2-Selmer parity for Jacobians of hyperelliptic curves in quadratic extensions

Adam John Morgan

School of Mathematics

July, 2015

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Science

To my grandad, Stewart Woodcock, whose love of maths and science has been an inspiration to me.

Abstract

We study the 2-parity conjecture for Jacobians of hyperelliptic curves over number fields. Under some mild assumptions on their reduction, we prove it over quadratic extensions of the base field, providing essentially the first examples of the 2-parity conjecture in dimension greater than one. The proof proceeds via a generalisation of a formula of Kramer and Tunnell relating local invariants of the curve, which may be of independent interest and works for positive characteristic and characteristic zero local fields alike. Particularly surprising is the appearance in the formula of terms that govern whether or not the Cassels-Tate pairing associated to the Jacobian is alternating, which first appeared in a paper of Poonen and Stoll. We prove the formula in many instances and show that in all cases it follows from standard global conjectures.

Acknowledgements

First and foremost I would like to thank Tim Dokchitser for suggesting the problem, for constant encouragement and many helpful discussions. I also thank Kęstutis Česnavičius for discussion regarding many aspects of the thesis, particularly regarding the ideas in Chapter 2. I thank Qing Liu for correspondence regarding the proof of Proposition 8.1.1, and Vladimir Dokchitser for helpful conversations. Last but not least, many thanks to my friends and family for making my time in Bristol, and my education to as a whole, such an enjoyable experience.

Declaration

I declare that the work in this thesis was carried out in accordance with the Regulations of the University of Bristol. The work is original except where indicated by special reference in the text and no part of the dissertation has been submitted for any other degree. Any views expressed in the dissertation are those of the author and do not necessarily represent those of the University of Bristol. The thesis has not been presented to any other university for examination either in the United Kingdom or overseas.

Date: August 11, 2021

Contents

Chapter 1

Introduction

1.1 Overview

In [KT82], Kramer and Tunnell conjectured and largely proved a formula relating local invariants of elliptic curves. The conjecture, now a theorem in all cases thanks to subsequent work of Dokchitser–Dokchitser [DD11] and Česnavičius–Imai [ČI15], yields one of the main unconditional results towards the parity conjecture for elliptic curves over number fields. Specifically, when combined with an arithmetic duality theorem of Kramer [Kra81, Theorem 1], it tells us that the 2–parity conjecture holds for any elliptic curve defined over a number field K, not over K itself, but over any quadratic extension. This can alternatively be viewed as a compatibility statement for the 2–parity conjecture under quadratic twist and this interpretation has found recent application in the groundbreaking work of Bhargava–Shankar on the average ranks of elliptic curves (see [BS15], especially Section 4).

In this thesis we conjecture an analogue of the Kramer–Tunnell formula for Jacobians of hyperelliptic curves and succeed in proving this under some mild restrictions on the reduction of the hyperelliptic curve. We prove also a generalisation of Kramer's theorem (in the context of arbitrary principally polarised abelian varieties) and combine the two to prove the 2-parity conjecture for large classes of (Jacobians of) hyperelliptic curves. This yields the first general result on the 2-parity conjecture over number fields for abelian varieties of dimension greater than 1.

Whilst the applications to the 2-parity conjecture make the work most interesting over local fields of characteristic zero (the 2-parity conjecture, and in fact the p-parity conjecture for all primes p, is known in full generality for all abelian varieties over global

fields of positive characteristic due to Trihan and Yasuda [TY14]), we conjecture that our formula holds for local fields of positive characteristic and characteristic 0 alike. In fact, the exisiting parity results for global fields of positive characteristic allow us to deduce that any hyperelliptic curve defined over a global field of chacteristic $p > 2$ satisfies our local formula over every completion. In characteristic 0, using standard global conjectures as the input we show the same result (now conditionally) and so it seems reasonable to believe our conjecture in all cases.

The most prominent new feature of the work when compared to the elliptic curve case has to do with the phenomenon, observed by Poonen and Stoll in [PS99], that the Shafarevich–Tate group of a principally polarised abelian variety can (if finite) fail to have square order. This global phenomenon contributes new terms to the generalisation of Kramer's theorem. This predicts that the Kramer–Tunnell formula needs additional compensating terms for hyperelliptic curves of even genus. Such terms do indeed appear in our conjecture, and we prove the formula in many cases where these terms are non trivial. We find this particularly interesting as it is one of the first times where the 'non-square Shafarevich–Tate group' pheonomenon has been seen to influence the local arithmetic of abelian varieties.

We now make this discussion precise and state the main results of the thesis.

1.2 The 2-parity conjecture

We begin by discussing the 2-parity conjecture. Let K be a global field (that is, either a number field or the function field of a connected, smooth proper curve over a finite field) and A/K an abelian variety. The completed L-series, $L^\star(A/K, s)$, of A/K conjecturally has a meromorphic continuation to the whole of the complex plane and satisfies a functional equation

$$L^\star(A/K, s) = w(A/K)L^\star(A/K, 2 - s)$$

where $w(A/K) \in \{\pm 1\}$ is the global root number of A/K. The Birch and Swinnerton-Dyer conjecture asserts that the Mordell–Weil rank of A/K agrees with the order of vanishing at $s = 1$ of $L^\star(A/K, s)$:

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

If $w(A/K) = 1$ (resp. -1), then $L^\star(A/K, s)$ is an even (resp. odd) function around $s = 1$ and as such its order of vanishing there is even (resp. odd). Thus a consequence of the

Birch and Swinnerton-Dyer conjecture is the parity conjecture;

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

Essentially all progress towards the parity conjecture has proceeded via the p-parity conjecture. For a fixed prime p, we denote by $\mathrm{rk}_p(A/K)$ the p-infinity Selmer rank of A/K. Under the conjectural finiteness of the Shafarevich–Tate group (or indeed, under the weaker assumption that its p-primary part is finite), $\mathrm{rk}_p(A/K)$ agrees with $\mathrm{rk}(A/K)$. The p-parity conjecture is the assertion that

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

Note that, without knowing finiteness of the Shafarevich–Tate group, these conjectures for different p are inequivalent, and so there is interest in knowing the p-parity conjecture for multiple values of p.

Over global fields of positive characteristic, the p-parity conejcture holds for all abelian varieties and all primes p thanks to the work of Trihan and Yasuda [TY14]. In the characteristic zero case, Dokchitser and Dokchitser have shown that for all elliptic curves over $\mathbb{Q}$, the p-parity conjecture is true for all primes p [DD10, Theorem 1.4]. More recently, Nekovář has extended this result to replace $\mathbb{Q}$ by any totally real number field, excluding some elliptic curves with potential complex multiplication [Nek13, Theorem A]. For a general number field K, Česnavičius [Čes14b, Theorem 1.4] has shown that the p-parity conjecture holds for elliptic curves possessing a p-isogeny, whilst work of Kramer–Tunnell [KT82] and Dokchitser–Dokchitser [DD11] proves that the 2-parity conjecture holds for all elliptic curves E/K, not over K itself, but over any quadratic extension of K.

For higher dimensional abelian varieties over number fields, much less is known. The most general result at present is due to Coates, Fukaya, Kato and Sujatha, who prove in [CFKS10, Theorem 2.1] that for odd p, the p-parity conjecture holds for a g-dimensional abelian variety with an isogeny of degree p^g, provided some additional technical conditions are satisfied.

In the present work, following on from that of Kramer–Tunnell and Dokchitser–Dokchitser, we consider the 2-parity conjecture for Jacobians of hyperelliptic curves over quadratic extensions of the field of definition. Specifically, we prove the following result, which provides essentially the first examples of the 2-parity conjecture in dimension greater than 1 over number fields (see Convention 1.7.1 for our conventions regarding hyperelliptic curves).

Theorem 1.2.1. *Let K be a number field and L/K a quadratic extension. Let C/K be the hyperelliptic curve $y^2 = af(x)$ with $a \in K^\times$ and $f \in \mathcal{O}_K[x]$ a monic separable polynomial of degree $2g+1$ or $2g+2$, and let J be the Jacobian of C. Suppose that*

(i) for each prime $\mathfrak{p} \lhd \mathcal{O}_K$ not dividing 2 that ramifies in L/K, either J has good reduction at $\mathfrak{p}$ or the reduction $\bar{f}(x)$ mod $\mathfrak{p}$ is cube free,

(ii) for each prime $\mathfrak{p} \lhd \mathcal{O}_K$ dividing 2 which does not split in L/K, J has good reduction at $\mathfrak{p}$, and moreover if such a prime $\mathfrak{p}$ ramifies in L/K then J has good ordinary reduction at $\mathfrak{p}$ and $f(x)$ splits over an odd degree Galois extension of $K_\mathfrak{p}$.

Then the 2-parity conjecture holds for J/L.

In fact, as will be detailed in Section 3.1, we need only assume that J satisfies the above conditions over an odd degree Galois extension F/K (relative to the extension FL/F). Moreover, if the genus of C is 2, one can weaken the assumption that J has good reduction at each prime dividing 2 and inert in L/K to assume only that J has semistable reduction at such primes (see Remark 6.0.15). Moreover, (again see Section 3.1) if a hyperelliptic curve C has a quadratic twist satisfying the conditions of Theorem 1.2.1 for every quadratic extension of K, then C also satisfies the 2-parity conjecture over every quadratic extension of K. Theorem 1.2.1 then gives a large supply of hyperelliptic curves satisfying the 2-parity conjecture over every quadratic extension of their field of definition (for explicit conditions on the polynomial defining C that ensure the conditions of Theorem 1.2.1 at the prime 2 are satisfied, see Corollary 8.3.2).

1.3 Decomposing the parity of the 2-infinity Selmer rank over a quadratic extension

For a global field K and an abelian variety A/K, the root number $w(A/K)$ decomposes as a product of local terms:

$$w(A/K) = \prod_{v \in M_K} w(A/K_v),$$

where here M_K is the set of all places of K and $w(A/K_v) \in \{\pm 1\}$ is the local root number of A over the completion K_v. Thus a natural strategy to prove the p-parity conjecture for some prime p is to first attempt to similarly decompose the parity of the p-infinity Selmer rank into local terms, and then compare these with the local root numbers place

by place. Whilst this is indeed how many of the existing results on the p-parity conjecture proceed, such local decompositions of Selmer ranks can be difficult to obtain. One classical case where this can be done is if $A = E$ is an elliptic curve defined over a number field K and we work not over K itself but over a quadratic extension L/K. Here Kramer [Kra81, Theorem 1] gives a local decompositon of $\mathrm{rk}_2(E/L)$. Before stating Kramer's theorem we need to introduce some notation. We define, for each place v of K, the *local norm map* $N_{L_w/K_v} : E(L_w) \to E(K_v)$ by

$$P \mapsto N_{L_w/K_v}(P) := \sum_{\sigma \in \mathrm{Gal}(L_w/K_v)} \sigma(P)$$

where w is any place of L extending v (by definition, this is the identity map on $E(K_v)$ in the case that L_w/K_v is trivial). The group $E(K_v)/N_{L_w/K_v}E(L_w)$ is a finite dimensional $\mathbb{F}_2$-vector space and we have

Theorem 1.3.1. (Kramer, [Kra81, Theorem 1]). *Let K be a number field, L/K a quadratic extension and E/K an elliptic curve. Then*

$$\mathrm{rk}_2(E/L) \equiv \sum_{v \in M_K} \dim_{\mathbb{F}_2} E(K_v)/N_{L_w/K_v}E(L_w) \pmod 2.$$

The starting point for proving Theorem 1.2.1 is to give a generalisation of this where the elliptic curve E is replaced by the Jacobian of a hyperelliptic curve. In fact, we consider the more general case where the number field K is replaced by an arbitrary global field, L/K is a separable quadratic extension, and the elliptic curve E is replaced by an arbitrary principally polarised abelian variety (the proof of Kramer's theorem likely generalises immediately to elliptic curves over global fields of odd characteristic, but the characteristic 2 case is more difficult and our result is new in this setting even for elliptic curves). Our method of proof is quite different to that of Kramer's and instead is modelled on the proof of [KMR13, Theorem 3.9] of Klagsbrun–Mazur–Rubin, which contains Kramer's theorem as a special case. Much of the technical input for this method of proof is generalised to higher dimensions and arbitrary characteristic by Česnavičius in [Čes14a, Theorem 5.9]. This setup allows us to handle all global fields alike. The result is the following:

Theorem 1.3.2. *Let K be a global field, A/K a principally polarised abelian variety and*

L/K a separable quadratic extension. Let A^L/K be the quadratic twist of A by L. Then

$$\begin{aligned}\mathrm{rk}_2(A/L) \;\equiv\; & \sum_{v\in M_K} \dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v}A(L_w) \\ & + \dim_{\mathbb{F}_2} Ш_0(A/K)[2] + \dim_{\mathbb{F}_2} Ш_0(A^L/K)[2] \pmod 2.\end{aligned}$$

(Here for an abelian variety X/K, we write $Ш_0(X/K)$ for the quotient of the Shafarevich–Tate group of X/K by its maximal divisible subgroup. Implicit in this result is that $\dim_{\mathbb{F}_2} A(K_v)/N_{L_w/K_v}A(L_w)$ is always finite, as is the whole sum.)

When A is an elliptic curve, the Cassels–Tate pairings for A and A^L give non-degenerate, alternating pairings on $\dim_{\mathbb{F}_2} Ш_0(A/K)[2]$ and $\dim_{\mathbb{F}_2} Ш_0(A^L/K)[2]$ respectively, which is why these terms do not feature in Kramer's theorem. However, for general principally polarised abelian varieties, Poonen and Stoll show in [PS99] that these terms can be non-trivial in general (even when one considers A and its quadratic twist simultaneously). This phenomenon therefore provides an obstruction to decomposing the parity of $\mathrm{rk}_2(A/L)$ into local terms. However, when $A = J$ is the Jacobian of a (smooth, proper, geometrically integral) curve C/K, the parity of $\dim_{\mathbb{F}_2} Ш_0(J/K)[2]$ can itself be decomposed into local terms. Specifically, define $i_d(C_v)$ to be -1 if C is deficient over K_v, that is, if it has no K_v-rational divisor of degree $g-1$ where g is the genus of C, and 1 otherwise. Then Poonen and Stoll show in [PS99, Theorem 8] that the parity of $\dim_{\mathbb{F}_2} Ш_0(J/K)[2]$ is even or odd according to whether the number of places $v \in M_K$ for which C is deficient at v is even or odd. Thus if C/K is a hyperelliptic curve, denoting by C^L the quadratic twist of C by L we can combine Theorem 1.3.2 with the result of Poonen–Stoll to obtain a purely local decomposition of the parity of $\mathrm{rk}_2(J/L)$ where J/K is the Jacobian of C. (The key point here is that the Jacobian of the quadratic twist of the curve is the quadratic twist of the Jacobian, so both J/K and J^L/K are Jacobians of explicit curves over K; this is the main reason why all our results on the 2-parity conjecture are restricted to Jacobians of hyperelliptic curves.)

We thus have

Corollary 1.3.3. *Let K be a global field, C/K a hyperelliptic curve, J/K its (canonically principally polarised) Jacobian and L/K a separable quadratic extension. Then*

$$(-1)^{\mathrm{rk}_2(J/L)} = \prod_{v\in M_K} i_d(C_v) i_d(C_v^L) (-1)^{\dim_{\mathbb{F}_2} J(K_v)/N_{L_w/K_v}J(L_w)}.$$

1.4 The Kramer–Tunnell formula

As above, let K be a global field, L/K a separable quadratic extension, C/K a hyperelliptic curve and J/K its Jacobian. Then both $w(J/L)$ and $(-1)^{\mathrm{rk}_2(J/L)}$ have decompositions into local terms. Ideally, one might hope that these local terms simply agree place by place. However, this is not the case and thus the strategy hinges on computing the discrepancy between them and showing that it vanishes globally. In [KT82], Kramer and Tunnell showed that, away from local fields with residue characteristic 2, the two terms we related by a certain Artin symbol (which vanishes globally by the product formula), and conjectured that this was always the case. This was shown to be true by work of Dokchitser–Dokchitser [DD11, Theorem 1.5] and Česnavičius–Imai [ČI15, Theorem 1.3] who dealt with the remaining mixed characteristic and equal characteristic cases respectively. The culmination of this work shows the validity of the following formula, which we refer to as the *Kramer–Tunnell formula*.

Theorem 1.4.1. (Kramer–Tunnell, Dokchitser–Dokchitser, Česnavičius–Imai). *Let K be a local field, L/K a separable quadratic extension and E/K an elliptic curve. Then*

$$w(E/L) = (\Delta_E, L/K)(-1)^{\dim_{\mathbb{F}_2} E(K)/N_{L/K}E(L)}.$$

Here $(\cdot, L/K)$ is the Artin symbol with respect to L/K and Δ_E is the discriminant of any Weierstrass equation defining E. As the discriminant of two such equations differs by a square, so the Artin symbol is independent of this choice. The above formulation of the Kramer–Tunnell formula is the one given in [ČI15], where the equivalence with the statements of [KT82] and [DD11] is shown.

For a hyperelliptic curve C over a local field K, Jacobian J/K, one needs to take account of the extra terms in Corollary 1.3.3 compared with the case of elliptic curves. However, we conjecture that the discrepancy between the local terms appearing in Corollary 1.3.3 and the local root numbers is the same. That is, we make the following conjecture.

Conjecture 1. *Let K be a local field, L/K a separable quadratic extension, C/K a hyperelliptic curve, and J its Jacobian. Then*

$$w(J/L) = (\Delta_C, L/K) i_d(C) i_d(C^L) (-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L)}.$$

Here, analagously to the case of elliptic curves, Δ_C is the discriminant of any Weierstrass equation defining C (see [Liu96, Section 2]). As before, the discriminant of two such

equations differs by a square.

Since the Artin symbol appearing in the conjecture vanishes globally by the product formula, it is immediate from the discussion above that verifying this conjecture implies the 2-parity conjecture. We will prove Conjecture 1 under the assumptions on the reduction of C given by Theorem 1.2.1, hence proving the theorem. Specifically, we prove the following cases of Conjecture 1.

Theorem 1.4.2. *Let K be a local field, L/K a separable quadratic extension, C/K a hyperelliptic curve and J/K its Jacobian. Then Conjecture 1 holds for C and L/K if any of the following holds:*

(i) K is archimedean,

(ii) K has odd residue characteristic and L/K is unramified,

(iii) K has odd residue characteristic, L/K is ramified and either J has good reduction over K or C is given by an equation of the form $y^2 = af(x)$ with $a \in K^\times$ and $f(x) \in \mathcal{O}_K[x]$ monic, integral and with cube free reduction,

(iv) K is a finite extension of $\mathbb{Q}_2$, J has good reduction over K and either L/K is unramified or J further has good ordinary reduction over K and all 2–torsion is defined over an odd degree Galois extension of K.

1.5 Deducing cases of Conjecture 1 for global information

Suppose K is a global field, L/K a separable quadratic extension and C/K a hyperelliptic curve. If we know that Conjecture 1 holds for C over each (non-trivial) local extension L_w/K_v *save one*, then the 2-parity conjecture for C over L becomes equivalent to Conjecture 1 over the remaining local extension. Thus it becomes possible to deduce cases of Conjecture 1 from global information. By carefully choosing our global extension L/K (noting that all relevant local invariants are trivial at places of v split in L) we are able to prove

Theorem 1.5.1. *Let K be a global field of characteristic different from 2, C/K a hyperelliptic curve, J/K its Jacobian and v_0 a place of K. If K has characteristic 0, assume the*

2-parity conjecture for J over every quadratic extension of K. Then Conjecture 1 holds for J/K_{v_0} and every quadratic extension L/K_{v_0}.

Unfortunately, Theorem 1.5.1 falls short of proving Conjecture 1 in positive characteristic (not equal to 2) and giving an implication of the form '2-parity implies Conjecture 1' in characteristic 0, since Conjecture 1 is stated for hyperelliptic curves defined over local fields, whilst Theorem 1.5.1 concerns only curves arising as the base change of one defined over a global field. To bridge the gap, one would want to show that if one fixes a Weierstrass equation of a hyperelliptic curve C defined over a local field, and slightly deforms the coefficients of this curve (with respect to the usual norm on the local field), then all terms in Conjecture 1 remain unchanged. Such 'local constancy' of the relevant invariants is shown for elliptic curves (at least in the characteristic 0 case) in [DD11, Section 3]. We have not currently been able to do this for hyperelliptic curves in higher genus, but hope to address this question in later work. Nethertheless, we believe that Theorem 1.5.1 gives very strong evidence in favour of Conjecture 1, at least for local fields of characteristic different from 2. Whilst we currently do not say anything in the equal characteristic 2 case, we believe that the fact that both the Kramer–Tunnell formula for elliptic curves and the generalisation of Kramer's theorem hold independently of the characteristic of the fields involved make it reasonable to believe Conjecture 1 also holds independently of the characteristic of the local field K.

1.6 Layout of the thesis

The layout of the thesis is as follows. In Chapter 1 we work with arbitrary principally polarised abelian varieties, prove some basic properties of the local norm map which will be of use later and then combine these results with an arithmetic duality theorem due to Česnavičius [Čes14a, Theorem 5.9] to prove Theorem 1.3.2. In Chapter 2 we give some compatibility statements relating to Conjecture 1 and prove some preliminary results which facilitate the computations of the terms involved in Conjecture 1. In Chapter 3 we apply the results of Chapter 2 to prove Conjecture 1 in some simple cases. Namely when the local field K is archimedean, or when the local field K has odd residue characteristic and J/K has good reduction. With these cases in hand, we use the global–to–local argument sketched above to prove Theorem 1.5.1. Chapters 4 and 5 are concerned with proving Conjecture 1 when the local field K has odd residue characteristic and the extension L/K is unramified. This results from a study of the minimal proper regular model of C over

the ring of integers $\mathcal{O}_K$. The key fact we use is that the formation of the minimal proper regular model commutes with unramified base change; this facilitates a comparison between invariants of C and those of its unramified quadratic twist. Attached to the minimal proper regular model $\mathcal{C}$ is a certain corank 1, integral symmetric matrix, whose entries record the intersection numbers between the irreducible components of the special fibre of $\mathcal{C}$. In Chapter 4 we give some results applying to arbitrary corank 1, integral symmetric matrices, and in Chapter 5 we apply the results to prove the case of Conjecture 1 in hand. Chapter 6 proves Conjecture 1 when K has odd residue characteristic, L/K is ramified, and C is given by an equation of the form $y^2 = af(x)$ where $a \in K^\times$, $f(x)$ is monic and integral, and the reduction of $f(x)$ is cube free. This again results from a study of the minimal proper regular model of C and its quadratic twist, but now the fact that L/K is ramified makes the computations significantly more involved, and we find ourselves restricted to the case above where we can explicitly construct the relevant minimal proper regular models from the starting equation. We do however sketch a more general method for attacking Conjecture 1 for ramified extensions, before specialising to this situation. In Chapter 7 we give some partial results towards Conjecture 1 for local fields of residue characteristic 2 which completes the proof of Theorems 1.2.1 and 1.4.2. Finally, in the appendix, we study the behaviour of the 'non-square Shafarevich–Tate group' phenomenon in field extensions and give some applications to the parity conjecture for general principally polarised abelian varieties.

1.7 Notation and conventions

Convention 1.7.1 (Hyperelliptic Curves)**.** In what follows, a *hyperelliptic curve* C over a field K will mean a smooth,proper, geometrically connected curve of genus $g \geq 2$, defined over K, and admitting a finite separable morphism $C \to \mathbb{P}^1_K$ of degree 2 (the assumption that $g \geq 2$ is made since this is the only case of interest and allows us to avoid dealing separately with some special cases in an ad hoc manner). When K has characteristic different from 2, one can always find a separable polynomial $f(x) \in K[x]$ of degree $2g+1$ or $2g+2$ such that C is the union of the two affine open subschemes

$$U_1 = \mathrm{Spec} \frac{K[x,y]}{y^2 - f(x)}$$

and

$$U_2 = \mathrm{Spec}\frac{K[u,v]}{v^2 - g(u)}$$

where $g(u) = u^{2g+2}f(1/u)$ and the schemes glue via the relations $x = 1/u$ and $y = x^{g+1}v$. Conversely, for any such f, the two schemes defined above glue to give a hyperelliptic curve of genus g, the degree 2 morphism to $\mathbb{P}^1_K$ being given by the x-coordinate. By an abuse of notation, we will often say that such a hyperelliptic curve is given by the equation $y^2 = f(x)$. We refer to the points in $U_2(\bar{K}) \setminus U_1(\bar{K})$ as the *points at infinity*. There are two such points if $\deg(f)$ is even, and one otherwise. If the characteristic of K is 2, one needs to use slightly more general Weierstrass equations. Since we shall not work with such equations, we omit the details, but refer the reader to [Liu96, Section 1].

Independently of the characteristic of K, the morphism to $\mathbb{P}^1_K$ induces an extension of function fields $K(C)/K(x)$ (where x is an indeterminate) which is Galois of degree 2. The non-trivial element of this Galois group gives an involution ι of C which we call the *hyperelliptic involution*. Since $g \geq 2$, ι is unique in the sense of [Liu02, Proposition 4.29]. Let L/K be a separable quadratic extension. Then there is a homomorphism from the Galois group of L/K to $\mathrm{Aut}(C)$, sending the non-trivial element to the hyperelliptic involution. Viewed as a 1-cocyle in $\mathrm{H}^1\left(L/K, \mathrm{Aut}_L(C)\right)$, this corresponds to a twist C^L/K of C, becoming isomorphic to C over L. We call this the *quadratic twist* of C by L/K. As the hyperelliptic involution preserves the map to $\mathbb{P}^1_K$, C^L/K is also hyperelliptic. If $\mathrm{char}(K) \neq 2$, C is given by an equation of the form $y^2 = f(x)$, and $L = K(\sqrt{d})$, then C^L is easily seen to be given by an equation of the form $y^2 = df(x)$ (indeed, here the hyperelliptic involution on C just sends y to $-y$). Since the hyperelliptic involution induces multiplication by -1 on the Jacobian of C, the quadratic twist of C by L/K is (isomorphic over K to) the quadratic twist of the Jacobian of C by L/K.

Notation

By a local field we mean a locally compact, valued field and by a global field we mean either a number field or the function field of a connected, smooth proper curve over a finite field. For a global field K, M_K will denote the set of all places of K. For each place $v \in M_K$, K_v will denote the corresponding completion. For K a local or global field, L/K will almost always denote a quadratic extension.

Notation for a non-archimedean local field K:

$\mathcal{O}_K$	ring of integers of K
k	residue field of K
$\bar{K}$	separable closure of K
$\bar{k}$	separable closure of k
K^{nr}	the maximal unramified subextension of $\bar{K}/K$
$(a, L/K)$	Artin symbol of $a \in K^\times$ in L/K. We will always take L/K separable quadratic in which case we regard this symbol as 1 or -1 in the obvious way. If $\mathrm{char}(K) \neq 2$ we conflate this with the Hilbert symbol $(a, b)_K$ where $L = K(\sqrt{b})$.

Notation for a hyperelliptic curve C over a field K:

Δ_C	the discriminant of (any) Weierstrass equation for C. See [Liu96, Section 2]. We will always consider Δ_C only up to squares in K so this does not depend on the choice of Weierstrass equation. If C is given by an equation $y^2 = f(x)$ we can equivalently take Δ_C to be the discriminant of f.
$i_d(C)$	Defined to be -1 if C is deficient over a local field K and 1 otherwise. See [PS99, Section 8].
C^L	the quadratic twist of C by the separable quadratic extension L/K
J/K	the Jacobian of C/K
J^L/K	the quadratic twist of J by the separable quadratic extension L/K
$c(J/K)$	the local Tamagawa number (for K a local field)
$Ш(J/K)$	the Shafarevich-Tate group of J/K (for K a number field)
$Ш_0(J/K)$	the quotient of $Ш(J/K)$ by its maximal divisible subgroup
$w(J/K)$	the global root number of J/K for K a global field, or the local root number of J/K for K a local field.

Chapter 2

Arithmetic duality

The main goal of this chapter is to prove Theorem 1.3.2, decomposing the parity of the 2-infinity Selmer rank of a principally polarised abelian variety over a separable quadratic extension of its field of definition. This will ultimately result from [Čes14a, Theorem 5.9], due to Česnavičius, which gives a local decompostion, up to squares, of the difference between Selmer groups whose defining local conditions satisfy certain assumptions. The Selmer groups we are interested in comparing are the 2-Selmer groups over the ground field of A and its quadratic twist respectively. However, some work is required both to show that these Selmer groups satisfy the conditions of loc. cit., and to show that the local terms arising upon applying this result may be interpreted in terms of the local norm map. We begin by proving some basic properties of the cokernel of the local norm map, which will be used throughout this thesis, but which are also needed for the second of these aims. After that, we study certain quadratic forms defined on local cohomology groups, which provides the technical input required in order to apply the aforementioned result of Česnavičius.

2.1 Basic properties of the local norm map

In this section we prove some basic properties of the cokernel of the local norm map. We work with arbitrary principally polarised abelian varieties as everything in this section goes through in this generality. We begin by reviewing a general method for constructing isogenies between twists of abelian varieties, due to Milne [Mil72, Section 2], and apply it to construct an isogeny which will be of particular interest in what follows. See [DD10, Section 4.2] for a similar summary.

2.1.1 Isogenies between twists of products of abelian varieties

Let K be a field, L/K a finite Galois extension with Galois group G, and A/K a principally polarised abelian variety, with fixed principal polarisation μ.

For $n \geq 1$, view $\mathrm{Mat}_n(\mathbb{Z})$ and $\mathrm{GL}_n(\mathbb{Z})$ inside $\mathrm{End}_K(A^n)$ (resp. $\mathrm{Aut}_K(A^n)$) in the obvious way. If M is a free $\mathbb{Z}$-module of rank n, equipped with a linear action of G, then specifying a basis for M we obtain a homomorphism $\rho : G \to GL_n(\mathbb{Z})$ which we view as a one cocycle ρ_σ from G to $\mathrm{Aut}_L(A^n)$. Thus there is an L/K-twist B of A, equipped with an L-isomorphism $\psi : A \to B$, such that $\psi^{-1}\psi^\sigma = \rho_\sigma$ for all $\sigma \in G$. We denote this twist by $(A \otimes M, \psi)$, or just $A \otimes M$.

If M_1 and M_2 are two G-modules of rank n, and $f : M_1 \to M_2$ is an injective $\mathbb{Z}[G]$-module homomorphism, then fixing bases for M_1 and M_2, we view f as a matrix $X_f \in \mathrm{Mat}_n(\mathbb{Z})$ and hence as an element of $\mathrm{End}_K(A^n)$. Then $\phi_f = \psi_{M_2} X_f \psi_{M_1}^{-1}$ is an isogeny from $A \otimes M_1$ to $A \otimes M_2$ defined over K and this association is functorial; given $f : M_1 \to M_2$ and $g : M_2 \to M_3$ as above, we have $\phi_g \circ \phi_f = \phi_{gf}$. Now let $\hat{A}/K$ denote the dual abelian variety of A and $\mu : A \to \hat{A}$ a principal polarisation, defined over K. If $\phi : A^n \to A^n$ is an isogeny represented by the matrix $\phi = (\phi_{ij})$ for $\phi_{ij} \in \mathrm{End}(A)$, then the Rosati involution $\phi^\dagger = \lambda^{-1}\phi^t\lambda$ (where ϕ^t is the dual isogeny) of ϕ with respect to the product polarisation $\lambda = \mu^n$ is given by $\phi^\dagger = (\phi_{ji}^\dagger)$ where $\phi_{rs}^\dagger$ denotes the Rosati involution of ϕ_{rs} with respect to μ. For an L/K-twist $(A \otimes M, \psi)$ of A^n, cocycle ρ_σ, the principal polarisation $\lambda_M = (\psi^t)^{-1}\lambda\psi^{-1}$ on $A \otimes M$ is defined over K if and only if $\rho_\sigma^\dagger \rho_\sigma = \mathrm{id}_{A^n}$ for all $\sigma \in G$ [How01, Proposition 2.2].

2.1.2 An isogeny between twists of A^2

Retaining the setup of Section 2.1.1, suppose now that L/K is a separable quadratic extension and let σ denote the generator of $G = \mathrm{Gal}(L/K)$. Then $A \otimes \mathbb{Z}[G] = \mathrm{Res}_{L/K}(A)$ is the Weil restriction of A/L to K, and letting M be the G-module $\mathbb{Z} \oplus \mathbb{Z}$ where σ acts trivially on the first factor and as multiplication by -1 on the second factor, we have $A \otimes M = A \times A^L$. By the discussion in the previous subsection, we immediately see that the product polarisation on $A \times A$ descends to principal polarisations on both $\mathrm{Res}_{L/K}(A)$ and $A \times A^L$ respectively. Similarly, the principal polarisation μ on A descends to one on the quadratic twist A^L. We have an injective homomorphism of G-modules $f : \mathbb{Z}[G] \to M$ defined by

$$f(a + b\sigma) = (a + b, a - b)\,,$$

corresponding to the matrix

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

We thus obtain an isogeny

$$\phi_f : \mathrm{Res}_{L/K}(A) \longrightarrow A \times A^L.$$

Fix L-isomorphisms $\psi : A \to A^L$ such that $\psi^{-1}\psi^\sigma = [-1]$ and $\psi' : A \times A \to \mathrm{Res}_{L/K}(A)$ such that $(\psi')^{-1}(\psi')^\sigma$ is the endomorphism of $A \times A$ sending (P, Q) to (Q, P). Via the isomorphism ψ we identify $A^L(L)$ with $A(L)$ and $A^L(K)$ as a subgroup $\ker\left(N_{L/K} : A(L) \to A(K)\right)$ of $A(L)$. Moreover, under the identification above, the map $N_{L/K} : A^L(L) \to A^L(K)$ then becomes the map sending $P \in A(L)$ to $P - \sigma(P)$. To avoid confusion, we denote this map by $N^L_{L/K}$. Similarly, we use the isomorphism ψ' to identify $\mathrm{Res}_{L/K}(A)(K)$ with the subgroup

$$\{(P, Q) \in A(L) \times A(L) \ : \ Q = \sigma(P)\}$$

of $A(L) \times A(L)$ and projection onto the first factor gives an isomorphism onto $A(L)$. With the identifications above, the map ϕ_f on K-points corresponds to the homomorphism $A(L) \longrightarrow A(K) \times A^L(K)$ given by $P \mapsto \left(N_{L/K}(P), N^L_{L/K}(P)\right)$.

Lemma 2.1.1. *The natural inclusion $A^L(K) \subseteq A(K) \times A^L(K)$ sending P to $(0, P)$ induces an injection*

$$A^L(K)/2A^L(K) \hookrightarrow \left(A(K) \times A^L(K)\right)/\phi_f\left(\mathrm{Res}_{L/K}(A)(K)\right)$$

whose cokernel is isomorphic to $A(K)/N_{L/K}A(L)$ via projection onto the first factor.

Proof. This is immediate from the description, given above, of the map ϕ_f on K-points. □

2.1.3 The cokernel of the local norm map

Now take K to be a local field, L/K a separable quadratic extension and A/K a principally polarised abelian variety, with fixed principal polarisation μ defined over K. The short exact sequence (of fppf group schemes over K)

$$0 \to A[2] \longrightarrow A \xrightarrow{[2]} A \longrightarrow 0$$

yields an injection

$$A(K)/2A(K) \overset{\delta}{\hookrightarrow} H^1_{\mathrm{fppf}}(K, A[2]).$$

We have also the corresponding injection for A^L. Let $\psi : A \times_K L \to A^L \times_K L$ be such that $\psi^{-1}\psi^\sigma = [-1]$ where σ is the non-trivial element of $\mathrm{Gal}(L/K)$. This restricts to an isomorphism of group schemes $A[2] \cong A^L[2]$ over K and hence induces an isomorphism $\tilde{\psi}^{-1} : \mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2]) \xrightarrow{\sim} \mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$. Denote by δ^L the resulting injection

$$\delta^L : A^L(K)/2A^L(K) \hookrightarrow \mathrm{H}^1_{\mathrm{fppf}}(K, A[2]).$$

Lemma 2.1.2. *We have*

$$A(K)/N_{L/K}A(L) \cong \frac{\delta\left(A(K)/2A(K)\right)}{\delta\left(A(K)/2A(K)\right) \cap \delta^L\left(A^L(K)/2A^L(K)\right)}.$$

Proof. Let ψ be as above, and let $\psi' : A \times A \to \mathrm{Res}_{L/K}A$ (over L) be the isomorphism coming from the construction of $\mathrm{Res}_{L/K}$ as a twist of $A \times A$. Further, let ϕ be the isogeny of Section 2.1.2. We then have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A^L[2] & \longrightarrow & A^L & \xrightarrow{2} & A^L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \psi' \circ (\psi^{-1} \times [-1] \circ \psi^{-1})} & & \downarrow{\scriptstyle 0 \times \mathrm{id}} & & \\
0 & \longrightarrow & \left(\mathrm{Res}_{L/K}A\right)[\phi] & \longrightarrow & \mathrm{Res}_{L/K}A & \xrightarrow{\phi} & A \times A^L & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow{\scriptstyle \psi' \circ (\mathrm{id} \times \mathrm{id})} & & \uparrow{\scriptstyle \mathrm{id} \times 0} & & \\
0 & \longrightarrow & A[2] & \longrightarrow & A & \xrightarrow{2} & A & \longrightarrow & 0,
\end{array}$$

(all maps shown descending to K) and one easily checks that the restrictions

$$\psi' \circ (\psi^{-1} \times [-1]\psi^{-1}) : A^L[2] \longrightarrow \mathrm{Res}_{L/K}A[\phi]$$

and

$$\psi' \circ (1 \times 1) : A[2] \longrightarrow \mathrm{Res}_{L/K}A[\phi]$$

are isomorphisms and that the induced map $A^L[2] \xrightarrow{\sim} A[2]$ is just the map ψ. This induces

a commutative diagram

$$\begin{array}{ccc} A^L(K)/2A^L(K) & \xrightarrow{\delta} & \mathrm{H}^1_{\mathrm{fppf}}\left(K, A^L[2]\right) \\ \downarrow & & \downarrow \\ \left(A(K)\times A^L(K)\right)/\phi\left((\mathrm{Res}_{L/K}A)(K)\right) & \xrightarrow{\delta} & \mathrm{H}^1_{\mathrm{fppf}}\left(K, \left(\mathrm{Res}_{L/K}A\right)[\phi]\right) \\ \uparrow & & \uparrow \\ A(K)/2A(K) & \xrightarrow{\delta} & \mathrm{H}^1_{\mathrm{fppf}}\left(K, A[2]\right) \end{array}$$

and we are thus reduced to showing that

$$A(K)/N_{L/K}A(L) \cong \frac{A(K)/2A(K)}{A(K)/2A(K)\cap A^L(K)/2A^L(K)}$$

with the groups on the right being viewed inside $\left(A(K)\times A^L(K)\right)/\phi\left((\mathrm{Res}_{L/K}A)(K)\right)$. To see this, note that

$$\frac{A(K)/2A(K)}{A(K)/2A(K)\cap A^L(K)/2A^L(K)} \cong \frac{A(K)/2A(K)+A^L(K)/2A^L(K)}{A^L(K)/2A^L(K)}$$

$$= \frac{\left(A(K)\times A^L(K)\right)/\phi\left((\mathrm{Res}_{L/K}A)(K)\right)}{A^L(K)/2A^L(K)}$$

whence the result follows from Lemma 2.1.1. □

Remark 2.1.3. *In the case where K has characteristic not equal to 2, we may interpret the fppf cohomology groups as Galois cohomology groups. In this context, the result is shown in* [MR07, Proposition 5.2] *via an explicit cocycle computation inside* $\mathrm{H}^1(K, A[2])$.

Corollary 2.1.4. *For any abelian variety A over a local field K, and any separable quadratic extension L/K, the group $A(K)/N_{L/K}A(L)$ is a finite dimensional $\mathbb{F}_2$-vector space.*

Proof. Clearly $A(K)/N_{L/K}A(L)$ is annihilated by multiplication by 2, being a quotient of $A(K)/2A(K)$. It remains to prove finiteness. In the case where K has characteristic different from 2, the group $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ is well known to be finite and the result is immediate. In general, the groups $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ and $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ can be infinite, but carry a natural topology making them into Hausdorff, locally compact abelian topological groups (see [Česl4c] for a discussion of the topology carried by cohomology groups of finite type

group schemes over a local field). Moreover, the isomorphism between $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ and $\mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2])$ used previously is a homeomorphism since it is induced by an isomorphism of the underlying group schemes. Now the image of $A(K)/2A(K)$ inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ is compact and open (combine, for example, [Čes14c, Section 1.4] which shows that the connecting morphism is both closed and open, and Lemma 2.12.1 of op. cit. which shows that $A(K)$ is compact (with the natural topology coming from that on K)). Now the result follows since Lemma 2.1.2 realises $A(K)/N_{L/K}A(L)$ as the quotient of a compact topological group by an open subgroup. □

Remark 2.1.5. *In the case where A is an elliptic curve, the above result is shown in* [KT82, Proposition 7.3]*, although the proof is different.*

In fact, the finiteness part of Corollary 2.1.4 holds for general finite separable extensions, not just when L/K is quadratic. The following argument, which proves this, is due to Kęstutis Česnavičius.

Proposition 2.1.6. *Let K be a local field, A/K an abelian variety and L/K a finite separable extension. Then the group*

$$A(K)/N_{L/K}A(L)$$

is finite.

Proof. Since L/K is separable, the Weil restriciton of scalars, $\mathrm{Res}_{L/K}(A_L)$, is also an abelian variety over K and (also over K) there is a norm morphism of abelian varieties from $\mathrm{Res}_{L/K}(A_L)$ into A. The Lie algebra, $\mathrm{Lie}\left(\mathrm{Res}_{L/K}(A)\right)$, of $\mathrm{Res}_{L/K}(A)$ is canonically isomorphic to $\mathrm{Lie}(A_L) = \mathrm{Lie}(A) \otimes_K L$ and the induced map on Lie algebras associated to the norm morphism above is the map $\mathrm{id} \otimes \mathrm{Trace}_{L/K}$ from $\mathrm{Lie}(A) \otimes_K L$ to $\mathrm{Lie}(A)$. The separability of L/K means that the trace map from L to K is surjective, and hence so is the map of Lie algebras. The norm morphism is therefore smooth and induces an open map on K-points. This implies finiteness of its cokernel (as its image is a compact topological group), which is the required result. □

The final lemma of this section expresses the cokernel of the local norm map in terms of Tamagawa numbers. We will not use this in the proof of Theorem 1.3.2, but it will be very useful later on when we prove cases of Conjecture 1, and we find this a convenient place to record it. The special case of this result for elliptic curves is due to Kramer and Tunnell

[KT82, Corollary 7.6]. Here and in what follows, we denote by $c(A/K)$ the Tamagawa number of A/K. That is, the order of the k-rational points in the group of components of the Neron model of A over $\mathcal{O}_K$ (see [BL99] for a definition).

Lemma 2.1.7. *Assume the residue characteristic of K is odd. Then*

$$\dim_{\mathbb{F}_2} A(K)/N_{L/K}A(L) = \mathrm{ord}_2 \frac{c(A/K)c(A^L/K)}{c(A/L)}.$$

Proof. Let $X = \mathrm{Res}_{L/K}A$ and $Y = A \times A^L$. Since K has odd residue characteristic, it follows from Lemma 2.1.1 and a formula of Schaefer [Sch96, Lemma 3.8] that

$$\dim_{\mathbb{F}_2} A(K)/N_{L/K}A(L) = \mathrm{ord}_2 \frac{c(Y/K)}{c(X/K)}.$$

The behaviour of Tamagawa numbers under Weil restriction is studied by Lorenzini in [Lor11] whose Proposition 3.19 gives $c(X/K) = c(A/L)$. Since we also have $c(Y/K) = c(A/K)c(A^L/K)$ (see part (c) of the proof of the aforementioned proposition) we obtain the result. □

2.2 Quadratic forms on $\mathbf{H^1_{fppf}}(K, A[2])$

We maintain the notation of Section 2.1.3, so that in particular, K is a local field (though this is not really important for the time being) and A/K a principally polarised abelian variety. In this section we show that the images of δ and δ^L (in the notation of Lemma 2.1.2) inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ are both maximal isotropic subspaces with respect to a certain quadratic form q on $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ constructed by Poonen and Rains in [PR12, Section 4]. This will be important for a number of later results and underpins the arithmetic duality arguments that lead to Theorem 1.3.2. In loc. cit. it is shown that the image of δ is a maximal isotropic subspace for q. Similarly, the image of $A^L(K)/2A^L(K)$ in $\mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2])$ is maximal isotropic for the analagous quadratic form q^L on $\mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2])$. The problem is then to show that the isomorphism $\tilde{\psi}^{-1} : \mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2]) \xrightarrow{\sim} \mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ of the previous section identifies the quadratic forms q and q^L. In fact, there are some choices to be made in the construction of q and q^L; we will show that q and q^L may be constructed in such a way that they do become indeed identified by the map $\tilde{\psi}^{-1}$. The case of elliptic curves is treated in [KMR13, Lemma 5.2] where a choice is made at the outset for the quadratic forms and it is then shown that they agree.

We begin by recalling the construction of the relevant quadratic forms from [PR12, Section 4]. Fix a principal polarisation μ on A, defined over K. Whilst it is not necessarily true that μ is of the form $\phi_{\mathcal{L}}$ for a symmetric line bundle $\mathcal{L}$ on A (even with the symmetry condition (i.e. $[-1]^*\mathcal{L} \cong \mathcal{L}$) dropped), it is the case that 2μ is of this form (we use the same definition of $\phi_{\mathcal{L}}$ as in [PR12, Section 4] and refer to there for more details). Specifically, if one takes $\mathcal{L} = (1,\mu)^*\mathcal{P}$ where $\mathcal{P}$ is the Poincare bundle on $A \times \hat{A}$ (here $\hat{A}$ is the dual abelian variety) then $\mathcal{L}$ is symmetric and one has $2\mu = \phi_{\mathcal{L}}$ (see Remark 4.5. of loc. cit.). The choice of $\mathcal{L}$ subject to the condition $2\mu = \phi_{\mathcal{L}}$ is determined up to elements of $\hat{A}[2](K)$, as follows from the exact sequence (14) of [PR11].

Now let $\mathcal{H}(\mathcal{L})$ be the Heisenberg group attached to $\mathcal{L}$ (again, see [PR12, Section 4] for the definition and basic properties). It is a finite-type group scheme over K and fits in an exact sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{H}(\mathcal{L}) \longrightarrow A[2] \longrightarrow 0.$$

Then by [PR12, Corollary 4.7], the connecting homomorphism $q : \mathrm{H}^1_{\mathrm{fppf}}(K, A[2]) \longrightarrow \mathrm{H}^2_{\mathrm{fppf}}(K, \mathbb{G}_m)$ is a quadratic form whose associated bilinear form is that given by the Weil pairing $e_2^{\mu} : A[2] \times A[2] \to \mathbb{G}_m$ associated to the polarisation μ and cup-product. To define e_2^{μ}, let

$$e_2 : A[2] \times \hat{A}[2] \longrightarrow \mathbb{G}_m$$

be the Weil pairing, and define $e_2^{\mu}(x,y) = e_2(x, \mu(y))$. For a local field K, the composition $\mathrm{inv} \circ q : \mathrm{H}^1_{\mathrm{fppf}}(K, A[2]) \longrightarrow \mathbb{Q}/\mathbb{Z}$ (here inv denotes the local invariant map of K) is continuous and the image of $\delta : A(K)/2A(K) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ is a compact open, maximal isotropic subgroup of the quadratic space $\big(\mathrm{H}^1_{\mathrm{fppf}}(K, A[2]), \mathrm{inv} \circ q\big)$.

As discussed above, we wish to study the effect of 'quadratic twisting' this construction. Since the quadratic form q depends on $\mathcal{L}$ rather than just the polarisation μ, we write $q_{\mathcal{L}}$ in what follows. As in Section 2.1.2, the principal polarisation μ descends to a principal polarisation μ^L on the twist A^L and so we obtain associated quadratic forms on $\mathrm{H}^1_{\mathrm{fppf}}(K, A^L[2])$ too. However, since it is the data of a symmetric line bundle that yields the quadratic form, we are additionally interested in descending symmetric line bundles to the quadratic twist.

Lemma 2.2.1. *Let K be a field and A/K an abelian variety. Further, let L/K be a separable quadratic extension and $\mathcal{L}$ a symmetric line bundle on A. Then there is a symmetric line bundle $\mathcal{L}^L$ on A^L/K which becomes isomorphic to $\mathcal{L}$ upon base-change to L.*

Proof. By an abuse of notation, write $\mathcal{L}$ also for the line bundle on $A \times_K L$ obtained

by pulling back $\mathcal{L}$ under the canonical projection. Let σ be the non-trivial element of $\mathrm{Gal}(L/K)$. Then as $\mathcal{L}$ arises as the base-change of a line bundle on A/K, there is a natural isomorphism

$$\rho_\sigma : \sigma^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}$$

such that $\rho_\sigma \circ \sigma^*(\rho_\sigma)$ is the identity map on $\sigma^*\sigma^*\mathcal{L} = \mathcal{L}$. To descend $\mathcal{L}$ to A^L/K, we need an construct the analagous isomorphism for the twisted Galois action where the generator of $\mathrm{Gal}(L/K)$ acts as $\sigma \circ [-1]$. Using the symmetry of the line bundle $\mathcal{L}$, we may fix an isomorphism $\tau : [-1]^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}$ which we choose to be normalised in such a way that the restriction of τ to the identity section is trivial. In this case, the composition

$$\mathcal{L} \xrightarrow{[-1]^*\tau} [-1]^*\mathcal{L} \xrightarrow{\tau} \mathcal{L}$$

is the identity (as can be seen by restricting to the identity section). Moreover, the map τ commutes with the (untwisted) action of σ since the normalisation described above uniquely determines τ and we could have done this over K rather than L.

Now define the isomorphism $\rho'_\sigma : [-1]^*\sigma^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}$ as the composition

$$[-1]^*\sigma^*\mathcal{L} \xrightarrow{[-1]^*(\rho_\sigma)} [-1]^*\mathcal{L} \xrightarrow{\tau} \mathcal{L}.$$

Using the cocycle property for ρ_σ, and the normalisation and Galois invariance of τ, one easily verifies that $\rho'_\sigma \circ (\sigma \circ [-1])^*(\rho'_\sigma)$ is the identity map, and hence the line bundle $\mathcal{L}$ descends to A^L/K. Moreover, it is clear that the isomorphism τ is Galois equivariant for the twisted Galois action too, hence the descended line bundle is also symmetric. □

Returning to the situation where $\mathcal{L}$ is a symmetric line bundle on A such that $2\mu = \phi_{\mathcal{L}}$, we see that the symmetric line bundle $\mathcal{L}^L$ on A^L provided by Lemma 2.2.1 is such that $2\mu^L = \phi_{\mathcal{L}^L}$.

We now wish to compare the quadratic forms $q_{\mathcal{L}}$ and $q_{\mathcal{L}^L}$ on $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ (where we view $q_{\mathcal{L}^L}$ as a quadratic form on $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ via $\tilde{\psi}^{-1}$ as usual). As in (the proof of) [PR12, Corollary 4.7] there is a natural isomorphism of group schemes over K between $\mathcal{H}(\mathcal{L})$ and $\mathcal{H}([-1]^*\mathcal{L})$, and composing with the isomorphism $\mathcal{H}([-1]^*\mathcal{L}) \xrightarrow{\sim} \mathcal{H}(\mathcal{L})$ induced by the normalised isomorphism $\tau : [-1]^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}$ (in fact, this last map is independent of the choice of isomorphism between $[-1]^*\mathcal{L}$ and $\mathcal{L}$) we obtain an automorphism i of the Heisenberg group $\mathcal{H}(\mathcal{L})$.

Lemma 2.2.2. *If the automorphism i of $\mathcal{H}(\mathcal{L})$ described above is the identity, the quadratic*

forms $q_{\mathcal{L}}$ and $q_{\mathcal{L}^L}$ on $H^1_{fppf}(K, A[2])$ agree.

Proof. We will construct a morphism $f : \mathcal{H}(\mathcal{L}) \longrightarrow \mathcal{H}(\mathcal{L}^L)$ of group schemes over K fitting into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}(\mathcal{L}) & \longrightarrow & A[2] & \longrightarrow & 0 \\ & & \| & & \downarrow f & & \downarrow \psi & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}(\mathcal{L}^L) & \longrightarrow & A^L[2] & \longrightarrow & 0. \end{array}$$

From here, the result follows from the construction of the quadratic form and standard properties of the connecting morphism in the long exact sequence for fppf-cohomology.

To construct f, we note that the identifications above of A with A^L and $\mathcal{L}$ with $\mathcal{L}^L$ after base change to L induces an isomorphism between $\mathcal{H}(\mathcal{L})$ and $\mathcal{H}(\mathcal{L}^L)$ fitting into the diagram above *after base change to L*. We then need to check that this isomorphism descends to one over K. Using the group-functor description of the Heisenberg group as in [PR12, Section 4] and unwinding the definitions of the relevant morphisms, interpreted as natural transformations between the associated group functors, one sees that the Galois invariance of the morphism described follows from the statement that i acts trivially on $\mathcal{H}(\mathcal{L})$. □

We are now left with the question of when the automorphism i of $\mathcal{H}(\mathcal{L})$ defined above is trivial. This is not always the case, and depends on the choice of $\mathcal{L}$. However, we will show that $\mathcal{L}$ can, in our case, be chosen in such a way as to force i to be trivial.

Associated to $\mathcal{L}$, as in [PR11, Section 3.4], we have a map of fppf-sheaves

$$\mathfrak{q}_{\mathcal{L}} : A[2] \longrightarrow \mu_2.$$

To define $\mathfrak{q}_{\mathcal{L}}$, let S be a K-scheme and $x : S \longrightarrow A[2]$ be a morphism (viewed as a morphism into A in the obvious way). Pulling back the normalised isomorphism $\tau : [-1]^*\mathcal{L} \longrightarrow \mathcal{L}$ along x gives an automorphism of the line bundle $x^*\mathcal{L}$ on S (since $[-1] \circ x = x$), and hence a section of $\mathbb{G}_m$ over S. Since $[-1]^*(\tau) = \tau^{-1}$, it follows that $x^*(\tau)$ actually gives a section of μ_2 over S. This defines to map $\mathfrak{q}_{\mathcal{L}}$.

Lemma 2.2.3. *Let S be a K-scheme. Then the automorphism i of $\mathcal{H}(\mathcal{L})$ sends a pair $(x, \phi) \in \mathcal{H}(\mathcal{L})(S)$ to the pair $(x, \mathfrak{q}_{\mathcal{L}}(x)\phi)$.*

Proof. This is shown in [Mum66, Proposition 2.3] over an algebraically closed field of characteristic different from 2. The argument carries over unchanged upon replacing geometric

points with arbitrary scheme-valued points. □

To summarise the discussion above, we now see that if $\mathcal{L}$ is chosen in such a way that the map $\mathfrak{q}_{\mathcal{L}} : A[2] \longrightarrow \mu_2$ is trivial, then the two quadratic forms $q_{\mathcal{L}}$ and $q_{\mathcal{L}^L}$ on $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ coincide.

The following Lemma was explained to us by Kęstutis Česnavičius.

Lemma 2.2.4. *Let $\mu : A \longrightarrow \hat{A}$ be a principal polarisation, defined over K, and let $\mathcal{P}$ be the Poincare divisor on $A \times \hat{A}$. Then the map $\mathfrak{q}_{\mathcal{L}} : A[2] \longrightarrow \mu_2$ attached to the symmetric line bundle $\mathcal{L} := (1, \mu)^*\mathcal{P}$ on A is trivial.*

Proof. Since we can check triviality of this morphism after an fppf (or indeed fpqc) extension, we are at liberty to assume that μ is of the form $\phi_{\mathcal{M}}$ for a symmetric line bundle $\mathcal{M}$ on A (this need not be true over K, as is discussed in [PR12, Remark 4.5]). In this case, we have $\mathcal{L} \cong \mathcal{M}^2$. Indeed, it follows from the definition of the Poincare bundle that the pull back of $\mathcal{P}$ under the morphism

$$1 \times \mu : A \times A \longrightarrow A \times \hat{A}$$

is equal to $m^*\mathcal{M} \otimes p_1^*\mathcal{M}^{-1} \otimes p_2^*\mathcal{M}^{-1}$ where here $m : A \times A \to A$ is multiplication, and p_1 and p_2 are the first and second projections $A \times A \to A$ respectively. Pulling back further along the diagonal morphism $A \to A \times A$ yields

$$\mathcal{L} \cong [2]^*\mathcal{M} \otimes \mathcal{M}^{-2}.$$

Now [Mil86, Corollary 6.6] gives $[2]^*\mathcal{M} \cong \mathcal{M}^3 \otimes [-1]^*\mathcal{M}$. Thus we finally obtain

$$\mathcal{L} \cong \mathcal{M} \otimes [-1]^*\mathcal{M}.$$

Since $\mathcal{M}$ is symmetric, $\mathcal{L} \cong \mathcal{M}^2$. It now follows from [PR11, Proposition 3.6 (a)] that the associated quadratic form $\mathfrak{q}_{\mathcal{L}}$ is trivial. □

Remark 2.2.5. *Suppose that we take $\mathcal{L}$ as above, and then replace it by $\mathcal{L}' = \mathcal{L} \otimes \mathcal{F}$ where $\mathcal{F} \in \hat{A}[2](K)$. Then by* [PR11, Proposition 3.2 (a) and (b)], *$\mathfrak{q}_{\mathcal{L}'}$ is now $e_2(-, \mathcal{F})$ where e_2 denotes the Weil-pairing on $A[2] \times \hat{A}[2]$. Thus in general, having imposed the condition $\phi_{\mathcal{L}} = 2\mu$, there is only one choice for $\mathcal{L}$ to make $\mathfrak{q}_{\mathcal{L}}$ trivial.*

Combining the discussion above with [PR12, Proposition 4.11], we have proved.

Proposition 2.2.6. *Let K be a local field, A/K a principally polarised abelian variety with fixed principal polarisation μ defined over K and L/K a separable quadratic extension. Let $\mathcal{L}$ be the symmetric line bundle $(1,\mu)^*\mathcal{P}$ on A, and $\mathcal{L}^L$ the corresponding symmetric line bundle on the quadratic twist A^L. Then under the isomorphism*

$$\tilde{\psi}^{-1} : H^1_{fppf}(K, A^L[2]) \xrightarrow{\sim} H^1_{fppf}(K, A[2])$$

(as detailed at the start of this section) the quadratic forms $q_{\mathcal{L}}$ and $q_{\mathcal{L}^L}$ are identified. In particular, both $\delta(A(K)/2A(K))$ and $\delta^L(A^L(K)/2A^L(K))$ are open, compact, maximal isotropic subspaces of the non-degenerate quadratic space $\left(H^1_{\mathrm{fppf}}(K, A[2]), \mathrm{inv} \circ q\right)$.

Corollary 2.2.7. *Let K be a local field, A/K a principally polarised abelian variety with fixed principal polarisation μ defined over K and L/K a separable quadratic extension. Let*

$$\langle\ ,\ \rangle : H^1_{fppf}(K, A[2]) \times H^1_{fppf}(K, A[2]) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

be the pairing induced by combining the Weil pairing on $A[2]$ associated to μ, cup product, and the local invariant map. Let $\langle\ ,\ \rangle_L$ be the pairing on $H^1_{fppf}(K, A[2])$ coming from the analogous construction for the twist A^L (with respect to the polarisation μ^L) and the usual identification of $H^1_{fppf}(K, A[2])$ with $H^1_{fppf}(K, A^L[2])$. Then the pairings $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle_L$ coincide.

Proof. Let $q_{\mathcal{L}}$ and $q^L_{\mathcal{L}}$ be the quadratic forms on $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ of Proposition 2.2.6. Then by [PR12, Corollary 4.7], the quadratic forms $q_{\mathcal{L}}$ and $q^L_{\mathcal{L}}$ induce the pairings $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle_L$ respectively. Since the quadratic forms agree, so do the resulting pairings. □

Before proceeding with the proof of Corollary 1.3.3, we record 2 additional corollaries of Proposition 2.2.6 which will be useful when proving compatibility results involving Conjecture 1.

Corollary 2.2.8. *Let K be a local field, A/K a principally polarised abelian variety and L/K a separable quadratic extension. Then*

$$\dim_{\mathbb{F}_2} A(K)/N_{L/K}A(L) = \dim_{\mathbb{F}_2} A^L(K)/N_{L/K}A^L(L).$$

Proof. Let $X = \delta(A(K)/2A(K))$ and $Y = \delta^L(A^L(K)/2A^L(K))$ inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ and let $q = q_{\mathcal{L}}$ be the quadratic form of Proposition 2.2.6. Then by Lemma 2.1.2 we need to

show that the dimensions of

$$X/X \cap Y \quad \text{and} \quad Y/X \cap Y$$

agree. Now since X and Y are both maximal isotropic with respect to q, we have $(X \cap Y)^{\perp} = X + Y$ whence, as in [PR12, Remark 2.4], the restriction of q gives a non-degenerate quadratic form on the now finite dimensional (by the argument of Corollary 2.1.4) $\mathbb{F}_2$-vector space $Z := (X+Y)/X \cap Y$. Write $\bar{X}$ and $\bar{Y}$ for the images of X and Y in Z. Then we can equivalently show that $\bar{X}$ and $\bar{Y}$ have the same dimension. As everything is now finite dimensional, we are reduced to showing that $\bar{X}$ and $\bar{Y}$ has the same dimension. But this is now clear since these are maximal isotropic subspaces of the finite dimensional space Z, and hence both have dimension equal to half the (necessarily even) dimension of Z. □

Corollary 2.2.9. *Let K be a local field and A/K a principally polarised abelian variety. Let L_1/K and L_2/K be distinct, separable quadratic extensions and L_3/K be the third quadratic subextension of L_1L_2/K. Then*

$$\dim_{\mathbb{F}_2} A(K)/N_{L_1/K}A(L_1) + \dim_{\mathbb{F}_2} A(K)/N_{L_2/K}A(L_2) \equiv \dim_{\mathbb{F}_2} A^{L_1}(K)/N_{L_3/K}A^{L_1}(L_3) \pmod 2.$$

Proof. Again this will follow from the images of the various Kummer maps being maximal isotropic subspaces of $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$. The case where A/K is an elliptic curve and K has characteristic 0 is [KMR13, Lemma 5.6] and the argument is the same, save for a modification to allow for the possibility that $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ is infinite. Write X_0 for the image of δ inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$, and similarly for $i = 1, 2, 3$, write X_i for the image of δ^{L_i} inside the same space. Then

$$A(K)/N_{L_i/K}A(L_i) = X_0/(X_0 \cap X_i)$$

for $i = 1, 2, 3$, and

$$A^{L_1}(K)/N_{L_3/K}A^{L_1}(L_3) = X_1/(X_1 \cap X_2).$$

Then each X_i is a maximal isotropic subspace of $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$, endowed with the quadratic form $q_{\mathcal{L}}$ of Proposition 2.2.6. As in the previous argument, by replacing all X_i with their images inside the finite dimensional quadratic space $(X_0+X_1+X_2+X_3)/(X_0 \cap X_1 \cap X_2 \cap X_3)$, we reduce to the case where the ambient space is finite dimensional. The result now follows from [KMR13, Corollary 2.5] which is a general result concerning the dimension of the

intersection of maximal isotropic subspaces of a finite dimensional quadratic space. The one difference from the case there is that now the quadratic form $q_{\mathcal{L}}$ (in general) takes values in $\mathbb{Z}/4\mathbb{Z}$ rather than just in $\mathbb{F}_2$ as they assume. However, one readily verifies that this assumption is not used in the proof of the cited result. □

2.3 The proof of Theorem 1.3.2

We are now able to complete the proof of our generalisation of Kramer's theorem.

Proof of Theorem 1.3.2. We let K be a global field, L/K a separable quadratic extension and A/K a principally polarised abelian variety with principal polarisation μ. Write $\hat{A}$ for the dual abelian variety, $\mathcal{A}$ for the (global) Neron model of A and $\hat{\mathcal{A}}$ for that of $\hat{A}$. We now combine the results of the previous section with those of [Čes14a, Sections 6] to prove Theorem 1.3.2. We take $A = B$ in the notation/setup of Section 6 of loc. cit. and let U be the open subscheme of (Spec of) the ring of integers of K consisting of the primes of K where both A has good reduction, and the extension L/K is unramified. We also take $\mathcal{G} = \mathcal{A}[2]_U$ and $\mathcal{H} = \hat{\mathcal{A}}[2]_U$. As discussed in Proposition 6.1 of op. cit., at any $v \in U$, the local condition going into the definition of the 2-Selmer group $\mathrm{Sel}_2(A)$ of A over K is $\mathrm{H}^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[2])$. In other words, the group $\mathrm{H}^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[2])$ inside $\mathrm{H}^1_{\mathrm{fppf}}(K_v, A[2])$ coincides with the image of the local Kummer homomorphism at all $v \in U$. Moreover, as the local extension L_v/K_v is unramified at places of U, so $\mathcal{A}^L$ has good reduction at each $v \in U$. As the formation of Neron models commutes with unramified base change, there is an isomorphism $\mathcal{A}[2] \cong \mathcal{A}^L[2]$ (where $\mathcal{A}^L$ is the Neron model of A^L) over $\mathcal{O}_v$ extending the usual one on the generic fibre. It follows that under the usual identification of $\mathrm{H}^1_{\mathrm{fppf}}(K_v, A[2])$ with $\mathrm{H}^1_{\mathrm{fppf}}(K_v, A^L[2])$, the subgroups $\mathrm{H}^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[2])$ and $\mathrm{H}^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}^L[2])$ become identified at places $v \in U$. Consequently, the Selmer group $\mathrm{Sel}_2(A^L)$, viewed inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$, is cut out by the same local consitions as $\mathrm{Sel}_2(A)$ at places $v \in U$. In the notation of Section 5.4 of op. cit., we define the Selmer groups $\mathrm{Sel}^1(\mathcal{G})$ and $\mathrm{Sel}^2(\mathcal{G})$ by taking the respective local conditions at $v \notin U$ to be the images of the kummer maps δ and δ^L of the previous section respectively. Then (again in the notation of [Čes14a, Sections 5]), we have $\mathrm{Sel}^1(\mathcal{G}) = \mathrm{Sel}_2(A)$ and $\mathrm{Sel}^2(\mathcal{G}) = \mathrm{Sel}_2(A^L)$. The results of Section 6 of op. cit. applied to A and A^L (the polarisation μ plays the role of their $\tilde{\theta}$), as well as Proposition 2.2.6 and Corollary 2.2.7 to show that the identification of the local cohomology groups $\mathrm{H}^1_{\mathrm{fppf}}(K_v, A[2])$ and $\mathrm{H}^1_{\mathrm{fppf}}(K_v, A^L[2])$ identifies the relevant pairings and quadratic forms, implies that the groups $\mathrm{Sel}^1(\mathcal{G})$ and $\mathrm{Sel}^2(\mathcal{G})$ satisfy the conditions of

[Čes14a, Theorem 5.9]. Applying the theorem, we get

$$\frac{\#\mathrm{Sel}_2(A)}{\#\mathrm{Sel}_2(A^L)} \equiv \prod_{v \notin U} \# \left(\frac{\delta\left(A(K)/2A(K)\right)}{\delta\left(A(K)/2A(K)\right) \cap \delta^L\left(A^L(K)/2A^L(K)\right)} \right) \mod \mathbb{Q}^{\times 2}.$$

Applying Lemma 2.1.2 to reinterpret the right side, and noting that the discussion above also shows that the cokernel of the local norm map is trivial at places $v \in U$, we obtain

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A) + \dim_{\mathbb{F}_2}\mathrm{Sel}_2(A^L) \equiv \sum_{v \in M_K} A(K_v)/N_{L_w/K_v}A(L_w) \pmod 2$$

where here w denotes any place of L extending a place v of K, and we note that Lemma 2.1.2 also remains valid (with the obvious interpretation) when the local extension is trival.

Finally, since

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(A) = \mathrm{ord}_2\ \mathrm{rk}_2(A/K) + \dim_{\mathbb{F}_2}A[2](K) + \dim_{\mathbb{F}_2}Ш_0(A/K)[2],$$

we have the analagous equality for A^L (noting that $\dim_{\mathbb{F}_2}A[2](K) = \dim_{\mathbb{F}_2}A^L[2](K)$), and we have $\mathrm{rk}_2(A/L) = \mathrm{rk}_2(A/K) + \mathrm{rk}_2(A^L/K)$, we obtain the result. □

Corollary 1.3.3, which gives a purely local decomposition of $\mathrm{rk}_2(J/L)$ when J is the Jacobian of a hyperelliptic curve, follows immediately form Theorem 1.3.2 and the discussion preceding its statement.

Chapter 3

Preliminary results

In this chapter we make some preliminary observations and computations involving the terms in Conjecture 1, primarily when the residue characteristic of the local field in question is odd. These basic results will facilitate the proof of various cases of Conjecture 1 in forthcoming sections.

3.1 Compatibility results

In this section we prove several compatibility results regarding the terms of Conjecture 1. This provides some evidence in favour of the conjecture, and will also be used to make some reductions as part of the proof of Theorem 1.2.1.

3.1.1 Odd degree Galois extensions

Consider a separable quadratic extension L/K of local fields, and let F be an odd degree Galois extension of K. First, we show that Conjecture 1 for L/K is equivalent to the corresponding statement for LF/F.

Lemma 3.1.1. *Every individual term in Conjecture 1 is unchanged under odd degree Galois extension of the base field. In particular, if L/K is a quadratic extension of local fields and F/K is an odd degree Galois extension, then Conjecture 1 holds for L/K if and only if it holds for LF/F.*

Proof. That the Artin symbol and the terms involving the deficiency of C and its twist are individually invariant under odd degree extensions (not necessarily even Galois) is clear. The statement for each of the root numbers is also standard. See, for example,

[DD09a, Lemma A.1] or [KT82, Proposition 3.4]. For the cokernel of the local norm map, the statement for elliptic curves is [KT82, Proposition 3.5]. The argument for general abelian varieties is identical. □

3.1.2 Quadratic twist

We now give two compatibility results concerning the behaviour of Conjecture 1 under quadratic twisting.

Lemma 3.1.2 (Quadratic twist I)**.** *Let L/K be a separable quadratic extension of local fields and C/K a hyperelliptic curve with Jacobian J. Then Conjecture 1 holds for J/K (and the extension L/K) if and only if it holds for J^L/K (and the same extension).*

Proof. Since the root numbers and terms involving deficiency appear symmetrically between J and J^L in Conjecture 1, it suffices to show that

$$(\Delta_C, L/K) = (\Delta_C^L, L/K)$$

and

$$\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L) \equiv \dim_{\mathbb{F}_2} J^L(K)/N_{L/K}J(L) \pmod 2.$$

The second statement is Corollary 2.2.8 (and in fact the dimensions are equal as opposed to just congruent modulo 2). For the first, it suffices to show that Δ_C and Δ_{C^L} lie in the same class in $K^\times/K^{\times 2}$. To see this we will fix specific models for C and C^L. If the characteristic of K is not 2, then we can find a Weierstrass equation for C of the form $y^2 = f(x)$ where $f(x)$ is a separable polynomial in $K[x]$ of degree $2g+1$ or $2g+2$ where g is the genus of C. Then the discriminant of this Weierstrass equation (as detailed in the introduction) is, up to squares, the same as the discriminant of $f(x)$. Moreover, the equation $y^2 = df(x)$ is a Weierstrass equation for the twist C^L where $d \in K^\times$ is such that $L = K(\sqrt{d})$. Since the discriminant of $df(x)$ is equal to $d^{2(\deg(f)-1)}$ times the discriminant of $f(x)$, we have the claim. In the case where the characteristic of K is 2, we can find a Weierstrass equation for C of the form

$$y^2 + Q(x)y = P(x)$$

where

$$2g+1 \leq \max\{2\deg Q(x), \deg P(x)\} \leq 2g+2,$$

as detailed in [Liu96, Section 2]. The hyperelliptic involution is then given by sending x to x and y to $y + Q(x)$. Write the separable quadratic extension L/K as $L = K(\theta)$ where θ is a solution to the Artin-Schrier equation $\theta^2 - \theta + \gamma = 0$. Consider the hyperelliptic curve defined by the equation

$$C' : y^2 + Q(x)y = P(x) + \gamma Q(x)^2.$$

There is an isomorphism onto C, defined over L, given by sending x to x and y to $y+\theta Q(x)$. The corresponding cocycle sends the non-trivial element of $\mathrm{Gal}(L/K)$ to the hyperelliptic involution inside the automorphism group $\mathrm{Aut}_L(C)$ of C over L. Hence C' is (K-isomorphic to) the quadratic twist of C by L. On the other hand, applying the formula given in [Liu96, Section 2] to the L-isomorphism above we see that the discriminants of the Weierstrass equations for C and C' above are exactly equal as elements of $K^\times$, so again we have the claim. □

The second compatibility result involving quadratic twists is more subtle. That such a compatibility result should exist for elliptic curves is discussed in the original paper [KT82] of Kramer and Tunnell (remark following Proposition 3.3) and is proved (again for elliptic curves) by Klagsbrun, Mazur and Rubin [KMR13, Lemma 5.6].

Lemma 3.1.3 (Quadratic twist II)**.** *Let K be a local field, C/K a hyperelliptic curve and J/K its Jacobian. Let L_1/K and L_2/K be distinct, separable quadratic extensions. Let L_3/K be the third (necessarily separable) quadratic subextension of L_1L_2. Then Conjecture 1 for J/K and the extensions L_1/K and L_2/K implies Conjecture 1 for J^{L_1}/K and the extension L_3/K.*

Proof. Conjecture 1 for J/K and the extensions L_1/K and L_2/K is the assertion that

$$w(J/K)w(J^{L_1}/K) = ((-1)^g\Delta_C, L_1/K)i_d(C)i_d(C^{L_1})(-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L_1/K}J(L_1)} \qquad (3.1.4)$$

and

$$w(J/K)w(J^{L_2}/K) = ((-1)^g\Delta_C, L_2/K)i_d(C)i_d(C^{L_2})(-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L_2/K}J(L_2)}. \qquad (3.1.5)$$

(Here we use [?KES141, Proposition 3.11] (or rather, its immediate generalisation to higher dimensions) which gives $w(J/L) = w(J/K)w(J^L/K)((-1)^g, L/K)$ for any separable quadratic extension L/K.) Multiplying together Equations (3.1.4) and (3.1.5), noting that $J^{L_2} =$

$(J^{L_1})^{L_3}$, that (as above) the class of Δ_C in $K^\times/K^{\times 2}$ does not change under quadratic twist, and applying the congruence Corollary 2.2.9, we obtain the formula of Conjecture 1 for J^{L_1} and the extension L_3/K. □

Remark 3.1.6. *For a local field K and hyperelliptic curve C/K, by Lemma 3.1.2 and Lemma 3.1.3, if we seek to prove Conjecture 1 for C/K and all quadratic extensions of K, then we may first make an arbitrary quadratic twist and prove the corresponding result for the new curve.*

3.2 Two torsion in the Jacobian of a hyperelliptic curve over a field of characteristic $\neq 2$

Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus g over a field K of characteristic different from 2 and let J/K be its Jacobian. Let $\mathcal{W} = \{\alpha_1, ..., \alpha_{2g+2}\}$ be the $G_K = \mathrm{Gal}(\bar{K}/K)$-set of roots of f in $\bar{K}$ (if $\deg(f) = 2g+1$, replace α_{2g+2} with the K-rational point at infinity on C). Write $\mathbb{F}_2[\mathcal{W}]$ for the $\mathbb{F}_2$-vector space with basis $\{w \in \mathcal{W}\}$. This carries a natural action of G_K from the action on $\mathcal{W}$. Then as G_K-modules we have

$$J[2] \cong \ker\left(\mathbb{F}_2[\mathcal{W}] \xrightarrow{\Sigma} \mathbb{F}_2\right)/\mathbb{F}_2 \cdot \Delta$$

where $\Sigma : \mathbb{F}_2[\mathcal{W}] \to \mathbb{F}_2$ is the sum map and $\Delta = \sum_{w \in \mathcal{W}} w$ (see [PS97, Section 6]). In particular, one sees that as $g \geq 2$, $K(J[2])/K$ is the splitting field of f.

We now compute the $\mathbb{F}_2$-dimension of the rational 2-torsion $J(K)[2]$. The case where $K(J[2])/K$ is cyclic is treated already in [Cor01, Theorem 1.4] (but note the erratum [Cor05]) whilst the case where f has an odd degree factor over K is [PS97, Lemma 12.9]. We will require a slightly more general statement however.

Lemma 3.2.1. *Let n be the number of irreducible factors of f over K. If $\deg(f)$ is odd, interpret the rational point at infinity on C as an odd degree factor of f over K so that it contributes to n. Then if f has an odd degree factor over K,*

$$\dim_{\mathbb{F}_2} J(K)[2] = n - 2.$$

On the other hand, if each irreducible factor of f over K has even degree, let F/K be the splitting field of f and let m be the number of quadratic subextensions of F/K over which

f factors into two conjugate polynomials. Then

$$\dim_{\mathbb{F}_2} J(K)[2] = \begin{cases} n-1 & g \text{ even} \\ n+\log_2(m+1)-1 & g \text{ odd.} \end{cases}$$

Proof. Denote by G the Galois group of F/K and let M be the G-module

$$M = \ker\left(\mathbb{F}_2[\mathcal{W}] \xrightarrow{\Sigma} \mathbb{F}_2\right).$$

Then we have an exact sequence

$$0 \longrightarrow \mathbb{F}_2 \cdot \Delta \longrightarrow M^G \longrightarrow J[2]^G \longrightarrow \ker\left(\mathrm{H}^1(G, \mathbb{F}_2 \cdot \Delta) \to \mathrm{H}^1(G, M)\right) \longrightarrow 0. \qquad (3.2.2)$$

Now

$$\dim_{\mathbb{F}_2} M^G = \dim_{\mathbb{F}_2} \ker\left(\mathbb{F}_2[\mathcal{W}]^G \xrightarrow{\Sigma} \mathbb{F}_2\right) = \begin{cases} n-1, & \text{if } f \text{ has an odd degree factor over } K, \\ n, & \text{else,} \end{cases}$$

and so we must show that $\dim_{\mathbb{F}_2} \ker\left(\mathrm{H}^1(G, \mathbb{F}_2 \cdot \Delta) \to \mathrm{H}^1(G, M)\right)$ is equal to 0 or $\log_2(m+1)$ according to whether g is even or odd respectively.

Now $\mathrm{H}^1(G, \mathbb{F}_2 \cdot \Delta) = \mathrm{Hom}(G, \mathbb{F}_2 \cdot \Delta)$ and the non-trivial homomorphisms from G into $\mathbb{F}_2 \cdot \Delta$ correspond to the quadratic subextensions of F/K. Now let ϕ be such a homomorphism, corresponding to a quadratic extension E/K. Then ϕ maps to 0 in $\mathrm{H}^1(G, M)$ if and only if there is $x \in M$ with $\sigma(x) + x = \phi(\sigma)\Delta$ for each $\sigma \in G$. Now the $x \in \mathbb{F}_2[\mathcal{W}]$ satisfying this equation correspond to factors f_1 of f over E for which $f = f_1\sigma(f_1)$ and $f_1 \neq \sigma(f_1)$. Finally, note that any such x is in the sum-zero part of $\mathbb{F}_2[\mathcal{W}]$ if and only if g is odd (since $|\mathcal{W}| = 2g+2$). □

Now let Δ_f be the discriminant of f. It is a square in K if and only if the Galois group of $f(x)$ is a subgroup of the alternating group A_n where $n = \deg f$. As a corollary of Lemma 3.2.1, we observe that if $K(J[2])/K$ is cyclic then whether or not the discriminant of f is a square in K may be detected from the rational 2-torsion in J as follows.

Corollary 3.2.3. *Suppose that $K(J[2])/K$ is cyclic. Then Δ_f is a square in K if and only if one of the following holds*

(i) $(-1)^{\dim J(K)[2]} = 1$ and either g is odd, or f has an odd degree factor over K;

(ii) $(-1)^{\dim J(K)[2]} = -1$, *g is even, and all factors of f over K have even degree.*

Proof. Let σ be a generator of $\mathrm{Gal}\,(K(J[2])/K)$. Then Δ_f is a square in K if and only if $\epsilon(\sigma) = 1$, where $\epsilon(\sigma)$ is the sign of σ as a permutation on the roots of f. Suppose σ has cycle type $(d_1, ..., d_s)$, so that the d_i are also the degrees of the irreducible factors of f over K (unlike in the previous lemma, here when the degree of f is odd we do not consider the point at infinity as a factor). Then we have $\epsilon(\sigma) = (-1)^{\sum_{i=1}^{s}(d_i-1)} = (-1)^{\deg(f)-s}$. Note that $J[2]^\sigma = J(K)[2]$. First suppose that f has odd degree, so that, in particular, f has an odd degree factor over K. Then Lemma 3.2.1 (remembering the convention about the point at infinity) gives

$$\dim_{\mathbb{F}_2} J(K)[2] = s + 1 - 2 = s - 1 \equiv \deg(f) - s \pmod 2$$

and we are done. Now suppose that $\deg(f)$ is even. Since $K(J[2])/K$ is assumed to be cyclic, it contains at most one quadratic extension. Moreover, f factors into 2 conjugate polynomials over this extension (if it exists) if and only if each d_i is even (and conversely, if each d_i is even then there is such a quadratic extension). Now again, the result follows from Lemma 3.2.1. □

3.3 Deficiency

Let K be a local field and C/K a hyperelliptic curve. Recall [PS99, Section 8] that C is said to be *deficient* over K if $\mathrm{Pic}^{g-1}(C) = \emptyset$ (here $\mathrm{Pic}(C)$ refers to the Picard group of C, and not the K rational points of the Picard functor; the difference betweem these two objects is closely related to the notion of deficiency). In this section we give two criteria for determining whether or not the hyperelliptic curve C is deficient over K. The first covers the case where the two-torsion of its Jacobian is defined over a cyclic extension of K. This works for all local fields of odd characteristic. The second criterion concerns non-archimedean local fields of arbitrary characteristic and characterises deficiency in terms of the components of the special fibre of the minimal proper regular model of C.

3.3.1 Deficiency when the defining polynomial admits a certain factorisation

In this subsection, we suppose that K does not have characteristic 2.

We first remark that as C has K-rational divisors of degree 2 (arising as the pull back of points on $\mathbb{P}^1_K$) if g is odd then C is never deficient.

We have short exact sequences of $\mathrm{G}_K = \mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow \bar{K}(C)^\times/\bar{K}^\times \xrightarrow{\text{div}} \mathrm{Div}(C_{\bar{K}}) \longrightarrow \mathrm{Pic}(C_{\bar{K}}) \longrightarrow 0$$

and

$$0 \longrightarrow \bar{K}^\times \longrightarrow \bar{K}(C)^\times \longrightarrow \bar{K}(C)^\times/\bar{K}^\times \longrightarrow 0.$$

Combining the associated long exact sequences for Galois cohomology we obtain an exact sequence

$$0 \longrightarrow \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}(C_{\bar{K}})^{\mathrm{G}_K} \longrightarrow \mathrm{Br}(K).$$

Denote by $\phi : \mathrm{Pic}(C_{\bar{K}})^{\mathrm{G}_K} \to \mathbb{Q}/\mathbb{Z}$ the composition of the map above and the local invariant map $\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$. In (the proof of) [PS99, Theorem 11], Poonen and Stoll show that if $\mathcal{L} \in \mathrm{Pic}(C_{\bar{K}})^{\mathrm{G}_K}$ is a rational divisor class of degree n on C then $\mathrm{Pic}^n(C)$ is empty (resp. non-empty) according to $n\phi(\mathcal{L}) = \frac{1}{2}$ (resp. 0) in $\mathbb{Q}/\mathbb{Z}$.

We will apply this to the case where the polynomial defining C either has an odd degree factor, or factors as a product of two odd degree polynomials which are conjugate over a quadratic extension of K (see [BGW13, Section 1] where this condition also arises).

Proposition 3.3.1. *Let K be a local field of characteristic different from 2 and C be the hyperelliptic curve $y^2 = df(x)$ of even genus g, where $f \in K[x]$ is monic. Suppose further that f has either an odd degree factor over K, or factors as two conjugate, odd degree polynomials over a quadratic extension of K. Let L be the étale algebra $L = K[x]/(f)$. Then C is deficient over K if and only if $d \in N_{L/K}(L^\times)K^{\times 2}$.*

Proof. First, we deal with some trivial cases. Since C has K-rational divisors of degree 2, having a K-rational divisor of degree $g-1$ is equivalent to having a K-rational divisor of any odd degree, which in turn is equivalent to having a rational point over some odd degree extension of K. If f has an odd degree factor over K then C has a rational Weierstrass point over an odd degree extension and is not deficient. Moreover, $N_{L/K}(L^\times)K^{\times 2} = K^\times$ in this case. Thus we assume f factors into two conjugate, odd degree polynomials over a quadratic extension F/K. Then over F, we may write $f = f_1 f_2$ where each f_i has degree $g+1$ and f_1 and f_2 are conjugate over F. Denote the roots of f_1 by $\alpha_1, \alpha_3, ..., \alpha_{2g+1}$ and the roots of f_2 by $\alpha_2, \alpha_4, ..., \alpha_{2g+2}$. For each i, let $P_i = (\alpha_i, 0) \in C(\bar{K})$ and let D be the

degree $g+1$ divisor

$$D = \sum_{i \text{ odd}} (P_i).$$

If $\chi : \mathrm{G}_K \to \{\pm 1\}$ is the quadratic character associated to the extension F/K then for all $\tau \in \mathrm{G}_K$ we have $\tau(D) = D$ or $\tau(D) = \sum_{i \text{ even}}(P_i)$ according to $\chi(\tau) = 1$ or -1. Since

$$\mathrm{div}\left(\frac{y}{\prod_{i \text{ odd}}(x-\alpha_i)}\right) = \sum_{i \text{ even}} (P_i) - \sum_{i \text{ odd}} (P_i)$$

it follows that D represents a K-rational divisor class. Since $\mathrm{Pic}^{g-1}(C) = \emptyset$ if and only if $\mathrm{Pic}^{g+1}(C) = \emptyset$, it follows that C is deficient if and only if $(g+1)\phi(D) = \frac{1}{2}$ in $\mathbb{Q}/\mathbb{Z}$ (here we write D for the divisor class of D also). The discussion above shows that the cocycle $f_\tau : \mathrm{G}_K \to \bar{K}(C)^\times/\bar{K}^\times$ that sends τ to 1 if $\chi(\tau) = 1$ and (the class of) $\frac{y}{\prod_{i \text{ odd}}(x-\alpha_i)}$ if $\chi(\tau) = -1$, represents the image of D under the connecting homomorphism

$$\delta : \mathrm{Pic}(C_{\bar{K}})^{\mathrm{G}_K} \to \mathrm{H}^1(K, \bar{K}(C)^\times/\bar{K}^\times).$$

Viewing f_τ instead as a cochain with values in $\bar{K}(C)^\times$ in the obvious way, the image of f_τ in $\mathrm{Br}(K)$ is represented by the 2-cocycle $a_{\tau,\rho} = {f_\tau}^\tau f_\rho f_{\tau\rho}^{-1}$. A straightforward computation gives $a_{\tau,\rho} = 1$ unless $\chi(\tau) = -1 = \chi(\rho)$ in which case it is equal to

$$\frac{y}{\prod_{i \text{ odd}}(x-\alpha_i)} \cdot \frac{y}{\prod_{i \text{ even}}(x-\alpha_i)} = d.$$

I now claim that under $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, $a_{\tau,\rho}$ is mapped to 0 if d is a norm from $F^\times$ and $1/2$ otherwise. Indeed, by Hilbert's Theorem 90, the inflation map

$$\mathrm{inf} : \mathrm{H}^2(\mathrm{Gal}(F/K), F^\times) \longrightarrow \mathrm{H}^2(K, \bar{K}^\times)$$

is an injection and since $a_{\tau,\rho}$ depends only on τ and ρ through their image under χ, $a_{\tau,\rho}$ is in the image of this map. Specifically, writing η for the non-trivial element of $\mathrm{Gal}(F/K)$, $a_{\tau,\rho}$ is the image of the cocycle $a'_{\tau,\rho}$ in $\mathrm{H}^2(\mathrm{Gal}(F/K), F^\times)$ that takes the value 1 apart from at the element (η, η) where it takes the value d. By definition, this cocycle is trivial in $\mathrm{H}^2(\mathrm{Gal}(F/K), F^\times)$ if and only if there is a function $\phi : \mathrm{Gal}(F/K) \to F^\times$ for which

$$a'_{\tau,\rho} = \phi(\tau)^\tau \phi(\rho)\phi(\tau\rho)^{-1}.$$

Taking $\tau = \rho = 1$ forces $\phi(1) = 1$. Setting $\phi(\eta) = t \in F^\times$ we see that $a'_{\tau,\rho}$ agrees with the right hand side of the above expression everywhere if and only if $d = N_{F/K}(t)$. Thus $a_{\tau,\rho}$ is trivial in $\mathrm{Br}(K)$ if and only if $d \in N_{F/K}(F^\times)$. On the other hand, it has order one or two as the whole of $\mathrm{H}^2(\mathrm{Gal}(F/K), F^\times)$ is annihilated by two. Since the local invariant map is an injection to $\mathbb{Q}/\mathbb{Z}$, we have the claim. We have therefore shown that $(g+1)\phi(D)$ is 0 if and only if $d \in N_{F/K}(F^\times)$. It remains to show that $N_{L/K}(L^\times)K^{\times 2} = N_{F/K}(F^\times)$. Indeed, factorise f into irreducibles $g_1, ..., g_r$ over K and let $L_i = K[x]/(g_i)$. The assumption on the K-factorisation of f implies that F is contained in each L_i. Thus $N_{L/K}(L^\times)K^{\times 2} \subseteq N_{F/K}(F^\times)$. Conversely, since $\deg(f) \equiv 2 \pmod 4$, there is some i for which $\deg(g_i) \equiv 2 \pmod 4$ also. Then $[L_i : F] = 2m+1$ is odd and for any $x \in F^\times$ we have $N_{L_i/K}(x) = N_{F/K}(x)N_{F/K}(x)^{2m}$. Thus $N_{F/K}(x) \in N_{L/K}(L^\times)K^{\times 2}$ and we are done. □

Corollary 3.3.2. *Let K be a local field of characteristic different from 2 and C be the hyperelliptic curve associated to the equation $y^2 = df(x)$ where $f \in K[x]$ is monic and separable of degree $2g+1$ or $2g+2$ where g is even. Suppose moreover that $K(J[2])/K$ is cyclic. Then C is deficient over K if and only if all irreducible factors of f over K have even degree, and $(d, F/K) = -1$ where F/K is the unique quadratic subextension of $K(J[2])/K$.*

Proof. As before we may assume that each irreducible factor of f over K has even degree, in which case f has degree $2g+2$. Then the assumption that $K(J[2])/K$ is cyclic ensures that there is indeed a unique quadratic subextension of $K(J[2])/K$ and that f factors into two conjugate odd degree polynomials over F. The claimed result now follows from Proposition 3.3.1. □

3.3.2 Deficiency in terms of the minimal proper regular model

We conclude the section by characterising deficiency in terms of the minimal proper regular model of C. We will make extensive use of this criterion later. Since at times we will work with curves that are not necessarily hyperelliptic, we state the result in this generality here. In this section K will be a non-archimedean local field, which may now have characteristic 2.

Lemma 3.3.3. *Let K be a non-archimedean local field with ring of integers $\mathcal{O}_K$ and residue field k. Let X/K be a smooth, proper, geometrically integral curve of genus g, $\mathcal{X}/\mathcal{O}_K$ its minimal proper regular model and $\Gamma_1, ..., \Gamma_n$ the irreducible components of the special fibre*

$\mathcal{X}_k$ of $\mathcal{X}$. For each component Γ_i, let d_i be the multiplicity of Γ_i in $\mathcal{X}_k$ and $r_i = [\bar{k} \cap k(\Gamma_i) : k]$. Then X is deficient over K if and only if $\gcd_{1 \leq i \leq n}\{r_i d_i\}$ does not divide $g - 1$.

Proof. This is [GLL13, Theorem 8.2]. See also the remark following the proof of Lemma 16 in [PS99]. In fact, the minimality assumption is unnecessary, but we will always work with the minimal proper regular model when applying the result. □

Remark 3.3.4. *We can rephrase Lemma 3.3.3 as follows. Let $\mathcal{X}_{\bar{k}}$ be the special fibre of the minimal proper regular model of X over $\mathcal{O}_K$, base-changed to $\bar{k}$ (this coincides with the special fibre of the minimal proper regular model of X over K^{nr}). If a component $\bar{\Gamma}$ of $\mathcal{X}_{\bar{k}}$ with multiplicity $\bar{d}$ lies over a component Γ of $\mathcal{X}_k$ of multiplicity d, then $\bar{d} = d$. Moreover, under the natural action of $\mathrm{Gal}(\bar{k}/k)$ on the components of $\mathcal{X}_{\bar{k}}$, we have*

$$[\bar{k} \cap k(\Gamma) : k] = |\mathrm{orb}_{\mathrm{Gal}(\bar{k}/k)}(\bar{\Gamma})|.$$

Consequently, letting $\bar{\Gamma}_1, ..., \bar{\Gamma}_m$ be the irreducible components of $\mathcal{X}_{\bar{k}}$, multiplicities $\bar{d}_i$, we see that X is deficient over K if and only if

$$\gcd_{1 \leq i \leq m}\{\bar{d}_i \cdot |\mathrm{orb}_{\mathrm{Gal}(\bar{k}/k)}(\bar{\Gamma}_i)|\}$$

does not divide $g - 1$.

Chapter 4

The first cases of Conjecture 1 and a global to local argument

4.1 First cases of Conjecture 1

In this section we prove Conjecture 1 in two cases, namely for archimedean places and for places of good reduction and odd residue characteristic. It will turn out that these are the only cases needed to prove Theorem 1.5.1 (in fact, even the archimedean places are not necessary for this).

4.1.1 Archimedean places

Here we consider archimedean local fields. Clearly the only case of interest is the extension $\mathbb{C}/\mathbb{R}$. In this case, we can answer Conjecture 1 completely.

Proposition 4.1.1. *Conjecture 1 holds for the extension $\mathbb{C}/\mathbb{R}$ and every hyperelliptic curve $C/\mathbb{R}$.*

Proof. Let $J/\mathbb{R}$ be the Jacobian of C. Since J is an abelian variety of dimension g (the genus of C) over the reals, we have an isomorphism of real Lie groups

$$J(\mathbb{R}) \cong (\mathbb{R}/\mathbb{Z})^g \times (\mathbb{Z}/2\mathbb{Z})^k \tag{4.1.2}$$

where $0 \leq k \leq g$ (see, for example, [Sil89, Proposition 1.9 and Remark 1.12]). Now $N_{\mathbb{C}/\mathbb{R}}$ is a continuous map from the connected group $J(\mathbb{C})$ to $J(\mathbb{R})$ and it follows that the image of $N_{\mathbb{C}/\mathbb{R}}$ is contained in the connected component of the identity in $J(\mathbb{R})$, denoted $J^0(\mathbb{R})$.

Under the isomorphism (4.1.2), $J^0(\mathbb{R})$ is the factor corresponding to $(\mathbb{R}/\mathbb{Z})^g$. On the other hand, we have $2J(\mathbb{R}) \subseteq N_{\mathbb{C}/\mathbb{R}}A(\mathbb{C})$ and we see again from (4.1.2) that multiplication by 2 is surjective on $J^0(\mathbb{R})$. Thus $N_{\mathbb{C}/\mathbb{R}}J(\mathbb{C}) = J^0(\mathbb{R})$. In particular, $|J(\mathbb{R})/N_{\mathbb{C}/\mathbb{R}}J(\mathbb{C})| = 2^{-g}|J(\mathbb{R})[2]|$. We have also $w(J/\mathbb{C}) = (-1)^g$ (see, for example, [Sab07, Lemma 2.1]), and so to verify Conjecture 1 we must show that

$$(-1)^{\dim_{\mathbb{F}_2} J(\mathbb{R})[2]} = (\Delta_C, -1)i_d(C)i_d(C_{-1})$$

where C_{-1} dentoes the quadratic twist of C by $\mathbb{C}/\mathbb{R}$.

Now certainly $K(J[2])/K$ is cyclic and, moreover, $(\Delta_C, -1) = 1$ if and only if Δ_C is a square in $\mathbb{R}$. Consequently, Corollary 3.2.3 gives $(-1)^{\dim_{\mathbb{F}_2} J(\mathbb{R})[2]} = (\Delta_C, -1)$ except when g is even and all irreducible factors of f over $\mathbb{R}$ have even degree, in which case the two expressions differ by a sign. Since by Corollary 3.3.2 this is exactly the case where $i_d(C)i_d(C_{-1}) = -1$, we have verified Conjecture 1. □

4.1.2 Good reduction in odd residue characteristic

Suppose now that K is a non-archimedean local field with odd residue characteristic and that C/K is a hyperelliptic curve over K whose Jacobian J has good reduction over K. Let L/K be a quadratic extension. The following lemma describes the cokernel of the norm map from $J(L)$ to $J(K)$.

Lemma 4.1.3. *Let K be a non-archimedean local field, L/K a quadratic extension, and A a principally polarised abelian variety with good reduction over K. If L/K is unramified then $A(K)/N_{L/K}A(L)$ is trivial whilst if L/K is ramified we have $N_{L/K}A(L) = 2J(K)$. In particular,*

$$\left|A(K)/N_{L/K}A(L)\right| = \begin{cases} 1 & L/K \text{ unramified} \\ |A(K)[2]| & L/K \text{ ramified.} \end{cases}$$

Proof. The case L/K is unramified is a result of Mazur [Maz72, Corollary 4.4]. In fact, this case does not require that K has odd residue characteristic. Alternatively, one can use the discussion in the proof of Theorem 1.3.2 to note that the local images of the Kummer maps inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[2])$ corresponding to A and A^L are both equal to $\mathrm{H}^1(\mathcal{O}_K, \mathcal{A}[2])$ (here $\mathcal{A}$ is the Néron model of A) and then apply Lemma 2.1.1 to conclude. The case L/K ramified is essentially Corollary 4.6 in op. cit. . The argument is as follows. Again, let $\mathcal{A}$ denote the Néron model of A over K. Since A has good reduction, the Néron model of A over L

is given by $\mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_L$. If $A(K)_1$ and $A(L)_1$ denote the kernels of reduction modulo $\mathfrak{m}_K$ and $\mathfrak{m}_L$ (the maximal ideals in the rings of integers of K and L respectively) respectively. We have an exact sequence of $G = \mathrm{Gal}(L/K)$-modules

$$0 \to A(L)_1 \to A(L) \to \tilde{A}(k) \to 0 \tag{4.1.4}$$

where $\tilde{A} := \mathcal{A} \times_{\mathcal{O}_K} k$ and has trivial G-action, and $A(L)_1^G = A(K)_1$. Since $\mathrm{char}(k) \neq 2$, multiplication by 2 is an isomorphism on $A(K)_1$. It follows that $A(K)_1/N_{L/K}A(L)_1$ is trivial and that reduction gives an isomorphism

$$\hat{\mathrm{H}}^0(G, A(L)) \xrightarrow{\sim} \hat{\mathrm{H}}^0(G, \tilde{A}(k)).$$

On the other hand, considering (4.1.4) with L replaced by K (as a sequence of trivial G-modules) and noting that the actions on $\tilde{A}(k)$ in each sequence coincide, we similarly obtain an isomorphism

$$A(K)/2A(K) \xrightarrow{\sim} \hat{H}^0(G, \tilde{A}(k))$$

again induced by reduction. The result now follows easily. □

Corollary 4.1.5. *Let K be a non-archimedean local field with odd residue characteristic and L/K a quadratic extension. Let C/K be a hyperelliptic curve and suppose that the Jacobian J of C has good reduction over K. Then Conjecture 1 holds for C and the extension L/K.*

Proof. The assumptions on the reduction give $w(J/L) = 1$ so we are reduced to showing that

$$(-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L)} = (\Delta_C, L/K) i_d(C) i_d(C^L).$$

If L/K is unramified then Lemma 4.1.3 gives $(-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L)} = 1$. Moreover, the assumptions on the reduction mean $K(J[2])/K$ is unramified and so adjoining a square root of Δ_C to K yields an unramified extension. In particular, $(\Delta_C, L/K) = 1$ or, equivalently, Δ_C has even valuation. Finally, Corollary 3.3.2 gives $i_d(C) i_d(C^L) = 1$ also.

Now suppose L/K is ramified. Lemma 4.1.3 gives $(-1)^{\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L)} = (-1)^{\dim_{\mathbb{F}_2} J(K)[2]}$. Moreover, as $v_K(\Delta_C)$ is even, Δ_C is a unit modulo squares in K and hence $(\Delta_C, L/K) = 1$ if and only if Δ_C is a square in K. Indeed, as L/K is ramified quadratic, $\mathcal{O}_K^\times / N_{L/K}(\mathcal{O}_L^\times)$ has order two by Local Class Field Theory, whilst $\mathcal{O}_K^\times / \mathcal{O}_K^{\times 2}$ also has order two since the residue characteristic of K is odd. As $\mathcal{O}_K^{\times 2} \subseteq N_{L/K}(\mathcal{O}_L^\times)$, it follows that $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^{\times 2}$. Corol-

lary 3.2.3 and Corollary 3.3.2 then give the desired result, noting that if u is a non-square unit then $(u, L/K) = -1$. □

4.2 Deducing cases of conjecture 1 from global results

We have now proved enough cases of Conjecture 1 to prove Theorem 1.5.1.

Proof of Theorem 1.5.1. Write $F = K_{v_0}(\sqrt{\alpha})$ with $\alpha \in K$. Let S be a finite set of places of K containing all places where J has bad reduction, all places dividing 2 and all archimedean places. Set $T = S - \{v_0\}$.

Now let L/K be a quadratic extension such that each place $v \in T$ splits in L/K and such that there is exactly one place $w_0|v_0$ and which satisfies $L_{w_0} = F$. Explicitly, we may take $L = K(\sqrt{\beta})$ where $\beta \in K$ is chosen, by weak approximation, to be sufficiently close to α v_0-adically, and sufficiently close to 1 v-adically for all $v \in T$. Then the products

$$\prod_{v \in M_K, v \text{ non-split}} w(J/L_w)$$

and

$$\prod_{v \in M_K, v \text{ non-split}} (\Delta_C, L_w/K_v) i_d(C_v) i_d(C_v^{L_w}) (-1)^{\dim_{\mathbb{F}_2} J(K_v)/N_{L_w/K_v} J(L_w)}$$

(where w always denotes a place of L lying over v) multiply to $w(J/L)$ and $\mathrm{rk}_2(J/L)$ respectively and hence agree under the assumption that the 2-parity conjecture holds over L. On the other hand, by Corollary 4.1.5 the contributions to each product from a single place v agree save possible at $v = v_0$ (then key point is that if a place v splits in L/K then there is nothing to show). Thus the contributions from $v = v_0$ must agree too. □

Chapter 5

Corank 1 integral symmetric matrices

In this Chapter we prove some results about a certain finite group Φ which we attach to a corank one, integral symmetric matrix. This group naturally arises as the component group of the Neron model of the Jacobian of a curve (as explained in Example 5.1.2). In the next chapter we will apply these results to study Conjecture 1 in the case that the quadratic extension is unramified. The main tool for this will be Theorem 5.2.2. Even though our application is to hyperelliptic curves, the theorem holds in the more general context of integral, corank one, symmetric matrices, so we prove the result in this context. Studying this more general setup also allows us to prove some auxilliary results concerning the Jacobian of a finite graph (see Example 5.1.3 for the relevance to graphs).

5.1 General setup

Let $M = (m_{i,j})_{i,j \in I}$ be an integral symmetric $n \times n$ matrix of rank $n-1$. Let $\mathbb{Z}^I$ be the free $\mathbb{Z}$-module with basis $\{\Gamma_i \mid i \in I\}$ and $\alpha : \mathbb{Z}^I \to \mathbb{Z}^I$ be the linear map with matrix M (with respect to this standard basis). Let $0 \neq F := \sum_i d_i \Gamma_i$ be such that $d_i \in \mathbb{Z}$ and $F \in \ker(\alpha)$. Then as M has rank $n-1$, we see that $\ker(\alpha)$ is the free $\mathbb{Z}$-module generated by $\frac{1}{d}F$ where $d := \gcd_{i \in I}\{d_i\}$. Define $\beta : \mathbb{Z}^I \to \mathbb{Z}$ by $\beta(\Gamma_i) = d_i$. Note that $\mathrm{im}(\beta) = d\mathbb{Z}$ and that, since M is symmetric, we have $\mathrm{im}(\alpha) \subseteq \ker(\beta)$. Since β is not the zero map and M has rank $n-1$, it follows that the group

$$\Phi := \ker(\beta)/\mathrm{im}(\alpha)$$

is finite. Note that this depends only on the matrix M, not on the choice of $F \in \ker(\alpha)$.

We define a symmetric pairing $\langle \cdot, \cdot \rangle$ on $\mathbb{Z}^I$ by setting $\langle \Gamma_i, \Gamma_j \rangle = m_{i,j}$. For $D \in \mathbb{Z}^I$, we denote $\langle D, D \rangle$ by D^2.

Let p be a function associating, to each Γ_i, an integer $p(\Gamma_i)$. We define the *genus* of the triple (M, F, p) to be

$$g := 1 + \sum_{i \in I} d_i (p(\Gamma_i) - 1 - \frac{1}{2} m_{i,i})$$

which we shall soon see is an integer.

Lemma 5.1.1. *There is a unique extension $p : \mathbb{Z}^I \to \mathbb{Z}$ of p such that the function $\phi : \mathbb{Z}^I \to \mathbb{Z}$ given by*

$$\phi(D) = 2p(D) - 2 - D^2$$

is a homomorphism. Moreover, we have $p(F) = g$, whence g is an integer.

Proof. Let $D = \sum_i n_i \Gamma_i$. For ϕ to be a homomorphism, we must have

$$2p(D) - 2 - D^2 = \phi(D) = \sum_i n_i \phi(\Gamma_i) = \sum_i n_i (2p(\Gamma_i) - 2 - m_{i,i}).$$

That is, we must set

$$p(D) := 1 + \frac{1}{2} D^2 + \sum_i n_i (p(\Gamma_i) - 1 - \frac{1}{2} m_{i,i}).$$

This shows uniqueness, and we note that this function does indeed extend p. Defining p by this formula, we see immediately that the associated function ϕ is a homomorphism.

It remains to show that $p(D) \in \mathbb{Z}$ for all $D \in \mathbb{Z}^I$. That is, for any $D = \sum_i n_i \Gamma_i \in \mathbb{Z}^I$, we must show that

$$D^2 - \sum_i n_i m_{i,i} \in 2\mathbb{Z}.$$

This is clear, since (as M is symmetric) we have

$$D^2 - \sum_i n_i m_{i,i} = 2 \sum_{i<j} n_i n_j m_{i,j} + \sum_i n_i (n_i - 1) m_{i,i}.$$

It is immediate that $g = p(F)$. □

We now describe two instances where this setup naturally occurs.

Example 5.1.2. *Let K be a discrete valuation field with ring of integers $\mathcal{O}_K$ and algebraically closed residue field k. Let $\mathcal{C}$ be a proper, regular, flat curve over $\mathcal{O}_K$ with*

geometrically irreducible generic fibre C. Let $\{\Gamma_i,\ i \in I\}$ be the set of irreducible components of the special fibre $\mathcal{C}_k$ of $\mathcal{C}$, let d_i be the multiplicity of Γ_i in the special fibre and $F := \sum_i d_i\Gamma_i$. Define the symmetric, rank $n-1$ ($n=\#I$) matrix M by setting $m_{i,j}$ to be the intersection number of Γ_i and Γ_j (see, for example, [BLR90, Lemma 9.6.10] *for the asserition about the rank and kernel of the matrix M). Finally, let $p(\Gamma_i)$ be the arithmetic genus of the component Γ_i. Then in this context, the group Φ is the component group of the Neron model of the Jacobian of C* [BL99, Theorem 1.1]*, and the adjunction formula (combine* [Liu02, Proposition 9.1.35 and Theorem 9.1.37]*) shows that g is the genus of C. In fact, it is the adjunction formula which motivates Lemma 5.1.1 and here the function ϕ of Lemma 5.1.1 is just the function which sends a divisor D to its intersection number with the canonical class $K_{\mathcal{C}/\mathcal{O}_K}$.*

Example 5.1.3. *Let G be a finite connected graph with no loops but possibly multiple edges. We denote the vertices of G by Γ_i, for $i \in I$. Further, write $E(G)$ for the set of edges of G, set $V := \#I$ and $E = \#E(G)$. Define the symmetric, integral matrix $M = (m_{i,j})$ by*

$$m_{i,j} = \begin{cases} \text{the number of edges joining } \Gamma_i \text{ and } \Gamma_j, & \text{if } i \neq j, \\ -\deg(\Gamma_i), & \text{if } i = j. \end{cases}$$

Thus M is the (negative of the) Laplacian matrix of G and has rank $V-1$. Its kernel is generated by $F := \sum_i \Gamma_i$. We set $d_i := 1$ for all i. Then M and F together give the corresponding maps α and β as above. Finally, we set $p(\Gamma_i) = 0$ for all i. In this situation,

$$g = 1 + \sum_{i \in I} \left(-1 + \frac{1}{2}\deg(\Gamma_i) \right) = E - V + 1$$

is the (first) Betti-number of the graph G. The group Φ appears in the literature as the Jacobian or Sandpile group of G. See, for example, the papers [BN07] *and* [BN09] *of Baker and Norine, and the references therein, for a discussion of this group and some of its properties.*

5.2 The action on Φ by permutations of I

Now let $\mathfrak{G}$ be the group of all permutations σ of I commuting with α and β and such that $p(\sigma\Gamma_i) = p(\Gamma_i)$ for each $i \in I$. For each $\sigma \in \mathfrak{G}$, set $r_i(\sigma) := |\mathrm{orb}_\sigma(\Gamma_i)|$, let $d'(\sigma) :=$

$\gcd_{i\in I}\{d_i r_i(\sigma)\}$ and set

$$q(\sigma) = \begin{cases} 2, & \text{if } d'(\sigma) \nmid g-1, \\ 1, & \text{else.} \end{cases}$$

The defining conditions of $\mathfrak{G}$ ensure that each $\sigma \in \mathfrak{G}$ acts naturally on the group Φ.

The following result is essentially [BL99, Theorem 1.17], due to Bosch and Liu. There the result is proved in the context of Example 5.1.2, though the residue field is not assumed to be algebraically closed and a certain Galois group takes the role of $\mathfrak{G}$. We use Lemma 5.1.1 to replace each occurence of the adjunction formula in their proof. For convenience, we state the general result and give the complete proof. The essential points of the argument are repeated, almost verbatim, from loc. cit. .

Theorem 5.2.1. *For each $\sigma \in \mathfrak{G}$, $q(\sigma)d$ divides $d'(\sigma)$. Moreover, we have a short exact sequence*

$$0 \longrightarrow \mathrm{im}(\alpha)^\sigma \longrightarrow \ker(\beta)^\sigma \longrightarrow \Phi^\sigma \longrightarrow \frac{q(\sigma)d\mathbb{Z}}{d'(\sigma)\mathbb{Z}} \longrightarrow 0.$$

Proof. We first show that $q(\sigma)d$ divides $d'(\sigma)$. Let $O_1, ..., O_k$ be the orbits of σ on the set $\{\Gamma_i | i \in I\}$. For each $j = 1, ..., k$ let $\Gamma_{j,0}$ be a representative of the orbit O_j. Now

$$2g-2 = \phi(F) = \sum_{i\in I} d_i \phi(\Gamma_i).$$

As $\sigma \in \mathfrak{G}$, it follows that the quantities d_i and $\phi(\Gamma_i)$ depend only on the orbit of Γ_i under σ. We write d_j for the common value of the d_i on the orbit O_j and write r_j for the order of the orbit O_j. Then

$$2g-2 = \sum_{j=1}^{k} d_j r_j \phi(\Gamma_{j,0})$$

(noting that $\phi(\Gamma_{j,0})$ does not depend on the choice of representative for the orbit O_j. It follows that $d'(\sigma)$ divides $2g-2$. On the other hand, $g-1$ is divisible by d. Indeed, replacing each d_i by $\frac{d_i}{d}$, we see from Lemma 5.1.1 that $\frac{g-1}{d}$ is an integer the same way that $g-1$ itself is.

We now turn to the short exact sequence. Let H be the subgroup of $\mathfrak{G}$ generated by σ and let $m = |H|$. The short exact sequence

$$0 \longrightarrow \mathrm{im}(\alpha) \longrightarrow \ker(\beta) \longrightarrow \Phi \longrightarrow 0$$

is equivariant for the action of H and hence yields the exact sequence for cohomology

$$0 \longrightarrow \mathrm{im}(\alpha)^\sigma \longrightarrow \ker(\beta)^\sigma \longrightarrow \Phi^\sigma \longrightarrow \ker\left(\mathrm{H}^1(H, \mathrm{im}(\alpha)) \to \mathrm{H}^1(H, \ker(\beta))\right).$$

The identical argument to [BL99, Lemma 1.19] now shows that both $\mathrm{H}^1(H, \mathrm{im}(\alpha))$ and $\mathrm{H}^1(H, \ker(\beta))$ are (abstractly) isomorphic to $\frac{d\mathbb{Z}}{d'(\sigma)\mathbb{Z}}$. Moreover, the proof of [BL99, Theorem 1.17] shows that the image of the map between these two groups is generated by the class in $d\mathbb{Z}/d'(\sigma)\mathbb{Z}$ of the integer n where

$$n = -\frac{d'(\sigma)}{2} V_1^2,$$

for $V_1 := \sum_{j=1}^k \frac{r_j d_j}{d'(\sigma)} \Gamma_{j,0}$. Consequently, we have

$$n = \frac{d'(\sigma)}{2}\left(2 - 2p(V_1) + \phi(V_1)\right) \equiv \frac{d'(\sigma)}{2}\phi(V_1) \pmod{d'(\sigma)}.$$

Now one easily computes $N(V_1) = \frac{m}{d'(\sigma)} F$ where $N = 1 + \sigma + ... + \sigma^{m-1}$ and as ϕ commutes with σ (as $\sigma \in \mathfrak{G}$), we have

$$\phi(V_1) = \frac{1}{m}\phi(N(V_1)) = \frac{1}{d'(\sigma)}\phi(F) = \frac{2g-2}{d'(\sigma)}.$$

Thus $n \equiv g - 1 \pmod{d'(\sigma)}$. Since $d'(\sigma)$ divides $2g - 2$ we are done, we see that the kernel of the map between $\mathrm{H}^1(H, \mathrm{im}(\alpha))$ and $\mathrm{H}^1(H, \ker(\beta))$ is given by $q(\sigma)d\mathbb{Z}/d'(\sigma)\mathbb{Z}$ as desired. □

We now give the main result of the section.

Theorem 5.2.2. *The map*

$$D : \mathfrak{G} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

defined by

$$D(\sigma) = \frac{\#\Phi}{\#\Phi^\sigma} \cdot q(\sigma)$$

is a homomorphism.

Proof. Fix $\sigma \in \mathfrak{G}$, define $d = \gcd_{i\in I}\{d_i\}$ and $d'(\sigma) = \gcd_{i\in I}\{|\mathrm{orb}_\sigma(\Gamma_i)|d_i\}$. By Theorem 5.2.1 we have

$$\#\Phi^\sigma \cdot q(\sigma) = \left|\frac{\ker(\beta)^\sigma}{\mathrm{im}(\alpha)^\sigma}\right| \cdot \frac{d'(\sigma)}{d}.$$

To ease notation in what follows, we write Λ for the $\mathbb{Z}$-module $\mathbb{Z}^I$, along with its action of σ.

Now

$$\ker(\beta)^\sigma/\mathrm{im}(\alpha)^\sigma \cong \ker\left(\beta : \Lambda^\sigma/(\alpha(\Lambda)^\sigma) \to d'(\sigma)\mathbb{Z}\right)$$

and applying the snake lemma to the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{\Lambda^\sigma}{\alpha(\Lambda)^\sigma} & \longrightarrow & \frac{\Lambda}{\alpha(\Lambda)} & \longrightarrow & \frac{\Lambda}{\alpha(\Lambda)+\Lambda^\sigma} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} & & \downarrow{\scriptstyle \beta_3} & & \\ 0 & \longrightarrow & d'(\sigma)\mathbb{Z} & \longrightarrow & d\mathbb{Z} & \longrightarrow & d\mathbb{Z}/d'(\sigma)\mathbb{Z} & \longrightarrow & 0 \end{array}$$

(where each vertical arrow is induced by β) yields, upon noting that all vertical arrows are surjective,

$$D(\sigma) = \frac{dq(\sigma)^2}{d'(\sigma)} |\ker(\beta_3)| = q(\sigma)^2 \frac{d^2}{d'(\sigma)^2} \left| \frac{\Lambda}{\alpha(\Lambda) + \Lambda^\sigma} \right|.$$

Thus as a function $\mathfrak{G} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ we have

$$D(\sigma) = \left| \frac{\Lambda}{\alpha(\Lambda) + \Lambda^\sigma} \right|.$$

Now $\sigma - 1$ yields an isomorphism

$$\frac{\Lambda}{\alpha(\Lambda) + \Lambda^\sigma} \xrightarrow{\sim} \frac{(\sigma-1)\Lambda}{(\sigma-1)\alpha(\Lambda)} = \frac{(\sigma-1)\Lambda}{\alpha((\sigma-1)\Lambda)}$$

where for the last equality we use that σ commutes with α.

Now $(\sigma - 1)\Lambda$ is a free $\mathbb{Z}$-module of finite rank and α is a linear endomorphism of this group. By properties of Smith normal form, the order of the group

$$\frac{(\sigma-1)\Lambda}{\alpha((\sigma-1)\Lambda)}$$

is equal to the absolute value of the determinant of α as a linear map on the $\mathbb{Q}$-vector space $(\sigma - 1)V$, where $V := \Lambda \otimes \mathbb{Q}$. That is, we have shown that

$$D(\sigma) = |\det(\alpha|(\sigma-1)V)|.$$

The passage from $\mathbb{Z}$-modules with $\mathfrak{G}$-action to $\mathbb{Q}$-vector spaces with $\mathfrak{G}$-action now allows us to make use of representation theory in characteristic zero. Noting that the matrix

representing α on V (with respect to the natural permutation basis) is symmetric we see that the minimal polynomial of α as an endomorphism of V splits over $\mathbb{R}$. Moreover, the kernel of α is $\mathbb{Q} \cdot (\sum_{i \in I} d_i \Gamma_i)$ which is fixed by $\mathfrak{G}$. The result is now a consequence of the following two lemmas. $\square$

Lemma 5.2.3. *Let G be a finite cyclic group, generator σ, and let V be a $\mathbb{Q}[G]$-representation. Let $\alpha \in \mathrm{End}_{\mathbb{Q}[G]} V$ be a G-endomorphism of V whose minimal polynomial splits over $\mathbb{R}$ and such that $\ker(\alpha) \subseteq V^G$. Then, as elements of $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$,*

$$\det(\alpha | (\sigma - 1)V) = \det(\alpha | V_{-1,\sigma})$$

where $V_{-1,\sigma}$ is the (-1)-eigenspace for σ on V. (Here if $V_{-1,\sigma} = 0$ we define $\det(\alpha | V_{-1,\sigma}) = 1$.)

Proof. Let $V = \bigoplus_{i=1}^n V_i^{d_i}$ be an isotypic decomposition of V, so that each V_i is an irreducible $\mathbb{Q}[G]$-representation and $V_i \ncong V_j$ for $i \neq j$. Suppose, without loss of generality, that V_1 is the trivial representation. Then α preserves this decomposition and $(\sigma - 1)V = \bigoplus_{i=2}^n V_i^{d_i}$. By assumption, we see that the restriction of α to each $V_i^{d_i}$ with $i \geq 2$ is non-singular. Thus we are reduced to showing that if $V = W^d$ for an irreducible $\mathbb{Q}[G]$-representation, χ is the character of a complex irreducible constituent of W, and χ is non-real (so $\chi(\sigma) \notin \{\pm 1\}$), then $\det(\alpha) \in \mathbb{Q}^{\times 2}$. Now $A = \mathrm{End}_{\mathbb{Q}[G]} V \cong \mathrm{M}_d\left(\mathrm{End}_{\mathbb{Q}[G]} W\right)$ is a finite dimensional simple algebra over $\mathbb{Q}$. Set $D = \mathrm{End}_{\mathbb{Q}[G]} W$ so that D is a division algebra. Let $K/\mathbb{Q}$ be the centre of D. Note that if χ is the character of a complex irreducible component of W then (up to isomorphism over $\mathbb{Q}$) we have $K \cong \mathbb{Q}(\chi)$ where $\mathbb{Q}(\chi)$ is the character field of χ (see, for example, [Rei61] for proofs of representation theoretic facts used). Note that $K/\mathbb{Q}$ is abelian.

Now via the diagonal embedding of K into $\mathrm{End}_{\mathbb{Q}[G]} V$, V becomes a $K[G]$-module. Since K is the centre of $\mathrm{End}_{\mathbb{Q}[G]} V$, each $\mathbb{Q}[G]$-endomorphism of V is in fact K-linear so the natural inclusion $\mathrm{End}_{K[G]} V \subseteq \mathrm{End}_{\mathbb{Q}[G]} V$ is an equality. In particular, we may view α as a $K[G]$-endomorphism of V. Let $\det_K$ denote the determinant of a K-endomorphism of V and $\det_{\mathbb{Q}}$ denote the determinant of the same endomorphism now viewed as a $\mathbb{Q}$-endomorphism. Then we have

$$\det_{\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\det_K(\alpha))$$

(see, for example, [Cas67, Theorem A.1]).

As K in not totally real, there is an index 2 totally real subfield K^+ of K. I claim that for each $\sigma \in G$, $\det(\alpha)$ is in K^+. Indeed, since the minimal polynomial of α as

a $\mathbb{Q}$-endomorphism of V splits over $\mathbb{R}$, each root of the minimal polynomial of α as a K-endomorphism of V is totally real. It follows that $\det(\alpha)$ is a product of totally real numbers and hence in K^+. Thus

$$\det_{\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\det_K(\alpha)) = \left(N_{K^+/\mathbb{Q}}(\det_K(\alpha))\right)^2 \in \mathbb{Q}^{\times 2}$$

as desired. □

Lemma 5.2.4. *Let G be a finite group and V a $\mathbb{Q}[G]$-representation. Let $\alpha \in \mathrm{End}_{\mathbb{Q}[G]}V$ be a G-endomorphism of V whose minimal polynomial splits over $\mathbb{R}$ and such that $\ker(\alpha) \subseteq V^G$. For each $\sigma \in G$, let $V_{-1,\sigma}$ denote the (-1)-eigenspace for σ on V. Then the function*

$$\phi : G \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

defined by

$$\phi(\sigma) = \det(\alpha|V_{-1,\sigma})$$

is a homomorphism. (Here if $V_{-1,\sigma} = 0$ we define $\phi(\sigma) = 1$.)

Proof. We begin similarly to the proof of Lemma 5.2.3. By considering an isotypic decomposition of V we may assume that $V = W^d$ where W is an irreducible $\mathbb{Q}[G]$-representation and that α is non-singular. Let $A = \mathrm{End}_{\mathbb{Q}[G]}V \cong \mathrm{M}_d\left(\mathrm{End}_{\mathbb{Q}[G]}W\right)$, a finite dimensional simple algebra over $\mathbb{Q}$, let D be the division algebra $D = \mathrm{End}_{\mathbb{Q}[G]}W$, and $K/\mathbb{Q}$ be the centre of D. Again, if χ is the character of a complex irreducible component of W then (up to isomorphism over $\mathbb{Q}$) we have $K \cong \mathbb{Q}(\chi)$, and $K/\mathbb{Q}$ is abelian.

As before we view V as a $K[G]$-module and note that the natural inclusion $\mathrm{End}_{K[G]}V \subseteq \mathrm{End}_{\mathbb{Q}[G]}V$ is an equality so that we may view α as a $K[G]$-endomorphism of V. For all $\sigma \in G$ we have

$$\det_{\mathbb{Q}}(\alpha|V_{-1,\sigma}) = N_{K/\mathbb{Q}}(\det_K(\alpha|V_{-1,\sigma})).$$

That is, if $\phi_{\mathbb{Q}}$ is the map ϕ defined previously and ϕ_K is the function $G \to K^\times/K^{\times 2}$ defined by

$$\sigma \mapsto \det_K(\alpha|V_{-1,\sigma}),$$

we have $\phi_{\mathbb{Q}} = N_{K/\mathbb{Q}} \circ \phi_K$.

First suppose that K in not totally real. Then there is an index 2 totally real subfield K^+ of K and as in the proof of Lemma 5.2.3, for each $\sigma \in G$, $\det(\alpha|V_{-1,\sigma})$ is in K^+. Thus

for each $\sigma \in G$,

$$\phi_{\mathbb{Q}}(\sigma) = N_{K/\mathbb{Q}}\phi_K(\sigma) = \left(N_{K^+/\mathbb{Q}}\phi_K(\sigma)\right)^2 \in \mathbb{Q}^{\times 2}.$$

Thus $\phi_{\mathbb{Q}}$ is trivial in this case.

We may now assume that K is totally real, or equivalently that χ is real valued. Let m be the Schur index of χ (over $\mathbb{Q}$ or equivalently K). Suppose first that χ is realisable over $\mathbb{R}$. Then, via a chosen embedding $K \hookrightarrow \mathbb{R}$, we have $V \otimes_K \mathbb{R} \cong U^{md}$ for some irreducible real representation U. Fix $\sigma \in G$. Then $V_{-1,\sigma} \otimes_K \mathbb{R} = (V \otimes_K \mathbb{R})_{-1,\sigma}$ and viewing α as an element of $\mathrm{End}_{\mathbb{R}[G]}\left(U^{md}\right) \cong \mathrm{M}_{md}(\mathbb{R})$ we wish to compute the determinant of α on $(U_{-1,\sigma})^{md}$. Viewing α as a $md \times md$ matrix M over the reals via the identification discussed above, we see that the required determinant is given by $\det(M)^{\dim U_{-1,\sigma}}$. In fact, one sees that $\det(M)$ is equal to $\mathrm{Nrd}(\alpha) \in K^\times$ where here Nrd denotes the reduced norm on the central simple algebra $A = \mathrm{End}_{\mathbb{Q}[G]}V$ over K. Thus to show that ϕ_K is a homomorphism (and hence $\phi_{\mathbb{Q}}$ as $N_{K/\mathbb{Q}}$ is), we want to show that the congruence

$$\dim U_{-1,\sigma} + \dim U_{-1,\tau} \equiv \dim U_{-1,\sigma\tau} \pmod 2$$

holds for all σ and τ in G. However, U is a real vector space and each $\sigma \in G$ acts on U as a finite order matrix which is hence diagonalisable over $\mathbb{C}$. Base-changing to $\mathbb{C}$, diagonalising σ and noting that the eigenvalues of σ are roots of unity appearing in conjugate pairs, one sees that for each $\sigma \in G$ we have

$$\det(\sigma) = (-1)^{\dim U_{-1,\sigma}},$$

which proves the desired congruence.

Finally, suppose that χ is not realisable over $\mathbb{R}$. Then we have $V \otimes_K \mathbb{C} \cong U^{md}$ where U is an irreducible representation over $\mathbb{C}$ and, by assumption, U and hence U^{md} possesses a non-degenerate G-invariant alternating form, which we denote by $\langle \cdot, \cdot \rangle$. The argument for the previous case again gives $\det_K(\alpha | V_{-1,\sigma}) = \mathrm{Nrd}(\alpha)^{\dim U_{-1,\sigma}}$. I claim that now $\dim U_{-1,\sigma}$ is even for each $\sigma \in G$, from which it follows that ϕ_K, and hence $\phi_{\mathbb{Q}}$, is trivial.

Indeed, the pairing $\langle\ ,\ \rangle$ gives a G-equivariant isomorphism from U to its dual U^*. In partiular, this isomorphism respects the σ-eigenspace decomposition on each side and hence restricts to an isomoprhism $U_{-1,\sigma} \xrightarrow{\sim} U^*_{-1,\sigma}$ whose associated bilinear pairing is alternating. Thus $\dim U_{-1,\sigma}$ is even.

This completes the proof of the lemma. □

The proof of Theorem 5.2.2 facilitates the computation of Tamagawa numbers of Jacobians of curves, at least up to squares, and to end the section we record this in the following proposition.

Proposition 5.2.5. *Let K be a nonarchimedean local field, X/K a smooth, proper, geometrically integral curve of genus g, $\mathcal{X}/\mathcal{O}_K$ its minimal proper regular model and $\mathcal{X}_{\bar{k}}$ the special fibre of $\mathcal{X}$, base-changed to $\bar{k}$. Let Φ be the component group of the special fibre of the Néron model of the the Jacobian of X and $I = \{\Gamma_1, ..., \Gamma_n\}$ be the set of irreducible components of $\mathcal{X}_{\bar{k}}$. For each Γ_i let $d(\Gamma_i)$ be its multiplicity in $\mathcal{X}_{\bar{k}}$ and $r(\Gamma_i)$ the size of the orbit of Γ_i under the action of $Gal(\bar{k}/k)$ on I. Write $d' = \gcd_{i\in I}\{d(\Gamma_i)r(\Gamma_i)\}$ and define q to be 2 if d' does not divide $g-1$, and 1 otherwise. Finally, let $S_1, ..., S_m$ be the even sized orbits of $\mathrm{Gal}(\bar{k}/k)$ on $\{\Gamma_1, ..., \Gamma_n\}$, let $r_i = |S_i|$ and for each $1 \leq i \leq m$, write*

$$\epsilon_i = \sum_{i=0}^{r_i - 1} (-1)^i \sigma^i(\Gamma_{i,1})$$

where $\sigma \in \mathrm{Gal}(\bar{k}/k)$ denotes the Frobenius element and $\Gamma_{i,1}$ is a representative of the orbit S_i. Then

$$q\frac{|\Phi(\bar{k})|}{|\Phi(k)|} \equiv \left|\det\left(\frac{1}{r_j}\langle \epsilon_i, \epsilon_j\rangle\right)_{1\leq i,j\leq m}\right| \pmod{\mathbb{Q}^{\times 2}}$$

where $\langle\cdot,\cdot\rangle$ denotes the intersection pairing on $\mathcal{X}_{\bar{k}}$.

Proof. The special fibre $\mathcal{X}_{\bar{k}}$ is naturally identified with the special fibre of the minimal proper regular model of X over $\mathcal{O}_{K^{\mathrm{nr}}}$. We are now in the situation of Example 5.1.2. Noting that each element of $\mathrm{Gal}(\bar{k}/k)$ acts on the components of $\mathcal{X}_{\bar{k}}$ as elements of the group $\mathfrak{G}$, the (proof of) Theorem 5.2.2, along with Lemma 5.2.3, gives

$$q\frac{|\Phi(\bar{k})|}{|\Phi(k)|} \equiv |\det(\alpha|\mathbb{Q}[I]_{-1})| \pmod{\mathbb{Q}^{\times 2}}$$

where $\mathbb{Q}[I]_{-1}$ denotes the (-1)-eigenspace of $\mathrm{Gal}(\bar{k}/k)$ on the permutation module $\mathbb{Q}[I]$ and α is the linear map given by $\Gamma_i \mapsto \sum_j \langle \Gamma_i \cdot \Gamma_j\rangle \Gamma_j$. One easily sees that $\{\epsilon_1, ..., \epsilon_k\}$ forms a basis for $\mathbb{Q}[I]_{-1}$ (so the dimension of this space is the number of even sized orbits on $\{\Gamma_1, ..., \Gamma_n\}$). Moreover, using $\mathrm{Gal}(\bar{k}/k)$-invariance of the intersection pairing, one computes

$$\alpha(\epsilon_i) = \sum_{j=1}^{k} \langle \epsilon_i, \Gamma_{j,1}\rangle \epsilon_j = \sum_{j=1}^{k} \frac{1}{r_j}\langle \epsilon_i, \epsilon_j\rangle \epsilon_j$$

and the result follows. □

5.3 2-torsion in the component group of a hyperelliptic curve having semistable reduction

Let K be a nonarchimedean local field of odd residue characteristic and C/K a hyperelliptic curve with semistable reduction over K. Let $\mathcal{C}/\mathcal{O}_{K^{\mathrm{nr}}}$ be the minimal proper regular model of C over the maximal unramified extension K^{nr}. Then $\mathcal{C}$ is semistable by [Liu02, Theorem 10.3.34]. Let G be the *intersection* graph of its special fibre. That is, the vertices of G are the irreducible components of the special fibre, and two vertices corresponding to distinct components Γ_i and Γ_j are joined by one edge for each of the intersection points between Γ_i and Γ_j (the semitability assumption means all intersection multiplicities are one). Thus G has no 1-edge loops, but may have multiple edges. The semistability assumption ensures that the multiplicity of each irreducible component is 1, and so the Jacobian of G is precisely the component group of the curve. Now the hyperelliptic involution of C extends to an automorphism ι of $\mathcal{C}$ by [Liu02, Proposition 10.1.16] and hence induces a graph theoretic automorphism ι on G. Indeed, ι clearly permutes the irreducible components and similarly permutes the intersection points between components. Now ι induces multiplication by -1 on the component group since the hyperelliptic involution induces multiplication by -1 on the Jacobian of C (see also the proof of [BL99, Theorem 1.1]). Now consider the quotient scheme $\mathcal{Y} := \mathcal{C}/\iota$. This exists since $\mathcal{C}$ is projective (this is a result of Lichtenbaum, [Lic68, Theorem 2.8]). Moreover, the quotient morphism $\psi : \mathcal{C} \to \mathcal{Y}$ is finite flat, and $\mathcal{Y}$ is semistable by [Liu02, Proposition 10.3.48]. As the quotient commutes with flat base-change, we see that the generic fibre of $\mathcal{Y}$ is isomorphic to $\mathbb{P}^1_{K^{\mathrm{nr}}}$ (as the quotient of C by the hyperelliptic involution is isomorphic to $\mathbb{P}^1_K$). Moreover, $\mathcal{Y}$ is flat over $\mathcal{O}_K$ since $\mathcal{C}$ is and so the special fibre $\mathcal{Y}_{\bar{k}}$ has arithmetic genus 0. In particular, the intersection graph of $\mathcal{Y}_{\bar{k}}$ is a tree (this is the graph whose vertices are the irreducible components of $\mathcal{Y}_{\bar{k}}$ and such that two distinct vertices are joined by one edge for every intersection point between the corresponding components (each intersection point being counted with multiplicity one)). Moreover, by [LL99, Remark 1.7], the base-change of the quotient morphism ψ to the special fibre realises $\mathcal{Y}_{\bar{k}}$ as the quotient of $\mathcal{C}_{\bar{k}}$ by the extension of the hyperelliptic involution. Note that this uses the assumption that the residue characteristic is coprime to the order of ι; taking quotients does not commute with base-change to the special fibre in general. In particular, the quotient of the graph G by the automorphism of G induced

by ι is a tree.

Thus we are in the following situation: G is a finite connected graph, without loops, possessing an automorphism ι inducing multiplication by -1 on $\Phi := \mathrm{Jac}(G)$, such that the quotient of G by ι is a tree. In fact, these last two conditions are very closely related. See [BN09, Theorem 5.12] for more details. (To construct the quotient, one takes the vertices to be the orbits of ι on $V(G)$, and the edges to be the orbits of ι on the subset of $E(G)$ consisting of edges whose endpoints are inequivalent (with the orbit of a given edge joining the orbits of its endpoints).) We are interested in the group $\Phi[2]$, and in particular in the parity of its $\mathbb{F}_2$-dimension. The result is the following.

Theorem 5.3.1. *Let G be a finite connected graph, without loops, endowed with an automorphism ι inducing multiplication by -1 on $\Phi := Jac(G)$, and such that the quotient of G by ι is a tree. Let $\mathcal{W}$ be the set of vertices fixed by ι. Further, let $g = |E(G)| - |V(G)| + 1$, $b(G)$ denote the number of bridges in G, and $b_{\mathcal{W}}(G)$ denote the number of bridges in G whose endpoints are both in $\mathcal{W}$. Then*

$$\dim_{\mathbb{F}_2}\Phi[2] = \begin{cases} |\mathcal{W}| - b_{\mathcal{W}}(G) - 1, & \text{if } \mathcal{W} \neq \emptyset, \\ 0, & \text{if } \mathcal{W} = \emptyset \text{ and } g \text{ even}, \\ 1, & \text{if } \mathcal{W} = \emptyset \text{ and } g \text{ odd}. \end{cases}$$

Moreover, we have

$$\dim_{\mathbb{F}_2}\Phi[2] \equiv \begin{cases} |V(G)| - b(G) - 1, & \text{if } \mathcal{W} \neq \emptyset, \text{ or, in the case } \mathcal{W} = \emptyset, \text{ either } g \text{ is odd or } g = 0 \\ |V(G)| - b(G), & \text{else.} \end{cases}$$

Proof. Throughout the proof of the theorem we will use the fact that the Jacobian of a (connected) tree is trivial. More generally, the order of the group Φ is equal to the number of spanning trees of the graph G. This follows from Kirchoff's Matrix Tree Theorem (see [Big97, Section 14]).

Since ι induces multiplication by -1 on Φ, we have an isomorphism between $\Phi[2]$ and the Tate-cohomology group $\hat{\mathrm{H}}^0(\iota, \Phi)$ (here we write ι in place of the order two subgroup of $\mathrm{Aut}(G)$ which it generates). In light of Theorem 5.2.1, we have an exact sequence

$$\hat{\mathrm{H}}^0(\iota, \mathrm{im}(\alpha)) \longrightarrow \hat{\mathrm{H}}^0(\iota, \ker(\beta)) \longrightarrow \Phi[2] \longrightarrow q\mathbb{Z}/d'\mathbb{Z} \longrightarrow 0$$

where d' is the greatest common divisor of the lengths of the orbits of ι on $V(G)$ and q is

equal to 1 if d' divides $g-1$, and 2 else (the maps α and β are as in Example 5.1.3). Thus we have

$$q\mathbb{Z}/d'\mathbb{Z} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } \mathcal{W} = \emptyset \text{ and } g \text{ odd}, \\ 0, & \text{else.} \end{cases}$$

It remains to determine the group

$$A := \frac{\hat{\mathrm{H}}^0(\iota, \ker(\beta))}{\mathrm{im}\left(\hat{\mathrm{H}}^0(\iota, \mathrm{im}(\alpha))\right)}.$$

Writing $F = \sum_{v \in G} v$ and letting the set I index the vertices of G, as in Example 5.1.3 we have a short exact sequence

$$0 \longrightarrow F\mathbb{Z} \longrightarrow \mathbb{Z}^I \xrightarrow{\alpha} \mathrm{im}(\alpha) \longrightarrow 0$$

from which we deduce that the map

$$\hat{\mathrm{H}}^0(\iota, \mathbb{Z}^I) \xrightarrow{\alpha} \hat{\mathrm{H}}^0(\iota, \mathrm{im}(\alpha))$$

is surjective. Moreover, we have $\hat{\mathrm{H}}^0(\iota, \mathbb{Z}^I) = \mathbb{F}_2^{\mathcal{W}}$. Next, taking the long exact sequence for Tate-cohomology associated to the short exact sequence

$$0 \longrightarrow \ker(\beta) \longrightarrow \mathbb{Z}^I \xrightarrow{\beta} \mathbb{Z} \longrightarrow 0$$

gives

$$\hat{\mathrm{H}}^0(\iota, \ker(\beta)) = \ker\left(\mathbb{F}_2^{\mathcal{W}} \xrightarrow{\Sigma} \mathbb{F}_2\right)$$

where here the map Σ sends $\sum_{w \in \mathcal{W}} n_w w$ to $\sum_{w \in \mathcal{W}} n_w$.

The discussion above shows that the group A may be identified with the cokernel of the map

$$\bar{\alpha} : \mathbb{F}_2^{\mathcal{W}} \longrightarrow \ker\left(\mathbb{F}_2^{\mathcal{W}} \xrightarrow{\Sigma} \mathbb{F}_2\right)$$

which is given by lifting an element of $\mathbb{F}_2^{\mathcal{W}}$ to $\mathbb{Z}^{\mathcal{W}}$, applying α, projecting onto $\mathbb{Z}^{\mathcal{W}}$ and then reducing the coefficients modulo 2 to land in $\ker\left(\mathbb{F}_2^{\mathcal{W}} \xrightarrow{\Sigma} \mathbb{F}_2\right)$.

We now study the cokernel of $\bar{\alpha}$ viewed as an endomorphism of $\mathbb{F}_2[\mathcal{W}]$. That is, we study the group

$$B := \frac{\mathbb{F}_2^{\mathcal{W}}}{\bar{\alpha}\left(\mathbb{F}_2^{\mathcal{W}}\right)},$$

whose $\mathbb{F}_2$-dimension is 1 more than the dimension of A, save when $\mathcal{W} = \emptyset$, where the two dimensions agree and are both 0.

Suppose $x_1 \neq x_2$ are distinct elements of $\mathcal{W}$ and that e is an edge in G between x_1 and x_2. I claim that either $\iota(e) \neq e$, or e is a bridge in G. Indeed, suppose $\iota(e) = e$. As x_1 and x_2 are distinct and both fixed by ι, they yield distinct vertices $\bar{x}_1$ and $\bar{x}_2$ in the quotient $T := G/\iota$. Now suppose that $e_1...e_l$ is a path from x_1 to x_2 in G. This reduces to a path $\bar{e}_1...\bar{e}_l$ from $\bar{x}_1$ to $\bar{x}_2$ in T (if an edge e_i has its ends equivalent, we omit it in the reduction). Now T is a tree so $\bar{e}$ appears in this path. Since e is fixed by ι, e must appear as one of the e_i in the original path. Thus e is a bridge in G and we have proved the claim.

Now let T' be the subgraph of G spanned by the elements of $\mathcal{W}$ and the bridges in G between them and let $\alpha' : \mathbb{Z}^{\mathcal{W}} \to \mathbb{Z}^{\mathcal{W}}$ be the intersection map associated to T' in the usual way. The discussion above shows that α' reduces to $\bar{\alpha} : \mathbb{F}_2^{\mathcal{W}} \to \mathbb{F}_2^{\mathcal{W}}$ (the only thing that doesn't immediately follow from the above is that the diagonal entries match up, but this is clear since any vertex x of G not fixed by ι contributes an even number to the degree of any $w \in \mathcal{W}$ when considered along with $\iota(x)$).

Now as each vertex of T' and each edge of T' is fixed by ι, T' is naturally a subgraph of T. Thus T' is a disjoint union of connected trees, $T_1, ..., T_l$ say. Correspondingly, the matrix of α' is block diagonal with blocks $\alpha_1, ..., \alpha_l$, where α_i is the 'intersection' matrix associated to the tree T_i. Since each T_i is a tree, the Jacobian of each T_i is trivial. Thus we deduce, for each i, the existence of exact sequences

$$\mathbb{Z}^{T_i} \xrightarrow{\alpha_i} \mathbb{Z}^{T_i} \xrightarrow{\Sigma} \mathbb{Z} \longrightarrow 0$$

where as before, Σ denotes the 'sum of coefficients' map. Tensoring by $\mathbb{F}_2$ yields exact sequences

$$\mathbb{F}_2^{T_i} \xrightarrow{\alpha_i} \mathbb{F}_2^{T_i} \xrightarrow{\Sigma} \mathbb{F}_2 \longrightarrow 0.$$

It follows that for each i, the cokernel of α_i is isomorphic to $\mathbb{F}_2$. We deduce that $\dim_{\mathbb{F}_2} B$ is equal to l, the number of connected components of T'. Since T' is a disjoint union of trees, we see that l is equal to the difference of the number of vertices of T' and the number of edges in T'. That is, $l = |\mathcal{W}| - b_{\mathcal{W}}(G)$. This completes the proof of the formula for $\dim_{\mathbb{F}_2} \Phi[2]$.

To prove the congruence, first note that since each orbit of ι on $V(G)$ has order either 1 or 2, $|\mathcal{W}|$ is congruent modulo 2 to $|V(G)|$. We now wish to compare $b_{\mathcal{W}}(G)$ and $b(G)$. The involution ι acts on the set of bridges in G, so $b(G)$ is congruent modulo 2 to the number

of bridges in G fixed by ι. Each such bridge either joins 2 elements of $\mathcal{W}$, or has its ends swapped. Suppose that G has a bridge e which has its ends swapped by ι. I claim that then $\mathcal{W} = \emptyset$ and G is a tree. From this the result follows easily. Let e be such an edge. Let x_1 and x_2 be its (distinct) endpoints. Removing e from G splits G into 2 connected components G_1 and G_2, with (without loss of generality) $x_1 \in G_1$ and $x_2 \in G_2$. We see that ι must map G_1 onto G_2 and hence $\mathcal{W} = \emptyset$. Moreover, as there are no edges other than e between G_1 and G_2, there a no other edges which have their endpoints swapped. It follows that T is isomorphic to G_i for each i and hence both G_1 and G_2 are trees. Since e was a bridge in G, it follows that G too is a tree. □

In [BN09], the notion of a *hyperelliptic* graph is introduced and it is shown that 2-edge connected hyperelliptic graphs of genus $g = \#E(G) - \#V(G) + 1 \geq 2$ and their Jacobians enjoy many properties analogous to hyperelliptic curves and their Jacobians. One of the equivalent conditions for a 2-edge connected graph G of genus at least 2 to be hyperelliptic is that is possesses an involution ι such that the quotient graph G/ι is a tree (in fact, this also ensures that ι induces multiplication by -1 on the Jacobian of G, see [BN09, Theorem 5.12]). Theorem 5.3.1 enables us to deduce another property of 2-edge connected, hyperelliptic graphs of genus $g \geq 2$ analogous to that of hyperelliptic curves. Namely, the description of the 2-torsion in their Jacobian in terms of the points fixed by the hyperelliptic involution. The result is the following, and the analogue for hyperelliptic curves is discussed in Section 3.2.

Corollary 5.3.2. *Let G be a finite, 2-edge connected graph with genus $g \geq 2$ with no loops (but possibly multiple edges). Suppose that G posesses an involution ι such that the quotient G/ι is a tree. Let $\mathcal{W}$ be the set of fixed points of ι and let Φ be the Jacobian of G. Then if $\mathcal{W} \neq \emptyset$ or the genus of g is even, we have an isomorphism*

$$\Phi[2] \cong \ker\left(\mathbb{F}_2[\mathcal{W}] \overset{\text{sum}}{\to} \mathbb{F}_2\right).$$

On the other hand, if $\mathcal{W} = \emptyset$ and the genus of G is odd, we have $\Phi[2] \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. This follows immediately from (the proof of) Theorem 5.3.1 as the assumption that G is 2-edge connected means there are no bridges in G. □

We end by giving a description of the parity of the $\mathbb{F}_2$-dimension of the 2-torsion in the Jacobian of a semistable hyperelliptic curve.

Corollary 5.3.3. *Let K be a local field of odd residue characteristic and C/K a semistable hyperelliptic curve of genus $g \geq 2$. Let J/K be the Jacobian of C and Φ its component group. Let $\mathcal{C}/\mathcal{O}_K$ be the minimal proper regular model of C and let $\mathcal{C}_{\bar{k}}$ be its special fibre, base-changed to $\bar{k}$. Let $\epsilon(C)$ be equal to 1 if g is even and no irreducible component of $\mathcal{C}_{\bar{k}}$ is fixed by (the extension to $\mathcal{C}$ of) the hyperelliptic involution, and 0 else. Finally, let n be the number of irreducible components of $\mathcal{C}_{\bar{k}}$ and let b be the number of singular points x of $\mathcal{C}_{\bar{k}}$ such that $\mathcal{C}_{\bar{k}} - \{x\}$ is disconnected. Then*

$$\dim_{\mathbb{F}_2}\Phi[2] + \epsilon(C) \equiv n - 1 + b \pmod 2.$$

Proof. By Theorem 5.3.1 and the discussion preceding it, we just need to show that if the intersection graph G of $\mathcal{C}_{\bar{k}}$ is a tree, then the hyperelliptic involution does not act without fixed points. However, since G is a tree and $g \geq 0$, it follows that there is at least one component with strictly positive (arithmetic) genus. This must then be fixed by the hyperelliptic involution else this would contradict the quotient by the extension of the hyperelliptic involution having arithmetic genus 0. This produces the required fixed vertex of G. □

Chapter 6

Unramified extensions

In this chapter we prove Conjecture 1 in the case that the local field K is non-archimedean, the separable quadratic extension L/K is unramified and the residue characteristic of K is odd. The main reason that we can say more when L/K is unramified is that the formation of Neron models and minimal proper regular models commutes with unramified base-change. This makes the relevant Tamagawa numbers easier to describe and relate to other quantities.

We begin by studying Conjecture 1 without insisting that the residue characteristic of K is odd, though we will eventually do this. Whilst we only prove a very small number of additional cases of Conjecture 1 in residue characteristic 2 (see Remark 6.0.15), we make a substantial reduction in all residue characteristics (the precise statement of which is Corollary 6.0.6). In particular, we reduce Conjecture 1 to a statement which only depends on the curve C considered over the maximal unramified extension of K. In odd residue characteristic we then give a proof of this.

Fix now a non-archimedean local field K and let L/K be its unique quadratic unramified extension. As usual, let C be a hyperelliptic curve over K and J/K its Jacobian.

Lemma 6.0.1. *We have*

$$w(J/L) = (-1)^{\mathfrak{f}(J/K)}$$

and

$$\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L) = \dim_{\mathbb{F}_2} \mathrm{H}^1(k_L/k, \Phi(k_L)),$$

where $\mathfrak{f}(J/K)$ denotes the conductor exponent of J and Φ is the component group of (the special fibre of the Néron model of) J.

Proof. For the statement about root numbers see [KT82, Proposition 2.4(c)] which proves

the result for elliptic curves, and [Čes14a, Corollary A.6] which proves a more general statement for arbitrary abelian varieties. The statement about the norm map follows from [Maz72, Proposition 4.3]. □

Lemma 6.0.1 describes two of the terms appearing in Conjecture 1 and we also note that as L/K is unramified, we have

$$(\Delta_C, L/K) = (-1)^{v_K(\Delta_C)}.$$

To ease notation in subsequent formulas, we define

$$\epsilon(C, K) = \frac{1 - i_d(C_K)}{2}$$

so that $\epsilon(C, K)$ is equal to 1 if C is deficient over K, and 0 else. (We have added explicit dependence on K when defining $\epsilon(C, K)$ as we shall shortly wish to vary the base field). The discussion above shows that Conjecture 1 for L/K is the assertion that

$$\mathfrak{f}(J/K) \equiv v_K(\Delta_C) + \dim_{\mathbb{F}_2} \mathrm{H}^1(k_L/k, \Phi(k_L)) + \epsilon(C, K) + \epsilon(C^L, K) \pmod 2. \tag{6.0.2}$$

Since the conductor and valuation are unchanged under unramified extensions, this predicts that the quantity

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(k_L/k, \Phi(k_L)) + \epsilon(C, K) + \epsilon(C^L, K) \tag{6.0.3}$$

is also unchanged modulo 2 upon replacing K by a finite unramified extension F, and replacing L by the unique quadratic unramified extension F'/F. If F is chosen to be sufficiently large, then $\mathrm{Gal}(\bar{k}/k_F)$ will act trivially on $\Phi(\bar{k})$ whence

$$\mathrm{H}^1(k_{F'}/k_F, \Phi(k_{F'})) = \Phi(\bar{k})[2].$$

Moreover, as soon as F contains a separable quadratic extension of K and $\mathrm{Gal}(\bar{k}/k_F)$ acts trivially on the components of $\mathcal{C}_{\bar{k}}$ (where as usual $\mathcal{C}$ denotes the minimal proper regular model of C over $\mathcal{O}_K$), it follows from Proposition 8.3.6 and Remark 3.3.4 that $\epsilon(C, F) = 0$ and $\epsilon(C^{F'}, F)$ is equal to 1 if and only if C has even genus and the hyperelliptic involution does not fix any odd multiplicity components of $\mathcal{C}_{\bar{k}}$. To emphasize that this last statement is independent of the field, we set $\epsilon(C)$ to be 1 if this happens, and 0 otherwise. (In fact, since $\mathcal{C}_{\bar{k}}$ coincides with the special fibre of the minimal regular model of $\mathcal{C}$ over $\mathcal{O}_{K^{nr}}$, $\epsilon(C)$ depends only on C through its base change to K^{nr}.) Thus instead of just predicting

that (6.0.3) is unchanged modulo 2 in unramified extensions, we can write down a (so far conjectural but soon to be proven) expression for it which clearly has this property. That is, we have:

Lemma 6.0.4. *Let K be a local field of characteristic zero and L/K an unramified quadratic extension. Then*

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(L/K, \Phi(k_L)) + \epsilon(C, K) + \epsilon(C^L, K) \equiv \dim_{\mathbb{F}_2} \Phi(\bar{k})[2] + \epsilon(C) \pmod 2.$$

Proof. This will result from Theorem 5.2.2 of the previous chapter. We work in the setup of Example 5.1.2. We take $\mathcal{C}$ to be the base-change to $\mathcal{O}_{K^{\mathrm{nr}}}$ of the minimal proper regular model of C over $\mathcal{O}_K$ (as the formation of the minimal proper regular model commutes with unramified base-change, this is just the minimal proper regular model of C over $\mathcal{O}_{K^{\mathrm{nr}}}$). The associated group Φ is the component group of the Néron model of J and elements of $\mathrm{Gal}(\bar{k}/k)$ act naturally on the components of the special fibre of $\mathcal{C}$ in such a way that they lie in the group $\mathfrak{G}$ associated to the data of Example 5.1.2. Moreover, the induced action on Φ is the natural one (see [BL99, Theorem 1.1]). The hyperelliptic involution of C extends uniquely to an automorphism of $\mathcal{C}$ and its induced action on the components of the special fibre is also an element of $\mathfrak{G}$. The hyperelliptic involution ι on C extends to an automorphism of the minimal regular model of C and may therefore be viewed as an element of $\mathfrak{G}$. Moreover, as the induced automorphism ι_* of the Jacobian of C is multiplication by -1, the action on Φ induced by $\iota \in \mathfrak{G}$ is multiplication by -1 also (see the proof of [BL99, Theorem 1.1]). Thus

$$\Phi(\bar{k})[2] = (\ker(\beta)/\mathrm{im}(\alpha))^{\iota}.$$

Let σ denote the Frobenius element in $\mathrm{Gal}(\bar{k}/k)$. Then

$$\left|\mathrm{H}^1\left(\mathrm{Gal}(k_L/k), \Phi(k_L)\right)\right| = \left|\frac{\ker\left(1+\sigma|\Phi(\bar{k})^{\sigma^2}\right)}{\mathrm{im}\left(1-\sigma|\Phi(\bar{k})^{\sigma^2}\right)}\right| = \frac{\left|\Phi(\bar{k})^{-\sigma}\right| \cdot \left|\Phi(\bar{k})^{\sigma}\right|}{\left|\Phi(\bar{k})^{\sigma^2}\right|}.$$

(Incidentally, this shows that Lemma 2.1.7 continues to hold in residue characteristic 2, as long as the quadratic extension is unramified.) Moreover, we have $\epsilon(C) = \mathrm{ord}_2\left(q(\iota)\right)$, $\epsilon(C, K) = \mathrm{ord}_2\left(q(\sigma)\right)$ and $\epsilon(C^L, K) = \mathrm{ord}_2\left(q(\iota \circ \sigma)\right)$ (where here q is the function defined on $\mathfrak{G}$ as in Section 5.2). Indeed, for this last equality, since the formation of minimal proper regular models commutes with unramified base-change, we may identify the base-change

to $\bar{k}$ of the special fibre of the minimal proper regular model of C^L over K with that of C, except now the action of $\mathrm{Gal}(\bar{k}/k)$ has been twisted by the hyperelliptic involution. Finally, Proposition 8.3.6 gives $\epsilon(C, L) = \mathrm{ord}_2(q(\sigma^2)) = 0$. On the other hand, it follows from Theorem 5.2.2 that

$$D(\sigma)D(\iota \circ \sigma)D(\sigma^2) = D(\iota)$$

(with D as in the statement of Theorem 5.2.2) as elements of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Taking 2-adic valuations of this equation gives the desired congruence. □

Remark 6.0.5. *It is not simply true that*

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(L/K, \Phi(k_L)) \equiv \dim_{\mathbb{F}_2} \Phi(\bar{k})[2] \pmod 2$$

and

$$\epsilon(C, K) + \epsilon(C^L, K) \equiv \epsilon(C) \pmod 2$$

individually. Indeed, the genus 2 curve

$$C : y^2 = (x^2 + 3)((x - i)^2 - 3^2)((x + i)^2 - 3^2)$$

over $\mathbb{Q}_3$ (here i is a square root of -1 in $\bar{\mathbb{Q}}_3$) has $\epsilon(C, \mathbb{Q}_3) = \epsilon(C) = 0$, yet $\epsilon(C^L, \mathbb{Q}_3) = 1$ (where $L = \mathbb{Q}_3(i)$ is the unique quadratic unramified extension of $\mathbb{Q}_3$). This follows easily from the description in Section 7.2.2 of the minimal regular model, along with action of Frobenius, of hyperelliptic curves (in odd residue characteristic) of the form $y^2 = f(x)$ where $f(x)$ is monic and has cube free reduction.

Corollary 6.0.6. *Let K be a non-archimedean local field, L/K its unique quadratic unramified extension, C/K a hyperelliptic curve and J/K its Jacobian. Then Conjecture 1 holds for C and the extension L/K if and only if*

$$\mathfrak{f}(J/K) \equiv v_K(\Delta_C) + \dim_{\mathbb{F}_2} \Phi(\bar{k})[2] + \epsilon(C) \pmod 2 \tag{6.0.7}$$

where here $\epsilon(C)$ is equal to 1 if C has even genus and the hyperelliptic involution does not fix any odd multiplicity component of $\mathcal{C}_{\bar{k}}$ ($\mathcal{C}$ is the minimal proper regular model of C over $\mathcal{O}_K$), and 0 else.

Remark 6.0.8. *It follows from Section 4.1 that over local fields of odd residue characteristic (6.0.7) holds for hyperelliptic curves whose Jacobian has good reduction. In Section 8.1*

we will extend this to include the case of good reduction of the Jacobian over local fields of characteristic zero but residue characteristic two.

6.0.1 Establishing (6.0.7) in odd residue characteristic

Assume now that the residue characteristic of K is odd. Under this assumption, we now establish the congruence (6.0.7).

Lemma 6.0.9. *We have*

$$\mathfrak{f}(J/K) = \mathfrak{f}(J[2]) + \dim_{\mathbb{F}_2} \Phi(\bar{k})[2]$$

where here $\mathfrak{f}(J[2])$ *denotes the Artin conductor exponent of* $J[2]$.

Proof. This is observed by Česnavičius in [Čes14a, Lemma 4.2]. Note that this requires the assumption that the residue characteristic of K is odd. □

It thus remains to show that

$$\mathfrak{f}(J[2]) \equiv v_K(\Delta_C) + \epsilon(C) \pmod 2.$$

Denote by K^{nr} the maximal unramified extension of K and let v be the normalised valuation on K^{nr}. As usual, let C be given by the equation $y^2 = f(x)$ where $f \in K[x]$ is a separable polynomial of degree $2g+1$ or $2g+2$ for $g \geq 2$. In fact, we may suppose that the degree is $2g+2$. Indeed, if not, one can make a change of variables over K to ensure that none of the points at infinity on C are ramified in the degree two 'x-coordinate' map to $\mathbb{P}^1_K$. The resulting polynomial then has even degree. Let E/K^{nr} be the field extension $E = K^{\mathrm{nr}}(J[2])$, and set $G = \mathrm{Gal}(E/K)$. As in Section 3.2, E coincides with the splitting field of f over K^{nr}. Let $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots$ be the ramification filtration of G, and $g_i = |G_i|$. Thus G_1 is the wild inertia group of E/K^{nr} and is a p-group, where $p = \mathrm{char}(k)$ (so in particular has odd order) and G/G_1 is cyclic. Let $\mathcal{W}$ denote the G-set of roots of f in E. Then by definition we have

$$\mathfrak{f}(J[2]) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \mathrm{codim}_{\mathbb{F}_2} J[2]^{G_i}.$$

Proposition 6.0.10. *Define $\epsilon(f)$ to be 1 if the genus g of C is even and each irreducible factor of f over K^{nr} has even degree, and 0 else. Then*

$$\mathfrak{f}(J[2]) \equiv v(\Delta_f) + \epsilon(f) \pmod 2.$$

Proof. This is an immediate consequence of the following two lemmas. □

Lemma 6.0.11. *Let $\epsilon(f)$ be as above, and let $V = \mathbb{C}[\mathcal{W}]$ be the complex permutation representation for G associated to $\mathcal{W}$. Then we have*

$$\mathfrak{f}(J[2]) = \mathfrak{f}(V) + \epsilon(f).$$

Proof. This will follow from the definition of $\mathfrak{f}(J[2])$ and $\mathfrak{f}(V)$, along with a comparison between $\mathrm{codim}_{\mathbb{C}} V^{G_i}$ and $\mathrm{codim}_{\mathbb{F}_2} J[2]^{G_i}$ for each i (afforded by Lemma 3.2.1).

First let $i \geq 1$ so that G_i has odd order. Then necessarily f has an odd degree factor over E^{G_i} and it follows from Lemma 3.2.1 that $\dim_{\mathbb{F}_2} J[2]^{G_i} = \dim_{\mathbb{C}} V^{G_i} - 2$. Since also $\dim_{\mathbb{F}_2} J[2] = \dim_{\mathbb{C}} V - 2$, we see that

$$\sum_{i=1}^{\infty} \frac{g_i}{g_0} \mathrm{codim}_{\mathbb{F}_2} J[2]^{G_i} = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \mathrm{codim}_{\mathbb{C}} V^{G_i}$$

and all that remains is to show that

$$\mathrm{codim}_{\mathbb{F}_2} J[2]^{G} \equiv \mathrm{codim}_{\mathbb{C}} V^{G} + \epsilon(f) \pmod 2.$$

If g is even, Lemma 3.2.1 gives $\dim_{\mathbb{F}_2} J[2]^G = \dim_{\mathbb{C}} V^G - 2 + \epsilon(f)$ and we are done. Thus suppose that g is odd. If f has an odd degree factor over K^{nr} then again we conclude immediately from Lemma 3.2.1.

Finally, suppose each irreducible factor of f over K^{nr} has even degree. By one last application of Lemma 3.2.1 it suffices to show that there is a unique quadratic subextension of E/K^{nr} over which f factors into two conjugate polynomials. To see this, first note that there is a unique quadratic subextension of E/K^{nr}. Indeed, any such extension must necessarily be contained in E^{G_1}, yet E^{G_1}/K^{nr} is cyclic and has even order by the assumption on the degrees of the irreducible factors of f over K. To see that f admits the required factorisation over this extension, let $S = \{h_1, ..., h_l\}$ be the set of irreducible factors of f over E^{G_1}, each of which necessarily has odd degree. The cyclic group G/G_1 acts on S and as each factor of f over K^{nr} has even degree, each orbit of G/G_1 on S has even order.

Denote these disjoint orbits by $S_1, ..., S_k$, and write $S_i = \{h_{i,1}, ..., h_{i,d_i}\}$. Fix a generator σ of G/G_1 and assume without loss of generality that $\sigma(h_{i,j}) = h_{i,j+1 \pmod{d_i}}$.Then the polynomial

$$h = \prod_{i=1}^{k} \prod_{j \text{ odd}} h_{i,j}$$

is fixed by σ^2, has $\sigma(h) \neq h$, and $f = h\sigma(h)$. □

Lemma 6.0.12. *Let K be a local field, $f(x) \in K[x]$ a separable polynomial, E/K its splitting field and $G = \mathrm{Gal}(E/K)$. Let R be the set of roots of $f(x)$ in E, $V = \mathbb{C}[R]$ the corresponding complex permutation module,*

$$\mathfrak{f}(V) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \mathrm{codim} V^{G_i}$$

the Artin conductor exponent of V as a G-representation, and Δ the discriminant of $f(x)$. Then

$$\mathfrak{f}(V) \equiv v_K(\Delta) \pmod 2.$$

Proof. We may suppose that $f(x)$ is monic and integral. Indeed, $c \in K^\times$ be such that cr is integral for each $r \in R$. Then from the definition of the discriminant in terms of the roots of $f(x)$ we see that the polynomial $g(x) = \prod_{r \in R}(x - cr)$, which is monic and has coefficients in $\mathcal{O}_K$, has the same discriminant as $f(x)$ up to squares in $K^\times$, and the same permutation module up to isomorpism (of $\mathrm{Gal}(\bar{K}/K)$-modules).

Now let the disjoint orbits of G on R be denoted $S_1, ..., S_k$, corresponding to the factorisation of f as $f_1 ... f_k$ into irreducibles over K. Then V is a direct sum of the permutation modules $V_i = \mathbb{C}[S_i]$, and $\mathfrak{f}(V)$ is the sum of the $\mathfrak{f}(V_i)$. Let H_i be the stabiliser in G of a (arbitrarily chosen) root $x_i \in S_i$. Then $V_i \cong \mathbb{C}[G/H_i]$ and so by the conductor-discriminant formula [Ser79, VI.2 corollary to Proposition 4], $\mathfrak{f}(V_i) = v_K(\Delta_{E^{H_i}/K})$, where $\Delta_{E^{H_i}/K}$ denotes the discriminant of E^{H_i}/K. Now as a subfield of E we have $E^{H_i} = K(x_i)$ and consequently $v_K(\Delta_{E^{H_i}/K}) \equiv v_K(\Delta(f_i)) \pmod 2$. To see this, note that the ring $\mathcal{O}_K[x_i]$ has finite index inside $\mathcal{O}_{E^{H_i}}$ (note that $f(x)$ was assumed to be integral). The first ring has discriminant equal to the discriminant of $f_i(x)$ (or rather, its discriminant ideal is generated by the discriminant of $f_i(x)$). In particular, $v_K(\Delta_{E^{H_i}/K})$ is equal to $v_K(\Delta(f_i))$ up to squares in $K^\times$. Finally, since for polynomials h_1, h_2 we have $\Delta(h_1 h_2) = \Delta(h_1)\Delta(h_2)\mathrm{Res}(h_1, h_2)^2$, the discriminant of f is, up to squares in K, the product of the discriminants of the f_i (here $\mathrm{Res}(h_1, h_2)$ denotes the resultant of h_1 and h_2). □

Having established Proposition 6.0.10 we now seek to reinterpret the 'correction' term $\epsilon(f)$.

Lemma 6.0.13. *For any sufficiently large finite unramified extension F/K, and F'/F the unique unramified quadratic extension, we have $\epsilon(f) = 1$ if and only if the quadratic twist $C^{F'}/F$ of C by F' is deficient over F. In particular, $\epsilon(f) = \epsilon(C)$ as defined previously.*

Proof. The last paragraph of the proof of Lemma 6.0.11 applies equally well to the even genus case and shows that f either has an odd degree factor of K^{nr}, or factors into two conjugate, odd degree polynomials over the unique quadratic ramified extension of K^{nr} (since g is even, the polynomial h constructed there is forced to have odd degree). Thus also for every sufficiently large unramified extension F/K, f has an odd factorisation over a totally ramified quadratic extension of F. By enlarging F/K if necessary, we may also assume that the leading coefficient of f is a norm from this quadratic extension. The result now follows from Proposition 3.3.1. □

Corollary 6.0.14. *Let K be a local field of odd residue characteristic, let L/K be the unique quadratic unramified extension and C/K be a hyperelliptic curve. Then Conjecture 1 holds for C and L/K.*

Proof. Lemma 6.0.13 shows that $\epsilon(f) = \epsilon(C)$ and the result now follows from Proposition 6.0.10, Lemma 6.0.9 and Corollary 6.0.6. □

Remark 6.0.15. *If the genus of C is 2 then one can hope to establish (6.0.7), and hence additional cases of Conjecture 1, by using Liu's generalisation to genus 2 of Ogg's formula* [Liu94a, Theoreme 1]. *Indeed, by combining Theoreme 1, Theoreme 2 and Proposition 1 of loc. cit., one obtains, independently of the residue characteristic of K,*

$$f(J/K) \equiv v_K(\Delta_C) + n - 1 + \frac{d-1}{2} \pmod 2$$

where n is the number of irreducible components of $\mathcal{C}_{\bar{k}}$ ($\mathcal{C}$ is the minimal regular model of C over $\mathcal{O}_K$) and d is a more complicated expression involving the minimal regular model and is defined in the statement of Liu's Theoreme 1. In Section 5.2 of loc. cit., Liu computes the term $\frac{d-1}{2}$ in a large number of cases (but not all if the residue characteristic is 2) depending on the structure of $\mathcal{C}_{\bar{k}}$ (that is, on the 'type' of the special fibre as classified in [NU73] *and* [Ogg66]*). This includes all cases where C, or equivalently J, has semistable reduction and it is then easy to establish (6.0.7) for all semistable curves of genus 2 from*

the description, given by Liu in [Liu94b, Section 8]*, of the component group of a genus* 2 *curve in terms of its type. Thus Conjecture 1 holds for unramified quadratic extensions in residue characteristic* 2*, and semistable hyperelliptic curves of genus* 2*.*

Chapter 7

Ramified extensions

7.1 Ramified extensions; generalities

Let L/K be a ramified quadratic extension of nonarchimedean local fields where K has odd residue characteristic. We will now prove Conjecture 1 (with respect to L/K) when C is given by an equation of the form $y^2 = af(x)$ where $a \in K^\times$, $f(x) \in \mathcal{O}_K[x]$ is monic, and the reduction of f is cube free. By Lemma 2.1.7 we have

$$\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L) = \mathrm{ord}_2 \frac{c(J/K)c(J^L/K)}{c(J/L)}.$$

Moreover, the assumptions on f mean that C is semistable over K (see, for example, [Liu02, Example 10.3.29]). We begin by describing a method for computing the ratio $\frac{c(J/L)}{c(J/K)}$, at least up to squares, for general semistable curves and then apply it to our particular case. Secondly, we compute $c(J^L/K)$ (again up to squares) by analysing the minimal regular model of the quadratic twist C^L of C by L. Since C^L will no longer be semistable, we use results from Chapter 5 instead.

As we shall see, the terms of Conjecture 1 involving deficiency and root numbers will naturally appear as part of the forthcoming computations.

7.1.1 The minimal regular model of a semistable curve

Suppose C/K has semistable reduction over K and denote by $\mathcal{C}/\mathcal{O}_K$ its minimal proper regular model over $\mathcal{O}_K$, and by $\mathcal{C}_{\bar{k}}$ the special fibre of $\mathcal{C}$, base changed to $\bar{k}$. If $\mathcal{C}'$ denotes the minimal proper regular model of C over K^{nr}, then $\mathcal{C}_{\bar{k}}$ is the special fibre of $\mathcal{C}'$. The

following two paragraphs and Theorem 7.1.1 essentially summarise [Pap13, Section 3.4], to which we refer for more details. The only difference is that we wish to consider in addition the action of $\mathrm{Gal}(\bar{k}/k)$ on the objects involved.

The set S of singular points, and I of irreducible components, of $\mathcal{C}_{\bar{k}}$ both carry natural actions of $\mathrm{Gal}(\bar{k}/k)$ and we define the *dual graph* $\mathcal{G}$ of $\mathcal{C}_{\bar{k}}$ to be the graph whose vertices are the irreducible components of $\mathcal{C}_{\bar{k}}$ and such that $\Gamma_1, \Gamma_2 \in I$ are joined by one edge for each singular point of $\mathcal{C}_{\bar{k}}$ lying on both Γ_1 and Γ_2 (thus G may have both loops and multiple edges).

Associated to $\mathcal{G}$ we have an exact sequence (coming from simplicial homology)

$$0 \to H_1(\mathcal{G}, \mathbb{Z}) \longrightarrow \bigoplus_{x \in S} \mathbb{Z}[x] \xrightarrow{\partial} \bigoplus_{\Gamma \in I} \mathbb{Z}[\Gamma] \xrightarrow{\epsilon} \mathbb{Z} \to 0.$$

The map ϵ sends $\sum_{\Gamma \in I} n_\Gamma \Gamma$ to $\sum_{\Gamma \in I} n_\Gamma$. To define the map $\partial : \bigoplus_{x \in S} \mathbb{Z}[x] \to \bigoplus_{\Gamma \in I} \mathbb{Z}[\Gamma]$, we fix once and for all an orientation on the edges of $\mathcal{G}$. Then if $x \in S$ gives rise to an edge e of $\mathcal{G}$ from Γ_1 to Γ_2, we set $\partial(x) = \Gamma_2 - \Gamma_1$. Then $H_1(\mathcal{G}, \mathbb{Z})$, as defined by the exact sequence, is a free $\mathbb{Z}$-module of rank $\beta(\mathcal{G}) := |S| - |I| + 1$, which coincides with the toric rank of $\mathcal{C}$. We view $\bigoplus_{\Gamma \in I} \mathbb{Z}[\Gamma]$ as a $\mathrm{Gal}(\bar{k}/k)$-module by extending $\mathbb{Z}$-linearly the action of $\mathrm{Gal}(\bar{k}/k)$ on I. Moreover, we view $\bigoplus_{x \in S} \mathbb{Z}[x]$ as a $\mathrm{Gal}(\bar{k}/k)$-module in the same way, except we include $\pm$ signs to take account of the orientation of the edges. Thus the $\mathrm{Gal}(\bar{k}/k)$-action on I and S determines the action on $\bigoplus_{x \in S} \mathbb{Z}[x]$ save in the case where there are loops in the graph. To define the action here, note that each loop corresponds to a node lying on a single component. To each such singular point x we associate the two 'tangents' $t_x^{\pm}$ where we make a choice as to which tangent we associate the sign '+' to (here by tangents we mean the two points lying over x in the normalisation of this component). If $\sigma \in \mathrm{Gal}(\bar{k}/k)$ maps x to x', x' is also a node and σ maps the tangents $t_x^{\pm}$ at x onto the tangents $t_{x'}^{\pm}$ at x'. If t_x^+ is mapped by σ to $t_x'^+$ then we associate a '+' sign in the action on $\bigoplus_{x \in S} \mathbb{Z}[x]$, and associate a '-' sign otherwise. Whilst this depends on a choice of which tangent to identify which signs to, the resulting $\mathbb{Z}[\mathrm{Gal}(\bar{k}/k)]$-module structure on $\bigoplus_{x \in S} \mathbb{Z}[x]$ is well-defined up to isomorphism, and the same is true for the choice of orientation on the edges of $\mathcal{G}$. The exact sequence above then becomes $\mathrm{Gal}(\bar{k}/k)$-equivariant and $H_1(\mathcal{G}, \mathbb{Z})$ inherits a natural action of $\mathrm{Gal}(\bar{k}/k)$. Now define a pairing on $\bigoplus_{x \in S} \mathbb{Z}[x]$ by setting

$$\langle x, x' \rangle = \begin{cases} 1, & \text{if } x = x', \\ 0, & \text{else,} \end{cases}$$

and extending bilinearly. The restriction of this pairing to $H_1(\mathcal{G},\mathbb{Z})$ induces a $\mathbb{Z}$-valued symmetric non-degenerate $\mathrm{Gal}(\bar{k}/k)$-equivariant pairing on $H_1(\mathcal{G},\mathbb{Z})$. Denote by Λ the dual lattice of $H_1(\mathcal{G},\mathbb{Z})$ inside $H_1(\mathcal{G},\mathbb{Z})\otimes\mathbb{Q}$. We will henceforth denote $H_1(\mathcal{G},\mathbb{Z})$ by $\Lambda^\vee$. Note that $\Lambda^\vee\subseteq\Lambda$.

Theorem 7.1.1. *Let J/K be the Jacobian of C and $X(T)$ the character group of the toric part of the Raynaud parametrisation of J (see* [CFKS10, Section 2.10]*), so that $X(T)$ is a free $\mathbb{Z}$-module of rank equal to the toric rank of J. The $\mathbb{Z}$-module $X(T)$ carries a natural action of $\mathrm{Gal}(K^{\mathrm{nr}}/K)\cong\mathrm{Gal}(\bar{k}/k)$ and the monodromy pairing gives a symmetric, bilinear, non-degenerate pairing on $X(T)$. Then*

(i) $X(T)$ is isomorphic to $H_1(\mathcal{G},\mathbb{Z})$ as $\mathbb{Z}[\mathrm{Gal}(\bar{k}/k)]$-lattices equipped with a pairing.

(ii) If F/K it totally ramified of degree e, then $\Phi_F(\bar{k})$ is isomorphic to $\frac{\Lambda}{e\Lambda^\vee}$ as $\mathrm{Gal}(\bar{k}/k)$-modules.

(iii) Suppose J attains split semistable reduction over the (without loss of generality) unramified extension E/K (so that $\mathrm{Gal}(K^{nr}/K)$ acts on $H_1(\mathcal{G},\mathbb{Z})$ through $\mathrm{Gal}(E/K)$), let F/K be a Galois extension containing E and τ a complex representation of $\mathrm{Gal}(F/K)$. Then we have

$$w(J/K,\tau)=w(\tau)^{2g}(-1)^{\langle\tau,H_1(\mathcal{G},\mathbb{Z})\otimes\mathbb{C}\rangle}$$

where $w(J/K,\tau)$ denotes the root number of J/K twisted by τ, $w(\tau)$ denotes the root number of the representation τ of $Gal(F/K)$ and $\langle\ ,\ \rangle$ denotes the usual representation-theoretic inner product.

Proof. Part (i) follows from [Pap13, Theorem 3.8] and the references therein (see, in particular, [BLR90, Section 9.2]). For parts (ii) and (iii), see [DD09a, Section 3.v]. □

7.1.2 Computing the ratio $\frac{c(J/L)}{c(J/K)}$

Let $\Lambda^\vee$ and Λ be as in the previous section. By Theorem 7.1.1 we have

$$\frac{c(J/L)}{c(J/K)}=\frac{\left|\left(\frac{\Lambda}{2\Lambda^\vee}\right)^F\right|}{\left|\left(\frac{\Lambda}{\Lambda^\vee}\right)^F\right|},$$

where here F denotes the Frobenius automorphism viewed as a finite order endomorphism of the lattice Λ. Let $D = F - 1$ and $N = 1 + F + F^2 + ... + F^{n-1}$, where n is the order of F. Moreover, set $V = \Lambda \otimes \mathbb{Q}$, let G be the finite cyclic subgroup of $\mathrm{Aut}(\Lambda)$ generated by F, and define the group

$$\mathcal{B} = \mathcal{B}_{\Lambda,\Lambda^\vee} := \mathrm{im}\left(\mathrm{H}^1\left(G, \Lambda^\vee\right) \longrightarrow \mathrm{H}^1\left(G, \Lambda\right)\right).$$

The following Theorem is due to Betts and Dokchitser [BD14].

Theorem 7.1.2. *Let $e \geq 1$. Then we have*

$$\left|\left(\frac{\Lambda}{e\Lambda^\vee}\right)^F\right| = \left|\left(\frac{\Lambda}{\Lambda^\vee}\right)^F\right| \cdot |\mathcal{B}[e]| \cdot e^r$$

where $r := \mathrm{rk}\Lambda^F$.

Proof. The group $\mathcal{B}$ is introduced by Betts and Dokchitser in [BD14] (in part with the purpose of studying the ratio of Tamagawa numbers that we are also interested in). Whilst their definition of $\mathcal{B}$ is *a priori* different from ours, upon noting that, since V is uniquely divisible, $\mathrm{H}^1(G, V)$ is trivial whence $\ker(N|V) = \mathrm{im}(D|V)$, the equivalence with our definition is precisely given by cite[Lemma 2.3.6]BD2012. The statement of the theorem now follows immediately from [BD14, Theorem 1.1.1]. □

Corollary 7.1.3. *We have*

$$(-1)^{\mathrm{ord}_2 \frac{c(J/K)}{c(J/L)}} w(J/L) = (-1)^{\dim_{\mathbb{F}_2} \mathcal{B}[2]}.$$

Proof. Theorem 7.1.1 gives $w(J/L) = (-1)^r$ where r is $\mathrm{rk}\Lambda^F$. Now apply Theorem 7.1.2 with $e = 2$. □

The following lemma will be useful in the computation of the group $\mathcal{B}$.

Lemma 7.1.4. *Fix $r \geq 1$ and let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial dividing $x^r - 1$. Let G be a cyclic group of order r, generator σ, and suppose that G acts on the free $\mathbb{Z}$-module $\Lambda = \frac{\mathbb{Z}[x]}{(p(x))}$ with σ acting as multiplication by x. Then if $p(1) \neq 0$, $\mathrm{H}^1\left(G, \Lambda\right)$ is cyclic of order $p(1)$, whilst if $p(1) = 0$ it is trivial. Write $N = 1 + \sigma + ... + \sigma^{r-1}$ and $D = \sigma - 1$. Then $\ker(N|\Lambda)/\mathrm{im}(D|\Lambda)$ (which is isomorphic to $\mathrm{H}^1\left(G, \Lambda\right)$) is generated by $1 \in \mathbb{Z}[x]$.*

Proof. We have

$$\ker(N|\Lambda)/\mathrm{im}(D|\Lambda) = \frac{\ker(1+x+...+x^{r-1})}{\mathrm{im}(x-1)},$$

and it is clear that

$$\ker\left(1+x+...+x^{r-1}\right) = \frac{\frac{p(x)}{\gcd(p(x),1+x+...+x^{r-1})}\mathbb{Z}[x]}{p(x)\mathbb{Z}[x]}.$$

Since $p(x) \mid x^r - 1$, we have

$$\gcd(p(x), 1+x+...+x^{r-1}) = \begin{cases} p(x), & \text{if } p(1) \neq 0, \\ p(x)/(x-1), & \text{if } p(1) = 0. \end{cases}$$

Thus

$$\mathrm{H}^1(G,\Lambda) \cong \begin{cases} \frac{\mathbb{Z}[x]}{(x-1,p(x))} \cong \mathbb{Z}/p(1)\mathbb{Z}, & \text{if } p(1) \neq 0, \\ 0, & \text{if } p(1) = 0, \end{cases}$$

as desired. That $1 \in \mathbb{Z}[x]$ generates $\ker(N|\Lambda)/\mathrm{im}(D|\Lambda)$ is clear from the argument above. □

7.2 Ramified extensions; the case of cube free reduction

Let K be a non-archimedean local field with odd residue characteristic and let L/K be a ramified quadratic extension. Let C/K be a hyperelliptic curve. Recall that we wish to prove Conjecture 1 (with respect to L/K) when C is given by an equation of the form $y^2 = af(x)$ where $a \in K^\times$, $f(x) \in \mathcal{O}_K[x]$ is monic, and the reduction of f is cube free. By Lemma 3.1.2, it suffices to prove this after first twisting C by the extension L/K. Since the residue characteristic of K is odd, we may write $L = K(\sqrt{\pi_K})$ for some uniformiser π_K for K. Now write $a = u\pi_K^r$ where $r \in \mathbb{Z}$ and u is a unit in K. Twisting by L/K has the effect of multiplying the equation defining C by π_K, so we may assume that r is even. Absorbing even powers of π_K into the variable y, we may thus assume that a is a unit. We now apply the results of the previous section to compute the ratio $\frac{c(J/L)}{c(J/K)}$ (up to squares) in the case that C is given by an integral equation $y^2 = af(x)$ where a is a unit in K and f has cube free reduction. We will begin by fixing some notation. We assume henceforth the degree is even to ease notation. The odd degree case follows from an easy adaptation of the arguments of this section (in fact, it is substantially easier as, amongst other things,

deficiency never enters in this case).

The assumption on the reduction $\bar{f}(x)$ of $f(x)$ means that, over $\bar{k}$, we may write

$$\bar{f}(x) = \bar{u}\prod_{i=1}^{l}(x-\bar{u}_i)^2\prod_{j=l+1}^{2(g-l+1)}(x-\bar{w}_j)$$

where the $\bar{u}_i$ and $\bar{w}_j$ are all pairwise distinct. Since we may lift coprime factorisations over $\bar{k}$ to K^{nr} by Hensel's lemma, after completing the square of each (lifted) quadratic factor, we may factor $f(x)$ over K^{nr} as

$$f(x) = u\prod_{i=1}^{l}\left((x-u_i)^2 - v_i\pi_K^{n_i}\right)\prod_{j=l+1}^{2(g-l+1)}(x-w_j) \tag{7.2.1}$$

where π_K is a (henceforth fixed) choice of uniformiser for K, each $n_i \geq 1$, each u_i reduces to $\bar{u}_i$, each w_i reduces to $\bar{w}_i$ and each $v_i \in \mathcal{O}_{K^{\mathrm{nr}}}^{\times}$. For each double root $\bar{u}_i$ of $\bar{f}$, we associate the two 'tangents'

$$t_i^{\pm} = \pm\sqrt{g_i(\bar{u}_i)} \in \bar{k}$$

where

$$g_i(x) = \bar{u}\prod_{j\neq i}(x-\bar{u}_j)^2\prod_{j=l+1}^{2(g-l+1)}(x-\bar{w}_j) \in \bar{k}[x].$$

By convention, we choose the square roots so that, for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$, if $\sigma(\bar{u}_i) = \bar{u}_j$ and $i \neq j$, then $\sigma(t_i^+) = t_j^+$ (this is possible as $\mathrm{Gal}(\bar{k}/k)$ is procyclic).

The two schemes

$$U_1 = \mathrm{Spec}\frac{\mathcal{O}_K[x,y]}{(y^2 - f(x))}$$

and

$$U_2 = \mathrm{Spec}\frac{\mathcal{O}_K[u,v]}{(v^2 - h(u))}$$

where $h(u) = u^{2g+2}f(1/u)$ glue via the relations $x = 1/u$ and $y = x^{g+1}v$ to define a proper model $\mathcal{C}_0$ of C over $\mathcal{O}_K$. Moreover, the assumption on the reduction of $f(x)$ means that this model is semistable and, in fact, is the unique (up to isomorphism) stable model of C over $\mathcal{O}_K$ (see [Liu02, Example 10.3.29]). Now consider the base change, $\mathcal{C}_{0,K^{nr}}$, of $\mathcal{C}_0$ to $\mathcal{O}_{K^{nr}}$. The special fibre is smooth away from the singular points $(x,y) = (\bar{u}_i, 0)$. If every root of $\bar{f}$ is a double root (i.e. if $l = g+1$) then the special fibre consists of 2 irreducible components, intersecting in the $g+1$ points $(\bar{u}_i, 0)$. On the other hand, if $l < g+1$ so

that $\bar{f}$ has at least one single root, then the special fibre is irreducible, and each of the l-many points of the form $(\bar{u}_i, 0)$ is a node. The scheme $\mathcal{C}_{0,K^{nr}}$ is regular, save possibly at the singular points $(\bar{u}_i, 0)$ on the special fibre. In fact, these points are easily seen to be regular if and only if $n_i = 1$. To obtain a regular model of C (over $\mathcal{O}_{K^{nr}}$), one needs to blow up $(n_i - 1)$-times at each of the singular points, which serves to replace these points with a chain of $n_i - 1$ copies of $\mathbb{P}^1_{\bar{k}}$. This gives a regular model $\mathcal{C}_{K^{nr}}$ of C over $\mathcal{O}_{K^{nr}}$ which is easily seen to be the minimal regular model. Moreover, each of the copies of $\mathbb{P}^1_{\bar{k}}$ introduced has multiplicity 1 in the special fibre, self-intersection -2, and all their intersections with other irreducible components are transversal.

Since the form of the minimal proper regular model differs depending on whether or not each root of $\bar{f}$ is a double root, we now split into cases.

7.2.1 The case where $\bar{f}(x)$ has at least one single root

Keep the notation of the previous discussion, and suppose further that the reduction $\bar{f} \in k[x]$ of f has at least one single root in $\bar{k}$. If $\mathcal{C}$ denotes the minimal proper regular model of C over $\mathcal{O}_K$, and $\mathcal{C}_{\bar{k}}$ denotes its special fibre, base-changed to $\bar{k}$, then, as remarked previously, $\mathcal{C}_{\bar{k}}$ coincides with the special fibre of the minimal regular model of C over K^{nr}. Thus $\mathcal{C}_{\bar{k}}$ is as shown in Figure (7.1) below (in the figure, an 'n_1'-gon is to be interpreted as a node). The corresponding dual graph is shown in Figure (7.1) also. For what follows, we also label the edges of the dual graph.

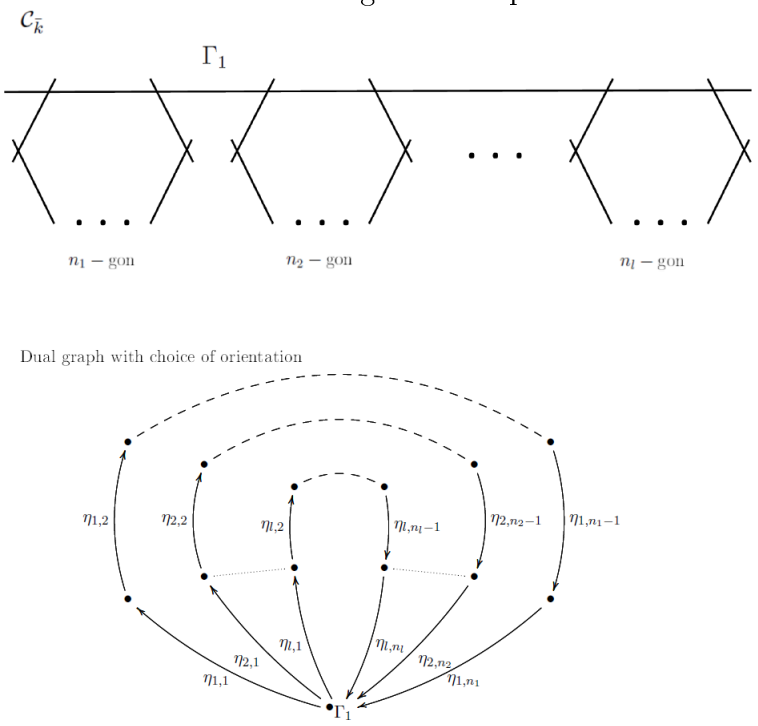
The elements $h_1 := \sum_{i=1}^{n_1} \eta_{1,i}, ..., h_l := \sum_{i=1}^{n_l} \eta_{l,i}$ form a $\mathbb{Z}$-basis for $\mathrm{H}_1(\mathcal{G}, \mathbb{Z})$. Moreover, the pairing on $\mathrm{H}_1(\mathcal{G}, \mathbb{Z})$ is given by

$$\langle h_i, h_j \rangle = \begin{cases} n_i, & \text{if } i = j, \\ 0, & \text{else.} \end{cases}$$

Now $\mathrm{Gal}(\bar{k}/k)$ acts on $H_1(\mathcal{G}, \mathbb{Z})$, and on the irreducible components of $\mathcal{C}_{\bar{k}}$, through a finite cyclic quotient, G say. In the notation of Section 7.1, we have $\Lambda = \bigoplus_{i=1}^{l} \mathbb{Z}\frac{1}{n_1} h_i$ and $\Lambda^\vee = \bigoplus_{i=1}^{l} \mathbb{Z} h_i$. Let $S_1, ..., S_m$ be the disjoint orbits of G on the h_i, n_i' be the common value of the n_j on S_i, and let $d_i = |S_i|$. Setting $\Lambda_i = \bigoplus_{h \in S_i} \mathbb{Z}\frac{1}{n_i'} h$ and $\Lambda_i^\vee = \bigoplus_{h \in S_i} \mathbb{Z} h$ (with signed G-action), we have

$$\mathcal{B} = \mathcal{B}_{\Lambda, \Lambda^\vee} = \bigoplus_{i=1}^{k} \mathcal{B}_{\Lambda_i, \Lambda_i^\vee}.$$

Figure 7.1: Special fibre and dual graph



Moreover, as $\mathbb{Z}[G]$-modules, either $\Lambda_i \cong \frac{\mathbb{Z}[x]}{(x^{d_i}-1)}$ or $\Lambda_i \cong \frac{\mathbb{Z}[x]}{(x^{d_i}+1)}$, with a chosen generator of G acting as multiplication by x. These $\mathbb{Z}[G]$-modules are non-isomorphic and in the first case we call the orbit S_i *split* and in the second we call S_i *non-split*. Noting that $\mathcal{B}_{\Lambda_i,\Lambda_i^\vee} = \mathcal{B}_{\Lambda_i,n_i'\Lambda_i}$ is just given by $n_i'\mathrm{H}^1(G,\Lambda_i)$, a simple application of Lemma 7.1.4 and Corollary 7.1.3 yields the following result.

Lemma 7.2.2. *Let r be the number of non-split orbits S_i for which n_i' is odd. Then we have $\mathcal{B} \cong (\mathbb{Z}/2\mathbb{Z})^r$. In particular, since by Remark 3.3.4 we have that C can never be deficient over K in this case, we have*

$$(-1)^{\mathrm{ord}_2 \frac{c(J/K)}{c(J/L)}} w(J/L) i_d(C) = (-1)^r.$$

Finally, we wish to describe the number of non-split orbits in terms of the explicit form of $f(x)$ given in (7.2.1). Now each h_i corresponds to the double root $\bar{u}_i$ of $\bar{f}(x)$ and it's clear that the *unsigned* action of G on S is identical to the action of $\mathrm{Gal}(\bar{k}/k)$ on the set $\mathcal{U} = \{\bar{u}_1, ..., \bar{u}_l\}$. Thus the total number of orbits of G on S is equal to the number of orbits of $\mathrm{Gal}(\bar{k}/k)$ on $\mathcal{U}$. Moreover, from the construction of the minimal proper regular model, one can determine if a given orbit is split or not by looking at the corresponding

tangents. Specifically, one sees that an orbit S_i containing h_j is split if and only if (either of the tangents) $t_j^{\pm}$ is in the field $k(\bar{u}_j)$ (*a priori* it is only in a quadratic extension of this field). This follows from the definition on the dual graph and [Liu02, Example 10.3.10]. One easily verifies that this does not depend on the choice of h_j in the orbit S_i. That is, we have the following restatement of Lemma 7.2.2.

Corollary 7.2.3. *Suppose $f(x)$ has at least one single root in $\bar{k}$. For each orbit O_i of $\mathrm{Gal}(\bar{k}/k)$ on the set $\mathcal{U} = \{\bar{u}_1, ..., \bar{u}_l\}$, pick $\bar{u}_i \in O_i$. Let r be the number of such orbits for which*

$$\bar{u}\prod_{j\neq i}(\bar{u}_i - \bar{u}_j)^2 \prod_{j=l+1}^{2(g-l+1)} (\bar{u}_i - \bar{w}_j)$$

is a non-square in $k(\bar{u}_i)$, and n_i is odd. Then

$$(-1)^{\mathrm{ord}_2 \frac{c(J/K)}{c(J/L)}} w(J/L) i_d(C) = (-1)^r.$$

7.2.2 The case where $\bar{f}(x)$ has $g+1$ distinct double roots

Suppose now that $\bar{f}(x)$ is a product of $g+1$ distinct double roots (over $\bar{k}$). Then now $\mathcal{C}_{\bar{k}}$ is as shown in Figure (7.2) below. As before, the corresponding dual graph, along with a choice of orientation on the edges, is also depicted.

Again, $\mathrm{Gal}(\bar{k}/k)$ acts on $H_1(\mathcal{G}, \mathbb{Z})$, and on the irreducible components of $\mathcal{C}_{\bar{k}}$, through a finite cyclic quotient, say G. We choose G such that, without loss of generality, G has order divisible by 2. Let $h_1 = \sum_{i=1}^{n_1} \eta_{1,i}, ..., h_l = \sum_{i=1}^{n_l} \eta_{l,i}$. The (signed) action of G on the $\eta_{i,j}$ gives $M := \bigoplus_{i=1}^{l} \mathbb{Z}h_i$ the structure of a G-module. Note that either Γ_1 and Γ_2 are both fixed by G, in which case G acts on the h_i by permutation, or else (any) generator σ for G maps Γ_1 to Γ_2 and then G acts on the h_i as the unsigned permutation, twisted by the unique order 2 character of G (thus G acts on the h_i by signed permutation, but unlike the previous case, the sign is controlled 'globally').

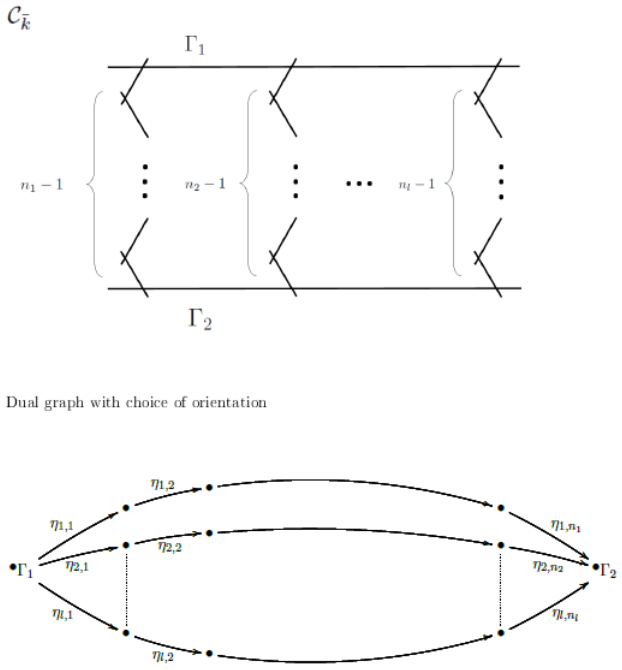
Now define a (non-degenerate, G-invariant) pairing on M by setting

$$\langle h_i, h_j \rangle = \begin{cases} n_i, & i = j, \\ 0, & \text{else.} \end{cases}$$

Then we have

$$\mathrm{H}_1(\mathcal{G}, \mathbb{Z}) = \ker\left(M \xrightarrow{\Sigma} \mathbb{Z}\right)$$

Figure 7.2: Special fibre and dual graph



with the pairing and G-action being that induced from those defined above on M (here Σ is the sum-map sending each h_i to 1 and extending linearly). Define Λ to be the dual lattice of $\mathrm{H}_1(\mathcal{G},\mathbb{Z})$ inside $\mathrm{H}_1(\mathcal{G},\mathbb{Z})\otimes\mathbb{Q}$, so that $\Lambda^\vee = \mathrm{H}_1(\mathcal{G},\mathbb{Z})$. Set $S = \{h_1,...,h_l\}$, endowed with unsigned G-action, so that G acts by permutation on S. Now S splits into G-orbits $S = S_1 \sqcup ... \sqcup S_m$ of sizes $d_1,...,d_m$. We write $S_i = \{h_{i,1},...,h_{i,d_i}\}$. If h_i and h_j are in the same orbit, S_t say, then we write n'_t for the common value of the n_t on this orbit.

We view M as a G-module with its signed action. As in Section 7.2.1, the dual lattice of M inside $M\otimes\mathbb{Q}$ is given by $M^\vee = \bigoplus_{i=1}^{l}\mathbb{Z}\frac{1}{n_i}h_i$. We identify this with M as a G-module in the obvious way so that the inclusion $M\to M^\vee$ corresponds to the map

$$\begin{array}{ccc} M & \longrightarrow & M \\ h_i & \mapsto & n_i h_i. \end{array}$$

We saw in Section 7.2.1 that the group $\mathcal{B}_{M^\vee,M}$ is easy to compute. Thus to compute $\mathcal{B}_{\Lambda,\Lambda^\vee}$ we wish to relate $\mathcal{B}_{\Lambda,\Lambda^\vee}$ to $\mathcal{B}_{M^\vee,M}$. We see in the following lemma that the difference between these two groups is controlled by whether or not C is deficient over K.

Lemma 7.2.4. *With the notation of the previous discussion, we have*

$$(-1)^{\dim_{\mathbb{F}_2}\mathcal{B}_{\Lambda,\Lambda^\vee}} = i_d(C)(-1)^{\dim_{\mathbb{F}_2}\mathcal{B}_{M^\vee,M}}.$$

(Implicit in this is the statement that $\mathcal{B}_{\Lambda,\Lambda^\vee}$ is in fact a $\mathbb{F}_2$-vector space; we already know that $\mathcal{B}_{M^\vee,M}$ is.)

Proof. We have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda^\vee & \longrightarrow & M & \xrightarrow{\Sigma} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle h_i \mapsto n_i h_i} & & & & \\ 0 & \longleftarrow & \Lambda & \longleftarrow & M & \longleftarrow & \mathbb{Z} & \longleftarrow & 0. \end{array} \tag{7.2.5}$$

Here the bottom row is the dual of the top, the map $\Lambda^\vee \to \Lambda$ is the natural inclusion and the map $\mathbb{Z} \to M$ on the bottom row is easily seen to take 1 to $\sum_{i=1}^{l} h_i$. This induces the following commutative diagram for group cohomology, again having exact rows

$$\begin{array}{ccccc} \mathrm{H}^1(G,\Lambda^\vee) & \xrightarrow{f} & \mathrm{H}^1(G,M) & \longrightarrow & \mathrm{H}^1(G,\mathbb{Z}) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle g} & & \\ \mathrm{H}^1(G,\Lambda) & \xleftarrow{h} & \mathrm{H}^1(G,M) & \longleftarrow & \mathrm{H}^1(G,\mathbb{Z}). \end{array}$$

(Here we define the action of G on $\mathbb{Z}$ so as to make the sequence G-equivariant.) By definition, we have

$$\mathcal{B}_{\Lambda,\Lambda^\vee} = \mathrm{im}(\phi) = \mathrm{im}(h \circ g \circ f)$$

whilst

$$\mathcal{B}_{M^\vee,M} = \mathrm{im}(g).$$

If both Γ_1 and Γ_2 are fixed by G then G acts on M by permutation and $\mathrm{H}^1(G,M) = 0$ (this follows from Shapiro's lemma). In particular, both $\mathcal{B}_{\Lambda,\Lambda^\vee}$ and $\mathcal{B}_{M^\vee,M}$ are trivial. Since moreover C is not deficient in this case, we are done.

In what follows, we will make some computations involving the cohomology of finite cyclic groups, the theory of which is detailed in [AW67, Section 8]. We recall that for any G-module A, the is an isomorphism $\mathrm{H}^1(G,A) \cong \ker(N|A)/\mathrm{im}(D|A)$ where $D = \sigma - 1$ for any generator σ of G, and $N = 1 + \sigma + ... + \sigma^{|G|-1}$. Moreover, given a homomorphism of G-modules $A \to A'$, we may fix the isomorphisms $\mathrm{H}^1(G,A) \cong \ker(N|A)/\mathrm{im}(D|A)$ and

$\mathrm{H}^1(G, A') \cong \ker(N|A)/\mathrm{im}(D|A')$ in such a way that the diagram

$$\begin{array}{ccc} H^1(G, A) & \longrightarrow & H^1(G, A') \\ \downarrow & & \downarrow \\ \ker(N|A)/\mathrm{im}(D|A) & \longrightarrow & \ker(N|A')/\mathrm{im}(D|A') \end{array}$$

commutes, where the vertical arrows are the chosen isomorphisms, the horizontal map on the top row is the natural map induced on cohomology from the map $A \to A'$, and the bottom horizontal map is induced similarly from the map $A \to A'$. For all G-modules A, we will think of $\mathrm{H}^1(G, A)$ as being the group $\ker(N|A)/\mathrm{im}(D|A)$ in what follows, noting that choosing compatible isomorphisms in the sense above allows us to be make this identification without worrying about the possible choices involved in doing this.

Suppose now that some (equivalently any) generator σ of G maps Γ_1 onto Γ_2. For each i, write M_i for the G-module $\bigoplus_{h \in S_i} \mathbb{Z}h$. Then one sees that for each i, as G-modules, we have (noncanonical) isomorphisms

$$M_i \cong \begin{cases} \frac{\mathbb{Z}[x]}{(x^{d_i}-1)} & d_i \text{ even} \\ \frac{\mathbb{Z}[x]}{(x^{d_i}+1)} & d_i \text{ odd} \end{cases}$$

where σ acts on the right as multiplication by x in both cases. Explicitly, one such isomorphism is given by sending $h_{i,1}$ to 1. Now Lemma 7.1.4 gives $\mathrm{H}^1(G, M_i) = 0$ if d_i is even, whilst if d_i is odd, we see that $\mathrm{H}^1(G, M_i) \cong \mathbb{Z}/2\mathbb{Z}$, and that $h_{i,1}$ generates $\mathrm{H}^1(G, M_i)$ in the sense that $h_{i,1} \in \ker(N|M_i)$ but $h_{i,1} \notin \ker(D|M_i)$. By symmetry, $h_{i,j}$ also generates $\mathrm{H}^1(G, M_i)$ for all j and hence, as d_i is odd and $\mathrm{H}^1(G, M_i)$ has a unique nontrivial element, so does $f_i := \sum_{i=1}^{d_i} h_{i,j}$. In conclusion,

$$\mathrm{H}^1(G, M_i) = \ker(N|M_i)/\mathrm{im}(D|M_i) = \mathbb{Z}f_i/2\mathbb{Z}f_i.$$

Clearly we have a G-module decomposition

$$M \cong \bigoplus_{i=1}^{k} M_i.$$

We therefore have

$$\mathrm{H}^1(G, M) = \bigoplus_{|S_i| \text{ odd}} \mathbb{Z}f_i/2\mathbb{Z}f_i.$$

Moreover, the sum map $\Sigma : M \to \mathbb{Z}$ and the corresponding map $\mathbb{Z} \to M$ obtained by taking duals, are G-equivariant if we endow $\mathbb{Z}$ with the action of G for which σ acts as multiplication by -1. With this action on $\mathbb{Z}$, we have

$$\mathrm{H}^1(G, \mathbb{Z}) = \ker(N|\mathbb{Z})/\mathrm{im}(D|\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}.$$

By exactness of the diagram (7.2.5), we obtain

$$f\left(\mathrm{H}^1(G, \Lambda^\vee)\right) = \ker\left(\bigoplus_{|S_i| \text{ odd}} \mathbb{Z}f_i/2\mathbb{Z}f_i \xrightarrow{\Sigma} \mathbb{Z}/2\mathbb{Z}\right).$$

Now the map $g : \bigoplus_{|S_i| \text{ odd}} \mathbb{Z}f_i/2\mathbb{Z}f_i \to \bigoplus_{|S_i| \text{ odd}} \mathbb{Z}f_i/2\mathbb{Z}f_i$ sends f_i to $n_i' f_i$. From this, one sees that $\mathrm{im}(g \circ f) = \mathrm{im}(g)$ unless n_i' is odd whenever $|S_i|$ is odd and there is at least one i with d_i odd. In this case $\mathrm{im}(g \circ f)$ has index two in $\mathrm{im}(g)$.

On the other hand, provided there is at least one i for which d_i is odd, we have

$$\ker(h) = \mathrm{im}\left(\mathrm{H}^1(G, \mathbb{Z}) \to \mathrm{H}^1(G, M)\right) = \mathbb{Z}/2\mathbb{Z},$$

with $\sum_{|S_i| \text{ odd}} f_i$ representing the unique nontrivial element.

We first deal with the expectional case where all d_i are even. Then the arguments above show that both $\mathcal{B}_{\Lambda,\Lambda^\vee}$ and $\mathcal{B}_{\Lambda,\Lambda^\vee}$ are trivial. Moreover, each d_i being even forces l, the total number of double roots, to be even. This means that the degree of $f(x)$ is divisible by four, and hence the genus g is odd. In particular, $i_d(C) = 1$ and we have the desired result.

Now suppose that there is some i for which d_i is odd. Then $\sum_{|S_i| \text{ odd}} f_i$ is in the image of g if and only if each n_i' is odd whenever $|S_i|$ is odd, in which case it is in the image of $g \circ f$ if and only if the number of odd-sized orbits on S is even. That is, if and only if $g = l - 1$ is odd.

Putting everything together, we have, providing there is an i for which d_i is odd,

$$\dim_{\mathbb{F}_2} \mathcal{B}_{\Lambda,\Lambda^\vee} = \begin{cases} \dim_{\mathbb{F}_2} \mathcal{B}_{M^\vee,M} - 2, & \text{if } \sigma(\Gamma_1) = \Gamma_2, \text{ each } n_i' \text{ odd whenever } |S_i| \text{ odd, } g \text{ odd,} \\ \dim_{\mathbb{F}_2} \mathcal{B}_{M^\vee,M} - 1, & \text{if } \sigma(\Gamma_1) = \Gamma_2, \text{ each } n_i' \text{ odd whenever } |S_i| \text{ odd, } g \text{ even,} \\ \dim_{\mathbb{F}_2} \mathcal{B}_{M^\vee,M}, & \text{else.} \end{cases}$$

To conclude, we must show that C is deficient over K if and only if g is even, $\sigma(\Gamma_1) = \Gamma_2$ and n_i' is odd whenever $|S_i|$ is. By Remark 3.3.4, C is deficient over K if and only if g is

even and each component of $\mathcal{C}_{\bar{k}}$ has an even length orbit under G. From Figure (7.2), we see that this happens precisely when g is even, $\sigma(\Gamma_1) = \Gamma_2$, and n_i' is odd (recall that the n_i' tell us the lengths of the chains of components appearing in Figure (7.2)). □

In the previous section, we called an orbit S_i of G on the set $\{h_1, ..., h_l\}$ split if the corresponding signed permutation module $\mathbb{Z}[S_i]$ was isomorphic to $\frac{\mathbb{Z}[x]}{(x^{d_i}-1)}$ and non-split otherwise. Now with the same convention applied here, every orbit is split if $\sigma(\Gamma_1) = \Gamma_1$, whilst the non-split orbits when $\sigma(\Gamma_1) = \Gamma_2$ are exactly those of odd size. An immediate corollary is then the following.

Corollary 7.2.6. *Define r to be the number of non-split orbits S_i for which n_i' is odd. Then*

$$(-1)^{ord_2 \frac{c(J/K)}{c(J/L)}} w(J/L) i_d(C) = (-1)^r.$$

Again, we wish to reinterpret the integer r in terms of the explicit form of $f(x)$ given in (7.2.1). First note that $\sigma(\Gamma_1) = \Gamma_1$ if and only if the (reduction of the) leading coefficient $\bar{u}$ is a square in k. Thus if $\bar{u}$ is a square in k then every orbit is split, whilst if u is a non-square in k then the even length orbits on S are split, whilst the odd length orbits are not. To prove this last assertion, note that the orbits on S correspond to the orbits of $\mathrm{Gal}(\bar{k}/k)$ on the set $\mathcal{U} = \{\bar{u}_1, ..., \bar{u}_l\}$ of double roots of $\bar{f}$. Since every root of $\bar{f}$ is a double root, I claim that each tangent $t_i^{\pm}$ is a square in $k(\bar{u}_i)$ if and only if $\bar{u}$ is a square in $k(\bar{u}_i)$. Indeed, over $k(\bar{u}_i)$, $\bar{f}(x)$ factors as $\bar{f}(x) = \bar{u}(x - \bar{u}_i)^2 g(x)$ for some polynomial $g(x) \in k(\bar{u}_i)[x]$ all of whose roots are double roots over $\bar{k}$. Thus $g(x)$ is actually the square of a polynomial in $k(\bar{u}_i)[x]$, from which the claim follows. Moreover, $\bar{u}$ is a square in $k(\bar{u}_i)$ is and only if the $\mathrm{Gal}(\bar{k}/k)$-orbit of $\bar{u}_i$ is even in length, as this is precisely the condition that $k(\bar{u}_i)$ contain $k(\bar{u})$. Thus we see that the description of r in terms of (7.2.1) exactly the same as in the previous case. Specifically, we have the following Corollary.

Corollary 7.2.7. *Suppose $f(x)$ has $g+1$ distinct double roots in $\bar{k}$. For each orbit O_i of $\mathrm{Gal}(\bar{k}/k)$ on the set $\mathcal{U} = \{\bar{u}_1, ..., \bar{u}_l\}$ pick $\bar{u}_i \in O_i$. Let r be the number of such orbits for which*

$$\bar{u} \prod_{j \neq i} (\bar{u}_i - \bar{u}_j)^2 \prod_{j=l+1}^{2(g-l+1)} (\bar{u}_i - \bar{w}_j)$$

is a non-square in $k(\bar{u}_i)$ and n_i is odd. Then

$$(-1)^{\mathrm{ord}_2 \frac{c(J/K)}{c(J/L)}} w(J/L) i_d(C) = (-1)^r.$$

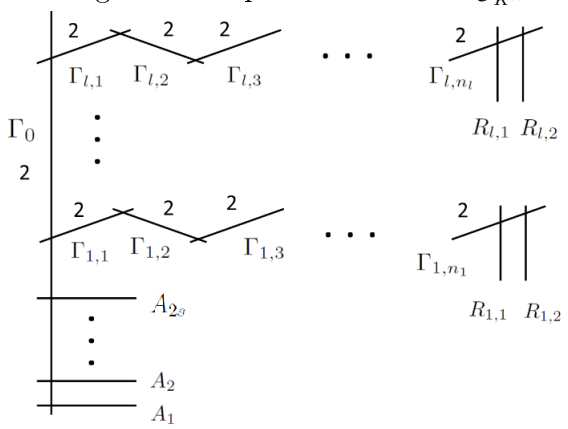
7.2.3 Computing $c(J^L/K)$

Fix a uniformiser π_K in K such that $L = K(\sqrt{\pi_K})$. Then C^L is given by the equation

$$C^L : y^2 = \pi_K f(x) = u\pi_K \prod_{i=1}^{l} \left((x-u_i)^2 - v_i \pi_K^{n_i}\right) \prod_{j=l+1}^{2(g-l+1)} (x - w_j). \tag{7.2.8}$$

Recall that each $n_i \geq 1$. Since the equation defining C^L above, and the corresponding one for the chart at infinity, are integral, they define a proper model of C^L over $\mathcal{O}_K$ in the obvious way. Let $\mathcal{C}^L_{0,K^{nr}}$ be the base change of this model to $\mathcal{O}_{K^{nr}}$. Its special fibre consists of one irreducible component having multiplicity 2 in the special fibre. Call this component Γ_0. We now perform the necessary blow-ups to obtain the minimal proper regular model. The procedure is (an easy generalisation of) the proof of steps 6 and 7 of Tate's algorithm as described in [Sil94, IV.9]. We do all computations over K^{nr} and keep track of the action of $\mathrm{Gal}(K^{nr}/K)$. The result is that the special fibre of the minimal proper regular model $\mathcal{C}^L$ of C^L, after base changing to $\bar{k}$, has the form given in Figure (7.3), where we set $s = g + 1 - l$ (the number of single roots of the reduction of $f(x)$). Here the numbers in the picture indicate the multiplicity of the components in the special fibre. If no number is given the multiplicity is 1. Moreover, all intersections between components are transversal.

Figure 7.3: Special fibre of $\mathcal{C}^{\mathcal{L}}{}_{\mathcal{O}_{K^{nr}}}$



We now perform the blow-ups to verify this.

The non-regular points of $\mathcal{C}^L_{0,K^{nr}}$ are precisely those points $(x, y) = (\alpha, 0)$ on the special fibre, for α a root of $f(x)$. In particular, all points which are only seen in the chart at infinity are regular, and we need not worry about this chart. We now blow up along the

component Γ_0. To do this, we set $x = x_1$ and $y = \pi_K y_1$ and divide the resulting equation by π_k to obtain the scheme $\mathcal{V}_0$ given by the vanishing of

$$\pi_K y_1^2 = u \prod_{i=1}^{l} \left((x_1 - u_i)^2 - v_i \pi_K^{n_i} \right) \prod_{j=l+1}^{2(g-l+1)} (x_1 - w_j).$$

Our model now consists of $\mathcal{C}^L_{0,K^{nr}}$ and the scheme $\mathcal{V}_0$, glued in the obvious way. The special fibre consists of the component Γ_0, of multiplicity 2, along with the reduction $\tilde{\mathcal{V}_0}$, which is given by the equation $\bar{f}(x_1) = 0$. Thus the special fibre consisits of Γ_0, along with a copy of $\mathbb{P}^1_{\bar{k}}$ with muliplicity one for each single root of $\bar{f}$, and a copy of $\mathbb{P}^1_{\bar{k}}$ with multiplicity two in the special fibre for each double root of $\bar{f}$. The $\mathrm{Gal}(\bar{k}/k)$-action on the special fibre is to fix Γ_0 and act on the remaining components accoring to the action on the roots of $\bar{f}$. If $\bar{f}$ has no double roots then this model is already regular (and is also minimal). On the other hand, if $\bar{f}$ has double roots, we proceed by blowing up along the multiplicity two components corresponding to double roots. In either case, the single roots contribute the components $A_1, ..., A_2 s$ in Figure (7.3). We first blow up along the component corresponding to the double root $\bar{u}_1$ of $\bar{f}(x)$. First shift this root so it is at $x_1 = 0$. Then $\mathcal{V}_0$ is now given by the equation

$$\pi_K y_1^2 = u(x_1^2 - v_i \pi_K^{n_1}) \prod_{i=2}^{l} \left((x_1 + u_1 - u_i)^2 - v_i \pi_K^{n_i} \right) \prod_{j=l+1}^{2(g-l+1)} (x_1 + u_1 - w_j).$$

We now blow up along the double line at $x_1 = 0$ on the special fibre (which is $\Gamma_{1,1}$ in Figure (7.3)). To do this, we replace x_1 by $\pi_K x_2$, and y_1 with y_2, and divide the equation by π_K, resulting in the scheme $\mathcal{V}_{1,1}$ which has equation

$$y_2^2 = u(\pi_K x_2^2 - v_1 \pi_K^{n_1 - 1}) \prod_{i=2}^{l} \left((\pi_K x_2 + u_1 - u_i)^2 - v_i \pi_K^{n_i} \right) \prod_{j=l+1}^{2(g-l+1)} (\pi_K x_2 + u_1 - w_j).$$

We have two possibilities for the reduction modulo π_K of $\mathcal{V}_{1,1}$. The first case is when $n_1 = 1$. Then the reduction $\tilde{\mathcal{V}_{1,1}}$ has equation

$$y_2^2 = -\bar{u}\bar{v_1} \prod_{i=2}^{l} (\bar{u_1} - \bar{u_i})^2 \prod_{j=l+1}^{2(g-l+1)} (\bar{u}_1 - \bar{w}_j) = -\bar{v_1}(t_1^{\pm})^2.$$

This consists of two copies of $\mathbb{P}^1_{\bar{k}}$, each appearing with multiplicity one. These are the

components $R_{1,1}$ and $R_{1,2}$ in Figure (7.3). They are fixed or swapped by $\mathrm{Gal}\left(\bar{k}/k(\bar{u}_1)\right)$ according to whether or not $-\bar{v}_1(t_1^{\pm})^2$ is a square in $k(\bar{u}_1)$ or not. The second case is when $n_1 > 1$. Then the reduction of $\tilde{\mathcal{V}}_1$ has equation

$$y_2^2 = 0$$

which contributes a double line to the special fibre. This is the component $\Gamma_{1,2}$ in Figure (7.3). If we are in this case, we proceed by blowing up along this component. This is now done by replacing y_2 by $\pi_K y_3$, x_2 by x_3 and dividing by π_K. We obtain the scheme $\mathcal{V}_{1,2}$ which has equation

$$\pi_K y_3^2 = u(x_3^2 - v_1\pi_K^{n_1-1})\prod_{i=2}^{l}\left((\pi_K x_3 + u_1 - u_i)^2 - v_i\pi_K^{n_i}\right)\prod_{j=l+1}^{2(g-l+1)}(\pi_K x_3 + u_1 - w_j).$$

Again, we have two cases. If $n_1 = 2$ then the reduction of $\mathcal{V}_{1,2}$ has equation

$$0 = \bar{u}(x_3^2 - \bar{v}_1)\prod_{i=2}^{l}(\bar{u}_1 - \bar{u}_i)^2\prod_{j=l+1}^{2(g-l+1)}(\bar{u}_1 - \bar{w}_j) = (t_1^{\pm})^2(x_3^2 - \bar{v}_1).$$

Then consists of two lines of multiplicity one, which are fixed or swapped by $\mathrm{Gal}\left(\bar{k}/k(\bar{u}_1)\right)$ according to whether or not $\bar{v}_1$ is a square in $k(\bar{u}_1)$ or not. These two lines correspond to the components $R_{1,1}$ and $R_{1,2}$ in Figure (7.3). On the other hand, if $n_1 > 2$, then the reduction of $\mathcal{V}_2$ has equation

$$0 = (t_1^{\pm})^2 x_3^2$$

which is a line of multiplicity two. This is the component $\Gamma_{1,3}$ in Figure (7.3). As usual, we then blow up along this component.

Continuing the process above, we define schemes $\mathcal{V}_{1,1},...,\mathcal{V}_{1,n_1-1}$ and obtain the components $\Gamma_{1,1},...,\Gamma_{1,n_1}$ and $R_{1,1}$ and $R_{1,2}$ of the special fibre shown in Figure (7.3). We see that each $\Gamma_{1,i}$ appears with multiplicity two, whilst $R_{1,1}$ and $R_{1,2}$ appear with multiplicity one. Moreover, if n_1 is odd then $R_{1,1}$ and $R_{1,2}$ are fixed or swapped by $\mathrm{Gal}\left(\bar{k}/k(\bar{u}_1)\right)$ according to whether or not $-\bar{v}_1(t_1^{\pm})^2$ is a square in $k(\bar{u}_1)$ or not, whilst if n_1 is even, then $R_{1,1}$ and $R_{1,2}$ are fixed or swapped by $\mathrm{Gal}\left(\bar{k}/k(\bar{u}_1)\right)$ according to whether or not $\bar{v}_1$ is a square in $k(\bar{u}_1)$ or not.

We are now done with the components corresponding to the root $\bar{u}_1$. We now shift so that the root $\bar{u}_2$ is at 0, and repeat the process above with u_1 replaced by u_2. We then do

this process for each of $u_3, ..., u_l$ in turn. At the end of this, our model is then the minimal proper regular model of C^L over $\mathcal{O}_{K^{\mathrm{nr}}}$ and we see that it is indeed given by that shown in Figure (7.3). Moreover, we have determined the action of $\mathrm{Gal}(\bar{k}/k)$ on the components of the special fibre.

We now wish to compute the Tamagawa number $c(J^L/K) = \Phi(k)$. In fact, we need only compute $(-1)^{\mathrm{ord}_2 c(J^L/K)}$ and this will prove easier to compute thanks to the results of Chapter 5. Now $\mathrm{Gal}(\bar{k}/k)$ acts on the components of $\mathcal{C}^L_{\bar{k}}$ through a finite cyclic quotient G. Fix a generator σ of G. Then G acts on the set $S = \{\Gamma_{i,1} \ : \ 1 \leq i \leq l\}$ by permutation (this follows by symmetry, and the assumption that $g \geq 2$). Moreover, on each orbit on S, the corresponding value of n_i is constant. Suppose $O = \{\Gamma_{i_1,1}, ..., \Gamma_{i_r,1}\}$ is an orbit, and that σ acts as the cycle $(\Gamma_{i_1,1} \ ... \ \Gamma_{i_r,1})$ on this. Then we have two possibilities. Either (after relabeling if necessary), $\{R_{i_1,1}, ..., R_{i_r,1}\}$ and $\{R_{i_1,2}, ..., R_{i_r,2}\}$ are two G-orbits of length r with σ acting as the obvious r-cycle on each, or $\{R_{i_1,1}, ..., R_{i_r,1}, R_{i_1,2}, ..., R_{i_r,2}\}$ is an orbit of length $2r$ and σ cycles the $2r$ elements of this orbit in the order they are written. In the first case, we call the orbit O *small*, and in the second we call it *large*. Finally, let $\mathcal{W}$ be the set of components $\{A_1, ..., A_{2s}\}$, along with the natural action of G.

Lemma 7.2.9. *Keeping the notation of the previous paragraph, we have*

$$(-1)^{\mathrm{ord}_2 c\left(J^L/K\right)} i_d(C^L) = (-1)^{\#\textit{orbits on } \mathcal{W} + \#\textit{large orbits on } S}.$$

Proof. We will compute the quantity $(-1)^{\mathrm{ord}_2 c\left(J^L/K\right)} i_d(C^L)$ in two stages. We first compute the order of the $\bar{k}$-points in the component group Φ^L of C^L (i.e. we compute $|\Phi^L(\bar{k})|$) using [BLR90, Proposition 9.6.6], which applies in much greater generality. Secondly, we compute the quantity

$$(-1)^{\mathrm{ord}_2 \frac{|\Phi^L(\bar{k})|}{|\Phi^L(k)|}} i_d(C^L)$$

by an application of Proposition 5.2.5.

Let Y be the graph associated to $\mathcal{C}^L_{\bar{k}}$ by taking the vertices to be the irreducible components, and joining two distinct vertices by a single edge if the corresponding components have non-trivial intersection number. It is clear that Y is a tree. Moreover, the intersection number of any two distinct components is either 0 or 1 (as seen from the construction preceeding this lemma), and the greatest common divisor of the multiplicities of the components is 1. Let I denote the set of all irreducible components of $\mathcal{C}^L_{\bar{k}}$, and for each component $\Gamma \in I$ let $d(\Gamma)$ denote the multiplicity of Γ in $\mathcal{C}_{\bar{k}}$, and $s(\Gamma)$ be the number of components

(distinct from Γ) that meet Γ. Then [BLR90, Proposition 9.6.6] gives

$$|\Phi^L(\bar{k})| = \prod_{i\in I} d(\Gamma)^{s(\Gamma)-2} = 2^{2k+2l-2} = 2^{2g}.$$

In particular, we see that $\mathrm{ord}_2|\Phi^L(\bar{k})|$ is even and we now wish to show that

$$(-1)^{\mathrm{ord}_2 \frac{|\Phi^L(\bar{k})|}{|\Phi^L(k)|} i_d(C^L)} = (-1)^{\#\text{orbits on } \mathcal{W} + \#\text{large orbits on } S}.$$

Let $O_1, ..., O_t$ be the even sized orbits of $\mathrm{Gal}(\bar{k}/k)$ on I, let $r_i = |O_i|$ and for each $1 \leq i \leq t$, write

$$\epsilon_i = \sum_{i=0}^{r_i - 1} (-1)^i \sigma^i(\Gamma^{(i)})$$

where σ generates G (we can take σ to be the Frobenius element in G) and $\Gamma^{(i)}$ is a representative of the orbit O_i. Then Proposition 5.2.5 gives

$$(-1)^{\mathrm{ord}_2 \frac{|\Phi^L(\bar{k})|}{|\Phi^L(k)|} i_d(C^L)} = (-1)^{\mathrm{ord}_2 |\det(\frac{1}{r_j}\langle \epsilon_i, \epsilon_j \rangle_{i,j}|}.$$

Now the matrix $A = (\frac{1}{r_j}\langle \epsilon_i, \epsilon_j \rangle_{i,j}$ is block diagonal, with a block corresponding to each even sized orbit on $\mathcal{W}$, and a block corresponding to each orbit of S, save for the odd sized small orbits on S which do not contribute. From this, one sees immediately that each even sized orbit on $\mathcal{W}$ contributes a factor of -2 to the determinant of A, as does each odd sized large orbit on S. The contribution from each small even orbit on S is λ_n where n is the common value of the n_i on the orbit, and λ_r denotes the determinant of the $r+2$ by $r+2$ matrix

$$\begin{pmatrix}
-2 & 1 & & & & & & \\
1 & -2 & & & & & & \\
 & 1 & & & & & & \\
 & & \ddots & 1 & & & & \\
 & & & -2 & 1 & & & \\
 & & & 1 & -2 & 1 & 1 \\
 & & & & 1 & -2 & 0 \\
 & & & & 1 & 0 & -2
\end{pmatrix}.$$

(Some of the 1's appearing in this matrix could become -1's had we chosen the labelling of the components of $\mathcal{C}^L_{\bar{k}}$ in a less compatible way. However, there is clearly a choice

of labelling for which the matrix does have the form shown above, and the determinant will be independent of the choice.) Noting that λ_r satisfies the recurrence relation $\lambda_r = -2\lambda_{r-1} - \lambda_{r-2}$, we obtain $\lambda_r = (-1)^r \cdot 4$. For the large even orbits, the contribution is the determinant of the $n+1$ by $n+1$ matrix (with n as above)

$$\begin{pmatrix} -2 & 1 & & & & & \\ 1 & -2 & & & & & \\ & 1 & & & & & \\ & & \ddots & 1 & & & \\ & & & -2 & 1 & & \\ & & & 1 & -2 & 1 & \\ & & & & 2 & -2 \end{pmatrix}.$$

This may be treated similarly to the previous case, and we obtain a contribution of $(-1)^n \cdot 2$.

In total, we have

$$(-1)^{\mathrm{ord}_2 \frac{|\Phi(\bar{k})|}{|\Phi(k)|} i_d(C^L)} = (-1)^{\#\text{even sized orbits on } \mathcal{W} + \#\text{large orbits on } S}.$$

Finally, we conclude by noting that, as $|\mathcal{W}|$ is even, the number of even sized orbits on $\mathcal{W}$ is congruent modulo 2 to the total number of orbits on $\mathcal{W}$. □

We now seek to describe the number of orbits on $\mathcal{W}$ and the number of large orbits of S in terms of the explicit equation for C^L given in (7.2.8). From the construction of the minimal proper regular model, one sees that the set $\{A_1, ..., A_{2s}\}$ corresponds exactly (as a set with $\mathrm{Gal}(\bar{k}/k)$-action) to the set $\{\bar{w}_{l+1}, ..., \bar{w}_{2(g-l+1)}\}$ of single roots of $\bar{f}(x)$. Thus the number of orbits on these two sets coincide. Moreover, one sees that the orbits on S correspond similarly to the orbits on $\{\bar{u}_1, ..., \bar{u}_l\}$. Finally, one sees from the discussion preceeding Lemma 7.2.9 that an orbit, corresponding to the orbit of $\bar{u}_i$ say, is large if and only if the product $-\bar{v}_i(t_i^{\pm})^2$ is a non-square in $k(\bar{u}_i)$ if n_i is odd, and if and only if $\bar{v}_i$ alone is a non-square in $k(\bar{u}_i)$ if n_i is even (compare also with the formula for $\tilde{\mathcal{V}}_n$ in step 7 of Tate's algorithm in [Sil94, page 374]).

We may now put everything together to prove Conjecture 1 in this case.

Corollary 7.2.10. *Let K be a non-archimedean local field with odd residue characteristic. Let C/K be a hyperelliptic curve given by the equation $y^2 = f(x)$ and L/K be a ramified quadratic extension and suppose that $f(x)$ has unit leading coefficient and that the reduction*

of $f(x)$ is cube free. Then Conjecture 1 holds for C and the extension L/K.

Proof. We are assuming that C, over K^{nr}, is given by an equation of the form

$$C : y^2 = f(x) := u \prod_{i=1}^{l} \left((x - u_i)^2 - v_i \pi_K^{n_i} \right) \prod_{j=l+1}^{2(g-l+1)} (x - w_j) \tag{7.2.11}$$

where the reduction $\bar{u}_i$ and $\bar{w}_j$ are all pairwise distinct and, without loss of generality, the uniformiser π_K is chosen such that $L = K(\sqrt{\pi_K})$.

Let $\mathcal{U}$ be the $\mathrm{Gal}(\bar{k}/k)$-set

$$\mathcal{U} = \{\bar{u}_1, ..., \bar{u}_l\},$$

let $O_1, ..., O_t$ be the disjoint orbits on $\mathcal{U}$, and for each orbit O_i, fix $\bar{u}_i \in O_i$, along with associated v_i, and set

$$t_i' := \bar{u} \prod_{j \neq i} (\bar{u}_i - \bar{u}_j)^2 \prod_{j=l+1}^{2(g-l+1)} (\bar{u}_i - \bar{w}_j)$$

(so that t_i' is the square of the tangents $t_i^{\pm}$ defined previously). For each orbit O_i, let n_i' be the common value of the n_j in (7.2.11) associated to the $u_j \in O_i$. Moreover, let $\mathcal{W}$ be the $\mathrm{Gal}(\bar{k}/k)$-set

$$\mathcal{W} = \left\{ \bar{w}_{l+1}, ..., \bar{w}_{2(g-l+1)} \right\}.$$

Finally, for a finite field $\mathbb{F}$ of odd characteristic, let $\rho_{\mathbb{F}} : \mathbb{F}^{\times} \to \{\pm 1\}$ be the homomorphism whose kernel consists of the squares in $\mathbb{F}^{\times}$.

By Corollaries 7.2.3 and 7.2.7, we have

$$(-1)^{\mathrm{ord}_2 \frac{c(J/K)}{c(J/L)}} w(J/L) i_d(C) = \prod_{\substack{i=1 \\ n_i' \text{ odd}}}^{t} \rho_{k(\bar{u}_i)}(t_i').$$

Moreover, by Lemma 7.2.9 (in conjunction with the discussion following this lema), we have

$$(-1)^{\mathrm{ord}_2 c(J^L/K)} i_d(C^L) = (-1)^{\#\text{orbits on } \mathcal{W}} \times \prod_{\substack{i=1 \\ n_i' \text{ odd}}}^{t} \rho_{k(\bar{u}_i)} \left((-1)^{n_i'} \bar{v}_i t_i' \right) \prod_{\substack{i=1 \\ n_i' \text{ even}}}^{t} \rho_{k(\bar{u}_i)} \left((-1)^{n_i'} \bar{v}_i \right).$$

As each $\rho_{k(\bar{u}_i)}$ is a homomorphism, to complete the proof we must show that

$$(\Delta_C, L/K) = (-1)^{\#\text{orbits on } \mathcal{W}} \times \prod_{i=1}^{t} \rho_{k(\bar{u}_i)} \left((-1)^{n'_i} \bar{v}_i \right).$$

To see this, observe that, as $-\pi_K$ is a norm from L, $(\Delta_C, L/K) = 1$ if and only if Δ_C is a square in $F = K(\sqrt{-\pi_K})$. Moreover, it is clear from (7.2.11) that all roots of $f(x)$ lie in $F^{\mathrm{nr}} = FK^{\mathrm{nr}}$. Thus $\mathrm{Gal}(F^{\mathrm{nr}}/F)$ acts on the roots of $f(x)$ and letting $\sigma \in \mathrm{Gal}(F^{\mathrm{nr}}/F)$ denote the Frobenius element, we deduce that $(\Delta_C, L/K)$ is equal to the sign of σ as a permutation on the roots of $f(x)$. Now the roots of $f(x)$ in $\bar{K}$ are

$$\left\{ u_i \pm \sqrt{(-1)^{n_i} v_i} \cdot \sqrt{(-\pi_K)^{n_i}} \ : \ 1 \leq i \leq l \right\} \cup \{ w_j \ : \ l+1 \leq j \leq 2(g-l+1) \}.$$

Since $\sqrt{(-\pi_K)^{n_i}} \in F$ for each i, the action of σ on these roots is the same as the action of the Frobenius element in $\mathrm{Gal}(\bar{k}/k)$ on the set

$$\left\{ \bar{u}_i \pm \sqrt{(-1)^{n_i} \bar{v}_i} \right\} \cup \mathcal{W}$$

and the result now follows easily. □

Chapter 8

Residue characteristic 2

In this chapter we consider Conjecture 1 over non-archimedean local fields of characerisitc 0 and residue characteristic 2. That is, over finite extensions of $\mathbb{Q}_2$. The reason we exclude the equal characteristic 2 case is that we wish to use the result [Fon85, Théorème A] of Fontaine, which does not include this case. The residue characteristic being 2 results in the the norm map and root numbers becoming considerably more complicated and we will only say anything in the case of good reduction of the Jacobian, and will impose additional assumptions when the quadratic extension is ramified.

8.1 Unramified extensions

Suppose that L/K is an unramified quadratic extension of nonarchimedean local fields. We are interested in the case where K has characteristic zero and residue characteristic two, but this is unecessarily restrictive for the arguments. Let C/K by a hyperelliptic curve and suppose that the Jacobian J/K of C has good reduction over K. The result of Mazur [Maz72, Corollary 4.4] used in the proof of Lemma 4.1.3 did not in fact assume that the residue characteristic of K was odd. In particular, we still have $|J(K)/N_{L/K}J(L)| = 1$ and moreover $w(J/L) = 1$. Since L/K is unramified, the quadratic twist J^L of J also has good reduction. To verify Conjecture 1 we must prove that $(\Delta_C, L/K)i_d(C)i_d(C^L) = 1$. We will show that, when K has characteristic not 2, that both $(\Delta_C, L/K)$ and $i_d(C)i_d(C^L)$ are equal to 1 individually. That the first of these quantities is, is the result of the next proposition, which may be of independent interest.

Proposition 8.1.1. *Let K be a nonarchimedean local field of characteristic different from two. Let C/K be a hyperelliptic curve over K whose Jacobian J has good reduction over*

K. Then the discriminant Δ_C of any Weierstrass equation for C has even valuation. In particular, for L/K the unique unramified quadratic extension of K, $(\Delta_C, L/K) = (-1)^{v_K(\Delta_C)} = 1$.

Proof. Assume first that the residue characteristic of K is odd. Then $J[2]$ is unramified and hence Δ_C is a square in K^{nr}, thus has even valuation. Now suppose that K has characteristic zero, but residue characteristic two. Let $\mathcal{J}/\mathcal{O}_K$ be the Néron model of J. The assumption that J has good reduction over K implies that $\mathcal{J}[2]$ is a finite flat group scheme over $\mathcal{O}_K$ [Mil86, Proposition 20.7]. Letting e denote the absolute ramification index of K, it is a theorem of Fontaine that G_K^u acts trivially on $\mathcal{J}[2](\bar{K}) = J[2]$ provided $u > 2e-1$ [Fon85, Théorème A] (here G_K is the absolute Galois group of K). Note that we are using Serre's upper numbering for the higher ramification groups. Let $L = K\left(\sqrt{\Delta_C}\right)$ and $G = \mathrm{Gal}(L/K)$. By Herbrand's theorem (see, for example, [Ser79, IV, Lemma 3.5]), G^u is trivial for $u \geq 2e$. In particular, the conductor $\mathfrak{f}(L/K)$ satisfies $\mathfrak{f}(L/K) \leq 2e$. On the other hand, supposing $v_K(\Delta_C)$ is odd, we have $L = K\left(\sqrt{\pi_K}\right)$ for some uniformiser π_K of K. Letting σ be the non-trivial element of G, we obtain

$$v_L\left(\sigma\left(\sqrt{\pi_K}\right) - \sqrt{\pi_K}\right) = v_L(2) + 1 = 2e + 1,$$

whence $\mathfrak{f}(L/K) = 2e + 1$, a contradiction. □

Lemma 8.1.2. *Suppose J has good reduction over K and let L/K be the unique quadratic unramified extension. Then C is deficient over K if and only if its quadratic twist C^L is. That is, we have $i_d(C)i_d(C^L) = 1$.*

Proof. Let $\mathcal{C}_{\bar{k}}$ and $\mathcal{C}^L_{\bar{k}}$ denote the special fibres of the minimal proper regular models over K^{nr} of C and C^L respectively. Since the formation of minimal proper regular models commutes with unramified base-change, we may identify $\mathcal{C}_{\bar{k}}$ and $\mathcal{C}^L_{\bar{k}}$, the only difference being that the natural action of $\mathrm{Gal}(\bar{k}/k)$ differs by twisting by the hyperelliptic involution ι which extends uniquely to an automorphism of $\mathcal{C}$ (here $\mathcal{C}$ is the minimal proper regular model of C over K^{nr}). Thus by Remark 3.3.4 it suffices to show that the hyperelliptic involution acts trivially on the components of $\mathcal{C}_{\bar{k}}$. Since J has good reduction, the dual graph of $\mathcal{C}_{\bar{k}}$ is a tree (see [Liu02, Proposition 10.1.51] or [BLR90, Proposition 9.6.3]), and as there are no exceptional curves in $\mathcal{C}_{\bar{k}}$, each leaf corresponds to a positive genus component (the multiplicity of each component is one since the assumption that J has good reduction forces $\mathcal{C}$ to be semistable). As in Section 5.3, we may form the quotient scheme $\mathcal{Y} := \mathcal{C}/\iota$ which is semistable and flat over $\mathcal{O}_{K^{\mathrm{nr}}}$ with generic fibre isomorphic to $\mathbb{P}^1_K$ (note that the

quotient of $\mathcal{C}_{\bar{k}}$ by ι need not coincide with the special fibre of $\mathcal{Y}$). If Z is a positive genus component of $\mathcal{C}_{\bar{k}}$ which is not fixed by ι, the it is birational to its image in the special fibre of a model of $\mathbb{P}^1_K$ (under the base-change of the quotient morphism), which is impossible. Thus the hyperelliptic involution fixes every positive genus component of $\mathcal{C}_{\bar{k}}$ and hence fixes every leaf of the dual graph. It therefore acts trivially on the dual graph, and we are done. □

We have thus shown

Corollary 8.1.3. *Suppose that K is a finite extension of $\mathbb{Q}_2$, L/K is an unramified quadratic extension and J has good reduction over K. Then Conjecture 1 holds for J and L/K.*

8.2 Ramified extensions

We restrict now to the case where K is a finite extension of $\mathbb{Q}_2$. Let L/K be a ramified quadratic extension. Assume further that J/K has good ordinary reduction. Let $J(K)_1$ denote the kernel of reduction on $J(K)$, and likewise for $J(L)_1$. We begin by considering the norm map from $J(L)_1$ to $J(K)_1$.

Lemma 8.2.1. *We have*

$$\left|J(K)_1/N_{L/K}J(L)_1\right| = |J(K)_1[2]|.$$

Proof. Let $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$. Let g be the genus of C so that by [LR78, Theorem 1], there is a $g \times g$ matrix u over $\mathbb{Z}_2$ (the *twist matrix* associated to the formal group of J) such that

$$J(K)_1/N_{L/K}J(L)_1 \cong G^g/(I-u)G^g$$

(here I is the $g \times g$ identity matrix). On the other hand (see Lemma in *loc.cit.*), denoting by T the completion of K^{nr}, we have

$$J(K)_1 \cong \left\{\alpha \in \left(\mathcal{O}_T^\times\right)^g \ : \ \alpha^\phi = \alpha^u\right\},$$

where ϕ denotes the K-Frobenius automorphism of T. In particular, we obtain

$$J(K)_1[2] \cong \left\{\alpha \in \{\pm 1\}^g \ : \ \alpha^{I-u} = 1\right\}.$$

Identifying the groups G and $\{\pm 1\}$ in the obvious way, we see that $J(K)_1[2]$ becomes identified with the kernel of multiplication by $I - u$ on G. We now conclude by noting that the cokernel and kernel of an endomorphism of a finite group always have the same order. $\square$

Lemma 8.2.2. *Suppose that all the 2-torsion of J is defined over an odd degree Galois extension of K. Then we have*

$$\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L) \equiv 0 \pmod 2.$$

Proof. By Lemma 3.1.1, we can actually assume that all the 2-torsion is rational and we will show that then

$$\dim_{\mathbb{F}_2} J(K)/N_{L/K}J(L) = 2g.$$

Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_1(L) & \longrightarrow & J(L) & \longrightarrow & \tilde{J}(k) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle 2} & & \\ 0 & \longrightarrow & J_1(K) & \longrightarrow & J(K) & \longrightarrow & \tilde{J}(k) & \longrightarrow & 0. \end{array}$$

The assumption that all the 2-torsion is defined over K means that reduction is a surjection from $J(K)[2]$ to $\tilde{J}(k)[2]$. In particular, in the exact sequence arising from applying the snake lemma to the diagram above, the connecting homomorphism is trivial. Thus we deduce the short exact sequence

$$0 \longrightarrow J(K)_1/N_{L/K}J_1(L) \longrightarrow J(K)/N_{L/K}J(L) \longrightarrow \tilde{J}(k)/2\tilde{J}(k) \longrightarrow 0.$$

As J is ordinary (and again using that all the 2-torsion is rational), we have

$$\left|\tilde{J}(k)/2\tilde{J}(k)\right| = |\tilde{J}(k)[2]| = 2^g.$$

On the other hand, by Lemma 8.2.1 we have

$$\left|J(K)_1/N_{L/K}J(L)_1\right| = |J(K)_1[2]| = 2^g$$

also (where again in the last equality we are using that all the 2-torsion is rational). The

result is now clear. □

Corollary 8.2.3. *Suppose that K is a finite extension of $\mathbb{Q}_2$, L/K is a ramified quadratic extension, J has good ordinary reduction over K and all of $J(\bar{K})[2]$ is defined over an odd degree Galois extension of K. Then Conjecture 1 holds for J and L/K.*

Proof. Again by Lemma 3.1.1 we assume that all the 2-torsion of J is in fact rational. In particular, f splits over K and hence $(\Delta_C, L/K) = 1$. Similarly, both C and C^L have a rational Weierstrass point and so $i_d(C)i_d(C^L) = 1$. By Lemma 8.2.2 we have $(-1)^{\mathrm{ord}_2 J(K)/N_{L/K}J(L)} = 1$ also. Finally, $w(J/L) = 1$. □

Theorems 1.2.1 and 1.4.2 now follow from Corollary 1.3.3, Proposition 4.1.1 and Corollaries 4.1.5, 6.0.14, 7.2.10, 8.1.3 and 8.2.3.

8.3 Constructing examples

For the purpose of giving examples we now describe how to construct hyperelliptic curves over $\mathbb{Q}$ whose Jacobians satisfy the conditions of Corollary 8.2.3 over $\mathbb{Q}_2$.

Lemma 8.3.1. *Let $f(x) \in \bar{\mathbb{F}}_2[x]$ be a monic separable polynomial of degree $g+1$ and $h(x) \in \bar{\mathbb{F}}_2[x]$ a polynomial of degree $\leq g$, coprime to f. Then the Jacobian J of the hyperelliptic curve*

$$C : y^2 - f(x)y = h(x)f(x) \quad /\bar{\mathbb{F}}_2$$

has 2-torsion group scheme $J[2] \cong (\mathbb{Z}/2\mathbb{Z} \oplus \mu_2)^g$. In particular, J is ordinary.

Proof. Let $\alpha_1, ..., \alpha_{g+1} \in \bar{\mathbb{F}}_2$ be the distinct roots of f and $c_1, ..., c_{g+1} \in \bar{\mathbb{F}}_2^\times$ be arbitrary. Then by [EP13, Theorem 1.3], the Jacobian of the hyperelliptic curve

$$y^2 - y = \sum_{i=1}^{g+1} \frac{c_i}{x - \alpha_i} = \frac{1}{f(x)} \sum_{i=1}^{g+1} c_i \prod_{j \neq i} (x - \alpha_i)$$

over $\bar{\mathbb{F}}_2$ has 2-torsion group scheme of the required form. Now the polynomials $f_i(x) = \prod_{j \neq i}(x - \alpha_i)$ are $g+1$ in number and of degree g. Since the α_i are distinct, it follows that they form a basis for the $\bar{\mathbb{F}}_2$-vector space of polynomials of degree $\leq g$ over $\bar{\mathbb{F}}_2$. In particular, we may choose $c_1, ..., c_{g+1}$ such that

$$h(x) = \sum_{i=1}^{g+1} c_i f_i(x)$$

and the assumption that $f(x)$ and $h(x)$ are coprime ensures that none of the c_i are zero. Thus the hyperelliptic curve

$$y^2 - y = \frac{h(x)}{f(x)} \quad /\bar{\mathbb{F}}_2$$

has 2-torsion group scheme $(\mathbb{Z}/2\mathbb{Z} \oplus \mu_2)^g$. A simple change of variables shows that this is the curve C in the statement. □

Corollary 8.3.2. *Suppose $f(x) \in \mathbb{Z}[x]$ has odd leading coefficient and degree $g+1$, and suppose that the reduction of $f \pmod 2$ is separable with each irreducible factor having odd degree. Further, let $h(x) \in \mathbb{Z}[x]$ of degree $\leq g$ be such that the reduction of $h \pmod 2$ is coprime to that of f. Then the Jacobian of the hyperelliptic curve*

$$C : y^2 = f(x)(f(x) + 4h(x))$$

has good ordinary reduction over $\mathbb{Q}_2$, and moreover has all its 2-torsion defined over an odd degree Galois extension of $\mathbb{Q}_2$.

Proof. One easily sees that a change of variables over $\mathbb{Q}_2$ brings C into the form $y^2 - f(x)y = h(x)f(x)$. This equation, along with the corresponding equation at infinity Convention 1.7.1, is integral, and together they define a proper smooth model of C over $\mathbb{Z}_2$. Thus C has good reduction over $\mathbb{Q}_2$ and moreover, by Lemma 8.3.1, the Jacobian of C has good ordinary reduction over $\mathbb{Q}_2$. Moreover, both $f(x)$ and $f(x) + 4h(x)$ reduce to separable polynomials over $\mathbb{F}_2$ whose irreducible factors have odd degree. It follows from Hensel's lemma that $f(x)(f(x) + 4h(x))$ splits over an odd degree unramified (and hence cyclic) extension of $\mathbb{Q}_2$ and hence all the 2-torsion of J is also defined over such an extension. □

Appendix A: The 2-primary part of the Shafarevich-Tate group of principally polarised abelian varieties in field extensions

In this appendix, for a principally polarised abelian variety A over a global field K, we study the parity of $\dim_{\mathbb{F}_2} Ш_0(A/L)[2]$ where L/K is a finite field extension. The result is Proposition 8.3.3 and has been independently observed by Česnavičius [Čes14a, Lemma 3.4]. As a consequence, we remove the assumption in two theorems of T. and V. Dokchtiser ([DD09a, Theorem 1.6(b)] and [DD09b, Theorem 1.6]) that the princpal polarisation on the abelian variety in question is induced by a rational divisor.

Proposition 8.3.3. *Let K be a global field, A/K a principally polarised abelian variety and L/K a finite field extension. Then*

$$\dim_{\mathbb{F}_2} Ш_0(A/L)[2] \equiv [L:K] \dim_{\mathbb{F}_2} Ш_0(A/K)[2] \pmod 2.$$

Proof. Fix a principal polarisation λ on A and let $\langle\ ,\ \rangle_K$ be the associated Cassels-Tate pairing on $Ш(A/K)$. This is antisymmetric and it follows that $\dim_{\mathbb{F}_p} Ш_0(A/K)[p]$ is even for all p except possibly $p = 2$. In [PS99, Section 4], Poonen and Stoll associate an element $c \in Ш(A/K)$ to λ and show (Theorem 8 in loc. cit.) that $\dim_{\mathbb{F}_2} Ш_0(A/K)[2]$ is even if and only if $\langle c, c\rangle_K$ (which a priori is in $\{0, \frac{1}{2}\}$) is equal to 0. On replacing K by L, λ gives also a principal polarisation on A_L and one readily checks that the image of c under restriction in $Ш(A/L)$ coincides with the element associated to λ viewed as a principal polarisation of A_L. However, we now have $\langle c, c\rangle_L = [L:K]\,\langle c, c\rangle_K$ as a consequence of the commutative

diagram

$$\begin{array}{ccc} \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}_{K_v}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle [L_w:K_v]} \\ \mathrm{Br}(L_w) & \xrightarrow{\mathrm{inv}_{L_w}} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{8.3.4}$$

for each place v of K and each place w of L dividing v. □

Remark 8.3.5. *One can also replace* $\dim_{\mathbb{F}_2} Ш_0(A/K)[2]$ *by* $\dim_{\mathbb{F}_2} Ш_0(A/K)[2^\infty]$ *in Proposition 8.3.3. See* [PS99, Theorem 8].

For curves, an analogous local statement holds. Here, as in [PS99, Section 8], we call a (smooth, proper, geometrically integral) curve X *deficient* over a local field K if $\mathrm{Pic}^{g-1}(X_K) = \emptyset$. Again, we stress that $\mathrm{Pic}^{g-1}(X_K)$ is the degree $g-1$ subset of the Picard group of the curve X_K, and not the K-points of the degree $g-1$ part of the Picard functor of X. For A the Jacobian of a curve over a number field, in [PS99, Corollary 12] Poonen and Stoll characterise when $Ш_0(A/K)[2]$ has odd $\mathbb{F}_2$-dimension in terms of the number of deficient places of the curve.

Proposition 8.3.6. *Let K be a local field, X/K a (smooth, proper, geometrically integral) curve, and L/K a finite separable field extension. Let $\varepsilon(X,K)$ be equal to 1 if X is deficient over K, and 0 else, and define $\varepsilon(X,L)$ similarly. Then we have*

$$\varepsilon(X,L) \equiv [L:K]\varepsilon(X,K) \pmod 2.$$

Proof. Let $\phi_K : \mathrm{Pic}(X_{\bar{K}})^{\mathrm{G}_K} \to \mathbb{Q}/\mathbb{Z}$ be the map defined in Section 3.3 (and also [PS99, Section 7]). Then again as in Section 3.3, it is proved by Poonen and Stoll in [PS99, Theorem 11] that if $\mathcal{L} \in \mathrm{Pic}(X_{\bar{K}})^{\mathrm{G}_K}$ is a rational divisor class of degree n on X then $\mathrm{Pic}^n(X)$ is empty (resp. non-empty) according to $n\phi_K(\mathcal{L}) = \frac{1}{2}$ (resp. 0) in $\mathbb{Q}/\mathbb{Z}$.

Fix now a rational divisor class $\mathcal{L}$ in $\mathrm{Pic}^{g-1}(X_K)$ (that such a class exists is due to Lichtenbaum [Lic69], but see also [PS99, Section 4]). Then $(g-1)\phi_K(\mathcal{L}) \in \mathbb{Q}/\mathbb{Z}$ is $\frac{1}{2}$ or 0 according to whether X is deficient over K or not. On the other hand, $\mathcal{L}$ also yields a rational divisor class of degree $g-1$ in $\mathrm{Pic}^{g-1}(X_L)$ and the commutativity of (8.3.4) shows that $(g-1)\phi_L(\mathcal{L}) = [L:K](g-1)\phi_K(\mathcal{L})$, completing the proof. □

Proposition 8.3.3 has the following consequence.

Corollary 8.3.7. *In the notation of* [DD09a], *for L/K a Galois extension of global fields and A/K a principally polarised abelian variety, the function*

$$\{\text{Subgroups } H \text{ of } G\} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

defined by

$$H \mapsto \dim_{\mathbb{F}_2} Ш_0(A/L^H)[2] \pmod 2$$

is representation-theoretic.

Proof. By Proposition 8.3.3 we have

$$\dim_{\mathbb{F}_2} Ш_0(A/L^H)[2] \equiv [L^H : K] \dim_{\mathbb{F}_2} Ш_0(A/K)[2] \pmod 2.$$

The result now follows since the function

$$\{\text{Subgroups } H \text{ of } G\} \longrightarrow \mathbb{Z}$$

given by

$$H \mapsto [L^H : K]$$

is representation theoretic. Indeed, noting that

$$[L^H : K] = \dim_{\mathbb{C}} \mathbb{C}[G/H]$$

gives the result. □

We now explain how Corollary 8.3.7 allows us to remove the assumption that the principally polarised abelian variety in the theorems [DD09a, Theorem 1.6(b)] and [DD09b, Theorem 1.6] of T. and V. Dokchitser has its principal polarisation induced from a rational divisor. The context of the two theorems cited above is the theory of Brauer relations and regulator constants, and is described in [DD09a, Section 2]. For brevity, we wil adopt the notation detailed in this paper, as it is summarised in [BGW13, Proof of Theorem A.3]. In particular, we set K a number field, A/K a principally polarised abelian variety, F/K a finite Galois extension with Galois group G and $\mathcal{S}$ the set of irreducible, self-dual $\mathbb{Q}_p[G]$-representations for a prime p, and let $\Theta = \sum_i n_i H_i$ be a Brauer relation in G. For $\rho \in \mathcal{S}$, we write $\mathcal{C}(\Theta, \rho)$ for the corresponding regulator constant (see [DD09a, Definition

2.13]). As in [BGW13, Proof of Theorem A.3] define

$$\mathcal{S}_\Theta = \{\rho \in \mathcal{S} \ : \ \mathrm{ord}_p \mathcal{C}(\Theta, \rho) \equiv 1 \pmod 2\}\,.$$

Then T. and V. Dokchitser show [BGW13, Theorem A.7] that for any $\rho \in \mathcal{S}$, we have

$$\sum_{\rho \in \mathcal{S}_\Theta} m_\rho \equiv \mathrm{ord}_p \prod_i \tilde{c}_{A/F^{H_i}}^{n_i} |Ш(A/F^{H_i})[p]|^{n_i} \pmod 2$$

where m_ρ denotes the multiplicity of ρ in the dual p^∞-Selmer group of A/F and $\tilde{c}_{A/F^{H_i}}$ is the product over places of F^{H_i} of the local Tamagawa numbers of A/F^{H_i}, multiplied by a contribution coming from differentials on A (see [BGW13, Proof of Theorem A.3] for the precise definition). As T. and V. Dokchitser remark, for odd p, each term $\mathrm{ord}_p|Ш(A/F^{H_i})[p]|$ is even individually, so these terms do not contribute. However, whilst when $p = 2$ they need not be trivial individually, it follows immediately from Corollary 8.3.7 that the product

$$\mathrm{ord}_2 \prod_i |Ш(A/F^{H_i})[2]|^{n_i}$$

is even as a whole. Thus we may remove the Ш terms completely. We obtain

Corollary 8.3.8. *Let K be a number field and A/K a principally polarised abelian variety. Then, maintaining the notation above, we have*

$$\sum_{\rho \in \mathcal{S}_\Theta} m_\rho \equiv \mathrm{ord}_p \prod_i \tilde{c}_{A/F^{H_i}}^{n_i} \pmod 2.$$

Comparing with the statement of [DD09b, Theorem 1.6] we now see that the asumption that A/K has a principal polarisation associated to a K-rational divisor is unecessary. Since the use of this result was the only place in the proof of [DD09a, Theorem 1.6(b)] that required this assumption, we may remove it there as well.

Remark 8.3.9. *Recent work of Betts and Dokchitser* [BD14] *has weakened the assumptions of* [DD09a, Theorem 1.6] *at $p = 2$ in a different direction.*

Bibliography

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 94–115. MR0219512 (36 #2593)

[BD14] A. Betts and V. Dokchitser, *Finite quotients of $\mathbb{Z}[C_n]$-lattices and tamagawa numbers of abelian varieties*, Preprint **arXiv:1405.3151** (2014).

[BGW13] Manjul Bhargava, Benedict Gross, and Xiaoheng Wang, *Pencils of quadrics and the arithmetic of hyperelliptic curves*, Preprint **http://arxiv.org/abs/1310.7692** (2013).

[Big97] Norman Biggs, *Algebraic potential theory on graphs*, Bull. London Math. Soc. **29** (1997), no. 6, 641–682. MR1468054 (98m:05120)

[BL99] Siegfried Bosch and Qing Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math. **98** (1999), no. 3, 275–293. MR1717533 (2000i:11094)

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[BN07] Matthew Baker and Serguei Norine, *Riemann-Roch and Abel-Jacobi theory on a finite graph*, Adv. Math. **215** (2007), no. 2, 766–788. MR2355607 (2008m:05167)

[BN09] ———, *Harmonic morphisms and hyperelliptic graphs*, Int. Math. Res. Not. **15** (2009), 2914–2955. MR2525845 (2010e:14031)

[BS15] Manjul Bhargava and Arul Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621. MR3275847

[Cas67] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 42–84. MR0222054 (36 #5106)

[Česl4a] Kęstutis Česnavičius, *The l-parity conjecture over the constant quadratic extension*, Preprint **http://arxiv.org/abs/1402.2939** (2014).

[Česl4b] ———, *The p-parity conjecture for elliptic curves with a p-isogeny*, Preprint **http://arxiv.org/abs/1207.0431** (2014).

[Česl4c] ———, *Topology on cohomology of local fields*, Preprint **http://arxiv.org/abs/1405.2009** (2014).

[CFKS10] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), no. 1, 19–97. MR2551757 (2011a:11127)

[ČI15] Kęstutis Česnavičius and Naoki Imai, *The remaining cases of the kramer-tunnell conjecture*, Preprint **http://arxiv.org/abs/1504.02546** (2015).

[Cor01] Gunther Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. (Basel) **77** (2001), no. 3, 241–246. MR1865865 (2002g:11082)

[Cor05] ———, *Erratum to: 'Two-torsion in the Jacobian of hyperelliptic curves over finite fields'*, Arch. Math. (Basel) **85** (2005), no. 6, loose erratum.

[DD09a] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71. MR2534092 (2010j:11089)

[DD09b] ———, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 2, 257–267. MR2475965 (2010a:11219)

[DD10] ———, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596. MR2680426 (2011h:11069)

[DD11] ———, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39–64. MR2831512 (2012h:11084)

[EP13] Arsen Elkin and Rachel Pries, *Ekedahl-Oort strata of hyperelliptic curves in characteristic 2*, Algebra Number Theory **7** (2013), no. 3, 507–532. MR3095219

[Fon85] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), no. 3, 515–538. MR807070 (87g:11073)

[GLL13] Ofer Gabber, Qing Liu, and Dino Lorenzini, *The index of an algebraic variety*, Invent. Math. **192** (2013), no. 3, 567–626. MR3049930

[How01] Everett W. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, Moduli of abelian varieties (Texel Island, 1999), 2001, pp. 203–216. MR1827021 (2002g:11079)

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320. MR3043582

[Kra81] Kenneth Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR597871 (82g:14028)

[KT82] K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352. MR664648 (83m:14031)

[Lic68] Stephen Lichtenbaum, *Curves over discrete valuation rings*, Amer. J. Math. **90** (1968), 380–405. MR0230724 (37 #6284)

[Lic69] ———, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136. MR0242831 (39 #4158)

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. MR1917232 (2003g:14001)

[Liu94a] ———, *Conducteur et discriminant minimal de courbes de genre* 2, Compositio Math. **94** (1994), no. 1, 51–79. MR1302311 (96b:14038)

[Liu94b] ———, *Modèles minimaux des courbes de genre deux*, J. Reine Angew. Math. **453** (1994), 137–164. MR1285783 (95k:14024)

[Liu96] ———, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610. MR1363944 (97h:11062)

[LL99] Qing Liu and Dino Lorenzini, *Models of curves and finite covers*, Compositio Math. **118** (1999), no. 1, 61–102. MR1705977 (2000f:14033)

[Lor11] Dino Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 5, 1995–2037 (2012). MR2961846

[LR78] Jonathan Lubin and Michael I. Rosen, *The norm map for ordinary abelian varieties*, J. Algebra **52** (1978), no. 1, 236–240. MR0491735 (58 #10936)

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR0330174 (48 #8512)

[Mil86] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 103–150. MR861974

[MR07] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. MR2373150 (2009a:11127)

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354. MR0204427 (34 #4269)

[Nek13] Jan Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra Number Theory **7** (2013), no. 5, 1101–1120. MR3101073

[NU73] Yukihiko Namikawa and Kenji Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscripta Math. **9** (1973), 143–186. MR0369362 (51 #5595)

[Ogg66] A. P. Ogg, *On pencils of curves of genus two*, Topology **5** (1966), 355–362. MR0201437 (34 #1321)

[Pap13] Mihran Papikian, *Non-archimedean uniformization and monodromy pairing*, Contemporary Mathematics **605** (2013), 123–160.

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318. MR2915483

[PR12] ———, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269. MR2833483

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188. MR1465369 (98k:11087)

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984 (2000m:11048)

[Rei61] Irving Reiner, *The Schur index in the theory of group representations*, Michigan Math. J. **8** (1961), 39–47. MR0122892 (23 #A224)

[Sab07] Maria Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. **359** (2007), no. 9, 4259–4284 (electronic). MR2309184 (2008c:11090)

[Sch96] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114. MR1370197 (97e:11068)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[Sil89] Robert Silhol, *Digression on real abelian varieties and classification of real abelian surfaces*, Real algebraic surfaces, 1989, pp. 75–94.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[TY14] Fabien Trihan and Seidai Yasuda, *The ℓ-parity conjecture for abelian varieties over function fields of characteristic $p > 0$*, Compos. Math. **150** (2014), no. 4, 507–522. MR3200666