$  denotes the rightmost connected component of  $\mathcal{G}$ , these are  $(0, 0, 0)$  corresponding to  $\emptyset$  and  $(D_S, 0, D_{S \cup \mathcal{R}_{f_2}})$  with  $S = \{-\sqrt{2}, \sqrt{2}\}$  corresponding to  $\Gamma$ .

This can also be seen directly, using that  $\ker \phi_{-1}$  is as given in Example 3.3.8, alongside Lemma 8.4.7 and the following plots of  $(X_1)_{-1}$ ,  $(X_2)_{-1}$  and  $(X_0)_{-1}$  over  $\mathbb{R}$  (Figure 8.3).



**Figure 8.3:** The curves  $y^2 = -f_1(x)$ ,  $z^2 = -f_2(x)$ ,  $w^2 = -f_1(x)f_2(x)$  when  $f_1(x) = (x^2 - 2)(x + 5)$ ,  $f_2(x) = (x - 1)^2 - 3$ .

Note that if  $f_1(x) = (x^2 - 2)(x + 5)(x^2 + 1)$ , then Lemma 8.4.7 indicates that 4 elements of  $\ker \phi_{-1}$  belong to  $\text{Jac}_{(X_1)_{-1}} \times \text{Jac}_{(X_2)_{-1}} \times \text{Jac}_{(X_0)_{-1}}(\mathbb{R})^\circ$ . These are  $(0, 0, 0)$  and  $(D_S, 0, D_{S \cup \mathcal{R}_{f_2}})$  for  $S = \{-\sqrt{2}, \sqrt{2}\}$ ,  $\{-i, i\}$  and  $\{-\sqrt{2}, \sqrt{2}, -i, i\}$ . However, the graph  $\mathcal{G}$  remains unchanged.

**Lemma 8.4.10.** *Let  $\mathcal{K} \cong \mathbb{R}$  and suppose that  $f_1(x)$ ,  $f_2(x)$  are monic with  $a_1$ ,  $a_2$  pairs of complex conjugate roots respectively. Let  $\mathcal{G}$  be the graph constructed in Definition 8.4.8. Then*

$$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)} w_{\mathcal{K}}(\text{Jac}_{X_1}) w_{\mathcal{K}}(\text{Jac}_{X_2}) w_{\mathcal{K}}(\text{Jac}_{X_0}) = (-1)^{n_{\mathcal{G}} - 1 + a_1 + a_2}.$$

*Proof.* By assumption,  $X_1(\mathcal{K})$ ,  $X_2(\mathcal{K})$ ,  $X_0(\mathcal{K})$ ,  $X(\mathcal{K}) \neq \emptyset$  and so  $\mu = 1$  for each curve. Therefore, writing  $A = \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$  and applying Lemma 8.4.5, the

lefthand-side is precisely

$$(-1)^{\text{ord}_2 \# \ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ}}.$$

Suppose that  $\mathcal{R}_{f_1 f_2} \cap \mathbb{R} \neq \emptyset$ . When  $\mathcal{R}_{f_1 f_2} \subset \mathbb{R}$  (i.e.  $a_1 = a_2 = 0$ ), by construction there is a one-to-one map between  $\ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ}$  and the collection of connected subsets of  $\mathcal{G}$ , up to complements. Therefore  $\# \ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ} = 2^{n_{\mathcal{G}}-1}$ . When  $f_1(x)f_2(x)$  has complex roots,  $\mathcal{G}$  only accounts for the points of  $\ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ}$  corresponding to subsets of real roots. The remaining elements are constructed by appending all possible collections of pairs of complex conjugate roots (as in Example 8.4.9), giving that  $\# \ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ} = 2^{n_{\mathcal{G}}-1+a_1+a_2}$ .

Now suppose that  $\mathcal{R}_{f_1 f_2} \cap \mathbb{R} = \emptyset$ , i.e.  $n_1 = 2a_1$ ,  $n_2 = 2a_2$  (where  $n_1, n_2$  are the degrees of  $f_1, f_2$ ) and  $n_{\mathcal{G}} = 0$ . Then, by Lemma 8.4.7, there is a two-to-one correspondence between elements of  $\ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ}$  and even sized subsets  $S \subseteq \mathcal{R}_{f_1}, T \subseteq \mathcal{R}_{f_2}$  which are closed under conjugation, up to complements. Therefore,  $\# \ker \phi_{-1}|_{A_{-1}(\mathbb{R})^\circ} = 2^{a_1-1+a_2-1+1} = 2^{-1+a_1+a_2}$ .  $\square$

**Lemma 8.4.11.** *Let  $\mathcal{G}$  be the graph constructed in Definition 8.4.8. Then*

$$n_{\mathcal{G}} \equiv \sum_{i+j \equiv n_1+n_2+1 \pmod{2}} \mathbf{1}_{\alpha_i < \beta_j} + \begin{cases} \frac{1}{2}(n_1 + n_2(n_2 + 1)) - (a_1 + a_2) & n_1 \text{ even} \\ \frac{1}{2}(n_1 + 1) - a_1 & n_1 \text{ odd} \end{cases} \pmod{2}$$

using the notation fixed in 8.4.3.

*Proof.* First suppose that  $n_1$  is even. If  $\beta_{n_2-2a_2} < \alpha_1$  then the connected components of  $\mathcal{G}$  are  $\{\alpha_{2i+1}, \alpha_{2i+2}\}, \{\beta_{2j+1}, \beta_{2j+2}\}$  when  $n_2$  is even, and  $\{\alpha_{2i+1}, \alpha_{2i+2}\}, \{\beta_1\}, \{\beta_{2j+2}, \beta_{2j+3}\}$  when  $n_2$  is odd. Therefore  $n_{\mathcal{G}} = \frac{n_1}{2} + \lceil \frac{n_2}{2} \rceil - (a_1 + a_2)$ .

If  $\alpha_1 \in (\beta_{n_2-2a_2-2i}, \beta_{n_2-2a_2-2i+2}), \alpha_2 \in (\beta_{n_2-2a_2-2k-1}, \beta_{n_2-2a_2-2k+1})$  and  $\beta_{n_2-2a_2} < \alpha_3$  then  $\{\alpha_1, \alpha_2, \beta_{n_2-2a_2-2i+1}, \dots, \beta_{n_2-2a_2-2k}\}$  is now a connected component. Since the other connected components are those listed above,

$$\begin{aligned} n_{\mathcal{G}} &= \frac{n_1}{2} + \left\lceil \frac{n_2}{2} \right\rceil - (a_1 + a_2) - i + k \\ &\equiv \frac{1}{2}(n_1 + n_2(n_2 + 1)) - (a_1 + a_2) + \sum_{i+j \equiv n_2+1} \mathbf{1}_{\alpha_i < \beta_j} \pmod{2}. \end{aligned}$$

Relaxing the condition that  $\beta_{n_2-2a_2} < \alpha_3$ , we see that each pair  $\{\alpha_{2l+1}, \alpha_{2l+2}\}$  behaves like  $\{\alpha_1, \alpha_2\}$ . This gives the required formula.

Now suppose that  $n_1$  is odd. If  $\beta_{n_2-2a_2} < \alpha_1$  then the connected components of  $\mathcal{G}$  are  $\{\beta_1, \dots, \beta_{n_2-2a_2}, \alpha_1\}$  and  $\{\alpha_{2i+2}, \alpha_{2i+3}\}$ . Therefore  $n_{\mathcal{G}} = \frac{n_1+1}{2} - a_1$ .

Relaxing the condition that  $\beta_{n_2-2a_2} < \alpha_1$ , we see that pairs  $\{\alpha_{2l+2}, \alpha_{2l+3}\}$  behave like the pair  $\{\alpha_1, \alpha_2\}$  in the case when  $n_1$  is even. This gives rise to the required expression, namely

$$n_{\mathcal{G}} \equiv \frac{1}{2}(n_1 + 1) - a_1 + \sum_{i+j \equiv n_2} \mathbb{1}_{\alpha_i < \beta_j} \pmod{2}. \quad \square$$

**Proposition 8.4.12.** *Theorem 8.3.10 holds when  $\mathcal{K} \cong \mathbb{R}$ .*

*Proof.* Combining Corollary 8.4.4 and Lemma 8.4.10, it remains to show that

$$\begin{aligned} \left\lceil \frac{(n_1 - 1)(n_2 - 1)}{2} \right\rceil + \frac{1}{2}n_1(n_2(1 - n_1) + 2a_2) + \sum_{i+j \equiv n_1+n_2+1 \pmod{2}} \mathbb{1}_{\alpha_i < \beta_j} \\ \equiv n_{\mathcal{G}} - 1 + a_1 + a_2 \pmod{2}. \end{aligned}$$

This is an easy check using the expression for  $n_{\mathcal{G}} \pmod{2}$  given in Lemma 8.4.11.  $\square$

## 8.4.2 Proof over non-Archimedean fields for nice reduction types

We now consider non-Archimedean local fields, beginning by proving that Theorem 8.3.10 holds when  $\mathcal{K}/\mathbb{Q}_p$  is a finite extension for an odd prime  $p$  and the reduction of  $f_1(x)f_2(x)$  has at worst one double root.

We write  $\pi$  for a fixed choice of uniformiser of  $\mathcal{K}$  and  $v$  for a normalised valuation on  $\overline{\mathcal{K}}$ , i.e.  $v(\pi) = 1$ .

As before, we first consider the term  $H_{\mathcal{K}}(f_1, f_2)$ .

**Lemma 8.4.13.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and let  $T = \{r_1, r_2, s\} \in \mathcal{T}$*

satisfy  $v(r_2 - s) = 0$ . Then  $H_{\mathcal{K}}(T)$  equals

$$\begin{cases} +1 & \text{if } v(r_1 - r_2), v(r_1 - s) = 0, \\ \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r_2)/\mathcal{K}}} \left( \frac{1}{2}(r_1 + s) - \sigma(r_2) \right), \pi \right)_{\mathcal{K}}^d & \text{if } v(r_1 - r_2) = 0, v(r_1 - s) = d, \\ \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(s)/\mathcal{K}}} \left( \frac{1}{2}(r_1 + r_2) - \sigma(s) \right), \pi \right)_{\mathcal{K}}^d & \text{if } v(r_1 - r_2) = \frac{d}{2}, v(r_1 - s) = 0. \end{cases}$$

*Proof.* Write  $\mathcal{L} = \mathcal{K}(T)$  and let  $\pi_{\mathcal{L}}$  denote a fixed choice of uniformizer for  $\mathcal{L}$ .

Case 1. Both  $-(r_1 - s)(r_2 - s)$ ,  $(r_1 - r_2)^2$  are units in  $\mathcal{L}$ . If  $\frac{1}{2}(r_1 + r_2) - s$  is also a unit, then clearly  $H_1(T) = H_2(T) = +1$ . Else,  $H_1(T)H_2(T) = \left( \frac{1}{2}(r_1 + r_2) - s, -(r_1 - s)(r_2 - s)(r_1 - r_2)^2 \right)_{\mathcal{L}}$  where  $-(r_1 - s)(r_2 - s)(r_1 - r_2)^2 \equiv \frac{1}{4}(r_1 - r_2)^4 \pmod{\pi_{\mathcal{L}}}$ , i.e. the second entry is a square.

Case 2.  $\mathcal{L} = \mathcal{K}(r_2)$  and both  $\frac{1}{2}(r_1 + r_2) - s$ ,  $(r_1 - r_2)^2$  are units in  $\mathcal{L}$ , therefore  $H_2(T) = +1$ . By Lemma 2.7.5(ii),  $H_1(T) = (2s - (r_1 + r_2), \pi)_{\mathcal{L}}^d = \left( \prod_{\sigma \in \text{Gal}_{\mathcal{L}/\mathcal{K}}} \sigma(2s - r_1 - r_2), \pi \right)_{\mathcal{K}}^d$  and the result follows using that  $\sigma(2s - r_1) = 2s - r_1 \equiv \frac{1}{2}(r_1 + s) \pmod{\pi}$  for each  $\sigma \in \text{Gal}_{\mathcal{L}/\mathcal{K}}$ .

Case 3.  $\mathcal{L} = \mathcal{K}(s)$  and both  $\frac{1}{2}(r_1 + r_2) - s$ ,  $-(r_1 - s)(r_2 - s)$  are units in  $\mathcal{L}$ , therefore  $H_1(T) = +1$ . By Lemma 2.7.5(ii),  $H_2(T) = \left( \frac{1}{2}(r_1 + r_2) - s, \pi \right)_{\mathcal{L}}^d = \left( \prod_{\sigma \in \text{Gal}_{\mathcal{L}/\mathcal{K}}} \sigma\left(\frac{1}{2}(r_1 + r_2) - s\right), \pi \right)_{\mathcal{K}}^d$  and the result follows using that  $r_1 + r_2 \in \mathcal{K}$ .  $\square$

**Lemma 8.4.14.** Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and suppose that  $\Sigma_{X_0/\mathcal{K}} =$

$\langle \circ \circ \rangle_d \cdots \langle \bullet \bullet \rangle \cdots \langle \diamond \diamond \rangle_0$  where the twin is given by  $\mathbf{t} = \{r, s\}$  with  $r \in \mathcal{R}_{f_1}$ ,  $s \in \mathcal{R}_{f_2}$ . Then


$$H_{\mathcal{K}}(f_1, f_2) = \left( \frac{f_1(x)f_2(x)}{(x-r)(x-s)} \Big|_{x=\frac{1}{2}(r+s)}, \pi \right)_{\mathcal{K}}^d.$$

*Proof.* By Lemma 8.4.13, triples  $\mathbf{t} \notin T \in \mathcal{T}$  contribute trivially to  $H_{\mathcal{K}}$ . All remaining

triples are of the second type detailed in Lemma 8.4.13, thus

$$\begin{aligned}
H_{\mathcal{K}}(f_1, f_2) &= \prod_{r' \in (\mathcal{R}_{f_1} - \{r\})/G_{\mathcal{K}}} H_{\mathcal{K}}(\{r, r', s\}) \prod_{s' \in (\mathcal{R}_{f_2} - \{s\})/G_{\mathcal{K}}} H_{\mathcal{K}}(\{s, s', r\}) \\
&= \left( \prod_{\substack{r' \in (\mathcal{R}_{f_1} - \{r\})/G_{\mathcal{K}} \\ \sigma \in \text{Gal}_{\mathcal{K}(r')/\mathcal{K}}} \left(\frac{1}{2}(r+s) - \sigma(r')\right) \prod_{\substack{s' \in (\mathcal{R}_{f_2} - \{s\})/G_{\mathcal{K}} \\ \sigma \in \text{Gal}_{\mathcal{K}(s')/\mathcal{K}}} \left(\frac{1}{2}(r+s) - \sigma(s')\right), \pi \right)_{\mathcal{K}}^d \\
&= \left( \prod_{z \in \mathcal{R}_{f_1 f_2} - \mathfrak{t}} \left(\frac{1}{2}(r+s) - z\right), \pi \right)_{\mathcal{K}}^d. \quad \square
\end{aligned}$$

**Lemma 8.4.15.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and suppose that  $\Sigma_{X_0/\mathcal{K}} =$*

 where the twin is given by  $\mathfrak{t} = \{r_1, r_2\} \subseteq \mathcal{R}_{f_1}$ . Then

$$H_{\mathcal{K}}(f_1, f_2) = \left( f_2 \left( \frac{1}{2}(r_1 + r_2) \right), \pi \right)_{\mathcal{K}}^d.$$

Similarly upon replacing  $f_1$  by  $f_2$ .

*Proof.* By Lemma 8.4.13, triples  $\mathfrak{t} \notin T \in \mathcal{T}$  contribute trivially to  $H_{\mathcal{K}}$ . All remaining triples are of the third type detailed in Lemma 8.4.13, thus

$$\begin{aligned}
H_{\mathcal{K}}(f_1, f_2) &= \prod_{s \in \mathcal{R}_{f_2}/G_{\mathcal{K}}} H_{\mathcal{K}}(\{r_1, r_2, s\}) \\
&= \left( \prod_{\substack{s \in \mathcal{R}_{f_2}/G_{\mathcal{K}} \\ \sigma \in \text{Gal}_{\mathcal{K}(s)/\mathcal{K}}} \left(\frac{1}{2}(r_1 + r_2) - \sigma(s)\right), \pi \right)_{\mathcal{K}}^d \\
&= \left( \prod_{s \in \mathcal{R}_{f_2}} \left(\frac{1}{2}(r_1 + r_2) - s\right), \pi \right)_{\mathcal{K}}^d. \quad \square
\end{aligned}$$

Recall that when  $\mathcal{K}/\mathbb{Q}_p$  is finite and  $p \neq 2$ ,

$$\lambda_{\mathcal{K}}(f_1, f_2) = \frac{c_{\mathcal{K}}(\text{Jac}_{X_1})c_{\mathcal{K}}(\text{Jac}_{X_2})c_{\mathcal{K}}(\text{Jac}_{X_0})}{c_{\mathcal{K}}(\text{Jac}_X)} \frac{\mu_{\mathcal{K}}(X_1)\mu_{\mathcal{K}}(X_2)\mu_{\mathcal{K}}(X_0)}{\mu_{\mathcal{K}}(X)}.$$

**Proposition 8.4.16.** *Theorem 8.3.10 holds when  $\mathcal{K}/\mathbb{Q}_p$  is finite for  $p \neq 2$  and the reduction of  $f_1(x)f_2(x)$  has at worst one double root.*



*Proof.* Without loss of generality, we assume that  $X_2$  has good reduction so that  $c_{\mathcal{K}}(\text{Jac}_{X_2}) = 1$ ,  $\mu_{\mathcal{K}}(X_2) = 1$  and  $w_{\mathcal{K}}(\text{Jac}_{X_2}) = +1$ . Since  $(-1, -1)_{\mathcal{K}} = +1$ , it remains to prove that

$$H_{\mathcal{K}}(f_1, f_2) = (-1)^{\text{ord}_2 \frac{c_{\mathcal{K}}(\text{Jac}_{X_1})c_{\mathcal{K}}(\text{Jac}_{X_0})\mu_{\mathcal{K}}(X_1)\mu_{\mathcal{K}}(X_0)}{c_{\mathcal{K}}(\text{Jac}_X)\mu_{\mathcal{K}}(X)}} w_{\mathcal{K}}(\text{Jac}_{X_1})w_{\mathcal{K}}(\text{Jac}_{X_0}).$$

The inputs of Table 8.1 (columns 1 and 2) are the possible non-trivial clusters belonging to  $\Sigma_{\text{Jac}_{X_1}}$  and  $\Sigma_{\text{Jac}_X}^{\text{chr}}$  (or ignoring the colouring,  $\Sigma_{\text{Jac}_{X_0}}$ ), where the roots of  $f_1$  and  $f_2$  are denoted by red circles ( $\bullet$ ) and blue diamonds ( $\blacklozenge$ ) respectively.

Column 3 gives the dual graph of the minimal regular model of  $X/\mathcal{K}$ , denoted  $\Upsilon_X$ , where an arrow is used to indicate the action of Frobenius. This is determined using Theorem 2.4.14 (note that  $B = X$ ).

Columns 4 and 5 list the Tamagawa numbers for  $\text{Jac}_{X_1}$  and  $\text{Jac}_{X_0}$ , calculated from their respective cluster pictures using Theorem 2.4.9 (or from the cluster picture of the Jacobian as given in Table 6.2 if either  $\deg f_1$  or  $\deg f_1 + \deg f_2 = 4$ ).

Similarly, column 6 contains the Tamagawa number for  $\text{Jac}_X$  but this time calculated from  $\Upsilon_X$  using Theorem 2.3.3.

Columns 7 and 8 keep track of the deficiency contribution from  $X_1$  and  $X_0$  using Theorem 2.4.11 (or, when  $X_1 : y^2 = x^2 + ax + b$ ,  $\mu(X_1) = +1$  since the points at infinity are defined over  $\mathcal{K}$ ).

Similarly, column 9 lists the deficiency contribution from  $X$  computed via [47, Lemma 6.11] or [53] (these results indicate that  $\mu$  is determined from  $\Upsilon$ , so we could instead identify a hyperelliptic curve  $C/\mathcal{K}$  such that  $\Upsilon_C = \Upsilon_X$  and then use Theorem 2.4.11).

Column 10 gives the value of  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)}$ .

Columns 11 and 12 list  $w_{\mathcal{K}}(\text{Jac}_{X_1})$  and  $w_{\mathcal{K}}(\text{Jac}_{X_0})$ , calculated using Theorem 2.3.5 or Theorem 2.4.10.

Column 13 displays the value of  $H_{\mathcal{K}}$ . For row 1, this is  $+1$  since all triples in  $\mathcal{T}$  are of the first type detailed in Lemma 8.4.13. For rows 2 and 3, we observe Lemma 8.4.14 and note that the first entry of the Hilbert symbol is a square precisely when the sign attached to  $\mathfrak{t}$  is  $+$  (c.f. Remark 2.4.7). Similarly for rows 4-7, we observe

		$\Upsilon_X$	$c(\text{Jac}_{X_1})$	$c(\text{Jac}_{X_0})$	$c(\text{Jac}_X)$	$\mu(X_1)$	$\mu(X_0)$	$\mu(X)$	$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)}$	$w_{\mathcal{K}}(\text{Jac}_{X_1})$	$w_{\mathcal{K}}(\text{Jac}_{X_0})$	$H_{\mathcal{K}}(f_1, f_2)$
When $\Sigma_{X_1} \neq \textcircled{\bullet} \textcircled{\bullet} \textcircled{\bullet}$ with $d \neq 0$												
$\emptyset$	$\emptyset$		1	1	1	1	1	1	+1	+1	+1	+1
$\emptyset$	$\emptyset$		1	2d	d	1	1	1	-1	+1	-1	+1
$\emptyset$	$\emptyset$		1	2	$\tilde{d}$	1	1	1	$(-1)^d$	+1	+1	$(-1)^d$
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		d	d	$d^2$	1	1	1	+1	-1	-1	+1
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		$\tilde{d}$	d	d	1	1	1	$(-1)^{d+1}$	+1	-1	$(-1)^d$
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		d	$\tilde{d}$	d	1	1	1	$(-1)^{d+1}$	-1	+1	$(-1)^d$
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		$\tilde{d}$	$\tilde{d}$	$(\tilde{d})^2$	1	1	1	+1	+1	+1	+1
When $\Sigma_{X_1} = \textcircled{\bullet} \textcircled{\bullet} \textcircled{\bullet}$ and $d \neq 0$												
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		1	d	2d	1	1	1	-1	+1	-1	+1
$\textcircled{\bullet} \textcircled{\bullet}$	$\textcircled{\bullet} \textcircled{\bullet}$		1	$\tilde{d}$	2	1	1	1	$(-1)^d$	+1	+1	$(-1)^d$

Notation:  $\tilde{d} = \text{gcd}(2, d)$ .

Table 8.1: Data for Proposition 8.4.16

Lemma 8.4.15 and note that the first entry of the Hilbert symbol is a square precisely when the sign attached to  $\mathfrak{t}$  in each cluster picture is the same (c.f. Remark 2.4.7).  $\square$

Having now dealt with Theorem 8.3.10 when  $\mathcal{K}$  is non-Archimedean of odd residue characteristic, we turn our attention to what happens when  $\mathcal{K}/\mathbb{Q}_2$  and  $X_1, X_2, X_0$  have cluster pictures

$$\begin{aligned} \Sigma_{X_1} &= \left( \overset{\circ}{\circ} \overset{\circ}{\circ} \cdots \overset{\circ}{\circ} \right)_0, & \Sigma_{X_2} &= \left( \overset{\circ}{\circ} \overset{\circ}{\circ} \cdots \overset{\circ}{\circ} \right)_0, \\ \Sigma_{X_0} &= \left( \overset{\circ}{\circ} \cdots \overset{\circ}{\circ} \overset{\circ}{\circ} \cdots \overset{\circ}{\circ} \right)_0. \end{aligned}$$

**Lemma 8.4.17.** *Let  $\mathcal{K}/\mathbb{Q}_2$  be finite,  $r_1 \neq r_2 \in \mathcal{R}_{f_1}$  and  $s, s' \in \mathcal{R}_{f_2}$  satisfy  $v(s - s') = v(4)$ . If  $T = \{r_1, r_2, s\}$ ,  $T' = \{r_1, r_2, s'\}$  are not  $G_{\mathcal{K}}$ -conjugate, then  $H_1(T)H_1(T') = H_2(T)H_2(T') = +1$ . Similarly, upon swapping the roles of  $f_1, f_2$ .*

*Proof.* Write  $\mathcal{L} := \mathcal{K}(T) = \mathcal{K}(T')$  and  $s - s' = 4t$  where  $t \in \mathcal{O}_{\mathcal{L}}^{\times}$ . We will repeatedly use the Hilbert symbol identity given in Lemma 2.7.6 and the fact that  $1 + 8x = \square$  whenever  $x \in \mathcal{O}_{\mathcal{L}}^{\times}$ .

Suppose that  $v(r_1 - r_2) = v(4)$ . Then  $u := \frac{1}{2}(r_1 + r_2) - s \in \mathcal{O}_{\mathcal{L}}^{\times}$  and  $H_2(T)H_2(T') = (u, (r_1 - r_2)^2)_{\mathcal{L}}(u + 4t, (r_1 - r_2)^2)_{\mathcal{L}} = (u^2(1 + 4tu^{-1}), (r_1 - r_2)^2)_{\mathcal{L}} = +1$ . Now write  $v := -(r_1 - s)(r_2 - s) \in \mathcal{O}_{\mathcal{L}}^{\times}$ , then  $H_1(T)H_1(T') = (-2u, v)_{\mathcal{L}}(-2(u + 4t), v(1 - 8tv^{-1}(u + 2t)))_{\mathcal{L}} = (4u^2(1 + 4tu^{-1}), v)_{\mathcal{L}} = +1$ .

Instead suppose that  $v(r_1 - r_2) = 0$  then  $u := r_1 + r_2 - 2s \in \mathcal{O}_{\mathcal{L}}^{\times}$  and  $H_2(T)H_2(T') = (\frac{1}{2}u, (r_1 - r_2)^2)_{\mathcal{L}}(\frac{1}{2}(u + 8t), (r_1 - r_2)^2)_{\mathcal{L}} = (u^2(1 + 8tu^{-1}), (r_1 - r_2)^2)_{\mathcal{L}} = +1$ . With  $v$  as before,  $H_1(T)H_1(T') = (-u, v)_{\mathcal{L}}(-u(1 + 8tu^{-1}), v(1 - 4tv^{-1}(u + 4t)))_{\mathcal{L}} = +1$ .  $\square$

**Lemma 8.4.18.** *Let  $\mathcal{K}/\mathbb{Q}_2$  be finite,  $r_1 \neq r_2 \in \mathcal{R}_{f_1}$  and  $s, s' \in \mathcal{R}_{f_2}$  satisfy  $v(s - s') = v(4)$ . If  $T = \{r_1, r_2, s\}$ ,  $T' = \{r_1, r_2, s'\}$  are  $G_{\mathcal{K}}$ -conjugate, then  $H_1(T) = H_2(T) = +1$ . Similarly, upon swapping the roles of  $f_1, f_2$ .*

*Proof.* Write  $\mathcal{L} := \mathcal{K}(T)$  and  $\mathcal{L}_0 := \mathcal{K}(ss', s + s', r_1r_2, r_1 + r_2)$  where  $[\mathcal{L} : \mathcal{L}_0] = 2$  (since  $s \notin \mathcal{L}_0$ ). Write  $s - s' = 4t$  where  $t \in \mathcal{O}_{\mathcal{L}}^{\times}$  and note that  $t^2 \in \mathcal{L}_0$ . Let  $z := \frac{1}{2}(r_1 + r_2) - \frac{1}{2}(s + s') \in \mathcal{L}_0$ . Either  $z$  is a unit (when  $v(r_1 - r_2) = v(4)$ ) or

$2z$  is a unit (when  $v(r_1 - r_2) = 0$ ). In both cases,  $H_2(T) = (z - 2t, (r_1 - r_2)^2)_{\mathcal{L}} = (z^2(1 - 4t^2z^{-2}), (r_1 - r_2)^2)_{\mathcal{L}_0} = +1$  since  $(r_1 - r_2)^2 \in \mathcal{L}_0$ .

Suppose that  $z$  is a unit, i.e.  $r_1 - r_2 = 4v$  for  $v \in \mathcal{O}_{\mathcal{L}}^{\times}$  with  $v^2 \in \mathcal{L}_0$ . Then  $(r_1 - s)(r_2 - s) = (z - 2t)^2 - 4v^2$  and

$$\begin{aligned} H_1(T) &= (-2(z - 2t), -(z - 2t)^2(1 - 4v^2(z - 2t)^{-2}))_{\mathcal{L}} \\ &= (-2(z - 2t), -1)_{\mathcal{L}}(2, 1 - 4v^2(z - 2t)^{-2})_{\mathcal{L}} \\ &= (4z^2(1 - 4t^2z^{-2}), -1)_{\mathcal{L}_0}(2, 1 - 8v^2(z^2 - 4t^2)^{-2}(z^2 + 4t^2) + 16v^4(z^2 - 4t^2)^{-2})_{\mathcal{L}_0} \\ &= +1 \end{aligned}$$

having used Lemma 2.7.5(ii).

Suppose instead that  $2z$  is a unit. Then

$$\begin{aligned} H_1(T) &= (-2z(1 - 4t(2z)^{-1}), -(r_1 - s)(r_2 - s))_{\mathcal{L}} \\ &= (-2z, -(r_1 - s)(r_2 - s))_{\mathcal{L}} \\ &= (-2z, (r_1 - s)(r_2 - s)(r_1 - s')(r_2 - s'))_{\mathcal{L}_0} \end{aligned}$$

having used Lemma 2.7.5(ii). Since  $(r_1 - s)(r_1 - s') = (r_1 - \frac{1}{2}(s + s'))^2 - 4t^2$  and similarly for  $(r_2 - s)(r_2 - s')$ , we see that the right-hand entry can be replaced by  $(r_1 - \frac{1}{2}(s + s'))^2(r_2 - \frac{1}{2}(s + s'))^2$  which is a square in  $\mathcal{L}_0$ . Therefore  $H_1(T) = +1$ .  $\square$

**Corollary 8.4.19.** *Let  $\mathcal{K}/\mathbb{Q}_2$  be finite and  $X_1, X_2, X_0$  be as in Theorem 8.3.10. Then  $H_{\mathcal{K}}(f_1, f_2) = +1$ .*

*Proof.* This is immediate from Lemmata 8.4.17 and 8.4.18.  $\square$

**Lemma 8.4.20.** *Let  $\mathcal{K}/\mathbb{Q}_2$  be a finite extension and  $X_1, X_2, X_0$  be as in Theorem 8.3.10. Then*

$$\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2) \equiv [\mathcal{K} : \mathbb{Q}_2] \left( \frac{1}{2}(\deg f_1 + \deg f_2) - 1 \right) \pmod{2}.$$

*Proof.* We first note that  $\mu_{\mathcal{K}} = 1$  for all curves since they are assumed to have good

reduction. By Lemma 4.2.5 and [24, Theorem A.1] with  $A = \text{Jac}_{X_1} \times \text{Jac}_{X_2} \times \text{Jac}_{X_0}$ ,

$$\lambda_{\mathcal{K}}(f_1, f_2) = \frac{\#\ker \phi(\mathcal{K})}{\#\text{coker } \phi(\mathcal{K})} = 2^{-[\mathcal{K}:\mathbb{Q}_2] \dim_{\mathbb{F}_2}(A_1(\bar{\mathcal{K}})[2] \cap A(\bar{\mathcal{K}})[\phi])}$$

where the elements of  $A_1(\bar{\mathcal{K}})$  (the kernel of reduction on  $A$ ) are described in [25, Proposition 1.16]. In particular, using Notation 2.1.11 and writing  $T_1, T_2$  for the collections of twins in  $\Sigma_{X_1}, \Sigma_{X_2}$ ,

$$A_1(\bar{\mathcal{K}}) = \left\{ (D_{S_1}, D_{S_2}, D_{S_0}) : S_1 \in \mathcal{P}(T_1), S_2 \in \mathcal{P}(T_2), S_0 \in \mathcal{P}(T_1 \sqcup T_2) \right\}$$

where  $\mathcal{P}$  denotes the power set and we recall that  $D_S = D_{S^c}$ . By Lemma 3.3.7, such an element additionally belongs to  $A(\bar{\mathcal{K}})[\phi]$  when either  $S_0 = S_1 \cup S_2$  or  $(\mathcal{R}_{f_1} - S_1) \cup S_2$ . Therefore,  $\#(A_1(\bar{\mathcal{K}})[2] \cap A(\bar{\mathcal{K}})[\phi]) = 2^{\frac{\deg f_1}{2} + \frac{\deg f_2}{2} - 1}$  (i.e. twice the number of possible  $S_1$ , up to complements, times the number of possible  $S_2$ , up to complements) and the result follows.  $\square$

**Proposition 8.4.21.** *Theorem 8.3.10 holds when  $\mathcal{K}/\mathbb{Q}_2$  is finite and  $X_1, X_2, X_0$  have good ordinary reduction with*

$$\begin{aligned} \Sigma_{X_1} &= \left( \begin{array}{c} \textcircled{\text{red}}_{v(4)} \textcircled{\text{red}}_{v(4)} \cdots \textcircled{\text{red}}_{v(4)} \end{array} \right)_0, & \Sigma_{X_2} &= \left( \begin{array}{c} \textcircled{\text{blue}}_{v(4)} \textcircled{\text{blue}}_{v(4)} \cdots \textcircled{\text{blue}}_{v(4)} \end{array} \right)_0, \\ \Sigma_{X_0} &= \left( \begin{array}{c} \textcircled{\text{red}}_{v(4)} \cdots \textcircled{\text{red}}_{v(4)} \textcircled{\text{blue}}_{v(4)} \cdots \textcircled{\text{blue}}_{v(4)} \end{array} \right)_0. \end{aligned}$$

*Proof.* By assumption,  $w_{\mathcal{K}}(\text{Jac}_{X_1}) = w_{\mathcal{K}}(\text{Jac}_{X_2}) = w_{\mathcal{K}}(\text{Jac}_{X_0}) = +1$ . By Corollary 8.4.19,  $H_{\mathcal{K}}(f_1, f_2) = +1$ . Finally,

$$(-1, -1)_{\mathcal{K}}^{\lceil \frac{(\deg f_1 - 1)(\deg f_2 - 1)}{2} \rceil} = (-1)^{[\mathcal{K}:\mathbb{Q}_2] \frac{(\deg f_1 - 1)(\deg f_2 - 1) + 1}{2}} \stackrel{\text{Lem. 8.4.20}}{=} (-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_1, f_2)}$$

since  $\deg f_1, \deg f_2$  are even.  $\square$

## 8.5 Proof of Local Theorem IV

Throughout this section we assume the set up of Theorem 8.3.12. In particular,  $\mathcal{K}$  is a local field of characteristic 0,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  is a quadratic extension and  $f_0(x)$ ,

$\bar{f}_0(x) \in \mathcal{K}(\sqrt{\xi})[x]$  are monic,  $\text{Gal}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}}$ -conjugate of degree  $n = 2^m \geq 4$  such that  $f_0(x)\bar{f}_0(x)$  is separable and Assumption  $(\star)$  holds. We define hyperelliptic curves by

$$C_0/\mathcal{K}(\sqrt{\xi}) : y^2 = f_0(x), \quad C/\mathcal{K} : w^2 = f_0(x)\bar{f}_0(x),$$

and an additional curve by

$$X'/\mathcal{K} : u^4 - 2(f_0(x) + \bar{f}_0(x))u^2 + (f_0(x) - \bar{f}_0(x))^2 = 0.$$

### 8.5.1 Proof over Archimedean fields

As in §8.4, we first prove that Theorem 8.3.12 holds when  $\mathcal{K}$  is an Archimedean local field. Since  $\mathcal{K}(\xi)/\mathcal{K}$  is not a quadratic extension when  $\mathcal{K} \cong \mathbb{C}$ , we restrict our attention to  $\mathcal{K} \cong \mathbb{R}$  and  $\sqrt{\xi} \notin \mathbb{R}$ .

Recall that

$$\lambda_{\mathcal{K}}(f_0; \sqrt{\xi}) = \# \ker \phi|_{(\text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C)(\mathcal{K})^\circ} \frac{n_{\text{Jac}_C/\mathcal{K}} \mu_{\mathcal{K}}(C)}{n_{\text{Jac}_{X'}/\mathcal{K}} \mu_{\mathcal{K}}(X')}.$$

We first compute the contribution coming from the kernel of  $\phi$ , for which require the following analogue of Lemma 8.4.7.

**Lemma 8.5.1** (To appear in [46]). *Let  $f(x) \in \mathbb{R}[x]$  be monic, separable, have no real roots and such that  $\deg f \equiv 0 \pmod{4}$ . Define  $C : y^2 = f(x)$  and let  $S' \subseteq \mathcal{R}_f$  have even size. Then,  $D_{S'} \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if*

(1)  $S' = \bar{S}'$  and  $\#S' \equiv 0 \pmod{4}$ , or

(2)  $S' \sqcup \bar{S}' = \mathcal{R}_f$  and  $\#\{r \in S' : \text{Im}(r) < 0\} \equiv 0 \pmod{2}$ .

*Sketch proof.* We note that  $n_{C/\mathbb{R}} = n_{\text{Jac}_C/\mathbb{R}} = 2$  and write  $\mathfrak{c}^+$  (respectively,  $\mathfrak{c}^-$ ) for the connected component of  $C(\mathbb{R})$  consisting of points of the form  $(x, y)$  with  $y > 0$  (respectively,  $y < 0$ ) along with one of the points at infinity  $P_\infty^+$  (respectively,  $P_\infty^-$ ).

The result is a consequence of the following observations:

(i)  $D_{\{r, \bar{r}\}} \notin \text{Jac}_C(\mathbb{R})^\circ$  for all  $r \in \mathcal{R}_f$ , and

- (ii)  $D_{S'} \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if  $\#\{r \in S' : \text{Im}(r) < 0\} \equiv 0 \pmod{2}$  for some  $S' \subset \mathcal{R}_f$  such that  $S' \sqcup \bar{S}' = \mathcal{R}_f$ .

For (i), this is immediate from [29, Proposition 4.2] (i.e.  $D_S \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if  $\deg(D_S \cap \mathfrak{c}^\pm)$  are even).

For (ii), to be able to apply [29, Proposition 4.2] we first need to identify a divisor linearly equivalent to  $D_{S'}$  that is fixed by complex conjugation. Define  $f_1(x) = \prod_{r \in S'} (x - r)$  and write  $f_1(x) = g(x) + ih(x)$  for  $g(x), h(x) \in \mathbb{R}[x]$ . Then  $D_{S'} = \mathcal{D} \in \text{Jac}_C$  where

$$\mathcal{D} := - \sum_{\alpha \text{ root of } h(x)} [(\alpha, g(\alpha))] - (\tfrac{1}{4} \deg f - \deg h)[P_\infty^+] + \tfrac{1}{4} \deg f [P_\infty^-].$$

Since  $\mathcal{D}$  is fixed by complex conjugation,  $D_{S'} \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if  $\deg(\mathcal{D} \cap \mathfrak{c}^\pm)$  are even. We see that

$$\deg(\mathcal{D} \cap \mathfrak{c}^+) = -\deg(\mathcal{D} \cap \mathfrak{c}^-) = -\#\{\alpha : h(\alpha) = 0, g(\alpha) > 0\} - \tfrac{1}{4} \deg f + \deg h$$

and the right-hand-side is even if and only if

$$(-1)^{\frac{1}{4} \deg f} R_{g,h} > 0 \iff R_{f_1, \bar{f}_1} > 0 \iff \prod_{r \in S'} \text{Im}(r) > 0$$

using standard properties of the resultant. □

**Lemma 8.5.2.** *When  $\mathcal{K} \cong \mathbb{R}$ ,*

$$\#\ker \phi|_{(\text{Res}_{\mathcal{K}(\sqrt{\bar{\xi}})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C)(\mathcal{K})^\circ} = \begin{cases} 2^{\deg f_0 - 1} & \text{if } R_{f_0, \bar{f}_0} > 0, \\ 2^{\deg f_0 - 2} & \text{if } R_{f_0, \bar{f}_0} < 0, \end{cases}$$

where  $R_{f_0, \bar{f}_0}$  denotes the resultant of  $f_0, \bar{f}_0$ .

*Proof.* Using Lemma 8.2.4, we deduce that

$$\ker \phi(\mathcal{K}) = \left\{ ((D_S, D_{\bar{S}}), D_{S \cup \bar{S}}), ((D_S, D_{\bar{S}}), D_{(\mathcal{R}_{f_0 - S} \cup \bar{S})}) : S \subseteq \mathcal{R}_{f_0} \text{ has even size} \right\}.$$

Since  $n_{\text{Res}_{\mathcal{K}(\sqrt{\bar{\epsilon}})/\mathcal{K}} \text{Jac}_{C_0}/\mathcal{K}} = 1$ , we need only check when  $D_{S \cup \bar{S}}, D_{(\mathcal{R}_{f_0} - S) \cup \bar{S}} \in \text{Jac}_C(\mathbb{R})^\circ$ . By Lemma 8.5.1, the first is always on the identity component (since  $S$  has even size), and  $D_{(\mathcal{R}_{f_0} - S) \cup \bar{S}} \in \text{Jac}_C(\mathbb{R})^\circ$  if and only if

$$\begin{aligned} & \#\{r \in (\mathcal{R}_{f_0} - S) \cup \bar{S} : \text{Im}(r) < 0\} \\ & \equiv \#\{r \in (\mathcal{R}_{f_0} - S) : \text{Im}(r) < 0\} + \#\{r \in S : \text{Im}(r) > 0\} \\ & \equiv \#\{r \in \mathcal{R}_{f_0} : \text{Im}(r) < 0\} \\ & \equiv 0 \pmod{2}. \end{aligned}$$

Therefore,  $\#\{D_{(\mathcal{R}_{f_0} - S) \cup \bar{S}} \in \text{Jac}_C(\mathbb{R})^\circ\} = 2^{\deg f_0 - 2}$  if  $\#\{r \in \mathcal{R}_{f_0} : \text{Im}(r) < 0\}$  is even and 0 otherwise. In particular,

$$\#\ker \phi|_{(\text{Res}_{\mathcal{K}(\sqrt{\bar{\epsilon}})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C)(\mathcal{K})^\circ} = \begin{cases} 2^{\deg f_0 - 1} & \text{if } \prod_{r \in \mathcal{R}_{f_0}} \text{Im}(r) > 0, \\ 2^{\deg f_0 - 2} & \text{otherwise.} \end{cases}$$

The result then follows upon observing that  $R_{f_0, \bar{f}_0} = \prod_{r, s \in \mathcal{R}_{f_0}} (r - \bar{s}) \equiv (-1)^{\frac{\deg f_0}{2}} \prod_{r \in \mathcal{R}_{f_0}} (r - \bar{r}) \equiv \prod_{r \in \mathcal{R}_{f_0}} \text{Im}(r) \pmod{\mathbb{R}_{>0}^\times}$ .  $\square$

We now turn our attention to the curve  $X'$ . Let  $s(x), t(x) \in \mathbb{R}[x]$  be such that  $f_0(x) = s(x) + it(x)$  (since  $f_0$  is assumed monic, so is  $s(x)$  and  $\deg f_0 = \deg s > \deg t$ ), then

$$X' : u^4 - 4s(x)u^2 + 4t(x)^2 = 0.$$

Observe that  $X'(\mathbb{C}) = \{(x, u_{+,+}), (x, u_{+,-}), (x, u_{-,+}), (x, u_{-,-}) : x \in \mathbb{C}\}$  where

$$u_{\pm,+} := \pm \sqrt{2s(x) + 2\sqrt{s(x)^2 - t(x)^2}}, \quad u_{\pm,-} := \pm \sqrt{2s(x) - 2\sqrt{s(x)^2 - t(x)^2}},$$

define 4 distinct points unless  $t(x) = 0$  (then  $u_{+,-} = u_{-,-}$  when  $s(x) > 0$  and  $u_{+,+} = u_{-,+}$  when  $s(x) < 0$ ), or  $s(x)^2 = t(x)^2$  (then  $u_{+,+} = u_{+,-}$  and  $u_{-,+} = u_{-,-}$ ).

In particular, we have that

$$X'(\mathbb{R}) = \{(x, u_{+,+}), (x, u_{+,-}), (x, u_{-,+}), (x, u_{-,-}) : x \in \mathbb{R}, s(x) > 0, s(x)^2 \geq t(x)^2\}$$



and  $X'(\mathbb{R}) \neq \emptyset$  (since  $X'$  has real points as  $|x| \rightarrow \infty$ ), therefore  $\mu_{\mathbb{R}}(X') = 1$ . To visualise the behaviour of  $X'$  at infinity we view it via the following two models.

*Model 1.* Let  $v = 1/x$  and  $w = x^{\frac{1}{2} \deg s}/u$ . Then

$$X' : 1 - 4w^2(v^{\deg s}s(1/v)) + 4w^4v^{2(\deg s - \deg t)}(v^{\deg t}t(1/v))^2 = 0.$$

Fixing  $v = 0$  gives the smooth points  $(v, w) = (0, \pm 1/2)$ , which correspond to two of the points at infinity in the coordinates  $(x, u)$ . In particular, we see that points satisfying  $u/x^{\frac{1}{2} \deg s} \rightarrow 2$  as  $|x| \rightarrow \infty$  approach each other (these are  $(x, u_{+,+})$  as  $x \rightarrow \pm\infty$ ), and similarly for those satisfying  $u/x^{\frac{1}{2} \deg s} \rightarrow -2$  (these are  $(x, u_{-,+})$  as  $x \rightarrow \pm\infty$ ).

*Model 2.* Now let  $v = 1/x$  and  $w = x^{\deg t}/ux^{\frac{1}{2} \deg s}$ . Then

$$X' : v^{2(\deg s - \deg t)} - 4w^2(v^{\deg s}s(1/v)) + 4w^4(v^{\deg t}t(1/v))^2 = 0.$$

Fixing  $v = 0$  gives the smooth points  $(v, w) = (0, \pm 1/c_t)$  (where  $c_t$  is the lead coefficient of  $t(x)$ ), which correspond to the other two points at infinity in the coordinates  $(x, u)$ . In particular, we see that points satisfying  $ux^{\frac{1}{2} \deg s}/x^{\deg t} \rightarrow c_t$  as  $|x| \rightarrow \infty$  approach each other (assume that  $c_t > 0$ , these are  $(x, u_{+,-})$  as  $x \rightarrow \pm\infty$  when  $\deg t$  is even and  $(x, u_{+,-})$  as  $x \rightarrow +\infty$ ,  $(x, u_{-,-})$  as  $x \rightarrow -\infty$  when  $\deg t$  is odd), and similarly for those satisfying  $ux^{\frac{1}{2} \deg s}/x^{\deg t} \rightarrow -c_t$  (again assuming that  $c_t > 0$ , these are  $(x, u_{-,-})$  as  $x \rightarrow \pm\infty$  when  $\deg t$  is even and  $(x, u_{-,-})$  as  $x \rightarrow +\infty$ ,  $(x, u_{+,-})$  as  $x \rightarrow -\infty$  when  $\deg t$  is odd).

We use this to count the number of connected components of  $X'$  over  $\mathbb{R}$ .

**Remark 8.5.3.** We note that the given model for  $X'$  may be singular and that we must consider its desingularization when counting connected components.

**Lemma 8.5.4.** Fix a monic polynomial  $f_0(x) = s(x) + it(x)$  where  $s(x), t(x) \in \mathbb{R}[x]$ . Then,

$$n_{X'/\mathbb{R}} \equiv \#\{r \in \mathbb{R} : t(r) = 0, s(r) < 0\} \pmod{2}.$$

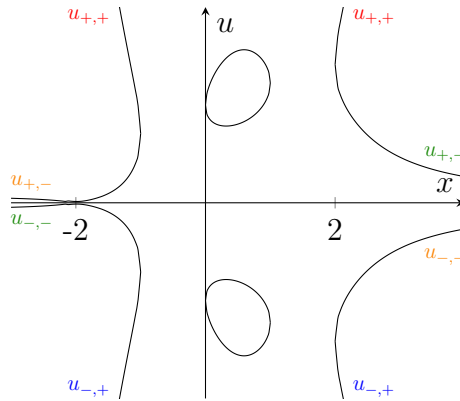
*Proof.* Suppose that  $s(x) > 0$  and  $s(x)^2 \geq t(x)^2$  if and only if  $x \in (-\infty, a] \cup I_1 \cup$

$\dots \cup I_m \cup [b, \infty)$  for  $(-\infty, a], I_1, \dots, I_m, [b, \infty) \subset \mathbb{R}$ . Write  $n_i$  ( $n_\infty$  respectively) for the number of connected components of  $X'$  over  $\mathbb{R}$  with  $x \in I_i$  ( $x \in (-\infty, a] \cup [b, \infty)$  respectively). Then  $n_{X'/\mathbb{R}} = n_\infty + n_1 + \dots + n_m$ . We observe that  $n_i = 2$  if  $\#\{r \in I_i : t(r) = 0\}$  is even and 1 otherwise. Additionally, the discussion about the behaviour of  $X'$  at infinity preceding this lemma allows us to deduce that  $n_\infty = 2$  if  $\deg t + \#\{r \in (-\infty, a] \cup [b, \infty) : t(r) = 0\}$  is even, and 1 otherwise (see Example 8.5.5). Therefore,

$$\begin{aligned} n_{X'/\mathbb{R}} &\equiv \deg t + \#\{r \in (-\infty, a] \cup [b, \infty) : t(r) = 0\} + \sum_{i=1}^m \#\{r \in I_i : t(r) = 0\} \\ &\equiv \deg t + \#\{r \in \mathbb{R} : t(r) = 0, s(r) > 0\} \\ &\equiv \#\{r \in \mathbb{R} : t(r) = 0, s(r) < 0\} \pmod{2}. \end{aligned} \quad \square$$

**Example 8.5.5.** Let  $f_0(x) = x^4 - 2x^3 - x^2 + (3 + i)x + 2(1 + i)$ , then  $s(x) = x^4 - 2x^3 - x^2 + 3x + 2$  and  $t(x) = x + 2$ .

Notice that  $X'$  has real points (i.e.  $s(x) > 0$  and  $s(x)^2 \geq t(x)^2$ ) whenever  $x \in (-\infty, -1] \cup [0, 1] \cup [2, \infty)$ . In particular, we have the following plot.



**Figure 8.4:** The curve  $X' : u^4 - 4(x^4 - 2x^3 - x^2 + 3x + 2)u^2 + 4(x^2 + 4x + 4) = 0$

Our earlier discussion indicates that  $u_{+,+}$  joins itself as  $x \rightarrow \pm\infty$  and similarly for  $u_{-,+}$ . Since  $\deg t$  is odd,  $u_{+,-}$  as  $x \rightarrow +\infty$  joins  $u_{-,-}$  as  $x \rightarrow -\infty$  and vice versa. (This is illustrated in Figure 8.4 by the colouring of the labels.) We therefore observe that  $n_{X'/\mathbb{R}} = 4$ .

**Corollary 8.5.6.** *Fix a monic polynomial  $f_0(x) = s(x) + it(x)$  where  $s(x), t(x) \in \mathbb{R}[x]$  and  $\deg f_0 \equiv 0 \pmod{4}$ . Then,*

$$\text{ord}_2 n_{\text{Jac}_{X'}/\mathbb{R}} \equiv \begin{cases} 0 & \text{if } R_{f_0, \bar{f}_0} < 0 \\ 1 & \text{if } R_{f_0, \bar{f}_0} > 0 \end{cases} \pmod{2}$$

where  $R_{f_0, \bar{f}_0}$  denotes the resultant of  $f_0, \bar{f}_0$ .

*Proof.* By Lemmata 2.1.8 and 8.5.4,  $\text{ord}_2 n_{\text{Jac}_{X'}/\mathbb{R}} = n_{X'/\mathbb{R}} - 1 \equiv \#\{x \in \mathbb{R} : t(x) = 0, s(x) < 0\} + 1 \pmod{2}$ . Therefore  $\text{ord}_2 n_{\text{Jac}_{X'}/\mathbb{R}} \equiv 0$  precisely when  $R_{s,t} < 0$ , where  $R_{s,t} \equiv (-1)^{\frac{\deg f_0}{2}} R_{f_0, \bar{f}_0} \pmod{\mathbb{R}_{>0}^\times}$  (using standard properties of resultants).  $\square$

**Proposition 8.5.7.** *Theorem 8.3.12 holds when  $\mathcal{K} \cong \mathbb{R}$ .*

*Proof.* Since  $\mathcal{R}_{f_0} \cap \mathbb{R}, \mathcal{R}_{\bar{f}_0} \cap \mathbb{R} = \emptyset$  (else  $f_0(x)\bar{f}_0(x)$  is not separable), we see that  $H_{\mathcal{K}}(f_0, \bar{f}_0) = +1$  by Lemma 8.4.2. Using that  $w_{\mathcal{K}}(\text{Jac}_C) = w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) = -1$  (Lemma 2.3.4), it remains to show that  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \sqrt{\xi})} = +1$ .

We observe that  $n_{C/\mathcal{K}} = 2$ . Therefore  $\mu_{\mathcal{K}}(C) = 1$  and  $n_{\text{Jac}_C/\mathcal{K}} = 2$  (by Lemma 2.1.8). Additionally,  $\mu_{\mathcal{K}}(X') = 1$  (as noted in the discussion preceding Lemma 8.5.4). Combining this with Lemmata 8.5.2 and 8.5.6 gives the required result.  $\square$

## 8.5.2 Proof over non-Archimedean fields for nice reduction types

We now consider non-Archimedean local fields, beginning with the case where  $\mathcal{K}/\mathbb{Q}_p$  is a finite extension for an odd prime  $p$  and the reduction of  $f_0(x)\bar{f}_0(x)$  has at worst two double roots. We then move onto the case where  $\mathcal{K}/\mathbb{Q}_2$  is a finite extension and  $C_0, C$  have good ordinary reduction.

We write  $\pi$  for a fixed choice of uniformiser of  $\mathcal{K}$  and  $v$  for a normalised valuation on  $\bar{\mathcal{K}}$ , i.e.  $v(\pi) = 1$ .

**Remark 8.5.8.** We note that, when  $p \neq 2$ , the assumption on the reduction of  $f_0(x)\bar{f}_0(x)$  ensures that  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  is unramified, and consequently that  $\text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0}$  and  $\text{Jac}_{X'}$  are semistable over  $\mathcal{K}$ . In particular, if  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  is

ramified then for each  $r \in \mathcal{R}_{f_0}$  there's an  $s \in \mathcal{R}_{\bar{f}_0}$  such that  $v(r - s) > 0$  (since  $\text{Gal}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} = I_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}}$  acts trivially on the residue field) and the reduction of  $f_0(x)\bar{f}_0(x)$  has worse than two double roots.

**Lemma 8.5.9.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$ .*

(i) If  $\Sigma_{C/\mathcal{K}} = \boxed{\circledast_{d_1} \circledast_{d_2} \cdots \circledast_{d_n}}_0$  where the twin is given by  $\mathfrak{t} = \{r, s\}$  with  $r \in \mathcal{R}_{f_0}$ ,  $s \in \mathcal{R}_{\bar{f}_0}$ , then

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \left( \frac{f_0(x)\bar{f}_0(x)}{(x-r)(x-s)} \Big|_{x=\frac{1}{2}(r+s)}, \pi \right)_{\mathcal{K}}^d.$$

(ii) If  $\Sigma_{C/\mathcal{K}} = \boxed{\circledast_{d_1} \circledast_{d_2} \cdots \circledast_{d_n}}_0$  where the twins are given by  $\mathfrak{t}_1 = \{r_1, s_1\}$ ,  $\mathfrak{t}_2 = \{r_2, s_2\}$  with  $r_1, r_2 \in \mathcal{R}_{f_0}$ ,  $s_1, s_2 \in \mathcal{R}_{\bar{f}_0}$ , then

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \left( \frac{f_0(x)\bar{f}_0(x)}{(x-r_1)(x-s_1)} \Big|_{x=\frac{1}{2}(r_1+s_1)}, \pi \right)_{\mathcal{K}}^{d_1} \left( \frac{f_0(x)\bar{f}_0(x)}{(x-r_2)(x-s_2)} \Big|_{x=\frac{1}{2}(r_2+s_2)}, \pi \right)_{\mathcal{K}}^{d_2}.$$

(iii) If  $\Sigma_{C/\mathcal{K}} = \boxed{\circledast_{d_1} \circledast_{d_2} \cdots \circledast_{d_n}}_0$  where the twins are given by  $\mathfrak{t}_1 = \{r_1, s_1\}$ ,  $\mathfrak{t}_2 = \{r_2, s_2\}$  with  $r_1, r_2 \in \mathcal{R}_{f_0}$ ,  $s_1, s_2 \in \mathcal{R}_{\bar{f}_0}$ , then

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \left( \frac{f_0(x)\bar{f}_0(x)}{(x-r_1)(x-s_1)} \Big|_{x=\frac{1}{2}(r_1+s_1)} \frac{f_0(x)\bar{f}_0(x)}{(x-r_2)(x-s_2)} \Big|_{x=\frac{1}{2}(r_2+s_2)}, \pi \right)_{\mathcal{K}}^d.$$

*Proof.* (i). By Lemma 8.4.13, triples  $\mathfrak{t} \notin T \in \mathcal{T}$  contribute trivially to  $H_{\mathcal{K}}$ . Therefore, using that  $H_2(\{r, r', s\}) = +1$  for each  $r' \in \mathcal{R}_{f_0} - \{r\}$  (as in the proof of Lemma

8.4.13),  $H_{\mathcal{K}}(f_0, \bar{f}_0) = \prod_{r' \in (\mathcal{R}_{f_0} - \{r\})/G_{\mathcal{K}(\epsilon)}} H_1(\{r, r', s\})$  where

$$\begin{aligned}
H_1(\{r, r', s\}) &= (2s - (r + r'), -(r - s)(r' - s))_{\mathcal{K}(r, r')} \\
&= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r, r')/\mathcal{K}}} \sigma(2s - (r + r')), \pi \right)_{\mathcal{K}}^d \\
&= \left( \prod_{\substack{r'' \in \mathcal{R}_{f_0} - \{r\} \\ G_{\mathcal{K}}\text{-conjugate to } r'}} (2s - (r + r'')) \prod_{\substack{s'' \in \mathcal{R}_{\bar{f}_0} - \{s\} \\ G_{\mathcal{K}}\text{-conjugate to } r'}} (2r - (s + s'')), \pi \right)_{\mathcal{K}}^d \\
&= \left( \prod_{\substack{z \in \mathcal{R}_{f_0 \bar{f}_0} - \mathfrak{t} \\ G_{\mathcal{K}}\text{-conjugate to } r'}} \left( \frac{1}{2}(r + s) - z \right), \pi \right)_{\mathcal{K}}^d.
\end{aligned}$$

(Note that  $\mathcal{K}(\{r, r', s\}) = \mathcal{K}(r, r')$  since  $\mathfrak{t}$  is fixed by  $\text{Gal}_{\mathcal{K}(\sqrt{\epsilon})/\mathcal{K}}$ .)

(ii). This follows from (i).

(iii). Note that  $G_{\mathcal{K}}$  swaps  $r_1$  with  $s_2$  and  $r_2$  with  $s_1$ . As in the previous cases, we see that

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \prod_{i=1,2} H_1(\{r_1, r_2, s_i\}) \prod_{r \in (\mathcal{R}_{f_0} - \{r_1, r_2\})/G_{\mathcal{K}(\sqrt{\epsilon})}} H_1(\{r, r_1, s_1\}) H_1(\{r, r_2, s_2\}).$$

The result follows upon first observing that

$$\begin{aligned}
\prod_{i=1,2} H_1(\{r_1, r_2, s_i\}) &= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r_1, r_2)/\mathcal{K}}} \sigma(2s_1 - (r_1 + r_2)) \sigma(2s_2 - (r_1 + r_2)), \pi \right)_{\mathcal{K}}^d \\
&= \left( \left( \frac{1}{2}(r_1 + s_1) - r_2 \right) \left( \frac{1}{2}(r_1 + s_1) - s_2 \right) \left( \frac{1}{2}(r_2 + s_2) - r_1 \right) \left( \frac{1}{2}(r_2 + s_2) - s_1 \right), \pi \right)_{\mathcal{K}}^d
\end{aligned}$$

and second that for each  $r \in \mathcal{R}_{f_0} - \{r_1, r_2\}$ ,

$$\begin{aligned}
\prod_{i=1,2} H_1(\{r, r_i, s_i\}) &= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r_1, r_2, r)/\mathcal{K}}} \sigma(2s_1 - (r_1 + r)) \sigma(2s_2 - (r_2 + r)), \pi \right)_{\mathcal{K}}^d \\
&= \left( \prod_{\substack{z \in \mathcal{R}_{f_0 \bar{f}_0} - (\mathfrak{t}_1 \cup \mathfrak{t}_2) \\ G_{\mathcal{K}}\text{-conjugate to } r}} \left( \frac{1}{2}(r_1 + s_1) - z \right) \left( \frac{1}{2}(r_2 + s_2) - z \right), \pi \right)_{\mathcal{K}}^d. \quad \square
\end{aligned}$$

**Lemma 8.5.10.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be a finite extension for  $p \neq 2$  and suppose that  $\Sigma_{C/\mathcal{K}} = \overline{\left( \begin{array}{c} \circ \circ \circ \\ \circ \circ \circ \\ \circ \circ \circ \\ \circ \circ \circ \end{array} \right)}_0$  where the twins are given by  $\mathfrak{t}_1 = \{r_1, r_2\} \subset \mathcal{R}_{f_0}$  and  $\mathfrak{t}_2 = \{s_1, s_2\} \subset \mathcal{R}_{\bar{f}_0}$ . Then*

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \left( f_0\left(\frac{1}{2}(s_1 + s_2)\right) \bar{f}_0\left(\frac{1}{2}(r_1 + r_2)\right), \pi \right)_{\mathcal{K}}^d.$$

*Proof.* Suppose first that  $G_{\mathcal{K}}$  permutes  $\mathfrak{t}_1 \cup \mathfrak{t}_2$  in two orbits. By Lemma 8.4.13, triples  $\mathfrak{t}_i \not\subset T \in \mathcal{T}$  for some  $i = 1, 2$  contribute trivially to  $H_{\mathcal{K}}$ . Therefore, using that  $H_1(\{r_1, r_2, s\}) = +1$  for each  $s \in \mathcal{R}_{\bar{f}_0}$  (as in the proof of Lemma 8.4.13), we see that

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = \prod_{i=1,2} H_2(\{r_1, r_2, s_i\}) \prod_{s \in (\mathcal{R}_{\bar{f}_0} - \mathfrak{t}_2)/G_{\mathcal{K}(\sqrt{\varepsilon})}} H_2(\{r_1, r_2, s\}).$$

The result follows upon first observing that

$$\begin{aligned} \prod_{i=1,2} H_2(\{r_1, r_2, s_i\}) &= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r_1, r_2)/\mathcal{K}}} \sigma\left(\frac{1}{2}(r_1 + r_2) - s_1\right) \sigma\left(\frac{1}{2}(r_1 + r_2) - s_2\right), \pi \right)_{\mathcal{K}}^d \\ &= \left( \left(\frac{1}{2}(r_1 + r_2) - s_1\right) \left(\frac{1}{2}(r_1 + r_2) - s_2\right) \left(\frac{1}{2}(s_1 + s_2) - r_1\right) \left(\frac{1}{2}(s_1 + s_2) - r_2\right), \pi \right)_{\mathcal{K}}^d \end{aligned}$$

and second that for each  $s \in \mathcal{R}_{\bar{f}_0} - \mathfrak{t}_2$ ,

$$\begin{aligned} H_2(\{r_1, r_2, s\}) &= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(s, r_1+r_2, r_1 r_2)/\mathcal{K}}} \sigma\left(\frac{1}{2}(r_1 + r_2) - s\right), \pi \right)_{\mathcal{K}}^d \\ &= \left( \prod_{\substack{s' \in \mathcal{R}_{\bar{f}_0} - \mathfrak{t}_2 \\ G_{\mathcal{K}}\text{-conjugate to } s}} \left(\frac{1}{2}(r_1 + r_2) - s'\right) \prod_{\substack{r' \in \mathcal{R}_{f_0} - \mathfrak{t}_1 \\ G_{\mathcal{K}}\text{-conjugate to } s}} \left(\frac{1}{2}(s_1 + s_2) - r'\right), \pi \right)_{\mathcal{K}}^d. \end{aligned}$$

Now suppose that  $G_{\mathcal{K}}$  acts transitively on  $\mathfrak{t}_1 \cup \mathfrak{t}_2$  so that  $\{r_1, r_2, s_1\}, \{r_1, r_2, s_2\}$  are  $G_{\mathcal{K}}$ -conjugate and

$$H_{\mathcal{K}}(f_0, \bar{f}_0) = H_2(\{r_1, r_2, s_1\}) \prod_{s \in (\mathcal{R}_{\bar{f}_0} - \mathfrak{t}_2)/G_{\mathcal{K}(\sqrt{\varepsilon})}} H_2(\{r_1, r_2, s\}).$$

Arguing as above, and using that in this case we have

$$\begin{aligned} H_2(\{r_1, r_2, s_1\}) &= \left( \prod_{\sigma \in \text{Gal}_{\mathcal{K}(r_1)/\mathcal{K}}} \sigma\left(\frac{1}{2}(r_1 + r_2) - s_1\right), \pi \right)_{\mathcal{K}}^d \\ &= \left( \left(\frac{1}{2}(r_1 + r_2) - s_1\right) \left(\frac{1}{2}(r_1 + r_2) - s_2\right) \left(\frac{1}{2}(s_1 + s_2) - r_1\right) \left(\frac{1}{2}(s_1 + s_2) - r_2\right), \pi \right)_{\mathcal{K}}^d, \end{aligned}$$

completes the proof. □

Recall that

$$\lambda_{\mathcal{K}}(f_0; \sqrt{\xi}) = \frac{c_{\mathcal{K}}(\text{Jac}_C) c_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) \mu_{\mathcal{K}}(C) \mu_{\mathcal{K}(\sqrt{\xi})}(C_0)}{c_{\mathcal{K}}(\text{Jac}_{X'}) \mu_{\mathcal{K}}(X')}.$$

To understand the curve  $X'$  over  $\mathcal{K}$ , we will make use of the following lemma.

**Lemma 8.5.11.** *Let  $\mathcal{K}/\mathbb{Q}_p$  be finite for  $p \neq 2$  and  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  unramified. When  $C/\mathcal{K}$  and  $C_0/\mathcal{K}(\sqrt{\xi})$  are semistable, the eigenvalues of the  $\text{Frob}_{\mathcal{K}}$ -action on  $H_1(\Upsilon_{X'/\mathcal{K}}, \mathbb{Z})$  are given by the multi-set*

$$\begin{aligned} &\{\pm\sqrt{\lambda} : \lambda \text{ an eigenvalue of } \text{Frob}_{\mathcal{K}(\sqrt{\xi})} \text{ on } H_1(\Upsilon_{C_0/\mathcal{K}(\sqrt{\xi})}, \mathbb{Z})\} \\ &\cup \{\text{eigenvalues of } \text{Frob}_{\mathcal{K}} \text{ on } H_1(\Upsilon_{C/\mathcal{K}}, \mathbb{Z})\}. \end{aligned}$$

*Proof.* Fix a prime  $\ell \neq p$ . For a semistable curve  $Y/\mathcal{K}$ ,  $H_1(\Upsilon_{Y/\mathcal{K}}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell} \cong (V_{\ell} \text{Jac}_Y)_t$ , the toric part of  $V_{\ell}$ , as  $G_{\mathcal{K}}$ -representations (see [22, 2.18]). Using that  $V_{\ell}$  is invariant under isogeny, respects products, and  $V_{\ell} \text{Res}_{\mathcal{L}/\mathcal{K}} A \cong \text{Ind}_{G_{\mathcal{L}}}^{G_{\mathcal{K}}} V_{\ell} A$ , we see that

$$H_1(\Upsilon_{X'/\mathcal{K}}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell} \cong \text{Ind}_{G_{\mathcal{K}(\sqrt{\xi})}}^{G_{\mathcal{K}}} (H_1(\Upsilon_{C_0/\mathcal{K}(\sqrt{\xi})}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell}) \oplus H_1(\Upsilon_{C/\mathcal{K}}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell}.$$

The result follows since  $\text{Ind}_{G_{\mathcal{K}(\sqrt{\xi})}}^{G_{\mathcal{K}}} W \cong W \oplus \text{Frob}_{\mathcal{K}} W$ . □

**Example 8.5.12.** Let  $\mathcal{K} = \mathbb{Q}_3$ ,  $\xi = 5$  and  $f_0(x) = (x - \sqrt{5})(x - 1 - 3\sqrt{5})(x^2 - x - \sqrt{5})$ .

Then  $\Sigma_{C/\mathcal{K}} = \left( \begin{array}{c} \circ \circ \bar{\circ} \circ \circ \circ \circ \circ \circ \\ \circ \circ \circ \circ \circ \circ \circ \circ \end{array} \right)_0$  and  $\Sigma_{C/\mathcal{K}(\sqrt{\xi})} = \left( \begin{array}{c} \circ \circ \circ \circ \circ \circ \circ \circ \\ \circ \circ \circ \circ \circ \circ \circ \circ \end{array} \right)_0$ .

Let  $B/\mathcal{K}(\sqrt{\xi}) : \{y^2 = f_0(x), z^2 = \bar{f}_0(x)\}$  and note that  $B \cong X'$  over  $\mathcal{K}(\sqrt{\xi})$  (they have the same function fields). Theorem 2.4.14 with  $f_1 = f_0, f_2 = \bar{f}_0$  gives that  $\Upsilon_{X'/\mathcal{K}(\sqrt{\xi})} = \textcircled{1}$ .

By Lemma 8.5.11,  $\text{Frob}_{\mathcal{K}}$  acts on  $\Upsilon_{X'/\mathcal{K}}$  and  $\Upsilon_{C/\mathcal{K}}$  with the same eigenvalues. In particular, it must be that  $\Upsilon_{X'/\mathcal{K}} = \textcircled{\updownarrow}$ .

Now let  $f_0(x) = (x - \sqrt{5})(x + 2\sqrt{5})(x^2 - x - \sqrt{5})$  so that  $\Sigma_{C_0/\mathcal{K}(\sqrt{\xi})} = \textcircled{\textcircled{\bullet}\textcircled{\bullet}}_i$  and  $\Sigma_{C/\mathcal{K}} = \textcircled{\textcircled{\bullet}\textcircled{\updownarrow}\textcircled{\bullet}}_i$ .

Since  $\Sigma_{C/\mathcal{K}(\sqrt{\xi})} = \textcircled{\textcircled{\bullet}\textcircled{\updownarrow}\textcircled{\bullet}}_i$ , Theorem 2.4.14 gives that  $\Upsilon_{X'/\mathcal{K}(\sqrt{\xi})} = \textcircled{\textcircled{\bullet}\textcircled{\updownarrow}\textcircled{\bullet}}_i$ .

By Lemma 8.5.11,  $\text{Frob}_{\mathcal{K}}$  acts on  $\Upsilon_{X'/\mathcal{K}}$  with eigenvalues  $1, 1, i, -i$ . In particular, it must be that  $\Upsilon_{X'/\mathcal{K}} = \textcircled{\textcircled{\bullet}\textcircled{\updownarrow}\textcircled{\bullet}}_i$ .

**Proposition 8.5.13.** *Theorem 8.3.12 holds when  $\mathcal{K}/\mathbb{Q}_p$  is finite for  $p \neq 2$ , and the reduction of  $f_0(x)\bar{f}_0(x)$  has at worst two double roots.*

*Proof.* Since  $(-1, -1)_{\mathcal{K}} = +1$ , we must prove that

$$H_{\mathcal{K}}(f_0; \sqrt{\xi}) = (-1)^{\text{ord}_2} \frac{c_{\mathcal{K}(\text{Jac}_C)} c_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) \mu_{\mathcal{K}(\sqrt{\xi})}(C_0)}{c_{\mathcal{K}(\text{Jac}_{X'})} \mu_{\mathcal{K}(X')}} w_{\mathcal{K}}(\text{Jac}_C) w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}),$$

where we've used that  $\mu_{\mathcal{K}}(C) = 1$  (the genus of  $C$  is odd).

The inputs of Table 8.2 (columns 1 and 2) are the non-trivial clusters belonging to  $\Sigma_{C_0/\mathcal{K}(\sqrt{\xi})}$  and  $\Sigma_{X'/\mathcal{K}}^{\text{chr}}$  (or, ignoring the colouring,  $\Sigma_{C/\mathcal{K}}$ ), where the roots of  $f_0$  and  $\bar{f}_0$  are denoted by red circles ( $\bullet$ ) and blue diamonds ( $\blacklozenge$ ) respectively.

Column 3 gives the dual graph of the minimal regular model of  $X'/\mathcal{K}$ , denoted  $\Upsilon_{X'/\mathcal{K}}$ , where an arrow is used to indicate the action of Frobenius. This is determined using Theorem 2.4.14 and Lemma 8.5.11 as in Example 8.5.12.

Columns 4 and 5 list the Tamagawa numbers for  $\text{Jac}_{C_0}/\mathcal{K}(\sqrt{\xi})$  and  $\text{Jac}_C/\mathcal{K}$ , calculated from their respective cluster pictures using Theorem 2.4.9.

Similarly, column 6 contains the Tamagawa number for  $\text{Jac}_{X'}/\mathcal{K}$  but this time calculated from  $\Upsilon_{X'}$  using Theorem 2.3.3.

Column 7 keeps track of the deficiency contribution from  $C_0/\mathcal{K}(\sqrt{\xi})$  using The-



		$\Upsilon_{X'/\mathcal{K}}$	$c_{\mathcal{K}(\xi)}(\text{JACC}_0)$	$c_{\mathcal{K}}(\text{JACC})$	$c_{\mathcal{K}}(\text{JACX}')$	$\mu_{\mathcal{K}(\xi)}(C_0)$	$\mu_{\mathcal{K}}(X')$	$(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \xi)}$	$w_{\mathcal{K}(\xi)}(\text{JACC}_0)$	$w_{\mathcal{K}}(\text{JACC})$	$H_{\mathcal{K}}(f_0, \bar{f}_0)$
$\emptyset$	$\emptyset$		1	1	1	1	1	+1	+1	+1	+1
$\emptyset$	$\emptyset$		1	2d	d	1	1	-1	+1	-1	+1
$\emptyset$	$\emptyset$		1	2	$\tilde{d}$	1	1	$(-1)^d$	+1	+1	$(-1)^d$
$\emptyset$	$\emptyset$		1	4d_1d_2	d_1d_2	1	1	+1	+1	+1	+1
$\emptyset$	$\emptyset$		1	4d_1	d_1\tilde{d}_2	1	1	$(-1)^{d_2+1}$	+1	-1	$(-1)^{d_2}$
$\emptyset$	$\emptyset$		1	4	$\tilde{d}_1\tilde{d}_2$	1	1	$(-1)^{d_1+d_2}$	+1	+1	$(-1)^{d_1+d_2}$
$\emptyset$	$\emptyset$		1	2d	d	1	1	-1	+1	-1	+1
$\emptyset$	$\emptyset$		1	2	$\tilde{d}$	1	1	$(-1)^d$	+1	+1	$(-1)^d$
$\emptyset$	$\emptyset$		d	d	d^2	1	1	+1	-1	-1	+1
$\emptyset$	$\emptyset$		$\tilde{d}$	d	d	1	1	$(-1)^{d+1}$	+1	-1	$(-1)^d$
$\emptyset$	$\emptyset$		d	$\tilde{d}$	d	1	1	$(-1)^{d+1}$	-1	+1	$(-1)^d$
$\emptyset$	$\emptyset$		$\tilde{d}$	$\tilde{d}$	$(\tilde{d})^2$	1	1	+1	+1	+1	+1

Notation:  $\tilde{d} = \text{gcd}(2, d)$ .

Table 8.2: Data for Proposition 8.5.13

orem 2.4.11.

Column 8 lists the deficiency contribution of  $X'/\mathcal{K}$  computed from  $\Upsilon_{X'}$  via [47, Lemma 6.11], [53].

Column 9 gives the value of  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \sqrt{\xi})}$ .

Columns 10 and 11 list  $w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0})$  and  $w_{\mathcal{K}}(\text{Jac}_C)$ , calculated using Theorem 2.3.5 or Theorem 2.4.10.

Column 12 records the value of  $H_{\mathcal{K}}(f_0, \bar{f}_0)$ . For row 1, this is +1 since all triples in  $\mathcal{T}$  are of the first type detailed in Lemma 8.4.13. For rows 2-8, we observe Lemma 8.5.9. In particular, in case (i) the first entry of the Hilbert symbol is a square precisely when the sign attached to  $\mathfrak{t}$  is + and similarly in cases (ii) and (iii) (c.f. Definition 2.4.6). For rows 9-12, we observe Lemma 8.5.10 and note that the first entry of the Hilbert symbol is a square precisely when the signs attached to  $\textcircled{\circ\circ}_{\mathfrak{t}}$  and  $\textcircled{\circ\circ\circ}_{\mathfrak{t}}$  are the same (again, c.f. Definition 2.4.6). □

When the residue characteristic of  $\mathcal{K}$  is even, we instead have an analogue of Proposition 8.4.21.

**Proposition 8.5.14.** *Theorem 8.3.12 holds when  $\mathcal{K}/\mathbb{Q}_2$  is finite,  $\mathcal{K}(\sqrt{\xi})/\mathcal{K}$  is unramified and  $C_0, C$  have good ordinary reduction with*

$$\Sigma_{C_0/\mathcal{K}(\sqrt{\xi})} = \left( \textcircled{\circ\circ}_{v(4)} \textcircled{\circ\circ}_{v(4)} \cdots \textcircled{\circ\circ}_{v(4)} \right)_0, \quad \Sigma_{C/\mathcal{K}} = \left( \textcircled{\circ\circ}_{v(4)} \cdots \textcircled{\circ\circ}_{v(4)} \textcircled{\circ\circ\circ}_{v(4)} \cdots \textcircled{\circ\circ\circ}_{v(4)} \right)_0.$$

*Proof.* By assumption,  $w_{\mathcal{K}(\sqrt{\xi})}(\text{Jac}_{C_0}) = w_{\mathcal{K}}(\text{Jac}_C) = +1$ . Recall that  $\phi$  lifts to the isogeny  $\text{Jac}_{C_0} \times \text{Jac}_{\bar{C}_0} \times \text{Jac}_C \rightarrow \text{Jac}_{X'}$  constructed in §3.3 over  $\bar{\mathcal{K}}$ , so applying [24, Theorem A.1] with  $A = \text{Res}_{\mathcal{K}(\sqrt{\xi})/\mathcal{K}} \text{Jac}_{C_0} \times \text{Jac}_C$  and arguing as in the proof of Lemma 8.4.20 gives that  $(-1)^{\text{ord}_2 \lambda_{\mathcal{K}}(f_0; \sqrt{\xi})} = (-1)^{[\mathcal{K}:\mathbb{Q}_2]}$ . It then suffices to prove that  $H_{\mathcal{K}}(f_0, \bar{f}_0) = +1$ , which follows as in Corollary 8.4.19 (using Lemmata 8.4.17 and 8.4.18). □

## 8.6 Global consequences

We conclude this thesis by discussing the instances of the parity conjecture, for Jacobians of hyperelliptic curves, that we are able to deduce from the preceding local analysis.

**Theorem 8.6.1.** *Let  $K$  be a number field and  $X_1 : y^2 = f_1(x)$ ,  $X_2 : z^2 = f_2(x)$ ,  $X_0 : w^2 = f_1(x)f_2(x)$  for  $f_1(x), f_2(x) \in K[x]$  such that  $f_1(x)f_2(x)$  is separable. Assuming Conjecture 8.3.8, the 2-parity conjecture holds for  $\text{Jac}_{X_0}$  if and only if it holds for  $\text{Jac}_{X_1} \times \text{Jac}_{X_2}$ .*

*Proof.* Suppose that  $f_1(x), f_2(x)$  satisfy Assumption  $(\star)$  (if not, let  $t$  be as in Lemma 8.3.1 and replace  $f_1(x), f_2(x)$  by  $f_1(\frac{x}{1-tx}), f_2(\frac{x}{1-tx})$ ). Consider the equality asserted by Conjecture 8.3.8 when  $\mathcal{K} = K_v$  for  $v$  a place of  $K$ . Taking the product over all such  $v$  and then invoking Theorem 4.5.2, the product law for Hilbert symbols, and Theorem 8.3.7, gives that

$$(-1)^{\text{rk}_2(\text{Jac}_{X_1})+\text{rk}_2(\text{Jac}_{X_2})+\text{rk}_2(\text{Jac}_{X_0})} w(\text{Jac}_{X_1})w(\text{Jac}_{X_2})w(\text{Jac}_{X_0}) = +1. \quad \square$$

**Theorem 8.6.2.** *Let  $K$  be a number field,  $K(\sqrt{\xi})/K$  be a quadratic extension and  $C : w^2 = f_0(x)\bar{f}_0(x)$ ,  $C_0 : y^2 = f_0(x)$  for  $\text{Gal}_{K(\sqrt{\xi})/K}$ -conjugate  $f_0(x), \bar{f}_0(x) \in K(\sqrt{\xi})[x]$  of degree  $2^m > 1$  such that  $f_0(x)\bar{f}_0(x)$  is separable. Assuming Conjecture 8.3.11, the 2-parity conjecture holds for  $\text{Jac}_C/K$  if and only if it holds for  $\text{Jac}_{C_0}/K(\sqrt{\xi})$ .*

*Proof.* Suppose that  $f_0(x), \bar{f}_0(x)$  satisfy Assumption  $(\star)$  (if not, let  $t$  be as in Lemma 8.3.1 and replace  $f_0(x), \bar{f}_0(x)$  by  $f_0(\frac{x}{1-tx}), \bar{f}_0(\frac{x}{1-tx})$ ). Consider the equality asserted by Conjecture 8.3.11 when  $\mathcal{K} = K_v$  for  $v$  a place of  $K$ . Taking the product over all such  $v$  and then invoking Theorem 8.2.8, the product law for Hilbert symbols, and Theorem 8.3.7, gives that

$$(-1)^{\text{rk}_2(\text{Jac}_C/K)+\text{rk}_2(\text{Jac}_{C_0}/K(\sqrt{\xi}))} w(\text{Jac}_C/K)w(\text{Jac}_{C_0}/K(\sqrt{\xi})) = +1. \quad \square$$

**Theorem 8.6.3.** *Assuming Conjectures 8.3.8 and 8.3.11, the 2-parity conjecture holds for all hyperelliptic curves  $y^2 = f(x)$  such that  $\text{Gal}(f)$  is a 2-group.*

*Proof.* Let  $C : w^2 = f(x)$  be a hyperelliptic curve over a number field  $K$  such that  $\text{Gal}(f)$  is a 2-group.

When  $\deg f \leq 2$ ,  $\text{Jac}_C = 0$  and so the 2-parity conjecture is already known to hold.

Let  $n \in \mathbb{N}$  and assume that the 2-parity conjecture holds whenever  $\deg f < n$ . Now fix  $\deg f = n$ . By the proof of Theorem 8.1.1,  $C$  is either a  $C_2 \times C_2$ - or  $D_8$ -hyperelliptic curve. In the first case,  $f(x)$  admits a factorisation  $f_1(x)f_2(x)$  over  $K$  and Theorem 8.6.1 then asserts that the 2-parity conjecture holds for  $\text{Jac}_C$  since, by assumption, it holds for  $\text{Jac}_{y^2=f_1(x)}$  and  $\text{Jac}_{z^2=f_2(x)}$ . If  $C$  is a  $D_8$ -hyperelliptic curve then we instead use Theorem 8.6.2.  $\square$

**Corollary 8.6.4.** *Let  $C : y^2 = f(x)$  be a semistable hyperelliptic curve over a number field  $K$  and write  $\mathcal{R} \subset \overline{K}$  for the set of roots of  $f(x)$ . Assuming Conjectures 8.3.8 and 8.3.11, and that  $\#\text{III}(\text{Jac}_C/K(\mathcal{R}))[p^\infty]$  is finite for each prime  $p \leq \deg f$ , the parity conjecture holds for the Jacobian of  $C$  over  $K$ .*

*Proof.* This is an immediate consequence of Theorems 8.1.1 and 8.6.3.  $\square$

Using the cases of Conjectures 8.3.8 and 8.3.11 proved in Theorems 8.3.10 and 8.3.12, we're also able to provide some unconditional global results.

We begin with an explicit example.

**Example 8.6.5.** Consider the genus 2 hyperelliptic curve

$$X_0/\mathbb{Q} : w^2 = (x-1)(x-13)(x^2-5x+5)(x^2-13x+41).$$

We will show that the 2-parity conjecture holds for its Jacobian.

Write  $f_1(x) = (x-1)(x-13)$ ,  $f_2(x) = (x^2-5x+5)(x^2-13x+41)$ ,  $r_1 = \frac{1}{2}(5+\sqrt{5})$ ,  $\bar{r}_1 = \frac{1}{2}(5-\sqrt{5})$ ,  $r_2 = \frac{1}{2}(13+\sqrt{5})$ ,  $\bar{r}_2 = \frac{1}{2}(13-\sqrt{5})$  and define additional curves by  $X_1/\mathbb{Q} : y^2 = f_1(x)$ ,  $X_2/\mathbb{Q} : z^2 = f_2(x)$  and  $X/\mathbb{Q} : \{y^2 = f_1(x), z^2 = f_2(x)\}$ .

Whenever  $v \neq 5$  is a place of  $\mathbb{Q}$ , Theorem 8.3.10 guarantees that

$$(-1)^{\text{ord}_2 \lambda_v(f_1, f_2)} w_v(\text{Jac}_{X_2}) w_v(\text{Jac}_{X_0}) = H_v(f_1, f_2). \tag{8.1}$$

We show that this also holds when  $v = 5$ . Since  $\Sigma_{X_2/\mathbb{Q}_5} = \left( \begin{array}{c} \textcircled{\textcircled{\textcircled{2}}_2} \\ \textcircled{\textcircled{\textcircled{3}}_3} \\ \textcircled{\textcircled{\textcircled{0}}_0} \end{array} \right)^{\dagger}$  and

$\Sigma_{X_0/\mathbb{Q}_5} = \left( \begin{array}{c} \bullet \bullet \\ \circ \circ \\ \circ \circ \end{array} \right)_0$ , we compute that  $c_5(\text{Jac}_{X_1}) = 1$ ,  $c_5(\text{Jac}_{X_2}) = 2$  (see Table 7.1),  $c_5(\text{Jac}_{X_0}) = 1$  (by Theorem 2.4.9),  $\mu_5(X_1) = \mu_5(X_0) = 1$  ( $X_1, X_0$  have  $\mathbb{Q}$ -points) and  $\mu_5(X_2) = \mu_5(X) = +1$  ( $X_2$  has genus 1 and the divisor  $(0, \sqrt{5}, \sqrt{41}) + (0, -\sqrt{5}, \sqrt{41})$  on  $X$  is  $\mathbb{Q}_5$ -rational). Observing the colouring in the cluster picture for  $X_0/\mathbb{Q}_5$ , [27, Theorems 3.1 & 3.3] gives that  $\Upsilon_{X/\mathbb{Q}_5} = \begin{array}{c} \circ \\ \updownarrow \\ \circ \end{array}$  and so  $c_5(\text{Jac}_X) = 4$  by Theorem 2.3.3 (alternatively,  $\Upsilon_X = \Upsilon_C$  for  $C/\mathbb{Q}_5$  a hyperelliptic curve with  $\Sigma_C = \left( \begin{array}{c} \circ \circ \\ \circ \circ \\ \circ \circ \end{array} \right)_0$  so that  $c_5(\text{Jac}_X) = c_5(\text{Jac}_C)$  can then be determined using [2, Theorem 10.3]). In particular,  $\text{ord}_2 \lambda_5(f_1, f_2) = -1$ . From the relevant cluster pictures, we also see that  $w_5(\text{Jac}_{X_2}) = -1$  (see Table 7.1) and  $w_5(\text{Jac}_{X_0}) = +1$  (by Theorem 2.4.10). It remains to show that  $H_5(f_1, f_2) = +1$ . This is clear from Table 8.3.

$T_O$	$H_1(T_O)H_2(T_O)$
$\{1, 13, r_1\}$	$(-9 + \sqrt{5}, \frac{1}{2}(29 + 9\sqrt{5}))_{\mathbb{Q}_5(\sqrt{5})} (\frac{1}{2}(9 - \sqrt{5}), 144)_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{1, 13, r_2\}$	$(-1 + \sqrt{5}, \frac{1}{2}(69 + \sqrt{5}))_{\mathbb{Q}_5(\sqrt{5})} (\frac{1}{2}(1 - \sqrt{5}), 144)_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_1, r_2, 1\}$	$(-7 - \sqrt{5}, -\frac{1}{2}(19 + 7\sqrt{5}))_{\mathbb{Q}_5(\sqrt{5})} (\frac{1}{2}(7 + \sqrt{5}), 16)_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_1, \bar{r}_2, 1\}$	$(-7, -7 - 2\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} (\frac{7}{2}, 21 - 8\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_1, \bar{r}_1, 1\}$	$(-3, -1)_{\mathbb{Q}_5} (\frac{3}{2}, 5)_{\mathbb{Q}_5} = +1$
$\{r_2, \bar{r}_2, 1\}$	$(-11, -29)_{\mathbb{Q}_5} (\frac{11}{2}, 5)_{\mathbb{Q}_5} = -1$
$\{r_1, r_2, 13\}$	$(17 - \sqrt{5}, -\frac{1}{2}(139 - 17\sqrt{5}))_{\mathbb{Q}_5(\sqrt{5})} (-\frac{1}{2}(17 - \sqrt{5}), 16)_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_1, \bar{r}_2, 13\}$	$(17, -67 - 2\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} (-\frac{17}{2}, 21 - 8\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_1, \bar{r}_1, 13\}$	$(21, -109)_{\mathbb{Q}_5} (-\frac{21}{2}, 5)_{\mathbb{Q}_5} = -1$
$\{r_2, \bar{r}_2, 13\}$	$(13, -41)_{\mathbb{Q}_5} (-\frac{13}{2}, 5)_{\mathbb{Q}_5} = +1$

**Table 8.3:** Data for  $H_5(f_1, f_2)$  in Example 8.6.5

Considering (8.1), taking the product over all places, and implementing Theorems 8.3.7 & 4.5.2, we see that

$$(-1)^{\text{rk}_2(\text{Jac}_{X_2}) + \text{rk}_2(\text{Jac}_{X_0})} w(\text{Jac}_{X_2}) w(\text{Jac}_{X_0}) = +1,$$

i.e. the 2-parity conjecture holds for the abelian surface  $\text{Jac}_{X_0}$  if and only if it holds for the elliptic curve  $\text{Jac}_{X_2}$ .

Now write  $g_1(x) = x^2 - 5x + 5$ ,  $g_2(x) = x^2 - 13x + 41$  and  $Y/\mathbb{Q} : \{y^2 = g_1(x), z^2 = g_2(x)\}$ . Similarly to above, whenever  $v \neq 5$  is a place of  $\mathbb{Q}$ , Theorem 8.3.10 guarantees that

$$(-1)^{\text{ord}_2 \lambda_v(g_1, g_2)} w_v(\text{Jac}_{X_2}) = (-1, -1)_v H_v(g_1, g_2). \tag{8.2}$$

We again verify this equality when  $v = 5$ . Since  $\text{Jac}_{y^2=g_1(x)} = \text{Jac}_{z^2=g_2(x)} = 0$ ,  $\lambda_5(g_1, g_2) = c_5(\text{Jac}_{X_2})/c_5(\text{Jac}_Y)$ . By above,  $c_5(\text{Jac}_{X_2}) = 2$ . Using that  $\Sigma_{Y/\mathbb{Q}_5}^{\text{chr}} = \langle \langle \text{red circles} \rangle \rangle_0^+$ , [27, Theorems 3.1 & 3.3] gives  $\Upsilon_{Y/\mathbb{Q}_5} = \langle \langle \text{blue circle} \rangle \rangle_1$  so that  $c_5(\text{Jac}_Y) = 4$  (by Theorem 2.3.3). Therefore  $\text{ord}_2 \lambda_5(g_1, g_2) = -1$  and, as above,  $w_5(\text{Jac}_{X_2}) = -1$ . In this case, the computation of  $H_5$  is more succinct and we see, via Table 8.4, that  $H_5(g_1, g_2) = +1$ .

$T_O$	$H_1(T_O)H_2(T_O)$
$\{r_1, \bar{r}_1, r_2\}$	$(8 + \sqrt{5}, -16 - 4\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} \cdot (-\frac{1}{2}(8 + \sqrt{5}), 5)_{\mathbb{Q}_5(\sqrt{5})} = +1$
$\{r_2, \bar{r}_2, r_1\}$	$(-8 + \sqrt{5}, -16 + 4\sqrt{5})_{\mathbb{Q}_5(\sqrt{5})} \cdot (\frac{1}{2}(8 - \sqrt{5}), 5)_{\mathbb{Q}_5(\sqrt{5})} = +1$

**Table 8.4:** Data for  $H_5(g_1, g_2)$  in Example 8.6.5

Taking the product over all places of (8.2), and again implementing Theorems 8.3.7 & 4.5.2, we see that

$$(-1)^{\text{rk}_2(\text{Jac}_{X_2})} w(\text{Jac}_{X_2}) = +1$$

i.e. the 2-parity conjecture holds for the elliptic curve  $\text{Jac}_{X_2}$  and, moreover, it holds for the abelian surface  $\text{Jac}_{X_0}$ .

More generally, we are able to prove the following case of the 2-parity conjecture for hyperelliptic curves of arbitrary genus.

**Theorem 8.6.6.** *Let  $K$  be a number field. Let  $f(x) \in \mathcal{O}_K[x]$  be separable, monic and such that  $\text{Gal}_{K(\mathcal{R})/K}$  is a 2-group and  $G_K$  preserves a partition  $\{\alpha_1, \beta_1\}, \dots, \{\alpha_n, \beta_n\}$  of  $\mathcal{R}$  (the roots of  $f$ ). Let  $\mathfrak{p}$  denote a prime of  $\mathcal{O}_K$  and suppose that the reduction of  $f(x)$  modulo  $\mathfrak{p}$  has at worst one double root whenever  $\mathfrak{p} \nmid 2$ , and that*

- $(x - \alpha_i)(x - \beta_i) \in K_{\mathfrak{p}}^{nr}[x]$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \beta_i) = \text{ord}_{\mathfrak{p}}(4)$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \alpha_j) = \text{ord}_{\mathfrak{p}}(\beta_i - \beta_j) = \text{ord}_{\mathfrak{p}}(\alpha_i - \beta_j) = 0$  for all  $i \neq j$ ,

whenever  $\mathfrak{p} \mid 2$ . The 2-parity conjecture holds for the Jacobian of  $C : w^2 = f(x)$ .

*Proof.* When  $\deg f \leq 2$ ,  $\text{Jac}_C = 0$  and so the 2-parity conjecture is already known to hold.

Let  $\deg f = 4$ . Suppose that  $f_i(x) := (x - \alpha_i)(x - \beta_i) \in K[x]$  and that  $f_1(x), f_2(x)$  satisfy Assumption  $(\star)$  (if not, let  $t$  be as in Lemma 8.3.1 and replace  $f_1(x), f_2(x)$  by  $f_1(\frac{x}{1-tx}), f_2(\frac{x}{1-tx})$ ). Since the assumptions of Theorem 8.3.10 are satisfied when  $\mathcal{K} = K_v$  for each place  $v$  of  $K$ , we take the product over all places of the asserted equality to obtain that

$$\begin{aligned} (-1)^{\text{rk}_2(\text{Jac}_{y^2=f_1(x)}) + \text{rk}_2(\text{Jac}_{z^2=f_2(x)}) + \text{rk}_2(\text{Jac}_C)} w(\text{Jac}_{y^2=f_1(x)}) w(\text{Jac}_{z^2=f_2(x)}) w(\text{Jac}_C) \\ = (-1)^{\text{rk}_2(\text{Jac}_C)} w(\text{Jac}_C) = +1 \end{aligned}$$

(having noted Theorem 4.5.2, the product law for Hilbert symbols and Theorem 8.3.7). By assumption, if  $f_i(x) \notin K[x]$  then  $f_i(x) \in K(\sqrt{\xi})[x]$  for some  $\xi \in K$ . In this case,  $\text{Jac}_C$  is an elliptic curve with a  $K$ -rational 2-torsion point (see Remark 2.1.7) for which the 2-parity conjecture is already known to hold by [20, Theorem 1.8].

We proceed by induction on the degree of  $f$ . In particular, fix  $N \in \mathbb{N}$  and assume that the 2-parity conjecture holds whenever  $\deg f < N$  and the roots of  $f(x)$  satisfy the assumptions of the theorem.

Let  $\deg f = N$ . Write  $O_1, \dots, O_m$  for the  $G_K$ -orbits of  $\{\alpha_1, \beta_1\}, \dots, \{\alpha_n, \beta_n\}$ , and  $g_i(x) = \prod_{\{\alpha_j, \beta_j\} \in O_i} (x - \alpha_j)(x - \beta_j) \in K[x]$ . Suppose that  $m \geq 2$  and, without loss of generality, that  $g_1(x), g_2(x) \cdots g_m(x)$  satisfy Assumption  $(\star)$ . Since the assumptions of Theorem 8.3.10 (with  $f_1 = g_1, f_2 = g_2 \cdots g_m$ ) are satisfied when  $\mathcal{K} = K_v$  for each place  $v$  of  $K$ , we take the product over all places of the asserted equality to obtain that

$$(-1)^{\mathrm{rk}_2(\mathrm{Jac}_{y^2=g_1}) + \mathrm{rk}_2(\mathrm{Jac}_{z^2=g_2 \cdots g_m}) + \mathrm{rk}_2(\mathrm{Jac}_C)} w(\mathrm{Jac}_{y^2=g_1}) w(\mathrm{Jac}_{z^2=g_2 \cdots g_m}) w(\mathrm{Jac}_C) = +1$$

(having noted Theorem 4.5.2, the product law for Hilbert symbols and Theorem 8.3.7). Since  $\deg g_1, \deg g_2 \cdots g_m < N$ , the 2-parity conjecture holds for  $\mathrm{Jac}_{y^2=g_1}$  and  $\mathrm{Jac}_{z^2=g_2 \cdots g_m}$  by assumption, and so we get the result for  $\mathrm{Jac}_C$ . If  $m = 1$ , then (as in the proof of Theorem 8.1.1) there is a quadratic extension  $K(\sqrt{\xi})/K$  such that  $G_{K(\sqrt{\xi})}$  permutes  $\{\alpha_1, \beta_1\}, \dots, \{\alpha_n, \beta_n\}$  in two orbits  $O_1, O_2$ . Define  $f_0(x) = \prod_{\{\alpha_j, \beta_j\} \in O_1} (x - \alpha_j)(x - \beta_j) \in K(\sqrt{\xi})[x]$  and, without loss of generality, suppose that  $f_0(x), \bar{f}_0(x)$  (the  $\mathrm{Gal}_{K(\sqrt{\xi})/K}$ -conjugate of  $f_0$ ) satisfy Assumption  $(\star)$ . Since the assumptions of Theorem 8.3.12 are satisfied when  $\mathcal{K} = K_v$  for each place  $v$  of  $K$ , we take the product over all places of the asserted equality to obtain that

$$(-1)^{\mathrm{rk}_2(\mathrm{Jac}_C/K) + \mathrm{rk}_2(\mathrm{Jac}_{C_0}/K(\sqrt{\xi}))} w(\mathrm{Jac}_C/K) w(\mathrm{Jac}_{C_0}/K(\sqrt{\xi})) = +1$$

where  $C_0 : y^2 = f_0(x)$  (having noted Theorem 8.2.8, the product law for Hilbert symbols and Theorem 8.3.7). Since  $\deg f_0 < N$ , the 2-parity conjecture holds for  $\mathrm{Jac}_{C_0}/K(\sqrt{\xi})$  by assumption, and so we get the result for  $\mathrm{Jac}_C$ .  $\square$

As a consequence, imposing relevant assumptions on the size of the Shafarevich–Tate group, we deduce the following instance of the parity conjecture for hyperelliptic curves.

**Corollary 8.6.7.** *Let  $K$  be a number field. Let  $f(x) \in \mathcal{O}_K[x]$  be separable, monic, such that  $\mathrm{Gal}_{K(\mathcal{R})/K}$  is a 2-group and  $G_K$  preserves a partition  $\{\alpha_1, \beta_1\}, \dots, \{\alpha_n, \beta_n\}$  of  $\mathcal{R}$  (the roots of  $f$ ). Let  $\mathfrak{p}$  denote a prime of  $\mathcal{O}_K$  and suppose that the reduction of  $f(x)$  modulo  $\mathfrak{p}$  has at worst one double root whenever  $\mathfrak{p} \nmid 2$ , and that*



- $(x - \alpha_i)(x - \beta_i) \in K_{\mathfrak{p}}^{nr}[x]$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \beta_i) = \text{ord}_{\mathfrak{p}}(4)$  for all  $i$ ,
- $\text{ord}_{\mathfrak{p}}(\alpha_i - \alpha_j) = \text{ord}_{\mathfrak{p}}(\beta_i - \beta_j) = \text{ord}_{\mathfrak{p}}(\alpha_i - \beta_j) = 0$  for all  $i \neq j$ ,

whenever  $\mathfrak{p} \mid 2$ . Write  $C : y^2 = f(x)$ . Assuming that  $\#\text{III}(\text{Jac}_C/K(\mathcal{R}))[p^\infty]$  is finite for each prime  $p \leq \deg f$ , the parity conjecture holds for the Jacobian of  $C$ .

*Proof.* Applying [24, Theorem B.1] with  $F = K(\mathcal{R})$  and  $A = \text{Jac}_C$  (for which there are no primes of unstable reduction), we see that it is enough to prove the parity conjecture for  $\text{Jac}_C/K(\mathcal{R})^H$  whenever  $H \leq \text{Gal}_{K(\mathcal{R})/K}$  is a 2-group.

By Theorem 8.6.6, the 2-parity conjecture holds for such  $\text{Jac}_C/K(\mathcal{R})^H$  and this is equivalent to the parity conjecture since  $\#\text{III}(\text{Jac}_C/K(\mathcal{R}))[2^\infty] < \infty \Rightarrow \#\text{III}(\text{Jac}_C/K(\mathcal{R})^H)[2^\infty] < \infty$ .  $\square$

# Bibliography

- [1] E. A. Bender. A lifting formula for the Hilbert symbol. *Proc. Amer. Math. Soc.*, 40:63–65, 1973.
- [2] A. J. Best, L. A. Betts, M. Bisatt, R. van Bommel, V. Dokchitser, O. Faraggi, S. Kunzweiler, C. Maistret, A. Morgan, S. Muselli, and S. Nowell. A user’s guide to the local arithmetic of hyperelliptic curves. *Bull. Lond. Math. Soc.*, 54(3):825–867, 2022.
- [3] B. J. Birch. Conjectures concerning elliptic curves. In *Proc. Sympos. Pure Math.*, Vol. VIII, pages 106–112. 1965.
- [4] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.
- [5] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.
- [6] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.
- [7] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.
- [8] K. Česnavičius. The  $p$ -parity conjecture for elliptic curves with a  $p$ -isogeny. *J. Reine Angew. Math.*, 719:45–73, 2016.

- [9] J. Coates, T. Fukaya, K. Kato, and R. Sujatha. Root numbers, Selmer groups, and non-commutative Iwasawa theory. *J. Algebraic Geom.*, 19(1):19–97, 2010.
- [10] G. Cornelissen. Two-torsion in the Jacobian of hyperelliptic curves over finite fields. *Arch. Math. (Basel)*, 77(3):241–246, 2001.
- [11] J. E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.*, 31(1-2):71–87, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).
- [12] P. Deligne. Les constantes des équations fonctionnelles. In *Séminaire Delange-Pisot-Poitou: 1969/70, Théorie des Nombres, Fasc. 2, Exp. 19 bis*, page 13. Secrétariat mathématique, Paris, 1970.
- [13] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
- [14] J. Docking.  $2^\infty$ -Selmer rank parities via the Prym construction, 2023. ArXiv preprint, arXiv.2108.09564.
- [15] J. Docking. *Arithmetic of Curves of Genus Three and Their Jacobians*. PhD thesis, University College London, 2023.
- [16] T. Dokchitser. Notes on the parity conjecture. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 201–249. Birkhäuser/Springer, Basel, 2013.
- [17] T. Dokchitser and V. Dokchitser. Parity of ranks for elliptic curves with a cyclic isogeny. *J. Number Theory*, 128(3):662–679, 2008.
- [18] T. Dokchitser and V. Dokchitser. Regulator constants and the parity conjecture. *Invent. Math.*, 178(1):23–71, 2009.
- [19] T. Dokchitser and V. Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1):567–596, 2010.

- [20] T. Dokchitser and V. Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658:39–64, 2011.
- [21] T. Dokchitser and V. Dokchitser. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.*, 367(6):4339–4358, 2015.
- [22] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Arithmetic of hyperelliptic curves over local fields. *Math. Ann.*, 385(3-4):1213–1322, 2023.
- [23] V. Dokchitser, H. Green, A. Konstantinou, and A. Morgan. Parity of ranks of Jacobians of curves, 2022. ArXiv preprint, arXiv.2211.06357.
- [24] V. Dokchitser and C. Maistret. On the parity conjecture for abelian surfaces. *Proceedings of the London Mathematical Society*, 127(2):295–365, 2023.
- [25] V. Dokchitser and A. Morgan. A note on hyperelliptic curves with ordinary reduction over 2-adic fields. *J. Number Theory*, 244:264–278, 2023.
- [26] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
- [27] O. Faraggi. Models of bihyperelliptic curves, 2021. ArXiv preprint, arXiv.2103.09730.
- [28] H. Green and C. Maistret. The 2-parity conjecture for elliptic curves with isomorphic 2-torsion. *Proc. of the Royal Soc. A*, 478(2265):Paper No. 20220112, 16, 2022.
- [29] B. H. Gross and J. Harris. Real algebraic curves. *Ann. Sci. École Norm. Sup. (4)*, 14(2):157–182, 1981.
- [30] B. H. Gross and D. B. Zagier. Heegner points and derivatives of  $L$ -series. *Invent. Math.*, 84(2):225–320, 1986.
- [31] A. Grothendieck. Modeles de Néron et monodromie, exp IX in groupes de monodromie en géométrie algébrique, SGA 7, part I. *Lecture Notes in Mathematics*, 288, 1971.

- [32] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
- [33] M. Kim and S. H. Marshall. Crystalline subrepresentations and Néron models. *Math. Res. Lett.*, 7(5-6):605–614, 2000.
- [34] M. Kisin. Local constancy in  $p$ -adic families of Galois representations. *Math. Z.*, 230(3):569–593, 1999.
- [35] V. A. Kolyvagin. Finiteness of  $E(\mathbf{Q})$  and  $\text{III}(E, \mathbf{Q})$  for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.
- [36] K. Kramer. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.*, 264(1):121–135, 1981.
- [37] K. Kramer and J. Tunnell. Elliptic curves and local  $\varepsilon$ -factors. *Compositio Math.*, 46(3):307–352, 1982.
- [38] S. Kunzweiler and W. Wewers. Integral differential forms for superelliptic curves, 2023. ArXiv preprint, arXiv.2003.12357.
- [39] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern e, Oxford Science Publications.
- [40] Barry Mazur and Karl Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Ann. of Math. (2)*, 166(2):579–612, 2007.
- [41] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.
- [42] J. S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1986.
- [43] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

- [44] J. S. Milne. Abelian varieties (v2.00), 2008. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [45] J. S. Milne. Class field theory (v4.03), 2020. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [46] A. Morgan. Paper in preparation.
- [47] A. Morgan. 2-Selmer parity for hyperelliptic curves in quadratic extensions. *Proceedings of the London Mathematical Society*, 127(5):1507–1576, 2023.
- [48] J. Nekovář. On the parity of ranks of Selmer groups. IV. *Compos. Math.*, 145(6):1351–1359, 2009. With an appendix by Jean-Pierre Wintenberger.
- [49] J. Nekovář. Some consequences of a formula of Mazur and Rubin for arithmetic local constants. *Algebra Number Theory*, 7(5):1101–1120, 2013.
- [50] J. Nekovář. Compatibility of arithmetic and algebraic local constants (the case  $\ell \neq p$ ). *Compos. Math.*, 151(9):1626–1646, 2015.
- [51] J. Nekovář. Compatibility of arithmetic and algebraic local constants, II: the tame abelian potentially Barsotti-Tate case. *Proc. Lond. Math. Soc. (3)*, 116(2):378–427, 2018.
- [52] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [53] B. Poonen and M. Stoll. The Cassels–Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.
- [54] K. A. Ribet and W. A. Stein. Modular forms, Hecke operators, and modular abelian varieties. 2003. Preprint, available at <https://wstein.org/edu/Fall2003/252/lectures/all/252.pdf>.

- [55] D. E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.
- [56] H. G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.
- [57] M. Sabitova. Root numbers of abelian varieties. *Trans. Amer. Math. Soc.*, 359(9):4259–4284, 2007.
- [58] J. P. Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). In *Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 1: Exposés 1 à 15; Fasc. 2: Exposés 16 à 24*, page 15. Secrétariat Math., Paris, 1970.
- [59] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, Russian edition, 2013. Varieties in projective space.
- [60] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [61] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
- [62] The Stacks Project Authors. Stacks project, 2018. Available at <https://stacks.math.columbia.edu>.
- [63] W. A. Stein et al. *Sage Mathematics Software (Version 9.5)*. The Sage Development Team, 2023. <http://www.sagemath.org>.
- [64] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.
- [65] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume Vol. 476 of *Lecture Notes in Math*, pages pp 33–52. Springer, Berlin, 1975.

- [66] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.
- [67] R. van Bommel. Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over  $\mathbb{Q}$  up to squares. *Exp. Math.*, 31(1):138–145, 2022.
- [68] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.