UNIVERSITÄT
BAYREUTH

On computation of the Cassels-Tate pairing

Der Universität Bayreuth
zur Erlangung des Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
vorgelegte Abhandlung

von

Himanshu Shukla

aus Prayagraj (Allahabad)

Gutachter 1: Prof. Dr. Michael Stoll
Gutachter 2: Prof. Dr. Bjorn Poonen

Tag der Einreichung: 16.05.2024
Tag des Kolloquiums: 26.09.2024

Abstract

Let J be the Jacobian variety of a "nice" curve C/k. In this thesis we compute the Cassels-Tate pairing for Selmer groups of various isogenies on Jacobians of various types of curves. The main aim of the thesis is to use the Albanese-Albanese definition of the pairing to obtain an algorithm.

We start with computing the Cassels-Tate pairing on $\mathrm{Ш}^{(2)}(E/k) \times \mathrm{Ш}^{(2)}(E/k)$, where E/k is an elliptic curve. Furthermore, this provides an alternative proof that the pairing defined by Cassels is the same as the Cassels-Tate pairing.

Next, we generalize our method for computing the Cassels-Tate pairing to $\mathrm{Ш}^{(2)}(J/k)$, where J is the Jacobian variety of an odd-degree hyperelliptic curve. Furthermore, we give a conditional algorithm (conditioned on if a set of ternary quadratic forms have a global solution) inspired by the elliptic curve case. We use our conditional algorithm to compute the Cassels-Tate pairing in various cases including genus 3 and 4.

Apart from the above, we compute the Cassels-Tate pairing on $(1-\zeta_l)$-Selmer groups corresponding to the curves of the form $y^2 = x^l + A$ and use it compute some examples.

At last we discuss the computation of the Cassels-Tate pairing on Selmer groups of Richelot isogenies and $(3,3)$-isogenies (when the kernel is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ as a Galois module) on genus 2 Jacobians. We end this thesis with some discussion on computation of the pairing for the case of "True descents", and some future problems.

Acknowledgements

Zuerst danke ich meinem Betreuer Prof. Dr. Michael Stoll für seine stetige und tatkräftige Unterstützung (sowohl mathematisch als auch persönlisch) während dieses Prozesses, den Sekretärinnen am Lehrstuhl für Computer Algebra, Elvira Rettner und Katharina Ziegler dafür, dass sie mit meiner Faulheit in bürokratischen Angelegenheiten Schritt gehalten haben, und dem Schreibzentrum der Universität Bayreuth für seine Hilfe durch Schreibberatung mit der Doktorarbeit. Die Deutsche Forschungsgemeinschaft (DFG)–Grant STO-299/17-1 (AOBJ: 662415) hat mich während dieser Forschung unterstützt. Ich danke Jan Steffen Müller und Timo Keller für ihre Unterstützung während der CoViD-19 Zeiten, weil mehr als die Hälfte dieser Forschung im Zeitraum 2020-22 abgeschlossen wurde. Ohne die interessanten Gespräche mit Christian Gleissner, Massimiliano Alessandro, Michael Kiermaier, Pip Goodman, Fabian, Arihant Jain, Chary, and Mickaël Montessinos wäre diese Weg sehr eintönig gewesen.

मैं अपने परिवार (माँ, पिता और भाई सौरभ) के असीम प्रेम और विश्वास के लिए तहे दिल से आभारी हूँ। Ich danke meiner anderen Familie aus Bayreuth (Max, Marja, Julian, und Aaron) für ihre stetige Unterstützung während dieses Zeitraums, und Elena für ihren ständigen Druck mit “Kapitel eins, Kapitel zwei zack zack, und fertig”, ihre Unterstützung in den letzen Phasen dieser Doktorarbeit und eine schöne Zeit in Bayreuth.

I would like to thank all my friends (and Bayreuth in general) without whom I would have missed at least one of the various emotions that kept these times exciting. I apologize beforehand for just mentioning limited things about them: Isha (for every “Shukluu...” and an age-long friendship), Amit (for a keeping up with my randomness), Anurag and Rajeev (for being the elder brothers), Bhaskar, Gorav, Harry, and Rishab (for beautiful Saarbrücken times and enlightening discussions), DV (for keeping *Kabir* and my dialect alive in Germany), Björn (for being Björn), LP (for my rants), Veronica and Emiliano (for the interesting conversations, dark humor and sarcasm), Hannah and Hannah (for interesting Bayreuth times), Mira (for every “Hallo Hermanshuu..”), and at this point I can’t help but feel overwhelmed by the long list still left. Therefore, in all humility, I quote a story to convey my emotions:

“As a mango tree found itself bearing its first set of fruits, it got elated, It decided to acknowledge everything and everyone that made it possible. But what and whom is it supposed to acknowledge? Should it acknowledge the farmer who always made sure it got the necessary ambience and the crucial nutrients to the best of his knowledge and perception?

Or should it acknowledge the farmers little daughter who wanted a mango tree in their farm? Or rather her friend who introduced her to mangoes? Or should it thank everything and everyone responsible for the farmer and his familys health and well-being making sure that they successfully managed to care for it? Or the monkey who, after eating a mango, threw the seed in their garden which the farmer finally planted? Or should it be grateful to the numerous plants and animals who shed their wastes contributing to the richness of the soil? Or should it thank the weather cycles and the responsible planetary forces causing plants to shed leaves? Or the animals biological system and the responsible life forces making them shed their wastes regularly? Or should it thank all the birds feeding on the worms that were eating it when it was still a sapling, or the ecological system leading the birds to do so? Or should it acknowledge the sun, or its source? Or should it thank the passerby who ended up urinating around its roots when the little mango plant was about to die because of lack of water? Or should it thank the storm which blew away the unnoticed weeds that had been growing around it and had been taking up all its nutrients?

Overwhelmed by all this, it could not help but feel grateful towards every single atom and every single living being that have ever existed, and all the forces causing and sustaining them. It kept quiet and simply lived on, continuing to bear new flowers every spring and to bear new fruits every summer. " – [Pan21, Acknowledgement].

I end with the following lines I adapted from Harivanshrai Bachchan's *Madhushala.*

राह पकड़ कर एक, चल पड़ा था वह मतवाला।
बहुत दूर जाकर भी उसको, नहीं मिली जब मधुशाला।
निकला वह उन्मुक्त नशे से, ज्ञात हुआ मादकता का।
मदिरालय कोई अंत नहीं था, पथ ही थी वह मधुशाला।

Contents

Introduction

Given a "nice" curve C over a number field k, computing the set of k-rational points $C(k)$ is one of the fundamental problems in Arithmetic Geometry. If C is not a rational curve, then this problem usually turns out to be hard. Mordell's conjecture (now a theorem due to Faltings) implies that $C(k)$ is finite, if the genus g of C is larger than 1. One of the ways to compute $C(k)$ is to compute k-rational points on the Jacobian variety $J_C \simeq \mathrm{Pic}^0(C)$, which is a principally polarized abelian variety. The Mordell–Weil theorem for an abelian variety A/k implies that

$$A(k) \simeq A(k)_{\mathrm{tors}} \oplus \mathbb{Z}^{r_A},$$

where r_A is the *algebraic rank* associated to A/k and $A(k)_{\mathrm{tors}}$ is a finite abelian group. Therefore, computing k-rational points on J_C/k naturally requires the knowledge of r_{J_C}.

On the other hand, methods exist to bound the size of $C(k)$ just by knowing r_{J_C} over k and the number of points over a prime of good reduction. One such method is using Chabauty–Coleman which says that when $r_{J_C} < g$, $\mathfrak{p}$ is a prime of k above a rational prime $p > 2g$ and additionally if $\mathfrak{p}$ is a prime of good reduction for C, then

$$\#C(k) < \#\bar{C}(\overline{k_{\mathfrak{p}}}) + 2g - 2,$$

where $\bar{C}$ is the reduction of C mod $\mathfrak{p}$ and $\bar{k}_{\mathfrak{p}}$ is the residue field of the completion $k_{\mathfrak{p}}$. There are many variants of Chabauty's method available (for details see [Cor]) and all require knowledge of r_{J_C} or at least that the *Selmer-rank* is sufficiently small (as in the case of [Sto17b]) . Moreover, one obtains better bounds if $r_{J_C} \leq g - 2$ (see [Sto06]), and uniform bounds only in terms of the degree $d \coloneqq [k : \mathbb{Q}]$ and g if $r_{J_C} \leq g - 3$ (see [Sto19] when C is hyperelliptic and [KRZB15] for general C). Dimitrov, Gao and Habegger [DGH21] have been able to uniformly bound the number of the points on C/k in terms of g, r_{J_C} and d, providing a uniform bound on $\#C(k)$. However, these bounds are astronomical and given a concrete curve will be inefficient. Nonetheless, we observe that r_{J_C} plays a crucial role in computing $C(k)$.

Jacobians naturally are the next class of abelian varieties after elliptic curves (abelian varieties of dimension 1) to be considered. Furthermore, Matsusaka's theorem implies that every abelian variety over k is a quotient of the Jacobian of some

curve. Hence, computing the algebraic rank of a Jacobian is of independent importance to the verification of the BSD (Birch and Swinnerton-Dyer) conjecture (both weak and strong versions) in higher dimensional cases. If the weak BSD conjecture holds for a Jacobian variety J, then r_J can be obtained by computing the order of vanishing of the L-function $L(J/k, s)$ at $s = 1$. In order to verify the strong BSD conjecture (that connects the leading term of the L-function with the geometric and arithmetic invariants) it is important to have an idea about the size of the Tate-Shafarevich group and the Cassels-Tate pairing can be used to capture visible elements in the Tate-Shafarevich group, thus giving us information on its size. Here visible elements are the elements of the Tate-Shafarevich group that pair non-trivially under the Cassels-Tate pairing.

The focus of this PhD thesis is mainly to obtain better bounds on r_{J_C} using *descent* methods. Let J be a Jacobian and $\phi : J \to A$ be an isogeny (surjective and finite homomorphism). Let G_k be the absolute Galois group of k and $J[\phi]$ be the kernel of ϕ. Taking Galois cohomology (both locally and globally) on the exact sequence

$$0 \to J[\phi] \to J \to A \to 0,$$

one obtains

$$0 \to A(k)/\phi J(k) \to \mathrm{S}^{(\phi)}(J/k) \to Ш(J/k)[\phi] \to 0,$$

where $\mathrm{S}^{(\phi)}(J/k) \coloneqq \ker(\mathrm{H}^1(G_k, J[\phi]) \to \prod_v \mathrm{H}^1(G_{k_v}, J))$ is the *ϕ-Selmer group* and $Ш(J/k) \coloneqq \ker\left(\mathrm{H}^1(G_k, J) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right)$ is the *Tate-Shafarevich group* of J/k. Both Selmer and Tate-Shafarevich groups compute deviations from certain local-global principles and characterize geometric objects. The Selmer group is provably *finite*; hence, one may obtain an upper bound on r_J (also on r_A) by using $\#\mathrm{S}^{(\phi)}$, for example, in the case when ϕ is the multiplication by n isogeny. There are various algorithms known to compute the Selmer groups in various cases and we will discuss a few of them in this thesis.

Cassels and Tate (Cassels for elliptic curves and Tate for abelian varieties) defined a pairing, called the *Cassels-Tate pairing* (CTP)

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J/k) \times Ш(J/k) \to \mathbb{Q}/\mathbb{Z},$$

such that $nШ(J/k)$ is the exact annihilator of $Ш(J/k)[n]$. The pairing is in general anti-symmetric and non-degenerate on the maximal non-divisible quotient of $Ш(J/k)$. In particular, if $Ш(J/k)$ is finite (as is conjectured), then $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$ is a perfect pairing. One can pull back $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$ to define a pairing (that we again call Cassels-Tate pairing)

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : \mathrm{S}^{(n)}(J/k) \times \mathrm{S}^{(n)}(J/k) \to \mathbb{Q}/\mathbb{Z},$$

such that $\langle a, b \rangle_{\mathrm{CT}} = 0$ for all $b \in \mathrm{S}^{(n)}(J/k) \iff a \in \mathrm{Im}(\mathrm{S}^{(n^2)}(J/k)) \subset \mathrm{S}^{(n)}(J/k)$. From the following commutative diagram one concludes that r_J can be bounded in

terms of $\ker(\langle\cdot,\cdot\rangle_{\mathrm{CT}})$.

$$\begin{array}{ccc} J(k)/n^2J(k) & \hookrightarrow & \mathrm{S}^{(n^2)}(J/k) \\ \downarrow & & \downarrow \\ J(k)/nJ(k) & \hookrightarrow & \mathrm{S}^{(n)}(J/k). \end{array}$$

There are various definitions of the CTP known for principally polarized abelian varieties and algorithms for computing the CTP have been given in various cases. We mention a few cases in §2.6. Attempts to compute the CTP have been mainly via the Weil-pairing definition and the homogeneous space definition of the CTP. Using the Weil-pairing requires one to work with fields of n^2 torsion points $k(J[n^2])$. On the other hand, using the homogeneous space definition requires one to work with explicit equations for homogeneous spaces represented by the n-Selmer elements. The complication is clear in both cases. In the case of the Weil-pairing definition, $[k(J[n^2]) : k]$ is generally very large compared to the field of definition of 1-cocycles representing n-Selmer elements. Similarly for the homogeneous space definition, the explicit equations representing homogeneous spaces can be very complicated and cumbersome to work with.

This work is the first attempt to obtain an algorithm to compute the CTP using the Albanese-Albanese definition that requires one to work with the group of divisors on C, i.e., the group of formal sums of points on C, therefore, avoiding to work with complicated equations of homogeneous spaces. Another advantage can be not to expand the fields over which one needs to perform the arithmetic beyond the field of definition of our starting 1-cocycles representing the Selmer elements being paired, therefore, avoiding the expansion to $k(J[n^2])$. We make this definition effective in various cases, avoiding both the hurdles coming from the Weil-pairing and the homogeneous space definitions of the pairing. The major challenge is trying to obtain a 2-cochain ε with values in $\mathbb{G}_{\mathrm{m}}$ such that $\partial\varepsilon = \eta$, where η is a 3-cocycle constructed in the definition of the CTP, and ∂ is the coboundary operator. Apart from bounding the rank, computing the Cassels-Tate pairing is of independent interest, i.e., one can use the CTP to "visualize" elements in $Ш(J/k)$ (two Selmer elements which pair non-trivially necessarily represent non-trivial elements in $Ш(J/k)$).

The organization of this thesis is as follows: In Chapter 1 we discuss the preliminaries and the background relevant to the thesis.

We introduce the Cassels-Tate pairing in Chapter 2 via three different definitions for Jacobian varieties and discuss the previous work on its computation. We then extend the two Galois–equivariant pairings (between principal divisors and degree zero divisors) used in the Albanese-Albanese definition so that they are defined everywhere, rather than only on divisors with disjoint support. This helps us avoid some complications which arise from the assumption used in the original definition, which demands that the lifts of certain elements of $\mathrm{Pic}^0(C_{\overline{k}})$ to $\mathrm{Div}^0(C_{\overline{k}})$ have disjoint

support.

In Chapter 3 we use the Albanese-Albanese definition to obtain the CTP (previously obtained due to Cassels [Cas98]) on $\text{Ш}^{(2)}(E/k)$ for an elliptic curve E/k. This is the first attempt to compute the pairing using Albanese-Albanese definition.

In Chapter 4 we generalize the techniques used to compute the CTP in the case of elliptic curves to $\text{Ш}^{(2)}(J/k)$ for the Jacobian J of an odd-degree hyperelliptic curve of any genus. Furthermore, we discuss a conditional algorithm inspired by the elliptic curve case and show that the condition (empirically) is a mild one for genus 2 and becomes stronger as the genus increases. We also discuss some examples.

In Chapter 5 we discuss the computation of the CTP for $(1-\zeta_l)$-isogeny Selmer groups on the Jacobians of curves of the form $y^2 = x^l + A$ for $A \in \mathbb{Z}$ and l-odd. Furthermore, in §5.5 we consider a conditional case where we can avoid inverting a local point under the $(1-\zeta_l)$-isogeny. We also provide some examples for the computations.

We conclude this thesis by discussing the computation of the CTP on $(2,2)$-isogeny and $(3,3)$-isogeny Selmer groups in Chapter 6. For $(3,3)$-isogenies we provide a method for computing the global part of the pairing only.

The Magma programs checking the examples in the thesis and implementations of some of the algorithms can be found at https://github.com/highshukla/thesis_codes.

Chapter 1

Background and Preliminaries

1.1 Notation

Throughout this thesis, for the sake of simplicity, we assume that our base fields are of characteristic 0 unless stated otherwise even though most of the results can be extended to positive characteristic fields with suitable assumptions. Furthermore, if at some point we are working with positive characteristic fields, then we assume that they are perfect unless stated otherwise. In this section, we will list some of the notations which will be common throughout.

We denote by $\mathbb{Z}_+$ the set of positive integers. For a perfect field k, let $\overline{k}$ denote a fixed algebraic closure of k, $G_k := \mathrm{Gal}(\overline{k}/k)$, and $\mathbb{G}_{\mathrm{m}} := \overline{k}^{\times}$. For a number field k and a place v of k, we denote its completion at v by k_v, and for each completion we fix an embedding $\overline{k} \hookrightarrow \overline{k_v}$. This induces an embedding $G_{k_v} \hookrightarrow G_k$. Let k_v^{nr} denote the maximal unramified extension of k_v, and let $\mathfrak{k}_v$ denote the residue field associated to k_v. We have the natural identification $\mathrm{Gal}(k_v^{\mathrm{nr}}/k_v) \simeq \mathrm{Gal}(\overline{\mathfrak{k}_v}/\mathfrak{k}_v)$. If k is a number field, then let $\mathrm{Cl}(k)$ denote the class group of k.

For an algebra A over k and for each $n \geq 1$, we denote by $\mu_n(A) := \{\zeta : \zeta^n = 1\} \subset A^{\times}$, the nth roots of unity contained in A and $\bar{A} := A \otimes_k \overline{k}$, i.e., the extension of scalars to $\overline{k}$.

Let G be a group and M a G-module, i.e., an abelian group with a G-action compatible with the group operation. Then, by M^G, we denote the submodule fixed by G. For a G-set (a set with an action of group G on it) Δ and a G-module M, let M^{Δ} denote the set

$$\{m : m : \Delta \to M \text{ is a continuous map}\}.$$

Here, the continuity of maps is considered with respect to the topology on Δ and M, which in many cases will be discrete. M^{Δ} is clearly an abelian group and becomes a G-module under the natural action $g \cdot m : P \mapsto gm(g^{-1}P)$. If M is a G_k-module and K is an algebraic field extension of k, then $M(K) := M^{G_K}$. If $\phi : M \to M'$ is a homomorphism between abelian groups M and M', then we denote $\ker(\phi)$ with

$M[\phi]$. For a G_k-module M, let $k(M) := (\overline{k})^{\ker(G_k \to \mathrm{Aut}\,(M))}$. Note that $k(M)$ is a Galois extension of k with $G_{k(M)} = \ker(G_k \to \mathrm{Aut}\,(M))$. When k is a global field and v a place of k, we define M_v to be the module M viewed as G_{k_v}-module.

Let ∂, $\mathrm{C}^n(G, M)$, $\mathrm{Z}^n(G, M)$, $\mathrm{B}^n(G, M)$ and $\mathrm{H}^n(G, M)$ denote the coboundary map, the group of continuous n-cochains, n-cocycles, n-coboundaries and n-cohomology classes, respectively, with respect to the bar resolution (for definitions and details see §1.3). For a cochain $x \in \mathrm{C}^i(G_k, -)$ we will denote its restriction to $\mathrm{C}^i(G_{k_v}, -)$ by x_v using the fixed embedding $G_{k_v} \hookrightarrow G_k$. To simplify notation, we will denote $\mathrm{C}^i(G_k, \mathbb{G}_\mathrm{m})$ by $\mathrm{C}^i(k)$, and similarly for the groups of cocycles and cohomology classes. If L/k is a finite Galois extension, then we denote $C^i(\mathrm{Gal}(L/k), L^\times)$ by $\mathrm{C}^i(L/k)$ and similarly for the groups of cocycles and cohomology classes. Let $\mathrm{Br}(k) \simeq \mathrm{H}^2(k)$ denote the Brauer group, and $\mathrm{Br}(L/k) \simeq \mathrm{H}^2(L/k)$ denote the relative Brauer group.

We will write the group structure on the cochains/cohomology classes additively, even when they take values in a multiplicative group. However, after the evaluation of cochains at certain arguments, we will use the group operation of the corresponding G-module. For example, if $x, y \in \mathrm{C}^1(k)$, then we use $+$ to denote their addition $z := x + y$ as cochains, but for $\sigma \in G_k$, $z(\sigma) \in \mathbb{G}_\mathrm{m}$ will be written as $x(\sigma)y(\sigma)$, using the group operation of $\mathbb{G}_\mathrm{m}$.

We call a variety V over k "nice" if V is a projective, geometrically irreducible, and smooth variety defined over k. Unless stated otherwise we assume throughout that V is a nice variety. Let L/k be a field extension; then, we denote the base change of V/k to L by V_L. Let $\overline{k}(V_{\overline{k}})$ be the field of rational functions on $V_{\overline{k}}$ and $k(V) := \left(\overline{k}(V_{\overline{k}})\right)^{G_k}$ (see Remark 1.2.1 for why $k(V)$, i.e., the field of rational functions with coefficients in k is exactly the G_k invariant subfield of $\overline{k}(V_{\overline{k}})$). A curve X/k will be a "nice variety" of dimension 1 defined over k. Let $\mathrm{Div}(X_{\overline{k}})$, $\mathrm{Div}^0(X_{\overline{k}})$, $\mathrm{Princ}(X_{\overline{k}})$, $\mathrm{Pic}\,(X_{\overline{k}})$ and $\mathrm{Pic}^{\,0}(X_{\overline{k}})$ denote the standard objects, i.e., the group of divisors, the group of degree 0-divisors, principal divisors on $X_{\overline{k}}$ (i.e. supported on closed points of $X_{\overline{k}}$), the Picard group, and the degree zero component of the Picard scheme associated to $X_{\overline{k}}$, respectively. Similarly, $\mathrm{Div}(X)$, $\mathrm{Div}^0(X)$, $\mathrm{Princ}(X)$, $\mathrm{Pic}\,(X)$, and $\mathrm{Pic}^{\,0}(X)$ denote the above mentioned objects supported on closed points of X/k. In particular, $\mathrm{Pic}\,(X) = \mathrm{Div}(X)/\mathrm{Princ}(X)$ and $\mathrm{Pic}^{\,0}(X) = \mathrm{Div}^0(X)/\mathrm{Princ}(X)$. Note that $\mathrm{Div}(X) = \mathrm{Div}(X_{\overline{k}})^{G_k}$ and $\mathrm{Princ}(X) = \mathrm{Princ}(X_{\overline{k}})^{G_k}$. However, in general $\mathrm{Pic}\,(X) \neq \mathrm{Pic}\,(X_{\overline{k}})^{G_k}$ and the deviation from equality is characterized by the *period-index obstruction* (see [PS97, §3] for details). Furthermore, the elements of the group $\mathrm{Pic}\,(X_{\overline{k}})$ denote the $\overline{k}$-rational points of the Picard scheme and the action of G_k on both is compatible. Since we will be mostly working with the points on the Picard scheme, we deviate from the standard notation and use the same notation for both. In the next section, we talk about the above mentioned objects more precisely for general "nice" varieties V/k.

1.2 Geometric Preliminaries

In this section, we assume that k is algebraically closed unless stated otherwise. Let V/k be a nice variety. Let $W \subset V$ be an irreducible codimension 1 subvariety of V. Then W formally defines a *prime divisor* on V. The group generated by all (W), i.e., the group of the formal sums of the form

$$\sum_{W \text{prime divisors on V}} n_W(W),$$

where $n_W \in \mathbb{Z}$, and $n_W = 0$ for all but finitely many prime divisors W, is called the group of *Weil divisors* on V denoted by $\mathrm{Div}(V)$. If V/k, W/k are nice varieties and $D \in \mathrm{Div}(V \times W)$, then we define the *transpose divisor* ${}^tD$ of D to be divisor on $W \times V$ that is the image of D under the identification $V \times W \xrightarrow{\simeq} W \times V$. There is a well defined homomorphism $\deg : \mathrm{Div}(V) \to \mathbb{Z}$, given by $\sum_W n_W(W) \mapsto \sum_W n_W$ when V is a curve. Let $\mathrm{Div}^0(V) = \ker(\deg)$. In general, $\mathrm{Div}^0(V)$ is the group of divisors algebraically equivalent to 0 [Lan83, III §1]. Let $f \in k(V)^\times$. Then one can define a divisor associated to f denoted by $\mathrm{div}(f)$ as $\sum_W \mathrm{ord}_W(f)(W)$, where $\mathrm{ord}_W(f)$ is defined as valuation of f in the field of fractions of the discrete valuation ring $\mathcal{O}_{V,W}$ where $\mathcal{O}_V$ is the structure sheaf of V [Har77, II §6]. A divisor $D \in \mathrm{Div}(V)$ is called a *principal divisor* on V, if $D = \mathrm{div}(f)$ for some $f \in k(V)$. The set of principal divisors forms a subgroup of $\mathrm{Div}^0(V)$ [Lan83, III §1] denoted by $\mathrm{Princ}(V)$. One has the following exact sequence

$$0 \to k^\times \to k(V)^\times \to \mathrm{Princ}(V) \to 0. \tag{1.2.1}$$

For non-algebraically closed base fields k we have the following remark:

Remark 1.2.1. Using Hilbert's Theorem 90 and that $\mathrm{H}^1(G_k, \overline{k}^+) = 0$ for any number field k, one can show that the exact sequence (1.2.1) holds for any nice variety defined over k ([Sil09, Exercise 1.12]). One uses the fact that the ideal of an affine patch of the variety $I(V) \subset \overline{k}[X_1, \ldots, X_n]$, is isomorphic to a direct sum of $\overline{k}^+$ as a G_k-module.

We now state the following useful lemma called the moving lemma.

Lemma 1.2.2. [Lan83, VI, §4, Lemma 3] *Let k be a not necessarily algebraically closed field, and V be a "nice" variety over k. Let D be a k-rational divisor and S be a finite set of smooth points of V. Then there exists a function $f \in \overline{k}(V)$ such that no point in S lies in the support of $D + \mathrm{div}(f)$.*

We now give the definition of an abelian variety and in the following two subsections discuss two very important examples of abelian varieties, i.e., Picard and Albanese varieties associated to a "nice" variety V.

Definition 1.2.3. A projective, geometrically irreducible and smooth variety A/k with continuous surjective morphism

$$+ : A \times A \to A \quad \text{and an isomorphism} \quad \iota : A \to A$$

along with a specified point O is called an *abelian variety* denoted by the 4-tuple $(A, +, \iota, O)$, if $+(\_, O) = +(O, \_) = \mathrm{id}$ on A and $+(P, \iota(P)) = +(\iota(P), P) = O$, for each point $P \in A$. We will drop $+, \iota$, and O from the notation in order to ease it. One can show using the theorem of the cube [Lan83, III §2 Theorem 1, 2] and the completeness of A that under these conditions $(A, +, \iota, O)$ forms a commutative group variety.

We will from now on write the evaluation of the map the $+$ on an abelian variety A as $P+Q$ instead of $+(P, Q)$ for points $P, Q \in A$ and $\iota(P)$ as $-P$ for simplicity. A finite surjective morphism of abelian varieties which is also a group homomorphism is called an *isogeny*. Examples of isogenies include the multiplication by n maps. If $\phi : A \to B$ is an isogeny, then recall from §1.1 that $A[\phi]$ denotes the kernel of ϕ considered as a map on $A(k)$. When k is not algebraically closed, then $A[\phi] = \ker(\phi : A(\overline{k}) \to B(\overline{k}))$. This is a finite abelian group, therefore by the structure theorem of finite abelian groups, there exists a unique sequence of integers $n_1, \ldots, n_r$ with $n_i | n_{i+1}$, $n_i > 1$ such that $A[\phi] \simeq \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$. Hence, ϕ is called an $(n_1, n_2, \ldots, n_r)$-*isogeny*.

1.2.1 Picard variety

We have another exact sequence

$$0 \to \mathrm{Princ}(V) \to \mathrm{Div}(V) \to \mathrm{Pic}\,(V) \to 0, \tag{1.2.2}$$

where the quotient $\mathrm{Pic}\,(V)$ is the *Picard group* associated to V. Since $\mathrm{Princ}(V) \subset \mathrm{Div}^0(V)$, one can safely define the quotient $\mathrm{Pic}^{\,0}(V) \coloneqq \mathrm{Div}^0(V)/\mathrm{Princ}(V)$, which is the algebraically equivalent to zero part of the Picard group. It is possible to give a variety structure on $\mathrm{Pic}^{\,0}(V)$ if V is nice, and so it is called *Picard variety* associated to V. As remarked before we will abuse the notation and denote both the Picard variety, and the algebraically equivalent to zero part of the Picard group by $\mathrm{Pic}^{\,0}(V)$ because we will be mostly working with points on the Picard variety. The Picard variety is an abelian variety with the group structure induced by the natural group structure on $\mathrm{Pic}^{\,0}(V)$. Furthermore, if k is not algebraically closed, then the Picard variety is defined over k, and its $\overline{k}$-rational points are given by elements of $\mathrm{Pic}^{\,0}(V_{\overline{k}})$.

1.2.2 Albanese variety

One can associate another abelian variety to V, called the *Albanese variety*, denoted by the pair $(\mathrm{Alb}(V), \phi_{V,P_0})$, where $\phi_{V,P_0} : V \to \mathrm{Alb}(V)$ is a morphism such that

$\phi_{V,P_0} = 0$, and is called the *Albanese morphism*. The Albanese morphism depends on the choice of a base point $P_0 \in V(k)$. The Albanese variety is universal in the sense that for any rational map $g : V \to B$, where B is an abelian variety, there is a unique homomorphism $g_* : \mathrm{Alb}(V) \to B$, and $P \in B$ such that $g = g_* \circ \phi_{V,P_0} + P$. For a proof that $\mathrm{Alb}(V)$ always exists see [Lan83, Theorem 11, II §3]. Furthermore, there exists an $n \in \mathbb{Z}_+$ such that $\mathrm{Alb}(V)$ is the image of the natural map $\phi_{V,P_0}(V)^n \to \mathrm{Alb}(V)$ given by $(P_1, P_2, \ldots, P_n) \mapsto \sum_i P_i$. In view of the above, we obtain the following exact sequence

$$0 \to \mathcal{Y}(V) \to \mathcal{Z}^0(V) \to \mathrm{Alb}(V) \to 0, \tag{1.2.3}$$

where $\mathcal{Z}(V)$ is the group of 0-dimensional algebraic cycles on V (roughly one can think of it as a free abelian group supported on the points of V), $\mathcal{Z}^0(V)$ is the subgroup of degree zero 0-dimensional cycles, and $\mathcal{Y}(V)$ denotes the kernel of the map $\mathcal{Z}^0(V) \to \mathrm{Alb}(V)$ defined by $\sum_P n_P(P) \mapsto \sum_P n_P \phi_{V,P_0}(P)$. We will usually denote the Albanese variety by $\mathrm{Alb}(V)$ instead of a pair. The universal property of the Albanese variety implies that $\mathrm{Alb}(A) \simeq A$, when A is an abelian variety, via $P \mapsto [(P) - (O)]$, for $P \in A$.

Remark 1.2.4. Both $\mathrm{Alb}(V)$ and the Picard variety are defined over k even if k is not algebraically closed. Note that the field of definition of the morphism ϕ_{V,P_0} depends on the choice of P_0; hence, if $V(k) \neq \emptyset$, then the morphism $V \to \mathrm{Alb}(V)$ can be defined over k.

Remark 1.2.5. Let k be a number field and V/k, and W/k be two "nice" varieties. Let $\phi : V \to W$ be a rational map defined over k. Then we have natural maps $\phi_* : \mathrm{Alb}(V) \to \mathrm{Alb}(W)$ and $\phi^* : \mathrm{Pic}^0(W_{\overline{k}}) \to \mathrm{Pic}^0(V_{\overline{k}})$ induced from the natural maps on $\mathcal{Z}^0(V_{\overline{k}})$ and $\mathrm{Div}^0(V_{\overline{k}})$ such that ϕ_* and ϕ^* are defined over k. Furthermore, $\mathrm{Pic}^0(\mathrm{Alb}(V)_{\overline{k}}) \simeq \mathrm{Pic}^0(V_{\overline{k}})$. The Picard variety $\mathrm{Pic}^0(A_{\overline{k}})$ of an abelian variety A is also called the dual abelian variety and is denoted by $\widehat{A}$.

Furthermore, for the case of a "nice" curve X, the Picard and the Albanese varieties are canonically isomorphic because both $\mathcal{Z}^0(X)$ and $\mathrm{Div}^0(X)$ are supported on points of X and the universal property of the Albanese variety implies that $\mathcal{Y}(X) = \mathrm{Princ}(X)$. The Albanese variety associated to a curve is called its *Jacobian variety* and is denoted by J_X or $\mathrm{Jac}\,(X)$. We will drop the dependence of J_X or $\mathrm{Jac}\,(X)$ on X when it is clear from the context. We will identify J_X with $\mathrm{Pic}^0(X)$. The Jacobian varieties are self-dual and under sufficiently nice conditions one can get an embedding $X \hookrightarrow J_X$ defined even over the non-algebraically closed base field k, for example, if $\mathrm{Div}^1(X) := \{D \in \mathrm{Div}(X) \mid \deg(D) = 1\} \neq \emptyset$. We will discuss this in slightly more detail in §1.2.4.

1.2.3 Correspondences

Definition 1.2.6. Let V and W be "nice" varieties. Then a *correspondence* of V and W (for us) is a divisor on $V \times W$. In general, one can give the definition for a d-dimensional algebraic cycle.

Example 1.2.7.

- Let X be a codimension 1 subvariety of V. Then $X \times W$ is a correspondence on $V \times W$. Similarly, $V \times X$ is a correspondence if X is a codimension 1 subvariety of W.

- If D is a correspondence on $V \times W$, then ${}^tD$, called the *transpose correspondence*, is a correspondence on $W \times V$.

- Let p_1 and p_2 be the projection morphism from $V \times W$ to V and W, respectively. Then $p_i^*(D_i)$ is a correspondence on $V \times W$, where D_1, D_2 are divisors on V and W, respectively. One can identify the group generated by divisors D on V under the map p_1^* with $\mathrm{Div}(V)$ and similarly for W. Hence, we can identify the group generated by p_i^* with $\mathrm{Div}(V) \times \mathrm{Div}(W)$. Such correspondences are called *fibral correspondence* in case when V and W are curves, and the group of fibral correspondences is denoted by $\mathrm{Fib}(V \times W) \simeq \mathrm{Div}(V) \times \mathrm{Div}(W)$.

- A correspondence D is *prime, effective or principal*, respectively, if D is a prime, effective or principal as a divisor on $V \times W$.

Let V and W be nice varieties, let $v \in V(\overline{k})$ be a point on V, and let $D \in \mathrm{Div}(V \times W)$ be a correspondence such that $\{v\} \times W$ is not contained in D. Then $i_v^*(D)$ is a divisor on W, where i_v^* is the pull-back homomorphism induced by the morphism $i_v : W \to V \times W$ defined by $w \mapsto (v, w)$. Concretely, this is basically restricting the divisor D to the first coordinate v whenever we can. We denote this by $D(v)$. One can extend this linearly to define a partial map $D : \mathcal{Z}(V) \to \mathrm{Div}(W)$ whenever this makes sense. By the definition of algebraic equivalence, we have $D(\mathfrak{v}) \in \mathrm{Div}^0(W)$, for $\mathfrak{v} \in \mathcal{Z}^0(V)$.

Applying the above construction with V and W replaced by abelian varieties A and B, respectively, we have by [Lan83, III,§3, Corollary 2] that $D(\mathfrak{v}) \in \mathrm{Princ}(B)$ for every $\mathfrak{v} \in \mathcal{Y}(A)$; hence, by the moving lemma 1.2.2, the partial map $\lambda_D : \mathcal{Z}^0(A) \to \mathrm{Div}^0(B)$ given by $\mathfrak{v} \mapsto D(\mathfrak{v})$ induces a homomorphism $\lambda_D : A \to \mathrm{Pic}^0(B)$. Recall that the universal property of the Albanese variety implies that $\mathrm{Alb}(A) \simeq A$ via $P \mapsto [(P) - (O)]$, so for $D \in \mathrm{Div}(A \times B)$, one obtains homomorphisms $\lambda_D : A \to \mathrm{Pic}^0(B)$ and $\lambda_{{}^tD} : B \to \mathrm{Pic}^0(A)$.

Now we recall the definition of the dual of an abelian variety.

Definition 1.2.8. An abelian variety B is called the *dual abelian variety* of A denoted by $\widehat{A}$, if there exists a divisor $\mathcal{P} \in \mathrm{Div}(A \times B)$ with the property that the maps $\lambda_{{}^t\mathcal{P}} : B \to \mathrm{Pic}^0(A)$ and $\lambda_{\mathcal{P}} : A \to \mathrm{Pic}^0(B)$ given by $b \mapsto [{}^t\mathcal{P}(b) - {}^t\mathcal{P}(O)]$ and $a \mapsto [\mathcal{P}(a) - \mathcal{P}(O)]$, respectively, are isomorphisms. The divisor $\mathcal{P}$ is called the *Poincaré divisor* or the *Poincaré correspondence*. Theorem 1.2.10 implies that the isomorphisms $\lambda_{{}^t\mathcal{P}}$ and $\lambda_{\mathcal{P}}$ depend only on the correspondence class in $\frac{\mathrm{Pic}(A\times B)}{\mathrm{Pic}(A)\times\mathrm{Pic}(B)}$.

Proposition 1.2.9. [Lan83, IV, §4, Theorem 10] *For every abelian variety A, a dual abelian variety $\widehat{A}$ (unique up to isomorphism) exists along with the Poincaré class $\mathcal{P}$.*

An ample divisor D on A defines an isogeny $\lambda_D : A \to \widehat{A}$ given by $a \mapsto t_a^*(D) - D$, where $t_a : A \to A$ is the translation by a map defined as $P \mapsto P + a$. Such an isogeny λ_D is called a *polarization*. If k is not algebraically closed, then D is allowed to be in $\mathrm{Div}(A_{\overline{k}})$ but λ_D must be defined over k. If the polarization is an isomorphism, then it is called a *principal polarization*. Note that we have abused the notation by using λ_D for polarization arising from an ample divisor and for the homomorphism induced by a correspondence D on $V \times W$, for some nice varieties V and W. However, given $D \in \mathrm{Div}(A)$ one obtains a divisor $+^*(D) \in \mathrm{Div}(A \times A)$, where $+ : A \times A \to A$ is the addition operation on A. In this sense, $\lambda_{+^*(D)}$ defines the same homomorphism as the polarization λ_D; hence, the abuse of notation is justified.

Let A_V and A_W be the Albanese varieties of V and W, respectively, with morphisms $\phi_V : V \to A_V$ and $\phi_W : W \to A_W$, and Picard varieties identified with $\widehat{A_V}$ and $\widehat{A_W}$. Here we have dropped the dependence on the choice of basepoints in the definitions of ϕ_V and ϕ_W in order to simplify the notation. We now discuss the connection between $\mathrm{Div}(V \times W)$ and $\mathrm{Hom}(A_V, \widehat{A_W})$. Let $D' \coloneqq (\phi_V \times \phi_W)^*(D) \in \mathrm{Div}(V \times W)$; hence, D' defines a well-defined homomorphism $A_V \to \widehat{A_W}$ via the following diagram:

$$\begin{array}{ccc} \mathrm{Div}(A_V \times A_W) & \xrightarrow{D \mapsto \lambda_D} & \mathrm{Hom}(A_V, \widehat{A_W}) \\ \Big\downarrow{\scriptstyle (\phi_V \times \phi_W)^*(D)} & & \Big\| \\ \mathrm{Div}(V \times W) & \xrightarrow{D' \mapsto \lambda_{D'}} & \mathrm{Hom}(A_V, \widehat{A_W}). \end{array}$$

The following theorem discusses some properties of the maps in the above diagram.

Theorem 1.2.10. [Lan83, VI, §2, Theorem 2] *Call correspondences $D, D' \in \mathrm{Div}(V \times W)$ for nice varieties V and W equivalent, if D and D' differ by a divisor of the form $V \times Y + X \times W + \mathrm{div}(f)$, for some divisor X on V, some divisor Y on W, and $f \in k(V \times W)^\times$. The group of correspondence classes can be identified with*

$$\frac{\mathrm{Pic}(V \times W)}{\mathrm{Pic}(V) \times \mathrm{Pic}(W)},$$

and we have the following isomorphism of groups:

$$\frac{\mathrm{Pic}(V \times W)}{\mathrm{Pic}(V) \times \mathrm{Pic}(W)} \xrightarrow{\simeq} \mathrm{Hom}(A_V, \widehat{A_W}).$$

Moreover, if V and W are replaced with their Albanese varieties A_V and A_W, then we have the following commutative diagram.

$$\begin{array}{ccc} \frac{\mathrm{Pic}\,(V\times W)}{\mathrm{Pic}\,(V)\times\mathrm{Pic}\,(W)} & \xrightarrow{D'\mapsto\lambda'_D} & \mathrm{Hom}(A_V,\widehat{A_W}) \\ {\scriptstyle(\phi_V\times\phi_W)^{-1}(D')}\uparrow & & \downarrow{\scriptstyle =} \\ \frac{\mathrm{Pic}\,(A_V\times A_W)}{\mathrm{Pic}\,(A_V)\times\mathrm{Pic}\,(A_W)} & \xrightarrow{D\mapsto\lambda_D} & \mathrm{Hom}(A_V,\widehat{A_W}). \end{array}$$

Since we are going to be mainly dealing with curves, we recall some properties of correspondences when V and W are "nice" curves. Recall that $\mathrm{Div}(X)\simeq\mathcal{Z}(X)$ for a curve X. For a prime correspondence C on $V\times W$ we have

$$\mathrm{Div}(V)\xrightarrow{(p_1^C)^*}\mathrm{Div}(C)\xrightarrow{(p_2^C)_*}\mathrm{Div}(W),$$

where p_i is the projection map on ith component as before.

Proposition 1.2.11. [Smi05, Theorem 3.3.12]

Let V and W be nice curves. Then the following hold:

- *There is a well-defined map*

$$\phi:\mathrm{Div}(V\times W)\to\mathrm{Hom}(J_V,J_W),\quad \sum_i n_iC_i\mapsto\sum_i n_i(p_2^{C_i})^*\circ(p_1^{C_i})_*,$$

  which induces a well defined surjective *homomorphism*

$$\phi:\mathrm{Pic}\,(V\times W)\to\mathrm{Hom}(J_V,J_W)$$

  with kernel as the image of $\mathrm{Fib}(V\times W)$ *inside* $\mathrm{Pic}\,(V\times W)$*. Identifying the image of* $\mathrm{Fib}(V\times W)$ *with* $\mathrm{Pic}\,(V)\times\mathrm{Pic}\,(W)$

$$\mathrm{Hom}(J_V,J_W)\simeq\frac{\mathrm{Pic}\,(V\times W)}{\mathrm{Pic}\,(V)\times\mathrm{Pic}\,(W)},$$

  i.e., $\mathrm{Hom}(J_V,J_W)$ *measures how far* $\mathrm{Pic}\,(V\times W)$ *is from* $\mathrm{Pic}\,(V)\times\mathrm{Pic}\,(W)$*.*

- *There is a composition law on correspondences which in case when $V=W$ translates to the composition on endomorphisms. In other words, under the above mentioned composition law on correspondences we have the following ring isomorphism*

$$\mathrm{Pic}\,(V\times V)/\mathrm{Fib}(V\times V)\cong\mathrm{End}(J_V).$$

- *In particular, the diagonal correspondence $\Delta_V:=\{(v,v):v\in V\}$ induces the identity map on J_V.*

1.2.4 Jacobians of curves

Let C/k be a "nice" curve of genus $g > 0$. Then J_C is an abelian variety of dimension g (this is also true for $g = 0$ in which case $J_C = 0$). Recall that J_C is identified with $\mathrm{Pic}^0(C)$. Therefore, we would like to get hold of points on J_C in terms of the points of C. If k is not algebraically closed and C is defined over k, then J_C is also defined over k. Furthermore, if D is a k-rational divisor on C of degree 1, then the map $\alpha_D : C_{\overline{k}} \to \mathrm{Pic}^0(C_{\overline{k}})$ defined by $P \mapsto [(P) - (D)]$ is an embedding of C in J_C defined over k.

Proposition 1.2.12. [Sto, Corollary 4.14] *Identify J_C with $\mathrm{Pic}^0(C)$, and let Q be a point in $J_C(k)$. Then there is an effective divisor D_Q with $\deg(D_Q) \leq g$ such that $[D_Q - \deg(D_Q)D] = Q$. Furthermore, if k is not algebraically closed, D is k-rational, and $\deg(D_Q)$ is minimal possible, then D_Q is k-rational.*

One can extend α_D to a map of sets $C^{(r)} \to J_C$, which also turns out to be a morphism of varieties, where $C^{(r)}$ is the *r-symmetric product* of C, obtained by quotienting out the natural action of the symmetric group on r-points, S_r on C^r. The map $\alpha_D : C^{(r)} \to J_C$ is given by $(P_1, \ldots P_r) \mapsto \sum_{i=1}^{r} \alpha_D(P_i)$. Let Θ be the image of $C^{(g-1)}$ inside J. We have the following proposition:

Proposition 1.2.13. [HS00, Theorem A.8.1.1]

- *If $r \leq g$, then the image of $C^{(r)}$ is a dimension r subvariety of J_C.*
- *Θ is an ample divisor on J_C.*

For a more complete construction of the Jacobian variety and why it is defined over the base field see [Lan83, III, §2, Lemma 5, Theorem 8, 9, and 10]. Since Θ is an ample divisor, recall from §1.2.3 that one can define a polarization $\lambda_\Theta : J_C \to \widehat{J_C}$ via $P \mapsto [t_P^*(\Theta) - \Theta] = [\Theta_{-P} - \Theta]$, where Θ_{-P} is the translate of Θ under the t_{-P} map. The following proposition tells us more about λ_Θ.

Proposition 1.2.14. [Lan83, VI, §3, Theorem 3] *The polarization λ_Θ is principal and a Poincaré divisor on $J_C \times J_C$, by identifying J_C with $\widehat{J_C}$ using λ_Θ, is given by*

$$+^*(\Theta) = +^{-1}(\Theta).$$

Moreover, if k is not algebraically closed and $Q \in \mathrm{Pic}^0(J_{\overline{k}})$ is rational over an extension K of k, then the point P such that Q is represented by $\Theta_{-P} - \Theta$ is also K-rational, provided Θ is K-rational.

Recall from theorem 1.2.10 the isomorphism between correspondence classes and homomorphism groups of Albanese varieties. For a curve C the following proposition states concretely the homomorphism $\lambda_{\mathcal{P}}$ induced by $\mathcal{P}$ as in the above proposition.

Proposition 1.2.15. *Let $\mathcal{P} \in \mathrm{Div}(J_C \times J_C)$ be the Poincaré divisor as in Proposition 1.2.14. Then the homomorphism $\lambda_{\mathcal{P}} : J_C \to \widehat{J_C} \overset{\lambda_\Theta^{-1}}{\to} J_C$ induced by $\mathcal{P}$ is the identity map. In particular, the homomorphism* id *induced by the correspondence class of $\Delta \in \mathrm{Div}(C \times C)$, where Δ as before is the diagonal correspondence, is the same as $\lambda_{\mathcal{P}}$.*

Proof. Let $\mathcal{P} \in \mathrm{Div}(J_C \times J_C)$ be the Poincaré divisor as above. For $P \in J_C$, we have $[\mathcal{P}(P) - \mathcal{P}(O)] = [\Theta_{-P} - \Theta] \in \mathrm{Pic}^0(J_C)$. However, the map $\lambda_\Theta^{-1} : \widehat{J_C} \overset{\simeq}{\to} J_C$ maps the class of divisor $\Theta_{-P} - \Theta$ to P. Hence, the correspondence class of $\mathcal{P}$ maps to $\mathrm{id} \in \mathrm{Hom}(J_C, J_C)$, which is the image of the class of Δ correspondence on $C \times C$. □

1.2.5 Mumford representation on odd-degree hyperelliptic Jacobians

In this section we assume that the base field k is not necessarily algebraically closed. Let $C : y^2 = f(x)$ be an odd-degree hyperelliptic curve, i.e., $\deg(f) = 2g + 1$, of genus g, and view C as a curve in the weighted projective space $\mathbb{P}^2(1, g+1, 1)$. Then there is a unique point at infinity denoted by ∞ on C and given by $(1 : 0 : 0)$ in the weighted projective space $\mathbb{P}^2_{(1,g+1,1)}$. By Proposition 1.2.13 one can uniquely represent every point in $J_C(\overline{k})$ by an effective divisor of degree at most g.

Definition 1.2.16. A divisor D on $C_{\overline{k}}$ is said to be a *divisor in general position* if D is effective, $\infty \notin \mathrm{Supp}(D)$ and $D \not\geq P + \iota(P)$, for any point $P \in C(\overline{k})$, where $\iota : C \to C$ is the hyperelliptic involution given by $(x, y) \mapsto (x, -y)$, and the order $\geq$ is defined pointwise.

We now define the Mumford representation of points on an odd–degree hyperelliptic Jacobian.

Definition 1.2.17. [Sto, Lemma 4.16]

Let D be a divisor in general position on the odd–degree hyperelliptic curve. Then there are unique polynomials a, b such that

- a is monic with $\deg(a) = \deg(D)$,
- $\deg(b) < \deg(a)$,
- $f \equiv b^2 \mod a$,
- Let $P = (x, y) \in C(\overline{k})$. Then

$$P \in \mathrm{Supp}(D) \iff a(x) = 0 \text{ and } b(x) = y.$$

Furthermore, $v_P(D)$ is the multiplicity of x as a root of a.

The pair (a, b) is called the *Mumford representation* associated to a divisor D in general position.

Now if we can represent every point on J as a divisor in general position of degree at most g, then every point on J can be presented using the Mumford representation. The following theorem states this precisely.

Proposition 1.2.18. [Sto, 4.17] *Let C/k be an odd-degree hyperelliptic curve with Jacobian J and $P \in J(k)$ be a point. Then there is a unique divisor in general position D with $\deg(D) \leq g$ such that $P = [D - \deg(D)\infty]$. Additionally, the uniqueness of D implies that D is k-rational. In particular, there exists a Mumford representation (a, b) for P with a, b defined over $k[T]$.*

For working with odd-degree hyperelliptic curves we will be mainly using the Mumford representation of points.

1.3 Group Cohomology

In this section we recall some relevant definitions and results related to group cohomology and in particular Galois cohomology. Let G be a *topological group*, i.e., a group with a topology defined such that the group operations: $- : G \to G$ (given by $g \mapsto -g$), and $+ : G \times G \to G$ (given by $g_1, g_2 \mapsto g_1 + g_2$) are continuous maps.

Example 1.3.1.

1. Groups with discrete topology.

2. Let I be a partially ordered index set and G_i be a sequence of finite groups with morphisms $f_{ij} : G_j \to G_i$, if $j \geq i$. Moreover, if m, n, o, p are such that $p \geq n$, $p \geq o$, $n \geq m$, and $o \geq m$, then the composition $f_{mo} \circ f_{op} = f_{mn} \circ f_{np}$. Then the inverse limit $G_I := \varprojlim_I G_i \subset \prod_{i \in I} G_i$ is called a profinite group. Examples are absolute Galois groups of number fields and $\mathbb{Z}_p$. Profinite groups have a topology coming from the subspace topology of the product space $\prod_{i \in I} G_i$, with a basis of open sets as left or right cosets of finite index subgroups of G_I.

3. The groups $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$ under their usual topology.

For a topological group G and a G-module M with discrete topology we define

Definition 1.3.2. For each $n \geq 1$, define the set $\mathrm{C}^n(G, M)$ of *n-cochains* to be the group of continuous maps $m : G^n \to M$. In particular, $\mathrm{C}^0(G, M) = M$.

For each $n \geq 0$, we define the maps $\partial_n : \mathrm{C}^n(G, A) \to \mathrm{C}^{n+1}(G, A)$ by

$$\begin{aligned}\partial m(g_1, \ldots, g_{n+1}) &:= g_1 m(g_2, \ldots, g_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i m(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) + m(g_1, \ldots, g_n)\end{aligned}$$

One can directly check that $\partial_n \circ \partial_{n+1} = 0$. Therefore, we obtain a chain complex

$$0 \to M \xrightarrow{\partial_0} \mathrm{C}^1(G, M) \xrightarrow{\partial_1} \mathrm{C}^2(G, M) \xrightarrow{\partial_2} \cdots . \tag{1.3.1}$$

Given a complex computing the deviation from exactness is a natural thing to do. This motivates following definitions

Definition 1.3.3.

1. The group $\mathrm{Z}^n(G, M)$ of *n-cocycles* is defined as $\ker(\partial_n)$.
2. A cocycle x is called a *normalized cocycle* if $x(\mathrm{id}, \ldots, \mathrm{id}) = 0$.
3. The group $\mathrm{B}^n(G, M)$ of *n-coboundaries* is defined as $\mathrm{Im}(\partial_{n-1})$.
4. The group $\mathrm{H}^n(G, M) := \mathrm{Z}^n(G, M)/\mathrm{B}^n(G, M)$ of *n-cohomology classes* computes the deviation of the chain complex (1.3.1) from exactness.

Definition 1.3.4. We will say that a definition (property) which is stated (holds true) for cohomology classes holds at the *level of cochains or cocycles*, if the definition (property) can be made (remains true) when the cohomology groups are replaced by the corresponding group of cochains/cocycles. We will use the acronym *ATLOC* for this.

Remark 1.3.5. Throughout this section we will keep track of which definitions / propositions work at the level of cochains / cocycles, and will give the definition explicitly in terms of cochains / cocycles whenever / wherever possible.

Example 1.3.6.

1. One can easily check that $\mathrm{Z}^0(G, M) = M^G$. Furthermore, if G has a trivial action on M, then $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$.
2. Every cohomology class can be represented by a normalized cocycle. This follows from the definition of cocycles in odd dimension, and for even dimensions shift the given cocycle $x \in \mathrm{Z}^{2n}(G, M)$ by the coboundary ∂y, where

$$y(\bar{g}) := x(\underbrace{\mathrm{id}, \ldots, \mathrm{id}}_{2n \text{ times}}),$$

for all $(2n-1)$-tuples $\bar{g} \in G^{2n-1}$.

3. If $f : M \to M'$ is a map of G-modules, then we obtain a push-forward of f, $f_* : \mathrm{C}^n(G, M) \to \mathrm{C}^n(G, M')$, for each $n \geq 0$, defined canonically by $f_*(x)(g_1, \ldots, g_n) \mapsto f(x(g_1, \ldots, g_n))$. It is immediate from the definitions that f_* commutes with ∂_n, and therefore induces a map $f_* : \mathrm{H}^n(G, M) \to \mathrm{H}^n(G, M')$.

For a subgroup H of G, and for each $n \geq 0$, we have a natural map called the *restriction* homomorphism $\mathrm{res}^H_G : \mathrm{C}^n(G, M) \to \mathrm{C}^n(H, M)$, via $m \mapsto m\big|_{H^n}$. If H is a normal subgroup of G, then we obtain the *inflation* homomorphism $\mathrm{inf}^G_{G/H} : \mathrm{C}^n(G/H, M^G) \to \mathrm{C}^n(G, M)$ explicitly given by

$$(\mathrm{inf}(m))(g_1, \ldots, g_n) = m(g_1 H, \ldots, g_n H).$$

One can directly verify that both res and inf take cocycles to cocycles and coboundaries to coboundaries. We denote the induced maps at the level of cohomology classes also by res and inf, and for $n > 0$ and H a normal subgroup of G, inf and res fit in a complex called *inflation-restriction sequence* as follows

$$\mathrm{H}^n(G/H, M^G) \xrightarrow{\mathrm{inf}} \mathrm{H}^n(G, M) \xrightarrow{\mathrm{res}} \mathrm{H}^n(H, M). \tag{1.3.2}$$

One can define an action of G on the group of $\mathrm{C}^n(G, \_)$ via a map called *conjugation* homomorphism turning it into a G-module. Let H be a subgroup of G, let N be a H-submodule of M, and let $g \in G$. Then we have a map

$$g_* : \mathrm{C}^n(H, N) \to \mathrm{C}(gHg^{-1}, gN), \qquad g_*(m)(gg_1g^{-1}, \ldots, gg_ng^{-1}) = gm(g_1, \ldots, g_n).$$

It is a direct computation to show that conjugation commutes with the ∂ operator, and therefore induces an action on the cohomology classes which we will again denote by g_*, for $g \in G$. Let $g \in G$, and let M be a G-module. Then g_* is the identity map on $\mathrm{H}^n(G, M)$. This is easy to see for dimension 0, and for higher dimensions, it follows by dimension shifting (see §1.3.2 for details). In particular, for a normal subgroup H of G, H acts trivially on $\mathrm{H}^n(H, M)$, and we obtain a valid action of G/H on $\mathrm{H}^n(H, M)$. In view of the above definition and for $n > 0$, one can refine the complex (1.3.2) to obtain the following, which we again call the *inflation-restriction sequence*

$$\mathrm{H}^n(G/H, M^G) \xrightarrow{\mathrm{inf}} \mathrm{H}^n(G, M) \xrightarrow{\mathrm{res}} \mathrm{H}^n(H, M)^{G/H}. \tag{1.3.3}$$

The following proposition gives a condition when the above sequence is exact.

Proposition 1.3.7. [NSW08, Proposition 1.6.6, 1.6.7]

1. *The complex* (1.3.3) *is always exact in dimension 1. The exactness holds also at the level of 1-cocycles.*

2. *If* $\mathrm{H}^i(H, M) = 0$, *for all* $0 \leq i \leq n-1$, *then the complex* (1.3.3) *is exact. Moreover, this does not hold at the level of cocycles. Assuming that for* $0 \leq i \leq$

$n-1$, $\mathrm{H}^i(H,M)=0$, *one can extend* (1.3.3) *to a five term exact sequence given by*

$$0 \to \mathrm{H}^n(G/H, M^G) \xrightarrow{\inf} \mathrm{H}^n(G,M) \xrightarrow{\mathrm{res}} \mathrm{H}^n(H,M)^{G/H} \xrightarrow{\mathrm{tg}} \mathrm{H}^{n+1}(G/H, M^G) \xrightarrow{\inf} \mathrm{H}^{n+1}(G,M),$$

where the map $\mathrm{tg} : \mathrm{H}^n(H,M)^{G/H} \to \mathrm{H}^{n+1}(G/H, M^G)$ *is called the* transgression *map.*

3. *In particular, we always have the five term exact sequence in dimension 1. The injectivity of the map* $\inf : \mathrm{H}^1(G/H, M^H) \to \mathrm{H}^1(G,M)$ *follows from* $A^G \simeq (A^H)^{G/H}$.

4. *The transgression map in dimension 1 is concretely given as follows. Let* $s : G/H \to G$ *be a continuous section of the quotient* $G \to G/H$ *such that* $s(\mathrm{id}\,) = \mathrm{id}\,$. *Note that* s *can be chosen to be continuous because the quotient map is an open map. Let* x *be a 1-cocycle representing a class in* $\mathrm{H}^1(H,M)^{(G/H)}$ *and define* $y \in \mathrm{C}^1(G/H, M)$ *by*

$$s(\overline{g})_*(x)(h) - x(h) = h(y(\overline{g})) - y(\overline{g}),$$

for $\bar{g} \in G/H$ *and* $h \in H$. *Extend* y *to define a cochain* $y : G \to M$, *by defining* $y(s(\overline{g})h) = y(\overline{g}) + s(\overline{g})x(h)$, *for* $\overline{g} \in G/H$ *and* $h \in H$. *Then* $\partial y \in \mathrm{Z}^2(G/H, M^H)$ *and* $\mathrm{tg}([x])$ *is given by* $[\partial y]$.

If H is a finite index subgroup of G and M a G-module, then one can define a norm map $M^H \to M^G$ given by $m \mapsto \sum_{\bar{g} \in G/H} gm$. Such a map can be defined for all dimensions. Since res is induced by the inclusion $H \hookrightarrow G$, the map induced on the cochains in the opposite direction is called *corestriction*. Let R be a system of right coset representatives of G/H, and $r : G \to R$ be the map that maps an element g to the corresponding right coset representative in R and $c : G \to H$ be defined by $g \mapsto gr(g)^{-1}$. Now using the definition of the corestriction map in the standard resolution in [NSW08, §I.5.4] we get the following definition of the corestriction map in the bar resolution (which is what we are working with).

Definition 1.3.8. Let H be a subgroup of finite index inside G. Then corestriction is a homomorphism $\mathrm{cor}^G_H : \mathrm{C}^n(H,M) \to \mathrm{C}^n(G,M)$ explicitly given by

$$\mathrm{cor}^G_H(x)(g_1,\ldots,g_n) := \sum_{g \in R} g^{-1} x(c(gg_1), \ldots, c(gg_1 \ldots g_{i-1})^{-1} c(gg_1 \ldots g_i), \\ \ldots, c(gg_1 \ldots g_{n-1})^{-1} c(gg_1 \ldots g_n)).$$

Remark 1.3.9. The above explicit definition of the corestriction morphism at the level of cochains depends on the choice of coset representatives. The definition becomes independent for 0-cocycles and only for cohomology classes in higher dimensions.

Definition 1.3.10. Let M and M' be G-modules. Then $M \otimes M'$ is also a G-module with the natural action $g \cdot (x \otimes y) \coloneqq g \cdot x \otimes g \cdot y$. Then *cup product* $\cup : \mathrm{C}^p(G, M) \times \mathrm{C}^q(G, M') \to \mathrm{C}^{p+q}(G, M \otimes M')$ is defined by

$$x \cup y(g_1, \ldots, g_p, g'_1, \ldots, g'_q) := x(g_1, \ldots, g_p) \otimes g_1 \ldots g_p y(g'_1, \ldots, g'_q).$$

One can check that $\cup$ respects the ∂_p and ∂_q operators; hence, induces the cup product at the level of cohomology classes which we will again denote by $\cup$. Let $B : M \times M' \to N$ be a bilinear map of G-modules. Then by the universal property of the tensor products one defines a pairing map $\cup_B : \mathrm{C}^p(G, M) \times \mathrm{C}^q(G.M') \to \mathrm{C}^{p+q}(N)$ induced by the cup product and B. We will represent the induced map on the corresponding cohomology classes also by $\cup_B$. The following proposition states the interplay between all the above defined maps.

Proposition 1.3.11. [NSW08, Proposition 1.5.2–1.5.7]

The following hold ATLOC unless specified otherwise:

1. $\partial \circ \mathrm{res} = \mathrm{res} \circ \partial$.
2. $\partial \circ \mathrm{cor} = \mathrm{cor} \circ \partial$.
3. $\partial \circ g_* = g_* \circ \partial$.
4. *For* $x \in \mathrm{C}^p(G, M)$ *and* $y \in \mathrm{C}^q(G, M')$, $\partial(x \cup y) = \partial x \cup y + (-1)^p x \cup \partial y$.
5. *For* H *a finite index subgroup of* G, $\mathrm{cor} \circ \mathrm{res} = [G : H]$.
6. *For* H *and* U *closed subgroups of* G *with* H *being finite index in* G *we have*

$$\mathrm{res}^U_G \mathrm{cor}^G_H(z) = \sum_{g \in R} \mathrm{cor}^U_{U \cap gHg^{-1}} \mathrm{res}^{U \cap gHg^{-1}}_{gHg^{-1}} g_*(z), \tag{1.3.4}$$

   where R *is a system of double coset representatives of* $G = \bigsqcup_{g \in R} UgH$, *and* $z \in \mathrm{C}^i(H, A)$ *(*$\sqcup$ *denotes the disjoint union). This is known as the* double-coset formula .

7. *For any* $g \in G$, *and a subgroup* H *of* G, $g_* \circ \mathrm{res}^H_G = \mathrm{res}^{gHg^{-1}}_G \circ g_*$, *and if* H *is finite index in* G, *then* $g_* \circ \mathrm{cor}^G_H = \mathrm{cor}^G_{gHg^{-1}} \circ g_*$.
8. *For* $x \in \mathrm{C}^p(G, M)$ *and* $y \in \mathrm{C}^q(G, M)$, *we have* $\mathrm{res}(x) \cup \mathrm{res}(y) = \mathrm{res}(x \cup y)$.
9. *For a finite index subgroup* H *of* G, $x \in \mathrm{H}^p(G, M)$, *and* $y \in \mathrm{H}^q(H, M)$, $x \cup \mathrm{cor}(y) = \mathrm{cor}(\mathrm{res}(x) \cup y)$.
10. *Let* $f : M \to M'$ *be a homomorphism of* G*-modules. Then the maps* res, cor, inf, ∂ *and* g_* *commute with* f_*.

11. *Let $f : M \to M'$ and $g : N \to N'$ be maps of G-modules. Then we have $f_*(x) \cup g_*(y) = (f \otimes g)_*(x \cup y)$, where $f \otimes g : M \otimes N \to M' \otimes N'$ is the natural map defined by $m \otimes n \mapsto f(m) \otimes g(n)$.*

12. *We have*

    (a) $\mathrm{H}^q(G, \bigoplus_{i\in I} M_i) \simeq \bigoplus_{i\in I} \mathrm{H}^q(G, M_i)$.

    (b) $\mathrm{H}^q(G, \prod_{i\in I} M_i) \simeq \prod_{i\in I} \mathrm{H}^q(G, M_i)$.

    Furthermore, these isomorphisms are explicit ATLOC.

13. *Let $K \subset H \subset G$ be a sequence of subgroups of G. Then $\mathrm{cor}^G_H \circ \mathrm{cor}^H_K = \mathrm{cor}^G_K$ and $\mathrm{res}^K_H \circ \mathrm{res}^H_G = \mathrm{res}^K_G$. If H and K are normal in G, then $\inf^G_{G/K} \circ \inf^{G/K}_{G/H} = \inf^G_{G/H}$.*

The following proposition states a condition when part 9 of the above proposition holds at the level of cochains.

Proposition 1.3.12. *Let H be a subgroup of G and R a system of right coset representatives of H in G. Recall the maps $r : G \to R$ and $c : G \to H$ from the Definition 1.3.8. Let $x \in \mathrm{C}^p(G, M)$ be such that for all $g \in R$ and $\sigma_1, \ldots, \sigma_p \in G$*

$$g^{-1}(x(c(g\sigma_1), \ldots, c(g\sigma_1 \cdots \sigma_{p-1})^{-1} c(g\sigma_1 \cdots \sigma_p)) = x(\sigma_1, \ldots, \sigma_p).$$

Then for $y \in \mathrm{C}^q(H, M)$ we have $\mathrm{cor}(\mathrm{res}(x) \cup y) = x \cup \mathrm{cor}(y)$.

Proof. The quantity $\mathrm{cor}(\mathrm{res}(x) \cup y)(\sigma_1, \ldots, \sigma_p, \tau_1, \ldots, \tau_q)$ is given by

$$\begin{aligned}
&\sum_{g\in R} g^{-1}(\mathrm{res}(x) \cup y)(c(g\sigma_1), \ldots, c(g\sigma_1 \cdots \tau_{q-1})^{-1} c(g\sigma_1 \cdots \tau_q)) \\
&= \sum_{g\in R} g^{-1}(x(c(g\sigma_1), \ldots, c(g\sigma_1 \cdots \sigma_{p-1})^{-1} c(g\sigma_1 \cdots \sigma_p)) \otimes \\
&\quad c(g\sigma_1 \cdots \sigma_p) y(c(g\sigma_1 \cdots \sigma_p)^{-1} c(g\sigma_1 \cdots \tau_1), \ldots, c(g\sigma_1 \cdots \tau_{q-1})^{-1} c(g\sigma_1 \cdots \tau_q)) \\
&= x(\sigma_1, \ldots, \sigma_p) \otimes \sigma_1 \cdots \sigma_p \\
&\quad (\sum_{g\in R} r(g\sigma_1 \cdots \sigma_p)^{-1} y(c(g\sigma_1 \cdots \sigma_p)^{-1} c(g\sigma_1 \cdots \tau_1), \ldots, c(g\sigma_1 \cdots \tau_{q-1})^{-1} c(g\sigma_1 \cdots \tau_q))).
\end{aligned}$$

The last equality follows from our assumption on the cochain x. Note that $r(g_1 g_2) = r(r(g_1)g_2)$. Let $g' \coloneqq r(g\sigma_1 \cdots \sigma_p)$. Then

$$\begin{aligned}
&y(c(g\sigma_1 \cdots \sigma_p)^{-1} c(g\sigma_1 \cdots \tau_1), \ldots, c(g\sigma_1 \cdots \tau_{q-1})^{-1} c(g\sigma_1 \cdots \tau_q)) \\
&= y(r(g\sigma_1 \cdots \sigma_p)\tau_1 r(g\sigma_1 \cdots \tau_1)^{-1}, \ldots, r(g\sigma_1 \cdots \tau_{q-1})\tau_q r(g\sigma_1 \cdots \tau_q)^{-1}) \\
&= y(g'\tau_1 r(g'\tau_1)^{-1}, \ldots, r(g'\tau_1 \cdots \tau_{q-1})\tau_q r(g'\tau_1 \cdots \tau_q)^{-1}) \\
&= y(c(g'\tau_1), \ldots, c(g'\tau_1 \cdots \tau_{q-1})^{-1} c(g'\tau_1 \cdots \tau_q)).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\operatorname{cor}(\operatorname{res}(x) \cup y)(\sigma_1, \ldots, \sigma_p, \tau_1, \ldots, \tau_q) \\
&= x(\sigma_1, \ldots, \sigma_p) \otimes \sigma_1 \cdots \sigma_p \left(\sum_{g' \in R} g'^{-1} y(c(g'\tau_1), \ldots, c(g'\tau_1 \cdots \tau_{q-1})^{-1} c(g'\tau_1 \cdots \tau_q)) \right) \\
&= (x \cup \operatorname{cor}(y))(\sigma_1, \ldots, \sigma_p, \tau_1, \ldots, \tau_q).
\end{aligned}$$

□

1.3.1 Tate cohomology

Many interesting things happen when G is a finite group. In this case one can define cohomology groups for any dimension $n \in \mathbb{Z}$. This is done by extending the cochain complex (1.3.1) in the negative dimension. The extension below becomes more natural if we interpret the negative cohomology groups as homology groups with respect to the G-module M. The non-triviality is that the construction of group cohomology and group homology can be combined together in a *nice* way when G is finite. However, we stick to the essential and useful/direct definitions without motivating them too much.

For $n \in \mathbb{Z}_{<0}$, let $\mathrm{C}^n(G, M) := \{$ continuous maps $f : G^{-n+1} \to M\}$, and define $\partial_n : \mathrm{C}^n(G, M) \to \mathrm{C}^{n+1}(G, M)$ as

- $\partial_{-1}(x) := \sum_{g \in G} g \cdot x.$
- $\partial_{-2}(x) := \sum_{g \in G} (g^{-1} x(g) - x(g)).$
- For $n \leq -3$

$$\begin{aligned}
\partial_n(x)(g_1, \ldots, g_{-2-n}) := \sum_{g \in G} [&g^{-1} x(g, g_1, \ldots, g_{-n-2}) \\
&+ \sum_{i=1}^{-2-n} (-1)^i x(g_1, \ldots, g_{i-1}, g, g^{-1}, g_{i+1}, \ldots, g_{-n-2}) \\
&+ (-1)^{-n-1} x(g_1, \ldots, g_{-n-2}, g)]
\end{aligned}$$

One can verify explicitly that this extends the chain complex (1.3.1) for all $n \in \mathbb{Z}$; hence, we obtain the groups of cocycles, coboundaries, and cohomology classes for this new chain complex and denote them by $\hat{\mathrm{Z}}^n(G, M)$, $\hat{\mathrm{B}}^n(G, M)$ and $\hat{\mathrm{H}}^n(G, M)$ for $n \in \mathbb{Z}$. The cohomology groups thus obtained are known as *Tate cohomology* groups.

Example 1.3.13.

1. We have $\hat{\mathrm{H}}^n(G, M) = \mathrm{H}^n(G, M)$ when $n \geq 1$.
2. $\hat{\mathrm{H}}^0(G, M) = M^G/N_G(M)$, where $N_G : M \to M$ is the norm map sending $m \mapsto \sum_{g \in G} g \cdot m$.
3. $\hat{\mathrm{H}}^{-1}(G, M) = M_{N_G}/I_G(M)$, where $M_{N_G} := \{m \in M : N_G(m) = 0\}$ and $I_G \subset \mathbb{Z}[G]$ is the *augmentation ideal* defined by $\{\sum_{g \in G} n_g g \mid \sum_{g \in G} n_g = 0\}$.
4. $\hat{\mathrm{H}}^{-1}(G, \mathbb{Z}) = 0$, and $\hat{\mathrm{H}}^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$, with trivial G action.

In particular, if G is a cyclic group, then one can show the following useful result.

Proposition 1.3.14. *Let G be a cyclic group, and let M be a G-module. Then for $n \in \mathbb{Z}$ we have*

$$\hat{\mathrm{H}}^n(G, M) \simeq \hat{\mathrm{H}}^{n+2}(G, M).$$

The isomorphism above can be given explicitly between $\hat{\mathrm{H}}^{-1}(G, M) \simeq \hat{\mathrm{H}}^1(G, M)$ ATLOC via $m \mapsto x_m(g) = m$, where $m \in M_{N_G}$ and g is a generator of G. The general case follows by a technique known as dimension shifting (see section 1.3.2); hence, in order to give an isomorphism ATLOC explicitly, one will need an explicit version of dimension shifting, which we will see later.

1.3.2 Dimension shifting

Dimension shifting is an important technique in cohomology using which one can transfer/define maps for higher dimensional cohomology groups intrinsically using the definitions in the lower dimensions but for larger modules. This uses cohomological triviality of certain modules known as *induced modules* in every dimension, and the long exact sequence of cohomology groups obtained from a short exact sequence.

Lemma 1.3.15. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of G-modules. This gives a long exact sequence of cohomology groups as follows*

$$0 \longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \xrightarrow{\delta_0} \mathrm{H}^1(G, M') \longrightarrow \cdots \longrightarrow \mathrm{H}^n(G, M'') \xrightarrow{\delta_n} \mathrm{H}^{n+1}(G, M') \longrightarrow \cdots,$$

where for each $n \geq 0$, δ_n, called the connecting morphism*, is defined ATLOC by $\delta_n(x) = \partial(\tilde{x})$, where $\tilde{x} \in \mathrm{C}^n(G, M)$ is a lift of the cocycle $x \in \mathrm{Z}^n(G, M'')$. Since δ_n takes coboundaries to coboundaries, and different lifts of x will change $\delta_n(x)$ by an $n+1$ coboundary, one concludes that δ_n is well defined on cohomological classes.*

Remark 1.3.16. [Ser79, Appendix to VII] One can define dimension 0 and 1 cohomology sets in a similar way when M is not necessarily an abelian G-module. In this case the cohomology sets are not groups for dimension greater than 0 but just *pointed sets*, i.e., a set with a distinguished element, which in this case is the class of the trivial cocycle.

If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of non-abelian topological G-modules, then we get a long exact sequence of pointed sets

$$0 \to \mathrm{H}^0(G, M') \to \mathrm{H}^0(G, M) \to \mathrm{H}^0(G, M'') \xrightarrow{\delta} \cdots \to \mathrm{H}^1(G, M''),$$

where $\mathrm{H}^0(G, \_)$ are still groups. Furthermore, if the image of M' in M is contained in the center, then the above exact sequence extends to dimension 2 as follows

$$0 \to \mathrm{H}^0(G, M') \to \cdots \to \mathrm{H}^1(G, M'') \xrightarrow{\delta_1} \mathrm{H}^2(G, M').$$

Note that M' is abelian here, therefore, $\mathrm{H}^2(G, M')$ is also a group.

For simplicity of notation we will drop the subscript in the connecting morphism whenever clear from the context.

Definition 1.3.17. Let M be a G-module. Then we define the *induced module* $\mathrm{Ind}_G(M)$ of M with respect to G as $\{m \mid m : G \to M \text{ is continuous}\}$. The action of G on $\mathrm{Ind}_G(M)$ is naturally given by $(g'.f)(g) = g'f(g'^{-1}g)$. Moreover, if G is finite, then $\mathrm{Ind}_G(M) \simeq M \otimes \mathbb{Z}[G]$ via $x \mapsto \sum_{\sigma \in G} x(\sigma) \otimes \sigma$.

One immediately gets the following exact sequence

$$0 \to M \to \mathrm{Ind}_G(M) \to J_G(M) \to 0,$$

where $J_G(M)$ is the cokernel of the inclusion $M \to \mathrm{Ind}_G(M)$. Applying lemma 1.3.15, for $n \geq 0$ one connects $\mathrm{H}^n(G, M)$ with $\mathrm{H}^{n-1}(G, J_G(M))$ using the following proposition

Proposition 1.3.18. *$\mathrm{H}^n(G, \mathrm{Ind}_G(M)) = 0$ for all $n > 0$, and $\mathrm{Ind}_G(M)^G \simeq M$. Moreover, if G is finite, then $\hat{\mathrm{H}}^n(G, \mathrm{Ind}_G(M)) = 0$ for all $n \in \mathbb{Z}$.*

We give an explicit proof of the above proposition here, i.e., we explicitly construct an $n-1$ cochain for every given n-cocycle for $n \geq 1$. This is obtained by diagram chasing between the standard and the bar resolutions via explicit isomorphisms and inverses. However, one can give a more conceptual proof of the above proposition (see [NSW08, Proposition 1.3.6, 1.3.7]), and combined with a conceptual treatment of Tate cohomology using the standard resolution (see [Ser79, VIII, §1]) this immediately yields the proposition for all $n \in \mathbb{Z}$.

Proof. Let $n > 0$, and $f \in \mathrm{Z}^n(G, \mathrm{Ind}_G(M))$. Then we have $(\partial f)(g) = 0$ for $g \in G$. Let $b(g_1, \cdots, g_{n-1})(g) = gf(g^{-1}, g_1, \cdots, g_{n-1})(\mathrm{id}\,)$. Then $b \in \mathrm{C}^{n-1}(G, \mathrm{Ind}_G(M))$. We now explicitly check that $\partial b = f$,

$$\begin{aligned}
\partial b(g_1, \dots g_n) &= g_1 \cdot b(g_2, \dots, g_n) + \sum_{k=1}^{n-1} (-1)^k b(g_1, \dots, g_k g_{k+1}, \dots, g_n) \\
&\quad + (-1)^i b(g_1, \dots, g_{n-1}) \\
(\partial b(g_1, \dots g_n))(g) &= g_1 b(g_2, \dots, g_n)(g_1^{-1} g) \\
&\quad + \sum_{k=1}^{n-1} (-1)^k b(g_1, \dots, g_k g_{k+1}, \dots, g_n)(g) + (-1)^n b(g_1, \dots, g_{n-1})(g) \\
&= g_1 g_1^{-1} g f(g^{-1} g_1, g_2, \dots, g_n)(\mathrm{id}\,) \\
&\quad + \sum_{k=1}^{n-1} (-1)^k g f(g^{-1}, g_1, \dots, g_k g_{k+1}, \dots, g_n)(\mathrm{id}\,) \\
&\quad + (-1)^n g f(g^{-1}, g_1, \dots, g_{n-1})(\mathrm{id}\,) \\
&= g f(g^{-1} g_1, g_2, \dots, g_n)(\mathrm{id}\,) \\
&\quad + \sum_{k=1}^{n-1} (-1)^k g f(g^{-1}, g_1, \dots, g_k g_{k+1}, \dots, g_n)(\mathrm{id}\,) \\
&\quad + \left((-1)^n g f(g^{-1}, g_1, \dots, g_{n-1})\right)(\mathrm{id}\,) \\
&= -g(\partial f)(g^{-1}, g_1, \dots, g_n)(\mathrm{id}\,) + g(g^{-1} \cdot (f(g_1, \dots, g_n)))(\mathrm{id}\,) \\
&= f(g_1, \dots, g_n)(g).
\end{aligned}$$

If $f \in \mathrm{Ind}_G(M)^G$, then $f(gh) = gf(h)$ for all $h, g \in G$; hence, the map $\mathrm{Ind}_G(M)^G \to M$ sending $f \mapsto f(\mathrm{id}\,)$ is an isomorphism. □

As a corollary we obtain the following.

Corollary 1.3.19. *If $n > 0$, then $\mathrm{H}^{n-1}(G, J_G(M)) \overset{\delta}{\simeq} \mathrm{H}^n(G, M)$, and $\delta : M \simeq \mathrm{Ind}_G(M)^G \to \mathrm{H}^1(G, M)$ is surjective. If G is finite, then $\hat{\mathrm{H}}^{n-1}(G, J_G(M)) \overset{\delta}{\simeq} \hat{\mathrm{H}}^n(G, M)$ for all $n \in \mathbb{Z}$. Moreover since $J_G(M) \simeq J_G[\mathbb{Z}] \otimes M$, one obtains isomorphisms $\delta^n : \mathrm{H}^{q-n}(G, J_G(\mathbb{Z})^{\otimes n} \otimes M) \xrightarrow{\sim} \mathrm{H}^q(G, M)$ for $q > n > 0$.*

The next proposition discusses the interplay between various maps defined above.

Proposition 1.3.20. [NSW08, Proposition 1.5.2,3,4,5]

The maps cor, res, inf, g_* *and push forwards are functorial and commute with the dimension shifting morphism δ.*

Remark 1.3.21. The above proposition implies that all these maps arise from dimension 0 and their properties can be directly checked from dimension 0.

Proposition 1.3.22. *Let G be a finite group of order N. Then $N\hat{\mathrm{H}}^n(G, M) = 0$.*

Proof. Consider the sequence $M \xrightarrow{i} \mathrm{Ind}_G(M) \xrightarrow{\pi} M$, where i sends $m \mapsto (g \mapsto m)$ and π is given by $f \mapsto \sum_{g\in G} f(g)$. One easily checks that the maps i and π are G-module homomorphisms and $\pi \circ i = N$. Taking cohomology one gets $\pi_* \circ i_* = N_*$, however $\hat{\mathrm{H}}^n(G, \mathrm{Ind}_G(M)) = 0$. □

We now discuss one of the crucial results in group cohomology called *Shapiro's Lemma*. Let H be a finite index subgroup of G, let R be a system of coset representatives of G/H, and let M be an H-module. Then we define the induced G-module of M with respect to H as $\mathrm{Ind}_G^H(M) \coloneqq \bigoplus_{g\in R} M(g)$. Interpreting $\mathrm{Ind}_G^H(M)$ as the set of maps $R \to M$, one can represent an element m of $\mathrm{Ind}_G^H(M)$ by a formal sum of the form as $m \coloneqq \sum_{g\in R} m_g(g)$. Now the action of $g' \in G$ is given by $g' \cdot m \coloneqq \sum_{g\in G} gg'r(gg')^{-1} \cdot m_g(r(gg'))$, where $r : G \to R$ is the map taking $g \in G$ to its right coset representative as in the definition of the corestriction morphism. If M is a G-module, then there is a canonical isomorphism between $\mathrm{Ind}_G^H(M)$ and the set of continuous maps $x : G/H \to M$ considered as a G-module with its natural action $(g' \cdot x)(gH) = g'x(g'^{-1}gH)$. This is given by $m \mapsto x$, where $x(g^{-1}H) = r(g)m_{r(g)}$. We now state Shapiro's Lemma.

Lemma 1.3.23 (Shapiro's Lemma)**.** *For all $n \geq 0$, we have a canonical isomorphism*

$$sh : \mathrm{H}^n(G, \mathrm{Ind}_G^H(M)) \xrightarrow{\pi_* \circ \mathrm{res}} \mathrm{H}^n(H, M),$$

where $\pi : \mathrm{Ind}_G^H(M) \to M$ is the natural projection map onto the component corresponding to H in R.

Remark 1.3.24. The module $\mathrm{Ind}_G^H(M)$ can be defined generically without the assumption that H is a finite index subgroup as $\mathrm{Ind}_G^H(M) \coloneqq \mathrm{Ind}_G(M)^H$ which also justifies the use of similar notation. However, when H is of finite index in G one can show that the two definitions match.

Proposition 1.3.25. *Let R be a set of representatives for cosets of H in G, let M be an H-module, and let $A \coloneqq \mathrm{Ind}_G^H(M)$. Then by Shapiro's Lemma we have* $\mathrm{sh} : \mathrm{H}^i(G, A) \xrightarrow{\sim} \mathrm{H}^i(H, M)$*, where the isomorphism is given by the composition $\pi_* \circ \mathrm{res}$. The inverse of* sh *is given by the composition* $\mathrm{cor} \circ \iota_*$*, where ι_* is the map induced by the natural inclusion of H-modules $\iota : M \hookrightarrow A$.*

Proof. We prove this for dimension 0 and then the proof follows from dimension shifting, since ι_*, π_*, cor, res and sh are compatible with dimension shifting. In dimension 0, for $a \in A^G$, $\mathrm{sh} : a \mapsto a_M$, where a_M is the component of a corresponding

to M in the decomposition $A \simeq \bigoplus_{\sigma \in R} M(\sigma)$, whereas $\mathrm{cor} \circ \iota_* : d \mapsto \sum_{g \in R} d(g)$, for $d \in M^H$. In case when M is a G-module considered as an H-module, we identify $\mathrm{Ind}_G^H(M)$ with the G-module of continuous maps $x : G/H \to M$ as before. Then the maps $\mathrm{cor} \circ \iota_*(d) = \sum_{g \in G/H} gd$ and $\pi_* \circ \mathrm{res}$ will correspond to $x \mapsto x(H)$. One can easily check that $\mathrm{cor} \circ \iota_* \circ \mathrm{sh}$ and $\mathrm{sh} \circ \mathrm{cor} \circ \iota_*$ are identity on A^G and M^H. respectively. □

We prove a version of the above for Galois cohomology in the next section.

1.3.3 Galois Cohomology

In this section we recall some useful facts about Galois cohomology. Recall that we have already restricted ourselves to perfect fields. Recall from the previous section that profinite groups are topological groups. The absolute Galois group of a perfect field k can be viewed as a profinite group via

$$\mathrm{Gal}(\overline{k}/k) \xrightarrow{\sim} \varprojlim_{K/k} \mathrm{Gal}(K/k),$$

where the inverse limit is taken over all finite normal extensions K/k. We have the following criteria for a group to be a profinite group

Proposition 1.3.26. *Let G be a Hausdorff group. Then the following are equivalent:*

1. *G is the inverse limit of finite discrete groups.*
2. *G is compact and the identity element has a basis of neighbourhoods consisting of subsets which are both open and closed.*
3. *G is compact and totally disconnected.*

The following proposition shows that for a profinite group G, cohomology groups can be viewed as direct limits of cohomology groups of finite groups.

Proposition 1.3.27. *Let G be a profinite group and M be a G-module. Then*

$$\mathrm{H}^n(G, M) \simeq \varinjlim_{\substack{U \lhd G \\ [G:U] < \infty}} \mathrm{H}^n(G/U, M^U),$$

where the direct limit is taken with respect to the inflation maps.

Using the above, if $x \in \mathrm{C}^n(G, M)$, then we say x *factors through* a normal subgroup U of G if $x = \inf(y)$ for some $y \in \mathrm{C}^n(G/U, M^U)$. Moreover, if G is G_k, then we say x *factors through* a finite normal extension K/k, if x factors through G_K.

Proposition 1.3.28. *Let K/k be a finite Galois extension. Then*

1. $\mathrm{H}^n(\mathrm{Gal}(K/k), K^+) = 0$ *for all* $n \geq 1$*; hence,* $\mathrm{H}^n(G_k, \overline{k}^+) = 0$.
2. $\mathrm{H}^1(\mathrm{Gal}(K/k), K^\times) = 0$ *for all Galois extensions* K/k*. Therefore,* $\mathrm{H}^1(G_k, \mathbb{G}_\mathrm{m}) = 0$.
3. *We have the inflation-restriction exact sequence in dimension 2 for* K/k *Galois.*
$$0 \to \mathrm{H}^2(\mathrm{Gal}(K/k), K^\times) \xrightarrow{\inf} \mathrm{H}^2(G_k, \mathbb{G}_\mathrm{m}) \xrightarrow{\mathrm{res}} \mathrm{H}^2(G_K, \mathbb{G}_\mathrm{m})^{\mathrm{Gal}(K/k)}.$$
4. $\mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{GL}_n(K)) = 0$ *for* $n \in \mathbb{Z}_+$*, where the action of* $\mathrm{Gal}(K/k)$ *on* $\mathrm{GL}_n(K)$ *is point-wise.*

Proof. Let $\Gamma \coloneqq \mathrm{Gal}(K/k)$.

1. Using the normal basis theorem, there is a basis of K/k such that $\mathrm{Ind}_\Gamma(k^+) \simeq K^+$; hence, the result follows from Proposition 1.3.18 and 1.3.27.
2. In this case the proof is explicit i.e. given a 1-cocycle x we construct an explicit 0-cochain $y \in K^\times$ such that $\partial y = x$. Consider the endomorphism $b \coloneqq \sum_{g \in \Gamma} x(g)(g)$ of K/k. Linear independence of automorphisms implies that there exists $t \in K$ such that $b(t) \neq 0$ (in fact at least one the basis elements of K/k will work as t). The 1-cocycle relation implies that $b(t)/\sigma(b(t)) = x(\sigma)$ for $\sigma \in \Gamma$. Choose $y = 1/b(t)$.
3. This follows from 1.3.7 since $\mathrm{H}^1(G_K, \mathbb{G}_\mathrm{m}) = 0$.
4. [Ser79, X §1, Proposition 3].

□

Using the fact that res, cor, ι_*, π_* are well behaved under inflation maps ([NSW08, Proposition 1.5.5]), we can show that the following holds.

Corollary 1.3.29. *Let* K *be a finite extension of* k*, let* D *be a* G_K*-module, and let* A *be a finite* G_k/G_K *induced* G_k*-module with respect to* D*. Then*
$$\mathrm{H}^i(G_k, A) \simeq \mathrm{H}^i(G_K, D).$$

Proof. Since A is finite, the kernel of the natural map $G_k \to \mathrm{Aut}\,(A)$ (U say) is a normal subgroup of G_k of finite index. This corresponds to a normal extension L of k. Clearly $K \subset L$. Consider the inverse system of finite degree normal extensions of k containing L, $I_L \coloneqq \{L' : L \subset L'\}$. Noting that $G_{L'}$ acts trivially on A, we have the commutative diagram (inf, sh commute with dimension shifting):
$$\begin{array}{ccc} \mathrm{H}^i(\mathrm{Gal}(L'/k), A) & \xrightarrow{\mathrm{sh}} & \mathrm{H}^i(\mathrm{Gal}(L'/K), D) \\ \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\ \mathrm{H}^i(\mathrm{Gal}(L''/k), A) & \xrightarrow{\mathrm{sh}} & \mathrm{H}^i(\mathrm{Gal}(L''/K), D). \end{array}$$

Taking the direct limits with respect to inflation maps on both sides we get

$$\mathrm{H}^i(G_k, A) \simeq \varinjlim_{\substack{\mathrm{Gal}(L'/k),\\ L' \in I_L}} \mathrm{H}^i(\mathrm{Gal}(L'/k), A) \simeq \varinjlim_{\substack{\mathrm{Gal}(L'/k),\\ L' \in I_L}} \mathrm{H}^i(\mathrm{Gal}(L'/K), D) \simeq \mathrm{H}^i(G_K, D).$$

□

If k is a global field, then for each place v of k we have an inclusion map $\overline{k} \hookrightarrow \overline{k_v}$. Once we fix such an inclusion, then this induces an inclusion $G_{k_v} \hookrightarrow G_k$. Therefore, if M is a G_k-module, then the restriction map to the image of G_{k_v} in G_k induces a map, called the *localization map* , at a place v of k, $\mathrm{H}^n(G_k, M) \to \mathrm{H}^n(G_{k_v}, M)$ which we will denote by res_v. Under the embedding $G_{k_v} \hookrightarrow G_k$, G_{k_v} can be considered as a closed subgroup of G_k (G_k is Hausdorff and G_{k_v} is compact). Let L be a finite extension of k, and $w_1, \ldots, w_m$ be all the distinct places of L above v with w_1 being the one induced by the fixed embedding $\overline{k} \hookrightarrow \overline{k_v}$. There is a $g_i \in G_k$ corresponding to each w_i such that w_i is induced by the composite embedding $g_i : \overline{k} \to \overline{k} \hookrightarrow \overline{k_v}$. If $L = k(\theta_1)$, then g_i correspond to those embeddings of $L \hookrightarrow \overline{k}$ which map θ_1 to one of its G_k conjugates that is not a G_{k_v}-conjugate. This implies that $\{g_1, \ldots, g_m\}$ is a system of double coset representatives of G_k with respect to G_{k_v} and G_L, i.e., $G_k = \bigsqcup_{i=1}^{m} G_{k_v} g_i G_L$. Further, note that $G_{L_{w_i}} \subset G_{k_v}$ fixes the extension $g_i L$, and therefore $G_{L_{w_i}} = G_{k_v} \cap g_i G_L g_i^{-1}$. Using the double coset formula (1.3.4) and part 7 of Proposition 1.3.11 we have the following remark.

Remark 1.3.30. Let k, L, w_i, g_i be as above. Then

$$(\mathrm{cor}^{G_k}_{G_L}(z))_v = \mathrm{res}^{G_{k_v}}_{G_k} \circ \mathrm{cor}^{G_k}_{G_L}(z) = \sum_{i=1}^{m} \mathrm{cor}^{G_{k_v}}_{G_{L_{w_i}}} \circ \mathrm{res}^{G_{L_{w_i}}}_{G_{g_i L}} \circ (g_i)_*(z). \tag{1.3.5}$$

1.3.4 Brauer Groups

Definition 1.3.31. A *central simple algebra* A over k is a simple (no non-trivial two-sided ideals) associative algebra (possibly non commutative) with unity over k such that its center is isomorphic to k. Consider the category of all finite dimensional central simple algebras over k and denote it CSA_k.

There are various equivalent definitions for a finite dimensional algebra over k to be a central simple algebra. The following proposition states a few of them.

Proposition 1.3.32. [Poo17, Proposition 1.5.2] *Let A be a finite dimensional possibly non-commutative algebra over k. Then the following statements are equivalent.*

1. *There exists an $n \in \mathbb{Z}_+$ such that $A \otimes \overline{k} \simeq M_n(\overline{k})$ as a $\overline{k}$-algebra.*

2. *There exists a finite field extension L/k such that $A \otimes L \simeq M_n(L)$, for some $n \in \mathbb{Z}_+$.*

3. *A is a finite dimensional central simple algebra over k.*

4. *There is a k-algebra isomorphism $A \simeq M_r(D)$, for some $r \in \mathbb{Z}_+$ and a finite dimensional central division algebra D over k. Moreover, r, D are unique for every algebra A.*

Let A and B be central simple algebras. Then we say that $A \sim B$, if there are positive integers m and n such that $M_m(A) \simeq M_n(B)$ as k-algebras. Equivalently, $A \sim B$, if there exists a division algebra D and positive integers m and n such that $A \simeq M_m(D)$ and $B \simeq M_n(D)$ as k-algebras. Furthermore, we say that a central simple algebra A/k is *split* over a field extension K/k, if $A \otimes K \simeq M_n(K)$ over K. We now consider the set $CSA_k/\sim$. Let A be a central simple algebra over k. Then one can define A^{opp} by redefining multiplication in A by $a \cdot b = ba$. It can be checked that the map $A \to A^{\text{opp}}$ respects extension of scalars and $\sim$. Furthermore, if A and B are central simple algebras then $A \otimes B$ is also a central simple algebra. This leads to the following definition.

Definition 1.3.33. The set $CSA_k/\sim$ can be given a group structure with the class of split central simple algebras over k as the identity element, opp as the inverse and $\otimes$ as the group operation. This group is called the *Brauer group* over k. We denote it by $\mathrm{Br}(k)$.

It can be shown using the Skolem–Noether theorem that, for each $r \geq 1$,

$$\frac{\text{central simple algebras of dimension } r^2}{\sim} \hookrightarrow \mathrm{H}^1(G_k, \mathrm{PGL}_r(\overline{k})),$$

as pointed sets. In fact this map of pointed sets is a bijection. Now using non-abelian Galois cohomology (remark 1.3.16) on the exact sequence

$$1 \to \mathbb{G}_{\mathrm{m}} \to \mathrm{GL}_r(\overline{k}) \to \mathrm{PGL}_r(\overline{k}) \to 1,$$

and Proposition 1.3.28 we have the injection of pointed sets $\mathrm{H}^1(G_k, \mathrm{PGL}_r(\overline{k})) \hookrightarrow \mathrm{H}^2(k)$; i.e., for each central simple algebra A over k of dimension r^2, one gets a 2-cocycle γ_A with values in $\mathbb{G}_{\mathrm{m}}$. It can be shown that every 2-cocycle gives rise to a central simple algebra over k, and this leads to an isomorphism $\mathrm{Br}(k) \simeq \mathrm{H}^2(k)$ as abelian groups [Ser79, X §5]. The following proposition states a few properties of this isomorphism.

Proposition 1.3.34. [Poo17, Proposition 1.5.13]

1. *The isomorphism* $\mathrm{Br}(k) \simeq \mathrm{H}^2(k)$ *is functorial, i.e., for* L/k *a field extension of* k*, the following diagram*

$$\begin{array}{ccc} \mathrm{Br}(k) & \xrightarrow{\sim} & \mathrm{H}^2(k) \\ \downarrow{\scriptstyle [A]\mapsto[A\otimes L]} & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathrm{Br}(L) & \xrightarrow{\sim} & \mathrm{H}^2(L) \end{array}$$

   commutes.

2. *If* $\mathrm{char}(k) \nmid n$*, then* $\mathrm{Br}(k)[n] \simeq \mathrm{H}^2(G_k, \mu_n)$*.*

3. *The inflation-restriction exact sequence in dimension 2 implies that* $\mathrm{H}^2(L/k) \simeq \ker(\mathrm{Br}(k) \overset{\mathrm{res}}{\to} \mathrm{Br}(L))$*.*

1.3.5 From cocycle to algebra

Since we will be mostly working with cocycles throughout this thesis, it makes sense to get an explicit inverse for the isomorphism $\mathrm{Br}(k) \to \mathrm{H}^2(k)$ ATLOC. Let L/k be a finite extension of fields and $\gamma \in \mathrm{Z}^2(L/k)$ be a 2-cocycle. Let $A \simeq \bigoplus_{\sigma\in G} Lu_\sigma$ be an L-algebra defined by the relation $u_\sigma u_\tau = \gamma(\sigma,\tau)u_{\sigma\tau}$. Then we have the following theorem.

Theorem 1.3.35. [Jac96, Theorem 2.6.8] *Assume that* γ *is a normalized 2-cocycle. Then* $\partial\gamma(\sigma, \mathrm{id}\,, \mathrm{id}\,) = 1$ *implies that* $\gamma(\sigma, \mathrm{id}\,) = \gamma(\mathrm{id}\,, \sigma) = 1$*. Let* A *be the algebra defined above. Then* A *is a central simple algebra whose associated 2-cocycle is* γ*.*

Remark 1.3.36. Theorem 2.3.17 in [Jac96] mentions explicitly how to obtain the central simple algebra as a subalgebra of $M_n(L)$ associated with a Brauer factor set that is same as the 2-cocycle γ in the previous theorem considered in the standard resolution.

1.3.6 Facts on Brauer groups and class field theory

In this section we recall some important results on Brauer groups of some fields, class field theory and arithmetic duality theory.

Proposition 1.3.37. [Poo17, Proposition 1.5.34, 1.5.36]

1. *Let* k *be the function field of a curve over an algebraically closed field. Then* $\mathrm{Br}(k) = 0$*.*

2. *If* k *is a finite field, then* $\mathrm{Br}(k) = 0$*.*

3. *If* k *is a local field, i.e.,* K *is a finite extension of* $\mathbb{R}, \mathbb{Q}_p$*, or* $\mathbb{F}_q((t))$*, then*

(a) *There is an injection,* $\mathrm{inv} : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$, *called the* invariant map *whose image is*

$$\begin{cases} \frac{1}{2}\mathbb{Z}/\mathbb{Z}, & \text{if} \quad k = \mathbb{R}, \\ 0 & \text{if} \quad k = \mathbb{C}, \\ \mathbb{Q}/\mathbb{Z}, & \text{if } k \text{ is nonarchimedean.} \end{cases}$$

(b) *If L is a finite extension of k, then the diagram*

$$\begin{array}{ccc} \mathrm{Br}(k) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle [L:k]} \\ \mathrm{Br}(L) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

4. *If L/k is a finite extension of a local field k and $\gamma \in \mathrm{H}^2(k)$, then* $\mathrm{inv} \circ \mathrm{cor}(\gamma) = \mathrm{inv}(\gamma)$, *where* inv *on left and the right sides are the local invariant maps on* $\mathrm{Br}(k)$ *and* $\mathrm{Br}(L)$, *respectively.*

5. *Let k be a global field, and for each place v of k, let* inv_v *be the local invariant map* $\mathrm{Br}(k_v) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$ *as above. Then the following sequence, called the* Albert-Brauer-Hasse-Noether *sequence, is exact*

$$0 \to \mathrm{Br}(k) \to \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0. \tag{1.3.6}$$

Furthermore, if L is a finite extension of k, then the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Br}(k) & \longrightarrow & \bigoplus_v \mathrm{Br}(k_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \bigoplus_v \bigoplus_{w|v} \mathrm{res}_w} & & \downarrow{\scriptstyle [L:k]} & & \\ 0 & \longrightarrow & \mathrm{Br}(L) & \longrightarrow & \bigoplus_v \bigoplus_{w|v} \mathrm{Br}(L_w) & \xrightarrow{\sum_w \mathrm{inv}_w} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

commutes.

From the above proposition, it is clear that for a local field k, and an extension L/k of degree n, $\mathrm{H}^2(L/k) \simeq \mathbb{Z}/n\mathbb{Z}$. We recall some maps from local/global class field theory.

Proposition 1.3.38. [Neu99, V, Theorem 1.4] *Let k be a local field and L be a finite abelian extension of k. Then there is an isomorphism $(-, L/k) : k^\times/\mathrm{N}_{L/k}(L^\times) \simeq \mathrm{Gal}(L/K)$, called the* local Artin reciprocity *map, and the following statements hold.*

1. *If L is an unramified extension, then the class of any uniformizing element π_k of k is mapped to the Frobenius element in* $\mathrm{Gal}(L/k)$.

2. *The finite index open subgroups $\mathcal{N}$ of $k^\times$ are in an inclusion-reversing one-one correspondence with the finite abelian extensions of k.*

3. *Let L and L' be two finite abelian extensions of k. Then* $\mathrm{N}_{LL'/k}(LL') = \mathrm{N}_{L/K}(L) \cap \mathrm{N}_{L'/k}(L')$ *and* $\mathrm{N}_{L\cap L'/k}(L \cap L') = \mathrm{N}_{L/k}(L)\mathrm{N}_{L'/k}(L')$.

Assume $\mu_n \subset k^\times$ and fix a primitive nth root of unity ζ_n. Then we have a finite extension L of k such that $\mathrm{N}_{L/k}(L) = k^n$ (we can choose $L = k(k^{1/n})$; this is a finite extension because there are finitely many classes mod nth powers in a local field). This implies that $k^\times/(k^\times)^n \simeq \mathrm{Gal}(L/k)$. At the same time Kummer theory implies that $\mathrm{H}^1(G_k, \mu_n) \simeq k^\times/(k^\times)^n$. Therefore, we get a pairing

$$\left(\frac{-,-}{\mathfrak{p}}\right) : \frac{k^\times}{(k^\times)^n} \times \frac{k^\times}{(k^\times)^n} \to \mu_n, \quad (a,b) \mapsto \left(\frac{a,b}{\mathfrak{p}}\right) := (a, k(b^{1/n})/k)(b^{1/n})/b^{1/n},$$

where $\mathfrak{p}$ is the maximal ideal of the local field k. Furthermore, one can construct a pairing using the cup product and the bilinear pairing $\mu_n \times \mu_n \to \mu_n$ given by $(\zeta_n^a, \zeta_n^b) \to \zeta_n^{ab}$ on cohomology groups as follows

$$\mathrm{H}^1(G_k, \mu_n) \times \mathrm{H}^1(G_k, \mu_n) \to \mathrm{H}^2(G_k, \mu_n \otimes \mu_n) \simeq \mathrm{H}^2(G_k, \mu_n) \simeq \mathrm{Br}(k)[n].$$

We obtain the following commutative diagram [Neu99, V,§3]:

$$\begin{array}{ccccc} \frac{k^\times}{(k^\times)^n} & \times & \frac{k^\times}{(k^\times)^n} & \xrightarrow{\left(\frac{-,-}{\mathfrak{p}}\right)} & \mu_n \\ \downarrow\sim & & \downarrow\sim & \searrow^{=} & \\ \mathrm{H}^1(G_k,\mu_n) & \times & \mathrm{H}^1(G_k,\mu_n) & \xrightarrow{\cup} \mathrm{Br}(k)[n] \xrightarrow{\zeta_n^{\mathrm{inv}}} & \mu_n. \end{array} \tag{1.3.7}$$

In the above diagram, for $g \in \mathrm{Br}(k)$, the map ζ_n^{inv} is given by $\zeta_n^{\mathrm{inv}}(g) = \zeta_n^{\mathrm{inv}(g)}$. Therefore, for a 2-cocycle $\gamma \in \mathrm{Z}^2(G_k, \mu_n)$ which can be written as a cup-product of two 1-cocycles χ_a and χ_b in $\mathrm{Z}^1(G_k, \mu_n)$ corresponding to elements a, $b \in k^\times$, $\zeta_n^{\mathrm{inv}([\gamma])} = \left(\frac{a,b}{n}\right)$. Here $[\gamma]$ is the class of γ in $\mathrm{H}^2(k)$. As a consequence of the sequence (1.3.6), one can extend the definition of the Hilbert symbol to a global field when the characteristic of the global field does not divide n. Therefore, the dependence of the symbol on $\mathfrak{p}$ the maximal ideal of the localization is emphasized in the notation. However, sometimes we will use $(a,b)_k$ or $(a,b)_{\mathfrak{p}}$ to denote the Hilbert symbol. Given any 2-cocycle it is not always easy to compute the invariant map on the class it represents because the invariant map is defined on the cohomology class not on the cocycles. We will later see a way to be able to compute the invariant map given a cocycle. Note that this can be done in principle due to the existence of the inflation-restriction exact sequence in dimension 2. We state some useful properties of the Hilbert symbol in the following proposition.

Proposition 1.3.39. [Neu99, Proposition 3.2]

- $\left(\frac{aa',b}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a',b}{\mathfrak{p}}\right)$.
- $\left(\frac{a,bb'}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a,b'}{\mathfrak{p}}\right)$.
- $\left(\frac{a,b}{\mathfrak{p}}\right) = 1 \iff$ *a is a norm from the extension* $k(\sqrt[n]{b})$.
- $\left(\frac{a,b}{\mathfrak{p}}\right) = \left(\frac{b,a}{\mathfrak{p}}\right)^{-1}$.
- $\left(\frac{a,1-a}{\mathfrak{p}}\right) = \left(\frac{a,-a}{\mathfrak{p}}\right) = 1$.
- *If* $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$ *for all* $b \in k^\times$, *then* $a \in (k^\times)^n$.

We have the following useful proposition for computing the invariant map and the Hilbert symbol of certain cocycles.

Proposition 1.3.40. *If* $d_1, d_2 \in k_v^\times$, *then the 2-cocycle* z *given by* $(\sigma,\tau) \mapsto 1$ *if* $\sigma(\sqrt{d_2}) = \sqrt{d_2}$ *or* $\tau(\sqrt{d_2}) = \sqrt{d_2}$, *and* $(\sigma,\tau) \mapsto d_1$, *if* $\sigma(\sqrt{d_2}) = \tau(\sqrt{d_2}) = -\sqrt{d_2}$ *represents the class of the quaternion algebra* (d_1, d_2) *in* $\mathrm{Br}(k_v)$.

Proof. [Ser79, §XIV.2, Proposition 5] implies that the cocycle

$$x(\sigma,\tau) := \begin{cases} 1, & \text{if } \sigma(\sqrt{d_1}) = \sqrt{d_1} \text{ or } \tau(\sqrt{d_2}) = \sqrt{d_2}, \\ -1, & \text{otherwise.} \end{cases}$$

represents the class of quaternion algebra (d_1, d_2). Now it can be checked that $z = x - \partial y$ where

$$y(\sigma) := \begin{cases} 1, & \text{if } \quad \sigma(\sqrt{d_2}) = \sqrt{d_2}, \\ \frac{1}{\sqrt{d_1}}, & \text{if } \sigma(\sqrt{d_2}) = -\sqrt{d_2}. \end{cases}$$

□

1.3.7 Twisted powers of Galois modules and Poitou-Tate duality

Definition 1.3.41. Let Δ be a finite G_k-set (i.e. there is a group homomorphism $G_k \to \mathrm{Perm}(X)$, where $\mathrm{Perm}(\Delta)$ is the group of permutations of Δ), and M be a G_k-module. Then we can define

$$M^\Delta := \{\text{maps} \mid m : \Delta \to M\},$$

called the *twisted power* of M w.r.t. Δ.

The elements of M^Δ can be represented as formal sums of the form $\sum_{s\in\Delta} a_s(s)$ with $a_s \in M$. Under the natural action of G_k given by $(\sigma \cdot m)(P) = \sigma m(\sigma^{-1}P)$, M^Δ is a G_k-module. One can show the following properties.

Proposition 1.3.42.

1. $(M^{\Delta})^{\vee} \simeq (M^{\vee})^{\Delta}$, *where* $X^{\vee}$ *is the Cartier dual of the* G_k*-module* X.
2. $(\mathbb{G}_{\mathrm{m}}^{\Delta})^{G_k} \simeq \prod_{\text{orbits}} (\mathbb{G}_{\mathrm{m}}^{\Delta_i})^{G_k} \simeq \prod_{\text{orbits}} L_i^{\times}$, *where* Δ_i *is a* G_k*-orbit of* Δ *and* L_i *is the finite extension corresponding to the orbit* Δ_i. *To see how one associates a finite field extension with each orbit* Δ_i *note that each orbit is finite and has a transitive action of* G_k, *so we have a finite extension* L_i *of* k *corresponding to* Δ_i *such that* G_{L_i} *stabilizes an element of* Δ_i.
3. *The following generalization of Hilbert's Theorem 90 holds. We have* $\mathrm{H}^1(G_k, \mathbb{G}_{\mathrm{m}}^{\Delta}) = 0$.

In the view of the above one can consider Δ as a finite étale scheme with $L := k[x]/\langle f(x)\rangle$ as the ring of global sections of the structure sheaf, where $f = \prod_{\text{orbits}} f_i$ and f_i is a defining polynomial of the extension L_i. Moreover $\mathrm{H}^1(G_k, \mu_n(\bar{L})) \simeq L^{\times}/(L^{\times})^n$.

We have the following important result known as the *Poitou-Tate duality*.

Theorem 1.3.43. [NSW08, Theorem 8.6.7] *Let* k *be a number field, and let* A *be a finitely generated (as a* $\mathbb{Z}$*-module)* G_k*-module, and* $A^{\vee} := \mathrm{Hom}(A, \mathbb{G}_{\mathrm{m}})$. *For any* G_k*-module* M, *let*

$$Ш^i(M) := \ker(\mathrm{H}^i(G_k, M) \xrightarrow{\mathrm{loc}^i(M)} \prod_v \mathrm{H}^i(G_{k_v}, M)).$$

Then there is a perfect pairing

$$\mathrm{pt} : Ш^1(A^{\vee}) \times Ш^2(A) \to \mathbb{Q}/\mathbb{Z}.$$

Theorem 1.3.44. *Let* k *be a number field. Then* $\mathrm{H}^3(k) = 0$.

Proof. This is a direct consequence of Galois cohomology applied on the exact sequence

$$1 \to \overline{k}^{\times} \to I \to C \to 1,$$

where I is the *idèle group* of $\overline{k}$ and C is the *idèle class group* of $\overline{k}$, along with [NSW08, Proposition 8.1.7, 8.1.20]. □

1.4 Covering spaces and descent

One of the fundamental problems in arithmetic geometry is to determine the set $X(k)$ of k-rational points on a variety X/k given by some explicit equations. Another, important and equally (presumably) fundamental problem is to answer the following question.

Question 1.4.1. *Let X/k be a "nice" (projective, smooth, geometrically irreducible) variety. Is the set $X(k)$ empty?*

Obviously, when k is a number field, and $X(k_v) = \emptyset$ for at least one place v of k, then one concludes that $X(k) = \emptyset$. A Problem arises when $X(k_v) \neq \emptyset$ for all places v of k. Note that for each place v of k, the problem if $X(k_v) = \emptyset$ is decidable. This is true even if all the places are considered together. We say that X/k satisfies the *Hasse principle*, if $X(k_v) \neq \emptyset$ for all places v of k implies $X(k) \neq \emptyset$. The varieties defined by non-degenerate quadratic-forms are famous examples of varieties satisfying the Hasse principle. For cubics and beyond many counterexamples to the Hasse principle are known.

However, one can also use a different technique known as descent. Let $\pi : C \to X$ be a finite étale, geometrically Galois covering of X defined over k i.e. C and π both are defined over k. Geometrically Galois means that the extension $\overline{k}(C)/\overline{k}(X)$ is Galois. The Galois group $G := \mathrm{Gal}(\overline{k}(C)/\overline{k}(X))$ which is isomorphic to the group of deck transformations of C over X is a group scheme with a well defined action of G_k.

Definition 1.4.2. A *twist* of π is defined to be a covering $\pi' : C' \to X$ defined over k such that there is an isomorphism $\phi : C \to C'$ defined over $\overline{k}$ such that the following diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi} & X \\ \downarrow{\scriptstyle \phi} & \nearrow{\scriptstyle \pi'} & \\ C' & & \end{array}$$

Two twists π' and π'' of π are called *equivalent* if there is an isomorphism $\phi : C' \to C''$ defined over k such that the corresponding natural diagram commutes. Let $\mathrm{Twists}(\pi)$ be the pointed set of all the equivalence classes of twists of π with the class of π being the distinguished element. If $\sigma \in G_k$, then given a twist $\pi' : C' \to X$ with an isomorphism $\phi : C \to C'$, we get an automorphism of C which is a deck transformation of C/X as $(\sigma\phi)^{-1} \circ \phi$, i.e., we get a map $\xi : G_k \to \mathrm{Deck}(\pi)$. One can show that ξ is a 1-cocycle. Therefore, we get a map $\{\text{all twists of } \pi\} \to \mathrm{Z}^1(G_k, \mathrm{Deck}(\pi))$, and it can be shown that the induced map $\mathrm{Twists}(\pi) \to \mathrm{H}^1(G_k, \mathrm{Deck}(\pi))$ is well defined. Furthermore, note that $\mathrm{H}^1(G_k, \mathrm{Deck}(\pi))$ is a pointed set because there is no guarantee that $\mathrm{Deck}(\pi)$ is abelian group. We have the following useful theorem in regards to the $\mathrm{Twists}(\pi)$.

Theorem 1.4.3. [Sto17a]

1. *The map of pointed sets* $\mathrm{Twists}(\pi) \to \mathrm{H}^1(G_k, \mathrm{Deck}(\pi))$ *is an isomorphism.*

2. *Let $P \in X(k)$. Then there is a unique twist $\pi' : C' \to X$ of π such that*

$P \in \pi'(C(k))$. In particular,

$$X(k) = \bigsqcup_{\pi' \in \mathrm{Twists}(\pi)} \pi'(C'(k)),$$

where the $\sqcup$ denotes the disjoint union. If π is ramified, then the existence part still holds but the uniqueness part fails.

The use of the above theorem is immediate, i.e., if none of the twists of π have k rational points, then $X(k) = \emptyset$. However, we just saw that one of the necessary conditions for a variety to have a k-rational point in case of a global field k is that it has k_v rational point for every place v of k. So we are interested in the classes in Twists(π) which have points everywhere locally or which are *everywhere locally soluble*, also abbreviated as ELS in literature.

Definition 1.4.4. We define the Selmer set of π (denoted by $\mathrm{S}^{(\pi)}$) as the subset of Twists(π) which are ELS.

Immediately, we conclude that $X(k) = \emptyset$, if $\mathrm{S}^{(\pi)} = \emptyset$. Selmer sets are useful mainly because of the following result.

Proposition 1.4.5. *$\mathrm{S}^{(\pi)}$ is finite and in principle computable.*

Proof. Let S be the set of places of bad reduction of X, C and π. Clearly, S is finite. Since π remains unramified for a place of good reduction v, the fiber over any point in $X(k_v)$ lies in $C(k_v^{\mathrm{nr}})$. Clearly, if the twist is ELS, then the restriction of ξ_v (restriction of $\xi \in \mathrm{H}^1(G_k, \mathrm{Deck}(\pi))$ to $\mathrm{H}^1(G_{k_v}, \mathrm{Deck}(\pi))$) to $G_{k_v^{\mathrm{nr}}}$ is trivial, this is because if $\pi' : C' \to X$ is a twist of π, then π' has a good reduction at v, and therefore every fiber over $X(k_v)$ lies in $C'(k_v^{\mathrm{nr}})$. Hence, the isomorphism over $\overline{k_v}$ is actually defined over k_v^{nr}. Therefore,

$$\mathrm{S}^{\pi} \subset \mathrm{H}^1(G_k, \mathrm{Deck}(\pi); S) \coloneqq \{\xi \in \mathrm{H}^1(G_k, \mathrm{Deck}(\pi)) \mid (\mathrm{res}_v)_{\mathrm{nr}}(\xi) = 0 \ \forall \ v \notin S\},$$

where $(\mathrm{res}_v)_{\mathrm{nr}} : \mathrm{H}^1(G_k, \mathrm{Deck}(\pi)) \to \mathrm{H}^1(G_{k_v^{\mathrm{nr}}}, \mathrm{Deck}(\pi))$ is the usual restriction map. It is a well known fact that $\mathrm{H}^1(G_k, A; S)$ is finite for a finite module A because there are only finitely many extensions of bounded degree unramified outside a finite set of primes. □

1.5 Selmer groups and rank bounds

In this section, we assume that the base field k is a number field. Let A, B be abelian varieties over k and $\phi : A \to B$ be an isogeny defined over k. Then ϕ is a finite, étale and geometrically Galois covering of B with the set of deck transformations

isomorphic to the abelian group $A[\phi]$ the kernel of ϕ. Using the above theory we have $\mathrm{S}^{(\phi)} \subset \mathrm{H}^1(G_k, A[\phi])$. We have the following analogue of the Kummer sequence

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

Taking Galois cohomology both locally and globally we get the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{B(k)}{\phi(A(k))} & \xrightarrow{\delta} & \mathrm{H}^1(G_k, A[\phi]) & \longrightarrow & \mathrm{H}^1(G_k, A)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & \searrow^{\alpha} & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \\
0 & \longrightarrow & \prod_v \frac{B(k_v)}{\phi(B(k_v))} & \xrightarrow{\prod_v \delta_v} & \prod_v \mathrm{H}^1(G_{k_v}, A[\phi]) & \longrightarrow & \prod_v \mathrm{H}^1(G_{k_v}, A)[\phi] & \longrightarrow & 0
\end{array}$$

In view of the previous section we have $\mathrm{S}^{(\phi)} = \ker(\alpha)$. One has the following exact sequence for every isogeny ϕ called the *ϕ-descent sequence*

$$0 \to \frac{B(k)}{\phi(A(k))} \to \mathrm{S}^{(\phi)}(A/k) \to Ш(A/k)[\phi] \to 0,$$

where $Ш(A/k) := \ker(\mathrm{H}^1(G_k, A) \to \prod_v \mathrm{H}^1(G_{k_v}, A))$ is called the *Shafarevich-Tate* group associated to A/k.

One of the most interesting isogenies (that are always available) is the multiplication by n map, $[n]$, for $n \geq 2$. It is enough to understand the $\mathrm{S}^{(n)}(A/k)$, since for any isogeny ϕ, there is an n such that $A[\phi] \subset A[n]$ and one has the natural map $\mathrm{S}^{(\phi)}(A/k) \to \mathrm{S}^{(n)}(A/k)$ induced by the above inclusion $A[\phi] \hookrightarrow A[n]$. The kernel of the map $\mathrm{S}^{(\phi)}(A/k) \to \mathrm{S}^{(n)}(A/k)$ could be determined by studying the cokernel of the map $A(k)[n] \to (A[n]/A[\phi])^{G_k}$. Furthermore, for m, n coprime we have $\mathrm{S}^{(mn)}(A/k) \simeq \mathrm{S}^{(m)}(A/k) \times \mathrm{S}^{(n)}(A/k)$. This implies that it is enough to consider isogenies whose kernel is contained in $A[p^n]$ for some prime p and $n \in \mathbb{Z}_+$. One can make this n unique by looking at the maximum order of an element in the kernel of the isogeny. Therefore, we look at the descent sequence for p^n, and we obtain

$$\#A[p^n](k) \cdot p^{nr_A} \leq \#\mathrm{S}^{(p^n)}(A/k).$$

When $n = 1$, then we have the following interesting result:

Proposition 1.5.1. [Sto17a] *Let A be an abelian variety over a number field k and p be a prime number.*

1. *Let v be a finite place of k. Then*

$$\dim_{\mathbb{F}_p}\left(\frac{A(k_v)}{pA(k_v)}\right) = \dim_{\mathbb{F}_p}(A(k_v)[p]) + \begin{cases} [k_v : \mathbb{Q}_v]\dim(A) & \text{if } v \mid p \\ 0 & \text{else.} \end{cases}$$

If v is an infinite place of k, then $A(k_v)/pA(k_v) = 0$, if either v is complex or p is odd. If v is real and $p = 2$, then

$$\dim_{\mathbb{F}_2}\left(\frac{A(k_v)}{2A(k_v)}\right) = \dim_{\mathbb{F}_2}(A(k_v)[2]) - \dim(A).$$

2. *If v is a finite place of k such that $v \nmid p$ and v is a place of good reduction of A, then the image of $A(k_v)$ is exactly*

$$\inf(\mathrm{H}^1(\mathrm{Gal}(k_v^{\mathrm{nr}}/k_v), A[p])) = \ker(\mathrm{res} : \mathrm{H}^1(G_{k_v}, A[p]) \to \mathrm{H}^1(G_{k_v^{\mathrm{nr}}}, A[p])).$$

3. *Let S be the set of places of bad reduction of A, the infinite places and the places above p. Then we have*

$$\mathrm{S}^{(p)}(A/k) = \{\xi \in \mathrm{H}^1(G_k, A[p]; S) \mid \forall\ v \in S : \mathrm{res}_v(\xi) \in \mathrm{Im}(\delta_v)\},$$

where δ_v is the connecting morphism in Galois cohomology at the place v.

Proof sketch. The proof of the above proposition follows from the fact that for a finite place v of k, the group $A(k_v)$ contains a subgroup of finite index isomorphic to $\mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim(A)}$. Here q is the characteristic of the residue field of k_v. Using the snake lemma on the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim(A)} & \longrightarrow & A(k_v) & \longrightarrow & T & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle .p} & & \downarrow{\scriptstyle .p} & & \downarrow{\scriptstyle .p} & & \\ 0 & \longrightarrow & \mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim(A)} & \longrightarrow & A(k_v) & \longrightarrow & T & \longrightarrow & 0, \end{array}$$

and the fact that $\dim_{\mathbb{F}_p}(T[p]) = \dim_{\mathbb{F}_p} T/pT$ for a finite abelian group T, one can deduce the result. When $p = 2$ and v is a real place, we use the fact that $A(\mathbb{R})$ has a finite index subgroup isomorphic to $(\mathbb{R}/\mathbb{Z})^{\dim(A)}$.

□

There has been a lot of work on the computation of Selmer groups for various isogenies on Jacobians of curves. The idea usually is to get a good description of $\mathrm{H}^1(G_k, J[\phi])$ where J is the Jacobian variety associated to a nice curve. It is usually done by connecting $H^1(G_k, J[\phi])$ to the group $\mathrm{H}^1(G_k, \mu_n(L \otimes \overline{k}))$ or $\mathrm{H}^1(G_k, \mu(L \otimes \overline{k})/\mu_n(\overline{k}))$ for some étale algebra L related to ϕ and some suitable n. In the latter case we call the image of $\mathrm{S}^{\phi}(J/k)$ inside $\mathrm{H}^1(G_k, \mu(L \otimes \overline{k})/\mu_n(\overline{k}))$ the *fake-Selmer group* and in the former case we call it the *true-Selmer group*. The case of p-descent for a prime p on elliptic curves is always a true descent. The case of 2-descent on odd-degree hyperelliptic Jacobians is a case of true descent. The following theorem explicitly describes the group $\mathrm{H}^1(G_k, J[2])$, where J is an odd-degree hyperelliptic Jacobian.

Proposition 1.5.2. [Sto, §5, Lemma 5.2, 5.6] *Let $C : y^2 = f(x)$ be an odd-degree hyperelliptic curve over k, J be its Jacobian variety, and $A \coloneqq k[T]/\langle f(T)\rangle$. Then*

$$\mathrm{H}^1(G_k, J[2]) \simeq \ker\left(\mathrm{N} : A^\times/(A^\times)^2 \to k^\times/(k^\times)^2\right),$$

where N *is the map induced by the norm map $A^\times \to k^\times$.*

Let θ be the image of T in A, i.e., a root of f in A. Let $P = (a, b)$ be a point on J given by the Mumford representation, with $d = \gcd(a, f)$. Then, the connecting morphism $\delta : J(k)/nJ(k) \to \mathrm{H}^1(G_k, J[2])$ is explicitly given by

$$(a, b) \mapsto (-1)^{\deg(a/d)}(a/d)(\theta)\left((-1)^{\deg(d)}d(\theta) + (-1)^{\deg(f/d)}(f/d)(\theta)\right).$$

Note that we have the identification $\bar{A} \simeq \overline{k}^{\deg(f)}$ and $A \hookrightarrow \bar{A}$. So any element of $\mathrm{H}^1(G_k, J[2])$ can be represented by a $\deg(f)$-tuple by $(a(e_i))_i$ with $a \in A^\times$ and e_i are all roots of f in $\overline{k}$.

There has been significant progress on the computation and implementation of various Selmer groups in the last three decades. We quickly mention here a few of them. Poonen and Schaefer [PS97] compute the λ-Selmer groups, where $\lambda \coloneqq 1 - \zeta_l$ is the isogeny on the Jacobians J_C of degree l-cyclic cover, C of $\mathbb{P}^1$. If a model of C is given by $y^l = f(x)$, then they give a homomorphism $x - T$ which is the composition $J_C/\lambda J_C \hookrightarrow \mathrm{S}^{(\lambda)}(J_C/k) \to A^\times/k^\times(A^\times)^l$, where $A \coloneqq k[T]/\langle f(T)\rangle$. Furthermore, they provide necessary and sufficient conditions for $x-T$ to be injective. Stoll and van Luijk [SvL13] gave an embedding of the λ-Selmer group inside another group which is easy to handle. Schaefer [Sch96], studied the connections between the Selmer groups and class groups. Stoll in [Sto01] gave an efficient implementation of computing 2-Selmer groups for Jacobians of hyperelliptic curves. Schaefer and Stoll [SS04] gave a way of computing the p-Selmer group of an elliptic curve for a prime p. In [BPS16], the authors give a way of performing n-descent on an isogeny with exponent n on an abelian variety. However, all these methods are constrained by the class groups computations and therefore, become impractical for not so large values of the exponent of the isogeny.

Chapter 2

Cassels-Tate Pairing

The Cassels-Tate pairing (CTP for short) was defined by Cassels for the case of elliptic curves, and generalized by Tate to the case of abelian varieties. Let A/k be an abelian variety with dual $\widehat{A}$. Then the CTP is a pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(A/k) \times Ш(\widehat{A}/k) \to \mathbb{Q}/\mathbb{Z},$$

which is non-degenerate on the maximal non-divisible quotients of the groups $Ш(A/k)$ and $Ш(\widehat{A}/k)$. If $\lambda : A \to \widehat{A}$ is a polarization, then we define a pull-back pairing on $Ш(A/k) \times Ш(A/k)$, that we again denote by $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$, via $\langle a, a' \rangle_{\mathrm{CT}} \coloneqq \langle a, \lambda(a) \rangle_{\mathrm{CT}}$. It was shown by Tate that if the polarization λ is induced by a k-rational divisor, then the induced pairing on $Ш(A/k) \times Ш(A/k)$ is alternating. For general principally polarized abelian varieties A/k, Flach [Fla90] showed that the pulled back pairing, $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$ on $Ш(A/k) \times Ш(A/k)$ is anti-symmetric. If $Ш(A/k)$ is finite (as is conjectured), and A is principally polarized, then $\#Ш(A/k)$ is a square, when $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$ is alternating. Poonen and Stoll [PS99] later showed that the deviation of CTP from being alternating for a principally polarized abelian variety A/k can be characterized by whether λ is induced by a k-rational divisor or only by a k-rational divisor class. However, the criterion for deciding whether $\#Ш(A/k)$ is a square or not is more complicated; see [PS99, §6].

In what follows, we assume that k is a number field and A/k is *principally polarized*, i.e., there exists a k-rational polarization $\lambda : A \to \widehat{A}$. In [PS99] the authors gave various examples where the pairing fails to be alternating. They also provide various definitions in the same paper. In this chapter, we review three different definitions of the Cassels-Tate pairing. The authors mention in [PS99, §3] another definition called the Albanese-Picard definition, however, for the case of curves the Albanese and the Picard varieties are identified. Furthermore, we will focus on one of the definitions, the Albanese-Albanese definition, more than the others, as we will use this definition to make the Cassels-Tate pairing effective in various cases in the later chapters. Furthermore, we will review these definitions in the cases when A/k is a Jacobian variety of a nice curve C/k of genus g. Recall from section §1.2.4 that J_C

is a principally polarized abelian variety with principal polarization defined using the Θ divisor, which is the image of $C_{\overline{k}}^{(g-1)}$ inside $\mathrm{Pic}^0(C_{\overline{k}})$, that we have identified with $J_{C_{\overline{k}}}$. Note that all these objects are defined over the base field k.

Before moving further, we need definition of some pairings that will be useful later.

2.1 Some pairings

Let V/k be a nice variety. Then the moving lemma (Lemma 1.2.2) implies that one can always find a representative of the class of $D \in \mathrm{Div}(V_{\overline{k}})$ in $\mathrm{Pic}\,(V_{\overline{k}})$ avoiding a given finite set of points. Let V/k and W/k be nice varieties and $D \in \mathrm{Div}(V_{\overline{k}} \times W_{\overline{k}})$ be a divisor. Recall from §1.2.3 and Theorem 1.2.10 that there is a homomorphism $\lambda_D : \mathrm{Alb}(V) \to \widehat{\mathrm{Alb}(W)}$ induced from the homomorphism $\lambda_D : \mathcal{Z}^0(V_{\overline{k}}) \to \mathrm{Pic}^0(W_{\overline{k}})$ with $\mathcal{Y}(V_{\overline{k}}) \subset \ker(\lambda_D)$. Let $\mathfrak{v} \in \mathcal{Y}(V_{\overline{k}})$, and $\mathfrak{w} \in \mathcal{Z}^0(W_{\overline{k}})$. Then $D(\mathfrak{v}) = \mathrm{div}(f)$ for some $f \in \overline{k}(W)$. Define $D(\mathfrak{v}, \mathfrak{w})$ by linearly extending the evaluation of f on points $w \in W(\overline{k})$, outside poles and zeros of f, i.e., if $\mathfrak{w} = \sum_{P \in W(\overline{k})} v_P(P)$ such that $v_P = 0$ for all but finitely many P and when $f(P) = 0$ or ∞, then

$$D(\mathfrak{v}, \mathfrak{w}) \coloneqq \prod_{P \in W(\overline{k})} f(P)^{v_P}.$$

Recall the definition of ${}^tD$ from §1.2.3. Similarly using ${}^tD$ one can define ${}^tD(\mathfrak{w}, \mathfrak{v})$, where $\mathfrak{w} \in \mathcal{Y}(W_{\overline{k}})$ and $\mathfrak{v} \in \mathcal{Z}^0(V_{\overline{k}})$. This gives partially defined pairings:

$$\langle \cdot, \cdot \rangle_1 : \big(\mathcal{Y}(V_{\overline{k}}) \times \mathcal{Z}^0(W_{\overline{k}})\big)^{\perp} \to \mathbb{G}_{\mathrm{m}} \quad \text{and} \quad \langle \cdot, \cdot \rangle_2 : \big(\mathcal{Z}^0(V_{\overline{k}}) \times \mathcal{Y}(W_{\overline{k}})\big)^{\perp} \to \mathbb{G}_{\mathrm{m}}, \tag{2.1.1}$$

defined as $\langle \mathfrak{v}, \mathfrak{w} \rangle_1 \coloneqq D(\mathfrak{v}, \mathfrak{w})$ and $\langle \mathfrak{v}, \mathfrak{w} \rangle_2 \coloneqq {}^tD(\mathfrak{w}, \mathfrak{v})$, where the superscript $\perp$ represents that the $\mathfrak{v}$ and $\mathfrak{w}$ are chosen in a compatible way, i.e., a function with divisor $D(\mathfrak{v})$ does not have a zero or a pole at the points in $\mathrm{Supp}(\mathfrak{w})$ while defining $\langle \cdot, \cdot \rangle_1$ and vice versa for $\langle \cdot, \cdot \rangle_2$. One can always do this using the moving lemma, i.e., Lemma 1.2.2. One checks that the above defined pairings are Galois equivariant.

In the case when $\mathfrak{v}$ represents a point in $\mathrm{Alb}(V)(\overline{k})[n]$, then $n\mathfrak{v} \in \mathcal{Y}(V)$. Let $\mathfrak{v}$ and $\mathfrak{w}$ represent points in $\mathrm{Alb}(V)(\overline{k})[n]$ and $\mathrm{Alb}(W)(\overline{k})[n]$, respectively. Using $D \in \mathrm{Div}(V \times W)$ one defines the following map.

Definition 2.1.1.

$$e_{D,n} : \mathrm{Alb}(V)(\overline{k})[n] \times \mathrm{Alb}(W)(\overline{k})[n] \to \mu_n(\overline{k}),$$

given by

$$e_{D,n}(v, w) \coloneqq \frac{D(n\mathfrak{v}, \mathfrak{w})}{{}^tD(\mathfrak{v}, n\mathfrak{w})} = \frac{\langle n\mathfrak{v}, \mathfrak{w} \rangle_1}{\langle \mathfrak{v}, n\mathfrak{w} \rangle_2},$$

where $\mathfrak{v}$ and $\mathfrak{w}$ are some lifts of v and w to 0-cycles such that everything makes sense.

It is shown in [Lan83][VI, VII] using Lang reciprocity that the above map is well-defined, bilinear and Galois-equivariant and depends only on the correspondence class of D.

Definition 2.1.2. In the case when $V = A$ and $W = \widehat{A}$, the pairing defined above using the Poincaré divisor is non-degenerate and is called the *Weil pairing* associated to an abelian variety. It is denoted by e_n.

However, we know that $\mathrm{Pic}^0(V) \simeq \mathrm{Pic}^0(A) \simeq \widehat{A}$, where $A := \mathrm{Alb}(V)$. Therefore, we would like to define the pairing using divisors and 0-cycles on $V_{\overline{k}}$. This gives rise to what is called as *Albanese-Picard definition* of the Weil pairing. Identify $\widehat{A}$ with $\mathrm{Pic}^0(V)$.

2.1.1 The Albanese-Picard definition of the Weil pairing

Let V, A and $\widehat{A}$ be as above and $\mathcal{P}$ be a Poincaré divisor on $A \times \widehat{A}$. Fixing a base point $P_0 \in V(\overline{k})$, one has the map $\phi_{V,P_0} : V(\overline{k}) \to \mathrm{Alb}(V)(\overline{k})$. We have the morphism $V_{\overline{k}} \times \widehat{A}_{\overline{k}} \overset{\phi_{V,P_0}\times \mathrm{id}}{\Longrightarrow} A_{\overline{k}} \times \widehat{A}_{\overline{k}}$. Pulling back the divisor $\mathcal{P}$ we obtain a divisor $\mathcal{P}_0 \in \mathrm{Div}(V_{\overline{k}} \times \widehat{A}_{\overline{k}})$. Let $D \in \mathrm{Div}^0(V_{\overline{k}})$. Then the divisor D represents a point on $\widehat{A}(\overline{k})$. Now choose a 0-cycle $z \in \mathcal{Z}^0(\widehat{A}_{\overline{k}})$ summing up to the class of D in $\widehat{A}_{\overline{k}}$. Since $[D]-z \in \mathcal{Y}(\widehat{A}_{\overline{k}})$ and the Albanese variety of an abelian variety is itself, ${}^t\mathcal{P}_0([D] - z) \in \mathrm{Princ}(V)$. In fact, as we have identified $\mathrm{Pic}^0(A_{\overline{k}})$ with $\mathrm{Pic}^0(V_{\overline{k}})$, by [Lan83] [IV, §4] we have that $D - {}^t\mathcal{P}_0(z) = \mathrm{div}(f_{D,z}) \in \mathrm{Princ}(V_{\overline{k}})$. Furthermore, if $\mathfrak{v} \in \mathcal{Y}(V_{\overline{k}})$, then one defines a pairing

$$[\cdot,\cdot] : \big(\mathcal{Y}(V_{\overline{k}}) \times \mathrm{Div}^0(V_{\overline{k}})\big)^{\perp} \to \mathbb{G}_{\mathrm{m}} \quad \text{via} \quad (\mathfrak{v}, D) \mapsto f_{D,z}(\mathfrak{v})\mathcal{P}_0(\mathfrak{v}, z), \tag{2.1.2}$$

where z and $\mathfrak{v}$ have been adjusted so that everything is defined. In [PS99, §3.2], the authors show that $[\cdot,\cdot]$ is a well-defined pairing, i.e., independent of the choices made. One has the natural pairing on $(\mathcal{Z}^0(V_{\overline{k}}) \times \mathrm{Princ}(V_{\overline{k}}))^{\perp}$ given by $(\mathfrak{v}, \mathrm{div}(f)) \mapsto f(\mathfrak{v})$. To define $[\mathfrak{v}, \mathrm{div}(f)]$, one can choose $z = 0$, which implies that

$$[\mathfrak{v}, \mathrm{div}(f)] = f(\mathfrak{v}).$$

For a divisor $D \in \mathrm{Div}^0(V_{\overline{k}})$ such that $[D] \in \mathrm{Pic}^0(V_{\overline{k}})[n]$, let $f_{nD} \in \overline{k}(V)^{\times}$ be such that $\mathrm{div}(f_{nD}) = nD$. In view of the above, one can define the Weil-pairing as follows:

Definition 2.1.3.

$$\begin{aligned} e_{V,n} : A(\overline{k})[n] \times \widehat{A}(\overline{k})[n] &\to \mu_n, \\ (\mathfrak{v}, D) &\mapsto \frac{f_{nD}(\mathfrak{v})}{[n\mathfrak{v}, D]}. \end{aligned}$$

The following proposition shows that the above pairing is independent of the choices made.

Proposition 2.1.4. *The map $e_{V,n}$ is a well-defined pairing, i.e., independent of the choices made.*

Proof. If we shift $\mathfrak{v}$ with a $\mathfrak{y} \in \mathcal{Y}(V_{\overline{k}})$, then the discrepancy is given by

$$e_{V,n}(\mathfrak{y}, D) = \frac{f_{nD}(\mathfrak{y})}{[n\mathfrak{y}, D]} = \frac{f_{nD}(\mathfrak{y})}{[\mathfrak{y}, nD]} = \frac{f_{nD}(\mathfrak{y})}{f_{nD}(\mathfrak{y})} = 1,$$

since definition 2.1.3 is clearly bilinear and $nD \in \mathrm{Princ}(V_{\overline{k}})$. Next, if we shift D by $\mathrm{div}(f)$, then again the discrepancy is given by

$$e_{V,n}(\mathfrak{v}, \mathrm{div}(f)) = \frac{f(\mathfrak{v})^n}{[n\mathfrak{v}, \mathrm{div}\, f]} = \frac{f(\mathfrak{v})^n}{n[\mathfrak{v}, \mathrm{div}\, f]} = \frac{f(\mathfrak{v})^n}{f(\mathfrak{v})^n} = 1.$$

□

Proposition 2.1.5. [BPS16, §4.3, 4.4]

The following hold.

1. *If $\phi : V \to V'$ is a morphism of nice k-varieties, $x \in \mathcal{Y}(V_{\overline{k}})$, and $D' \in \mathrm{Div}^0(V'_{\overline{k}})$, then $[\phi_*(\mathfrak{v}), D'] = [\mathfrak{v}, \phi^*(D')]$.*
2. *Let $A = \mathrm{Alb}(V)$. Then under the identification of $\widehat{A}(\overline{k})$ with $\mathrm{Pic}^0(V_{\overline{k}})$ the pairings $e_{V,n}$, $e_{A,n}$, e_n defined in definitions 2.1.3 and 2.1.2 are equal.*

2.1.2 Pairings in case of Jacobians

Recall from §1.2.4 that when V is a nice curve C, the Albanese and the Picard varieties J_C are canonically identified, and $J_C(\overline{k}) \overset{\lambda_\Theta}{\simeq} \mathrm{Pic}^0((J_C)_{\overline{k}})$. Therefore, using Proposition 2.1.5 we compute the Weil pairing using the Albanese-Albanese definition. Recall that $\Delta \in \mathrm{Div}(C_{\overline{k}} \times C_{\overline{k}})$ induces the same homomorphism as $\mathcal{P} \in \mathrm{Div}((J_C \times J_C)_{\overline{k}})$, i.e., $\mathrm{id} \in \mathrm{Hom}_{\overline{k}}(J_C \times J_C)$. Hence, the pairing $e_{\Delta,n} : J_C(\overline{k})[n] \times J_C(\overline{k})[n] \to \mu_n$ is the same as the one defined by $e_{\mathcal{P},n} : J_C(\overline{k})[n] \times J_C(\overline{k})[n] \to \mu_n$. If $\mathfrak{p}$ and $\mathfrak{q}$ are two elements of $\mathrm{Div}^0(C_{\overline{k}})$ representing elements of $J_C[n]$ with disjoint supports, then the Weil-pairing is given as follows.

Definition 2.1.6. Let $\mathfrak{p}$, $\mathfrak{q}$ be as above, and $f_{n\mathfrak{p}}$, $f_{n\mathfrak{q}}$ be functions such that $\mathrm{div}(f_{n\mathfrak{p}}) = n\mathfrak{p}$ and $\mathrm{div}(f_{n\mathfrak{q}}) = n\mathfrak{q}$. Then the pairing $e_{J_C,n}$ is given by

$$e_{J_C,n}([\mathfrak{p}], [\mathfrak{q}]) = \frac{\Delta(n\mathfrak{p}, \mathfrak{q})}{{}^t\Delta(n\mathfrak{q}, \mathfrak{p})} = \frac{f_{n\mathfrak{p}}(\mathfrak{q})}{f_{n\mathfrak{q}}(\mathfrak{p})},$$

where all the quantities are well defined.

We will drop the abelian variety from the notation of the Weil pairing whenever it is clear from the context.

2.1.3 Extension of the pairings $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$ for Jacobians

In this section we extend the two pairings $\langle\cdot,\cdot\rangle_i$ in Equation (2.1.1) to be defined entirely on $\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Div}^0(C_{\overline{k}})$ and $\mathrm{Div}^0(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})$ using the Δ divisor on $C_{\overline{k}} \times C_{\overline{k}}$, such that they are Galois equivariant. Such an extension will simplify the computation of the CTP in later chapters.

Choose uniformizers t_P for $P \in C(\overline{k})$ for the local rings $\mathcal{O}_P$ such that the map $P \mapsto t_P$ is Galois-equivariant, and consider the Galois-equivariant pairings

$$\langle\cdot,\cdot\rangle_1 \colon \left(\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Div}^0(C_{\overline{k}})\right) \to \mathbb{G}_{\mathrm{m}} \tag{2.1.3}$$

$$\langle\cdot,\cdot\rangle_2 \colon \left(\mathrm{Div}^0(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})\right) \to \mathbb{G}_{\mathrm{m}} \tag{2.1.4}$$

defined as follows.

$$\langle \mathrm{div}(f), D\rangle_1 \coloneqq \prod_P (f t_P^{-v_P(f)})(P)^{v_P(D)},$$

and

$$\langle D, \mathrm{div}(f)\rangle_2 \coloneqq \prod_P (-1)^{v_P(f)v_P(D)} (f t_P^{-v_P(f)})(P)^{v_P(D)}.$$

The above pairings are well-defined and extend the partially defined pairings in Equation (2.1.1). Next we show that the two pairings defined above agree on the diagonal $\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})$.

Proposition 2.1.7. *Let $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$ be as above. Then $\langle\cdot,\cdot\rangle_1 = \langle\cdot,\cdot\rangle_2$ on $\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})$.*

Proof. Define the *tame symbol* at P for two nonzero functions f and g as follows:

$$[f,g]_P \coloneqq (-1)^{v_P(f)v_P(g)} \frac{f^{v_P(g)}}{g^{v_P(f)}}(P).$$

We have

$$\begin{aligned}\frac{\langle \mathrm{div}(f), \mathrm{div}(g)\rangle_1}{\langle \mathrm{div}(f), \mathrm{div}(g)\rangle_2} &= \prod_P (-1)^{v_P(f)v_P(g)} \frac{\left(f t_P^{v_P(f)}\right)(P)^{v_P(g)}}{\left(g t_P^{v_P(g)}\right)(P)^{v_P(f)}} \\ &= \prod_P (-1)^{v_P(f)v_P(g)} \left(\frac{f^{v_P(g)}}{g^{v_P(f)}}\right)(P) = \prod_P [f,g]_P = 1.\end{aligned}$$

The last equality is a consequence of strong Weil reciprocity [Wei38]. □

The following corollary shows that the Weil pairing can be defined using the above modified definitions of $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$.

Corollary 2.1.8. *Let $P, Q \in J_C(\overline{k})[n]$ be represented by degree 0 divisors $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Then*

$$e_{J_C,n}(P,Q) = \frac{\langle n\mathfrak{p}, \mathfrak{q}\rangle_1}{\langle \mathfrak{p}, n\mathfrak{q}\rangle_2}.$$

Proof. Let $P, Q \in J_C(\overline{k})[n]$ be represented by degree 0 divisors $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Using the moving lemma 1.2.2, we can choose functions f_P and f_Q such that the divisors $\mathfrak{p} + \operatorname{div}(f_P)$ and $\mathfrak{q} + \operatorname{div}(f_Q)$ have disjoint support. We have

$$\begin{aligned} e_{J_C,n}(P,Q) &= \frac{\langle n\mathfrak{p} + n\operatorname{div}(f_P), \mathfrak{q} + \operatorname{div}(f_Q)\rangle_1}{\langle \mathfrak{p} + \operatorname{div}(f_P), n\mathfrak{q} + n\operatorname{div}(f_Q)\rangle_2} && \text{(Definition 2.1.6)} \\ &= \frac{\langle n\mathfrak{p}, \mathfrak{q}\rangle_1}{\langle \mathfrak{p}, n\mathfrak{q}\rangle_2} && \text{(Proposition 2.1.7)} \end{aligned}$$

□

Using Proposition 2.1.7 one can show that the Weil pairing (Definition 2.1.6) can be defined using the modified definition of $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$.

2.1.4 e_2 for hyperelliptic Jacobians

In this section, we give an explicit definition of the 2-Weil pairing for hyperelliptic Jacobians. Let $C : y^2 = f(x) \coloneqq \sum_{i=1}^{d} f_i x^i$ be a hyperelliptic curve over k of genus $g = [(d-1)/2]$ with Weierstrass points $T_i \coloneqq (e_i, 0)$, where $e_i \in \overline{k}$ are the roots of f. When d is even, then we denote by D_∞ the divisor $(O_+) + (O_-)$, where $O_* = (1, *\sqrt{f_{2g+2}}, 0)$. When d is odd, then we denote by D_∞ the divisor (O). Any point P is represented by a divisor of the form $D_P - nD_\infty$, where $D_P = \sum_{i=1}^{2n}(P_i)$ in case d is even, and $D_P = \sum_{i=1}^{n}(P_i)$ when d is odd, for some $P_i \in C(\overline{k})$. If P is a 2-torsion point, then P_i in the support of D_P are taken from the Weierstrass points. The following proposition gives a formula for the 2-Weil pairing in the case of hyperelliptic curves.

Proposition 2.1.9. *Let P and Q be two points of $J(\overline{k})[2]$ represented by $D_P - nD_\infty$ and $D_Q - mD_\infty$, where $D_P = \sum_{i=1}^{2n}(P_i)$ and $D_Q = \sum_{i=1}^{2m}(Q_i)$ and d is even. If d is odd and for some $n \in \mathbb{Z}$, $\deg(D_P) = 2n - 1$, then set $\tilde{D}_P \coloneqq D_P + D_\infty$ (similarly define $\tilde{D}_Q$). Otherwise, set $\tilde{D}_* \coloneqq D_*$. Therefore, $P = [\tilde{D}_P - 2nD_\infty]$ (similarly for Q), and*

$$e_2(P,Q) = (-1)^{\#(\operatorname{Supp}(\tilde{D}_P) \cap \operatorname{Supp}(\tilde{D}_Q))}.$$

Proof. We start by assuming $n, m = 1$. We prove the proposition in this case and then extend the result using the bilinearity of the Weil pairing to prove the above. We have $2D_P - 2D_\infty = \operatorname{div}(x - x(P_1)(x - x(P_2)))$ when $\deg(D_P) = 2$, and $2D_P - 2D_\infty = \operatorname{div}(x - x(P_1))$, when $\deg(D_P) = 1$ (similarly for Q). Choose uniformizers $(x - e_i)/y$ at a Weierstrass point $(e_i, 0)$ and x^g/y at O_+, O_- and O depending on if d is odd or even. For every other point R, we choose $x - x(R)$ as a uniformizer. It is clear that if $D_P = D_Q$, then $e_2(P,Q) = 1$ and the proposition holds. So we assume that

$D_P \neq D_Q$. The evaluation of $(x - x_0)(x - x_0')$ at D_∞ yields the same value for all $x_0, x_0' \in \overline{k}$, and cancels out while computing the pairing because $v_{D_\infty}(x - x_0)(x - x_0')$ is even. Furthermore, $v_R(x - e_i)$ is even for all $R \in \mathrm{Supp}(D_\infty)$. Hence, $\langle D_P, 2D_Q\rangle_2 = \langle 2D_Q, D_P\rangle_1$. Using the definitions of $\langle\cdot,\cdot\rangle_1$ in §2.1.3

$$\langle 2D_P, D_Q\rangle_1 = \begin{cases} \prod_{i,j\in\{1,2\}} (x(Q_i) - x(P_j)), & \text{if } P_1, P_2 \notin \{Q_1, Q_2\} = \emptyset, \\ \frac{f}{x - x(P_1)}(x(P_1))(x(P_1) - x(P_2)) & \cdot \prod_{i\in\{1,2\}} (x(Q_2) - x(P_2)), \\ & \text{if } \qquad Q_1 = P_1. \end{cases}$$

This implies that

$$e_2(P, Q) = \begin{cases} 1, & \text{if } \mathrm{Supp}(D_P) \cap \mathrm{Supp}(D_Q) = \emptyset, \\ -1, & \text{if } \qquad P_1 = Q_1, \end{cases}$$

when d is even or d is odd and $\deg(P)$ and $\deg(Q)$ are even. Doing a similar computation as above shows the following. If d is odd, then $(x - x_0)$ has an order 2 pole at ∞ for all $x_0 \in \overline{k}$. If $\deg(D_P) = 1 = \deg(D_Q)$, then

$$e_2(P, Q) = (-1)^{\#\mathrm{Supp}(\tilde{D}_P)\cap\mathrm{Supp}(\tilde{D}_Q)}.$$

If $\deg(D_P) = 1$ and $\deg(D_Q) = 2$, then using bilinearity of the Weil pairing, we have $e_2(P, Q) = -1 \iff \mathrm{Supp}(D_P) \subset \mathrm{Supp}(D_Q)$ as $D_Q = \tilde{D}_Q$, or equivalently

$$e_2(P, Q) = (-1)^{\#\mathrm{Supp}(\tilde{D}_P)\cap\mathrm{Supp}(\tilde{D}_Q)}.$$

In the general case one can write $\tilde{D}_*$ as a sum of divisors of degree 2 with disjoint supports. Let $\tilde{D}_P := \sum_{i=1}^{n} \tilde{D}_i - n\tilde{D}_\infty$ with $\tilde{D}_\infty = D_\infty$ if d is even and $2D_\infty$ if d is odd, and $\tilde{D}_i$ of degree 2 for each i and possibly at most one for one i, $D_i \neq \tilde{D}_i$. Similarly, we write $\tilde{D}_Q := \sum_{i=1}^{m} \tilde{D}_i' - m\tilde{D}_\infty$. The pairing is then the product of (-1) taken

$$\sum_{i,j} \#(\mathrm{Supp}(\tilde{D}_i) \cap \mathrm{Supp}(\tilde{D}_j')) = \#\left(\bigsqcup_{i,j} \tilde{D}_i \cap \tilde{D}_j\right) = \#\left(\mathrm{Supp}(\tilde{D}_i) \cap \mathrm{Supp}(\tilde{D}_j')\right)$$

many times. □

2.2 The homogeneous space definition

We identify $J(\overline{k})$ with $\mathrm{Pic}^0(C_{\overline{k}})$, and J with $\mathrm{Pic}^0(J_{\overline{k}})$ using λ_Θ. Let $a, a' \in Ш(J/k)$, and X be a locally everywhere soluble homogeneous space of J over k representing

a. Now $\mathrm{Pic}^0(X_{\overline{k}})$ is canonically isomorphic to $\mathrm{Pic}^0(J_{\overline{k}}) \simeq J(\overline{k})$ as a G_k-module. Applying Galois cohomology to the exact sequence

$$0 \to \mathrm{Princ}(X_{\overline{k}}) \to \mathrm{Div}^0(X_{\overline{k}}) \to \mathrm{Pic}^0(X_{\overline{k}}) \to 0,$$

we have that a' corresponds to an element of $\mathrm{H}^1(G_k, \mathrm{Pic}^0(X_{\overline{k}}))$, and therefore gives rise to an element b' of $\mathrm{H}^2(G_k, \mathrm{Princ}(X_{\overline{k}}))$. Using Galois cohomology on the following exact sequence

$$0 \to \overline{k}^\times \to \overline{k}(X)^\times \to \mathrm{Princ}(X_{\overline{k}}) \to 0,$$

one can lift b' to an element f' of $\mathrm{H}^2(G_k, \overline{k}(X)^\times)$ since $\mathrm{H}^3(k) = 0$ (Theorem 1.3.44). Let v be a place of k. Since, a' is locally trivial, f'_v is in the kernel of the map $\mathrm{H}^2(G_{k_v}, \overline{k_v}(X)^\times) \to \mathrm{H}^2(G_{k_v}, \mathrm{Princ}(X_{\overline{k_v}}))$. Hence, it corresponds to the image of an element $c_v \in \mathrm{H}^2(k_v)$. c_v can be computed by evaluating f'_v on any local point $Q_v \in X(k_v)$ that avoids the poles and zeros of f'_v.

Definition 2.2.1. Recall the local invariant map on local Brauer groups from Proposition 1.3.37. In view of the above, the homogeneous space definition of the CTP is given by

$$\langle a, a' \rangle_{\mathrm{CT},HS} := \sum_v \mathrm{inv}_v(c_v).$$

2.3 The Weil pairing definition

Let $t, t' \in Ш(J/k)[n]$. Let $a, a' \in \mathrm{S}^{(n)}(J/k)$ be lifts of t, t', respectively, to the n-Selmer group interpreted as elements in $\mathrm{H}^1(G_k, J[n])$. Let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ be lifts of a, a', respectively. Let $\beta \in \mathrm{C}^1(G_k, J[n^2])$ be a lift of α. Using the connecting morphism, $\delta : \mathrm{H}^1(G_k, J[n]) \to \mathrm{H}^2(G_k, J[n])$ in the long exact cohomology sequence of the following exact sequence:

$$0 \to J(\overline{k})[n] \to J(\overline{k})[n^2] \to J(\overline{k})[n] \to 0,$$

we obtain $\eta := \delta(\alpha) \vee \alpha' = \partial\beta \vee \alpha' \in \mathrm{Z}^3(k)$, where $\vee$ is the cup-product induced by the Weil-pairing $e_n : J[n] \times J[n] \to \mu_n$. Since $\mathrm{H}^3(k) = 0$ (Theorem 1.3.44), let $\varepsilon \in \mathrm{C}^2(k)$ be such that $\partial\varepsilon = \eta$.

This is the global part of the pairing. We now use the local triviality of a. For every place v of k, recall that x_v represents the localization of a cochain x. There is a point $Q_v \in J(\overline{k_v})$ such that $\partial Q_v = \alpha_v = n\beta_v$. Let $P_v \in J(\overline{k_v})$ be such that $nP_v = Q_v$. This implies that $\beta_v - \partial P_v \in \mathrm{C}^1(G_{k_v}, J[n])$. We obtain a 2-cocycle $\gamma_v = (\beta_v - \partial P_v) \vee \alpha'_v - \varepsilon_v \in \mathrm{Z}^2(k_v)$.

Definition 2.3.1. Let γ_v be as above and c_v be the class represented by γ_v in $\mathrm{Br}(k_v)$, then the Weil pairing definition of the Cassels-Tate pairing is given by

$$\langle t, t' \rangle_{\mathrm{CT},WP} := \sum_v \mathrm{inv}_v(c_v), \tag{2.3.1}$$

where recall that inv_v is the local-invariant map on the $\mathrm{Br}(k_v)$.

2.4 The Albanese-Albanese definition

We now explain the *Albanese-Albanese definition* of the Cassels-Tate pairing on $Ш(J_C/k)$ with respect to the diagonal correspondence $\Delta \in \mathrm{Div}(C_{\overline{k}} \times C_{\overline{k}})$ using standard notations for Galois cochains, cocycles, as defined in §1.1 and §1.3.3. We will write the group structure on these objects additively also when they take values in a multiplicative group. Let $a, a' \in Ш(J/k)$, represented by 1-cocycles α, α', respectively, with values in $J(\overline{k})$. Lift α, α' to cochains $\mathfrak{a}$, $\mathfrak{a}'$, respectively, with values in the group $\mathrm{Div}^0(C_{\overline{k}})$. The Galois equivariant pairings $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$ induce the cup-products $\cup_1$ and $\cup_2$ at the level of cochains. Using the long-exact cohomology sequence associated to the exact sequence

$$0 \to \mathrm{Princ}(C_{\overline{k}}) \to \mathrm{Div}^0(C_{\overline{k}}) \to \mathrm{Pic}^0(C_{\overline{k}}) \simeq J \to 0,$$

we obtain 1-cocycles $\partial\mathfrak{a}$ and $\partial\mathfrak{a}'$ in $\mathrm{Z}^2(G_k, \mathrm{Princ}(C_{\overline{k}}))$. Let $\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' \in \mathrm{C}^3(k)$. Note that the cup products in η make sense. It is easy to see that η is in fact a 3-cocycle:

$$\partial\eta = \partial^2\mathfrak{a} \cup_1 \mathfrak{a}' + \partial\mathfrak{a} \cup_1 \partial\mathfrak{a}' - \partial\mathfrak{a} \cup_2 \partial\mathfrak{a}' + \mathfrak{a} \cup_2 \partial^2\mathfrak{a}' = 0, \tag{2.4.1}$$

since $\partial^2 = 0$ and the pairings are compatible on $\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})$ by Proposition 2.1.7. By Theorem 1.3.44, $\mathrm{H}^3(k) = 0$ for any number field k. Hence, there exists a 2-cochain $\varepsilon \in \mathrm{C}^2(k)$ such that $\eta = \partial\varepsilon$.

Formally, η looks like $\partial(\mathfrak{a} \cup_i \mathfrak{a}')$, but $\mathfrak{a} \cup \mathfrak{a}'$ does not make sense, since we cannot in general pair the values of $\mathfrak{a}$ and $\mathfrak{a}'$, so we can understand ε as a substitute for $\mathfrak{a} \cup_i \mathfrak{a}'$ with $i \in \{1, 2\}$.

We now make use of the fact that a is everywhere locally trivial. Let v be a place of k. Then $\alpha_v = \partial\beta_v$ for some $\beta_v \in J(\overline{k_v})$. We lift β_v to an element $\mathfrak{b}_v$ of $\mathrm{Div}^0(C_{\overline{k_v}})$. Then $\mathfrak{a}_v - \partial\mathfrak{b}_v$ takes values in the group of principal divisors, and the same is true of $\partial\mathfrak{a}'_v$, so we can define

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \varepsilon_v.$$

Interpreting ε as $\mathfrak{a} \cup_i \mathfrak{a}'$, γ_v looks formally like $-\partial(\mathfrak{b}_v \cup_i \mathfrak{a}'_v)$, but again, $\mathfrak{b}_v \cup_i \mathfrak{a}'_v$ does not make sense. We have that γ_v is a 2-cocycle with values in $\overline{k_v}^\times$:

$$\begin{aligned}\partial\gamma_v &= \partial\mathfrak{a}_v \cup_1 \mathfrak{a}'_v - (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \partial\mathfrak{a}'_v - \partial\mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v + \mathfrak{b}_v \cup_2 \partial^2\mathfrak{a}'_v - \partial\mathfrak{a}_v \cup_1 \mathfrak{a}'_v + \mathfrak{a}_v \cup_2 \partial\mathfrak{a}'_v \\ &= -(\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \partial\mathfrak{a}'_v + (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_2 \partial\mathfrak{a}'_v = 0.\end{aligned}$$

Here we again need to use that the two pairings are compatible. So γ_v represents some $c_v \in \mathrm{H}^2(k_v) \cong \mathrm{Br}(k_v)$. Recall the local invariant map $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. In view of the above, the Albanese-Albanese definition of the CTP on $Ш(J_C/k) \times Ш(J_C/k)$ is given as follows:

Definition 2.4.1. For $a, a' \in Ш(J_C)$, we have:

$$\langle a, a' \rangle_{\mathrm{CT},AA} := \sum_v \mathrm{inv}_v(c_v).$$

We now show that the above definition is independent on the choices made in defining it.

Proposition 2.4.2. *The pairing defined in Definition 2.4.1 is well-defined.*

Proof. We enumerate through all the choices made to establish the proposition.

1. Changing ε by a cocycle $\zeta \in \mathrm{Z}^2(k)$. This changes γ_v by subtracting ζ_v where ζ represents $z \in \mathrm{Br}(k)$, so the value of the pairing changes by $-\sum_v \mathrm{inv}_v(z_v) = 0$ (by part 4 of Proposition 1.3.37).

2. Changing $\mathfrak{a}$ by a cochain $\mathfrak{f}$ with values in principal divisors. Replacing $\mathfrak{a}$ by $\mathfrak{a} + \mathfrak{f}$, η changes by adding $\partial\mathfrak{f} \cup_1 \mathfrak{a}' - \mathfrak{f} \cup_2 \partial\mathfrak{a}' = \partial(\mathfrak{f} \cup_1 \mathfrak{a}')$. The equality follows from the compatibility of the pairings $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$ on $\mathrm{Princ}(C_{\overline{k}}) \times \mathrm{Princ}(C_{\overline{k}})$. Therefore, ε changes by addition of $\mathfrak{f} \cup_2 \mathfrak{a}'$, but γ_v remains unchanged.

3. Changing $\mathfrak{a}'$ by a cochain $\mathfrak{f}$ with values in principal divisors. Replacing $\mathfrak{a}'$ by $\mathfrak{a} + \mathfrak{f}$, η changes by adding $\partial\mathfrak{a} \cup_1 \mathfrak{f} - \mathfrak{a} \cup_2 \partial\mathfrak{f} = \partial\mathfrak{a} \cup_2 \mathfrak{f} - \mathfrak{a} \cup_2 \partial\mathfrak{f} = \partial(\mathfrak{a} \cup_2 \mathfrak{f})$ (using the compatibility of the pairings). Hence, ε changes by addition of $\mathfrak{a} \cup_2 \mathfrak{f}$, and therefore γ_v changes by

$$\begin{aligned}(\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{f}_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{f}_v - \mathfrak{a}_v \cup_2 \mathfrak{f}_v &= (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_2 \mathfrak{f}_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{f}_v - \mathfrak{a}_v \cup_2 \mathfrak{f}_v \\ &= -\partial(\mathfrak{b}_v \cup_2 \mathfrak{f}_v),\end{aligned}$$

   so c_v is unchanged.

4. Changing α by a coboundary $\partial\kappa$, with $\kappa \in J(\overline{k})$. Lift $\partial\kappa$ to a cochain $\partial\mathfrak{k}$, with $\mathfrak{k} \in \mathrm{Div}^0(C_{\overline{k}})$ representing κ. This changes $\mathfrak{a}$ by adding $\partial\mathfrak{k}$ and η by adding $-\partial\mathfrak{k} \cup_2 \partial\mathfrak{a}' = -\partial(\mathfrak{k} \cup_2 \partial\mathfrak{a}')$. So we can subtract $\mathfrak{k} \cup \partial\mathfrak{a}'$ from ε to correct for that. Then γ_v changes by nothing.

5. Changing α' by a coboundary $\partial\kappa$, $\kappa \in J(\overline{k})$. Now lift ∂k to a cochain $\partial\mathfrak{k}$, with $\mathfrak{k} \in \mathrm{Div}^0(C_{\overline{k}})$ representing κ. This changes $\mathfrak{a}'$ by adding $\partial\mathfrak{k}$ and η by adding $\partial\mathfrak{a} \cup_1 \partial\mathfrak{k} = \partial(\partial\mathfrak{a} \cup_1 \mathfrak{k})$. So we can add $\partial\mathfrak{a} \cup_1 \mathfrak{k}$ to ε to correct for that. Then γ_v changes by

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \partial\mathfrak{k}_v - \partial\mathfrak{a}_v \cup_2 \mathfrak{k} = (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \partial\mathfrak{k}_v - \partial\mathfrak{a}_v \cup_1 \mathfrak{k} = \partial((\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{k}),$$

   c_v is unchanged.

6. Changing $\mathfrak{b}_v$ by a principal divisor $\mathfrak{f}_v$ changes γ_v by

$$-\partial\mathfrak{f}_v \cup_1 \mathfrak{a}' - \mathfrak{f}_v \cup_2 \partial\mathfrak{a}' = \partial(\mathfrak{f}_v \cup_2 \mathfrak{a}'_v),$$

which implies that c_v remains unchanged.

7. Consider changing β_v by adding a point $\kappa_v \in J(k_v)$. Lifting κ_v to $\mathfrak{k}_v \in \mathrm{Div}^0(C_{\overline{k_v}})$, and changing $\mathfrak{b}_v$ by adding $\mathfrak{k}_v$, changes γ_v by

$$-\partial\mathfrak{k}_v \cup_1 \mathfrak{a}'_v - \mathfrak{k}_v \cup_2 \partial\mathfrak{a}'_v.$$

Note that $\partial\mathfrak{k}_v$ takes values in principal divisors, as $\kappa_v \in J(k_v)$. Further, we have $\alpha'_v = \partial\beta'_v$, for some $\beta'_v \in J(\overline{k_v})$ by the local triviality of α'. Lifting β'_v to $\mathfrak{b}'_v$, we have $\mathfrak{f}'_v := \mathfrak{a}'_v - \partial\mathfrak{b}'_v$ takes values in principal divisors and $\partial\mathfrak{a}'_v = \partial\mathfrak{f}'_v$, therefore

$$\begin{aligned} -\partial\mathfrak{k}_v \cup_1 \mathfrak{a}'_v - \mathfrak{k}_v \cup_2 \partial\mathfrak{a}' &= -\partial\mathfrak{k}_\mathfrak{v} \cup_1 \mathfrak{f}'_v - \partial\mathfrak{k}_v \cup_1 \partial\mathfrak{b}'_v - \mathfrak{k}_v \cup_2 \partial\mathfrak{f}'_v \\ &= -\partial\mathfrak{k}_\mathfrak{v} \cup_2 \mathfrak{f}'_v - \partial\mathfrak{k}_v \cup_1 \partial\mathfrak{b}'_v - \mathfrak{k}_v \cup_2 \partial\mathfrak{f}'_v \\ &= \partial(\partial\mathfrak{k}_v \cup_1 \mathfrak{b}'_v) - \partial(\mathfrak{k}_v \cup_2 \mathfrak{f}'_v), \end{aligned}$$

which implies that c_v remains unchanged. It is worth noting here that this is the only place where the local triviality of a' is used.

□

One can extend the above definition of the CTP to define a *not* well-defined pairing on $Ш(J/k) \times \mathrm{H}^1(G_k, J)$ which is the same as the CTP when the second argument is from $Ш(J/k)$. We denote this map also by $\langle\cdot,\cdot\rangle_{\mathrm{CT}}$ for obvious reasons. In this regard, we have the following remark.

Remark 2.4.3. The analogous map $\langle\cdot,\cdot\rangle_{\mathrm{CT}} : Ш(J/k) \times \mathrm{H}^1(G_k, J(\overline{k})) \to \mathbb{Q}/\mathbb{Z}$ is well-defined up to the choice of β_v, i.e., changing β_v to $\beta_v + \kappa_v$ for some $\kappa_v \in J_C(k_v)$ changes the value of the pairing. Let $\mathfrak{k}_v \in \mathrm{Div}^0(C_{\overline{k_v}})$ be a lift of κ_v. Then by part 7 of the previous proposition, the change in the value of the pairing at the place v is given by $-\mathrm{inv}_v([\partial\mathfrak{k}_v \cup_1 \mathfrak{a}'_v + \mathfrak{k}_v \cup_2 \partial\mathfrak{a}'_v])$.

2.5 Equivalence of definitions

We show the equivalence of the Albanese-Albanese definition with the Weil pairing definition first.

2.5.1 Equivalence with the Weil-pairing definition

Proposition 2.5.1 ([PS99, Proposition 34]). *Let $a, a', \alpha, \alpha', \beta, \mathfrak{a}'$ be as in the Weil pairing and Albanese-Albanese definitions of the CTP. Let $\mathfrak{s}$ be a lift of β to degree-0 divisors. Then $n\mathfrak{s}$ is a lift of α to degree-0 divisors. If we take another lift $\mathfrak{a}$ of α to degree-0 divisors, then $\mathfrak{f} := \mathfrak{a} - n\mathfrak{s}$ takes values in principal divisors. Define η_w, η_a, $\hat{\eta}_a$ to be the 3-cocycles obtained in the Weil pairing definition, Albanese-Albanese definition using $\mathfrak{a}$ as a lift, Albanese-Albanese definition using $n\mathfrak{s}$ as a lift of α, respectively. If $\varepsilon_w, \varepsilon_a$, and $\hat{\varepsilon}_a$ are the 2-cochains trivializing η_w, η_a, and $\hat{\eta}_a$, respectively, then one can choose $\varepsilon_w, \varepsilon_a$ such that:*

$$\varepsilon_w - \varepsilon_a = -\mathfrak{s} \cup_2 n\mathfrak{a}' - \mathfrak{f} \cup_1 \mathfrak{a}'.$$

Proof. We have:

$$\begin{aligned}
\eta_w - \hat{\eta}_a &:= \partial\beta \vee \alpha' - \partial n\mathfrak{s} \cup_1 \mathfrak{a}' + n\mathfrak{s} \cup_2 \partial\mathfrak{a}' \\
&= n\partial\mathfrak{s} \cup_1 \mathfrak{a}' - \partial\mathfrak{s} \cup_2 n\mathfrak{a}' - \partial n\mathfrak{s} \cup_1 \mathfrak{a}' + n\mathfrak{s} \cup_2 \partial\mathfrak{a}' \\
&= -\partial\mathfrak{s} \cup_2 n\mathfrak{a}' + \mathfrak{s} \cup_2 \partial n\mathfrak{a}' \\
&= -\partial(\mathfrak{s} \cup_2 n\mathfrak{a}')
\end{aligned}$$

Hence, we can choose $\hat{\varepsilon}_a$ such that $\varepsilon_w - \hat{\varepsilon}_a = -\mathfrak{s} \cup_2 n\mathfrak{a}'$. Since $\mathfrak{a} = n\mathfrak{s} + \mathfrak{f}$, we can choose ε_a such that $\varepsilon_a = \hat{\varepsilon}_a + \mathfrak{f} \cup_1 \mathfrak{a}'$. Combining with relation between $\varepsilon_w, \hat{\varepsilon}_a$ we have:

$$\varepsilon_w - \varepsilon_a = -\mathfrak{s} \cup_2 n\mathfrak{a}' - \mathfrak{f} \cup_1 \mathfrak{a}'.$$

□

To see that the Weil-pairing and the Albanese-Albanese definitions are equivalent, we now consider the local part. Keeping the notation as in the previous proposition, let v be a place of k and $\gamma_{v,w}$ and $\hat{\gamma}_{v,a}$ be the local 2-cocycles obtained during the local parts of the Weil pairing, and the Albanese-Albanese definition with $n\mathfrak{s}$ as a lift of α, respectively. Let $P_v, Q_v \in J_C(\overline{k_v})$ be such that $\partial Q_v = \alpha_v$ and $nP_v = Q_v$, $\mathfrak{p}_v \in \mathrm{Div}^0(C_{\overline{k_v}})$ be a lift of P_v, and $\mathfrak{q}_v = n\mathfrak{p}_v$ be a lift of Q_v. Then

$$\begin{aligned}
\gamma_{v,w} - \hat{\gamma}_{v,a} &= (\beta_v - \partial P_v) \vee \alpha'_v - (n\mathfrak{s}_v - \partial\mathfrak{q}_v) \cup_1 \mathfrak{a}'_v + \mathfrak{q}_v \cup_2 \partial\mathfrak{a}'_v + \mathfrak{s}_v \cup_2 n\mathfrak{a}'_v \\
&= (n\mathfrak{s}_v - \partial n\mathfrak{p}_v) \cup_1 \mathfrak{a}'_v - (\mathfrak{s}_v - \partial\mathfrak{p}_v) \cup_2 n\mathfrak{a}'_v - (n\mathfrak{s}_v - \partial\mathfrak{q}_v) \cup_1 \mathfrak{a}'_v \\
&\quad + \mathfrak{q}_v \cup_2 \partial\mathfrak{a}'_v + \mathfrak{s}_v \cup_2 n\mathfrak{a}'_v \\
&= \partial\mathfrak{p}_v \cup_2 n\mathfrak{a}'_v + \mathfrak{q}_v \cup_2 \partial\mathfrak{a}'_v = \partial\mathfrak{p}_v \cup_2 n\mathfrak{a}'_v + \mathfrak{p}_v \cup_2 n\partial\mathfrak{a}'_v = \partial(\mathfrak{p}_v \cup_2 n\mathfrak{a}'_v).
\end{aligned}$$

Therefore, $[\gamma_{v,w}] = [\hat{\gamma}_{v,a}] \in \mathrm{Br}(k_v)$, and $\langle a, a' \rangle_{\mathrm{CT},WP} = \langle a, a' \rangle_{\mathrm{CT},AA}$.

2.5.2 Equivalence with the homogeneous space definition

Showing equivalence with the homogeneous space definition requires a bit more work. We will briefly introduce the Albanese-Picard definition for a nice variety V/k with Albanese variety A/k and Picard variety A'/k. The procedure is very close to the one for the Albanese-Albanese definition, but the cup product $\cup_1$ is induced by the pairing (2.1.2), and $\cup_2$ is induced by the natural pairing $(\mathcal{Z}^0(V_{\overline{k}}) \times \mathrm{Princ}(V_{\overline{k}}))^{\perp} \to \mathbb{G}_{\mathrm{m}}$. We denote this by $\langle \cdot, \cdot \rangle_{\mathrm{CT},AP} : Ш(A/k) \times Ш(A'/k) \to \mathbb{Q}/\mathbb{Z}$. Similarly to part 1 of Proposition 2.1.5, we have the following functoriality for the Albanese-Picard definition of the CTP.

Proposition 2.5.2. [PS99, Proposition 31] *Let V/k be a nice variety and $A := \mathrm{Alb}(V)$. Fix a point $P_0 \in V(\overline{k})$. Then the Albanese morphism $\phi_{V_{\overline{k}}} : V_{\overline{k}} \to A_{\overline{k}}$ induces k-rational isomorphisms $\phi_* : A \to \mathrm{Alb}(A)$ and $\phi^* := \mathrm{Pic}^0(A_{\overline{k}}) \to \mathrm{Pic}^0(V_{\overline{k}})$. Here we have dropped the dependence on V in ϕ_* and ϕ^* in order to simplify the notation. Let $a \in Ш(A/k)$, and $a' \in Ш(\mathrm{Pic}^0(A/k))$. Then*

$$\langle a, \phi^*(a') \rangle_{\mathrm{CT},AP} = \langle \phi_*(a), a' \rangle_{\mathrm{CT},AP},$$

where the CTP on the LHS is with respect to V and on the RHS is with respect to A.

Let J be a Jacobian variety, let a and $a' \in Ш(J/k)$, and let X be a principal homogeneous space of J corresponding to a. Then $\mathrm{Alb}(X) \simeq J$. By Proposition 2.5.2, it suffices to show that $\langle a, a' \rangle_{\mathrm{CT},AP} = \langle a, a' \rangle_{\mathrm{CT},HS}$, where the LHS is with respect to X. We may take $\mathfrak{a}$, the lift of a to $\mathrm{C}^1(G_k, \mathcal{Z}^0(X_{\overline{k}}))$, to be ∂P, for some $P \in X(\overline{k})$ (here a is interpreted as an element in $\mathrm{H}^1(G_k, \mathrm{Alb}(X)(\overline{k}))$. Choose $\mathfrak{a}' \in \mathrm{C}^1(G_k, \mathrm{Div}^0(X_{\overline{k}}))$ representing a'. Then $\partial \mathfrak{a}' = f' \in \mathrm{Z}^2(G_k, \mathrm{Princ}(X_{\overline{k}}))$. The element $c_v \in \mathrm{Br}(k_v)$ is obtained by evaluating f'_v at the k_v-rational point Q_v of X. In the Albanese-Picard definition, we may choose $\mathfrak{b}_v = P_v - Q_v \in \mathcal{Z}^0(X_{\overline{k_v}})$. Therefore,

$$\eta = \partial \mathfrak{a} \cup \mathfrak{a}' - \mathfrak{a} \cup \partial \mathfrak{a}' = -\partial P \cup f' = \partial(-P \cup f').$$

Hence, we may take $\varepsilon = -P \cup f'$, and γ_v can be shown to be $Q_v \cup f'_v$ which is exactly the class of c_v from the homogeneous space definition.

Hence, from now on we will drop the subscripts WP, AA, and HS from the notation of the CTP and use $\langle \cdot, \cdot \rangle_{\mathrm{CT}}$ only.

2.6 Previous computation of the CTP

In the realm of elliptic curves, the CTP on $\mathrm{S}^{(2)}(E/k)$ was computed by Cassels [Cas98] using explicit models for 2-coverings representing elements of the 2-Selmer group and a combination of the Weil-pairing definition and the homogeneous space definitions. In [Bea00], Beaver computed the CTP on ϕ-Selmer groups on elliptic curves, where

ϕ is an isogeny of degree 5. Later Cassels's approach was generalized by Swinnerton-Dyer [SD13], Fisher and Newton [FN14], and Fisher and van Beek [FvB18] to compute the CTP on $\text{Ш}^{(2)}(E/k) \times \text{Ш}^{(2^m)}(E/k)$, $\text{Ш}^{(p)}(E/k) \times \text{Ш}^{(p)}(E/k)$, and for Selmer groups of isogenies of odd prime degrees, respectively. Using an approach of Donnelly based on the homogeneous space definition of the CTP, Fisher [Fis22] has given another way of computing the CTP on $\text{Ш}^{(2)}(E/K) \times \text{Ш}^{(2)}(E/K)$. Fisher also has an approach based on the homogeneous space definition for $\text{Ш}^{(3)}(E/K) \times \text{Ш}^{(3)}(E/K)$ (unpublished). In the next chapter we will use the Albanese-Albanese definition of the CTP to compute it, following the manuscript [SS23].

The story is rather far from complete for the Jacobians of higher genus curves. Jiali Yan, in her PhD thesis [Yan21b], [FY23], [Yan21a] gave algorithms to compute the Cassels-Tate pairing on [2] and $(2,2)$-isogeny Selmer groups, assuming all the Weierstrass points of the genus 2 hyperelliptic are defined over k [Yan21a], and on $\text{Ш}^{(2)}(J/k)$, assuming that the twisted Kummer surface has a k-rational point [FY23]. In all the above cases, the authors used one or both of the Weil-pairing definition and the homogeneous space definition of the CTP to obtain an algorithm. The algorithm obtained in [FY23] (though conditional) seems to be very efficient in practice. In Chapter 4 we give an algorithm to compute the CTP on the 2-Selmer groups of odd-degree hyperelliptic Jacobians. In Chapter 5 and 6 we obtain algorithms to compute the CTP on various isogenies on the Jacobians of certain types of curves.

The major obstacle in obtaining an algorithm using the Albanese-Albanese definition is to compute $\varepsilon \in \text{C}^2(k)$ trivializing $\eta \in \text{Z}^3(k)$. We overcome this by showing that computing ε is equivalent to computing some 1-cochains $e \in \text{C}^1(k)$ for some 2-cocycles $E \in \text{Z}^2(k)$ such that $\partial e = E$, where each E is obtained using η. The advantages of our methods are

1. Computing the pairing involves only computations in the Galois cohomology of number fields, with minimal reference to the geometry of the Jacobian variety.

2. Computing the pairing does not involve dealing with any explicit equations for principal homogeneous spaces of J.

3. We do not need to extend to any larger field extension (for example to the field of definition of n^2-torsion points as required in the Weil pairing definition) than already required for the definition of the Selmer elements when represented as 1-cocycles.

4. One can even compute the pairing in the case of certain isogenies for Jacobians of higher genus curves.

The disadvantage of our current method is that trivializing 2-cocycles representing the trivial class in the Brauer group of a number field is known to be a computationally hard problem, and not using any information on the geometry of the Jacobian

variety and its principal homogeneous space implies that the algorithms become inefficient very quickly as the degree of the field of definition of kernel of the isogeny in question grows. One can certainly hope to get more efficient algorithms if one combines the cohomological computations with the information on the geometry of principal homogeneous spaces.

Chapter 3

The CTP for elliptic curves

In this chapter we compute the CTP on 2-Selmer groups of elliptic curves using the Albanese-Albanese definition of the pairing. This chapter is based on the manuscript [SS23] (joint work with Michael Stoll). The CTP on 2-Selmer groups of elliptic curves has been computed before by Cassels himself using explicit descriptions of elements of the 2-Selmer group [Cas98]. However, it was not clear to Cassels whether the pairing computed by his method is indeed the CTP. It was proven later in [FSS10] using abstract methods that the pairing which Cassels computed is indeed the CTP. By computing the CTP using the Albanese-Albanese definition we give a more explicit proof of this result. On the other hand, to the best of our knowledge this is the first attempt to make the Albanese-Albanese definition of the CTP explicit.

We set some notations useful for this chapter beforehand.

3.1 Notation

Throughout this chapter E will be an elliptic curve over a number field k given by the equation

$$Y^2 = f(X) = X^3 + cX + d,$$

where $c, d \in k$, and $E[2]$ will denote the G_k–module $E(\overline{k})[2]$. Let $e_1, e_2, e_3 \in \overline{k}$ be the roots of f, let $T_i \coloneqq (e_i, 0)$ for $i \in \{1, 2, 3\}$, and let $T_0 \coloneqq \infty$ be the unique point at infinity. Recall the definition of M^Δ from Definition 1.3.41 for a finite G_k–set Δ and a G_k–module M. For $\Delta \coloneqq \{T_1, T_2, T_3\}$ we have

$$\mu_2^\Delta \cong E[2] \oplus \langle (-1)(T_1) + (-1)(T_2) + (-1)(T_3) \rangle;$$

the inclusion $E[2] \hookrightarrow \mu_2^\Delta$ is induced by the Weil pairing (§2.1.4), $P \mapsto \sum_{T \in \Delta} e_2(P, T)(T)$. Let $L \coloneqq k[X]/\langle f(X) \rangle$ be the étale algebra associated to Δ. Then

$$\mathrm{H}^1(G_K, E[2]) \cong \ker\left(\mathrm{N}\colon L^\times/(L^\times)^2 \longrightarrow k^\times/(k^\times)^2\right), \tag{3.1.1}$$

where N denotes the map induced by the norm map from L to k.

The elements of $L^\times/(L^\times)^2$ can be represented by elements of $L^\times$, which can be written in the form $\beta = l_0 + l_1\theta + l_2\theta^2$, where $l_0, l_1, l_2 \in k$ and θ is the image of x in L. We set $\beta_i = l_0 + l_1 e_i + l_2 e_i^2 \in k(e_i)^\times$. Under the identification $L \hookrightarrow \bar{L} \cong \overline{k}^3$, β is then mapped to $(\beta_1, \beta_2, \beta_3)$.

If β represents an element a of $\mathrm{H}^1(G_k, E[2])$ via (3.1.1), then $\beta_1\beta_2\beta_3 \in (k^\times)^2$. Fix square-roots $\sqrt{\beta_i}$ of β_i, for $1 \leq i \leq 3$, and consider the formal sum $\sum_{i=1}^{3} \sqrt{\beta_i}(T_i) \in \bar{L}^\times = \mathbb{G}_{\mathrm{m}}^{\Delta}$. This element is a square root $\sqrt{\beta}$ of $\beta \in L^\times$ considered as an element of $\mathbb{G}_{\mathrm{m}}^{\Delta}$. The 1-coboundary $\sigma \mapsto \sigma\sqrt{\beta}/\sqrt{\beta}$ then takes values in μ_2^{Δ} because β is fixed by G_k and represents

$$\chi_a(\sigma) \coloneqq \frac{\sigma \cdot \left(\sum_{i=1}^{3} \sqrt{\beta_i}(T_i)\right)}{\left(\sum_{i=1}^{3} \sqrt{\beta_i}(T_i)\right)}. \tag{3.1.2}$$

The cocycle χ_a is associated to a 1-cocycle representing a via $(\mathbb{Z}/2\mathbb{Z})^{\Delta} \to E[2]$ sending $\sum_{i=1}^{3} a_i(T_i) \mapsto \sum_{i=1}^{3} a_i T_i$ and the identification $\mu_2 \cong \mathbb{Z}/2\mathbb{Z}$ as G_k-modules.

Note that $\mu_2^{\Delta} \simeq \bigoplus_{\text{orbits}} \mu_2^{\Delta_i}$, where Δ_i are the G_k orbits of Δ. This induces an isomorphism $\mathrm{Z}^1(G_k, \mu_2^{\Delta}) \simeq \bigoplus_{\text{orbits}} \mathrm{Z}^1(G_k, \mu_2^{\Delta_i})$, so $\chi_a(\sigma)$ factors through the orbits of Δ, i.e., $\chi_a(\sigma) = \sum_{\text{orbits}} \chi_{a,i}(\sigma)$, where $\chi_{a,i}$ corresponds to a χ_a when the support Δ is replaced by a G_k–orbit Δ_i of Δ. We associate with $\sum_{i=1}^{3} a_i(T_i) \in \mu_2^{\Delta}$ the triple $(a_1, a_2, a_3) \in \mu_2^3$, and henceforth we will use this representation for the elements of μ_2^{Δ}. Write $\hat{0}$ for the triple $(1,1,1)$ and $\hat{i}$ for the triple with 1 in the ith position, and -1 elsewhere. The action of G_k on the triples in μ_2^3 is induced from the action on μ_2^{Δ}. If (x_1, x_2, x_3) is a triple representing an element of $(\mu_2^{\Delta})^{G_k}$, then define the product $\prod_i^{\diamond} x_i$ to be the product taken over one representative i of each G_k–orbit on Δ (note that $x_i = x_j$ when i and j are in the same orbit).

In the general case, $\mathrm{Gal}(k(\sqrt{\beta_1}, \sqrt{\beta_2})) \simeq S_3 \rtimes C_2^2$, where S_3 acts via permutation on the set $\{e_1, e_2, e_3\}$, and the two copies of the cyclic group of order 2, i.e., C_2 act by flipping the sign of $\sqrt{\beta_1}$ and $\sqrt{\beta_2}$, respectively. Throughout this chapter we work under the assumption that we are in a fairly generic setting, i.e., we assume that $\mathrm{Gal}(k(\sqrt{\beta_1}, \sqrt{\beta_2})) \simeq H \rtimes N \subset S_3 \rtimes C_2^2$, with $H \subset S_3$ and $N \subset C_2^2$, and the above holds for every 2-Selmer element we will consider.

In the following subsection we recall another definition of the CTP, which we call *Cassels' pairing*, that was given by Cassels in [Cas98].

3.1.1 Cassels' pairing

Let $a, a' \in \mathrm{Ш}^{(2)}(E/k)$ be represented by $\beta = (\beta_1, \beta_2, \beta_3)$ and $\beta' = (\beta'_1, \beta'_2, \beta'_3)$ as discussed above, and for pairwise distinct $1 \leq i, j, k \leq 3$, define quadratic forms in variables (U_1, U_2, U_3, T) by

$$H_i(U_1, U_2, U_3, T) := (\beta_j \Gamma_j^2 - \beta_k \Gamma_k^2)/(e_j - e_k) + T^2, \tag{3.1.3}$$

where $\Gamma_i := U_1 + U_2 e_i + U_3 e_i^2$. Note that $(U_1, U_2, U_3) \mapsto (\Gamma_1, \Gamma_2, \Gamma_3)$ is just a linear change of coordinates, and H_i is defined over $k(e_i)$. Any two of these quadratic forms define the same projective curve D_a in $\mathbb{P}^3$ with coordinates U_1, U_2, U_3, T. Choosing $j, k \in \{1, 2, 3\}$ cyclically for a given $i \in \{1, 2, 3\}$ we get $\sum_{i=1}^{3} (e_j - e_k) H_i = 0$. Hence, any two of the H_i define the same genus 1 curve D_a over k. The curve D_a has points for every completion k_v of k and is a 2-covering of E representing a. For details, see [Cas98, §2]. Since D_a has a point on the affine patch $T \neq 0$ locally everywhere, each H_i has a non-trivial solution over $k_v(e_i)$ for every place v of k, and therefore each H_i has a solution over every completion of $k(e_i)$. This implies that there is a point $\mathfrak{q}_i := (\mathfrak{u}_{i1} : \mathfrak{u}_{i2} : \mathfrak{u}_{i3} : 1)$ or $(\Gamma_{ij}^* : \Gamma_{ik}^* : 1)$ defined over $k(e_i)$ satisfying: $H_i = 0$ for each i, which is a consequence of the local-global principle for quadratic forms. Let $L_i(U_1, U_2, U_3, T)$ over $k(e_i)$ for $1 \leq i \leq 3$ be a linear form such that $L_i = 0$ is the tangent to H_i at $\mathfrak{q}_i$.

If $\mathfrak{q}_v$ is a point defined on D_a over k_v, then the Cassels' pairing [Cas98, Lemma 7.4] is defined as follows:

$$\langle \alpha, \alpha' \rangle_{\mathrm{Cas}} := \prod_v \prod_i{}^{\diamond} (L_i(\mathfrak{q}_v), \beta'_i)_{k_v(e_i)}. \tag{3.1.4}$$

In [Cas98], Cassels showed that the above definition gives a well-defined pairing and is independent of the choices made.

3.1.2 Some useful formulas

We now recall some equations which will be useful later. Let $P = (x, y)$ on E/k. Then

$$P + T_i = \left(\frac{e_i x + e_j e_k - e_i(e_j + e_k)}{(x - e_i)}, \frac{-(e_j - e_i)(e_k - e_i) y}{(x - e_i)^2} \right), \tag{3.1.5}$$

where $\{i, j, k\} = \{1, 2, 3\}$. Using the fact that the line through P and T_i passes through $-P - T_i$ and Equation (3.1.5), we deduce that

$$\frac{x(\pm P + T_i) - e_i}{x(\pm P) - e_i} = \frac{(e_j - e_i)(e_k - e_i)}{(x - e_i)^2} = -\frac{y(\pm P + T_i)}{y(\pm P)} \tag{3.1.6}$$

We also deduce from (3.1.5) that

$$x(\pm P + T_j) - e_i = \frac{(x - e_k)(e_j - e_i)}{(x - e_j)}, \tag{3.1.7}$$

which, along with the fact that the line passing through $P + T_i$ and T_k passes through $-P + T_j$, gives

$$\frac{y(\pm P + T_i)(x(\pm P) - e_k)}{y(\pm P)(x(\pm P + T_i) - e_k)} = \frac{(3d + 2ce_i)(x - e_k)}{e_i(x - e_i)(x - e_j)(e_i - e_k)} = \frac{(x - e_k)^2(e_j - e_i)}{y^2}. \tag{3.1.8}$$

3.2 Computing the CTP on $\mathrm{S}^2(E/k) \times \mathrm{H}^1(G_k, \langle T_1 \rangle)$

In this section we compute the CTP on $\mathrm{S}^2(E/k) \times \mathrm{H}^1(G_k, \langle T_1 \rangle)$ (in the sense of §2.4), assuming that $e_1 \in k$, i.e., $[k(E[2]) : k] \leq 2$. Remark 2.4.3 implies that the value of the CTP thus obtained depends on the choices made during the local part of the computation. Therefore, it is one of the possible values of the CTP on $\mathrm{S}^{(2)}(E/k) \times \mathrm{H}^1(G_k, \langle T_1 \rangle)$. Henceforth, we will always assume $1 \leq i, j, k \leq 3$, and if any subset of i, j, k appear together in an expression, they will be pairwise distinct. We use the notation from §3.1 during the process.

We begin with an explicit description of $a \in \mathrm{S}^{(2)}(E/k)$ and $a' \in \mathrm{H}^1(G_k, \langle T_1 \rangle) \simeq k^\times/(k^\times)^2$, represented by the triple $(\beta_1, \beta_2, \beta_3)$ and $\beta' \in k^\times$, respectively. Let the 1-cocycles α and α' representing a and a', respectively, be as follows:

$$\alpha(\sigma) = \begin{cases} T_0, & \text{if } \chi(\sigma) = \widehat{0}, \\ T_i, & \text{if } \chi(\sigma) = \widehat{i}, \end{cases} \quad \text{and} \quad \alpha'(\sigma) = \begin{cases} T_0, & \text{if } \chi'(\sigma) = 1, \\ T_1, & \text{if } \chi'(\sigma) = -1. \end{cases}$$

Here $\chi = \chi_\alpha$ (as defined in Equation (3.1.2)), but we have dropped the subscript for simplicity of notations. Further, $\chi'(\sigma) \coloneqq \sigma(\sqrt{\beta'})/\sqrt{\beta'}$, for a fixed square root $\sqrt{\beta'}$ of β'.

The next two subsections are dedicated to the computation of the CTP when a, a' are as above.

3.2.1 Global computation

Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(E_{\overline{k}})$ as follows:

$$\mathfrak{a}(\sigma) = \begin{cases} 0, & \text{if } \chi(\sigma) = \widehat{0}, \\ (T_i) - (T_0), & \text{if } \chi(\sigma) = \widehat{i}, \end{cases} \quad \text{and} \quad \mathfrak{a}'(\sigma) = \begin{cases} 0, & \text{if } \chi'(\sigma) = 1, \\ (T_1) - (T_0), & \text{if } \chi'(\sigma) = -1. \end{cases}$$

We have:

$$\partial\mathfrak{a}(\sigma,\tau) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0}, \\ 2(T_i) - 2(T_0) = \mathrm{div}(x - e_i), & \text{if } \chi(\sigma) = \widehat{i},\ \sigma \cdot \chi(\tau) = \widehat{i}, \\ (T_i) + (T_j) - (T_k) - (T_0) = \mathrm{div}(\frac{y}{x-e_k}), & \text{if } \chi(\sigma) = \widehat{i},\ \sigma \cdot \chi(\tau) = \widehat{j}. \end{cases} \tag{3.2.1}$$

Similarly, for $\mathfrak{a}'$ we have:

$$\partial\mathfrak{a}'(\sigma,\tau) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi'(\sigma) = 1 \text{ or } \chi'(\tau) = 1, \\ 2(T_1) - 2(T_0) = \mathrm{div}(x - e_1), & \text{if } \chi'(\sigma) = \chi'(\tau) = -1. \end{cases} \tag{3.2.2}$$

Let t_P denote a unifomizer at a point $P \in E(\overline{k})$. We assume $t_{T_0} = x/y$, $t_{T_i} = -(x - e_i)/y$ and $t_P = x - x(P)$ at all other points $P \notin E[2]$. The map defined by $P \mapsto t_p$, is Galois-equivariant. It is not hard to check that $\langle \mathrm{div}(f), D\rangle_1 = \langle D, \mathrm{div}(f)\rangle_2$, where $\mathrm{div}(f)$ and D appear in the values taken by $\partial\mathfrak{a}$, $\partial\mathfrak{a}'$, $\mathfrak{a}$, and $\mathfrak{a}'$. In what follows, we write $\langle f, D\rangle_1$ for $\langle \mathrm{div}(f), D\rangle_1$ in order to simplify the notation. Therefore,

$$\begin{aligned} \langle (x-e_i), (T_i) - (T_0)\rangle_1 &= \frac{y^2/(x-e_i)(T_i)}{(x-e_i)x^2/y^2(T_0)} = (e_i - e_j)(e_i - e_k), \\ \langle (x-e_i), (T_j) - (T_0)\rangle_1 &= \frac{(x-e_i)(T_j)}{(x-e_i)x^2/y^2(T_0)} = (e_j - e_i), \\ \langle y/(x-e_k), (T_i) - (T_0)\rangle_1 &= \frac{-y^2/(x-e_k)(x-e_i)(T_i)}{x/(x-e_k)(O)} = (e_j - e_i), \\ \langle y/(x-e_k), (T_k) - (T_0)\rangle_1 &= \frac{-y(x-e_k)/y(x-e_k)(T_k)}{x/(x-e_k)(O)} = -1. \end{aligned}$$

For $i \neq j$, we set $s_{ij} \coloneqq e_i - e_j$, and $s_i \coloneqq s_{ij}s_{ik}$. For $\sigma, \tau, \rho \in G_k$, the cup product, $(\partial\mathfrak{a} \cup_1 \mathfrak{a}')(\sigma,\tau,\rho)$ (resp. $(\mathfrak{a} \cup_2 \partial\mathfrak{a}')(\sigma,\tau,\rho)$) via the pairing $\langle\cdot,\cdot\rangle_1$ (resp. $\langle .,.\rangle_2$) is $\langle \partial\mathfrak{a}(\sigma,\tau), \sigma\tau(\mathfrak{a}'_1(\rho))\rangle_1$ (resp. $\langle \mathfrak{a}(\sigma), \sigma(\partial\mathfrak{a}'_1(\tau,\rho))\rangle_2$) using Definition 1.3.10. Therefore, for pairwise distinct $1, j, k$,

$$(\partial\mathfrak{a} \cup_1 \mathfrak{a})'(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0} \text{ or } \chi'(\rho) = 1, \\ s_1, & \text{if } \chi(\sigma) = \widehat{1},\ \sigma \cdot \chi(\tau) = \widehat{1},\ \chi'(\rho) = -1, \\ s_{1j}, & \text{if } \chi(\sigma) = \widehat{j},\ \sigma \cdot \chi(\tau) = \widehat{j},\ \chi'(\rho) = -1, \\ s_{j1}, & \text{if } {}^{(\chi(\sigma),\sigma\cdot\chi(\tau)) = (\widehat{1},\widehat{j}),\text{ or}}_{(\chi(\sigma),\sigma\cdot\chi(\tau)) = (\widehat{j},\widehat{1})},\ \chi'(\rho) = -1, \\ -1, & \text{if } (\chi(\sigma), \sigma\cdot\chi(\tau)) = (\widehat{k},\widehat{j}),\ \chi'(\rho) = -1, \end{cases} \tag{3.2.3}$$

and

$$(\mathfrak{a} \cup_2 \partial\mathfrak{a})'(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ s_1, & \text{if } \chi(\sigma) = \widehat{1}, \chi'(\tau) = \chi'(\rho) = -1, \\ s_{j1}, & \text{if } \chi(\sigma) = \widehat{j}, \chi'(\tau) = \chi'(\rho) = -1. \end{cases} \tag{3.2.4}$$

We want to find a 2-cochain ε such that $\partial\varepsilon = \eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}'$ which (as we will later see) will require us to express certain elements as norms. Since D_a is locally everywhere soluble, using the discussion in §3.1.1 we have a global solution $\mathfrak{q}_i = (\Gamma^*_{ij} : \Gamma^*_{ik} : 1)$ to $H_i(\Gamma_{ij} : \Gamma_{ik} : 1) = 0$ over $k(e_j, e_k)$, for $1 \le i \le 3$, where H_i are as in Equation (3.1.3) and we assume Γ^*_{ij} and Γ^*_{ik} to be conjugates over $k(e_i)$ if e_j and e_k are. We would like to express s_{ij} as norm from $k(\sqrt{\beta_1}, \sqrt{\beta_2})$ to an index 2 subfield of $k(\sqrt{\beta_1}, \sqrt{\beta_2})$. Therefore, we define the quantities

$$p_{jk} := \sqrt{\beta_j}\Gamma^*_{ij} + \sqrt{\beta_k}\Gamma^*_{ik}, \quad \text{and} \quad p_i := p_{ij}p_{ik}. \tag{3.2.5}$$

Remark 3.2.1. Let $\mathfrak{q}_i$ be as above, and $\sigma \in G_k$ be such that $\sigma(e_i) = e_k$, then we can assume that the solution of the conic $H_k = 0$ is $\mathfrak{q}_k := \sigma(\mathfrak{q}_i)$. Writing $\sigma \in G_{k(e_i)}$ as $\sigma_s\sigma_p$, where $\sigma_s \in G_{k(E[2])}$ is such that $\chi(\sigma) = \chi(\sigma_s)$, and $\chi(\sigma_p) = \widehat{0}$, we have

$$\sigma(p_{ij}) = \sigma_s(p_{\sigma\cdot i\sigma\cdot j}) \quad \text{and} \quad \sigma(p_i) = \sigma_s\left(\prod_{l\neq i} p_{\sigma\cdot i\sigma\cdot l}\right) = \sigma_s(p_{\sigma\cdot i}),$$

where for indices j, k, $\sigma \cdot j = k$ if $\sigma(e_j) = e_k$.

If x is an n-cochain that only depends on the value of χ and χ' on its arguments, then we will interchangeably use $x(\sigma_1, \ldots, \sigma_n)$ with $x(\chi(\sigma_1), \chi'(\sigma_1), \ldots, \chi(\sigma_n), \chi'(\sigma_n))$ and drop the dependence on $\chi(\sigma_i)$ or $\chi'(\sigma_i)$, if x is independent of $\chi(\sigma_i)$ or $\chi'(\sigma_i)$, respectively, for some i.

We now resume the computation of $\varepsilon \in \mathrm{C}^2(k)$ such that $\partial\varepsilon = \eta$. If $\varepsilon \in \mathrm{C}^2(k)$ is only dependent on $\chi(\tau)$, $\chi'(\tau)$ and $\chi'(\rho)$, then we use $\varepsilon(\tau,\rho)$ interchangeably with $\varepsilon(\chi(\tau), \chi'(\tau), \chi'(\rho))$. We have

$$(\partial\varepsilon)(\sigma,\tau,\rho) = \frac{\sigma(\varepsilon(\chi(\tau),\chi'(\tau),\chi'(\rho)))\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau\rho))}{\varepsilon(\chi(\sigma\tau),\chi'(\sigma\tau),\chi'(\rho))\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))},$$

is dependent on $\chi(\sigma), \chi(\tau), \chi'(\sigma), \chi'(\tau)$, $\chi'(\rho)$, and action of σ on the image of ε.

The following proposition gives one ε such that $\partial\varepsilon = \eta$.

Proposition 3.2.2. *Let $\varepsilon \in \mathrm{C}^2(k)$ be as follows:*

$$\varepsilon(\tau,\rho) = \begin{cases} 1, & \text{if } \substack{\chi(\tau)=\widehat{0},\ \chi'(\tau)\chi'(\rho)=-1 \\ \text{or } \chi(\tau)=\widehat{1},\ \chi'(\tau)\chi'(\rho)=1, \\ \text{or } \chi'(\rho)=1} \\ p_1, & \text{if } \quad \chi(\tau)=\widehat{1},\ \chi'(\tau)=1,\ \chi'(\rho)=-1, \\ 1/p_1, & \text{if } \chi(\tau)=\widehat{0},\ \chi'(\tau)=-1,\ \chi'(\rho)=-1, \\ p_{1j}, & \text{if } \quad \chi(\tau)=\widehat{j},\ \chi'(\tau)=1,\ \chi'(\rho)=-1, \\ 1/p_{1j}, & \text{if } \chi(\tau)=\widehat{k},\ \chi'(\tau)=-1,\ \chi'(\rho)=-1, \end{cases} \tag{3.2.6}$$

where p_{ij}, p_i are as defined in Equation (3.2.5) and $1, j, k$ are pairwise distinct, then $\partial\varepsilon = \eta$.

Proof. If $\chi'(\rho) = 1$, then

$$\partial\varepsilon(\sigma,\tau,\rho) = \frac{\sigma\varepsilon(\chi(\tau),\chi'(\tau),1)\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))}{\varepsilon(\chi(\sigma\tau),\chi'(\sigma\tau),1)\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))} = 1 = \eta(\sigma,\tau,\rho).$$

Therefore, we assume that $\chi'(\rho) = -1$ and observe that

$$p_1 = \frac{1}{\varepsilon(\widehat{0},-1,-1)} = \frac{\varepsilon(\chi(\tau),1,-1)}{\varepsilon(\chi(\tau),-1,-1)}, \tag{3.2.7}$$

for all values of $\chi(\tau)$. Using this for $\chi'(\rho) = -1$ and $\chi'(\sigma) = 1$ we have:

$$\partial\varepsilon\big|_{\chi'(\tau)=-1}(\sigma,\tau,\rho) = \frac{\sigma\varepsilon(\chi(\tau),-1,-1)\ \varepsilon(\chi(\sigma),1,1)}{\varepsilon(\chi(\sigma\tau),-1,-1)\ \varepsilon(\chi(\sigma),1,-1)} = (\partial\mathfrak{a} \cup_1 \mathfrak{a}')(\sigma,\tau,\rho)\Gamma(\sigma),$$

where

$$\Gamma(\sigma) \coloneqq \frac{p_1}{\sigma(p_1)\ \varepsilon(\chi(\sigma),1,-1)^2}.$$

Remark 3.2.1 implies that $\sigma(p_1) = \sigma_s(p_1)$ and therefore, $\Gamma(\sigma)$ depends only on $\chi(\sigma)$. Therefore, it is enough to show that $\Gamma(\sigma) = 1/\mathfrak{a} \cup \partial\mathfrak{a}'(\chi(\sigma),-1,-1)$, for $\sigma \in G_{k(E[2])}$ (see Appendix (table 3.1) for explicit verification).

Now we show that $\partial\varepsilon\big|_{\chi'(\sigma)=1} = \partial\varepsilon\big|_{\chi'(\sigma)=-1}$. If $\chi'(\sigma) = -1$ and $\chi'(\tau) = 1$, then we have:

$$\begin{aligned} \partial\varepsilon(\sigma,\tau,\rho) = \frac{\sigma\varepsilon(\chi(\tau),1,-1)\ \varepsilon(\chi(\sigma),-1,-1)}{\varepsilon(\chi(\sigma\tau),-1,-1)\ \varepsilon(\chi(\sigma),-1,1)} &= \frac{\sigma\varepsilon(\chi(\tau),1,-1)\ \varepsilon(\chi(\sigma),1,-1)}{\varepsilon(\chi(\sigma\tau),1,-1)\ \varepsilon(\chi(\sigma),-1,1)} \\ &= \partial\varepsilon\big|_{\chi'(\sigma)=1,\chi'(\tau)=1}(\sigma,\tau,\rho). \end{aligned}$$

(using (3.2.7))

If $\chi'(\tau) = \chi'(\sigma) = -1$, then we have

$$\partial\varepsilon(\sigma,\tau,\rho) = \frac{\sigma\varepsilon(\chi(\tau),-1,-1)}{\varepsilon(\chi(\sigma\tau),1,-1)\ \varepsilon(\chi(\sigma),-1,-1)} = \frac{\sigma\varepsilon(\chi(\tau),-1,-1)}{\varepsilon(\chi(\sigma\tau),-1,-1)\ \varepsilon(\chi(\sigma),1,-1)}$$
$$= \partial\varepsilon\big|_{\chi'(\sigma)=1,\chi'(\tau)=-1}(\sigma,\tau,\rho). \quad \text{(using (3.2.7))}$$

What is left now to show is that if $\chi'(\sigma) = 1$, then

$$\partial\varepsilon\big|_{\chi'(\tau)=1}(\sigma,\tau,\rho) = \eta\big|_{\chi'(\tau)=1}(\sigma,\tau,\rho) = \partial\mathfrak{a}\cup\mathfrak{a}'(\chi(\sigma),\chi(\tau),-1). \tag{3.2.8}$$

We observe that

$$\sigma(\varepsilon(\chi(\tau),\chi'(\tau),\chi'(\rho))) = \sigma_s\varepsilon(\sigma\cdot\chi(\tau),\chi'(\tau),\chi'(\rho)), \tag{3.2.9}$$

Remark 3.2.1 implies (3.2.9) as the values of ε are multiplicative combinations of p_{1j} and $\sigma(p_{1j}) = \sigma_s(p_{1\sigma\cdot j})$. This implies (assuming $\chi'(\sigma) = 1$):

$$\partial\varepsilon(\sigma,\tau,\rho)\big|_{\chi'(\tau)=1,\chi'(\rho)=-1} = \frac{\sigma\varepsilon(\chi(\tau),1,-1)\varepsilon(\chi(\sigma),1,-1)}{\varepsilon(\chi(\sigma\tau),1,-1)}$$
$$= \frac{\sigma_s\varepsilon(\sigma\cdot\chi(\tau),1,-1)\varepsilon(\chi(\sigma),1,-1)}{\varepsilon(\chi(\sigma)\sigma\cdot\chi(\tau),1,-1)}.$$

Therefore, for $\sigma,\tau \in G_k$ such that $\chi(\sigma) = \widehat{i}$ and $\chi(\tau) = \sigma^{-1}\cdot\widehat{j}$, respectively, $\partial\varepsilon\big|_{\chi'(\tau)=1,\chi'(\rho)=-1}(\sigma,\tau,\rho)$ takes the same value, which is similar to $\partial\mathfrak{a}\cup\mathfrak{a}'$. Hence, it is enough to verify Equation (3.2.8) assuming $\sigma,\tau \in G_{k(E[2])}$ along with $\chi'(\sigma) = 1 = \chi'(\tau) = 1$ and $\chi'(\rho) = -1$ (see Appendix (table 3.2) for explicit verification). □

The next subsection is dedicated to the local part of the computation of the CTP using ε obtained from the global part.

3.2.2 Local computation

We recall the assumption that T_1 (therefore, β') is defined over k_v. Using the local triviality of α, for each place v of k there exists a $P_v := (x_v, y_v) \in E(\overline{k_v})$ such that $\partial P_v(\sigma) = (\sigma-1)P_v = \alpha_v(\sigma)$. This implies that for $\sigma \in G_{k_v}$, $\sigma(P_v) = P_v$, if $\chi(\sigma) = \widehat{0}$, and $\sigma(P_v) = P_v + T_i$, if $\chi(\sigma) = \widehat{i}$. Hence, P_v is defined over a subfield of $k_v(\sqrt{\beta_1},\sqrt{\beta_2})$. If $P_v \in E[2]$, then $2P_v = O$, $\beta_v \in (L\otimes k_v)^\times$ is a square and $\mathfrak{a}_v$ is trivial, and therefore P_v can be chosen to be $O \in E$. In this case, choosing the lift $\mathfrak{b}_v$ of $P_v = O$ as $0 \in \mathrm{Div}^0(E_{\overline{k}})$ we obtain $\gamma_v = -\varepsilon_v$. Hence, in what follows we assume $P_v \notin E[2]$. Lifting P_v to a degree zero divisor $\mathfrak{b}_v = (P_v) - (T_0)$, we have

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi(\sigma) = \widehat{0} \\ (T_i) - (P_v+T_i) + (P_v) - (T_0) = \mathrm{div}\left(\frac{y - \frac{y_v(x-e_i)}{x_v-e_i}}{x-x(P_v+T_i)}\right), & \text{if } \chi(\sigma) = \widehat{i}. \end{cases} \tag{3.2.10}$$

For $1 \leq i \leq 3$, let $x_{v,i}$, $\theta_{v,i}$ and $\omega_{v,i}$ denote the quantities $x_v - e_i$, $\frac{y_v}{x_v - e_i}$ and $-\theta_{v,i}/p_{jk}$, respectively. This gives:

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v(\tau, \rho) = \begin{cases} 1, & \text{if } \chi(\tau)=\widehat{0} \text{ or } \chi'(\rho)=1, \\ z_{v,11}, & \text{if } \chi(\tau)=\widehat{1},\ \chi'(\rho)=-1, \\ z_{v,1j}, & \text{if } \chi(\tau)=\widehat{j},\ \chi'(\rho)=-1, \end{cases} \tag{3.2.11}$$

where using equations (3.1.6) and (3.1.8) we have

$$z_{v,11} = \left(\frac{\left(y - \frac{y_v(x-e_1)}{x_v - e_1}\right)\left(-\frac{y}{x-e_1}\right)}{(x - x(P_v + T_1))} \right)(T_1) \times \left(\frac{(x - x(P_v + T_1))}{\left(y - \frac{y_v(x-e_1)}{x_v-e_1}\right)(x/y)} \right)(T_0) = x_{v,1}$$

and

$$z_{v,1j} = \left(\frac{\left(y - \frac{y_v(x-e_j)}{x_v - e_j}\right)}{(x - x(P_v + T_j))} \right)(T_1) \times \left(\frac{(x - x(P_v + T_j))}{\left(y - \frac{y_v(x-e_j)}{x_v-e_j}\right)(x/y)} \right)(T_0) = -\theta_{v,k}$$

Further,

$$\mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v(\tau, \rho) = \begin{cases} 1, & \text{if } \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ x_{v,1}, & \text{if } \quad \chi'(\tau) = \chi'(\rho) = -1, \end{cases} \tag{3.2.12}$$

and $\gamma_v \coloneqq (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup \mathfrak{a}'_v - \mathfrak{b}_v \cup \partial\mathfrak{a}'_v - \varepsilon_v$ is given by:

$$\gamma_v \coloneqq \begin{cases} 1, & \text{if } \begin{array}{r} \chi(\tau)=\widehat{0},\ \chi'(\tau)\chi'(\rho)=-1 \\ \text{or } \chi(\tau)=\widehat{1},\ \chi'(\tau)\chi'(\rho)=1, \\ \text{or } \chi'(\rho)=1 \end{array} \\ x_{v,1}/p_1, & \text{if } \quad \chi(\tau) = \widehat{1},\ \chi'(\tau) = 1,\ \chi'(\rho) = -1, \\ p_1/x_{v,1}, & \text{if } \chi(\tau) = \widehat{0},\ \chi'(\tau) = -1,\ \chi'(\rho) = -1, \\ \omega_{v,k}, & \text{if } \quad \chi(\tau) = \widehat{j},\ \chi'(\tau) = 1,\ \chi'(\rho) = -1, \\ 1/\omega_{v,k}, & \text{if } \chi(\tau) = \widehat{k},\ \chi'(\tau) = -1,\ \chi'(\rho) = -1, \end{cases} \tag{3.2.13}$$

where $j, k \neq 1$ are distinct.

We discuss some properties of $\omega_{v,i}$ in order to determine the class c_v in $\mathrm{Br}(k_v)$ represented by γ_v. Here we digress from the assumption that $e_1 \in k_v$. Note that $\omega_{v,i}$ can be defined independently of this assumption. For $\sigma \in G_{k_v}$, satisfying $\chi(\sigma) = \widehat{i}$ and $\sigma\big|_{k_v(\sqrt{\beta_i})} = \mathrm{id}$, and using Equation (3.1.6) we have

$$\sigma(\omega_{v,i}) = \sigma\left(\frac{-y_v}{x_{v,i}p_{jk}}\right) = \frac{y(P_v + T_i)}{p_{jk}(x(P_v + T_i) - e_i)} = \frac{-y_v}{x_{v,i}p_{jk}} = \omega_{v,i}.$$

$$(\sigma(p_{jk}) = -\sigma_s p_{\sigma\cdot j, \sigma\cdot k} = -p_{jk}.)$$

This implies that $\omega_{v,i} \in k_v(\sqrt{\beta_i})$. Further, if $\sigma \in G_{k_v}$, with $\chi(\sigma) = \widehat{j}$ and $\sigma\big|_{k_v(E[2])} = \mathrm{id}$ (i.e., $\sigma\big|_{k_v(\sqrt{\beta_i})}$ is the non-trivial element of $\mathrm{Gal}(k_v(\sqrt{\beta_i})/k_v(\beta_i))$), then using Equation (3.1.7)

$$\sigma(\omega_{v,i}) = \sigma\left(\frac{-y_v}{x_{v,i}p_{jk}}\right) = \frac{-y(P_v+T_j)}{\sigma(p_{jk})(x(P_v+T_j)-e_i)} = \frac{-x_{v,i}p_{jk}}{y_v} = \frac{1}{\omega_{v,i}}. \qquad (\sigma(p_{jk})p_{jk} = s_{kj})$$

Assuming β_i is not a square in $k_v(e_i)$, we have $\mathrm{Norm}_{k_v(\sqrt{\beta_i})/k_v(e_i)}(\omega_{v,i}) = 1$. Also, if $\sigma \in G_{k_v}$ is such that $\chi(\sigma) = \widehat{0}$ then we have: $\sigma(\omega_{v,i}) = \omega_{v,j}$ if $\sigma(e_i) = e_j$. Using Hilbert's Theorem 90, we have a $h_{v,i} \in k_v(E[2], \sqrt{\beta_i})$, such that $\omega_{v,i} = \overline{h_{v,i}}/h_{v,i}$, where $x \mapsto \overline{x}$, represents the non-trivial automorphism of $k_v(\sqrt{\beta_i})$ over $k_v(e_i)$. We choose $h_{v,i}$ to be $1 + \overline{\omega_{v,i}} \in k_v(\sqrt{\beta_i})$, and define:

$$\delta_{v,i} \coloneqq h_{v,i}\overline{h_{v,i}} = (2 + \overline{\omega_{v,i}} + \omega_{v,i}) \in k_v(e_i)^\times. \qquad (3.2.14)$$

In view of the above we have the following remark:

Remark 3.2.3. Let $\delta_{v,i} \in k_v(e_i)^\times$ be as above. Then $\sigma(\delta_{v,i}) = \delta_{v,j}$ if $\sigma(e_i) = e_j$ for $\sigma \in G_k$. Therefore, we get: $\prod_{i=1}^{3} \delta_{v,i} \in k_v^\times$ and $\delta'_{v,i} \coloneqq \delta_{v,j}\delta_{v,k} \in k_v(e_i)^\times$.

Returning to our discussion in the case when $e_1 \in k_v$, we have: $\delta'_{v,1} \in k_v^\times$. We shift γ_v by the coboundary $\partial\xi_v$ where:

$$\xi_v(\tau) = \begin{cases} 1, & \text{if} \quad \chi'(\tau) = 1, \\ h_{v,2}h_{v,3}, & \text{if } \chi'(\tau) = -1. \end{cases} \qquad (3.2.15)$$

If $\gamma'_v \coloneqq \gamma_v - \partial\xi_v$, then we have:

$$\gamma'_v(\tau,\rho) = \begin{cases} 1, & \text{if } \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ \frac{1}{\delta'_{v,1}} \in k_v^\times, & \text{if} \quad \chi'(\tau) = \chi'(\rho) = -1, \end{cases} \qquad (3.2.16)$$

and that γ'_v also represents the class $c_v \in \mathrm{Br}(k_v)$. The Proposition 1.3.40 implies that c_v is the class of the quaternion algebra $(\delta'_{v,1}, \beta')$ and therefore $(-1)^{2\mathrm{inv}_{k_v}(c_v)} = (\delta'_{v,1}, \beta')_{k_v}$.

We now express $\delta_{v,i}$ in terms of $x(Q_v)$, and $y(Q_v)$, where $Q_v \coloneqq 2P_v \in E(k_v)$.

$$\begin{aligned} x(Q_v) - e_i &= \left(\frac{3x_v^2 + c}{2y_v}\right)^2 - (x_v - e_j) - (x_v - e_k) \\ &= \frac{1}{4}\left(\sum_{i=1}^{3} \theta_{v,i}\right)^2 - \theta_{v,i}\theta_{v,k} - \theta_{v,i}\theta_{v,j} = \frac{1}{4}\left(\theta_{v,j} + \theta_{v,k} - \theta_{v,i}\right)^2. \end{aligned}$$

There exists $w_{v,i} \in k_v(e_i)^\times$, such that $(x(Q_v) - e_i) = \beta_i w_{v,i}^2$; hence, $\theta_{v,i} = w_{v,j}\sqrt{\beta_j} + w_{v,k}\sqrt{\beta_k}$ and

$$\omega_{v,i} = -\frac{\theta_{v,i}}{p_{jk}} = -\frac{w_{v,j}\sqrt{\beta_j} + w_{v,k}\sqrt{\beta_k}}{\Gamma_j^*\sqrt{\beta_j} + \Gamma_k^*\sqrt{\beta_k}}.$$

Here $w_{v,i}$ are chosen to be conjugates over k_v if e_i are. Therefore,

$$\delta_{v,i} = 2\left(1 - \frac{\beta_j w_{v,j}\Gamma_j^* - \beta_k w_{v,k}\Gamma_k^*}{\beta_j(\Gamma_j^*)^2 - \beta_k(\Gamma_k^*)^2}\right) = 2\left(1 + \frac{\beta_k w_{v,k}\Gamma_k^* - \beta_j w_{v,j}\Gamma_j^*}{s_{kj}}\right). \tag{3.2.17}$$

A value of $\langle a, a'\rangle_{\mathrm{CT}}$ (depending on the choices made above) is then given by the following theorem.

Theorem 3.2.4. *In view of the above discussion and the choice of the point P_v made above, one of the values of CTP on $(a, a') \in \mathrm{S}^2(E) \times \mathrm{H}^1(G_k, \langle T_1\rangle)$ is equal to:*

$$\langle a, a'\rangle_{\mathrm{CT}} = \prod_v (\delta'_{v,1}, \beta')_{k_v}.$$

3.3 Computing the CTP on $\mathrm{S}^{(2)}(E/k) \times \mathrm{S}^{(2)}(E/k)$

Our main aim in this section is to prove the sufficiency of the computation done in the previous section.

3.3.1 Corestriction method

Let $a' \in \mathrm{S}^{(2)}(E/k)$ be represented by the 1-cocycle α' which corresponds to the triple $(\beta'_1, \beta'_2, \beta'_3)$ as in section 3.1, and we drop the subscript in $\chi_{\alpha'}$ and call it χ'. Note that this χ' is not the same as the one in the previous section. We choose a lift of α' to $\mathrm{C}^1(G_k, \mathrm{Div}^0(E_{\overline{k}}))$ as:

$$\mathfrak{a}'(\sigma) = \begin{cases} 0, & \text{if } \chi'(\sigma) = \widehat{0}, \\ (T_j) + (T_k) - 2(T_0), & \text{if } \chi'(\sigma) = \widehat{i}. \end{cases}$$

The following lemma implies that $\mathfrak{a}'$ can be written as a sum of corestrictions of certain cochains.

Lemma 3.3.1. *Let $\mathfrak{a}'$ be as above, and let $\Delta_1, \ldots, \Delta_n$ be different orbits of Δ with representatives $T_1, \ldots, T_n$ for $n \leq 3$. Then*

$$\mathfrak{a}' = \sum_{i=1}^{n} \mathrm{cor}(\mathfrak{t}_i),$$

where each $\mathfrak{t}_i \in \mathrm{C}^1(G_{k(e_i)}, \mathrm{Div}^0(E_{\overline{k}}))$ *is given by:*

$$\mathfrak{t}_i(\sigma) := \begin{cases} 0, & \text{if} \quad \sigma(\sqrt{\beta_i'}) = \sqrt{\beta_i'}, \\ (T_i) - (T_0), & \text{if } \sigma(\sqrt{\beta_i'}) = -\sqrt{\beta_i'}, \end{cases}$$

and the corestriction of $\mathfrak{t}_i$ *is taken with respect to the groups* $G_{k(e_i)}$ *and* G_k.

Proof. Let $T_i = P_{i,1}, \dots P_{i,k_i}$ be the points in the orbit of T_i and let $\beta_i' = b_{i,1}, \dots, b_{i,k_i}$ be the G_k-conjugates of β_i' in $\{\beta_1', \beta_2', \beta_3'\}$. Let $\{\mathrm{id} = \tau_{i,1}, \tau_{i,2}, \dots, \tau_{i,k_i}\}$ be representatives of the right cosets of $G_{k(e_i)}$ with $\tau_{i,j}(P_{i,j}) = T_i$ for $1 \leq j \leq k_i$, and $\tau_{i,j} \cdot \left(\sum_{l=1}^{k_i} \sqrt{b_{i,l}}(P_{i,l}) \right) = \sum_{l=1}^{k_i} \sqrt{b_{i,l}}(P_{i,l})$. To see that such a choice of coset-representatives is possible we note that any $\sigma \in G_k$ such that $\sigma(P) = T_i$ for some $P \in \Delta_i$ has the form $\sigma_s \sigma_p$ (as in Remark 3.2.1), and so σ_p has the required property. Let c, r be the maps as in the definition of the corestriction map (Definition 1.3.8). Then $c(\tau_{i,j}\sigma) \in G_{k(e_i)}$, therefore, $r(\tau_{i,j}\sigma)^{-1}(\sqrt{\beta_i'}) = \sqrt{b_{i,\sigma^{-1}\cdot j}}$, where $(i, \sigma^{-1} \cdot j) = (i, l)$ if $\sigma^{-1}(P_{i,j}) = P_{i,l}$. By Definition 1.3.8 and the definition of $\mathfrak{t}_i$,

$$\begin{aligned} \sum_{i=1}^{n} \mathrm{cor}_{G_{k(e_i)}}^{G_k}(\mathfrak{t}_i)(\sigma) &= \sum_{i=1}^{n} \sum_{j=1}^{k_i} \tau_{i,j}^{-1} \mathfrak{t}_i(c(\tau_{i,j}\sigma)) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{k_i} g\left(\frac{\sigma(\sqrt{b_{i,\sigma^{-1}\cdot j}})}{\sqrt{b_{i,j}}} \right) ((P_{i,j}) - (T_0)), \end{aligned}$$

where $g : \mu_2 \to \mathbb{Z}$ is such that $g(1) = 0$ and $g(-1) = 1$. Now using the definition of χ' (Equation (3.1.2)) we have $\chi'(\sigma) = \sum_{i=1}^{n} \sum_{j=1}^{k_i} \chi'_{i,j}(\sigma)(P_{i,j})$, where $\chi'_{i,j}(\sigma) := \frac{\sigma(\sqrt{b_{i,\sigma^{-1}\cdot j}})}{\sqrt{b_{i,j}}}$ denotes the value of $\chi'(\sigma)$ at $P_{i,j}$. Therefore, $\sum_{i=1}^{n} \mathrm{cor}_{G_{k(e_i)}}^{G_k}(\mathfrak{t}_i) = \mathfrak{a}'$. □

We show that our choice of lift $\mathfrak{a}$ of α, and our choice of right-coset representatives as in the proof of the Lemma 3.3.1, satisfy Proposition 1.3.12.

Proposition 3.3.2. *Let* k *be a number field or its localization at a prime,* $\mathfrak{a}$ *be as before, choose the set of right-coset representatives* R *of* $G_k(e_1)$ *in* G_k *such that* $\chi(g) = \widehat{0}$, *for all* $g \in R$, *as in the Lemma 3.3.1. Then*

$$g^{-1}\partial(\mathfrak{a})(c(g\sigma), c(g\sigma)^{-1}c(g\sigma\tau)) = \partial\mathfrak{a}(\sigma, \tau),$$

and

$$g^{-1}\mathfrak{a}(c(g\sigma)) = \mathfrak{a}(\sigma),$$

for $g \in R$, *and* σ *and* τ *in* G_k.

Proof. Recall the definition of $r : G \to R$, and that $c : G \to H$ is given by $c(\sigma) = \sigma r(\sigma)^{-1}$. We first show the second equality in the above proposition. We have

$$\begin{aligned} g^{-1}\mathfrak{a}(c(g\sigma)) &= g^{-1}\mathfrak{a}(g\sigma r(g\sigma)^{-1}) = \mathfrak{a}(g^{-1} \cdot \chi(g\sigma r(g\sigma)^{-1})) \\ &= \mathfrak{a}(g^{-1} \cdot (\chi(g\sigma)(g\sigma) \cdot \chi(r(g\sigma)^{-1})) = \mathfrak{a}(\chi(\sigma)) = \mathfrak{a}(\sigma). \end{aligned}$$

Now we prove for the part of the proposition involving $\partial\mathfrak{a}$. Let σ and τ be in G_k, and $g \in R$. Let $g' \coloneqq r(g\sigma)$. Then

$$\begin{aligned} g^{-1}\partial(\mathfrak{a})(c(g\sigma), c(g\sigma)^{-1}c(g\sigma\tau)) &= g^{-1}\left(\mathfrak{a}(c(g\sigma)) + c(g\sigma)\mathfrak{a}(c(g\sigma)^{-1}c(g\sigma\tau)) - \mathfrak{a}(c(g\sigma\tau))\right) \\ &= g^{-1}\left(g\mathfrak{a}(\sigma) - g\mathfrak{a}(\sigma\tau) + g\sigma g'^{-1}\mathfrak{a}(c(g'\tau))\right) \\ &= \mathfrak{a}(\sigma) + \sigma\mathfrak{a}(\tau) - \mathfrak{a}(\sigma\tau) = \partial(\mathfrak{a})(\sigma, \tau). \end{aligned}$$

□

Lemma 3.3.1 along with the Proposition 1.3.11 immediately gives us the following corollary.

Corollary 3.3.3. *Let $a, a' \in \mathrm{S}^{(2)}(E/k)$ and α, α', $\mathfrak{a}$ and $\mathfrak{a}'$ be as in the definition of CTP. Assume the notations of Lemma 3.3.1 and that $\mathfrak{a}'$ is chosen as in Lemma 3.3.1. Then $\eta \coloneqq \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' = \sum_{i=1}^{n} \mathrm{cor}^{G_k}_{G_{k(e_i)}} \eta_i$, where*

$$\eta_i \coloneqq \partial\mathrm{res}^{G_{k(e_i)}}_{G_k}(\mathfrak{a}) \cup_1 \mathfrak{t}_i - \mathrm{res}^{G_{k(e_i)}}_{G_k}(\mathfrak{a}) \cup_2 \partial\mathfrak{t}_i \in \mathrm{Z}^3(k(e_i)).$$

In particular, if $\varepsilon_i \in \mathrm{C}^2(k(e_i))$ are such that $\partial\varepsilon_i = \eta_i$, then $\varepsilon \in \mathrm{C}^2(k)$ such that $\partial\varepsilon = \eta$ can be chosen to be $\sum_{i=1}^{n} \mathrm{cor}^{G_k}_{G_{k(e_i)}}(\varepsilon_i)$.

Thus we reduce the case of computing the ε for $a, a' \in \mathrm{S}^{(2)}(E/k)$, to the case of computing ε_i which we have already done in Proposition 3.2.2 by setting k as $k(e_i)$ and T_1 as T_i.

Considering the local part of the computation we have: $\gamma_v = \sum_{i=1}^{n} \gamma'_{i,v}$ where

$$\gamma'_{i,v} \coloneqq (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \left(\mathrm{cor}^{G_k}_{G_{k(e_i)}}(\mathfrak{t}_i)\right)_v - \mathfrak{b}_v \cup_2 \partial\left(\mathrm{cor}^{G_k}_{G_{k(e_i)}}(\mathfrak{t}_i)\right)_v - \left(\mathrm{cor}^{G_k}_{G_{k(e_i)}}(\varepsilon_i)\right)_v.$$

By the double coset formula (Equation (1.3.5)),

$$\left(\mathrm{cor}^{G_k}_{G_{k(e_i)}}(\mathfrak{t}_i)\right)_v = \sum_{w|v} \mathrm{cor}^{G_{k_v}}_{G_{k(e_i)_w}} \mathfrak{t}_{i,w},$$

where $\mathfrak{t}_{i,w} \coloneqq \mathrm{res}^{G_{k(e_1)_w}}_{G_{k(e_{i,w})}}((g_{i,w})_*\mathfrak{t}_i) \in \mathrm{C}^1(G_{k(e_i)_w}, \langle(T_{i,w}) - (T_0)\rangle)$, $g_{i,w} \in G_k$ corresponds to the valuation w of $k(e_i)$ above v, and $e_{i,w}$, $T_{i,w}$ are $g_{i,w}$ conjugates of e_i, T_i, respectively. Concretely,

$$\mathfrak{t}_{i,w}(\sigma) \coloneqq \begin{cases} 0, & \text{if} \quad \sigma(\sqrt{\beta'_{i,w}}) = \sqrt{\beta'_{i,w}}, \\ (T_{i,w}) - (T_0), & \text{if } \sigma(\sqrt{\beta'_{i,w}}) = -\sqrt{\beta'_{i,w}}, \end{cases}$$

where $\beta'_{i,w} \coloneqq g_{i,w}(\beta'_i)$.

Similarly, applying the double coset formula for ε_i we get:

$$\left(\mathrm{cor}^{G_k}_{G_{k(e_i)}}\varepsilon_i\right)_v = \sum_{w|v} \mathrm{cor}^{G_{k_v}}_{G_{k(e_i)w}}\varepsilon_{i,w}.$$

One can choose $\mathfrak{b}_v$ such that $\sigma\mathfrak{b}_v = \mathfrak{b}_v$, for all $\sigma \in G_{k_v}$ such that $\chi(\sigma) = \widehat{0}$. Hence, $\gamma'_{i,v} = \sum_{w|v} \mathrm{cor}^{G_{k_v}}_{G_{k(e_i)w}}\gamma_{i,w}$, where

$$\gamma_{i,w} \coloneqq \left(\mathrm{res}^{G_{k(e_i)w}}_{G_k}(\mathfrak{a}) - \mathrm{res}^{G_{k(e_i)w}}_{G_{k_v}}(\partial\mathfrak{b}_v)\right) \cup_1 \mathfrak{t}_{i,w} - \mathrm{res}^{G_{k(e_i)w}}_{G_{k_v}}(\mathfrak{b}_v) \cup_2 \partial\mathfrak{t}_{i,w} - \varepsilon_{i,w}. \quad (3.3.1)$$

The following proposition shows that $\gamma_{i,w}$ is a 2-cocycle.

Proposition 3.3.4. $\gamma_{i,w} \in \mathrm{Z}^2(k(e_i)_w)$.

Proof. Using $\partial\varepsilon_i = \eta_i$ we have

$$\begin{aligned}
\partial\gamma_{i,w} &= \mathrm{res}^{G_{k(e_i)w}}_{G_k}\partial\mathfrak{a} \cup_1 \mathfrak{t}'_{i,w} - \mathrm{res}^{G_{k(e_i)w}}_{G_k}\mathfrak{a} \cup_2 \partial\mathfrak{t}'_{i,w} \\
&\quad - \mathrm{res}^{G_{k(e_i)w}}_{G_{k(g_w(e_i))}}(g_{i,w})_*\left(\partial\mathrm{res}^{G_{k(e_i)}}_{G_k}\mathfrak{a} \cup_1 \mathfrak{t}'_1 - \mathrm{res}^{G_{k(e_i)}}_{G_k}\mathfrak{a} \cup_2 \partial\mathfrak{t}'_i\right) \\
&= \mathrm{res}^{G_{k(e_i)w}}_{G_k}(\partial(\mathfrak{a} - (g_{i,w})_*\mathfrak{a})) \cup_1 \mathfrak{t}'_{1,w} - \mathrm{res}^{G_{k(e_1)w}}_{G_k}(\mathfrak{a} - (g_{i,w})_*\mathfrak{a}) \cup_2 \partial\mathfrak{t}'_{1,w}. \\
&\qquad\qquad ((g_{i,w})_* \text{ commutes with res, } \cup \text{ and } \partial)
\end{aligned}$$

So, if $(g_{i,w})_*(\mathfrak{a}) = \mathfrak{a}$, then $\partial\gamma_{i,w} = 0$. Note that $\mathfrak{a}(\tau)$ only depends on $\chi(\tau)$, therefore we can equivalently write $\mathfrak{a}(\chi(\tau))$ instead of $\mathfrak{a}(\tau)$. We have $\sigma\mathfrak{a}(\chi(\tau)) = \mathfrak{a}(\sigma \cdot \chi(\tau))$. To see this, recall the definition of $\chi(\tau)$; hence, if $\chi(\tau) = \widehat{j}$, then $\sigma\chi(\tau) = \widehat{\sigma \cdot j}$.

Now for $\sigma \in G_k$,

$$\begin{aligned}
((g_{i,w})_*(\mathfrak{a}))(\sigma) &= g_{i,w}\mathfrak{a}(g_{i,w}^{-1}\sigma g_{i,w}) && \text{(by definition)} \\
&= g_{i,w}\mathfrak{a}(\chi(g_{i,w}^{-1}\sigma g_{i,w})) = \mathfrak{a}(g_{i,w}\chi(g_{i,w}^{-1}\sigma g_{i,w})) \\
&= \mathfrak{a}(\chi(\sigma g_{i,w})\chi(g_{i,w})^{-1}) = \mathfrak{a}(\chi(\sigma)\sigma\chi(g_{i,w})\chi(g_{i,w})^{-1}) \\
&\qquad\qquad (\chi \text{ is a 1-cocycle})
\end{aligned}$$

Recall from the proof of Lemma 3.3.1 or from Remark 3.2.1 that $g_{i,w}$ can be chosen such that $\chi(g_{i,w}) = \widehat{0}$ via the decomposition $\sigma = \sigma_s\sigma_p$ for $\sigma \in G_k$. Making such a choice for $g_{i,w}$, we have

$$((g_{i,w})_*(\mathfrak{a}))(\sigma) = \mathfrak{a}(\chi(\sigma)\sigma\chi(g_{i,w})\chi(g_{i,w})^{-1}) = \mathfrak{a}(\chi(\sigma)) = \mathfrak{a}(\sigma). \qquad \square$$

The above proposition together with part 4 of Proposition 1.3.37 implies that

$$\mathrm{inv}_{k_v}([\gamma_v]) = \sum_{i=1}^{n} \mathrm{inv}_{k_v}([\gamma'_{i,v}]) = \sum_{i=1}^{n}\sum_{w|v} \mathrm{inv}_{k_v(e_{i,w})}([\gamma_{i,w}]),$$

where $[z]$ represents the cohomology class of the cocycle z, i.e., the contribution from a place v of k in the CTP is the sum of contributions from G_{k_v}–orbits of Δ. If for a place v of k, and $m \leq 3$, $\Delta_1, \ldots, \Delta_m$ are the G_{k_v}–orbits of Δ with Δ_i represented by T_i, then from the above computation and §3.2.2 we get $\delta'_{i,v} \in k_v(e_i)^\times$ such that the local contribution at v in the CTP is $\prod_{i=1}^{m}(\delta'_{i,v}, \beta'_i)_{k_v(e_i)}$. Therefore, we have the following theorem.

Theorem 3.3.5. *We have*

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \prod_i (\delta'_{i,v}, \beta'_i)_{k_v(e_i)},$$

where i runs through the G_{k_v}–orbits of Δ.

The following corollary says that we only need to consider contribution to the CTP from finitely many places.

Corollary 3.3.6. *Let $S_{a,a'}$ be the set of finite places v of k such that either of α_v, α'_v (the localizations at v of cocycles representing a, a' (resp.)) do not factor through an unramified extension, together with the places such that ε takes at least one value with non-trivial valuation. Then*

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v \in S_{a,a'}} \prod_{i=1}^{m} (\delta'_{i,v}, \beta'_i)_{k_v(e_i)},$$

where i runs through G_{k_v}–orbits of Δ.

Proof. This is a special case of Lemma 4.3.19, where it is proven more generally. □

3.3.2 Exact formula for the CTP

In order to compute a exact formula for the CTP, we express the formula for the CTP obtained in Theorem 3.3.5 in terms of the Hilbert symbols $(\delta_{v,i}, \beta'_i)_{k_v(e_i)}$ instead of $\delta'_{v,i}$. Remark 3.2.3 implies that there is a $d_v := \prod_i \delta'_{v,i} \in k_v^\times$ such that $\prod_{i=1}^{3} d_v \delta_{v,i} \in (k_v^\times)^2$. Previously, we expressed the CTP in terms of the Hilbert symbols $(\delta'_{v,i}, \beta'_i)_{k_v(e_i)}$. Recall the definition of $\prod^\diamond$ from section 3.1. By Theorem 3.3.5, if c_v denotes the class of γ_v in $\mathrm{Br}(k_v)$, then

$$\begin{aligned}
(-1)^{2\mathrm{inv}_{k_v}(c_v)} &= \prod_i{}^{\diamond} (\delta'_{v,i}, \beta'_i)_{k_v(e_i)} = \prod_i{}^{\diamond} (d_v^2, \beta'_i)_{k_v(e_i)} (\delta'_{v,i}, \beta'_i)_{k_v(e_i)} \\
&= \prod_i{}^{\diamond} (d_v^2 \delta'_{v,i}, \beta'_i)_{k_v(e_i)} = \prod_i{}^{\diamond} (d_v \delta_{v,i}, \beta'_i)_{k_v(e_i)} \\
&= \prod_i{}^{\diamond} (d_v, \beta'_i)_{k_v(e_i)} \prod_i{}^{\diamond} (\delta_{v,i}, \beta'_i)_{k_v(e_i)}.
\end{aligned}$$

Here $\delta'_{v,i} \coloneqq \delta_{v,j}\delta_{v,k}$ is as in Remark 3.2.3. We now show that $\overset{\diamond}{\prod_i}(d_v, \beta'_i)_{k_v(e_i)} = 1$. Here we use the fact that if L is a finite extension of k_v and $z \in k_v^\times$, $z' \in L^\times$, then $(z, z')_L = (z, \mathrm{Norm}_{L/k_v}(z'))_{k_v}$. Using this we get:

$$\overset{\diamond}{\prod_i}(d_v, \beta'_i)_{k_v(e_i)} = \overset{\diamond}{\prod_i}(d_v, \mathrm{Norm}_{k_v(e_i)/k_v}(\beta_i)')_{k_v} = (d_v, \beta'_1\beta'_2\beta'_3)_{k_v} = 1.$$

Therefore,

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \overset{\diamond}{\prod_i}(\delta_{v,i}, \beta'_i)_{k(e_i)}. \tag{3.3.2}$$

One verifies that the above equation looks similar to the expression in Equation (3.1.4) for the Cassels' pairing. The following theorem shows that the pairing $\langle\cdot,\cdot\rangle_{\mathrm{Cas}}$ is the same as $\langle\cdot,\cdot\rangle_{\mathrm{CT}}$, using the expression for $\delta_{v,i}$ (Equation (3.2.17)).

Theorem 3.3.7. *For $a, a' \in \mathrm{Ш}^{(2)}(E/k)$, we have*

$$\langle a, a'\rangle_{\mathrm{Cas}} = \langle a, a'\rangle_{\mathrm{CT}}.$$

Proof. Recall $\mathfrak{q}_i \coloneqq (\Gamma^*_{ij} : \Gamma^*_{ik} : 1)$ is a global point on $H_i(\Gamma_j, \Gamma_k, T)$ (as in Equation (3.2.5)). Then

$$\begin{aligned}
L_i &\coloneqq \sum_{l=1}^{3} U_l \frac{\partial H_i}{\partial U_l}(\mathfrak{q}_i) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i) \\
&= \frac{\partial H_i}{\partial \Gamma_j}(\mathfrak{q}_i)\left(\sum_{l=1}^{3} U_l \frac{\partial \Gamma_j}{\partial U_l}(\mathfrak{q}_i)\right) + \frac{\partial H_i}{\partial \Gamma_k}(\mathfrak{q}_i)\left(\sum_{l=1}^{3} U_l \frac{\partial \Gamma_k}{\partial U_l}(\mathfrak{q}_i)\right) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i) \\
&\qquad\qquad ((\Gamma_1, \Gamma_2, \Gamma_3) \text{ is linear change of coordinates from } (U_1, U_2, U_3)) \\
&= \Gamma_j \frac{\partial H_i}{\partial \Gamma_j}(\mathfrak{q}_i) + \Gamma_k \frac{\partial H_i}{\partial \Gamma_k}(\mathfrak{q}_i) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i),
\end{aligned}$$

defines the tangent line at $\mathfrak{q}_i$. Let $\mathfrak{q}_v = (w_{v,1} : w_{v,2} : w_{v,3} : 1)$ be the point on D_a (in $(\Gamma_1 : \Gamma_2 : \Gamma_3 : T)$ coordinates) corresponding to Q_v (as in the previous section). Then

$$L_i(\mathfrak{q}_v) = 2 + 2\frac{(\beta_k\Gamma^*_k w_{v,k} - \beta_j\Gamma^*_j w_{v,j})}{s_{kj}}.$$

Using the expression for $\delta_{v,i}$ in Equation (3.2.17), and $p_{kj} = \sqrt{\beta_k}\Gamma^*_k + \sqrt{\beta_j}\Gamma^*_j$, we have $\delta_{v,i} = L_i(\mathfrak{q}_v)$, so the pairing $\langle\cdot,\cdot\rangle_{\mathrm{Cas}}$ defined in Equation (3.1.4) is the same as the Cassels-Tate pairing.

□

3.4 Appendix

Let σ, τ, $\rho \in G_k$ be such that $\chi'(\tau) = \chi'(\rho) = -1$, then we have:

$\chi(\sigma)$	$1/\Gamma(\sigma)$	$\mathfrak{a} \cup \partial\mathfrak{a}'(\sigma, -1, -1)$
$\widehat{0}$	$\frac{p_1(1)^2}{p_1} = 1$	1
$\widehat{1}$	$\frac{\sigma(p_1)p_1^2}{p_1} = s_1$	s_1
$\widehat{j}$	$\frac{\sigma(p_1)p_{1j}^2}{p_1} = s_{j1}$	s_{j1}

Table 3.1: $1/\Gamma(\sigma) = \mathfrak{a} \cup \partial\mathfrak{a}'(\sigma, -1, -1)$.

Let σ, τ, $\rho \in G_k$ be such that $\chi'(\rho) = -1$, $\chi'(\tau) = 1$ and $\chi'(\sigma) = 1$. If $\chi(\sigma) = \widehat{0}$, then

$$\partial\varepsilon(\sigma, \tau, \rho) = \frac{\sigma_s\varepsilon(\sigma \cdot \chi(\tau), 1, -1)}{\varepsilon(\sigma \cdot \chi(\tau), 1, -1)} = 1 = \partial\mathfrak{a} \cup \mathfrak{a}'(\sigma, \tau),$$

and if $\chi(\tau) = \widehat{0}$, then

$$\partial\varepsilon(\sigma, \tau, \rho) = \frac{\varepsilon(\chi(\sigma), 1, -1)}{\varepsilon(\chi(\sigma), 1, -1)} = 1 = \partial\mathfrak{a} \cup \mathfrak{a}'(\sigma, \tau).$$

The following table symbolically verifies all the other possible cases:

$\chi(\sigma)$	$\sigma \cdot \chi(\tau)$	$\partial\varepsilon(\chi(\sigma), \sigma \cdot \chi(\tau), -1)\big\vert_{\chi_1'(\sigma)=\chi_1'(\tau)=1}$
$\widehat{1}$	$\widehat{1}$	$\sigma_s(p_1)p_1 = s_1$
$\widehat{j}$	$\widehat{j}$	$\sigma_s(p_{1j})p_{1j} = s_{1j}$
$\widehat{j}$	$\widehat{k}$	$\frac{\sigma_s(p_{1k})p_{1j}}{p_1} = -1$
$\widehat{1}$	$\widehat{k}$	$\frac{\sigma_s(p_{1k})p_1}{p_{1j}} = s_{k1}$
$\widehat{k}$	$\widehat{1}$	$\frac{\sigma_s(p_1)p_{1k}}{p_{1j}} = s_{k1}$

Table 3.2: $\partial\varepsilon\big\vert_{\chi'(\tau)=1,\chi'(\rho)=-1}(\sigma, \tau, \rho) = \partial\mathfrak{a} \cup \mathfrak{a}'(\sigma, \tau, \rho)$.

Chapter 4

The CTP for odd degree hyperelliptic Jacobians

In this chapter we discuss how to compute the CTP for the multiplication-by-2 isogeny on Jacobians of odd-degree hyperelliptic curves. Furthermore, we discuss a conditional algorithm to compute the pairing, taking motivation from the case of $\mathrm{S}^{(2)}(E/k)$ where E/k is an elliptic curve discussed in the previous chapter. We will see some empirical evidence that the condition on which our conditional algorithm depends seems to be very weak for genus 2 odd-degree hyperelliptic curves and seems to become stronger as the genus increases.

Let k be a number field, and let $C : y^2 = f(x)$ be an odd-degree hyperelliptic curve, with Jacobian variety denoted by $J \simeq \mathrm{Pic}^0(C)$. Let $\theta_1, \ldots, \theta_l \in \overline{k}$ be all the roots of the polynomial f. Without loss of generality one can assume that f is monic and $f(x) \in \mathcal{O}_k[x]$. Let $T_i := (\theta_i, 0)$ denote the Weierstrass points in $C(\overline{k})$, and let T_0 be the point at infinity. In what follows, we will denote $J(\overline{k})[2]$ by $J[2]$ in order to simplify the notation. Recall from §1.2.4 that one can embed $C \hookrightarrow J$ using the k-rational point T_0 via $P \mapsto [(P) - (T_0)]$.

In the next section we discuss one of the crucial steps used in the computation of the CTP for the case $\mathrm{S}^{(2)}(J/k)$ using the Albanese-Albanese definition. This is mainly an abstraction of arguments from Lemma 3.3.1 and §3.3.1.

Acknowledgements

I thank Michael Stoll, Timo Keller, Jiali Yan, Tom Fisher, Claus Fieker and Peter Schneider for various helpful discussions relevant to this chapter.

4.1 Corestriction method

Our aim in this section is to express the elements of $\mathrm{H}^1(G_k, J[2])$ as a sum of corestrictions of some special elements. Recall the definition of the G-module $\mathrm{Ind}_G^H(M)$

from Lemma 1.3.23 for an H-module M and $H \subset G$ of finite index. Let p be a prime such that $\mu_p \subset k^\times$, and $\Delta := \bigsqcup_{\text{orbits}} \Delta_i$ be a finite G_k-set where Δ_i are the G_k-orbits in Δ. Choose a representative P_i for each orbit Δ_i. Then $\mu_p^\Delta \simeq \bigoplus_{\text{orbits}} \mu_p^{\Delta_i}$ and

$$\mu_p^{\Delta_i} = \mathrm{Ind}_{G_k}^{G_{k(P_i)}}(\mu_p^{\{P_i\}}).$$

Let $\iota : \mu_p^{\{P_i\}} \to \mu_p^{\Delta_i}$ be the natural inclusion map of $G_{k(P_i)}$-modules. By Proposition 1.3.25 and Corollary 1.3.29,

$$\bigoplus_{\text{orbits}} \mathrm{H}^j(G_{k(P_i)}, \mu_p^{\{P_i\}}) \simeq \bigoplus_{\text{orbits}} \mathrm{H}^j(G_k, \mu_p^{\Delta_i}) \simeq \mathrm{H}^j(G_k, \mu_p^\Delta),$$

where the isomorphism on the left is given by $\mathrm{cor} \circ \iota_*$ in each component of the direct sum at the level of cohomology classes, and on the right is given by the sum map. In particular, we can choose the representative elements of $\mathrm{H}^1(G_k, \mu_p^\Delta)$ as elements in $\prod_{\text{orbits}} k(P_i)^\times / \left(k(P_i)^\times\right)^p$.

From this point onwards, we fix $\Delta := \{T_1, \ldots, T_l\}$, with orbits Δ_i represented by T_i. If A denotes the étale algebra associated to Δ, then $A = k[T]/\langle f(T)\rangle \simeq \bigoplus_{\text{orbits}} k(\theta_i)$. Therefore, by Proposition 1.5.2, an element $a \in \mathrm{H}^1(G_k, J[2])$ is represented by a tuple $(d_1, \ldots, d_l) \in \mathbb{G}_{\mathrm{m}}^l$, such that $d_i \in k(\theta_i)^\times$, $\prod_{i=1}^{l} d_i \in (k^\times)^2$, and if θ_i, θ_j are conjugates, then d_i, d_j are chosen to be conjugates as d_i is the value of an element of $A^\times$ considered as a polynomial at θ_i. In view of the above, we have the following proposition.

Proposition 4.1.1. *Identify μ_2 with $\mathbb{Z}/2\mathbb{Z}$. The map $w : J[2] \to \mu_2^\Delta$ given by $w(P) := e_2(P, \_) : \Delta \to \mu_2$, where e_2 is the Weil pairing on $J[2]$, is injective, and can be viewed as lift of elements of $J[2]$ to $\mathrm{Div}^0(C_{\overline{k}})$ by lifting $0, 1 \in \mathbb{Z}/2\mathbb{Z}$ as $0, 1 \in \mathbb{Z}$, respectively; i.e., the composition $J[2] \xrightarrow{w} \mu_2^\Delta \xrightarrow{\pi} J[2]$ is the identity, where $\pi : \mu_2^\Delta \to J[2]$ is the sum map. In other words, $\mu_2^\Delta \simeq J[2] \oplus \ker(\pi)$, and so, $\mathrm{H}^1(G_k, \mu_2^\Delta) \simeq \mathrm{H}^1(G_k, J[2]) \oplus \mathrm{H}^1(G_k, \ker(\pi))$, i.e., the induced morphisms on cohomology classes w_* and π_* are injective and surjective, respectively.*

Proof. The elements of Δ span $J[2]$ as a $\mathbb{Z}/2\mathbb{Z}$ module; i.e., $\pi : (\mathbb{Z}/2\mathbb{Z})^\Delta \to J[2]$ is surjective with kernel of order 2 generated by the constant $\mathbb{1}$ map ($P \mapsto 1 \in \mathbb{Z}/2\mathbb{Z}$ for all $P \in \Delta$). We have the exact sequence

$$0 \to \langle \mathbb{1} \rangle \to \mu_2^\Delta \xrightarrow{\pi} J[2] \to 0. \tag{4.1.1}$$

The non-degeneracy of the Weil pairing implies that w is an injection. We can extend w to $\bar{w} : \mu_2^\Delta \to \mu_2^\Delta$, via π. If $P := (P_1) + (P_2) + \ldots + (P_m) \in (\mathbb{Z}/2\mathbb{Z})^\Delta$, for $P_i \in \Delta$, then $e_2(P, T_n) = 1$ if m is odd and $T_n \in \{P_1, P_2, \ldots, P_m\}$ or m is even and $T_n \notin \{P_1, P_2, \ldots, P_m\}$, and $e_2(P, T_n) = -1$ otherwise. This is because $e_2(T_i, T_j) = 1$,

if $i = j$, and $e_2(T_i, T_j) = -1$ otherwise (Proposition 2.1.9). Further, $\ker(\bar{w}) = \langle \mathbb{1} \rangle$. Adding $\mathbb{1}$ to P, if necessary, we may as well assume that m is odd. Therefore,

$$\bar{w}(P) = \sum_{T_j \in \mathrm{Supp}(P)}^{l} 1(T_j) + \sum_{T_j \notin \mathrm{Supp}(P)} (-1)(T_j) = \sum_{T_j \notin \mathrm{Supp}(P)} (T_j) \in (\mu_2)^{\Delta}.$$

Therefore, $\pi(\bar{w}(P)) = \pi(P)$, so $\pi(w(\pi(P))) = \pi(P)$. □

We obtain a commutative diagram:

$$\begin{array}{ccccc}
\bigoplus\limits_{\text{orbits}} \mathrm{H}^1(G_{k(\theta_i)}, \mu_2^{\{T_i\}}) & \hookrightarrow & \bigoplus\limits_{\text{orbits}} \mathrm{H}^1(G_{k(\theta_i)}, \mu_2^{\Delta_i}) & \xrightarrow{\sum\limits_{\text{orbits}} \mathrm{cor}} & \mathrm{H}^1(G_k, \mu_2^{\Delta}) \\
\downarrow \pi_* & & \downarrow \pi_* & & \downarrow \pi_* \\
\bigoplus\limits_{\text{orbits}} \mathrm{H}^1(G_{k(\theta_i)}, \langle [(T_i) - (T_0)] \rangle) & \hookrightarrow & \bigoplus\limits_{\text{orbits}} \mathrm{H}^1(G_{k(\theta_i)}, J[2]) & \xrightarrow{\mathrm{cor}} & \mathrm{H}^1(G_k, J[2]),
\end{array} \tag{4.1.2}$$

where the left π_* map is induced by the isomorphism given by $(T_i) \mapsto [(T_i) - (T_0)]$. In view of the diagram above, we have the following corollary.

Corollary 4.1.2. *If $a \in \mathrm{H}^1(G_k, J[2])$, then there exist $\beta_i \in \mathrm{Z}^1(G_{k(\theta_i)}, \mu_2^{\{T_i\}})$, such that*

$$a = \left[\sum_{\text{orbits}} \mathrm{cor}(\pi_*(\beta_i)) \right].$$

Proof. We have $\pi_* \circ w_*$ is identity map on the cohomology classes and $\mathrm{H}^1(G_k, \mu_2^{\Delta_i}) \xrightarrow{\mathrm{sh}} \mathrm{H}^1(G_k, \mu_2^{\{T_i\}})$ is an isomorphism. □

Since the CTP only depends on the cohomology class, we will choose a 1-cocycle representing an element $a \in \mathrm{H}^1(G_k, J[2])$ as $\sum\limits_{\text{orbits}} \mathrm{cor} \circ \pi_*(\beta_i)$, where β_i are as in the above corollary. Moreover, if T_i and T_i' are G_k-conjugates, then $\mathrm{H}^1(G_{k(\theta_i)}, \mu_2^{\{T_i\}}) \simeq \mathrm{H}^1(G_k, \mu_2^{\Delta_i}) \simeq \mathrm{H}^1(G_{k(\theta_i')}, \mu_2^{\{T_i'\}})$ in the sense that the following diagram commutes:

$$\begin{array}{ccc}
\mathrm{H}^1(G_{k(\theta_i)}, \mu_2^{\{T_i\}}) & \xrightarrow{\mathrm{cor}} & \mathrm{H}^1(G_k, \mu_2^{\Delta_i}) \\
& \searrow^{\sigma_*} & \uparrow \mathrm{cor} \\
& & \mathrm{H}^1(G_{k(\theta_i')}, \mu_2^{\{T_i'\}})
\end{array}, \tag{4.1.3}$$

where $\sigma \in G_k$ is such that $\sigma(T_i) = T_i'$. Concretely, we have the following remark:

Remark 4.1.3. If $d_i \in k(\theta_i)^\times$ corresponds to a 1-cocycle z_i in $\mathrm{Z}^1(G_{k(\theta_i)}, \mu_2^{T_i})$, then $\sigma d_i \in k(\sigma\theta_i)^\times$ will correspond to the 1-cocycle $z_i' := \sigma_*(z_i)$. If we choose a lift $\mathfrak{z}_i \in \mathrm{C}^1(G_{K(\theta_i)}, \mathrm{Div}^0(C_{\overline{k}}))$ of z_i as follows:

$$\mathfrak{z}_i(\tau) := \begin{cases} 0, & \text{if} \quad \tau(\sqrt{d_i}) = \sqrt{d_i} \\ (T_i) - (T_0), & \text{if } \tau(\sqrt{d_i}) = -\sqrt{d_i}, \end{cases}$$

and similarly $\mathfrak{z}_i'$ for z_i', then $\sigma_*(\mathfrak{z}_i) = \mathfrak{z}_i'$ and $\mathrm{cor}((\sigma_i)_*\mathfrak{z}_i) = \mathrm{cor}(\mathfrak{z}_i)$. The proof of the last part is the same as the proof of Lemma 3.3.1.

4.2 Modified definition of the CTP for $\mathrm{S}^{(2)}(J/k)$

By Corollary 4.1.2, we can choose a lift $\mathfrak{a} \in \mathrm{C}^1(G_k, \mathrm{Div}^0(C_{\overline{k}}))$ of an element $\alpha \in \mathrm{Z}^2(G_k, J[2])$ as $\sum_{\text{orbits}} \mathrm{cor}(\mathfrak{t}_i)$, where $\mathfrak{t}_i$ is a 1-cochain corresponding to $d_i \in k(\theta_i)^\times$ given by $\mathfrak{t}_i(\sigma) = (T_i) - (T_0)$ if $\sigma(\sqrt{d_i}) = -\sqrt{d_i}$, and 0 otherwise.

We now split the CTP as sum of local invariants of certain explicit Brauer group elements over local orbits of Δ. This is done by mainly repeating the procedure in §3.3.1 from Corollary 3.3.3 till Proposition 3.3.1. We choose by Corollary 4.1.2 a lift $\mathfrak{a}' = \sum_{\text{orbits}} \mathrm{cor}(\mathfrak{t}_i')$ of a'. Then part 10 of Proposition 1.3.11 implies that the Corollary 3.3.3 from the elliptic curve case also holds here and we obtain, for each G_k-orbit Δ_i of Δ, ε_i, η_i in $\mathrm{C}^2(k(\theta_i))$ and $\mathrm{Z}^3(k(\theta_i))$, respectively, such that $\eta_i := \partial \mathrm{res}_{G_k}^{G_{k(\theta_i)}}(\mathfrak{a}) \cup_1 \mathfrak{t}_i' - \mathrm{res}_{G_k}^{G_{k(\theta_i)}}(\mathfrak{a}) \cup_2 \partial\mathfrak{t}_i'$ and $\partial\varepsilon_i = \eta_i$. Let v be a place of k, let w be a place of $k(\theta_i)$ above v, and let $g_{i,w} \in G_k$ be a double coset representative with respect to the subgroups $G_{k(\theta_i)}$ and G_{k_v} of G_k corresponding to w chosen similarly to §3.3.1. For each place w of $k(\theta_i)$ above a place v of k, we obtain the quantities $\gamma_{i,v}'$, $\gamma_{i,w}$ as before given by $\gamma_{i,v}' := \sum_{w|v} \mathrm{cor}_{G_{k(\theta_i)_w}}^{G_{k_v}} \gamma_{i,w}$, where

$$\gamma_{i,w} := \left(\mathrm{res}_{G_k}^{G_{k(\theta_i)w}}(\mathfrak{a}) - \mathrm{res}_{G_{k_v}}^{G_{k(\theta_i)w}}(\partial\mathfrak{b}_v)\right) \cup_1 \mathfrak{t}_{i,w}' - \mathrm{res}_{G_{k_v}}^{G_{k(\theta_i)w}}(\mathfrak{b}_v) \cup_2 \partial\mathfrak{t}_{i,w}' - \varepsilon_{i,w} \quad (4.2.1)$$

and $\varepsilon_{i,w}$ are restrictions of ε_i to a place $w|v$ of $k(\theta_i)$. Recall from the double coset formula that

$$\left(\mathrm{cor}_{G_{k(\theta_i)}}^{G_k} \varepsilon_i\right)_v = \sum_{w|v} \mathrm{cor}_{G_{k(\theta_i)_w}}^{G_{k_v}} \varepsilon_{i,w}.$$

Once again, the aim is to show that $\gamma_{i,w}$ is a 2-cocycle.

$$\begin{aligned} \partial\gamma_{i,w} &= \mathrm{res}_{G_k}^{G_{k(\theta_i)w}} \partial\mathfrak{a} \cup_1 \mathfrak{t}_{i,w}' - \mathrm{res}_{G_k}^{G_{k(\theta_i)w}} \mathfrak{a} \cup_2 \partial\mathfrak{t}_{i,w}' \\ &\quad - \mathrm{res}_{G_{k(g_w(\theta_i))}}^{G_{k(\theta_i)w}}(g_{i,w})_* \left(\partial \mathrm{res}_{G_k}^{G_{k(\theta_i)}} \partial\mathfrak{a} \cup_1 \mathfrak{t}_i' - \mathrm{res}_{G_k}^{G_{k(\theta_i)}} \mathfrak{a} \cup_2 \partial\mathfrak{t}_i'\right) \\ &= \mathrm{res}_{G_k}^{G_{k(\theta_i)w}} (\partial(\mathfrak{a} - (g_{i,w})_*\mathfrak{a})) \cup_1 \mathfrak{t}_{i,w}' - \mathrm{res}_{G_k}^{G_{k(\theta_i)w}} (\mathfrak{a} - (g_{i,w})_*\mathfrak{a}) \cup_2 \partial\mathfrak{t}_{i,w}'. \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ((g_{i,w})_* \text{ commutes with res, } \cup \text{ and } \partial) \end{aligned}$$

Recall the definition of $\cup_i$ induced by the pairings $\langle\cdot,\cdot\rangle_i$ from §2.4. We now show that for our specific choice of lift $\mathfrak{a}$ of α, the following equality holds

$$\mathfrak{a} = (g_{i,w})_*(\mathfrak{a}).$$

Recall that $\mathfrak{a} = \sum_{\text{orbits}} \mathrm{cor}(\mathfrak{t}_i)$. We have

$$(g_{i,w})_*(\mathfrak{a}) = \sum_{\text{orbits}} \mathrm{cor}^{G_k}_{G_{g_{i,w}k(\theta_j)}}((g_{i,w})_*(\mathfrak{t}_j)) = \sum_{\text{orbits}} \mathrm{cor}^{G_k}_{k(\theta_j)}(\mathfrak{t}_j) = \mathfrak{a}.$$

The last equality above uses Remark 4.1.3. With the above choice of $\mathfrak{a}$, $\gamma_{i,w} \in \mathrm{Z}^2(k(\theta_i)_w)$. Recall from part 2 of the proof of Proposition 2.4.2 that choosing another lift of $\mathfrak{a}$ will not change $\gamma_{i,v}$.

In view of the above, $\gamma_{i,w}$ denotes a class $c_{i,w} \in \mathrm{Br}(k(\theta_i)_w)$. Therefore, the class $c_{i,v}$ represented by $\gamma_{i,v}$ in $\mathrm{Br}(k_v)$ is

$$c_{i,v} = \sum_{w|v} \mathrm{cor}_w(c_{i,w}).$$

Proposition 1.3.37 implies that $\mathrm{inv}_v(c_{i,v}) = \sum_{w|v} \mathrm{inv}_{k(\theta_i)_w}(c_{i,w})$, and

$$\langle a, a'\rangle_{\mathrm{CT}} = \sum_v \sum_{\text{orbits}} \sum_{w|v} \mathrm{inv}_{k_v(\theta_i)_w}(c_{i,w}),$$

where the orbits on the right hand side are taken with respect to G_k. The two inner sums can be viewed as a single sum over the G_{k_v}-orbits of Δ. We summarize the above discussion in the following theorem.

Theorem 4.2.1. *If $a, a' \in \mathrm{S}^{(2)}(J)$, then*

$$\langle a, a'\rangle_{\mathrm{CT}} = \sum_v \sum_{\text{orbits}} \mathrm{inv}_{k_v(\theta_i)}(c_{i,v})$$

for $c_{i,v} \in \mathrm{H}^2(k_v(\theta_i))$ as above. The inner sum is taken over G_{k_v}-orbits of Δ.

The above theorem implies that one can perform the global computation restricting to the extension $k(\theta_i)$ corresponding to each G_k-orbit Δ_i of Δ, and then perform the local computation for each Δ_i restricting to the extensions corresponding to each G_{k_v}-orbit of Δ_i. One would expect this computation to be simpler because $\mathfrak{t}'_i$ has a simple form and its values are defined over the base field $k(\theta_i)$. Therefore, from now on we assume that $\theta_1 \in k$. In the following section we describe an algorithm to compute the CTP for $a \in \mathrm{S}^{(2)}(J)$ and $a'_1 \in \mathrm{H}^1(G_k, \langle[(T_1) - (T_0)]\rangle)$ in the sense of Remark 2.4.3.

4.3 The CTP on $\mathrm{S}^{(2)}(J/k) \times \mathrm{H}^1(G_k, \langle[(T_1) - (T_0)]\rangle)$

Assume $\theta_1 \in k$, and let $a \in \mathrm{S}^{(2)}(J)$ and $a_1' \in \mathrm{H}^1(G_k, \langle[(T_1) - (T_0)]\rangle)$. In this section we give an algorithm to compute the CTP in this situation. In view of §2.4 there are two computational bottlenecks in computing the CTP, namely:

1. *Global step:* Computing $\varepsilon \in \mathrm{C}^2(k)$ such that $\partial\varepsilon = \eta$.
2. *Local step:* Computing the local invariant map inv_v on the class c_v represented by γ_v.

Recall from §3.2.1 that ε was computed using solutions to quadratic forms arising in the description of the twisted curve. A description of the twist J_a of J corresponding to a tends to be very complex even for genus 2, and the complexity increases with the genus exponentially.

One of the possible advantages of using the Albanese-Albanese definition of the CTP is to be able to avoid explicit equations representing the twist J_a completely. One can solve the local step generically using [Fie09], [Pre13]. In §4.3.3 we explicitly determine the value of the invariant map in terms of Hilbert symbols without using the above generic algorithms. The hurdle in the global step is to compute a splitting field for the cohomological class of η, and then to compute the corresponding ε. For obvious reasons, we would like the splitting field to be of as small degree as possible. In the following section we explicitly solve for ε in the case of odd-degree hyperelliptic curves by showing that $[\eta]$ splits in the field of definition of η, where η is obtained using some specific choices for lifts $\mathfrak{a}$ and $\mathfrak{a}'$ of α and α', respectively.

4.3.1 Global computation

Since α is a 1-cocycle that takes values in $J[2]$, α always factors through a finite extension. Therefore, one can choose a lift $\mathfrak{a}$ of α such that $\mathfrak{a}$ also factors through a finite extension. Let $\mathfrak{a}$ be such a lift of α factoring through a finite extension K/k. Assume $\mathfrak{a}_1'$ to be as follows:

$$\mathfrak{a}_1'(\sigma) = \begin{cases} 0, & \text{if} \quad \chi_1'(\sigma) = 1, \\ (T_1) - (T_0), & \text{if } \chi_1'(\sigma) = -1, \end{cases}$$

where $\chi_1'(\sigma) := \sigma(\sqrt{d'})/\sqrt{d'}$ for some $d' \in k^\times$, and let $K' = k(\sqrt{d'})$. Here we have fixed a square root $\sqrt{d'}$ of d'. We have $\partial\mathfrak{a}_1'(\sigma, \tau) = 0$, if $\chi_1'(\sigma) = 1$ or $\chi_1'(\tau) = 1$. Let $F := KK'$ and let $\chi(\sigma)$ denote the restriction $\sigma\big|_K$ of $\sigma \in G_k$.

Remark 4.3.1. For $\sigma, \tau, \rho \in G_k$, $(\partial\mathfrak{a} \cup_1 \mathfrak{a}_1')(\sigma, \tau, \rho) = \langle \partial\mathfrak{a}(\sigma, \tau), \sigma\tau\mathfrak{a}'(\rho)\rangle_1$, and $(\mathfrak{a} \cup_2 \partial\mathfrak{a}')(\sigma, \tau, \rho) = \langle \mathfrak{a}(\sigma), \sigma\partial\mathfrak{a}_1'(\tau, \rho)\rangle_2$, where $\langle\cdot,\cdot\rangle_1, \langle\cdot,\cdot\rangle_2$ are the bilinear pairings which induce the cup products. Note that $\eta_1 := \partial\mathfrak{a} \cup_1 \mathfrak{a}_1' - \mathfrak{a} \cup_2 \partial\mathfrak{a}_1'$ is independent of $\sigma\big|_{K'}$

as the values of $\mathfrak{a}'_1, \partial\mathfrak{a}'_1$ are defined over k. Therefore, $\eta_1(\sigma, \tau, \rho)$ depends only on $\chi(\sigma), \chi(\tau), \chi'_1(\tau)$, and $\chi'_1(\rho)$ (using $\mathrm{Gal}(F/k) \subset \mathrm{Gal}(K/k) \times \mathrm{Gal}(K'/k)$), and takes values in $K^\times$; hence, η_1 can be viewed as image of an element in $\mathrm{Z}^3(F/k)$ under the inflation map. Therefore, we will interchangeably use $\eta_1(\chi(\sigma), \chi(\tau), \chi'_1(\tau), \chi'_1(\rho))$ and $\eta_1(\sigma, \tau, \rho)$. If we choose α to be a normalized 1-cocycle, then we can assume that $\mathfrak{a}$ is also a normalized 1-cochain. Hence, $\partial\mathfrak{a}(\sigma, \tau) = 0$, if $\chi(\sigma)$ or $\chi(\tau)$ is the identity on K.

In what follows, the aim is to show that F is a splitting field for $[\eta_1]$ and find a 2-cochain ε_1 such that $\partial\varepsilon_1 = \eta_1$. In order to solve for ε_1, we will first extract two 2-cocycles E_1 and $E_{1,g}$ representing the trivial class in $\mathrm{Br}(K')$, where $\{\mathrm{id}, g\}$ is a set of right coset representatives of $G_{K'}$ in G_k. Then we use 1-cochains e_1 and $e_{1,g}$ satisfying $\partial e_1 = E_1$ and $\partial e_{1,g} = E_{1,g}$, respectively, to obtain a 3-cocycle η'_1 that is cohomologically equivalent to η_1 but has many nice properties. At last, we trivialize η'_1 using a variant of Hilbert's Theorem 90 (see Proposition 4.3.8).

Consider the following 2-cochain

$$E_1(\sigma, \tau) := \eta_1\big|_{\sigma,\tau \in G_{K'}, \chi'_1(\rho) = -1} \in \mathrm{C}^2(K').$$

Note that E_1 is the inflation of an element in $\mathrm{C}^2(F/K')$. The following proposition shows that $E_1 \in \mathrm{Z}^2(K')$.

Proposition 4.3.2. *The 2-cochain E_1 is a 2-cocycle with values in $K^\times$.*

Proof. Since η_1 is a 3-cocycle

$$\frac{\sigma\eta_1(\tau, \rho, \theta)\eta_1(\sigma, \tau\rho, \theta)\eta_1(\sigma, \tau, \rho)}{\eta_1(\sigma\tau, \rho, \theta)\eta_1(\sigma, \tau, \rho\theta)} = 1. \tag{4.3.1}$$

Specializing to the case when $\chi'_1(\theta) = -1$, and $\sigma, \tau, \rho \in G_{K'}$, we have $\eta_1(\sigma, \tau, \rho) = 1$, and $\chi'_1(\rho\theta) = -1$. This gives

$$\frac{\sigma E_1(\tau, \rho)E_1(\sigma, \tau\rho)}{E_1(\sigma\tau, \rho)E_1(\sigma, \tau)} = 1,$$

and therefore, $E_1 \in \mathrm{Z}^2(K')$. □

The 2-cocycle E_1 is constructed from η_1, and if $\varepsilon'_1 \in \mathrm{C}^2(k)$ is such that $\eta_1 = \partial\varepsilon'_1$, then for $\sigma, \tau \in G_{K'}$ and ρ such that $\chi'_1(\rho) = -1$,

$$E_1(\sigma, \tau) = \frac{\sigma\varepsilon'_1(\tau, \rho)\varepsilon'_1(\sigma, \tau\rho)}{\varepsilon'_1(\sigma\tau, \rho)\varepsilon'_1(\sigma, \tau)}. \tag{4.3.2}$$

We now make the following assumption.

Assumption 4.3.3. *Assume that, in the second argument ρ, $\varepsilon_1'(\tau,\rho)$ only depends on the value of $\chi_1'(\rho)$ for a fixed τ, and $\varepsilon_1'(\tau,\rho)=1$, if $\chi_1'(\rho)=1$. It can be shown that this indeed is the case for odd-degree hyperelliptic curves. For details, see section 4.3.2 below.*

In view of the above assumption, E_1 is trivialized by the 1-cochain

$$e_1' := \varepsilon_1'\big|_{\tau\in G_{K'},\chi_1'(\rho)=-1}.$$

This is because, if $\sigma,\tau\in G_{K'}$ and $\chi_1'(\rho)=-1$, then $\chi_1'(\tau\rho)=-1$ and $\chi_1'(\tau)=1$, and using assumption 4.3.3, Equation (4.3.2) becomes

$$E_1(\sigma,\tau)=\frac{\sigma\varepsilon_1'(\tau,\rho)\varepsilon_1'(\sigma,\tau\rho)}{\varepsilon_1'(\sigma\tau,\rho)}=\frac{\sigma e_1'(\tau)e_1'(\sigma)}{e_1'(\sigma\tau)}=\partial e_1'(\sigma,\tau).$$

Hilbert's Theorem 90 implies the existence of the inflation-restriction exact sequence for Brauer groups. Hence, one can view E_1 as inflation of an element of $\mathrm{H}^2(F/K')$. Therefore, we have an $e_1\in \mathrm{C}^1(K')$ such that $\partial e_1=E_1$, and e_1 can be viewed as inflation of a 1-cochain in $\mathrm{C}^1(F/K')$. Note that e_1 only depends on $\sigma\big|_F$.

Let $\{\mathrm{id}\,,g\}$ be the right coset representatives of $G_{K'}$ in G_k. Denote by $\{\mathrm{id}\,,\bar{g}\}$ the right coset representatives of $\mathrm{Gal}(F/K')$ in $\mathrm{Gal}(F/k)$ corresponding to $\{\mathrm{id}\,,g\}$. For $\sigma\in G_{K'}$ define

$$f_{1,g}(\sigma) := \eta_1(\sigma,g,-1).$$

Then $f_{1,g}\in \mathrm{C}^1(K')$, and it can be viewed as inflation of an element in $\mathrm{C}^1(F/K')$. Define

$$E_{1,g}(\sigma,\tau) := \eta(\sigma,\tau g,-1)/\eta(\sigma,g,-1),$$

for $\sigma,\tau\in G_{K'}$. We show that $E_{1,g}$ is a 2-coboundary and therefore is a 2-cocycle.

Proposition 4.3.4. *Let ε_1' be as in assumption 4.3.3. Then*

$$e_{1,g}'(\tau) := \varepsilon_1'(\tau g,-1)/\varepsilon_1'(g,-1)$$

satisfies $\partial e_{1,g}'=E_{1,g}$.

Proof.

$$\begin{aligned}
\partial e_{1,g}'(\sigma,\tau) &= \frac{\sigma e_{1,g}'(\tau)e_{1,g}'(\sigma)}{e_{1,g}'(\sigma\tau)}\\
&= \frac{\sigma\varepsilon_1'(\tau g,-1)\varepsilon_1'(\sigma g,-1)\varepsilon_1'(g,-1)}{\sigma\varepsilon_1'(g,-1)\varepsilon_1'(g,-1)\varepsilon_1'(\sigma\tau g,-1)}\\
&= \frac{\sigma\varepsilon_1'(\tau g,-1)}{\varepsilon_1'(\sigma,-1)\varepsilon_1'(\sigma\tau g,-1)}\frac{\varepsilon_1'(\sigma g,-1)\varepsilon_1'(\sigma,-1)}{\sigma\varepsilon_1'(g,-1)}\\
&= \eta_1(\sigma,\tau g,-1)/\eta_1(\sigma,g,-1)=E_{1,g}(\sigma,\tau).
\end{aligned}$$

□

Once again (similar to E_1), one can view $E_{1,g}$ as inflation of an element of $\mathrm{Z}^2(F/K')$. We can choose $e_{1,g} \in \mathrm{C}^1(K')$ such that $\partial e_{1,g} = E_{1,g}$ to be inflation of an element in $\in \mathrm{C}^1(F/K')$. Hence, $e_{1,g}$ takes values in $F^\times$ (more precisely $K^\times$), and factors through $\mathrm{Gal}(F/K')$. Define $\phi_{1,g} \in \mathrm{C}^1(G_{K'})$ by

$$\phi_{1,g}(\sigma) := (f_{1,g} + e_{1,g} + e_1)(\sigma).$$

The following proposition shows that $\phi_{1,g}$ is a 1-cocycle.

Proposition 4.3.5. *The 1-cochain $\phi_{1,g}$ is a 1-cocycle, and factors through $\mathrm{Gal}(F/K')$, and has values in $F^\times$.*

Proof. Since $e_1, e_{1,g}$, $f_{1,g}$ are inflations of elements in $\mathrm{C}^1(F/K')$, so is $\phi_{1,g}$. Now using that η_1 is a 3-cocycle, for $\sigma, \tau \in G_{K'}$,

$$\begin{aligned} 1 = \partial\eta_1(\sigma,\tau,g,g) &= \frac{\sigma\eta_1(\tau,g,g)\eta_1(\sigma,\tau g,g)\eta_1(\sigma,\tau,g)}{\eta_1(\sigma\tau,g,g)\eta_1(\sigma,\tau,g^2)} \\ &= \frac{\sigma f_{1,g}(\tau) f_{1,g}(\sigma)}{f_{1,g}(\sigma\tau)} E_{1,g}(\sigma,\tau)E_1(\sigma,\tau) \qquad \text{(definition of } f_{1,g},\ E_{1,g}) \\ &= \partial(f_{1,g})(\sigma,\tau)\partial(e_{1,g})(\sigma,\tau)\partial(e_1)(\sigma,\tau) = \partial(\phi_{1,g})(\sigma,\tau). \end{aligned}$$

□

By Hilbert's Theorem 90, there is a $t_{1,g} \in F^\times$ such that $\partial t_{1,g} = \phi_{1,g}$. For $\sigma \in G_{K'}$ let $\sigma_g = g\sigma g^{-1} \in G_{K'}$. We have $g\sigma = \sigma_g g$.

Define a 2-cochain ε_1 as follows:

$$\varepsilon_1(\tau,\rho) := \begin{cases} 1, & \text{if} \quad \chi_1'(\rho) = 1, \\ e_1(\tau), & \text{if} \quad \chi_1'(\tau) = 1,\ \chi_1'(\rho) = -1, \\ t_{1,g}e_{1,g}(\tau'), & \text{if } \chi_1'(\tau) = -1,\ \chi_1'(\rho) = -1, \end{cases} \tag{4.3.3}$$

where τ' is such that $\tau = \tau' g$. Define $\eta_1' := \eta_1 - \partial\varepsilon_1$. Note that for fixed $\sigma, \tau \in G_k$, $\eta_1'(\sigma,\tau,\rho)$ depends only on $\chi_1'(\rho)$. In regards to η_1' we have the following proposition.

Proposition 4.3.6. $\eta_1'(\sigma,\tau,\rho) = 1$ *on* $G_{K'} \times G_k \times G_k \cup G_k \times G_k \times G_{K'}$.

Proof. If $\sigma, \tau \in G_k$ and $\chi_1'(\rho) = 1$, then

$$\partial\varepsilon_1(\sigma,\tau,\rho) = \frac{\sigma\varepsilon_1(\tau,1)\varepsilon_1(\sigma,\chi_1'(\tau))}{\varepsilon_1(\sigma\tau,1)\varepsilon_1(\sigma,\chi_1'(\tau))} = 1 = \eta_1(\sigma,\tau,\rho).$$

If $\sigma, \tau \in G_{K'}$ and $\chi_1'(\rho) = -1$, then

$$\partial\varepsilon_1(\sigma,\tau,\rho) = \frac{\sigma\varepsilon_1(\tau,-1)\varepsilon_1(\sigma,-1)}{\varepsilon_1(\sigma\tau,-1)\varepsilon_1(\sigma,1)} = \frac{\sigma e_1(\tau)e_1(\sigma)}{e_1(\sigma\tau)} = E_1(\sigma,\tau) = \eta_1(\sigma,\tau,-1).$$

If $\sigma, \tau \in G_{K'}$ and $\chi_1'(\rho) = -1$, then

$$\begin{aligned}\partial\varepsilon_1(\sigma, \tau g, \rho) &= \frac{\sigma\varepsilon_1(\tau g, -1)\varepsilon_1(\sigma, 1)}{\varepsilon_1(\sigma\tau g, -1)\varepsilon_1(\sigma, -1)} \\ &= \frac{\sigma t_{1,g}\sigma e_{1,g}(\tau)}{t_{1,g}e_{1,g}(\sigma\tau)e_1(\sigma)} = f_{1,g}(\sigma)e_{1,g}(\sigma)e_1(\sigma)\frac{\sigma e_{1,g}(\tau)}{e_{1,g}(\sigma\tau)e_1(\sigma)} \\ &= \eta_1(g, \sigma, -1)E_{1,g}(\sigma, \tau) = \eta_1(\sigma, g, -1)\frac{\eta_1(\sigma, \tau g, \rho)}{\eta_1(\sigma, g, -1)} \\ &= \eta_1(\sigma, \tau g, \rho).\end{aligned}$$

□

From now on, we assume $\sigma, \tau, \rho \in G_k$ satisfy $\sigma, \tau \in G_{K'}$ and $\chi_1'(\rho) = -1$. The following corollary is a consequence of the above proposition.

Corollary 4.3.7. *If $\sigma, \tau \in G_{K'}$ and $\rho \in G_k$ is such that $\chi_1'(\rho) = -1$, then*

$$\eta_1'(\sigma g, \tau, \rho) = \sigma\eta_1'(g, \tau, \rho) \quad \text{and} \quad \eta_1'(\sigma g, \tau g, \rho) = \sigma\eta_1'(g, \tau g, \rho).$$

Proof. Let σ, τ, ρ be as above. Using that η_1' is a 3-cocycle we have

$$\frac{\sigma\eta_1'(g, \tau, \rho)\eta_1'(\sigma, g\tau, \rho)\eta_1'(\sigma, g, \tau)}{\eta_1'(\sigma g, \tau, \rho)\eta_1'(\sigma, g, \tau\rho)} = 1,$$

$$\text{which by Proposition 4.3.6 gives} \quad \frac{\sigma\eta_1'(g, \tau, \rho)}{\eta_1'(\sigma g, \tau, \rho)} = 1.$$

Similarly,

$$\frac{\sigma\eta_1'(g, \tau g, \rho)\eta_1'(\sigma, g\tau g, \rho)\eta_1'(\sigma, g, \tau g)}{\eta_1'(\sigma g, \tau g, \rho)\eta_1'(\sigma, g, \tau g\rho)} = 1,$$

$$\text{which by Proposition 4.3.6 gives} \quad \frac{\sigma\eta_1'(g, \tau g, \rho)}{\eta_1'(\sigma g, \tau g, \rho)} = 1.$$

□

The above corollary implies that the values $\eta_1'(g, \tau, -1)$ and $\eta_1'(g, \tau g, -1)$ determine η_1' completely. Note that the above proof uses only that η_1' satisfies Proposition 4.3.6 and that it is a 3-cocycle. We will need the following variant of Hilbert's Theorem 90 in order to trivialize η_1'.

Proposition 4.3.8. *Recall that the set $\{\mathrm{id}, \bar{g}\}$ is the set of chosen right coset representatives of $\mathrm{Gal}(F/K')$ in $\mathrm{Gal}(F/k)$. If $x \in \mathrm{C}^1(F/k)$ is such that for $\sigma, \tau \in \mathrm{Gal}(F/K')$,*

1. $x(\sigma\tau) = \sigma_{\bar{g}}x(\tau)x(\sigma)$,

2. $x(\sigma\tau\bar{g})x(\sigma) = \sigma_{\bar{g}}x(\tau\bar{g})$,

3. $\bar{g}(x(\sigma))x(\bar{g}\sigma) = x(\bar{g})$,

4. $\bar{g}(x(\sigma\bar{g}))x(\bar{g})x(\bar{g}\sigma\bar{g}) = 1$,

then there is a $c \in F^\times$ *satisfying*

1. $x(\sigma) = \frac{c}{\sigma_{\bar{g}}(c)}$,

2. $x(\sigma\bar{g}) = \frac{\bar{g}\sigma(c)}{c}$.

Proof. Let $H := \mathrm{Gal}(F/K')$ and consider the endomorphism ϕ of F given by

$$\phi := \sum_{\tau\in H} x(\tau)\tau_{\bar{g}} + \sum_{\tau\in H} \frac{\tau_{\bar{g}}\bar{g}}{x(\tau\bar{g})}.$$

Since x takes values in $F^\times$, division by $x(\tau\bar{g})$ is justified in the above expression. By linear independence of automorphisms, there exists a $b \in F$ (one of the basis elements of F over K' could be chosen as b; see Remark 4.3.12), such that $\phi(b) \neq 0$. Therefore,

$$\begin{aligned}
\sigma_{\bar{g}}\phi(b) &= \sum_{\tau\in H} \sigma_{\bar{g}}x(\tau)\sigma_{\bar{g}}\tau_{\bar{g}}(b) + \sum_{\tau\in H} \frac{\sigma_{\bar{g}}\tau_{\bar{g}}\bar{g}(b)}{\sigma_{\bar{g}}x(\tau\bar{g})} && \text{(by properties 1 and 2 of } x\text{)} \\
&= \frac{1}{x(\sigma)} \left(\underbrace{\sum_{\tau\in H} x(\sigma\tau)(\sigma\tau)_{\bar{g}}(b) + \sum_{\tau\in H} \frac{(\sigma\tau)_{\bar{g}}\bar{g}(b)}{x(\sigma\tau\bar{g})}}_{\phi(b)} \right).
\end{aligned}$$

This gives $x(\sigma) = \frac{\phi(b)}{\sigma_{\bar{g}}(\phi(b))}$. Similarly,

$$\begin{aligned}
\bar{g}\phi(b) &= \sum_{\tau\in H} \bar{g}x(\tau)\bar{g}\tau_{\bar{g}}(b) + \sum_{\tau\in H} \frac{\bar{g}\tau_{\bar{g}}\bar{g}(b)}{\bar{g}x(\tau\bar{g})} && \text{(by properties 3 and 4 of } x\text{)} \\
&= x(\bar{g}) \left(\sum_{\tau\in H} \frac{\bar{g}\tau_{\bar{g}}(b)}{x(\bar{g}\tau)} + \sum_{\tau\in H} x(\bar{g}\tau\bar{g})\bar{g}\tau_{\bar{g}}\bar{g}(b) \right) \\
& && \text{(by } \bar{g}\tau_{\bar{g}}\bar{g} = (\tau_{\bar{g}}\bar{g}^2)_{\bar{g}} \text{ and } \bar{g}\tau_{\bar{g}} = (\tau_{\bar{g}})_{\bar{g}}\bar{g}\text{)} \\
&= x(\bar{g}) \left(\underbrace{\sum_{\tau\in H} \frac{(\tau_{\bar{g}})_{\bar{g}}\bar{g}(b)}{x(\tau_{\bar{g}}\bar{g})} + \sum_{\tau\in H} x(\tau_{\bar{g}}\bar{g}^2)(\tau_{\bar{g}}\bar{g}^2)_{\bar{g}}(b)}_{\phi(b)} \right).
\end{aligned}$$

This gives $x(\bar{g}) = \frac{\bar{g}\phi(b)}{\phi(b)}$. By property 4, for $\sigma \in G_{K'}$,

$$\bar{g}x(\sigma\bar{g}) = \frac{\phi(b)(\bar{g}\sigma\bar{g})_{\bar{g}}(\phi(b))}{\phi(b)\bar{g}\phi(b)} = \frac{\bar{g}\sigma_{\bar{g}}\bar{g}(\phi(b))}{\bar{g}\phi(b)} = \bar{g}\left(\frac{\sigma_{\bar{g}}\bar{g}(\phi(b))}{\phi(b)}\right).$$

This implies that $x(\sigma\bar{g}) = \bar{g}\sigma(\phi(b))/\phi(b)$. Now choose the c in the proposition to be $\phi(b)$. □

Define $f'_{1,g} \in \mathrm{C}^1(k)$ by

$$f'_{1,g}(\sigma) := \eta'_1(g, \sigma, -1).$$

First note that $f'_{1,g}$ can be viewed as inflation of an element in $\mathrm{C}^1(F/k)$. We have the following proposition regarding $f'_{1,g}$.

Proposition 4.3.9. *The 1-cochain $f'_{1,g}$ satisfies the hypothesis of Proposition 4.3.8.*

Proof. Assume that $\rho \in G_k$ is such that $\chi'_1(\rho) = -1$. If $\sigma, \tau \in G_{K'}$, then

$$\frac{g\eta'_1(\sigma,\tau,\rho)\eta'_1(g,\sigma\tau,\rho)\eta'_1(g,\sigma,\tau)}{\eta'_1(g\sigma,\tau,\rho)\eta'_1(g,\sigma,\tau\rho)} = 1, \text{ so } \frac{f'_{1,g}(\sigma\tau)}{\sigma_g f'_{1,g}(\tau) f'_{1,g}(\sigma)} = 1.$$

Similarly, the properties $\eta'_1(g,\sigma,\tau g) = \eta'_1(g,\sigma,\rho)$ and

$$\frac{g\eta'_1(\sigma,\tau g,\rho)\eta'_1(g,\sigma\tau g,\rho)\eta'_1(g,\sigma,\tau g)}{\eta'_1(g\sigma,\tau g,\rho)\eta'_1(g,\sigma,\tau g\rho)} = 1$$

give $\frac{f'_{1,g}(\sigma\tau g) f'_{1,g}(\sigma)}{\sigma_g f'_{1,g}(\tau g)} = 1$. Furthermore,

$$\frac{g\eta'_1(g,\tau g,\rho)\eta'_1(g,g\tau g,\rho)\eta'_1(g,g,\tau g)}{\eta'_1(g^2,\tau g,\rho)\eta'_1(g,g,\tau g\rho)} = 1, \text{ so } g f'_{1,g}(\tau g) f'_{1,g}(g) f'_{1,g}(g\tau g) = 1.$$

Similarly,

$$\frac{g\eta'_1(g,\tau,\rho)\eta'_1(g,g\tau,\rho)\eta'_1(g,g,\tau)}{\eta'_1(g^2,\tau g,\rho)\eta'_1(g,g,\tau\rho)} = 1, \text{ so } \frac{g f'_{1,g}(\tau) f'_{1,g}(g\tau)}{f'_{1,g}(g)} = 1.$$

□

The above computation implies that there exists a $c_{1,g} \in F^\times$ such that $f'_{1,g}(\sigma) = c_{1,g}/\sigma_g(c_{1,g})$ and $f'_{1,g}(\sigma g) = g\sigma(c_{1,g})/c_{1,g}$, for $\sigma \in G_{K'}$. Define

$$\varepsilon''_1(\tau,\rho) := \begin{cases} 1, & \text{if } \chi'_1(\tau) = 1 \text{ or } \chi'_1(\rho) = 1, \\ \tau'(c_{1,g}), & \text{if } \quad \chi'_1(\tau) = \chi'_1(\rho) = -1, \end{cases}$$

where $\tau' \in G_{K'}$ is such that $\tau = \tau' g$.

Proposition 4.3.10. *We have $\partial\varepsilon''_1 = \eta'_1$.*

Proof. One can check that η'_1 matches $\partial\varepsilon''_1$ on $G_{K'} \times G_{K'} \times G_k$ and $G_k \times G_k \times G_{K'}$. In what follows we assume $\rho \in G_k$ is such that $\chi'_1(\rho) = -1$. For $\sigma, \tau \in G_{K'}$ we have

$$\partial\varepsilon''_1(\sigma,\tau g,\rho) = \frac{\sigma\varepsilon''_1(\tau g,-1)\varepsilon''_1(\sigma,1)}{\varepsilon''_1(\sigma\tau g,-1)\varepsilon''_1(\sigma,-1)} = \frac{\sigma\tau(c_{1,g})}{\sigma\tau(c_{1,g})} = 1 = \eta'_1(\sigma,\tau g,\rho).$$

Similarly,

$$\begin{aligned}
\partial\varepsilon_1''(\sigma g, \tau, \rho) &= \sigma(\partial\varepsilon_1''(g, \tau, \rho)) \qquad (\because \partial\varepsilon_1'' \text{ is 3-cocycle satisfying Proposition 4.3.6}) \\
&= \sigma\left(\frac{g\varepsilon_1''(\tau, -1)\varepsilon_1''(g, -1)}{\varepsilon_1''(g\tau, -1)\varepsilon_1''(g, 1)}\right) = \sigma\left(\frac{c_{1,g}}{\tau_g(c_{1,g})}\right) = \sigma\left(f_{1,g}'(\tau)\right) \\
&= \sigma(\eta_1'(g, \tau, \rho)) = \eta_1'(\sigma g, \tau, \rho). \qquad \text{(definition of } c_{1,g})
\end{aligned}$$

Computing $\partial\varepsilon_1''(\sigma g, \tau g, \rho)$ we have

$$\begin{aligned}
\partial\varepsilon_1''(\sigma g, \tau g, \rho) &= \sigma(\partial\varepsilon_1''(g, \tau g, \rho)) \quad (\because \partial\varepsilon_1'' \text{ is 3-cocycle satisfying Proposition 4.3.6}) \\
&= \sigma\left(\frac{g\varepsilon_1''(\tau g, -1)\varepsilon_1''(g, 1)}{\varepsilon_1''(g\tau g, -1)\varepsilon_1''(g, -1)}\right) = \sigma\left(\frac{g\tau(c_{1,g})}{c_{1,g}}\right) = \sigma f_{1,g}'(\tau g) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(definition of } c_{1,g}) \\
&= \sigma(\eta_1'(g, \tau g, \rho)) = \eta_1'(\sigma g, \tau g, \rho).
\end{aligned}$$

□

As a consequence of the above, we get the following corollary.

Corollary 4.3.11. $\partial(\varepsilon_1 + \varepsilon_1'') = \eta_1$.

Therefore, computationally the global part boils down to trivializing E_1, $E_{1,g}$ and finding $t_{1,g}$, $c_{1,g}$. One can use following remark in order to find $t_{1,g}$, $c_{1,g}$:

Remark 4.3.12. Let L be a finite Galois extension of k, $\alpha \in \mathrm{C}^1(L/k)$, and $\{b_1, \ldots, b_n\}$ be a set of basis elements of L as a vector space over k. The map

$$T_\alpha := \sum_{g \in \mathrm{Gal}(L/k)} \alpha(g)g$$

is a k-linear map, and if for all i, $T_\alpha(b_i) = 0$, then $T_\alpha(\sum_{i=1}^{n} a_i b_i) = \sum_{i=1}^{n} a_i T_\alpha(b_i) = 0$. Hence, at least one of $\sum_{g \in \mathrm{Gal}(L/k)} \alpha(g)g(b_i) \neq 0$.

Finding e_1 such that $\partial e_1 = E_1$ and $e_{1,g}$ such that $\partial e_{1,g} = E_{1,g}$ are the bottleneck steps of this algorithm in terms of time complexity. There are algorithms which can be used for this purpose for example [Fie09] for local fields and [Pre13] in general, if an effective version of Hilbert's Theorem 90 exists.

4.3.2 Removing Assumption 4.3.3

We now will show that Assumption 4.3.3 is always satisfied for odd-degree hyperelliptic curves. We have the following commutative diagram of G_k-modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J[2] & \longrightarrow & J[4] & \xrightarrow{[2]} & J[2] & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J[2] & \longrightarrow & J & \xrightarrow{[2]} & J & \longrightarrow & 0.
\end{array} \tag{4.3.4}$$

Taking Galois cohomology we have

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \mathrm{H}^1(G_k, J[4]) & \xrightarrow{[2]_*} & \mathrm{H}^1(G_k, J[2]) & \xrightarrow{\delta} & \mathrm{H}^2(G_k, J[2]) & \longrightarrow \cdots \\
& \downarrow & & \downarrow & & \| & \\
\cdots \longrightarrow & \mathrm{H}^1(G_k, J) & \xrightarrow{[2]_*} & \mathrm{H}^1(G_k, J) & \xrightarrow{\delta} & \mathrm{H}^2(G_k, J[2]) & \longrightarrow \cdots \\
& \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{loc}^2(J[2])} & \\
\cdots \longrightarrow & \prod_v \mathrm{H}^1(G_{k_v}, J) & \xrightarrow{[2]_*} & \prod_v \mathrm{H}^1(G_{k_v}, J) & \xrightarrow{\delta} & \prod_v \mathrm{H}^2(G_{k_v}, J[2]) & \longrightarrow \cdots
\end{array} \tag{4.3.5}$$

If $Ш^2(J[2]) = 0$, then $\mathrm{loc}^2(J[2])$ is injective, and for an element $a \in \mathrm{S}^{(2)}(J/k)$ we have $\delta(a) = 0$. Hence, there is a $b \in \mathrm{H}^1(G_k, J[4])$ such that $[2]_*(b) = a$. In particular, using the construction of the map δ, given a 1-cocycle α representing a, one can choose a 1-cocycle $\beta \in \mathrm{Z}^1(G_k, J[4])$, such that $[2]_*\beta = \alpha$. The following proposition shows that $\mathrm{loc}^2(J[2])$ is injective. The case when all the 2-torsion points are defined over k is present in [Yan21b, Lemma 1.8.6].

Proposition 4.3.13. *Let C, J, f and Δ be as before. Then the map*

$$\mathrm{loc}^2(J[2]) : \mathrm{H}^2(G_k, J[2]) \to \prod_v \mathrm{H}^2(G_{k_v}, J[2]),$$

is injective.

Proof. By Proposition 4.1.1, $J[2] \oplus \mu_2 \simeq \mu_2^\Delta$ as G_k-modules, where Δ is the G_k-set of roots of f. Therefore, $Ш^2(J[2]) = 0 \iff Ш^2(\mu_2^\Delta) = 0$ ($\because Ш^2(\mu_2) = 0$). Note that $(\mu_2^\Delta)^\vee = (\mu_2^\vee)^\Delta \simeq \mu_2^\Delta$ as G_k modules. Finiteness of μ_2^Δ implies that $Ш^i(\mu_2^\Delta)$ is finite for all i. By Poitou-Tate duality (Theorem 1.3.43), there is a non-degenerate and perfect pairing

$$\mathrm{pt} : Ш^1(\mu_2^\Delta) \times Ш^2(\mu_2^\Delta) \to \mathbb{Q}/\mathbb{Z},$$

which implies that $Ш^1(\mu_2^\Delta) \simeq Ш^2(\mu_2^\Delta)'$. We have $Ш^1(\mu_2^\Delta) = 0 \iff Ш^2(\mu_2^\Delta)' = 0 \iff Ш^2(\mu_2^\Delta) = 0$. By [BPS16, Lemma 8.2], $Ш^1(\mu_2^\Delta) = 0$. Therefore, $\mathrm{loc}^2(J[2])$ is injective. □

One can also prove the above proposition using Proposition 1.3.25 and Corollary 1.3.29 and the Albert-Brauer-Hasse-Noether sequence, but the above proof is neat and possibly easy to generalize to other cases. The following corollary removes Assumption 4.3.3:

Corollary 4.3.14. *There exists an $\varepsilon_1' \in \mathrm{C}^2(k)$ such that $\partial\varepsilon_1' = \eta_1$ and such that for a fixed σ, $\varepsilon_1'(\sigma, \tau)$ depends only on $\chi_1'(\tau)$, and $\varepsilon_1'(\sigma, \tau) = 1$, if $\chi_1'(\tau) = 1$. Concretely, one such ε_1' is given by $\mathfrak{s} \cup 2\mathfrak{a}_1' + \mathfrak{f} \cup \mathfrak{a}_1'$, where $\mathfrak{s}, \mathfrak{f}$ are as in Proposition 2.5.1.*

Proof. By Proposition 4.3.13, one can choose the lift β of α to $\mathrm{C}^1(G_k, J[4])$ to be in $\mathrm{Z}^1(G_k, J[4])$. Hence, ε_w can be chosen to be the trivial 2-cochain (constant map to 1). By Proposition 2.5.1, $\varepsilon_1' = \mathfrak{s} \cup 2\mathfrak{a}_1' + \mathfrak{f} \cup \mathfrak{a}_1'$ which clearly satisfies $\varepsilon_1'(\sigma, \tau) = 1$, if $\chi_1'(\tau) = 1$, and for a fixed σ, $\varepsilon_1'(\sigma, \tau)$ only depends on $\chi_1'(\tau)$. □

4.3.3 Local computation

Let v be a place of k. Following the proof of Theorem 4.2.1, we can restrict the base field to the field over which one of the representative points of a local orbit of Δ is defined. Therefore, without loss of generality, we assume that $\theta_1 \in k_v$. Let w be the place of F above v under the fixed embedding $\overline{k} \hookrightarrow \overline{k_v}$. Let F_w be the completion of F with respect to w, and k_v, K_w and K_w' be the completions of the images of k, K, and K' inside F_w, respectively. Let $P_v \in J(\overline{k_v})$ and $\mathfrak{b}_v$ be as in the definition of the CTP. We want to find the class associated to $\gamma_{1,v}$ in $\mathrm{Br}(k_v)$.

$$\gamma_{1,v} := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup \mathfrak{a}_{1,v}' - \mathfrak{b}_v \cup \partial\mathfrak{a}_{1,v}' - \varepsilon_{1,v}.$$

In order to avoid dealing with the cases $K_w' \subset K_w$ and $K_w' \not\subset K_w$ separately, we abuse notation slightly and let $\chi(\sigma)$ denote the restriction of $\sigma \in G_{k_v}$ to F_w (instead of $\sigma\big|_{K_w}$) and $\chi_1'(\tau) := \tau\left(\sqrt{d_{1,w}'}\right)/\sqrt{d_{1,w}'}$, where $d_{1,w}'$ is the image of $\sqrt{d_1}'$ in K_w'.

Note that $\gamma_{1,v}$ takes values in $K_w^\times$ and factors through $\mathrm{Gal}(F_w/k_v)$. For a fixed $\sigma \in G_{k_v}$, $\gamma_{1,v}(\sigma, \tau)$ depends only on $\chi_1'(\tau)$; hence, we once again interchangeably use $\gamma_{1,v}(\chi(\sigma), \chi_1'(\tau))$ and $\gamma_{1,v}(\sigma, \tau)$. The following proposition implies that $\gamma_{1,v}$ encodes a 1-cocycle in $\mathrm{Z}^1(G_{K_w'}, \overline{k_v}^\times)$.

Proposition 4.3.15. *One can view $\gamma_{1,v}$ as image of an element of $\mathrm{Z}^2(F_w/k_v)$ under inflation. Define $\Gamma_{1,v}(h) := \gamma_{1,v}(h, -1)$, for $h \in G_{K_w'}$. $\Gamma_{1,v}$ defined above is a 1-cocycle in $\mathrm{Z}^1(K_w')$, and can be viewed as inflation of an element in $\mathrm{Z}^1(F_w/K_w')$.*

Proof. Since $\gamma_{1,v}$ is a 2-cocycle,

$$g_1\gamma_{1,v}(g_2, g_3)\gamma_{1,v}(g_1, g_2g_3) = \gamma_{1,v}(g_1g_2, g_3)\gamma_{1,v}(g_1, g_2).$$

Assuming that $g_1, g_2 \in G_{K_w'}$, and $g_3 \notin G_{K_w'}$, we have

$$g_1\gamma_{1,v}(\chi(g_2), -1)\gamma_{1,v}(\chi(g_1), -1) = \gamma_{1,v}(\chi(g_1g_2), -1), \text{ so } \partial\Gamma_{1,v}(\sigma, \tau) = 1.$$

□

Hilbert's Theorem 90 implies the existence of a $\omega_{1,v} \in L^\times$ such that $\Gamma_{1,v}(h) = h(\omega_{1,v})/\omega_{1,v}$. In fact, by Proposition 4.3.12, one can explicitly compute $\omega_{1,v}$, given $\gamma_{1,v}$. Choose representatives $\{\mathrm{id}, g\}$ of left cosets of $G_{K_w'}$ in G_{k_v}. For $h \in G_{K_w'}$ and $g' \notin G_{K_w'}$, the equation

$$g\gamma_{1,v}(h, g')\gamma_{1,v}(g, hg') = \gamma_{1,v}(gh, g')\gamma_{1,v}(g, h)$$

combined with $\chi'(h) = 1$ gives

$$\begin{aligned}\gamma_{1,v}(gh, -1) &= g\gamma_{1,v}(h, -1)\gamma_{1,v}(g, -1) \\ &= \frac{gh\omega_{1,v}}{g\omega_{1,v}}\gamma_{1,v}(g, -1). \end{aligned} \tag{4.3.6}$$

By Proposition 4.3.12, one can assume that the $\omega_{1,v}$, which trivializes $\Gamma_{1,v}$, is in $K_w \subseteq F_w$, because $\gamma_{1,v}$ (and therefore, $\Gamma_{1,v}$) takes values in $K_w^\times$. Therefore, the action of $G_{K'_w}$ on $\omega_{1,v}$ can be described in terms of $\sigma\big|_{K_w^\times}$ (this is true whether or not $K_w \cap K'_w = k_v$). Now consider the 1-cochain $\xi_{1,v} \in \mathrm{C}^1(G_{k_v}, F_w^\times)$ given by

$$\xi_{1,v}(\tau) := \begin{cases} 1, & \text{if} \quad \chi'_1(\tau) = 1, \\ \omega_{1,v}, & \text{if } \chi'_1(\tau) = -1. \end{cases}$$

We have

$$\partial\xi_{1,v}(\tau, \rho) := \begin{cases} 1, & \text{if} \qquad\qquad\quad \chi'_1(\rho) = 1, \\ \tau\omega_{1,v}/\omega_{1,v} = \Gamma_{1,v}(\tau), & \text{if} \quad \chi'_1(\tau) = 1, \ \chi'_1(\rho) = -1, \\ \tau\omega_{1,v} \cdot \omega_{1,v}, & \text{if } \chi'_1(\tau) = -1, \ \chi'_1(\rho) = -1. \end{cases}$$

Let $\gamma'_{1,v} := \gamma_{1,v} - \partial\xi_{1,v}$. Then for $\tau \in G_{K'_w}$, $\rho \in G_{k_v}$ we have $\gamma'_{1,v}(\tau, \rho) = 1$, and if $\tau \notin G_{K'_w}$, then $\tau = g\tau'$, for some $\tau' \in G_{K'_w}$. Using Equation (4.3.6)

$$\gamma'_{1,v}(\tau, \rho) = \frac{\gamma_{1,v}(g\tau', \rho)}{g\tau'(\omega_{1,v})\omega_{1,v}} = \frac{g\tau'\omega_{1,v}}{g\omega_{1,v}}\frac{\gamma_{1,v}(g, -1)}{g\tau'(\omega_{1,v})\omega_{1,v}} = \frac{\gamma_{1,v}(g, -1)}{g(\omega_{1,v})\omega_{1,v}}.$$

Note that $\gamma'_{1,v}(\tau, \rho)$ is independent of $\chi(\tau)$ and depends only on $\chi'_1(\tau)$ and $\chi'_1(\rho)$, and

$$\delta_{1,v} := \frac{\gamma_{1,v}(g, -1)}{g(\omega_{1,v})\omega_{1,v}} \tag{4.3.7}$$

depends only on the choice of coset representative g and $\omega_{1,v}$. Hence, by the condition that $\gamma'_{1,v}$ is a 2-cocycle we have $\delta_{1,v} \in k_v^\times$. To see this, let $g_1, g_2, g_3 \notin G_{K'_w}$. Then

$$g_1(\gamma'_{1,v}(g_2, g_3))\gamma'_{1,v}(g_1, g_2g_3) = \gamma'_{1,v}(g_1g_2, g_3)\gamma'_{1,v}(g_1, g_2), \text{ so } g_1\delta_{1,v} = \delta_{1,v}.$$

On the other hand, assuming $g_1 \in G_{K'_w}$ and $g_2, g_3 \notin G_{K'_w}$ gives

$$g_1(\gamma'_{1,v}(g_2, g_3))\gamma'_{1,v}(g_1, g_2g_3) = \gamma'_{1,v}(g_1g_2, g_3)\gamma'_{1,v}(g_1, g_2), \text{ so } g_1\delta_{1,v} = \delta_{1,v},$$

therefore, $\delta_{1,v} \in k_v^\times$. Now the class $c_{1,v}$ represented by $\gamma'_{1,v}$ (therefore, by $\gamma_{1,v}$) in $\mathrm{Br}(k_v)$ is the class of quaternion algebra $(\delta_{1,v}, d'_1)$. We have $(-1)^{2\mathrm{inv}_v(c_{1,v})} = (\delta_{1,v}, d'_1)_v$, where $(\cdot, \cdot)_v$ denotes the Hilbert symbol over k_v.

4.3.4 An explicit η_1

We assume $\theta_1 \in k$. We continue to use the notation from the previous section except for χ. We fix an order of the roots $\theta_1, \ldots, \theta_l$ of f, and correspondingly of $T_1, \ldots, T_l$ in Δ. A lot of this section is a natural generalization of the definitions made in §3.1 and §3.2.1.

If $a \in \mathrm{S}^{(2)}(J/k)$, then a maps to an element of $\mathrm{H}^1(G_k, \mu_2^\Delta)$ via w_* (defined in section 4.1). Therefore, we choose the cocycle α representing $w_*(a)$ as follows. Using the identification $\mathrm{H}^1(G_k, \mu_2^\Delta) \simeq A^\times/(A^\times)^2$, where recall that A is the étale algebra associated to the defining polynomial f, we choose a 1-cocycle $\chi_a \in \mathrm{Z}^1(G_k, \mu_2^\Delta)$, $\chi_a(\sigma) := \sigma(\sum_{i=1}^{l} \sqrt{d_i}(T_i))/(\sum_{i=1}^{l} \sqrt{d_i}(T_i))$ and $d_i \in k(\theta_i)^\times$ are as in Proposition 1.5.2 with the property that $\prod_{i=1}^{l} d_i \in (k^\times)^2$. Since $\pi_* \circ w_*$ is the identity morphism on cohomology classes, we will represent a by $\pi_*(\chi_a)$. As in §3.1, for each element m of μ_2^Δ, we associate an element in μ_2^l with ith entry being $m(T_i)$. Under this association, the values of χ_a will map to the l-tuples having exactly an odd number of 1's. Denote the tuple with 1 at $i_1, \ldots, i_t$ and -1 at other places by $\widehat{i_1, \ldots, i_t}$, and by $\widehat{0}$ the tuple with 1 everywhere. There is a natural action of G_k on these l-tuples, coming from the action on Δ. Under π the element of μ_2^Δ represented by $\widehat{i_1, \ldots, i_t}$ will map to $\sum_{n=1}^{t}[(T_{i_n}) - (T_0)]$. However, from the proof of Proposition 4.1.1, the element represented by $\widehat{i_1, \ldots, i_t}$ is in the image of the point $P \in J[2]$ represented by the divisor $\sum_{n \notin \{i_1, \ldots, i_t\}} ((T_{i_n}) - (T_0))$ which is the same as the point $\sum_{n=1}^{t}[(T_{i_n}) - (T_0)]$. Therefore, we can choose $\alpha \in \mathrm{Z}^1(G_k, J[2])$ representing a to be

$$\alpha(\sigma) = \sum_{n=1}^{t}[(T_{i_n}) - (T_0)], \qquad \text{if } \chi_a(\sigma) = \widehat{i_1, \ldots, i_t},$$

and the lift $\mathfrak{a}$ of α as

$$\mathfrak{a}(\sigma) = \sum_{n=1}^{t}((T_{i_n}) - (T_0)), \qquad \text{if } \chi_a(\sigma) = \widehat{i_1, \ldots, i_t} \neq \widehat{0}.$$

We define $\mathfrak{a}(\sigma) = 0$, for $\chi_a(\sigma) = \widehat{0}$. Recall the definition of $\mathfrak{a}_1'$ from §4.3.1. We note that $\mathfrak{a}$ factors through the field $K = k(\sqrt{d_1}, \ldots, \sqrt{d_l})$ with $\mathrm{Gal}(K/k) \subset C_2^{l-1} \rtimes S_{l-1}$, where S_{l-1} is the symmetric group acting on the set $\{T_2 \ldots T_l\}$, and C_2 is the cyclic group of order 2. Here for $1 \leq i \leq l-1$, the ith copy of C_2 acts by $\sqrt{d_{i+1}} \mapsto -\sqrt{d_{i+1}}$. Since we are going to compute symbolically, we assume that $\mathrm{Gal}(K/k) \simeq C_2^{l-1} \rtimes S_{l-1}$. If $\sigma \in \mathrm{Gal}(K/k)$, then $\sigma = \sigma_s\sigma_p$, where $\sigma_p \in S_{l-1}$ and $\sigma_s \in C_2^{l-1}$; hence, $\chi_a(\sigma_p) = \widehat{0}$. Since χ_a is a 1-cocycle, $\chi_a(\sigma_s) = \chi_a(\sigma)$. For simplicity of notation we set $\chi = \chi_a$. The subscripts s and p denote the sign part and the permutation part of an element

$\sigma \in \mathrm{Gal}(K/k)$ considered as an element in $C_2^{l-1} \rtimes S_{l-1}$. Recall the action of G_k on μ_2^l-tuples. For $\sigma, \tau \in \mathrm{Gal}(F/k)$, $\sigma \cdot \chi(\tau) = \sigma_p \cdot \chi(\tau)$, and $\sigma\mathfrak{a}(\tau) = \sigma_p\mathfrak{a}(\tau) = \mathfrak{a}(\sigma \cdot \chi(\tau)) = \mathfrak{a}(\sigma_p \cdot \chi(\tau))$. We have

$$\begin{aligned}\partial\mathfrak{a}(\sigma,\tau) &= \sigma\mathfrak{a}(\tau) + \mathfrak{a}(\sigma) - \mathfrak{a}(\sigma\tau)\\ &= \sigma\mathfrak{a}(\chi(\tau)) + \mathfrak{a}(\chi(\sigma)) - \mathfrak{a}(\chi(\sigma)\sigma_p \cdot \chi(\tau))\\ &= \mathfrak{a}(\sigma_p \cdot \chi(\tau)) + \mathfrak{a}(\chi(\sigma)) - \mathfrak{a}(\chi(\sigma)\sigma_p \cdot \chi(\tau)).\end{aligned}$$

Clearly $\partial\mathfrak{a}(\sigma,\tau)$ depends only on $\chi(\sigma)$ and $\sigma_p \cdot \chi(\tau)$. Let $\{\chi(\sigma)\}$ be the set associated to the tuple $\chi(\sigma)$ and with $\widehat{0}$ associate the set $\{1,\ldots,l\}$. Then $\{\chi(\sigma)\chi(\tau)\} = (\{\chi(\sigma)\} \cap \{\chi(\tau)\}) \cup (\{\chi(\sigma)\} \cup \{\chi(\tau)\})^c$, where $*^c$ is the complement of a subset $*$ of $\{1,\ldots,l\}$. Noting that $\mathfrak{a}(\chi(\sigma)) = \sum_{i\in\{\chi(\sigma)\}} ((T_i) - (T_0))$ when $\chi(\sigma) \neq \widehat{0}$, we treat the cases of $\chi(\sigma) = \widehat{0}$ or $\chi(\tau) = \widehat{0}$ or $\chi(\sigma) = \sigma_p \cdot \chi(\tau)$ separately. If $\chi(\sigma)$ or $\chi(\tau)$ is $\widehat{0}$, then $\partial\mathfrak{a}(\sigma,\tau) = 0$ and if $\chi(\sigma) = \sigma_p \cdot \chi(\tau)$, then $\partial\mathfrak{a}(\sigma,\tau) = \mathrm{div}(\prod_{i\in\{\chi(\sigma)\}} (x-\theta_i))$. In case $\chi(\sigma) \neq \sigma_p \cdot \chi(\tau)$ and $\chi(\sigma) \neq \widehat{0} \neq \sigma_p\chi(\tau)$,

$$\partial\mathfrak{a}(\chi(\sigma),\sigma_p\cdot\chi(\tau)) = \sum_{i=1}^{l}((T_i)-(T_0))-2\sum_{\substack{i\notin\{\chi(\sigma)\}\\ i\notin\{\sigma\cdot\chi(\tau)\}}}((T_i)-(T_0)) = \mathrm{div}\left(\frac{y}{\prod\limits_{\substack{i\notin\{\chi(\sigma)\}\\ i\notin\{\sigma\cdot\chi(\tau)\}}}(x-\theta_i)}\right).$$

Summarizing the above, we obtain

$$\partial\mathfrak{a}(\sigma,\tau) = \begin{cases}\mathrm{div}(1), & \text{if} \quad \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0},\\ \mathrm{div}\left(\prod\limits_{i\in\{\chi(\sigma)\}}(x-\theta_i)\right), & \text{if} \quad \chi(\sigma) = \sigma\cdot\chi(\tau) \neq \widehat{0},\\ \mathrm{div}\left(\frac{y}{\prod\limits_{\substack{i\notin\{\chi(\sigma)\}\\ i\notin\{\sigma\cdot\chi(\tau)\}}}(x-\theta_i)}\right), & \text{if } \widehat{0} \neq \chi(\sigma) \neq \sigma\cdot\chi(\tau) \neq \widehat{0}.\end{cases}$$

Similar to the elliptic curve case,

$$\partial\mathfrak{a}_1'(\tau,\rho) = \begin{cases}0 = \mathrm{div}(1), & \text{if } \chi_1'(\tau) = 1 \text{ or } \chi_1'(\rho) = 1,\\ 2(T_1) - 2(T_0) = \mathrm{div}(x-\theta_i), & \text{if} \quad \chi_1'(\rho) = \chi_1'(\tau) = -1.\end{cases}$$

Choose the uniformizers t_P at a non-Weierstrass point P on C as $x - x(P)$, as $(x-\theta_i)/y$ at a Weierstrass point T_i with $i \neq 0$, and x^g/y at T_0. Then, $(\partial\mathfrak{a} \cup_1 \mathfrak{a}_1')(\sigma,\tau,\rho) = 1$

if $\chi'(\rho) = 1$. If $\chi'(\rho) = -1$, then

$$\partial\mathfrak{a} \cup \mathfrak{a}'_1(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0}, \\ \prod\limits_{i\in\{\chi(\sigma)\}} s_{1i}, & \text{if } \chi(\sigma) = \sigma\cdot\chi(\tau),\ 1 \notin \{\chi(\sigma)\}, \\ s_1 \prod\limits_{\substack{i\neq 1 \\ i\in\{\chi(\sigma)\}}} s_{1i}, & \text{if } \chi(\sigma) = \sigma\cdot\chi(\tau),\ 1 \in \{\chi(\sigma)\}, \\ \frac{1}{\prod\limits_{\substack{i\notin\{\chi(\sigma)\} \\ i\notin\{\sigma\cdot\chi(\tau)\} \\ i\neq 1}} s_{1i}}, & \text{if } \chi(\sigma) \neq \sigma\cdot\chi(\tau),\ 1 \notin \{\chi(\sigma)\} \cup \{\sigma\cdot\chi(\tau)\}, \\ \frac{s_1}{\prod\limits_{\substack{i\notin\{\chi(\sigma)\} \\ i\notin\{\sigma\cdot\chi(\tau)\}}} s_{1i}}, & \text{if } \chi(\sigma) \neq \sigma\cdot\chi(\tau),\ 1 \in \{\chi(\sigma)\} \cup \{\sigma\cdot\chi(\tau)\}, \end{cases}$$

where $s_{ij} := \theta_i - \theta_j$, and $s_i := \prod\limits_{j\neq i} s_{ij}$. In the above expression for $\partial\mathfrak{a} \cup_1 \mathfrak{a}'(\sigma,\tau,\rho)$, we assume that $\chi(\sigma)$ and $\chi(\tau)$ are not $\widehat{0}$ except for the first case. Similarly,

$$\mathfrak{a} \cup \partial\mathfrak{a}'_1(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi'_1(\tau) = 1 \text{ or } \chi'_1(\rho) = 1, \\ \prod\limits_{i\notin\{\chi(\sigma)\}} s_{i1}, & \text{if } 1 \notin \{\chi(\sigma)\},\ \chi(\sigma) \neq \widehat{0},\ \chi'_1(\tau) = \chi'_1(\rho) = -1, \\ s_1 \prod\limits_{\substack{i\in\{\chi(\sigma)\} \\ i\neq 1}} s_{i1}, & \text{if } 1 \in \{\chi(\sigma)\},\ \chi(\sigma) \neq \widehat{0},\ \chi'_1(\tau) = \chi'_1(\rho) = -1. \end{cases}$$

We have the following useful lemma for finding a 1-cochain that trivializes a 2-cocycle representing the trivial class in the Brauer group of a number field, given that it factors through a nice extension.

Lemma 4.3.16. *Let L/k be a finite extension of fields with $G := \mathrm{Gal}(L/k)$. Let H, N be subgroups of G with N normal in G. Assume that $G \simeq N \rtimes H$, and write $g = nh$ for each element $g \in G$ with $n \in N$ and $h \in H$. Let $E \in \mathrm{Z}^2(L)$ represent the trivial class in $\mathrm{Br}(L/k)$ with the property that $\mathrm{res}^H_G(E) = 0$, $E(g,g') = E(n,n'_h)$, where $n'_h = hn'h^{-1}$, and E restricted to $G \times H \cup H \times G$ is trivial. Then there is $e \in \mathrm{C}^1(L)$ such that*

1. *$e(g) = e(n)$, for $g = nh \in G$,*
2. *$he(n') = e(n'_h)$ for each $n' \in N$ and $h \in H$,*

and $\partial e = E$.

Proof. If there is an $e \in \mathrm{C}^1(N, L^\times)$ satisfying only the second property above, and $\partial e = \mathrm{res}^N_G(E)$, then we extend e to define a 1-cochain (also called e) in $\mathrm{C}^1(G, L^\times)$ by $e(nh) = e(n)$. Now

$$\partial e(nh, n'h') = \frac{nhe(n')e(n)}{e(nn'_h)} = \frac{ne(n'_h)e'(n)}{e'(nn'_h)} = \partial e(n, n'_h) = E(n, n'_h) = E(g, g').$$

Therefore, the rest of the proof is trying to prove the existence of such an e.

Let $e : G \to L^\times$ be a 1-cochain such that $\partial e = E$. Then $E(h, n') = 1$ is equivalent to $e(hn') = he(n)e(h)$, and $E(h, h') = 1$ is equivalent to saying that $e(hh') = he(h')e(h')$. Then $\mathrm{res}^H_G(e)$ is a 1-cocycle. Hence, by Hilbert's Theorem 90, there is a $b \in L^\times$ such that $e(h) = h(b)/b$.

Using $E(nh, n') = E(n, n'_h)$,

$$n\left(\frac{he(n')}{e(n'_h)}\right) = \frac{e(nhn')e(n)}{e(nn'_h)e(nh)} = \frac{e(nhn')}{e(nn'_h)ne(h)} = \frac{nn'_he(h)}{ne(h)}.$$

This implies that

$$\frac{he(n')}{e(n'_h)} = \frac{n'_he(h)}{e(h)} = \frac{hn'(b)b}{n'_h(b)h(b)} \Longrightarrow h\left(\frac{e(n')}{n'(b)/b}\right) = \frac{e(n'_h)}{n'_h(b)/b}.$$

Now $e'(n) \coloneqq e(n)b/n(b)$ is an element of $\mathrm{C}^1(N, L^\times)$ such that $\partial e' = \mathrm{res}^N_G(E)$ and e' satisfies the second property in the statement of the proposition. Hence, by the first part of the proof, e' can be extended to give a 1-cochain $e'' \in \mathrm{C}^1(L^\times)$ such that $\partial e'' = E$. We can choose our e in the proposition to be e'' which proves the proposition. □

Remark 4.3.17. In the general setup E_1 and $E_{1,g}$ defined in §4.3.1 satisfy the above property as $\mathrm{Gal}(F/K') \simeq C_2^{l-1} \rtimes S_{l-1}$. Hence, one can reduce the case of computing e_1 and $e_{1,g}$ such that $\partial e_1 = E_1$ and $\partial e_{1,g} = E_{1,g}$, to only computing e_1 and $e_{1,g}$ such that $\partial e_* = \mathrm{res}^{G_{k(J[2])}}_{G_k} E_*$. This can be done by symbolically defining the algebras corresponding to the general symbolically defined cocycles E_1 and $E_{1,g}$ and then specializing them.

Recall the conjugation homomorphism on n-cochains from §1.3.3. The following remark is regarding σ_* on the 2-cochain $\partial\mathfrak{a} \cup \mathfrak{a}'_1(*, *, -1)$.

Remark 4.3.18. Let $E \coloneqq \partial\mathfrak{a} \cup \mathfrak{a}'_1(*, *, -1)$ and $\sigma \in \mathrm{Gal}(F/k)$ be such that $\chi(\sigma) = \widehat{0}$. Then E is invariant under σ_*. This is because $\sigma_*(E) = \sigma_*(\partial\mathfrak{a} \cup \mathfrak{a}'_1) \cup \sigma_*((T_1) - (T_0)) = \partial\sigma_*(\mathfrak{a}) \cup ((T_1) - (T_0))$. Now, $\sigma_*(\mathfrak{a})(\tau) = \sigma\mathfrak{a}(\sigma^{-1}\tau\sigma) = \sigma\mathfrak{a}(\sigma^{-1} \cdot \chi(\tau)) = \mathfrak{a}(\chi(\tau)) = \mathfrak{a}(\tau)$.

4.3.5 Prime bounds

Let $a, a' \in \mathrm{S}^{(2)}(J/k)$ be represented by $d, d' \in A^\times$ as before, and let ε be the corresponding ε. Let

$$S_{a,a'} \coloneqq \{v \mid v \text{ is a place of } k \text{ of bad reduction of } C \text{ or } \mathrm{ord}_v(\varepsilon(\sigma,\tau)) \neq 0 \text{ for some } \sigma,\, \tau\} \cup \{\text{places above 2 and } \infty\}.$$

In this regard, we have the following lemma.

Lemma 4.3.19. *Let $v \notin S_{a,a'}$ be a place of k. Then $(\delta_{i,v}, d_i)_v = 1$ for each G_{k_v}-orbit of Δ.*

Proof. We prove that $(\delta_{1,v}, d_1')_v = 1$, assuming $\theta_1 \in k$. If d_1' is a square, then there is nothing to prove. Hence, we assume that d_1' is not a square in k_v. Recall the definition of $\delta_{1,v} = \frac{\gamma_{1,v}(g,-1)}{g(\omega_{1,v})\cdot\omega_{1,v}}$ from Equation (4.3.7). We show that $\gamma_{1,v}$ factors through k_v^{nr} for $v \notin S_{a,a'}$ and $\mathrm{ord}_v(\gamma_{1,v}(g,-1))$ is even. Hence, $\omega_{1,v} \in (k_v^{\mathrm{nr}})^\times$ and $\mathrm{ord}_v(\delta_{1,v}) \equiv 0 \mod 2$ for $v \notin S_{a,a'}$. Recall that $\mathrm{S}^{(2)}(J/k) \subset \mathrm{H}^1(G_k, J[2]; S)$, where S is the set of primes of bad reduction of C (Proposition 1.4.5). If $d = (d_1, \ldots, d_l)$, then $\mathrm{ord}_w(d_i) \equiv 0 \mod 2$ for the place w above $k_v(\theta_i)$ for each i. Furthermore, the set primes of bad reduction of C contains the set of ramified primes of the component fields of the étale algebra A; hence, F/k is unramfied at v. In particular, if we choose $\mathfrak{b}_v$ to be defined over F_v, then $\gamma_{1,v}$ factors through $\mathrm{Gal}(k_v^{\mathrm{nr}}/k_v)$.

If $v \notin S_{a,a'}$, then the values taken by ε_1 have a trivial valuation at v, i.e., are units in $\mathcal{O}_{L_v}$ (recall from §4.3.1 that ε_1 factors through $F^\times$). Let

$$z \coloneqq (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 ((T_1) - (T_0)) \in \mathrm{C}^1(k_v).$$

We show that $z(g)$ and $\mathfrak{b}_v \cup_2 \mathrm{div}(x - \theta_i)$ have even valuations at v and therefore, $\gamma_{1,v}(g,-1)$ has even valuation. We have

$$\partial z = \partial\mathfrak{a}_v \cup_1 ((T_1) - (T_0))$$

which is the localization of the global 2-cocycle $\partial\mathfrak{a} \cup_1 ((T_1) - (T_0))$ at v (we will consider such 2-cocycles later again in Chapter 6 to give easier proofs of global computations). Recall from the previous section that one can choose $\mathfrak{a}$ such that the values taken by $\partial\mathfrak{a}_v \cup_1 ((T_1) - (T_0))$ are multiplicative expressions in s_{1j}. Hence, the values of $\partial\mathfrak{a}_v \cup_1 ((T_1) - (T_0))$ are units. In particular, for $g \in G_{k_v}$,

$$(\partial\mathfrak{a}_v \cup_1 ((T_1) - (T_0)))(g,g) = (\partial z)(g,g) = g(z(g))z(g).$$

Hence, $z(g)$ is a unit.

Without loss of generality, one can choose $\mathfrak{b}_v \coloneqq \sum_{i=1}^{(l-1)/2} ((P_{i,v}) - (T_0))$. Consider the field $F_v(P_{i,v})$ (this may be a ramified extension), and let w be the unique place

of $F_v(P_{i,v})$ above v with uniformizer π_w. Let $P_{i,v} := (x_i, y_i)$. If $\mathrm{ord}_w(y_i) = k_i$, then $\mathrm{ord}_w(f(x_i)) = 2k_i$. If $k_i = 0$, then $\mathrm{ord}_w(x_i - \theta_1) = 0$ and so is the case with conjugates of x_i, and the contribution from the orbit of the divisor $(P_{i,v}) - (T_0)$ in $\mathfrak{b}_v \cup_2 \mathrm{div}(x - \theta_1)$ is a unit. Therefore, we assume that $k_i \neq 0$. If $k_i < 0$, then $\mathrm{ord}_w(x_i - \theta_1) = \ldots = \mathrm{ord}_w(x_i - \theta_l)$ and $2|\mathrm{ord}_w(x_i - \theta_1)$. A similar argument for conjugates of x_i shows that the contribution from the orbit of the divisor $(P_{i,v}) - (T_0)$ in $\mathfrak{b}_v \cup_2 \mathrm{div}((x - \theta_1))$ has an even valuation. Lastly, if $k_i > 0$ and $\pi_w | x_i - \theta_1$, then $\pi_w \nmid x_i - \theta_j$ for $j \neq 1$. Otherwise, $\pi_w | s_{1j}$ but v is a prime of good reduction of f. Hence, $\mathrm{ord}_w(x_i - \theta_1) = 2k_i$ and so is the case with the conjugates of $(P_{i,v}) - (T_0)$. Therefore, $\mathrm{ord}_v(\mathfrak{b}_v \cup_2 \mathrm{div}(x_i - \theta_1))$ is even. □

In view of the §4.3.4 and the above lemma, we have the following corollary.

Corollary 4.3.20. *Let $a, a' \in \mathrm{S}^{(2)}(J/k)$ and $S_{a,a'}$ be as above. Then*

$$(-1)^{\langle a, a' \rangle_{\mathrm{CT}}} = \prod_{v \in S_{a,a'}} \prod_{\text{orbits}} (\delta_{i,v}, d_i)_{k_v(\theta_i)}.$$

4.3.6 Algorithm

The following is pseudocode that states the key steps of an algorithm to compute the CTP, based on the above computations. Here we have identified $\mathrm{S}^{(2)}(J/k)$, where J is the Jacobian of an odd-degree hyperelliptic curve $C : y^2 = f(x)$, with a subgroup of $A^\times/(A^\times)^2$, where A is the étale algebra $A = k[x]/\langle f \rangle$. The input elements $d, d' \in A^\times$ represent the 2-Selmer elements a, a', respectively.

Algorithm 1 Compute the CTP between $a, a' \in \mathrm{S}^{(2)}(J/k)$ represented by $d, d' \in A^\times$.

Require: $d, d' \in A^\times$.
Ensure: Value of $(-1)^{\langle a, a' \rangle_{\mathrm{CT}}}$ in variable CT.

```
CT ← 1                                              ▷ Value of CT.
LocalPoints ← [ ].                                  ▷ List storing P_v indexed by S_{a,a'}.
for v ∈ S_{a,a'} do
    Find Q_v ∈ J(k_v) such that δ(Q_v) = α_v.       ▷ α ∈ C^1(G_k, J[2]) is as in §4.3.4.
    K_v ← k_v(√d_v) and P_v ← (1/2)Q_v ∈ J(K_v).    ▷ Computed using Stoll's algorithm.
    for T ∈ J[2] and T ∉ J(k_v)[2] do               ▷ Adjust P_v.
        if ∂(P_v + T) = α_v then
            P_v ← P_v + T, and exit the inner loop.
        end if
    end for
    LocalPoints[v] ← P_v.
end for
```

$K \leftarrow k(\sqrt{d})$. ▷ Adjoining $\sqrt{d}$ means adjoining $\sqrt{d_1}, \ldots, \sqrt{d_l}$, where $(d_1, \ldots, d_l)$ is as in §4.3.4.
for $\theta \in \{\text{Factors of } f\}$ **do**
  $k_\theta \leftarrow k[x]/\langle\theta\rangle$ and $\theta_1 \leftarrow$ a root of θ.
  $d_1' \leftarrow d'(\theta_1)$ and $K' \leftarrow k_\theta(\sqrt{d_1'})$.
  Compute 2-cocycles $E_1, E_{1,g} \in \mathrm{Z}^2(KK'/K')$, using §4.3.4.
  Solve for $e_1, e_{1,g} \in \mathrm{C}^1(KK'/K')$ such that $\partial e_1 = E_1$ and $\partial e_{1,g} = E_{1,g}$. ▷ One can use generic algorithms available in Magma to obtain e_1 and $e_{1,g}$. Lemma 4.3.16 can be used to obtain e_1 and $e_{1,g}$ with nicer properties.
  Compute 1-cocycle $\phi_{1,g}$ and solve for a Hilbert's Theorem 90 element $t_{1,g}$.
  Compute 1-cochain $f_{1,g}'$ and solve for $c_{1,g}$, using Remark 4.3.12.
  for $v \in S_{a,a'}$ **do**
    for $w \in \{\text{Places of } k(\theta) \text{ above } v\}$ **do**
      $\theta_{1,w} \leftarrow$ Image of θ_1 under the embedding $k_\theta \hookrightarrow (k_\theta)_w$ and $d_{1,w}' \leftarrow d'(\theta_{1,w})$.
      Compute $\varepsilon_{1,w}$ and $\gamma_{1,w}$. ▷ By Equation (4.2.1).
      Compute $\Gamma_{1,w}$, $\omega_{1,w}$, and $\delta_{1,w}$. ▷ By Proposition 4.3.15 and Equation (4.3.7).
      $\mathrm{CT} \leftarrow \mathrm{CT} \cdot (\delta_{1,w}, d_{1,w})_{(k_\theta)_w}$
    end for
  end for
end for
return CT.

4.4 A conditional but simpler algorithm

In this section we give a simpler algorithm to compute the CTP for odd-degree hyperelliptic curves, conditioned on the existence of global solutions to certain ternary quadratic forms. Since checking if a ternary quadratic form has a global solution is equivalent to computing a finite number of local Hilbert symbols, it is not an expensive check. The simplicity of the algorithm lies in reducing the time complexity for the global step and being able to explicitly write down ε_1 such that $\partial\varepsilon_1 = \eta_1$ (as defined in the previous section) using the solutions to these quadratic forms. The motivation for doing so clearly comes from the case of elliptic curves in the previous chapter. However, unlike the case of elliptic curves, where the twisted curve is given by the vanishing of a pencil of ternary quadratic forms (§3.1.1), the equations describing a twist (corresponding to a 2-Selmer element) of the Jacobian of a genus $g \geq 2$ hyperelliptic curve are not necessarily ternary quadratic forms. Before moving ahead, we prove the following important lemma.

Lemma 4.4.1. *Let L/k be a finite extension with $G := \mathrm{Gal}(L/k) \simeq C_2^n$ with generators $g_1, \cdots, g_n$. Let $E \in \mathrm{Z}^2(L/k)$ be a 2-cocycle representing the trivial class in*

$\mathrm{Br}(L/k)$ *such that* E *takes values in* $k^\times$ *and* $E(g,h) = E(h,g)$ *for all* $g, h \in G$. *Let* $b_i \in L^\times$ *be such that* $E(g_i, g_i) = g_i(b_i)b_i$ *and* $g_j(b_i) = -b_i$ *for* $j \neq i$. *Then the 1-cochain* $e : G \to L^\times$ *given by*

$$e(g_{i_1} \cdots g_{i_t}) \coloneqq (-1)^{\frac{t(t-1)}{2}} \frac{\prod_{m=1}^{t} b_{i_m}}{\prod_{m=1}^{t-1} E(g_{i_m}, g_{i_{m+1}} \cdots g_{i_t})},$$

satisfies $\partial e = E$.

Proof. First we check that the definition of e makes sense i.e. if $g = \prod_{i \in S} g_i$ for some $S \subset \{1, \cdots n\}$, then $e(g)$ does not depend on the ordering of elements in S. We first show that e is well defined up to swaping of two consecutive elements in a given expression of g. Let $g = g_{i_1} \cdots g_{i_t}$ and say we swap g_{i_m} and $g_{i_{m+1}}$. From the expression of $e(g)$, we get that

$$\begin{aligned}\frac{e(g_{i_1} \cdots g_{i_t})}{e(g_{i_1} \cdots g_{i_{m+1}} g_{i_m} \cdots g_{i_t})} &= \frac{E(g_{i_m}, g_{i_{m+1}} \cdots g_{i_t}) E(g_{i_{m+1}}, g_{i_{m+2}} \cdots g_{i_t})}{E(g_{i_{m+1}}, g_{i_m} g_{i_{m+2}} \cdots g_{i_t}) E(g_{i_m}, g_{i_{m+2}} \cdots g_{i_t})} \\ &\qquad (E \text{ is a 2-cocycle}) \\ &= \frac{E(g_{i_m} g_{i_{m+1}}, g_{i_{m+2}} \cdots g_{i_t}) E(g_{i_m}, g_{i_{m+1}})}{E(g_{i_{m+1}} g_{i_m}, g_{i_{m+2}} \cdots g_{i_t}) E(g_{i_{m+1}}, g_{i_m})} = 1.\end{aligned}$$

Hence, e is independent of the order. Let $\sigma = \sigma_1 \cdots \sigma_t$ and $\tau = \sigma_1 \cdots \sigma_m \tau_{m+1} \cdots \tau_s$ be two elements of G with $\sigma_i, \tau_i \in \{g_1, \ldots, g_n\}$ and $\{\tau_{m+1}, \ldots, \tau_s\} \cap \{\sigma_1, \ldots, \sigma_t\} = \emptyset$. We have

$$\partial e(\sigma, \tau) = \frac{\sigma e(\tau) e(\sigma)}{e(\sigma_{m+1} \cdots \sigma_t \tau_{m+1} \cdots \tau_s)} = (-1)^z \Gamma \prod_{i=1}^{m} e(\sigma_i) \sigma_i(e(\sigma_i)),$$

where $z = \frac{t(t-1)}{2} + \frac{s(s-1)}{2} + m(t-1) + (s-m)t - \frac{(s+t-2m)(s+t-2m-1)}{2} = 2(m(s+t) - m^2)$ and

$$\begin{aligned}\Gamma &= \frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s)}{E(\sigma_1, \sigma_2 \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t) E(\sigma_1, \sigma_2 \cdots \tau_s) \cdots E(\sigma_m, \tau_{m+1} \cdots \tau_s)} \\ &\qquad (\partial E(g,g,h) = 1) \\ &= \frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s)}{E(\sigma_1, \sigma_2 \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t)} \\ &\quad \frac{E(\sigma_1, \sigma_1 \sigma_2 \cdots \tau_s) \cdots E(\sigma_m, \sigma_m \tau_{m+1} \cdots \tau_s)}{E(\sigma_1, \sigma_1) \cdots E(\sigma_m, \sigma_m)}.\end{aligned}$$

Applying repeatedly $\partial E(h, g, ghh') = 1$,

$$\begin{aligned}\partial e(\sigma, \tau) = &\frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s)}{E(\sigma_m, \sigma_{m+1} \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t)} \\ &\frac{E(\sigma_1 \cdots \sigma_m, \tau) E(\sigma_2, \sigma_1) \cdots E(\sigma_m, \sigma_1 \cdots \sigma_{m-1})}{E(\sigma_1, \sigma_2 \cdots \sigma_t) \cdots E(\sigma_{m-1}, \sigma_m \cdots \sigma_t)}.\end{aligned}$$

The expression $e(\sigma_1 \cdots \sigma_m) = e(\sigma_m \sigma_{m-1} \cdots \sigma_1)$ implies that

$$E(\sigma_2, \sigma_1) \cdots E(\sigma_m, \sigma_1 \cdots \sigma_{m-1}) = E(\sigma_1, \sigma_2 \cdots \sigma_m) \cdots E(\sigma_{m-1}, \sigma_m).$$

Combining this with $\partial E(\sigma_i, \sigma_{i+1} \cdots \sigma_m, \sigma_{m+1} \cdots \sigma_t) = 1$, we obtain

$$\begin{aligned}
\partial e(\sigma, \tau) &= \frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s) E(\sigma_1 \cdots \sigma_m, \tau)}{E(\sigma_m, \sigma_{m+1} \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t)} \\
&\quad \frac{E(\sigma_2 \cdots \sigma_m, \sigma_{m+1} \cdots \sigma_t)}{E(\sigma_1 \cdots \sigma_m, \sigma_{m_1} \cdots \sigma_t)} \cdots \frac{E(\sigma_m, \sigma_{m+1} \cdots \sigma_t)}{E(\sigma_{m-1}\sigma_m, \sigma_{m+1} \cdots \sigma_t)} \\
&\qquad\qquad \text{(canceling out the cascading product)} \\
&= \frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s) E(\sigma_1 \cdots \sigma_m, \tau)}{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t) E(\sigma_1 \cdots \sigma_m, \sigma_{m+1} \cdots \sigma_t)} \\
&\qquad\qquad (\because \partial E(\sigma_{m+1} \cdots \sigma_t, \sigma_1 \cdots \sigma_m, \tau) = 1) \\
&= \frac{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t \tau_{m+1} \cdots \tau_s) \cdots E(\sigma_t, \tau_{m+1} \cdots \tau_s)}{E(\sigma_{m+1}, \sigma_{m+2} \cdots \sigma_t) \cdots E(\sigma_{t-1}, \sigma_t) E(\sigma_{m+1} \cdots \sigma_t, \tau_{m+1} \cdots \tau_s)} E(\sigma, \tau) \\
&\qquad\qquad (\because \partial E(\sigma_i, \sigma_{i+1} \cdots \sigma_t, \tau_{m+1} \cdots \tau_s) = 1 \text{ for } i > m) \\
&= E(\sigma, \tau).
\end{aligned}$$

□

We begin with the assumption that $K \cap K' = k$ and $\mathrm{Gal}(F/k) \simeq (C_2^{l-1} \rtimes S_{l-1}) \times C_2$, and compute symbolically and explicitly. The general case will just be restriction of the generic output of the following computations to a subgroup of $(C_2^{l-1} \rtimes S_{l-1}) \times C_2$. Further, for $\sigma \in \mathrm{Gal}(F/K')$ we have $\sigma = \sigma_s \sigma_p$ with $\sigma_s \in \mathrm{C}_2^{l-1}$ and $\sigma_p \in S_{l-1}$, considering S_{l-1} and C_2^{l-1} as subgroups of $\mathrm{Gal}(F/K') \simeq C_2^{l-1} \rtimes S_{l-1}$. In this case note that $\chi(\sigma) = \chi(\sigma_s)$ and $\chi(\sigma) = \widehat{0}$ if $\sigma \in S_{l-1}$.

Define the affine plane curve

$$C_{1j} : d_j u_j^2 - d_1 v_j^2 + \theta_j - \theta_1 = 0,$$

where u_j and v_j are coordinates, for $2 \leq j \leq l$. Note that $\Delta \setminus \{T_1\}$ forms a G_k-set. Fix representatives of orbits of $\Delta \setminus \{T_1\}$. If C_{1j} has a $k(\theta_j)$-rational point (u_j, v_j), and $T_k \neq T_j$ is in the orbit of T_j, then for all $\sigma \in G_k$ such that $\sigma(T_j) = T_k$ the point $(\sigma(u_2), \sigma(v_2))$ is a point satisfying the conic C_{1k} (note that $(\sigma(u_j), \sigma(v_j)) \in k(\theta_k)$ is the same point for all $\sigma \in G_k$ such that $\sigma(T_j) = T_k$). Hence, for each T_k in the orbit of T_j, let $(u_k, v_k) := (\sigma(u_j), \sigma(v_j))$ for some $\sigma \in G_k$ with $\sigma(T_2) = T_k$. In this way we define $u_j, v_j \in k(\theta_j)$ for all $j \neq 1$ (assuming that each C_{1j} has a solution over $k(\theta_j)$). Define

$$p_{1j} = \sqrt{d_1} u_j + \sqrt{d_j} v_j,$$

for all $j \neq 1$, and $p_1 := \prod_{j \neq 1} p_{1j}$.

In view of the above discussion, we have the following useful observation.

Remark 4.4.2. Let $\sigma \in G_k$ be such that $\sigma(T_j) = T_k$. Then $\sigma(p_{1j}) = \sigma_s(p_{1k})$, and

$$\sigma(p_1) = \sigma_s\left(\prod_{l\neq 1} p_{1\sigma\cdot l}\right) = \sigma_s(p_1).$$

Assumption 4.4.3. *We assume that for all $j \neq 1$, the curves C_{1j} have solutions (u_j, v_j) with the property that if $\sigma\theta_j = \theta_k$, then $(u_k, v_k) = (\sigma u_j, \sigma v_j)$.*

Let $g_j \neq \mathrm{id}$ be the element of $\langle g_2, \ldots, g_l\rangle = \mathrm{Gal}(K/k(J[2])) \simeq C_2^{l-1}$ such that $g_j(\sqrt{d_j}) = \sqrt{d_j}$ and $g_j(\sqrt{d_k}) = -\sqrt{d_k}$ for $k \neq j$, in other words $\chi(g_j) = \widehat{j}$. Note that $\eta_1(\sigma,\tau,\rho) = \partial\mathfrak{a} \cup_1 \mathfrak{a}_1'(\sigma,\tau,\rho)$ when $\chi_1'(\sigma) = \chi_1'(\tau) = -\chi_1(\rho) = 1$. Therefore, for $\sigma,\tau,\theta \in G_{K'}$, $\partial(\partial\mathfrak{a} \cup_1 \mathfrak{a}_1'(-1))(\sigma,\tau,\theta) = 1$, i.e., $\partial\mathfrak{a} \cup_1 \mathfrak{a}_1'(-1)$ is a 2-cocycle factoring through $\mathrm{Gal}(K/k) \simeq C_2^{l-1} \rtimes S_{l-1}$. One can check that this is E_1 from §4.3.1, and that $E_1 = E_{1,g}$, with g such that $g\big|_K = \mathrm{id}$ and $\chi_1'(g) = -1$. Lemma 4.3.16 implies that there is a 1-cochain $e_1 \in \mathrm{C}^1(\mathrm{Gal}(K/k(J[2])), K^\times)$ such that $\partial e_1 = \mathrm{res}^{\mathrm{Gal}(K/k(J[2]))}_{\mathrm{Gal}(K/k)} E_1$, $e_1(\sigma_s\sigma_p) = e(\sigma_s)$ and $\sigma_p e_1(\tau_s) = e_1(\sigma_p \cdot \tau_s)$. We have $E_1(g_j, g_j) = s_{1j} = g_j(p_{1j})p_{1j}$ for each $j \neq 1$. Furthermore, $g_k(p_{1j}) = -p_{1j}$ for $j \neq k$ and E_1 takes values in $k(J[2])^\times$ and $E_1(\sigma,\tau) = E_1(\tau,\sigma)$ for $\sigma,\tau \in \mathrm{Gal}(K, k(J[2]))$. Lemma 4.4.1 implies that there exists $e_1 \in \mathrm{C}^1(K/k(J[2]))$ such that $e_1(g_i) = p_{1i}$, and

$$e_1(g_{i_1}\ldots g_{i_t}) = (-1)^{\frac{t(t-1)}{2}} \frac{\prod_{m=1}^{t} p_{1i_m}}{\prod_{m=1}^{t} E(g_{i_m}, g_{i_{m+1}}\ldots g_{i_t})}.$$

Since $g_2, \ldots, g_l$ generate a subgroup $\mathrm{Gal}(K/k(J[2]))$ and $\chi(g_i) = \widehat{i}$ for $2 \leq i \leq l$, for any σ there is a subset $S_\sigma \subset \{2, \ldots, l\}$ such that $\chi(\sigma) = \prod_{i\in S_\sigma} \widehat{i}$. The following proposition gives an ε_1 such that $\partial\varepsilon_1 = \eta_1$.

Proposition 4.4.4. *Let ε_1 be as follows:*

$$\varepsilon_1(\tau,\rho) = \begin{cases} 1 & \text{if } \substack{\chi(\tau)=\widehat{0},\ \chi_1'(\tau)\chi_1'(\rho)=-1 \\ \text{or } \chi(\tau)=\widehat{1},\ \chi_1'(\tau)\chi_1'(\rho)=1, \\ \text{or } \chi_1'(\rho)=1} \\ e(g_{i_1}\cdots g_{i_t}) & \text{if } \chi(\tau) = \prod_{m=1}^{t} \widehat{i_m},\ \chi_1'(\tau) = 1,\ \chi_1'(\rho) = -1, \\ e(g_{i_1}\cdots g_{i_t})/p_1 & \text{if } \chi(\tau) = \prod_{m=1}^{t} \widehat{i_m},\ \chi_1'(\tau) = -1,\ \chi_1'(\rho) = -1. \end{cases} \quad (4.4.1)$$

Then we have $\partial\varepsilon_1 = \eta_1$.

Proof. The proof will proceed similar to the proof of Proposition 3.2.2. Note that $\varepsilon_1(\tau,\rho)$ only depends on $\chi(\tau)$, $\chi_1'(\tau)$ and $\chi_1'(\rho)$; hence, we will interchangeably use $\varepsilon_1(\chi(\tau), \chi_1'(\tau), \chi_1'(\rho))$ for $\varepsilon_1(\tau,\rho)$. We first check that the 1-cochain $\partial\varepsilon_1(*, 1, -1) =$

E_1. All we need to check is that $e_1(*) = \varepsilon_1(*, 1, -1)$ satisfies $\sigma_p \cdot e_1(\tau) = e_1(\sigma_p \cdot \chi(\tau))$. This follows form the fact that $\sigma_p E_1(\tau, \rho) = E_1(\sigma_p \cdot \chi(\tau), \sigma_p \tau_p \rho_s)$ (Remark 4.3.18), and that $e_1(g_{i_1} \dots g_{i_t})$ is independent of the ordering of $g_{i_1}, \dots, g_{i_t}$. Hence, $\partial e_1 = E_1 = \partial\mathfrak{a} \cup_1 ((T_1) - (T_0))$ (Lemma 4.3.16). Noting that $\varepsilon_1(\sigma, -1, -1)/\varepsilon_1(\sigma, 1, -1) = \varepsilon_1(\widehat{0}, -1, -1) = 1/p_1$, the proof of Proposition 3.2.2 implies that it is enough to prove $(\partial\varepsilon_1 - \eta_1)(\sigma, \tau, \rho) = 1$ assuming $\chi_1'(\sigma) = 1$. Let σ, τ, ρ be such that $\chi_1'(\sigma) = 1$ and $\chi_1'(\tau) = \chi_1'(\rho) = -1$ (the case when $\chi_1'(\tau) = 1$ is equivalent to $\partial e_1 = E_1$). Then

$$\begin{aligned}\partial\varepsilon_1(\sigma, \tau, \rho) &= \frac{\sigma(\varepsilon_1(\chi(\tau), -1, -1))\varepsilon_1(\chi(\sigma), 1, 1)}{\varepsilon_1(\chi(\sigma)\sigma_p \cdot \chi(\tau), -1, -1)\varepsilon_1(\chi(\sigma), 1, -1)} \\ &= \frac{p_1 \sigma\varepsilon_1(\chi(\tau), 1, -1)\varepsilon_1(\chi(\sigma), 1, -1)}{\sigma_s(p_1)\varepsilon_1(\chi(\sigma)\sigma_p \cdot \chi(\tau), 1, -1)\varepsilon_1(\chi(\sigma), 1, -1)^2} \\ &= E_1(\chi(\sigma), \sigma_s \cdot \chi(\tau)) \frac{p_1}{\sigma_s(p_1) e_1(\chi(\sigma), 1, -1)^2}.\end{aligned}$$

If $\chi(\sigma) = \widehat{g_{i_1}} \cdots \widehat{g_{i_t}}$, then $\sigma_s = g_{i_1} \cdots g_{i_t}$ and

$$\frac{p_1}{\sigma_s p_1 e_1(g_{i_1} \dots g_{i_t})^2} = (-1)^{lt-2t} \frac{\left(\prod_{m=1}^{t} E_1(g_{i_m}, g_{i_{m+1}} \dots g_{i_t})\right)^2}{p_{1i_1} \dots p_{1i_t} g_{i_1}(p_{1i_1}) \dots g_{i_t}(p_{1i_t})}.$$

Note that whether $1 \in \{\chi(\sigma)\}$ or not depends on whether t is even or odd, respectively. Assume that t is odd. Then the expression of $\partial\mathfrak{a} \cup \mathfrak{a}_1'$ implies

$$E_1(g_{i_1}, g_{i_2} \cdots g_{i_t}) E_1(g_{i_2}, g_{i_3} \cdots g_{i_t}) = \frac{s_1}{\prod_{m=2}^{t} s_{1i_m}} \frac{1}{\prod_{j \notin \{i_2, \dots, i_t\}} s_{1j}} = 1.$$

Therefore,

$$\frac{p_1}{\sigma_s(p_1) e_1(g_{i_1} \cdots g_{i_t})^2} = \frac{1}{s_{i_1 1} \cdots s_{i_t 1}} = \frac{1}{\mathfrak{a} \cup \partial\mathfrak{a}_1'(\chi(\sigma), -1, -1)}.$$

When t is even,

$$\frac{p_1}{\sigma_s(p_1) e_1(g_{i_1} \cdots g_{i_t})^2} = \frac{1}{\prod_{j \notin \{i_1, \dots, i_t\}} s_{1j}^2} \frac{1}{s_{i_1 1} \cdots s_{i_t 1}} = \frac{1}{\mathfrak{a} \cup \partial\mathfrak{a}_1'(\chi(\sigma), -1, -1)}.$$

Therefore, $\partial\varepsilon_1(\sigma, \tau, \rho) = \frac{\partial\mathfrak{a} \cup \mathfrak{a}_1(\sigma, \tau, \rho)}{\mathfrak{a} \cup \partial\mathfrak{a}_1'(\sigma, \tau, \rho)} = \eta_1(\sigma, \tau, \rho)$.

□

4.4.1 Assumption 4.4.3 is not very strict

In this section, we discuss empirical evidence for the fact that assumption 4.4.3 is good enough to compute the kernel of the CTP on Ш[2] × Ш[2] in most cases. For this purpose, we say that $a \in \mathrm{S}^{(2)}(J/k)$ is *good*, if the tuple $(d_1, \dots, d_l)$ corresponding to a satisfies Assumption 4.4.3.

Definition 4.4.5. An odd-degree hyperelliptic curve C is said to be a *good curve* if the subgroup of $\mathrm{S}^{(2)}(J/k)$ generated by the good elements and the image of $J(k)/2J(k)$ is of index at most 2.

In [PS99] the authors show that $\langle\cdot,\cdot\rangle_{\mathrm{CT}}$ is an alternating pairing if C has a k-rational point. In our case C always has a k-rational point T_0. Therefore, it is enough to compute the CTP on $H \times \mathrm{S}^{(2)}(J)$, for an index 2 subgroup H of $\mathrm{S}^{(2)}(J)$. LMFDB [LMF24] mentions 1207 genus 2 curves with analytic rank 0 that admit an odd degree model, with at least 2 extra 2-Selmer group generators. All these curves are good. Furthermore, there are only the following 2 curves

$$y^2 = 8x^5 - 72x^4 + 64x^3 + 17x^2 - 16x - 4,$$
$$y^2 = 8x^5 + 72x^4 + 140x^3 - 103x^2 - 4x,$$

where the subgroup generated by good elements is of index 2, and for every other curve the extra part of the 2-Selmer group is generated by good elements.

Furthermore, in the family of curves $y^2 = x^5 + A$ (which will be the focus in the next chapter), every curve is a good curve for $|A| \leq 2000$. The following theorem proves that every curve is good in a certain family.

Theorem 4.4.6. *Let p be a prime, let $C_p \coloneqq y^2 = x(x^2 - p^2)(x^2 - 4p^2)$, let J_p be its Jacobian variety, and let T_p be the image of $J_p[2]$ inside $\mathrm{S}^{(2)}(J_p/\mathbb{Q})$. Then $\mathrm{S}^{(2)}(J_p)/T_p$ is generated by good elements.*

This theorem will be discussed in a work (joint with Tim Evink), where we compute the CTP explicitly for this family, and show that the rank bounds are equivalent to the ones obtained via visualization. We will not discuss this here in this thesis.

Naturally, every element of the 2-Selmer group of an elliptic curve is good, and therefore every 2-Selmer element of a curve in the family of elliptic curves, $E_p : y^2 = x(x^2 - p^2)$, for p an odd prime, is good. Note that this is a subfamily of the famous congruent number family. Let p be a prime number, and let $g \geq 2$. Define the hyperelliptic curve $C_{p,g} : y^2 = x \prod_{i=1}^{g} (x^2 - i^2p^2)$. Then in view of the previous theorem and the case of elliptic curves, it is a natural question to ask whether, for a fixed $g \geq 3$ and varying primes p, the curves $C_{p,g}$ are good? Unfortunately, experiments show that as the genus increases, the good curves in this family seem to become scarce very fast. For example, if $p < 2000$, then for $g = 3$ there are around 74% good curves. For $g = 4$, there are around 30% good curves, and for $g = 5$, we could not find any good curve. Genus 2 seems to be the sweet spot in this regard.

4.5 Algorithm, implementation and examples

All the computations in the following section and later were performed using the Magma computer algebra system. For computing half of a point, we used the algo-

rithm in [Sto17b, §5]. I thank Michael Stoll for providing me with an implementation of this algorithm over global fields, that was later modified to incorporate the computation over local fields. I also thank him for providing me with a more efficient program for checking whether a given odd-degree hyperelliptic curves is good. This was used in the previous section to get the empirical data.

Remark 4.5.1. The current implementation works over any number field under the assumption that at least one of the elements being paired is good. Apart from the global bottle-neck of solving norm equations, the current implementation uses a non-sophisticated mechanism for finding local points corresponding to the 2-Selmer elements. Hence, sometimes it is a bit slow and may fail in finding them. One idea will be to extract the image of $J(k_v)/2J(k_v)$ from the 2-Selmer group computation, which we anyway have to perform, and feed it inside the algorithm directly.

4.5.1 Algorithm for good elements

Here we provide pseudocode for an algorithm assuming that $a \in \mathrm{S}^{(2)}(J/k)$ is a good element. The code mimics Algorithm 1 for most parts.

Algorithm 2 Compute the CTP between $a, a' \in \mathrm{S}^{(2)}(J/k)$ represented by $d, d' \in A^\times$.

Require: $d, d' \in A^\times$ such that d represents a good 2-Selmer element.
Ensure: Value of $(-1)^{\langle a,a'\rangle_{\mathrm{CT}}}$ in variable CT.

$M \leftarrow$ 2-dimensional list of size $l \times l$ indexed by roots of f with entries as $(0,0)$.
▷ $M[\theta_1, \theta_2]$ will store solutions to the conic $(d(\theta_1)u^2 - d(\theta_2)v^2)/(\theta_1 - \theta_2) + 1 = 0$.
for $\theta \in \{$Factors of $f\}$ **do**
    $k_\theta \leftarrow k[x]/\langle\theta\rangle$ and $\theta_1 \leftarrow$ a root of θ in k_θ.
    for $\theta' \in \{$Factors of f over $k_\theta\}$ and $\theta'(\theta_1) \neq 0$ **do**
        $k_{\theta'} \leftarrow k_\theta[x]/\langle\theta'\rangle$ and $\theta_2 \leftarrow$ a root of θ' in $k_{\theta'}$.
        if $M[\theta_1, \theta_2] \neq (0,0)$ **then**
            Compute (u, v) such that $d(\theta_1)u^2 - d(\theta_2)v^2 = \theta_2 - \theta_1$ and $uv \neq 0$.
            $M[\theta_1, \theta_2] \leftarrow (u, v)$.
            Assign to M at Galois conjugates of the pairs (θ_1, θ_2), the corresponding Galois conjugate of (u, v).
        end if
    end for
end for
CT $\leftarrow 1$ ▷ Value of CT.
LocalPoints $\leftarrow$ [ ]. ▷ List storing P_v indexed by $S_{a,a'}$.
for $v \in S_{a,a'}$ **do**
    Find $Q_v \in J(k_v)$, such that $\delta(Q_v) = \alpha_v$. ▷ $\alpha \in \mathrm{C}^1(G_k, J[2])$ is as in §4.3.4.
    $K_v \leftarrow k_v(\sqrt{d_v})$, $P_v \leftarrow \frac{1}{2}Q_v \in J(K_v)$. ▷ Computed using Stoll's algorithm.

for $T \in J[2]$ and $T \notin J(k_v)[2]$ **do** ▷ Adjust P_v.
  if $\partial(P_v + T) = \alpha_v$ **then**
    $P_v \leftarrow P_v + T$, and exit the inner loop.
  end if
end for
LocalPoints$[v] \leftarrow P_v$.
end for
for $\theta \in \{\text{Factors of } f\}$ **do**
  $k_\theta \leftarrow k[x]/\langle\theta\rangle$ and $\theta_1 \leftarrow$ a root of θ, $d'_1 \leftarrow d'(\theta_1)$.
  for $v \in S_{a,a'}$ **do**
    for $w \in \{\text{Places of } k(\theta) \text{ above } v\}$ **do**
      $\theta_{1,w} \leftarrow$ Image of θ_1 under the embedding $k_\theta \hookrightarrow (k_\theta)_w$ and $d'_{1,w} \leftarrow d'(\theta_{1,w})$.
      Compute $\varepsilon_{1,w}$ and $\gamma_{1,w}$ as in Equation (4.2.1) using the row in M corresponding to $\theta_{1,w}$.
      Compute $\Gamma_{1,w}$, $\omega_{1,w}$, and $\delta_{1,w}$. ▷ By Proposition 4.3.15 and Equation (4.3.7).
      CT $\leftarrow$ CT $\cdot\, (\delta_{1,w}, d_{1,w})_{(k_\theta)_w}$.
    end for
  end for
end for
return CT.

4.5.2 Example of genus 2 (when f splits completely)

It is not hard to check that the curves C_p arise as quadratic twists of $C : y^2 = x(x^2-1)(x^2-4)$ by $\pm p$. We show that $\mathrm{rk}_{\mathbb{F}_2}\left(\ker(\langle\cdot,\cdot\rangle_{\mathrm{CT}})\right)$ is same as $\mathrm{rk}_{\mathbb{F}_2}\left(\mathrm{S}^{(2)}(J/k_p)\right)$, where J is the Jacobian of C and $k_p := \mathbb{Q}(\sqrt{\pm p})$, depending on the class of $p \mod 24$. Hence, it makes more sense to compute the CTP for J over k_p.

Example 4.5.2. Let $p := 1777$ and $k_p := \mathbb{Q}(\sqrt{p})$. Then the group $\mathrm{S}^{(2)}(J/k_p)/T_p$ is generated by

$$\{(1/2(-\sqrt{p}+25), 1/2(-\sqrt{p}+89), 1/2(-\sqrt{p}+39), 1/2(-\sqrt{p}-7), 1/2(-\sqrt{p}+39)),$$
$$(1, 1/2(\sqrt{p}+61), 1/2(\sqrt{p}+43), 1/2(\sqrt{p}-89), 1/2(\sqrt{p}-43)),$$
$$(1/2(-\sqrt{p}+39), 1, 1/2(-\sqrt{p}+41), 1/2(-\sqrt{p}+25), 1/2(-\sqrt{p}-7)),$$
$$(1, 1/2(-\sqrt{p}+43), 1, 1/2(\sqrt{p}-39), 1/2(\sqrt{p}+25))\},$$

and all these elements are good. The elements above are represented by tuples $(d_1, \ldots, d_5)$ corresponding to the elements in the étale algebra $k[T]/\langle f(T)\rangle$. Computing p_{ij}, we obtain that one needs to compute the CTP at primes of k_p above

$$\{2, 3, 5, 7, 11, 17, 31, 37, 43, 97, 271, 2579, 22541, 132371\} \cup \{\infty\}.$$

The primes apart from $\{2, 3, 1777, \infty\}$ appear because of the values of p_{ij} for different values of 2-Selmer elements. We need to compute the CTP at the places above the primes of bad reduction. If we denote the above generating set for the extra 2-Selmer group by α_i, for $i \in \{1 \dots 4\}$, we obtain the following matrix

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

where the (i, j)-entry of M_{CT} is $\langle \alpha_i, \alpha_j \rangle_{\mathrm{CT}}$. We obtain $\mathrm{rk}_{\mathbb{F}_2}(M_{\mathrm{CT}}) = 2$, so $\mathrm{rk}(J_p/\mathbb{Q}) \leq 2$.

Example 4.5.3. Let $p \coloneqq 409$ and $k_p \coloneqq \mathbb{Q}(\sqrt{p})$. Then the group $\mathrm{S}^{(2)}(J/k_p)/T_p$ is generated by

$$\{(1/2(-\sqrt{p}-3), 1, 1/2(-\sqrt{p}+5), 1/2(-\sqrt{p}-11), 1/2(-\sqrt{p}-19)),$$
$$(1, 1/2(-\sqrt{p}+29), 1/2(-\sqrt{p}+21), 1/2(-\sqrt{p}+5), 1/2(-\sqrt{p}-3))\},$$

The primes that may give a non-trivial contribution to CTP are above

$$\{2, 3, 53, 167, 359, 409\} \cup \{\infty\},$$

and

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 2, so $\mathrm{rk}(J_p/\mathbb{Q}) = 0$. This one cannot get simply by using a visualization argument.

Recall that $C_{p,g}$ is the curve given by $y^2 = x \prod_{i=1}^{g} (x^2 - i^2 p^2)$. In the next two sections, we consider curves of genus g higher than 2.

4.5.3 Example of genus 3

Example 4.5.4. Consider the curve $C_{71,3}$. The group $\mathrm{S}^{(2)}(J_{71,3}/\mathbb{Q})/T_{71,3}$ is generated by

$$\{(71, 2130, 1, 2, 3, 1, 5), (142, 71, 3, 1, 2, 3, 1),$$
$$(71, 213, 142, 71, 3, 1, 2), (142, 71, 71, 142, 2, 2, 1)\},$$

where $T_{71,3} \coloneqq J_{71,3}[2]$.

The non-trivial contribution to the pairing may come from the primes

$$\{2, 3, 5, 7, 11, 17, 19, 23, 41, 47, 67, 149, 167, 269, 4933\} \cup \{\infty\},$$

depending on which two elements are being paired. We obtain that

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 4, so $\mathrm{rk}(J_{71,3}/\mathbb{Q}) = 0$.

Next we give an example of computing the CTP for a hyperelliptic genus 3 curve where the defining polynomial f is not completely split.

Example 4.5.5. Consider the curve $C : y^2 = (x-p)(x^4-p^2)(x^2-2p)$, with $p = 179$. The group $\mathrm{S}^{(2)}(J_C/\mathbb{Q})/J_C(\mathbb{Q})[2]$ is generated by

$$\big\{(358, 7\sqrt{358}+179, -7\sqrt{358}+179, -9\sqrt{179}+179, 9\sqrt{179}+179, 2\sqrt{-179}, -2\sqrt{-179}),$$
$$(1, \sqrt{358}+19, -\sqrt{358}+19, -2, -2, (-\sqrt{-179}+11)/2, (\sqrt{-179}+11)/2)\big\}.$$

One can check computationally that the first element is a *good* 2-Selmer element. The non-trivial contribution to the pairing may come from the primes

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 59, 79, 89, 101, 179, 751, 839, 977, 5227\} \cup \{\infty\},$$

depending on which elements corresponding to the local factors are being paired. We obtain that

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 2, so $\mathrm{rk}(J_C/\mathbb{Q}) = 0$ and $J_C(\mathbb{Q}) = J_C(\mathbb{Q})[2]$.

Example 4.5.6. Consider $C : y^2 = x(x^3-p)(x^3-2p)$, with $p = 97$. The group $\mathrm{S}^{(2)}(J_C/\mathbb{Q})/J_C(\mathbb{Q})[2]$ is generated by

$$\big\{(1, -1, -1, -1, -1, -1, -1),$$
$$(97, \sqrt[3]{97}, \zeta_3\sqrt[3]{97}, \zeta_3^2\sqrt[3]{97}, 1, 1, 1),$$
$$(1, -\sqrt[3]{97}-18, -\zeta_3\sqrt[3]{97}-18, -\zeta_3^2\sqrt[3]{97}-18, -1, -1, -1)\big\}.$$

One can check computationally that all the three elements ares *good* 2-Selmer elements. The non-trivial contribution to the pairing may come from the primes

$$\{2, 3, 5, 11, 13, 17, 29, 31, 37, 41, 43, 97, 131,$$
$$179, 757, 997, 1579, 2069, 2099, 3433, 5407, 8839, 9461, 13619, 78167,$$
$$254027, 310229, 5347301, 7540909, 2319939481, 91230796032263161\} \cup \{\infty\},$$

depending on which elements corresponding to the local factors are being paired. We obtain that

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 2; hence, $\mathrm{rk}(J_C/\mathbb{Q}) = 1$ and $J_C(\mathbb{Q}) \simeq J_C(\mathbb{Q})[2] \times \mathbb{Z}$.

4.5.4 Examples of genus 4

Example 4.5.7. Consider the curve $C_{73,4}$. One can show that $C_{73,4}$ is a good curve with $\mathrm{S}^{(2)}(J_{73,4}/\mathbb{Q})/T_{73,4}$ generated by

$$\{(73,1,73,1,1,73,1,73,1),\\ (1,73,1,73,1,1,73,1,73)\},$$

where $T_{73,4} \coloneqq J_{73,4}(\mathbb{Q})[2]$.

The non-trivial contribution to the pairing may come from the primes

$$\{2,3,5,7,73,97\} \cup \{\infty\},$$

depending on which two elements are being paired. We obtain that

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 2, so $\mathrm{rk}(J_{73,4}/\mathbb{Q}) = 0$.

Here we give an example of computing the CTP for a hyperelliptic genus 4 curve where the defining polynomial f is not completely split.

Example 4.5.8. Consider the curve $C : y^2 = (x-p)(x^4-p^2)(x^4-4p^2)$, with $p = 137$. The group $\mathrm{S}^{(2)}(J_C/\mathbb{Q})/J_C(\mathbb{Q})[2]$ generated by

$$\big\{(1,1,1,1,1,1,1,-2,-2),\\ (-1955,-2\sqrt{274}-31,+2\sqrt{274}-31,3\sqrt{137}-411,-3\sqrt{137}-411,\\ 3\sqrt{-137}-411,-3\sqrt{-137}-411,3,3)\big\}.$$

One can check computationally that the first element is a *good* 2-Selmer element. The non-trivial contribution to the pairing may come from the primes

$$\{2,3,5,7,17,23,137,139,193,389,2447\} \cup \{\infty\},$$

depending on which elements corresponding to the local factors are being paired. We obtain that

$$M_{\mathrm{CT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

has $\mathbb{F}_2$-rank 2; hence, $\mathrm{rk}(J_C/\mathbb{Q}) = 0$ and $J_C(\mathbb{Q}) = J_C(\mathbb{Q})[2]$.

Chapter 5

The CTP for the Jacobian of $y^2 = x^l + A$

In this chapter we look into a special class of hyperelliptic curves of the form $C_A : y^2 = x^l + A$, for $A \in \mathbb{Z}$ and l an odd prime. There is a distinguished point at infinity (denoted by T_0, as in the previous chapter) defined over $\mathbb{Q}$, which we use to embed $C_A(\overline{k})$ into its Jacobian $J_A(\overline{k})$ via $P \mapsto [(P) - (T_0)]$. Fix an lth root of unity ζ_l. Then there is a natural automorphism of C_A defined by $(x, y) \mapsto (\zeta_l x, y)$. This induces an automorphism of J_A, also denoted by ζ_l. This choice of notation is justified since the automorphism $1 + \zeta_l + \ldots + \zeta_l^{l-1}$ is trivial on J_A. This is because if $D \coloneqq (P_1) + (P_2) + \ldots + (P_i)$ is a divisor not involving T_0, with $i \leq (l-1)/2$, representing a point on J_A (recall Definition 1.2.16), then $\sum_{j=0}^{l-1} \zeta_l^j(D) = \operatorname{div} \prod_{j=1}^{i}(y - y_j)$, where y_j is the y-coordinate of P_j. Therefore, $\mathbb{Z}[\zeta_l] \subset \operatorname{End}(J_A)$. Then $\lambda \coloneqq 1 - \zeta_l$ is an endomorphism on J_A defined over $k \coloneqq \mathbb{Q}(\zeta_l)$. Fix a square root $\sqrt{A}$ of A in $\overline{k}$, and let $L \coloneqq k(\sqrt{A})$. We will denote the group $J_A(\overline{k})[\lambda]$ by $J_A[\lambda]$. Further, the prime ideal $(1 - \zeta_l)$ is the only prime ideal above l in the maximal order $\mathbb{Z}[\zeta_l]$ of $\mathbb{Q}(\zeta_l)$ and $(l) = (\lambda)^{l-1}$. Hence, $\#J_A[\lambda] = l$ and is generated by the image of the point $P \coloneqq (\sqrt{A}, 0)$ in J_A. The group $J_A[\lambda]$ is defined over $\mathbb{Q}$, but its elements need not be rational points. Let $\mathrm{S}^{(\lambda)}(J_A/k)$ be the Selmer group of λ. Note that C_A can be viewed as a cyclic l-cover of $\mathbb{P}^1$ via the map $(x, y) \mapsto y$ on the affine patch. From the works of Schaefer [Sch96] and Poonen-Schaefer [PS97], we have a handle on $\mathrm{S}^{(1-\zeta_n)}(J_C/k)$, where C is a n-cyclic cover of $\mathbb{P}^1$. Stoll in [Sto98], using this explicit representation of λ-Selmer group for the curves of the form C_A, obtained explicit values of $\mathrm{rk}_{\mathbb{F}_l}(\mathrm{S}^{(\lambda)}(J_A/k))$ in terms of $\mathbb{F}_l$ ranks of $\ker(\mathrm{N} : \mathrm{Cl}(L)[l] \to \mathrm{Cl}(k)[l])$, where $\mathrm{Cl}(*)$ represents the class group of a number field $*$, under the following assumptions on A.

Assumption 5.0.1. [Sto98, Assumption 1.2, 1.3]

*We say that $A \in \mathbb{Z}$ lies in the l-*Stoll set *if A satisfies the following two assumptions:*

1. *$l \nmid A$, and A is not a square in $\mathbb{F}_l^\times$.*
2. *For every prime $p \mid 2A$ and a prime $\mathfrak{p}$ of $\mathbb{Z}[\zeta_l]$ above p, A is not a square in $k_\mathfrak{p}$.*

These assumptions force the local restriction maps $\mathrm{H}^1(G_k, J_A[\lambda]) \to \mathrm{H}^1(G_{k_v}, J_A[\lambda])$ to be trivial at all places v of k outside $\{\lambda\}$. The analysis proceeds by getting explicit elements in the image of $J_A(k_\lambda)/\lambda J_A(k_\lambda)$ inside $\mathrm{H}^1(G_{k_\lambda}, J_A[\lambda])$, and explicitly computing the kernel of the localization map $\mathrm{H}^1(G_k, J_A[\lambda]; \{\lambda\}) \to \mathrm{H}^1(G_{k_\lambda}, J_A[\lambda])$, where $\mathrm{H}^1(G_k, J_A[\lambda]; S)$ for a subset S of places of k is the subgroup of elements that is represented by cocycles which factor through k_v^{nr} for all places v of k outside S.

We know that $\mathrm{S}^{(\lambda)}(J_A/k) \subset \mathrm{H}^1(G_k, J_A[\lambda])$. Since the order of $\mathrm{Gal}(L/k)$ and $J_A[\lambda]$ are coprime to each other, we have $\hat{\mathrm{H}}^i(\mathrm{Gal}(L/k), J_A[\lambda]) = 0$ (Proposition 1.3.22). Therefore, using the inflation-restriction-transgression (part 2 of Proposition 1.3.7) exact sequence we have:

$$H^1(G_k, J_A[\lambda]) \overset{\mathrm{res}}{\to} H^1(G_L, J_A[\lambda])^{G_k/G_L} \simeq \ker\left(\mathrm{N} : L^\times/(L^\times)^l \to k^\times/(k^\times)^l\right),$$

where N is induced from the norm map: $L^\times \to k^\times$. We work with the image of $\mathrm{H}^1(G_K, J_A[\lambda])$ inside $\mathrm{H}^1(G_L, J_A[\lambda])$, which is enough since taking restriction multiplies the value of the pairing by 2, which acts invertibly on $\frac{1}{l}\mathbb{Z}/\mathbb{Z}$. For $d \in L^\times$ and $\sigma \in G_L$, define $\chi_d(\sigma) \coloneqq \sigma(\sqrt[l]{d})/\sqrt[l]{d}$. Note that χ_d takes values in μ_l. Identifying μ_l with $\frac{\mathbb{Z}}{l\mathbb{Z}}$ via $\zeta_l \mapsto 1$, we may assume that χ_d takes values in $\frac{\mathbb{Z}}{l\mathbb{Z}}$.

5.1 Global computation

Let a, $a' \in \mathrm{S}^{(\lambda)}(J_A/k)$ represented by $d, d' \in L^\times$, respectively. Then a 1-cocycle α, representing a, can be chosen as

$$\alpha(\sigma) \coloneqq i[(P) - (T_0)], \qquad \text{if } \chi_d(\sigma) = i,\ 0 \le i \le l-1.$$

Similarly, we can define α' depending on $\chi_{d'}$ representing the class a'. For simplicity of notation, we drop the subscripts in χ_d and $\chi_{d'}$, and denote them by χ and χ', respectively. Since the CTP is an alternating pairing on $Ш(J_A/L)[l]$, we can assume that $L(\sqrt[l]{d}) \cap L(\sqrt[l]{d'}) = L$; i.e., $d \not\equiv d'^z \mod ((L^\times)^l)$, for all $z \in \mathbb{Z}$. We take the following lift of α to $\mathrm{C}^1(G_L, \mathrm{Div}^0((C_A)_{\overline{k}}))$

$$\mathfrak{a}(\sigma) \coloneqq i(P) - i(T_0), \qquad \text{if } \chi(\sigma) = i,\ 0 \le i \le l-1.$$

Taking the coboundary gives

$$\partial\mathfrak{a}(\sigma, \tau) = \mathrm{div}((y - \sqrt{A})^n), \qquad \text{if } \chi(\sigma) = i,\ \chi(\tau) = j, \text{ and } n \coloneqq [(i+j)/l],$$

where $[\cdot]$ denotes the greatest integer function. Similarly, we choose a lift $\mathfrak{a}' \in \mathrm{C}^1(G_L, \mathrm{Div}^0((C_A)_{\overline{k}}))$ of α' as above; then

$$\partial\mathfrak{a}'(\sigma,\tau) = \mathrm{div}((y-\sqrt{A})^{n'}), \quad \text{if } \chi'(\sigma)=i,\ \chi'(\tau)=j, \text{ and } n' \coloneqq [(i+j)/l].$$

We choose the uniformizer as $x^{(l-1)/2}/y$ at T_0. If Q is a Weierstrass point, then we choose y as a uniformizer at Q. Choose $x - x(Q)$ as a uniformizer at all other $Q \in C_A$. The map $Q \mapsto t_Q$, where t_Q is the chosen uniformizer at $Q \in C_A(\overline{k})$ as above, is Galois equivariant. In what follows, we will use the letter k also as an index. However, this will be clear from the context, if it represents a field or index. Further, for $f \coloneqq (y-\sqrt{A})^n$ and $D \coloneqq k(P) - k(T_0)$,

$$\langle \mathrm{div}(f), D\rangle_1 = \frac{\left(\left(\frac{y-\sqrt{A}}{x^l}\right)^n(P)\right)^k}{\left(\left(\frac{(y-\sqrt{A})x^{l(l-1)/2}}{y^l}\right)^n(T_0)\right)^k} = \left(\frac{1}{2\sqrt{A}}\right)^{nk} = \langle D, \mathrm{div}(f)\rangle_2,$$

where $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$ are the modified pairings defined on $\mathrm{Princ}((C_A)_{\overline{k}}) \times \mathrm{Div}^0((C_A)_{\overline{k}})$ and $\mathrm{Div}^0((C_A)_{\overline{k}}) \times \mathrm{Princ}((C_A)_{\overline{k}})$, respectively, as in §2.1.3. We obtain

$$\partial\mathfrak{a} \cup \mathfrak{a}'(\sigma,\tau,\rho) = (2\sqrt{A})^{-nk}, \quad \text{if } \chi(\sigma)=i,\ \chi(\tau)=j,\ \chi'(\rho)=k,\ n=[(i+j)/l]$$

and

$$\mathfrak{a} \cup \partial\mathfrak{a}'(\sigma,\tau,\rho) = (2\sqrt{A})^{-n'k}, \quad \text{if } \chi(\sigma)=i,\ \chi'(\tau)=j,\ \chi'(\rho)=k,\ n'=[k+j)/l].$$

From now on we will assume, for $\sigma,\tau,\rho \in G_L$ and $0 \le i,j,j',k \le l-1$, $\chi(\sigma)=i$, $\chi(\tau)=j$, $\chi'(\tau)=j'$, $\chi'(\rho)=k$, $n=[(i+j)/l]$, and $n' \coloneqq [(j'+k)/l]$. Then $\eta \coloneqq \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' \in \mathrm{Z}^3(L)$ is given by

$$\eta(\sigma,\tau,\rho) = (2\sqrt{A})^{n'i-nk}.$$

Let $K \coloneqq L(\sqrt[l]{d})$, $K' \coloneqq L(\sqrt[l]{d'})$, and $F \coloneqq L(\sqrt[l]{d},\sqrt[l]{d'})$. Let σ_0, σ_0' be the generators of $\mathrm{Gal}(K/L)$, $\mathrm{Gal}(K'/L)$, respectively, such that $\chi(\sigma_0)=\chi'(\sigma_0')=1$. Note that η can be viewed as inflation of an element in $\mathrm{Z}^3(F/L)$. Furthermore, $\eta(\sigma,\tau,\rho)=\eta(\sigma',\tau,\rho')$ if $\chi(\sigma)=\chi(\sigma')$ and $\chi'(\rho)=\chi'(\rho')$. Hence if $\chi(\sigma)=i$, $\chi(\tau)=j$, $\chi'(\tau)=j'$ and $\chi'(\rho)=k$, then we will interchangeably use $\eta(\sigma,\tau,\rho)$ and $\eta(i,j,j',k)$. Here we have identified $\tau\big|_F$ with its image in $\mathrm{Gal}(F/L) \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

Remark 5.1.1. In view of the above, we have

$$\eta(\sigma,\tau,\rho) = \eta(i,(j,0),k)\eta(i,(0,j'),k).$$

The rest of this section is dedicated to solving for $\varepsilon \in \mathrm{C}^2(L)$ such that $\partial\varepsilon = \eta$. Computation of ε is done in two steps. First, we show that there is $\varepsilon' \in \mathrm{C}^2(L)$ such that $\partial\varepsilon' = \eta$ and that ε' has some special properties. Next, we use these properties of ε' to compute ε explicitly.

Proposition 5.1.2. *For $a \in \mathrm{Ш}^{(\lambda)}(J_A/k)$, there is a $g \in \mathrm{H}^1(G_k, J_A[\lambda^2])$ such that $\lambda_* g = a$, where λ_* is the map induced by λ.*

Proof. Using the Galois cohomology and localization on the lower row of the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_A[\lambda] & \longrightarrow & J_A[\lambda^2] & \xrightarrow{\lambda} & J_A[\lambda] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J_A[\lambda] & \longrightarrow & J_A & \xrightarrow{\lambda} & J_A & \longrightarrow & 0 \end{array}, \tag{5.1.1}$$

we have

$$\begin{array}{ccccc} \mathrm{H}^1(G_L, J_A[\lambda^2]) & \xrightarrow{\lambda_*} & \mathrm{H}^1(G_L, J_A[\lambda]) & \xrightarrow{\delta} & \mathrm{H}^2(G_L, J_A[\lambda]) \\ \downarrow & & \downarrow & & \| \\ \mathrm{H}^1(G_L, J_A) & \xrightarrow{\lambda_*} & \mathrm{H}^1(G_L, J_A) & \xrightarrow{\delta} & \mathrm{H}^2(G_L, J_A[\lambda]) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_v \mathrm{H}^1(G_{L_v}, J_A) & \xrightarrow{\lambda_*} & \prod_v \mathrm{H}^1(G_{L_v}, J_A) & \xrightarrow{\delta} & \prod_v \mathrm{H}^2(G_{L_v}, J_A[\lambda]). \end{array} \tag{5.1.2}$$

Since $J_A[\lambda] \simeq \mathbb{Z}/l\mathbb{Z}$ as G_L-module and $\mu_l \subset L$, the Albert-Brauer-Hasse-Noether exact sequence implies that the map $\mathrm{loc}^2(J_A[\lambda]) : \mathrm{H}^2(G_L, J_A[\lambda]) \to \prod_v \mathrm{H}^2(G_{L_v}, J_A[\lambda])$ is injective. Hence, if $a \in \mathrm{Ш}^{(\lambda)}(J_A/k)$, then $\delta(a) = 0$ and there is a $g \in \mathrm{H}^1(G_L, J_A[\lambda^2])$ such that $\lambda_* g = a$. □

We now look at the interaction of λ with the Galois equivariant pairings $\langle \cdot, \cdot \rangle_1$, and $\langle \cdot, \cdot \rangle_2$. Let $f \in \overline{k}(C_A)^\times$ and $D \in \mathrm{Div}^0((C_A)_{\overline{k}})$ be such that $\mathrm{Supp}(\mathrm{div}(f)) \cap \mathrm{Supp}(D) = \emptyset$ and $\mathrm{Supp}(\zeta_{l*} \mathrm{div}(f)) \cap \mathrm{Supp}(D) = \emptyset$. Then $\lambda \,\mathrm{div}(f) = \mathrm{div}(f) - \zeta_{l*}(\mathrm{div}(f)) = \mathrm{div}(f) - \mathrm{div}(\zeta_{l*} f) = \mathrm{div}(f) - \mathrm{div}(f \circ \zeta_l^{-1})$. We have

$$\langle D, \mathrm{div}(f \circ \zeta_l^{-1}) \rangle_2 = \langle \mathrm{div}(f \circ \zeta_l^{-1}), D \rangle_1 = \langle \mathrm{div}(f), \zeta_{l*}^{-1} D \rangle_1,$$

as

$$\prod_{P \in \mathrm{Supp}(D)} f(\zeta_l^{-1} P)^{v_P(D)} = \prod_{P \in \mathrm{Supp}(\zeta_{l*}^{-1} D)} f(P)^{v_P(\zeta_{l*}^{-1} D)}.$$

This implies that $\langle \lambda \,\mathrm{div}(f), D \rangle_1 = \langle \mathrm{div}(f), \hat{\lambda} D \rangle_1$, where $\hat{\lambda} := 1 - \zeta_{l*}^{-1}$. Similarly, $\langle D, \lambda \,\mathrm{div}(f) \rangle_2 = \langle \hat{\lambda} D, \mathrm{div}(f), \rangle 2$. Note that $\hat{\lambda}$ is defined over k.

Lemma 5.1.3. *Let η be as before. Then there is a 2-cochain ε' such that $\partial \varepsilon' = \eta$ with the property that $\varepsilon'(*, \sigma) = 1$, if $\chi'(\sigma) = 0$, and $\varepsilon'(\sigma, \tau) = \varepsilon'(\sigma, \tau')$, if $\chi'(\tau) = \chi'(\tau')$.*

Proof. Proposition 5.1.2 implies that there is a $\gamma \in \mathrm{Z}^1(G_k, J_A[\lambda^2])$ and a $z \in J_A[\lambda]$ such that $\lambda_*(\gamma) = \alpha + \partial z$. Let $\tilde{z} \in J_A[\lambda^2]$ be such that $\lambda \tilde{z} = z$. Then $\lambda_*(\gamma) =$

$\alpha + \partial\lambda_*(\tilde{z}) = \alpha + \lambda_*\partial\tilde{z}$. Therefore, possibly after shifting γ by a coboundary, we assume that $\lambda_*\gamma = \alpha$. Let $\mathfrak{g} \in \mathrm{C}^1(\mathrm{Div}^0((C_A)_{\overline{k}}))$ be a lift of γ such that $\mathfrak{g}$ and $\zeta_{l*}(\mathfrak{g})$ take values with support disjoint from the support of the values taken by $\mathfrak{a}'$. This is always possible by the moving lemma (Lemma 1.2.2). Note that $\lambda_*\mathfrak{g}$ is a lift of α to a 1-cochain with values in $\mathrm{Div}^0((C_A)_{\overline{k}})$, and the values taken by $\lambda_*\mathfrak{g}$ have disjoint support to the ones taken by $\mathfrak{a}'$. Now with the choice of lifts as above

$$\begin{aligned}\eta' \coloneqq \partial\lambda_*\mathfrak{g} \cup_1 \mathfrak{a}' - \lambda_*\mathfrak{g} \cup_2 \partial\mathfrak{a}' &= \lambda_*\partial\mathfrak{g} \cup_1 \mathfrak{a}' - \mathfrak{g} \cup_2 \partial\hat{\lambda}_*\mathfrak{a}' \\ &= \partial\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}' - \mathfrak{g} \cup_2 \partial\hat{\lambda}_*\mathfrak{a}' = \partial(\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}').\end{aligned}$$

The second to last equality above is because $\hat{\lambda}_*(\mathfrak{a}')$ takes values in principal divisors. Note that $\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}'$ has the property that $\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}'(\sigma,\tau) = \mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}'(\sigma,\tau')$, if $\chi'(\tau) = \chi'(\tau')$, and $\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}'(\sigma,\tau) = 1$, if $\chi'(\tau) = 0$. If $\mathfrak{a}$ is any other lift of α, then we have $\mathfrak{a} = \lambda_*\mathfrak{g} + \mathfrak{f}$, where $\mathfrak{f}$ is a 1-cochain with values in $\mathrm{Princ}((C_A)_{\overline{k}})$. This changes η' by $\partial(\mathfrak{f} \cup_1 \mathfrak{a}')$ and hence we choose ε' to be $\mathfrak{g} \cup_2 \hat{\lambda}_*\mathfrak{a}' + \mathfrak{f} \cup_1 \mathfrak{a}'$. Note that ε' satisfies the conclusion of the lemma. □

Similarly to η, we will interchangeably use $\varepsilon'(\sigma,\tau)$ and $\varepsilon'(\sigma,k)$ for $\sigma,\tau \in G_L$ and $\chi'(\tau) = k$. Now using ε' we will construct a "nice" ε explicitly such that $\partial\varepsilon = \eta$. The process is very similar to the one in §4.3.1. If $\sigma,\tau \in G_{K'}$ and $\chi'(\rho) = k$, then define $E_k \in \mathrm{C}^2(K')$ by

$$E_k(\sigma,\tau) \coloneqq \eta(\sigma,\tau,k).$$

Proposition 5.1.4. *We have $E_k \in \mathrm{Z}^2(K')$, for each $0 \le k \le l-1$. Furthermore, E_k represents the trivial class in $\mathrm{Br}(K')$.*

Proof. Let $\sigma,\tau,\rho \in G_{K'}$ and $\chi'(\theta) = k$. Then

$$\begin{aligned}1 = \partial\eta(\sigma,\tau,\rho,\theta) &= \frac{\sigma\eta(\tau,\rho,\theta)\eta(\sigma,\tau\rho,\theta)\eta(\sigma,\tau,\rho)}{\eta(\sigma\tau,\rho,\theta)\eta(\sigma,\tau,\rho\theta)} \\ &= \frac{\sigma E_k(\tau,\rho)E_k(\sigma,\tau\rho)}{E_k(\sigma\tau,\rho)E_k(\sigma,\tau)} = \partial E_k(\sigma,\tau,\rho). \\ &\qquad\qquad (\eta(\sigma,\tau,\rho) = 1 \text{ and } \chi'(\rho\theta) = k)\end{aligned}$$

Therefore, $E_k \in \mathrm{Z}^2(K')$. Let $e'_k \in \mathrm{C}^2(K')$ be defined as $e'_k(\sigma) \coloneqq \varepsilon'(\sigma,k)$. For $\sigma,\tau \in G_{K'}$,

$$E_k(\sigma,\tau) = \eta(\sigma,\tau,k) = \frac{\sigma\varepsilon'(\tau,k)\varepsilon'(\sigma,k)}{\varepsilon'(\sigma\tau,k)\varepsilon'(\sigma,0)} = \frac{\sigma e'_k(\tau,k)e'_k(\sigma,k)}{e'_k(\sigma\tau,k)} = \partial e'_k(\sigma,\tau).$$

Therefore, E_k represents the trivial class in $\mathrm{Br}(K')$. □

Note that E_k can be viewed as inflation of an element in $\mathrm{Br}(F/K')$. Therefore, there is $e_k \in \mathrm{C}^1(F/K')$ such that $\partial e_k = E_k$. Explicitly, E_k is given by

$$E_k(\sigma,\tau) \coloneqq (2\sqrt{A})^{-kn}, \qquad \chi(\sigma) = i,\ \chi(\tau) = j,\ n = [(i+j)/l].$$

Since $E_k = kE_1$, we can assume $e_k = ke_1$. Let $\sigma_0 \in \mathrm{Gal}(F/K')$ be the generator of $\mathrm{Gal}(F/K')$ such that $\chi(\sigma_0) = 1$. The triviality of E_1 implies that there is $c \in K^\times$ such that $2\sqrt{A} = \mathrm{N}_{K/L}(c)$. Hence, we choose e_1 to be given by

$$e_1(\sigma) \coloneqq \begin{cases} 1, & \text{if} \quad \chi(\sigma) = 0, \\ \prod_{m=0}^{i-1} \sigma_0^m(1/c), & \text{if } \chi(\sigma) = i,\ i \geq 1. \end{cases}$$

Identifying $\mathrm{Gal}(F/L)$ with $\mathrm{Gal}(K/L) \times \mathrm{Gal}(K'/L)$, for each $0 \leq m, k \leq l-1$, we can define $f_{m,k} \in \mathrm{C}^1(K')$ as $f_{m,k}(\sigma) \coloneqq \eta(\sigma, 0, m, k)$ and

$$F_{m,k} \coloneqq f_{m,k} + e_k + e_m - e_{(m+k) \mod l}.$$

If $\sigma, \tau \in G_{K'}$ and $\rho, \theta \in G_L$ are such that $\chi(\rho) = 0$, $\chi'(\rho) = m$, and $\chi'(\theta) = k$, then

$$\begin{aligned} 1 = \partial\eta(\sigma,\tau,\rho,\theta) &= \frac{\sigma\eta(\tau,\rho,\theta)\eta(\sigma,\tau\rho,\theta)\eta(\sigma,\tau,\rho)}{\eta(\sigma\tau,\rho,\theta)\eta(\sigma,\tau,\rho\theta)} \\ &= \frac{\sigma\eta(\tau,0,m,k)\eta(\sigma,\tau,m,k)\eta(\sigma,\tau,0,m)}{\eta(\sigma\tau,0,m,k)\eta(\sigma,\tau,0,(m+k) \mod l)} \\ &= \frac{\sigma\eta(\tau,0,m,k)\eta(\sigma,\tau,0,k)\eta(\sigma,0,m,k)\eta(\sigma,\tau,0,m)}{\eta(\sigma\tau,0,m,k)\eta(\sigma,\tau,0,(m+k) \mod l)} \\ &\qquad \text{(by Remark 5.1.1)} \\ &= \frac{\sigma f_{m,k}(\tau) f_{m,k}(\sigma) E_k(\sigma,\tau) E_m(\sigma,\tau)}{f_{m,k}(\sigma\tau) E_{(m+k) \mod l}(\sigma,\tau)} = \partial F_{m,k}(\sigma,\tau). \end{aligned}$$

This implies that $F_{m,k} \in \mathrm{Z}^1(K')$. Since $F_{m,k}$ takes values in $K^\times$ and factors through $\mathrm{Gal}(F/K') \simeq \mathrm{Gal}(K/L)$, we can view $F_{m,k}$ as image of an element in $\mathrm{Z}^1(K/L)$ under the inflation map. By Hilbert's Theorem 90 there is a $t_{m,k} \in K^\times$ such that $\partial t_{m,k} = F_{m,k}$. We choose $t_{m,k}$ to be 1 whenever $F_{m,k}$ is the trivial cocycle. By our choice of e_k, and the fact that $f_{m,k}(\sigma) = (2\sqrt{A})^{[(m+k)/l]\chi(\sigma)}$,

$$F_{m,k}(\sigma) = f_{m,k}(\sigma) e_1(\sigma)^{[(m+k)/l]} = \left((2\sqrt{A})^{\chi(\sigma)} e_1^l(\sigma)\right)^{[(m+k)/l]}.$$

If $m + k \geq l$, then $F_{m,k}(\sigma) = (2\sqrt{A})^{\chi(\sigma)} e_1^l(\sigma)$ and otherwise $F_{m,k}(\sigma) = 1$. We choose $t_{m,k} = t$ if $m + k \geq l$, where t is such that $\partial t(\sigma) = (2\sqrt{A})^{\chi(\sigma)} e_1^l(\sigma)$. In other words, $t_{m,k}$ can be chosen to be $t^{[(m+k)/l]}$, for $0 \leq m, k \leq l-1$. Using the following proposition one can explicitly write t.

Proposition 5.1.5. *Let $0 \leq m, k \leq l-1$ be such that $m + k \geq l$, and σ_0 be the generator of $\mathrm{Gal}(K/L)$ such that $\chi(\sigma_0) = 1$. Then $F_{m,k}(\sigma) = (2\sqrt{A})^{\chi(\sigma)} e_1^l(\sigma)$, and we can choose t such that $\partial t = F_{m,k}$ as $t \coloneqq \prod_{i=0}^{l-2} \sigma_0^i(c^{l-1-i})$.*

Proof.

$$\begin{aligned}\sigma_0(t) &= \prod_{i=1}^{l-1} \sigma_0^i(c^{l-i}) = \mathrm{N}(c)t/c^l \\ &= \frac{2\sqrt{A}}{c^l}t = 2\sqrt{A}e_1^l(\sigma_0)t.\end{aligned}$$

□

In view of the above, define

$$\varepsilon(\tau,\rho) \coloneqq t_{m,k}e_k(\tau) = t^{[(m+k)/l]}e_1^k(\tau), \qquad \chi'(\tau) = m,\ \chi'(\rho) = k,\ 0 \le m,k \le l-1. \tag{5.1.3}$$

Then $\varepsilon(\tau,\rho)$ depends on $\chi(\tau)$, $\chi'(\tau)$ and $\chi'(\rho)$ and therefore, we will interchangeably use $\varepsilon(\chi(\tau),\chi'(\tau),\chi'(\rho))$ with $\varepsilon(\tau,\rho)$. The following proposition shows that $\partial\varepsilon = \eta$.

Proposition 5.1.6. *We have $\partial\varepsilon = \eta$.*

Proof. Note that $\partial\varepsilon(\sigma,\tau,\rho)$ depends only on $\chi(\sigma),\chi'(\sigma),\chi(\tau),\chi'(\tau),\chi'(\rho)$. Assume that $\chi'(\sigma) = n$, $\chi'(\tau) = m$ and $\chi'(\rho) = k$ with $0 \le n,m,k \le l-1$. For simplicity of notations let $\overline{m+k} \coloneqq (m+k) \mod l$. Then

$$\begin{aligned}\partial\varepsilon(\sigma,\tau,\rho) &= \frac{\sigma\varepsilon(\chi(\tau),m,k)\varepsilon(\chi(\sigma),n,\overline{m+k})}{\varepsilon(\chi(\sigma\tau),\overline{m+n},k)\varepsilon(\chi(\sigma),n,m)} = \frac{\sigma(t_{m,k}e_k(\tau))e_{\overline{m+k}}(\sigma)t_{n,\overline{m+k}}}{t_{\overline{m+n},k}e_k(\sigma\tau)e_m(\sigma)t_{n,m}} \\ &= \frac{\sigma(t_{m,k}e_k(\tau))e_1^{\overline{m+k}}(\sigma)t^{[(n+\overline{m+k}/l)]}}{t^{[(\overline{m+n}+k)/l]}e_1^k(\sigma\tau)e_1^m(\sigma)t^{[(n+m)/l]}} = \frac{\sigma(t_{m,k}e_k(\tau))e_1^{\overline{m+k}}(\sigma)}{e_1^k(\sigma\tau)e_1^m(\sigma)t^{[(m+k)/l]}} \\ &= F_{m,k}(\sigma)\frac{\sigma e_k(\tau)e_{\overline{m+k}}(\sigma)}{e_k(\sigma\tau)e_m(\sigma)} = \left(\frac{f_{m,k}e_ke_m}{e_{\overline{m+k}}}\right)(\sigma)\frac{\sigma e_k(\tau)e_{\overline{m+k}}(\sigma)}{e_k(\sigma\tau)e_m(\sigma)} \\ &\qquad\qquad \text{(by the definition of } F_{m,k}) \\ &= f_{m,k}(\sigma)E_k(\sigma,\tau) \qquad\qquad (E_k = \partial e_k) \\ &= \eta(\chi(\sigma),0,m,k)\eta(\chi(\sigma),\chi(\tau),0,k) = \eta(\chi(\sigma),\chi(\tau),m,k) = \eta(\sigma,\tau,\rho).\end{aligned}$$

The second to last equality follows from Remark 5.1.1. □

Remark 5.1.7. One can generalize the above computation to the Selmer group of any isogeny on a Jacobian with cyclic kernel. Note that we will need to generalize the argument from Proposition 5.1.2 and Lemma 5.1.3. This can be done by using an argument similar to Proposition 6.1.3.

Remark 5.1.8. The methods used in this section along with the ones from §4.3.1 can be generalized to compute the global step of the CTP for the case of λ-Selmer group on Jacobian of any degree l-cyclic cover C of $\mathbb{P}^1$ such that the covering map $\pi : C \to \mathbb{P}^1$ is ramified at ∞. See §7.1.1 for more.

5.2 Local computation

Let v be a place of L, and fix an embedding $\overline{L} \hookrightarrow \overline{L_v}$. Let K_v be the completion of the image of K inside $\overline{L_v}$ under the above embedding. Since α is locally everywhere trivial, there exists a $\beta_v \in J_A(\overline{L_v})$ such that $\partial\beta_v = \alpha_v$. In particular, for all $\sigma \in G_{L_v}$ such that $\chi(\sigma) = 0$, $\sigma\beta_v - \beta_v = \alpha_v(\sigma) = 0$. Therefore, $\beta_v \in J_A(K_v)$. Since $C_A(k) \neq \emptyset$, by Proposition 1.2.13, there is a divisor D_{β_v} of minimal degree such that D_{β_v} is defined over K_v and $[D_{\beta_v} - \deg(D_{\beta_v})(T_0)] = \beta_v$. One can augment D_{β_v} by adding a multiple of (T_0) to ensure that $\deg(D_{\beta_v}) = (l-1)/2$, which we assume from now on.

Let $D_{\beta_v} \coloneqq \sum_{i=1}^{(l-1)/2} (P_{iv})$, where $P_{iv} \coloneqq (x_{iv}, y_{iv}) \in C_A(\overline{L_v})$, for $1 \leq i \leq (l-1)/2$. Choose $\mathfrak{b}_v \coloneqq D_{\beta_v} - \frac{l-1}{2}(T_0)$ as a lift of β_v to $\mathrm{Div}^0((C_A)_{\overline{k}})$. We have $\mathfrak{a}_v - \partial\mathfrak{b}_v \in \mathrm{C}^1(G_{L_v}, \mathrm{Princ}((C_A)_{\overline{k}}))$ given by

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi(\sigma) = 0, \\ i(P) + \sum_{n=1}^{l} ((P_{nv}) - (\sigma P_{nv})) - i(T_0) = \mathrm{div}(f_i), & \text{if } \chi(\sigma) = i. \end{cases} \tag{5.2.1}$$

where $f_i \in \bar{L}(C_A)$. We have

$$((\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v)(\sigma, \tau) = \begin{cases} 1 & \text{if } \chi(\sigma) = 0 \text{ or } \chi'(\tau) = 0, \\ \langle f_i, (P) - (T_0)\rangle_1^j & \text{if } \chi(\sigma) = i \text{ and } \chi'(\tau) = j. \end{cases}$$

Note that for $\sigma \in G_{L_v}$, $\sigma P = P$. Therefore, if $\mathrm{Gal}(K_v/L_v)$ is generated by σ_0, then $\sigma_0 \,\mathrm{div}(f_i) = i(P) + \sum_{n=1}^{(l-1)/2} ((\sigma_0 P_{nv}) - (\sigma_0^{n+1} P_{nv})) - i(T_0)$, and $\mathrm{div}(f_{i+1}) - \mathrm{div}(\sigma_0 f_i) = \mathrm{div}(f_1)$. Therefore, we can choose f_i to be $\prod_{n=0}^{i-1} \sigma_0^n f_1$. Recall that $\langle \cdot, \cdot \rangle_1$ is well defined up to the scaling of f_i by a constant. Similarly,

$$(\mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v)(\sigma, \tau) = \left(\prod_{i=1}^{(l-1)/2} (y_{iv} - \sqrt{A}) \right)^{n'},$$

where $\chi'(\sigma) = i$, $\chi'(\tau) = j$, and $n' = [(i+j)/l]$. Therefore, $\gamma_v \coloneqq ((\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \varepsilon_v)(\sigma, \tau)$ depends only on $\chi(\sigma)$, $\chi'(\sigma)$ and $\chi'(\tau)$. Hence, we will use $\gamma_v(\chi(\sigma), \chi'(\sigma), \chi'(\tau))$ interchangeably with $\gamma_v(\sigma, \tau)$.

If for all z, $d \not\equiv d'^z \mod (L_v^\times)^l$, then define for each $0 \leq k \leq l-1$ a 1-cochain $G_k \in \mathrm{C}^1(K'_v)$ by $G_k(\sigma) \coloneqq \gamma_v(\chi(\sigma), 0, k)$. Noting that $\varepsilon_v(\chi(\sigma), 0, k) = e_1^k(\chi(\sigma))$ we have $G_k = kG_1$. The abuse of notation (G_k as a 1-cocycle and G_k as the absolute Galois group of k) must be noted here. However, the use will be clear from the context. The following proposition shows that G_1 is a 1-cocycle and so is G_k.

Proposition 5.2.1. *Let G_1, γ_v be as above. Then $G_1 \in \mathrm{Z}^1(K'_v)$ and there is a $g \in K_v^\times$ such that $\partial g = G_1$.*

Proof. Note that γ_v takes values in $K_v^\times$ and can be viewed as the inflation of an element in $\mathrm{Z}^2(F_v/L_v)$. Using the isomorphism $\mathrm{Gal}(F_v/K'_v) \simeq \mathrm{Gal}(K_v/L_v)$ we can view G_1 as inflation of an element in $\mathrm{C}^1(K_v/L_v)$. If G_1 is a 1-cocycle, then Hilbert's Theorem 90 implies the existence of g.

Now we show that $G_1 \in \mathrm{Z}^1(K'_v)$. Using that γ_v is a 2-cocycle, for $\sigma, \tau \in G_{K'_v}$,

$$1 = \partial\gamma_v(\sigma,\tau,1) = \frac{\sigma\gamma_v(\tau,1)\gamma_v(\sigma,1)}{\gamma_v(\sigma\tau,1)\gamma_v(\sigma,\tau)} = \partial G_1(\sigma,\tau).$$

□

Therefore, for $0 \le k \le l-1$, $G_k(\sigma) = \langle f_i, (P)-(T_0)\rangle_1^k / e_k(\sigma)$, where $\chi(\sigma) = i$. It is easy to check that $\gamma_v(\sigma,\tau) = G_k(\sigma)$ when $\chi'(\tau) = k$ and $\chi'(\sigma) + \chi'(\tau) < l$. Now consider the 1-cochain ξ defined by $\xi(\sigma) = g^k$, if $\chi'(\sigma) = k$. It is easy to see that $\partial\xi(\tau,\rho)$ only depends on $\chi(\tau)$, $\chi'(\tau)$ and $\chi'(\rho)$; hence, we will interchangeably use $\partial\xi(\chi(\tau),\chi'(\tau),\chi'(\rho))$ with $\partial\xi(\tau,\rho)$. Let σ, $\tau \in G_{L_v}$ be such that $\chi(\sigma) = i$, $\chi'(\sigma) = j$, and $\chi'(\tau) = k$. Then

$$\partial\xi(\sigma,\tau) = \frac{\sigma\xi(\chi'(\tau))\xi(\chi'(\sigma))}{\xi(\chi'(\sigma\tau))} = \frac{\sigma\xi(j)\xi(k)}{\xi(\overline{j+k})} = \frac{\sigma(g)^k g^j}{g^{\overline{j+k}}} = G_1^k(\sigma)\frac{g^{j+k}}{g^{\overline{j+k}}}$$

If $j+k < l$, then $(\gamma_v - \partial\xi)(i,j,k) = 1$. Otherwise, $(\gamma_v - \partial\xi)(i,j,k) = \delta_v$, with

$$\begin{aligned}\delta_v &:= \frac{1}{c^l t \prod_{n=1}^{(l-1)/2}(y(P_{nv}) - \sqrt{A})} = \frac{\prod_{i=0}^{l-1} G_1(\sigma_0^i)}{\mathrm{N}(g)t \prod_{n=1}^{(l-1)/2}(y(P_{nv}) - \sqrt{A})} \\ &= \frac{\prod_{i=1}^{l-1}\prod_{m=0}^{i-1}\sigma_0^m(F_1 c)}{\mathrm{N}(g)t \prod_{n=1}^{(l-1)/2}(y(P_{nv}) - \sqrt{A})},\end{aligned}$$

where $F_1 := \langle f_1, (P)-(T_0)\rangle_1$ and $\mathrm{N} : K_v^\times \to L_v^\times$ is the norm map. Since $\gamma_v - \partial\xi$ is a 2-cocycle, one can easily check that $\delta_v \in L_v^\times$ by evaluating $\partial(\gamma_v - \partial\xi)$ at $(1, l-1, 1)$.

Therefore, $\zeta_l^{\mathrm{inv}_v([\gamma_v])} = (\delta_v, d')_v$, where $(\cdot,\cdot)_v$ represents the generalized Hilbert symbol of order l defined using the pairing in Diagram 1.3.7.

On the other hand, if $K_v = K'_v$, then one can view γ_v as the inflation of an element in $\mathrm{Z}^2(K'_v/L_v)$; hence, we will interchangeably use $\gamma_v(\sigma,\tau)$ with $\gamma_v(\chi'(\sigma),\chi'(\tau))$. The following proposition computes $\mathrm{inv}_v([\gamma_v])$ for this case.

Proposition 5.2.2. *Let γ_v be as above, and let $\xi \in \mathrm{C}^1(K'/k)$ be defined by*

$$\xi(\tau) \coloneqq \begin{cases} 1, & \text{if} \quad \chi'(\tau) = 0, \\ \prod_{n=0}^{i-1} \gamma_v(n,1), & \text{if } \chi'(\tau) = i,\ 1 \le i \le l-1. \end{cases}$$

Then $\partial\xi(\tau,\rho)$ only depends on $\chi'(\tau)$ and $\chi'(\rho)$, and

$$(\gamma_v - \partial\xi)(\tau,\rho) = \begin{cases} 1, & \text{if } \chi'(\tau) = i,\ \chi'(\rho) = j,\ i+j < l, \\ \delta_v \coloneqq \prod_{n=0}^{l-1} \gamma_v(n,1) \in L_v^\times, & \text{otherwise,} \end{cases}$$

where $0 \le i, j \le l-1$. Hence, $\zeta_l^{\mathrm{linv}_v([\gamma_v])} = (\delta_v, d')_v$, where $(\cdot,\cdot)_v$ denotes the generalized Hilbert symbol of order l and $[\gamma_v]$ is the class of γ_v in $\mathrm{Br}(L_v)$.

Proof. Let $\tau, \rho \in G_{L_v}$ be such that $\chi'(\tau) = i$ and $\chi'(\rho) = j$. One can check that the proposition holds if i or j is 0. If $0 < i + j < l$, then

$$\begin{aligned} \frac{\gamma_v(\tau,\rho)\xi(\overline{i+j})}{\sigma\xi(j)\xi(i)} &= \frac{\gamma_v(i,j)\prod_{n=0}^{j-1}\sigma\gamma_v(n,1)\prod_{n=0}^{i-1}\gamma_v(n,1)}{\prod_{n=0}^{i+j-1}\gamma_v(n,1)} \\ &= \gamma_v(i,j)\prod_{n=0}^{j-1}\frac{\gamma_v(\overline{n+i},1)\gamma_v(i,n)}{\gamma_v(i,\overline{n+1})}\frac{1}{\prod_{n=i}^{j+i-1}\gamma_v(n,1)} = 1. \end{aligned}$$

(γ_v is a 2-cocycle)

If $i + j \ge l$, then

$$\begin{aligned} \frac{\gamma_v(\tau,\rho)\xi(\overline{i+j})}{\sigma\xi(j)\xi(i)} &= \frac{\gamma_v(i,j)\prod_{n=0}^{j-1}\sigma\gamma_v(n,1)\prod_{n=0}^{i-1}\gamma_v(n,1)}{\prod_{n=0}^{i+j-l-1}\gamma_v(n,1)} \\ &= \gamma_v(i,j)\prod_{n=0}^{j-1}\frac{\gamma_v(\overline{n+i},1)\gamma_v(i,n)}{\gamma_v(i,\overline{n+1})}\frac{\prod_{n=0}^{i-1}\gamma_v(n,1)}{\prod_{n=0}^{j+i-l-1}\gamma_v(n,1)} \\ &= \frac{\prod_{n=0}^{i-1}\gamma_v(n,1)\prod_{n=i}^{j+i-1}\gamma_v(n,1)}{\prod_{n=0}^{j+i-l-1}\gamma_v(n,1)} = \prod_{n=0}^{l-1}\gamma_v(n,1). \end{aligned}$$

This finishes the proof. □

We have

$$\gamma(\sigma,1)=\frac{\langle f_i,(P)-(T_0)\rangle_1}{e_1(i)\left(t\prod\limits_{j=1}^{(l-1)/2}(y(P_{jv}-\sqrt{A}))\right)^{[(n+1)/l]}},$$

where $\chi(\sigma)=i$ and $\chi'(\sigma)=n$. Therefore,

$$\prod_{n=0}^{l-1}\gamma_v(n,1)=\frac{\prod\limits_{i=1}^{l-1}\prod\limits_{m=0}^{i-1}\sigma_0(F_1c)}{t\prod\limits_{j=1}^{(l-1)/2}(y(P_{jv})-\sqrt{A})},$$

If we choose $g=1$ (because $G_1=0$) in the case when $K_v=K_v'$, then in both the cases, i.e., whether or not $K_v=K_v'$, the expression for δ_v is same. Furthermore, $\delta_v=\Delta_v\delta_{\text{glob}}$ whenever $K_v,K_v'\neq L_v$, where

$$\delta_{\text{glob}}\coloneqq\frac{\prod\limits_{i=1}^{l-1}\prod\limits_{m=0}^{i-1}\sigma_0^m(c)}{t}\qquad\text{and}\qquad\Delta_v\coloneqq\frac{\prod\limits_{i=1}^{l-1}\prod\limits_{m=0}^{i-1}\sigma_0^m(F_1)}{\mathrm{N}_{K_v/L_v}(g)\prod\limits_{j=1}^{(l-1)/2}(y_{jv}-\sqrt{A})}.\tag{5.2.2}$$

In view of the above, we have the following proposition.

Proposition 5.2.3. *The quantity δ_{glob} is in $L^\times$. Therefore, $\Delta_v\in L_v^\times$.*

Proof. We have

$$\sigma_0(\delta_{\text{glob}})=\frac{\prod\limits_{i=1}^{l-1}\prod\limits_{m=1}^{i}\sigma_0^m(c)}{\sigma_0(t)}=\frac{c^l\prod\limits_{i=1}^{l-1}\prod\limits_{m=1}^{i}\sigma_0(c)}{2\sqrt{A}t}=\delta_{\text{glob}},$$

where the last equality follows from $\mathrm{N}_{K/L}(c)=2\sqrt{A}$. □

Remark 5.2.4. If we choose t to be as in the Proposition 5.1.5, then $\delta_{\text{glob}}=1$ and the above proposition trivially follows. Furthermore, we will in practice choose t to be like this because this way we avoid local computation at any new places other than those having a non-trivial valuation at c or above primes dividing $2lA$. In the case when $K_v=L_v$ we can choose β_v as 0 on J_A, and we obtain $\delta_v=1/t$. If $K_v'=L_v$, then $(\delta_v,d')_{L_v}=1$.

We now obtain an expression for F_1. Let $C_1\coloneqq y-\sum\limits_{i=0}^{g}m_ix^i$ be such that

$$(P)-(l)(T_0)+\sum_{i=1}^{g}(P_{iv})+\sum_{i=1}^{g}(\iota(P_{iv}))=\mathrm{div}(C_1).$$

Since $(0, \sqrt{A}) \in \mathrm{Supp}(\mathrm{div}(C_1))$, $m_0 = \sqrt{A}$. Therefore, f_1 can be chosen to be $C_1/\prod_{i=1}^{g}(x - x_{iv})$. We have $F_1 = \frac{(-1)^{g+1}m_1}{\prod_{i=1}^{g}\sigma_0(x_{iv})}$. Now using that 0 and $\sigma_0(x_{iv}), x_{iv}$ for $1 \leq i \leq g$ are the solutions to the equation $(\sum_{i=0}^{g} m_i x^i)^2 = x^l + A$, $\prod_{i=1}^{g}\sigma_0(x_{iv}) = -2\sqrt{A}m_1/\prod_{i=1}^{g} x_{iv}$. Therefore, $F_1 = (-1)^g \frac{\prod_{i=1}^{g} x_{iv}}{2\sqrt{A}}$.

5.3 The prime bound

Recall that $\mathrm{S}^{(\lambda)}(J_A/k) \subset \mathrm{H}^1(G_L, J_A[\lambda]; S)$, where S is the set of primes in L above primes dividing $2lA$. Therefore, for $d \in \mathrm{S}^{(\lambda)}(J_A/k)$ and any place $v \notin S$, $v_v(d) \equiv 0 \bmod l$ and $L_v(\sqrt[l]{d})$ is the unramified extension of degree 1 or l. Hence, we have the following proposition.

Proposition 5.3.1. *Let $d \in \mathrm{S}^{(\lambda)}(J_A/k)$ and $v \notin S$ be a place of L, such that $K_v \neq L_v$. Then we have $L_v(\sqrt[l]{\Delta_v})$ is unramified.*

Proof. All we need to show is $l | v_v(\Delta_v)$. Note that $x \in \mathscr{O}_{K_v}^{\times} \iff \mathrm{N}_{K_v/L_v}(x) \in \mathscr{O}_{L_v}^{\times}$. We have

$$\mathrm{N}_{K_v/L_v}(F_1) = \langle \sum_{i=0}^{l-1} \mathrm{div}\, \sigma_0^i(f_1), (P) - (T_0)\rangle_1 = \langle \mathrm{div}(y - \sqrt{A}), (P) - (T_0)\rangle_1 = \frac{1}{2\sqrt{A}}.$$

Therefore, $F_1 \in \mathscr{O}_{K_v}^{\times}$. In what follows, we assume that the points (x_{iv}, y_{iv}) are defined over K_v for each i. One can use arguments similar to the ones in the proof of Lemma 4.3.19 to reduce to this case by analyzing the orbits of the set $\{P_{1v}, \ldots, P_{(l-1)/2v}\}$. Let $\mathrm{ord}_v(x_{iv}) = k_i$. Then $\mathrm{ord}_v(y_{iv} - \sqrt{A}) = \mathrm{ord}_v(y_{iv} + \sqrt{A}) = k_i l/2$, if $k_i < 0$ and either $\mathrm{ord}_v(y_{iv} - \sqrt{A})$ or $\mathrm{ord}_v(y_{iv} + \sqrt{A})$ is $k_i l$, if $k_i \geq 0$. In either case, $\mathrm{ord}_v(y_{iv} - \sqrt{A}) \equiv 0 \bmod l$. Since K_v is unramified above L_v, we can choose the uniformizers for K_v and L_v to be the same and therefore, $L_v(\sqrt[l]{\Delta_v})$ is unramified. □

As a consequence of the above, we obtain the following corollary.

Corollary 5.3.2. *Let $a, a' \in \mathrm{S}^{(\lambda)}(J_A/k)$ be represented by $d, d' \in L^{\times}$ and S be the set of places of L above $2lA$. Then*

$$\zeta_l^{l\langle a, a'\rangle_{\mathrm{CT}}} = \prod_{v \in S} (\delta_v, d')_{L_v} \prod_{v \notin S} (\pi_v^{\mathrm{ord}_v(t)}, d'^{-1})_{L_v}.$$

Moreover, if A lies in the l-Stoll set, then

$$\zeta_l^{l\langle a, a'\rangle_{\mathrm{CT}}} = (\delta_\lambda, d')_{L_\lambda} \prod_{v \neq \lambda} (\pi_v^{\mathrm{ord}_v(t)}, d'^{-1})_{L_v}.$$

Proof. The only places we need to care about are $v \notin S$. If v is split in K, then $K_v = L_v$ and Remark 5.2.4 implies that $(\delta_v, d')_{L_v} = (1/t, d')_{L_v}$. If v is inert in K, then Proposition 5.3.1 implies that $(\delta_v, d')_{L_v} = (\delta_{\text{glob}}, d')_{L_v}$ and $\text{ord}_v(\delta_{\text{glob}}) = \text{ord}_v(1/t) + l(l-1)\text{ord}_v(c)/2 \equiv \text{ord}_v(1/t) \mod l$. □

Remark 5.3.3. In particular, if we choose t to be as in Proposition 5.1.5, then $\delta_{\text{glob}} = 1$, for a place $v \notin S$ of L that remains inert in K. The above corollary can be refined as

$$\zeta_l^{l\langle a,a'\rangle_{\text{CT}}} = \prod_{v\in S}(\delta_v, d')_{L_v} \prod_{\substack{v\notin S \\ v \text{ splits in } K}} (\pi_v^{\text{ord}_v(t)}, d'^{-1})_{L_v}.$$

In order to compute Δ_v, we require to compute the local point $\beta_v \in J_A(K_v)$. Vishal Arul in [Aru20] has given an algorithm to divide a point in the image of C_A in J_A by $(1-\zeta_l)$. If $Q_v := \sum_{i=1}^{n} Q_{iv}$, for $n \leq g$, is a divisor representing the local point on $J_A(k_v)$ such that Q_v maps to the λ-Selmer element a under the connecting morphism, then on can use Arul's algorithm to compute $P'_{iv} \in J_A(\overline{L_v})$ such that $(1-\zeta_l)P'_{iv} = Q_{iv}$ and use this to obtain the value for Δ_v. However, if A lies in the l-Stoll set, then in [Sto98, §6] it has been explicitly shown that the curve spans the local image at λ; hence, using the corresponding elements of the λ-Selmer group one can compute the inverse image under λ-isogeny using Arul's algorithm.

5.4 Algorithm

In this section we give pseudocode of an algorithm for computing the CTP between two elements $a, a' \in \text{Ш}^{(\lambda)}(J_A/k)$ represented by $d, d' \in L^\times$, respectively. Let

$$S_{a,a'} := S \cup \{v \mid v \text{ is a place of } L \text{ below a place } w \text{ of } K \text{ with } \text{ord}_w(c) \neq 0\}.$$

Algorithm 3 Compute the CTP between $a, a' \in \text{Ш}^{(\lambda)}(J_A/k)$ represented by $d, d' \in L^\times$.

Require: $d, d' \in L^\times$.
Ensure: Value of $(\zeta_l)^{\langle a,a'\rangle_{\text{CT}}}$ in variable CT.

1: CT $\leftarrow 1$. ▷ Value of CT.
2: LocalPoints $\leftarrow$ [ ]. ▷ List storing P_v indexed by places of L above primes dividing $2lA$.
3: **for** $v \in$ {places of L above primes dividing $2lA$} **do**
4: Find $Q_v \in J(k_v)$, such that $\delta(Q_v) = \alpha_v$.
5: $K_v \leftarrow L_v(\sqrt[l]{d_v})$, $P_v \leftarrow \frac{1}{\lambda}Q_v$. ▷ Computed using Arul's algorithm.

Adjust P_v via $P_v \mapsto P_v + T$ for some $T \in J[\lambda]$ such that $\partial P_v = \alpha_v$.
LocalPoints$[v] \leftarrow P_v$.
end for
Compute c such that $\mathrm{N}_{L(\sqrt[l]{d})/L}(c) = 2\sqrt{A}$ and t using Proposition 5.1.5.
for $v \in S_{a,a'}$ **do**
  if $v \in \{$places above primes dividing $2lA\}$ **then**
    Compute G_1, g and Δ_v. ▷ Using Proposition 5.2.1 and Equation (5.2.2).
    $\mathrm{CT} = \mathrm{CT} \cdot (\delta_v, d')_{L_v}$.
  else
    $\mathrm{CT} = \mathrm{CT} \cdot (\pi_v^{\mathrm{ord}_v(t)}, d'^{-1})_{L_v}$. ▷ Using Corollary 5.3.2.
  end if
end for
return CT.

In the following section we show that one can avoid the local computation under certain conditions entirely and use that to compute an example.

5.5 A special case of computation

In this section we will discuss a case where one does not need to compute the local point $P_\lambda \in J(K_\lambda)$, such that $\partial P_\lambda = \alpha_\lambda$, i.e.,the global computation is enough to compute the local values. We will need the following explicit version of trivializing a 3-cocycle in $\mathrm{Z}^3(G, M)$, for a cyclic group G and a G-module M, given that $\mathrm{H}^1(G, M) = 0$.

Proposition 5.5.1. *Let $\langle g \rangle = G$ be a cyclic group of order N and $\gamma \in \mathrm{Z}^3(G, M)$. Recall that every odd-dimensional cocycle is normalized by definition. Assume that $\mathrm{H}^1(G, M) = 0$. Then the theory of Tate cohomology for cyclic groups implies that $\mathrm{H}^3(G, M) = 0$ (Proposition 1.3.14), and there is a $\theta \in \mathrm{C}^2(G, M)$ such that $\partial\theta = \gamma$. One such θ can be obtained as follows. Let $c_g \in M$ be such that $\partial c_g = \sum_{j=0}^{N-1} \gamma(g, g^j, g)$ and*

$$\theta(g^i, g^j) := nc_g + \sum_{k=0}^{j-1} \gamma(g^i, g^k, g),$$

where $0 \leq i, j \leq N-1$ and $n := \left[\frac{i+j}{N}\right] \in \{0, 1\}$. Then $\partial\theta = \gamma$.

Proof. We first show that a c_g satisfying the hypothesis of the proposition exists. Consider the 1-cochain $f_g : \langle g \rangle \to M$ defined by $f_g(g^i) := \sum_{j=0}^{N-1} \gamma(g^i, g^j, g)$. Now we

have

$$\begin{aligned} g^k(f_g(g^i)) &= \sum_{j=0}^{N-1} g^k\gamma(g^i,g^j,g) \\ &= \sum_{j=0}^{N-1} \big(\gamma(g^{i+k},g^j,g)+\gamma(g^k,g^i,g^{j+1})-\gamma(g^k,g^{i+j},g)-\gamma(g^k,g^i,g^j)\big) \\ &= f_g(g^{i+k})-f_g(g^k)+\sum_{j=0}^{N-1}\big(\gamma(g^k,g^i,g^{j+1})-\gamma(g^k,g^i,g^j)\big) \\ &= f_g(g^{i+k})-f_g(g^k) \end{aligned}$$

This implies that f_g is a 1-cocycle and there is a $c_g \in M$ such that $f_g(g^i) = g^i c_g - c_g$.

Note that

$$\partial\theta(g^i,g^j,g^k) = g^i(\theta(g^j,g^k)) + \theta(g^i,g^{j+k}) - \theta(g^{i+j},g^k) - \theta(g^i,g^j).$$

We divide the proof into 4 cases depending on the possible values of $[(j+k)/N]$ and $[(i+j)/N]$.

Case 1: $j+k<N$ and $i+j<N$.

$$\begin{aligned} \partial\theta(g^i,g^j,g^k) &= \left[\frac{i+j+k}{N}\right]c_g + \left(\sum_{n=0}^{k-1} g^i\gamma(g^j,g^n,g)\right) + \left(\sum_{n=0}^{j+k-1}\gamma(g^i,g^n,g)\right) \\ &\quad - \left[\frac{i+j+k}{N}\right]c_g - \left(\sum_{n=0}^{k-1}\gamma(g^{i+j},g^n,g)\right) - \left(\sum_{n=0}^{j-1}\gamma(g^i,g^n,g)\right) \\ &= \sum_{n=0}^{k-1}\big(\gamma(g^{i+j},g^n,g)+\gamma(g^i,g^j,g^{n+1})-\gamma(g^i,g^{j+n},g)-\gamma(g^i,g^j,g^n)\big) \\ &\quad + \sum_{n=0}^{j+k-1}\gamma(g^i,g^n,g) - \left(\sum_{n=0}^{k-1}\gamma(g^{i+j},g^n,g)\right) - \left(\sum_{n=0}^{j-1}\gamma(g^i,g^n,g)\right) \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\gamma \text{ is a 3-cocycle}) \\ &= \gamma(g^i,g^j,g^k) + \sum_{n=0}^{j+k-1}\gamma(g^i,g^n,g) - \left(\sum_{n=0}^{k-1}\gamma(g^i,g^{j+n},g)\right) \\ &\quad - \left(\sum_{n=0}^{j-1}\gamma(g^i,g^n,g)\right) = \gamma(g^i,g^j,g^k). \end{aligned}$$

Case 2: $j+k<N$ and $i+j\geq N$.

In this case we have $g^{i+j} = g^{i+j-N}$ and $i+j-N+k<N$ as $j+k<N$ and

$i + j + k \geq N$. Therefore,

$$\partial\theta(g^i, g^j, g^k) = c_g + \sum_{n=0}^{k-1} g^i\gamma(g^j, g^n, g) + \sum_{n=0}^{j+k-1} \gamma(g^i, g^n, g) - c_g - \left(\sum_{n=0}^{k-1} \gamma(g^{i+j}, g^n, g)\right) - \left(\sum_{n=0}^{j-1} \gamma(g^i, g^n, g)\right),$$

which is the same as the computation in the previous case.

Case 3: $j + k \geq N$ and $i + j < N$.
Once again we have $i + j + k \geq N$ and $i + j + k - N < N$. Therefore,

$$\begin{aligned}
\partial\theta(g^i, g^j, g^k) &= (g^i c_g - c_g) + \sum_{n=0}^{k-1} g^i\gamma(g^j, g^n, g) + \sum_{n=0}^{j+k-N-1} \gamma(g^i, g^n, g) \\
&\quad - \left(\sum_{n=0}^{k-1} \gamma(g^{i+j}, g^n, g)\right) - \left(\sum_{n=0}^{j-1} \gamma(g^i, g^n, g)\right) \\
&= \sum_{n=0}^{N-1} \gamma(g^i, g^n, g) + \sum_{n=0}^{k-1} (\gamma(g^{i+j}, g^n, g) + \gamma(g^i, g^j, g^{n+1}) - \gamma(g^i, g^{j+n}, g) \\
&\quad - \gamma(g^i, g^j, g^n)) + \sum_{n=0}^{j+k-N-1} \gamma(g^i, g^n, g) - \left(\sum_{n=0}^{k-1} \gamma(g^{i+j}, g^n, g)\right) \\
&\quad - \left(\sum_{n=0}^{j-1} \gamma(g^i, g^n, g)\right) \qquad (f_g(g^i) = g^i c_g - c_g) \\
&= \gamma(g^i, g^j, g^k) + \sum_{n=j}^{N-1} \gamma(g^i, g^n, g) + \sum_{n=0}^{j+k-N-1} \gamma(g^i, g^n, g) - \sum_{n=0}^{k-1} \gamma(g^i, g^{j+n}, g) \\
&= \gamma(g^i, g^j, g^k) + \sum_{n=j}^{N-1} \gamma(g^i, g^n, g) + \sum_{n=N}^{j+k-1} \gamma(g^i, g^n, g) - \sum_{n=0}^{k-1} \gamma(g^i, g^{j+n}, g) \\
&= \gamma(g^i, g^j, g^k).
\end{aligned}$$

Case 4: $j + k \geq N$ and $i + j \geq N$.
In this case we get

$$\partial\theta(g^i, g^j, g^k) = (g^i c_g - c_g) + \sum_{n=0}^{k-1} g^i\gamma(g^j, g^n, g) + \sum_{n=0}^{j+k-N-1} \gamma(g^i, g^n, g) - \left(\sum_{n=0}^{k-1} \gamma(g^{i+j}, g^n, g)\right) - \left(\sum_{n=0}^{j-1} \gamma(g^i, g^n, g)\right).$$

Hence, the computation in this case is the same as in the previous case. □

We make the following assumption.

Assumption 5.5.2. *Let d, d' representing Selmer group elements a and a', respectively, be such that $d_\lambda = d'_\lambda u_\lambda^l$, for some $u_\lambda \in L_\lambda^\times$; i.e., $d/d' \in U := \ker(\mathrm{S}^{(\lambda)}(J/k) \to L_\lambda^\times/(L_\lambda^\times)^l)$.*

In this regard, we have the following proposition.

Proposition 5.5.3. *Assume that d and d' satisfy Assumption 5.5.2, and A lies in the l-Stoll set. Then $(\delta_\lambda, d')_{L_\lambda} = (\delta_{\mathrm{glob}}, d')_{L_\lambda}$.*

Proof. Since the pairing is alternating on the l-part of $Ш(J_A/k)$, we have $\zeta_l^{l\langle d,d\rangle_{\mathrm{CT}}} = \prod_v (\delta_v, d)_{L_v} = 0$. Since A lies in the l-Stoll set, Corollary 5.3.2 implies that the only place we need to compute the local point β_v is λ. If $d' = d$, then one finds that η factors through $\mathrm{Gal}(K/L) = \langle\sigma_0\rangle$, which is cyclic. Hence, applying Proposition 5.5.1 to compute ε on η gives us $f_g = 1$. This is because f_g takes values that are powers of $2\sqrt{A} \in \mathcal{O}_L$ which is not a unit. However, values taken by f_g must have norm 1, so $f_g = 1$. This implies that $c_g = 1$ and ε such that $\partial\varepsilon = \eta$ takes values which are powers of $2\sqrt{A}$. Therefore, the valuation of values taken by ε is trivial everywhere other than places above primes of bad reduction. Hence, $\zeta_l^{l\langle d,d\rangle_{\mathrm{CT}}} = (\delta_\lambda, d')_{L_\lambda} = (\delta_\lambda, d)_{L_\lambda} = 1$. Note that $\varepsilon(g^i, g) = \eta(g^i, \mathrm{id}\,, g) = 1$. Hence, $\delta_\lambda = \Delta_\lambda$. This implies that $(\Delta_\lambda, d')_{L_\lambda} = 1$.

Note that the contribution to the value of the CTP at λ when d, d' satisfy the Assumption 5.5.2 is exactly $(\delta_{\mathrm{glob}}, d')_{L_\lambda}$, since Δ_v in this case is the same as the Δ_v in the case when $d = d'$. □

We summarize the computation of the CTP in the following corollary.

Corollary 5.5.4. *Let A be an element of the l-Stoll set, let $d, d' \in \mathrm{S}^{(\lambda)}(J/k)$ satisfy Assumption 5.5.2, and let*

$$S_{d,d'} := \{\textit{places } \mathfrak{p} \textit{ of } L \mid \mathfrak{p} \neq \lambda, \mathrm{ord}_{\mathfrak{q}}(c) \neq 0, \textit{ for some prime } \mathfrak{q} \textit{ of } K \textit{ above } \mathfrak{p}\}.$$

Then

$$\zeta^{l\langle d,d'\rangle_{\mathrm{CT}}} = \prod_{\mathfrak{p}\in S_{d,d'}} (\delta_{\mathrm{glob}} t, d')_{L_\mathfrak{p}}^{-1}.$$

Proof. From Proposition 5.5.3 and Corollary 5.3.2, we have

$$\zeta^{l\langle d,d'\rangle_{\mathrm{CT}}} = \prod_{\mathfrak{p}\neq\lambda} (\delta_{\mathrm{glob}}, d')_{L_\mathfrak{p}}^{-1} \prod_{\mathfrak{p}\neq\lambda} (t, d')_{L_\mathfrak{p}}^{-1} = \prod_{\substack{\mathfrak{p}\neq\lambda \\ \mathfrak{p} \text{ is split in } K/L}} (\delta_{\mathrm{glob}} t, d')_{L_\mathfrak{p}}^{-1}$$
$$= \prod_{\mathfrak{p}\in S_{d,d'}} (\delta_{\mathrm{glob}} t, d')_{L_\mathfrak{p}}^{-1}.$$

□

The above computation implies that if Assumption 5.5.2 is satisfied and A is an element of the l-Stoll set, then one can completely avoid computing at λ. This is helpful because computing Hilbert symbol of order l at λ can be complicated. However, sometimes solving for $\mathrm{N}_{L(\sqrt[l]{d})/L} = 2\sqrt{A}$ is easier if $d \in U$. In this case, one would like to rather compute the Hilbert symbol $(1/t, d')_{L_\lambda}$ and use Remark 5.3.3 as t is not an element of L.

Remark 5.5.5. If A lies in the 3-Stoll set, then we have $\mathrm{rk}_{\mathbb{F}_3}(E_A(k_\lambda)/\lambda E_A(k_\lambda)) = 1$, and therefore Assumption 5.5.2 is always satisfied. Furthermore, [Sto98, Lemma 5.4] implies that $\mathrm{rk}_{\mathbb{F}_l}(U) = \mathrm{rk}_{\mathbb{F}_l}(\ker(\mathrm{N} : \mathrm{Cl}(L)[l] \to \mathrm{Cl}(k)[l]))$.

5.6 Examples

We use the theory from the previous section to compute the CTP for in two cases, firstly where 2-Selmer group computation is enough to obtain the rank, and secondly where it is not.

5.6.1 C_{23}

Let C_{23} be the curve give by the equation

$$y^2 = x^5 + 23.$$

A Selmer group computation shows that $\mathrm{S}^{(\lambda)}(J_{23}/k) \simeq \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^2$ and is generated by $d := (-5\zeta_5^3 - 5\zeta_5^2)\sqrt{23} - 10\zeta_5^3 - 10\zeta_5^2 + 21$ and $d' := (5\zeta_5^3 + 5\zeta_5^2 + 5)\sqrt{23} - 10\zeta_5^3 - 10\zeta_5^2 - 31$ in $L^\times$. One checks that in L_λ, $d_\lambda = (d'_\lambda)^4 \mod (L_\lambda^\times)^5$. We have

$$\begin{aligned}
505c := {} & ((113794\zeta_5^3 - 81381\zeta_5^2 + 120615\zeta_5 - 11033)\sqrt{23} + \\
& (546016\zeta_5^3 - 390192\zeta_5^2 + 578641\zeta_5 - 52880))(\sqrt[5]{d})^4 + \\
& ((-29334\zeta_5^3 - 14881\zeta_5^2 - 8961\zeta_5 - 33059)\sqrt{23} + \\
& (-141252\zeta_5^3 - 71412\zeta_5^2 - 43010\zeta_5 - 158646))(\sqrt[5]{d})^3 + \\
& ((-833\zeta_5^3 + 5072\zeta_5^2 - 3565\zeta_5 + 4536)\sqrt{23} + \\
& (-3405\zeta_5^3 + 24368\zeta_5^2 - 17216\zeta_5 + 22388))(\sqrt[5]{d})^2 + \\
& ((1347\zeta_5^3 + 63\zeta_5^2 + 768\zeta_5 + 897)\sqrt{23} + \\
& (5762\zeta_5^3 - 772\zeta_5^2 + 4248\zeta_5 + 3052))\sqrt[5]{d} + \\
& ((-224\zeta_5^3 - 623\zeta_5^2 - 87\zeta_5 - 521)\sqrt{23} + \\
& (-936\zeta_5^3 - 457\zeta_5^2 - 1103\zeta_5 - 644)),
\end{aligned}$$

where $c \in K := L(d^{1/5})$ is such that $\mathrm{N}_{K/L}(c) = 2\sqrt{23}$. The primes in $\mathcal{O}_K$ in the support of the fractional ideal (c) are some primes above $2, 23, 101$. Computing t we

get, the prime ideals of $\mathcal{O}_K$ in the support of the fractional ideal (t) are primes above $2, 5, 23, 101, 10040981, 64739112698544079629106251382620961$. There is exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ above 101 such that (c) and (t) have non-trivial valuation at some of the primes above $\mathfrak{p}$ of $\mathcal{O}_K$. In this case $\mathfrak{p}$ splits and if $\mathfrak{p}_K$ is a prime above $\mathfrak{p}$ of $\mathcal{O}_K$, then the valuation of (t) at $\mathfrak{p}_K$ is a multiple of 5. Note that the ideals (10040981) and $(64739112698544079629106251382620961)$ are coprime to (c). Therefore, if $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_K$ above them, then $v_{\mathfrak{q}}(\delta_{\mathrm{glob}} t) = 0$, where $1030301\delta_{\mathrm{glob}}$ is

$$\begin{aligned}&(-19841321740\zeta_5^3 + 13107227660\zeta_5^2 - 51815029910\zeta_5 + 33935425165)\sqrt{23}\\ +\quad &(-144881960000\zeta_5^3 + 118898270530\zeta_5^2 - 311590100680\zeta_5 + 142162447835).\end{aligned}$$

Hence, the only prime we need to compute is the prime $\mathfrak{p}$ above 101. Therefore, t contributes nothing and we get $\zeta_5^{5\langle d, d'\rangle_{\mathrm{CT}}} = (\delta_{\mathrm{glob}}, d')_{L_{\mathfrak{p}}}^{-1} = (\pi, d')_{L_{\mathfrak{p}}}^{3} = \zeta_5^{-1}$. Hence, $\mathrm{rk}(J_{23}/\mathbb{Q}) = \mathrm{rk}(J_{23}/k) = 0$. This result can also be obtained via a 2-Selmer group computation. We give another example where computing $\mathrm{S}^{(2)}(J/k)$ or $\mathrm{S}^{(\lambda)}(J/k)$ do not provide better bounds.

5.6.2 C_{62}

Let C_{62} be the curve given by the equation

$$y^2 = x^5 + 62.$$

One checks that 62 lies in the 5-Stoll set. We have $\mathrm{S}^{(\lambda)}(J/k) \simeq \langle d_1, d_2\rangle \simeq (\mathbb{Z}/5\mathbb{Z})^2$, where $d_1 \coloneqq -4\sqrt{62} - 32$ and $d_2 \coloneqq (-74\zeta_5^3 - 74\zeta_5^2 - 38)\sqrt{62} - 7\zeta_5^3 - 7\zeta_5^2 - 655$. One checks that d_1 is a 5th power in L_λ. Hence, we do not need to compute the local points. We obtain

$$\begin{aligned}c \coloneqq\ &(1/20(\zeta_5^3 + 8\zeta_5^2 + \zeta_5)\sqrt{62} + 1/20(8\zeta_5^3 - 55\zeta_5^2 - 4\zeta_5 + 14))\sqrt[5]{d_1}^4\\ &+ (1/20(-7\zeta_5^3 - 6\zeta_5^2 - 6\zeta_5 - 9)\sqrt{62} + 1/10(11\zeta_5^3 + 30\zeta_5^2 + 15\zeta_5 + 31))\sqrt[5]{d1}^3\\ &+ (1/10(-\zeta_5^3 - 3\zeta_5^2 + \zeta_5 - 1)\sqrt{62} + 1/10(-13\zeta_5^3 - 9\zeta_5^2 - 7\zeta_5 - 22))\sqrt[5]{d_1}^2\\ &+ (1/10(7\zeta_5^3 + 3\zeta_5^2 + 3\zeta_5 + 6)\sqrt{62} + 1/5(28\zeta_5^3 - 9\zeta_5^2 + 7\zeta_5 + 9))\sqrt[5]{d_1}\\ &+ 1/5(-2\zeta_5^3 + 5\zeta_5^2 - 3\zeta_5 + 1)\sqrt{62} + 1/5(-13\zeta_5^3 + 35\zeta_5^2 - 14\zeta_5 + 23);\end{aligned}$$

c is an algebraic integer with norm $2\sqrt{62}$, so only the prime ideals above 620 can have a non-trivial valuation. Computing t gives us one prime in L above each of the $461, 102386941$ and $816505440648910531024494824982592346488 01$ appearing with valuation -1 in the fractional ideal (t) (all the ideals above the above primes in L are inert in K). Computing at each of them we get a contribution of $3/5$, $4/5$ and $4/5$, respectively. At λ, since the contribution is $(1/t, d_2)_{L_\lambda}$, we check that t is a norm from $L_\lambda(\sqrt[5]{d_2})$ and therefore, the contribution is trivial. Therefore, $\zeta_5^{5\langle d_1, d_2\rangle_{\mathrm{CT}}} = \zeta_5$.

By a 2-Selmer group computation over $\mathbb{Q}$, and by checking that the 2-Selmer group over $\mathbb{Q}$ is not killed on base change to k, one obtains that 4 divides $\#Ш(J/k)^{\mathrm{Gal}(k/\mathbb{Q})}$.

Furthermore, d_1 is invariant under the Galois action of $L/\mathbb{Q}$. This implies that $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2 \subset Ш(J_{62}/\mathbb{Q})$. To see this, one uses the fact that

$$\mathrm{S}^{(5)}(J_{62}/k)^{\mathrm{Gal}(k/\mathbb{Q})} \simeq \mathrm{S}^{(5)}(J_{62}/\mathbb{Q}),$$

which follows from the fact that $[L : \mathbb{Q}] = 8$ is coprime to 5; see [Pat24, §1.1] for details. Since $J_{62}(k) = J_{62}(\mathbb{Q}) = 0$, $(Ш(J_{62}/k)[5])^{\mathrm{Gal}(k/\mathbb{Q})} = Ш(J_{62}/\mathbb{Q})[5]$. Since the CTP is alternating on the 5-part of Ш,

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^2 \subset Ш(J_{62}/\mathbb{Q}).$$

Remark 5.6.1. Computing the CTP on $Ш(J_{62}/\mathbb{Q})[2]$, takes a very long time as we are trying to solve norm equation over a degree 40 extension. However, one computes the CTP on the λ-Selmer group faster to compute the rank of J_{62}.

Chapter 6

Descent using some isogenies and the CTP

In this chapter we consider some isogenies on genus 2 Jacobians with kernel a maximal isotropic subgroup with respect to the Weil-pairing. Throughout this chapter, let $C : y^2 = f(x)$ be a genus 2 curve over k and let J be its Jacobian variety, where $f \coloneqq \sum_{i=0}^{6} a_i x^i$. Recall the definition of $D_\infty = (O_+) + (O_-)$ from §2.1.4. Specifically, we look at maximal isotropic subgroups of $J[2]$ and $J[3]$ with respect to e_2 and e_3 as G_k-modules. Since the Weil pairing is alternating, we naturally have that $\langle P \rangle \subset J[p]$ is an isotropic subspace, for every $P \in J[p]$. Recall that $\mathrm{rk}_{\mathbb{F}_p} J[p] = 4$. Hence, if $M \subset J[p]$ is a G_k-submodule of $\mathbb{F}_p$-rank 2 such that $e_p(P, Q) = 1$, for all $P, Q \in M$, then M is maximal isotropic in $J[p]$, so [Moo, Proposition 11.25] (choose $\lambda = 2\lambda_\Theta$ and $f : J \to J/M$ the quotient map) implies that J/M is a principally polarized abelian variety, and we have the following exact sequence of Galois modules

$$0 \to M \to J[p] \to M^\vee \to 0,$$

with $\mathrm{rk}_{\mathbb{F}_p}(M) = \mathrm{rk}_{\mathbb{F}_p}(M^\vee)$. Using $M \simeq (\mathbb{Z}/p\mathbb{Z})^2$ as an abelian group, we call the corresponding isogeny $\phi_M : J \to J/M$ a (p, p)-isogeny. A $(2, 2)$-isogeny is also known as *Richelot isogeny*. Since J/M is a principally-polarized abelian surface, J/M is isomorphic to the Jacobian of a genus 2 curve or to a product of elliptic curves. In [CF96, §9], the authors characterize all the genus 2 curves such that their Jacobians admit a $(2, 2)$-isogeny, and in [Fly94], the author has developed explicit descent via the Richelot isogeny. For $p = 3$, the results have been more limited. In [BFT14] the authors characterize the genus 2 curves whose Jacobians admit a $(3, 3)$-isogeny corresponding to a maximal-isotropic subgroup $M \simeq (\mathbb{Z}/3\mathbb{Z})^2$ as a G_k-module, and in [BFS23], the authors extend this to the case when $M \simeq \mathbb{Z}/3\mathbb{Z} \times \mu_3$ as G_k-module.

The organization of this chapter is as follows: We first review the explicit characterization of curves corresponding to $(2, 2)$- and $(3, 3)$-isogenies and then look into explicit descent procedure using which we compute the CTP for these two isogenies.

6.1 Richelot isogeny

Let $M \simeq \langle Q_1, Q_2 \rangle \subset J[2]$, where $Q_i := (T_i) + (T_i') - D_\infty$ and T_i, T_i' are Weierstrass points given by $(\theta_i, 0)$ and $(\theta_i', 0)$, respectively. Since $e_2(Q_1, Q_2) = 1$, using Proposition 2.1.9 we obtain $\{T_1, T_1'\} \cap \{T_2, T_2'\} = \emptyset$. This implies that f factors as a product of quadratic polynomials (not necessary monic) $Q_1Q_2Q_3$ over $k(M)$, where we abuse the notation slightly and denote the point Q_i and the polynomial corresponding to the x-coordinates of points T_i and T_i' by Q_i. In this regard the polynomial Q_3 represents the point $Q_1 + Q_2$. The interpretation of Q_i will be clear from the context. Recall that Aut $((\mathbb{Z}/2\mathbb{Z})^2) \simeq S_3$, so generically $\mathrm{Gal}(k(M)/k) \simeq S_3$.

We saw in the previous section that J/M is isomorphic to the Jacobian $\hat{J}$ of a genus 2 curve $\hat{C}$ (say) or to a product of elliptic curves. We assume that J/M is isomorphic to the Jacobian of a genus 2 curve. Recall from §1.2.3, Proposition 1.2.11 that the map $\phi : J \to \hat{J}$ arises from a correspondence of curves, i.e., an element in $\mathrm{Pic}\,(C_{\overline{k}} \times \hat{C}_{\overline{k}})$. Let $\hat{M}$ be the kernel of $\hat{\phi}$. Then the ϕ-Weil pairing shows that $\hat{M} \simeq \mathrm{Hom}(M, \mu_2) \simeq \mathrm{Hom}(M, \mathbb{Z}/2\mathbb{Z})$. Hence, $k(M) = k(\hat{M})$. Another way to see the above is the following. The Weil pairing implies that $J[2]/M \simeq \hat{J}[\hat{\phi}]$ as a G_k-module. Since the points $T_i + T_j$, for $i \neq j$ generate $J[2]/M$, an explicit computation shows that for all $\sigma \in G_{k(M)}$, $\sigma(T_i + T_j) - (T_i + T_j) \in M$, and that for $\sigma \in G_k$ such that $\sigma\big|_{k(M)} \neq \mathrm{id}$, $\sigma(T_i+T_j)-(T_i+T_j) \notin M$. Hence, $k(\hat{M}) = k(M)$. We work over $k(M)$ as our base field to write the expressions for $\hat{C}$ which will turn out to be $\mathrm{Gal}(k(M)/k)$-equivariant. Let $Q_i := f_iX^2 + g_iX + h_i$, $b_{ij} := \mathrm{Res}(Q_i, Q_j)$, $b_i := b_{ij}b_{ik}$, $\delta_i := \mathrm{disc}(Q_i)$ and $\Delta := \det(\mathcal{F})$, where $\mathrm{Res}(\_,\_)$ is the resultant of two polynomials, and the ith row of $\mathcal{F}$ is (f_i, g_i, h_i). Similarly, define $\hat{Q}_1 := Q_2Q_3' - Q_3Q_2'$ and cyclically $\hat{Q}_2$ and $\hat{Q}_3$, $\hat{b}_{ij} := \mathrm{Res}(\hat{Q}_i, \hat{Q}_j)$, $\hat{b}_i$ and $\hat{\delta}_i$. The following proposition summarizes some facts about curves whose Jacobians admit a Richelot isogeny.

Proposition 6.1.1. [CF96] *Let $\phi, \hat{\phi}, C, \hat{C}$, $J, \hat{J}, Q_i, b_{ij}$, b_i, δ_i, $\hat{Q}_i, \hat{b}_ij$, $\hat{b}_i, \hat{\delta}_i, \Delta$ be as above and $\Delta \neq 0$. Then $\hat{C}$ is given by the equation $\Delta y^2 = \prod_{i=1}^{3} \hat{Q}_i$, and the correspondence class giving rise to the Richelot isogeny can be represented by the vanishing locus D of the polynomials $Q_1(x)\hat{Q}_1(\hat{x}) + Q_2(x)\hat{Q}_2(\hat{x}), y\hat{y} - Q_1(x)\hat{Q}_1(\hat{x})$, where $\hat{x}, \hat{y}$ are the coordinates corresponding to $\hat{C}$. Since C and $\hat{C}$ have the same form and $Q_1 = \hat{Q}_2\hat{Q}_3' - \hat{Q}_3\hat{Q}_2'$ (up to scaling such that product of the scaling factors for Q_1, Q_2, and Q_3 is a square) and similarly, for Q_2 and Q_3, one gets a correspondence associated to the isogeny $\hat{\phi}$ which is given by D^t.*

Furthermore, there is an explicit embedding $J \to \mathbb{P}^{15}$ given by $P \mapsto (v_0 : \ldots : v_{15})$ such that the translations by points Q_1, Q_2 and Q_3 are given by the 16×16 matrices $M_1 := b_1\mathrm{Diag}(I_4, I_4, -I_4, -I_4)$, $M_2 := b_2\mathrm{Diag}(I_4, -I_4, I_4, -I_4)$, $M_3 := \frac{1}{b_{12}^2}M_1M_2$, respectively, where I_4 is the 4×4 identity matrix. Then the map $\tau : \mathbb{P}^{15} \to \mathbb{P}^{15}$ given

by

$$(v_0 : \ldots : v_{15}) \mapsto (v_0^2 : \ldots : v_0v_3 : v_4^2 : \ldots : v_4v_7 : v_8^2 : \ldots : v_8v_{11} : v_{12}^2 : \ldots : v_{12}v_{15}),$$

satisfies the property that $\tau(M_i(v)) = \tau(v)$*, for all* v *in* $\mathbb{P}^{15}$*. Moreover, there exist explicit* 16×16 *matrices* N*,* $\hat{N}$ *and* U *such that* $\phi = N\tau$ *and* $\hat{\phi} = U\hat{N}\tau$*.*

Let W be the set of Weierstrass points of C and $W' := \{\{T_i + T_i'\} \mid 1 \leq i \leq 3\}$. Similarly, define $\hat{W}, \hat{W}'$ w.r.t $\hat{C}$. Recall the definition of twisted powers (1.3.41). Let $\mathbb{1}_W$ and $\mathbb{1}_{W'}$ be the constant -1 maps in μ_2^W and $\mu_2^{W'}$, respectively, let $\mathrm{N}_W : \mu_2^W \to \mu_2$ be the natural map $m \mapsto \prod m(P)$, and let $\left(\mu_2^W\right)_0 := \ker(\mathrm{N}_W)$. Then $J[2] \simeq \left(\mu_2^W\right)_0 / \mathbb{1}_W$. Let $\psi : (\mu_2^W)_0 \to \mu_2^{W'}$ be the map $m \mapsto m'$, where $m'(\{T_i, T_i'\}) := m(T_i) + m(T_i')$. Then ψ is a homomorphism with $\ker(\psi) = \mu_2^{W'}$. We have

$$\mathrm{Im}(\psi) \simeq \left(\mu_2^W\right)_0 / \mu_2^{W'} \simeq \left(\left(\mu_2^W\right)_0 / \mathbb{1}_W\right) / \left(\mu_2^{W'} / \mathbb{1}_{W'}\right) \simeq J[2]/J[\phi] \simeq \hat{J}[\hat{\phi}].$$

Concretely, $\mathrm{Im}(\psi) \simeq \langle m_{ij} \rangle$, where $m_{ij}(\{T_k, T_k'\}) = 1$ if $k \notin \{i, j\}$ and -1 otherwise. There is a natural action of S_3 on W' and one checks that the transposition (i, j) has no action on m_{ij}, therefore under the identification of $\mathrm{Im}(\psi)$ with $J\hat{\phi}$, m_{ij} must map to $\hat{T}_k$ for pairwise distinct i, j, k.

The following theorem gives us information about the group $\mathrm{H}^1(G_k, J[2])$.

Theorem 6.1.2. [SvL13] *Let* J *be as above, and let* $A := k[x]/\langle f(x) \rangle$*. Then*

$$\mathrm{H}^1(G_k, J[2]) \simeq \mathrm{H}^1(G_k, \left(\mu_2^W\right)_0 / \mathbb{1}_W) \simeq \Gamma / \pi(A^\times)\iota(k^\times),$$

where $\Gamma := \{(a, t) \in A^\times \times k^\times \mid \mathrm{N}_{A/k}(a) = t^2\}$ *and* $\pi : A^\times \to \Gamma$ *and* $\iota : k^\times \to \Gamma$ *are the maps* $\theta \mapsto (\theta^2, \mathrm{N}_{A/k}(\theta))$ *and* $\theta \mapsto (\theta, \theta^3)$*. Furthermore, the connecting morphism* $J(k)/2J(k) \to \Gamma/\pi(A^\times)\iota(k^\times)$ *is given by* $P_1 + P_2 - D_\infty \mapsto ((x(P_1) - T)(x(P_2) - T)), a_6 y(P_1) y(P_2))$*, where* T *is a root of* f *in* A*.*

Combining the above theorem with previous discussion, we have the commutative diagram

$$\begin{array}{ccccc} J(k)/2J(k) & \longrightarrow & \mathrm{H}^1(G_k, J[2]) & \xrightarrow{\sim} & \Gamma/\pi(A^\times)\iota(k^\times) \\ \downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{N}_{A/K}} \\ J(k)/\hat{\phi}(\hat{J}(k)) & \longrightarrow & \mathrm{H}^1(G_k, \hat{J}[\hat{\phi}]) & \hookrightarrow & K^\times/(K^\times)^2 \end{array},$$

where $K \subset k[T]/\langle f(T) \rangle$ is the degree 3 étale subalgebra fixed by the transposition swapping T_1, T_1', and the vertical rightmost $\mathrm{N}_{A/K}$ is the norm map with respect to this transposition. This implies that the connecting morphism $J(k)/\hat{\phi}(\hat{J}(k)) \to \mathrm{H}^1(G_k, \hat{J}(\hat{\phi}))$ is given by

$$\begin{aligned} [P_1 + P_2 - D_\infty] &\mapsto \mathrm{N}_{A/K}(x(P_1) - T_1)(x(P_2) - T_1) \\ &= (x(P_1) - T_1)(x(P_2) - T_1)(x(P_1) - T_1')(x(P_2) - T_1') \\ &= Q_1(x(P_1))Q_1(x(P_2))/f_1^2, \end{aligned}$$

where recall that for $1 \leq i \leq 3$, f_i is the leading coefficient of the polynomial Q_i. Since we are only looking at the image modulo squares, we can safely define the connecting morphism by $[P_1 + P_2 - D_\infty] \mapsto (Q_i(P_1)Q_i(P_2))_{i=1}^3$. Note that, in the above discussion one can interchange C and $\hat{C}$ due to their symmetry and we will arrive at similar expressions.

The map $J[\phi] \to \mu_2^{W'}$ composed with the map $\mu_2^{W'} \to J[\phi]$ given by $m \mapsto \sum_{i=1}^{3} m(\{T_i, T_i'\})Q_i$ is the identity on $J[\phi]$, so $J[\phi] \oplus \mathbb{1}_{W'} \simeq \mu_2^{W'}$. Note that $\mu_2^{W'} \simeq \mu_2^{\hat{W}'}$ via $m_i \mapsto m_{jk}$, where m_i is a map with -1 at $\{T_i, T_i'\}$, and 1 otherwise, and $\hat{m}_{jk}$ is as defined above. We have $J[\phi] \simeq \mathrm{Im}(\hat{\psi})$, and $\mu_2^{\hat{W}'} \simeq \mathrm{Im}(\hat{\psi}) \oplus \mathbb{1}_{\hat{W}'}$. Therefore, $J[\phi] \hookrightarrow \mu_2^{\hat{W}'}$, and $\mathrm{H}^1(G_k, J[\phi]) \hookrightarrow \mathrm{H}^1(G_k, \mu_2^{\hat{W}'})$.

We are in the situation of the corestriction method from §4.1.

6.1.1 Computation of the pairing

Let a, a' denote elements of $\mathrm{S}^{(\phi)}(J/k)$ denoted by the triples (d_1, d_2, d_3), (d_1', d_2', d_3'), respectively, where d_i and d_j are conjugates if Q_i and Q_j are, and similarly for d_1', d_2', d_3'. Recall the definition of χ and χ' from the case of elliptic curves. Using the corestriction method as in the case of elliptic curves, we assume that Q_1 is defined over k. Let $\chi_1' \coloneqq \sigma(d_1)/d_1 \in \mu_2$ for $\sigma \in G_k$. We choose a lift $\mathfrak{a}$ of a as follows

$$\mathfrak{a}(\sigma) = \begin{cases} 0, & \text{if } \chi(\sigma) = \widehat{0}, \\ (T_i) + (T_i') - D_\infty, & \text{if } \chi(\sigma) = \widehat{i}, \end{cases}$$

and

$$\mathfrak{a}_1'(\sigma) = \begin{cases} 0, & \text{if } \chi_1'(\sigma) = 1, \\ (T_1) + (T_1') - D_\infty, & \text{if } \chi_1'(\sigma) = -1. \end{cases}$$

Using the corestriction method for the global step, we only need a method to compute ε_1, such that $\partial\varepsilon_1 = \eta_1 \coloneqq \partial\mathfrak{a} \cup \mathfrak{a}_1' - \mathfrak{a} \cup \partial\mathfrak{a}_1'$. We have

$$\partial\mathfrak{a}(\sigma, \tau) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0}, \\ 2(T_i) + 2(T_i') - 2D_\infty = \mathrm{div}(Q_i(x)), & \\ & \text{if } \chi(\sigma) = \widehat{i},\ \sigma \cdot \chi(\tau) = \widehat{i}, \\ (T_i) + (T_i') + (T_j) & \\ +(T_j') - (T_k) - (T_k') - D_\infty = \mathrm{div}(\frac{y}{Q_k(x)}), & \\ & \text{if } \chi(\sigma) = \widehat{i},\ \sigma \cdot \chi(\tau) = \widehat{j}. \end{cases}$$

Similarly, for $\mathfrak{a}'_1$,

$$\partial\mathfrak{a}'_1(\sigma,\tau) = \begin{cases} 0 = \mathrm{div}(1), & \text{if } \chi'(\sigma) = 1 \text{ or } \chi'(\tau) = 1, \\ 2(T_1) + 2(T'_1) - 2D_\infty = \mathrm{div}(Q_1), & \text{if } \quad \chi'(\sigma) = \chi'(\tau) = -1. \end{cases}$$

Choose the uniformizers t_P at the points $P \in C(\bar{k})$ as $t_{T_i} \coloneqq (\theta_i - \theta'_i)(x - \theta_i)/y$, $t_{\infty_+} = t_{\infty_-} \coloneqq x^2/y$, and $t_p \coloneqq x - x(P)$ otherwise. Once again we have $\langle\cdot,\cdot\rangle_1 = \langle\cdot,\cdot\rangle_2$ for the functions appearing in the expressions for $\partial\mathfrak{a}$ and $\partial\mathfrak{a}'_1$. Using the above, we obtain

$$\begin{aligned} &\langle (Q_1, (T_1) + (T'_1) - D_\infty\rangle_1 = b_1 f_2^2 f_3^2, \quad \langle (Q_i, (T_j) + (T'_j) - D_\infty\rangle_1 = b_{ij} f_k^2, \\ &\langle y/Q_k, (T_1) + (T'_1) - D_\infty\rangle_1 = b_{1j} f_k^2, \quad \langle y/Q_1, (T_1) + (T'_1) - D_\infty\rangle_1 = 1. \end{aligned}$$

The expressions for $\partial\mathfrak{a} \cup \mathfrak{a}'_1$ and $\mathfrak{a} \cup \partial\mathfrak{a}'_1$ are given by

$$(\partial\mathfrak{a} \cup_1 \mathfrak{a}'_1)(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \quad \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0} \text{ or } \chi'_1(\rho) = 1, \\ b_1 f_2^2 f_3^2, & \text{if } \quad \chi(\sigma) = \widehat{i},\ \sigma\cdot\chi(\tau) = \widehat{1},\ \chi'(\rho) = -1, \\ b_{1j} f_k^2, & \text{if } \quad \chi(\sigma) = \widehat{j},\ \sigma\cdot\chi(\tau) = \widehat{j},\ \chi'(\rho) = -1, \\ b_{1j} f_k^2, & \text{if } \quad {}^{(\chi(\sigma),\sigma\cdot\chi(\tau))=(\widehat{1},\widehat{j}),\text{ or}}_{(\chi(\sigma),\sigma\cdot\chi(\tau))=(\widehat{j},\widehat{1})},\ \chi'(\rho) = -1, \\ 1, & \text{if } (\chi(\sigma),\sigma\cdot\chi(\tau)) = (\widehat{k},\widehat{j}),\ \chi'(\rho) = -1, \end{cases} \tag{6.1.1}$$

and

$$(\mathfrak{a} \cup_2 \partial\mathfrak{a}'_1)(\sigma,\tau,\rho) = \begin{cases} 1, & \text{if } \chi(\sigma) = \widehat{0} \text{ or } \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ b_1 f_2^2 f_3^2, & \text{if } \quad \chi(\sigma) = \widehat{1}, \chi'(\tau) = \chi'(\rho) = -1, \\ b_{ij} f_k^2, & \text{if } \quad \chi(\sigma) = \widehat{j}, \chi'(\tau) = \chi'(\rho) = -1. \end{cases} \tag{6.1.2}$$

In order to solve for ε_1, we would like to apply the method developed in §4.3.1. However, for the method to be applied we want a version of Assumption 4.3.3 for the Richelot isogeny. Note that we required Assumption 4.3.3 only to show that the two cocycles E_1 and $E_{1,g}$ are cohomologically trivial. Recall the definition of fields K and K' associated with the $\mathfrak{a}$ and $\mathfrak{a}'_1$. In what follows, we show that the 2-cocycles E_1 and $E_{1,g}$ extracted from η_1 are indeed cohomologically trivial in a simpler way. Recall that E_1 and $E_{1,g} \in \mathrm{Z}^2(K')$ are defined by $E_1(\sigma,\tau) \coloneqq \eta_1(\sigma,\tau,-1)$ and $E_{1,g}(\sigma,\tau) \coloneqq \eta_1(\sigma,\tau g,-1)/\eta_1(\sigma,g,-1)$, where $g \in G_k$ is chosen such that $\chi'_1(g) = -1$.

Proposition 6.1.3. *The 1-cocycles E_1 and $E_{1,g}$ represent the trivial class in $\mathrm{H}^1(K')$.*

Proof. $E_1(\sigma,\tau) = \langle \partial\mathfrak{a}(\sigma,\tau), \mathfrak{a}_1'(-1)\rangle_1 = \langle \partial\mathfrak{a}(\sigma,\tau), (T_1)+(T_1')-D_\infty\rangle_1$. Hence $E_1 = \partial\mathfrak{a} \cup ((T_1)+(T_1')-D_\infty)$. Similarly, $E_{1,g} = \partial\tilde{\mathfrak{a}} \cup ((T_1)+(T_1')-D_\infty)$, where $\tilde{\mathfrak{a}}(\sigma) \coloneqq \mathfrak{a}(\sigma g) - \mathfrak{a}(g)$. Since $\mathrm{H}^2(K')$ satisfies the local-global principle, for each place v of K', $E_{1v} \coloneqq \partial\mathfrak{a}_v \cup ((T_1)+(T_1')-D_\infty)$ represents the trivial class in $\mathrm{Br}(K_v')$, and similarly for $E_{1,g}$. Since a is locally trivial, there is a point $P_v \in J(\overline{k_v})$ represented by a degree–0 divisor $\mathfrak{b}_v$, such that P_v witnesses the local triviality of the 1-cocycle representing a_v. The 1-cochain $\mathfrak{a}_v - \partial\mathfrak{b}_v$ takes values in principal divisors. Let $e_{1v} \coloneqq (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 ((T_1)+(T_1')-D_\infty)$, and $\tilde{e_{1v}}(\sigma) \coloneqq \langle (\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma g) - (\mathfrak{a}_v - \partial\mathfrak{b}_v)(g), ((T_1)+(T_1')-D_\infty)\rangle_1$. Then $\partial e_{1v} = \partial\mathfrak{a} \cup ((T_1)+(T_1')-D_\infty) = E_{1v}$ and

$$\begin{aligned}\partial\tilde{e_{1v}}(\sigma,\tau) &= \langle (\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma g) - (\mathfrak{a}_v - \partial\mathfrak{b}_v)(g) + \\ &\quad \sigma((\mathfrak{a}_v - \partial\mathfrak{b}_v)(\tau g)) - \sigma((\mathfrak{a}_v - \partial\mathfrak{b}_v)(g)) \\ &\quad - (\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma\tau g) + (\mathfrak{a}_v - \partial\mathfrak{b}_v)(g), ((T_1)+(T_1')-D_\infty)\rangle_1 \\ &= (\partial\tilde{\mathfrak{a}} \cup_1 ((T_1)+(T_1')-D_\infty))(\sigma,\tau) = (E_{1,g})_v(\sigma,\tau).\end{aligned}$$

Therefore, E_1 and $E_{1,g}$ are cohomologically locally everywhere trivial. □

Hence, one can compute ε_1 such that $\partial\varepsilon_1 = \eta_1$ using the method developed in §4.3.1.

Remark 6.1.4. One can prove results similar to the ones in section §4.3.2 for the case of Richelot isogeny using the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{J}[\hat{\phi}] & \longrightarrow & \hat{J}[2] & \xrightarrow{\hat{\phi}} & J[\phi] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \hat{J}[\hat{\phi}] & \longrightarrow & \hat{J} & \xrightarrow{\hat{\phi}} & J & \longrightarrow & 0 \end{array}.$$

We now look into the local computation. Let v be a place of k and let $P_v \in J(\overline{k_v})$ be such that $\partial P_v = \alpha_v$, where α is the 1-cocycle representing a whose lift is $\mathfrak{a}$. Computing $\phi(P_v) \in \hat{J}(k_v)$ can be achieved by computing $\hat{J}(k_v)/2\hat{J}(k_v)$, which has been implemented in many computer algebra systems for fake 2-descent. For the computation of P_v from $\phi(P_v)$, we use Proposition 6.1.1. Recall the embeddings of J and $\hat{J}$ in $\mathbb{P}^{15}$ via the coordinates v_i and $\hat{v}_i$, the τ map, and the matrix N from Proposition 6.1.1. We have $\phi(P_v) = N\tau(P_v)$ (here P_v and $\phi(P_v)$ are represented as points in $\mathbb{P}^{15}$), so $N^{-1}(\phi(P_v)) = \tau(P_v)$. Using the definition of the τ map, one sees that if we fix v_0, v_4, v_8, v_{12}, then we fix all the other v_i for a given $\phi(P_v)$, and there are at most 8 choices available since $\partial P_v = -\partial P_v$. Hence, one can easily invert an element in the image of ϕ and $\hat{\phi}$ locally.

Combining all this, and using the theory of §4.3.3, we have the following theorem

Theorem 6.1.5. *Let d and d' representing a and a' be as before, and for each place v of k, let k_{vi} be the extension of k_v corresponding to the G_{k_v}-orbit i of W'. Then*

for each place v of k, and each G_{k_v}-orbit i of W', there is an algorithm to compute $\delta_{vi} \in k_{vi}^{\times}$ such that

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \prod_i (\delta_{vi}, d_i)_{k_{vi}}.$$

Remark 6.1.6. The pseudocode for the algorithm mentioned in above theorem is almost same as the one from Algorithm 1, so we do not repeat it here.

6.2 $(3,3)$-isogeny

In this section we look into the $(3,3)$-isogeny. First we recall some known theory about curves whose Jacobians admit $(3,3)$-isogeny. Recall from the previous discussion that if J admits a $(3,3)$-isogeny ϕ with kernel M, then the abelian variety $\hat{J} \coloneqq J/M$ is the Jacobian of a genus 2 curve (say $\hat{C}$) or a product of two elliptic curves. In this section, we assume that $\hat{J}$ is the Jacobian of a genus 2 curve, and that $M \simeq (\mathbb{Z}/3\mathbb{Z})^2$ as a G_k-module.

Proposition 6.2.1. [BFT14, Lemma 1, 3] *Let C be a genus 2 curve given by $y^2 = cf(x)$, where $\deg(f) = 6$ and $c \in k^{\times}$, D_1 and D_2 be effective divisors of degree 2 and D_∞ be as before such that $D_1 - D_\infty$ and $D_2 - D_\infty$ represent distinct points T_1 and T_2 (resp.) of order 3 on J. Then we can assume that D_1, D_2 and D_∞ have pairwise disjoint supports. Furthermore, under the above assumption, there exist cubic polynomials G_1 and G_2 over k, $\lambda_1, \lambda_2 \in k^{\times}$ and monic quadratic polynomials H_1 and H_2 with $\gcd(H_1, H_2) = 1$ over k such that*

$$cf(x) = G_1^2 + \lambda_1 H_1^3 = G_2^2 + \lambda_2 H_2^3,$$

and D_i can be taken as $(x_{i1}, G_i(x_{i1})) + (x_{i2}, G_i(x_{i2}))$, where x_{ij} are roots of H_i for $i, j \in \{1, 2\}$.

We denote by g_i the leading coefficient of G_i above and by λ a fixed cube root of λ_1/λ_2. Since $\mathrm{disc}(f) \neq 0$, $\gcd(H_i, G_i) = 1$. We have $(G_1 - G_2)(G_1 + G_2) = \lambda_2(H_2 - \lambda H_1)(H_2 - \lambda\zeta_3 H_1)(H_2 - \lambda\zeta_3^2 H_1)$, so $G_1 - G_2$ does not vanish on x_{ij}. We have $3D_i - 3D_\infty = \mathrm{div}(y - G_i(x))$ and

$$\langle y - G_i(x), D_j - D_\infty\rangle_1 = \langle D_j - D_\infty, y - G_i\rangle_2 = c^3 \mathrm{res}(G_i - G_j, H_j)/\lambda_i.$$

This gives

$$e_3(T_1, T_2) = \frac{\lambda_2 \mathrm{res}(G_2 - G_1, H_2)}{\lambda_1 \mathrm{res}(G_1 - G_2, H_1)}.$$

The following proposition gives the condition when $M \coloneqq \langle T_1, T_2\rangle$ is maximal isotropic with respect to the Weil pairing.

Proposition 6.2.2. [BFT14, Lemma 5] *We have $e_3(T_1, T_2)$ is trivial if and only if none of the polynomials $H_1 - \lambda\zeta_3^i H_2$ divide $G_2 - G_1$.*

From now on we assume that $\mu_3 \subset k^\times$. This implies that $\hat{M} \simeq M^\vee \simeq (\mathbb{Z}/3\mathbb{Z})^2$, where $\hat{M}$ is the kernel of the dual isogeny $\hat{\phi} : \hat{J} \to J$. The moduli space of principally polarized abelian surfaces with a maximal isotropic subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ as G_k-module is of dimension 3. The following theorem allows us to generically and explicitly construct curves whose Jacobians have a maximal isotropic subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

Theorem 6.2.3. [BFT14, Theorem 6, 13] *Let J be the Jacobian of a genus 2 curve C admitting a $(3,3)$-isogeny ϕ with $J[\phi] \simeq (\mathbb{Z}/3\mathbb{Z})^2$. Then generically C can be obtained as a specialization of curve $C_{rst} := G_i^2(r,s,t) + \lambda_i(r,s,t)H_i(r,s,t)^3$, for $i \in \{1,2,3,4\}$ over $k(r,s,t)$, where G_i, H_i, and λ_i are rational functions in $k(r,s,t)^\times$. Furthermore, $\hat{J}$ is also the Jacobian of a suitable explicit specialization of a curve $\hat{C}_{rst}$ over $k(r,s,t)$ given by $\hat{C}_{rst} := \hat{G}_i^2(r,s,t) + \hat{\lambda}_i(r,s,t)\hat{H}_i^3(r,s,t)$ for $i \in \{1,2,3,4\}$.*

We now describe the connecting homomorphism, i.e.,

$$J(k)/\hat{\phi}(\hat{J}(k)) \to \mathrm{H}^1(G_k, \hat{J}[\hat{\phi}]) \simeq \mathrm{H}^1(G_k, (\mathbb{Z}/3\mathbb{Z})^2) \simeq \left(\frac{k^\times}{(k^\times)^3}\right)^2.$$

Lemma 6.2.4. [BFT14, Lemma 18] *Let J be the Jacobian of a curve such that J admits a $(3,3)$-isogeny ϕ with a trivial Galois action on $J[\phi]$. Then the map*

$$J(k)/\hat{\phi}(\hat{J}(k)) \to \left(\frac{k^\times}{(k^\times)^3}\right)^2$$

is induced by the partial map

$$(x,y) \in C \mapsto (y - G_1(x), y - G_2(x)).$$

Let $a \in \mathrm{S}^{(\phi)}(J/k)$, be represented by $(d_1, d_2) \in k^\times \times k^\times$. Fix a cube root $d_i^{1/3}$ of d_i. We fix a third root of unity ζ_3, and identify μ_3 with $\mathbb{Z}/3\mathbb{Z}$ via $\zeta_3 \mapsto 1$. Define $\chi_i(\sigma) := \sigma(d_i^{1/3})/d_i^{1/3}$, for $\sigma \in G_k$, and assume that χ_i takes values in $\mathbb{Z}/3\mathbb{Z}$ via the above identification. We choose a 1-cocycle α representing a as $\alpha_1 + \alpha_2$, where $\alpha_i(\sigma) := jT_i$ if $\chi_i(\sigma) = j$. If a' is another element in the ϕ-Selmer group represented by (d_1', d_2'), then similarly define χ_i', α_i', and α'.

6.2.1 Computation of the pairing

In this section we only discuss the global part of the pairing and describe a method for obtaining ε such that $\partial\varepsilon = \eta$ (ε and η are same as in the definition of the pairing in §2.4). Choose the lift $\mathfrak{a}$ of α as $\mathfrak{a}_1 + \mathfrak{a}_2$, where $\mathfrak{a}_i(\sigma) := j(D_i - D_\infty)$, if $\chi_i(\sigma) = j$, and similarly define $\mathfrak{a}_i'$ and $\mathfrak{a}'$ for α'. We have $\eta := \partial\mathfrak{a} \cup \mathfrak{a}' - \mathfrak{a} \cup \partial\mathfrak{a}' = \sum_{i,j} \eta_{ij}$, where $\eta_{ij} := \partial\mathfrak{a}_i \cup \mathfrak{a}_j' - \mathfrak{a}_i \cup \partial\mathfrak{a}_j'$. Define $\eta_i := \eta_{1i} + \eta_{2i}$. We have

$$\partial\mathfrak{a}_i(\sigma, \tau) = \mathrm{div}((y - G_i)^n),$$

where $n = [(\chi_i(\sigma) + \chi_i(\tau))/3]$ and $[.]$ is the greatest integer function. Similarly,

$$\partial \mathfrak{a}'_i(\sigma,\tau) = \mathrm{div}((y - G_i)^{n'}),$$

where $n'[(\chi'_i(\sigma) + \chi'_i(\tau))/3]$.

Let t_P be a uniformizer at $P \in C(\bar{k})$. Choose t_P as $(x-\theta)/y$ when P is a Weierstrass point $(\theta, 0)$, as x^2/y when P is in the support of D_∞, as $(x - x(P))(x_{i1} - x_{i2})$ if $P = (x_{i1}, G_i(x_{i1}))$, where x_{i1}, x_{i2} are roots of H_i as before, and $x - x(P)$ otherwise. Recall that

$$\langle y - G_i, D_j - D_\infty\rangle_1 = \langle D_j - D_\infty, y - G_i\rangle_2 = c^3 \mathrm{res}(G_i - G_j, H_j)/\lambda_i,$$

and

$$\langle y - G_i, D_i - D_\infty\rangle_1 = \langle D_i - D_\infty, y - G_i\rangle_2 = \frac{\lambda_i^2}{4\mathrm{res}(G_i, H_i)}.$$

We obtain

$$\eta_{ii}(\sigma,\tau,\rho) = \left(\frac{\lambda_2^2}{4\mathrm{res}(G_i, H_i)}\right)^{nk - n'j},$$

where $\chi_i(\sigma) = j$, $\chi'_i(\rho) = k$, $n := [(\chi_i(\sigma) + \chi_i(\tau))/3]$ and $n' := [(\chi'_i(\tau) + \chi'_i(\rho))/3]$, and

$$\eta_{ij}(\sigma,\tau,\rho) = \frac{\mathrm{res}(G_i - G_j, H_j)^{nk}\lambda_j^{n'l}}{\mathrm{res}(G_j - G_i, H_i)^{n'l}\lambda_i^{nk}} c^{3(nk - n'l)},$$

where $\chi_i(\sigma) = l$, $\chi'_j(\rho) = k$, $n := [(\chi_i(\sigma) + \chi_i(\tau))/3]$ and $n' := [(\chi'_j(\tau) + \chi'_j(\rho))/3]$.

Now we will look into a method very similar to the one in §4.3.1 to compute ε_i such that $\partial\varepsilon_i = \eta_i$. Let $K := k(d_1^{1/3}, d_2^{1/3})$, and $K'_i := k(d_i'^{1/3})$. Then η_i factors through the extension $F_i := KK'_i$ and $\eta_i(\sigma,\tau,\rho) = \eta_i(\sigma',\tau',\rho')$ if $\sigma\big|_K = \sigma'\big|_K$, $\tau\big|_K = \tau'\big|_{F_i}$ and $\rho\big|_{K'_i} = \rho'\big|_{K'_i}$. Since η_i only depends on χ'_i in its last coordinate, we will interchangeably write $\eta_i(\sigma,\tau,\chi'_i(\rho))$ and $\eta_i(\sigma,\tau,\rho)$. Choose the representative g_j of cosets of $\mathrm{Gal}(F/K'_i)$ in $\mathrm{Gal}(F/k)$ such that $\chi'_i(g_j) = j$. Define the 2-cochains in $\mathrm{C}^2(K'_i)$

$$E_{i,j}(\sigma,\tau) := \eta_i(\sigma,\tau,g_j) \quad \text{and} \quad E_{i,j,k}(\sigma,\tau) := \eta_i(\sigma,\tau g_j, g_k)/\eta_i(\sigma, g_j, g_k).$$

In what follows we do not give exact proofs as they are very close to the ones done before.

Proposition 6.2.5. *The 2-cochains $E_{i,j}$ and $E_{i,j,k}$ are 2-cocycles in $\mathrm{Z}^2(K'_i)$ and represent the trivial class in $\mathrm{H}^2(K'_i)$.*

Proof. We prove it only for $E_{i,j,k}$ because $E_{i,j}$ is obtained by replacing g_j by id and g_k by g_j. Define $\tilde{\mathfrak{a}}(\sigma) := \mathfrak{a}(\sigma g_j) - \mathfrak{a}(g_j)$. Then $E_{i,j,k} = \partial\tilde{\mathfrak{a}} \cup (k(D_i - D_\infty))$, so we have $\partial E_{i,j,k} = 0$. The proof of the cohomological triviality of $E_{i,j,k}$ and Ei,j is similar to the proof of the Proposition 6.1.3. □

Hence, there are 1-cochains $e_{i,j}$ and $e_{i,j,k}$ factoring through $\mathrm{Gal}(F/K_i')$. Here the indices are considered modulo 3.

Now construct 1-cochains $f_{i,j,k}$ and $\psi_{i,j,k}$ in $\mathrm{C}^1(K_i')$ given by $f_{i,j,k}(\sigma) \coloneqq \eta_i(\sigma, g_j, g_k)$ and

$$\psi_{i,j,k}(\sigma) \coloneqq f_{i,j,k} + e_{i,j,k} - e_{i,j} - e_{i,j+k}.$$

The following proposition shows that $\psi_{i,j,k}$ is a 1-cocycle.

Proposition 6.2.6. *Let $\psi_{i,j,k}$ be as above. Then $\psi_{i,j,k}$ is a 1-cocycle, and there exists $t_{i,j,k} \in F^\times$ such that $\psi_{i,j,k}(\sigma) = \sigma(t_{i,j,k})/t_{i,j,k}$.*

Proof. Similar to the proof of Proposition 4.3.5. □

One can choose $t_{i,j,k} = 1$ when $k = 0$ or $j = 0$ as $\psi_{i,j,k} = 0$ in both the cases. Similarly to Equation (4.3.3), define a 1-cochain $\varepsilon_i' \in \mathrm{C}^2(k)$ as

$$\varepsilon_i'(\tau, \rho) \coloneqq t_{i,j,k} e_{i,j,k}(\tau'),$$

where $\chi_i'(\tau) = g_j$, $\chi_i'(\rho) = g_k$, and $\tau' \in G_{K_i'}$ is such that $\tau = \tau' g_j$.

Proposition 6.2.7. *Let $\eta_i' \coloneqq \eta_i - \partial\varepsilon_i'$. Then $\eta_i'(\sigma, \tau, \rho) = 1$, if $(\sigma, \tau, \rho) \in G_{K_i'} \times G_k \times G_k \cup G_k \times G_k \times G_{K_i'}$, and if $\sigma, \tau \in G_{K_i'}$ and $\rho \in G_k$ be such that $\chi_i'(\rho) = k$, then $\eta_i'(\sigma g_j, \tau, \rho) = \sigma\eta_i'(g_j, \tau, g_k)$ and $\eta_i'(\sigma g_j, \tau g_l, g_k) = \sigma\eta_i'(g_j, \tau g_l, g_k)$.*

Proof. The proof is similar to the proof of Proposition 4.3.6 and Corollary 4.3.7. □

Let $\sigma_{g_k} \coloneqq g_k \sigma g_k^{-1}$ for $\sigma \in \mathrm{Gal}(F/K_i')$. We will need the following variant of Hilbert's Theorem 90 which is similar to Proposition 4.3.8.

Proposition 6.2.8. *Let g_k be as before and let $f \in \mathrm{C}^1(K/K_i')$ be such that, for $\sigma, \tau \in \mathrm{Gal}(K/K_i')$,*

$$f(\sigma\tau) = f(\sigma)\sigma_{g_k} f(\tau).$$

Then there is a $c \in K^\times$ such that $f(\sigma) = c/\sigma_{g_k}(c)$.

Proof. The proof is similar to the standard proof of Hilbert's Theorem 90. Let $H_i \coloneqq \mathrm{Gal}(K/K_i')$ and consider the endomorphism

$$\phi \coloneqq \sum_{\tau \in H_i} f(\tau)\tau_g.$$

By linear independence of automorphisms, there exists an element b in K such that $\phi(b) \neq 0$ and $\sigma_{g_k}\phi(b) = \phi(b)/f(\sigma)$. Choose c in the proposition to be $\phi(b)$. □

Define $f'_{i,j,k} \in \mathrm{C}^1(K/K'_i)$ as

$$f'_{i,j,k}(\sigma) \coloneqq \eta'_i(g_j, \sigma, g_k),$$

for $\sigma \in G_{K'}$. One can check that $f'_{i,j,k}$ satisfies the hypothesis of Proposition 6.2.8, so there exists $c_{i,j,k} \in K^\times$ such that, for $\sigma \in G_{K'}$, one has $f'_{i,j,k}(\sigma) = c_{i,j,k}/\sigma_{g_j}(c_{i,j,k})$. Let

$$\varepsilon''_i(\tau, \rho) \coloneqq \begin{cases} 1, & \text{if } \chi'_1(\tau) = \mathrm{id} \text{ or } \chi'_1(\rho) = \mathrm{id}\,, \\ \tau'(c_{i,j,k}), & \text{if } \chi'_i(\tau) = j \text{ and } \chi'_i(\rho) = k, \end{cases}$$

where $\tau' \in G_{K'_i}$ is such that $\tau = \tau' g_j$.

Proposition 6.2.9. *Let $\eta''_i \coloneqq \eta'_i - \partial\varepsilon''_i$. Then for $(\sigma, \tau, \rho) \in G_{K'_i} \times G_k \times G_k \cup G_k \times G_{K'_i} \times G_k \cup G_k \times G_k \times G_{K'_i}$, $\eta''_i(\sigma, \tau, \rho) = 1$. Furthermore, $\eta''_i \in \mathrm{Im}(\inf : \mathrm{Z}^3(K'_i/k) \to \mathrm{Z}^3(k))$.*

Proof. The proof is similar to the one of Proposition 6.2.7. □

Since K'_i/k is cyclic of degree 3, one finds ε''_i using Proposition 5.5.1. The local part of the computation also follows a similar approach as in §4.3.3. Currently, the only bottleneck we are left to tackle in explicitly computing the pairing is to compute for each place v the point $P_v \in \hat{J}(K_v)$ such that $\partial P_v = \alpha_v$. Since $\hat{\phi}(P_v) \in J(k_v)$, this reduces to obtaining an algorithm for computing a point in the preimage of the isogeny $\hat{\phi}$. We summarize the above discussion in the following theorem.

Theorem 6.2.10. *Let $a, a' \in \mathrm{S}^{(\hat{\phi})}(J/k)$ be represented by (d_1, d_2), (d'_1, d'_2), respectively. Assume that there is an oracle that for each place v computes a point in the preimage of a point under $\hat{\phi}$. Then for each place v of k, there is an algorithm to compute $\delta_{v,i}$ for $i \in \{1, 2\}$ such that*

$$\zeta_3^{3\langle a, a' \rangle_{\mathrm{CT}}} = \prod_v (\delta_{v,1}, d'_1)_{k_v} (\delta_{v,2}, d'_2)_{k_v},$$

where $(x, y)_{k_v}$ represents the cubic Hilbert symbol of $x, y \in k_v^\times$.

Let $S_{a,a'}$ be the union of the set of places v of k above 3, of the set of places of k where C or $\hat{C}$ has bad reduction, and the set of places of k where at least one value taken by ε has a non-trivial valuation. One can prove a version of Lemma 4.3.19 for the case of $(3,3)$-isogeny and show that for $v \notin S_{a,a'}$, the value of $\langle a, a' \rangle_{\mathrm{CT}} = 0$. The following is pseudocode for the algorithm mentioned in the above theorem.

Algorithm 4 Compute the CTP between $a, a' \in \mathrm{S}^{(\hat{\phi})}(\hat{J}/k)$ represented by (d_1, d_2), $(d_1', d_2') \in (k^\times)^2$.

Require: $(d_1, d_2), (d_1', d_2') \in (k^\times)^2$.
Ensure: Value of $(\zeta_3)^{\langle a, a' \rangle_{\mathrm{CT}}}$ in variable CT.

1: CT $\leftarrow 1$. ▷ Value of CT.
2: LocalPoints $\leftarrow [\ ]$. ▷ List storing P_v indexed by $v \in S_{a,a'}$.
3: **for** $v \in S_{a,a'}$ **do**
4: Find $Q_v \in J(k_v)$, such that $\delta(Q_v) = \alpha_v$. ▷ $\alpha \in \mathrm{Z}^1(G_k, \hat{J}[\hat{\phi}])$ represents a.
5: $K_v \leftarrow k_v(\sqrt[3]{d_1}, \sqrt[3]{d_2})$ and $P_v \in \hat{\phi}^{-1}(Q_v)$ such that $\partial P_v = \alpha_v$. ▷ Computed using the oracle.
6: LocalPoints$[v] \leftarrow P_v$.
7: **end for**
8: $K \leftarrow k(\sqrt[3]{d_1}, \sqrt[3]{d_2})$.
9: Compute $E_{i,1}$, $E_{i,j,1}$, $e_{i,1}$ and $e_{i,j,1}$ for $i \in \{1,2\}$ and $j \in \{1,2,3\}$ as in Proposition 6.2.5. ▷ $E_{i,k} = kE_{i,1}$ and $E_{i,j,k} = kE_{i,j,1}$. Hence, one can choose $e_{i,k} = ke_{i,1}$ and $e_{i,j,k} = ke_{i,j,1}$.
10: Compute $t_{i,j,k}$ and $c_{i,j,k}$ as in Proposition 6.2.6 and 6.2.8.
11: **for** $v \in S_{a,a'}$ **do**
12: Compute 1-cocycles $\Gamma_{i,k}(\sigma) := \gamma_{v,i}(\sigma, g_k)$ for $i \in \{1,2\}$ and $k \in \{1,2,3\}$, where $\gamma_{v,i}(\sigma, g_k) := ((\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_{i,v} - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}_{i,v} - \varepsilon_{i,v})(\sigma, g_k)$.
13: Compute $\theta_{v,i,1}$ such that $\partial\theta_{v,i,1} = \Gamma_{i,1}$.
14: Choose $\theta_{v,i,k} := \theta^k_{v,i,1}$ and compute $\delta_{v,i} \in k_v^\times$ as in the Theorem 6.2.10 using a computation similar to the one in §5.2. ▷ Note that $\partial\theta_{v,i,k} = \Gamma_{v,i,k}$.
15: CT $\leftarrow$ CT $\cdot \prod_{i=1}^{2} (\delta_{v,i}, d_i')_{k_v}$.
16: **end for**
17: **return** CT.

Chapter 7

Conclusion

It was remarked in [PS99] that the Albanese-Albanese definition of the CTP can lead to simpler computation of the pairing for Jacobian varieties, as we need to work only with the divisors on the curve. This thesis can been viewed as an attempt to do so. One of the main motivations of this thesis was to see what can be done if we completely avoid any reference to an explicit description of homogeneous spaces while computing the pairing. The 2-cocycles representing the trivial class in the Brauer group, that appeared while computing ε in various cases are in fact related to the principal homogeneous spaces represented by corresponding Selmer elements. Hence, it is definitely possible to obtain more efficient algorithms if we work with explicit equations of homogeneous spaces. In the next section we summarize what has been achieved during the course of this thesis and some generalizations that were obtained later and are not a part of this thesis. Thereafter, we see a few natural questions both of theoretical and computational nature arising from this work.

7.1 What's new

7.1.1 The CTP on 2-Selmer groups

The first problem we answer is the following.

Problem 7.1.1. Use the Albanese-Albanese definition to compute the CTP on $\mathrm{S}^{(2)}(E/k)$ for an elliptic curve E/k.

Though this is not a new result in itself, computing the pairing does provide us with insights that become useful in the higher genus cases. Using our computations along with explicit equations of curves representing the twist, we are able to obtain the same formulas as Cassels in [Cas98].

Next, we answer the following generalization to the previous problem.

Problem 7.1.2. Use the Albanese-Albanese definition to compute the CTP on $\mathrm{S}^{(2)}(J/k)$ of an odd-degree hyperelliptic Jacobian J/k.

We answer this question in Chapter 4. In essence, we show that the computation of the CTP is computationally not harder than trivializing matrix algebras, i.e., the problem of finding an explicit isomorphism $\phi : A \to M_n(k)$, given a central simple algebra A/k. This is done by showing that the 3-cocycle $\eta_1 \in \mathrm{H}^3(F/k)$ (recall the definition of F for §4.3.1) represents the trivial class, and the trivializer ε_1 is constructed via trivializing some 2-cocycles that represent the trivial class in the relative Brauer group $\mathrm{Br}(F/K')$. Abstractly, one can view this as showing that $\eta_1 = \inf^{\mathrm{Gal}(L/k)}_{\mathrm{Gal}(K'/k)}(e)$, for some $e \in \mathrm{H}^3(K'/k)$, and e is obtained via $\mathrm{tg} \circ \mathrm{res}$ on a 2-cocycle representing the trivial class in the relative Brauer group $\mathrm{Br}(L/k)$, where recall that tg is the transgression homomorphism in dimension 2. Furthermore, taking inspiration from the case of elliptic curves, in §4.4 we show that the 2-cocycles can be explicitly written as 2-coboundaries using solutions to a set of quadratic forms, and empirically show that for genus 2 curves the condition is not very strict. We use our conditional algorithm to compute the pairing in various examples.

One can view Theorem 4.2.1 and Corollary 4.3.20 as a generalization of [Cas98, Lemma 7.4]. It is important to note that we have avoided any reference to the explicit equations of homogeneous spaces represented by the 2-Selmer elements to be paired, while doing the above computations. However, using explicit descriptions of homogeneous spaces, might improve the efficiency of the algorithm significantly. In fact, in [FY23] the authors do achieve this along with using other efficient techniques, in the case of 2-Selmer groups associated to genus 2 Jacobians. However, the techniques that make their algorithm efficient are not so easily generalizable to higher genus Jacobians. To the best of my knowledge, this is the first attempt to compute the CTP on 2-Selmer groups of higher genus hyperelliptic curves.

In the following two subsections we comment on two generalizations and state some results that could be obtained but are not a part of this thesis.

The case of superelliptic curves

Let l be a prime and $f \in k[x]$ be a squarefree polynomial of degree d coprime to l. Assume that $\mu_l \subset k^\times$, and let Δ be the set of roots of f and $C \coloneqq y^l = f(x)$. Then the genus of C is $(l-1)(d-1)/2$ and as in the case of Chapter 5, the automorphism $\zeta_l : (x, y) \mapsto (x, \zeta_l y)$ induces an isogeny $\lambda \coloneqq 1 - \zeta_l$ on J_C defined over k. Let $\mathrm{N} : \mu_l^\Delta \to \mu_l$ be the norm map given by $m \mapsto \prod_{P \in \Delta} m_p$. Then the following is a split exact sequence

$$0 \to J_C[\lambda] \longrightarrow \mu_l^\Delta \xrightarrow{\mathrm{N}} \mu_l \to 1,$$

similar to §4.1. One can generalize §4.1 and §4.3.1 to show the following theorem for superelliptic curves of the above form.

Theorem 7.1.3. *Let C/k be a superelliptic curve as above, and let $A \coloneqq k[x]/\langle f(x)\rangle$ be the étale algebra corresponding to f. Let λ be the $1 - \zeta_l$ endomorphism as before,*

and denote the λ-Selmer elements a, a' by elements $z, z' \in A^\times/(A^l)^\times$, respectively. If we write $z = (z_1, \ldots, z_d)$ and similarly for z', then for each place v of k and each G_{k_v}-orbit Δ_i of Δ, there is an explicitly computable $\delta_{i,v} \in k_v(P_i)^\times$, where P_i is a representative of Δ_i, such that

$$\zeta_l^{l\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \prod_{\text{orbits}} (\delta_{i,v}, z_i')_v,$$

where $(\cdot,\cdot)_v$ is the generalized Hilbert symbol.

Remark 7.1.4. The only hurdle in computing δ_v is computing a local point $P_v \in J_C(\overline{k_v})$ such that $\partial P_v = \alpha_v$, where α_v is a 1-cocycle representing a. This is something that we will discuss in §7.2. As far as the global part of the pairing is concerned, we have an algorithm to compute ε.

When the twisted Kummer surface has a rational point

Let $a, a' \in Ш(J_C/k)[2]$, where J_C is the Jacobian of a curve of genus 2 (here we assume that the defining polynomial of the curve C is of even degree). Assume that the twisted Kummer surface $K_{a'}$ of the twist $J_{a'}$ corresponding to a' of J has a k-rational point Q. Then there is a k-rational point Q (abusing the notation slightly) on the Kummer surface $\mathcal{K}_C$ of J_C corresponding to Q. The authors in [FY23] work under this assumption and show empirically that one can expect to find twisted Kummer surfaces with a k-rational point that generate the 2-Selmer group. What we claim here is that this case can also be handled by our methods in §4.3.1.

Let $\tilde{Q}$ be a lift of Q on J_C. If $\tilde{Q}$ is defined over k. Then there is nothing to do. Therefore, we assume that $\tilde{Q}$ is defined over a quadratic extension $K' := k(\sqrt{m})$ of k. Let $P \in J_C(\bar{k})$ such that $\partial P = \mathrm{res}^{G_{K'}}_{G_k}(\alpha')$, where α' is a 1-cocycle with values in $J_C[2]$ representing P. Note that $2P = \tilde{Q}$. Let $\mathrm{Gal}(K'/k) = \langle g \rangle$. The inflation-restriction sequence at the level of 1-cocycles in dimension 1 implies that $\alpha' - \partial P \in \mathrm{Im}(\mathrm{inf}^{G_k}_{\mathrm{Gal}(K'/k)})$. In particular, if $\sigma \in G_k$ such that $\sigma\big|_{K'} = g$, then $\alpha'(\sigma) - \sigma(P) + P = Q'$, with $Q' \in J_C(K')$. Hence, one can represent a' with the following 1-cocycle

$$\alpha''(\sigma) = \begin{cases} 0, & \text{if} \quad \sigma(\sqrt{m}) = \sqrt{m}, \\ Q', & \text{if } \sigma(\sqrt{m}) = -\sqrt{m}. \end{cases}$$

α'' is a 1-cocycle implies that $g(Q') = -Q'$. At the same time, $g(\tilde{Q}) = -\tilde{Q}$, since it is a lift of a k-rational point on $\mathcal{K}_C$. Let $\sigma \in G_k$ restrict to g over K'. Then

$$2(Q' - \tilde{Q}) = 2\alpha'(\sigma) - 2\sigma(P) + 2P = 0 \Rightarrow Q' - \tilde{Q} \in J_C(K')[2].$$

In fact,

$$g(Q' - \tilde{Q}) = -(Q' - \tilde{Q}) = Q' - \tilde{Q} \Rightarrow Q' - \tilde{Q} \in J_C(k)[2].$$

One can view the above as mapping a point $Q \in \mathcal{K}_C(k)$ to a point $Q' \in Q + J_C(k)[2]$. If $J_C(k)[2] = \emptyset$ (which is the generic case), then $\tilde{Q} = Q'$. Otherwise, we need check which of the $Q' \in J_C[2](k)$ gives us a 1-cocycle α'' that is locally everywhere trivial. This is an easy check, as we only need to do it above 2, the primes of bad reduction of C, and the infinite primes. For each such place we only need to compute $R \in J_C(K'_v)$ such that $g(R) - R - Q' \in 2J_C(K'_v)$. This is because if $g(R) - R - Q' = 2Q''$, then writing $2Q'' = Q'' - g(Q'')$, $g(R + Q'') - (R + Q'') = Q'$. In particular, R can be chosen from the class $J_C(K'_v)/2J_C(K'_v)$. There are fast algorithms to compute the local group $J_C(K'_v)/2J_C(K'_v)$ due to efficient 2-Selmer group implementations (see [Sto01]).

In particular, representing a' by α'' we find ourselves in the case §4.3.1 and §4.3.3. One bypasses §4.3.2 using an analogue of Proposition 6.1.3. Up to the hurdle of computing $P_v \in J_C(k_v)$ such that $\partial P_v = \alpha_v$, we have the following theorem.

Theorem 7.1.5. *Let $a, a' \in \mathrm{S}^{(2)}(J_C/k)$ and $m \in k^\times$ be as above. Assume that there is an algorithm that for each place v of k can compute half of a point $Q_v \in 2J(k_v)$. Then, for each place v of k, there is an algorithm to compute $\delta_v \in k_v^\times$ such that*

$$(-1)^{\langle a, a' \rangle_{\mathrm{CT}}} = \prod_v (\delta_v, m)_v.$$

One can view the above as a rather inefficient generalization of [FY23] to higher genus hyperelliptic Jacobians.

7.1.2 The CTP for other isogenies

The next two chapters 5 and 6 were an attempt to compute the pairing for various isogenies including two isogenies of odd degree. To the best of our knowledge this was the first attempt to compute the CTP for any odd degree isogeny on higher genus Jacobians.

The following problem can be viewed as a special case of §7.1.1.

Problem 7.1.6. Compute the CTP on λ-Selmer group of Jacobians of the curves of the form $y^2 = x^l + A$, with $A \in \mathbb{Z}$.

We answer this question in generality. In fact, the method used to compute ε can be used to compute ε for any cyclic isogeny on a Jacobian. We show in Corollary 5.3.2 that we only need to compute the local trivializer, $P_v \in J_A(\overline{k_v})$ such that $\partial P_v = \alpha_v$, at the place λ for the l-Stoll set. In order to avoid the computation of the local trivializer P_v and compute some examples, we use an assumption that the λ-Selmer element is trivial. For $l = 5$, this is the case when the class group of $L \coloneqq \mathbb{Q}(\zeta_5, \sqrt{A})$ has 5-torsion. In, particular, for genus 2, we are able to compute the CTP whenever there are elements coming from non-trivial 5 torsion in $\mathrm{Cl}(L)$. The implementation is

done in Magma. We also implement the λ-Selmer group computation when A is an element of the l-Stoll set. This is because the in-built function `PhiSelmerGroup()`, is extremely inefficient due to its generic nature. Using the explicit local points at λ computed in [Sto98], one can significantly speed up the computation. In fact, for J_{62}, we use this to compute the algebraic rank, whereas our algorithm to compute the CTP on 2-Selmer groups in Chapter 4 seems to be inefficient.

In Chapter 6 we compute the global part of the pairing, i.e., compute ε for the Richelot and $(3,3)$-isogeny on genus 2 Jacobians. For the Richelot isogeny, we also outline an algorithm to compute the local point $P_v \in J(\overline{k_v})$ such that $\partial P_v = \alpha_v$.

7.2 Zukunftsmusik

In this section we state a few questions that arise naturally from the thesis.

7.2.1 True descent

Let k be a number field, and let C/k be a curve with Jacobian variety J/k. We recall the definition of true descent setup as defined in [BPS16].

Definition 7.2.1. A true descent setup is the data (n, Δ, D), where Δ is a finite étale k-scheme, i.e., $\Delta := \mathrm{Spec}\,(L)$ for some étale algebra L and $D \in \mathrm{Div}(C \times \Delta)$ such that $nD = \mathrm{div}(f) \in \mathrm{Princ}(C \times \Delta)$.

Hilbert's Theorem 90 implies that f can be chosen in a way that specializing f at any $P \in \Delta$ one obtains $f_P \in k(C)^\times$ in a G_k-equivariant way. As a consequence of the conditions on D and Δ one obtains a map

$$\phi : \mathrm{H}^1(G_k, J[n]) \to \mathrm{H}^1(G_k, \mu_n^\Delta) \simeq L^\times/(L^\times)^n.$$

We assume that the map ϕ above is an injection. There are non-trivial examples of the above available, e.g., p-descent on elliptic curves, 2-descent on odd-degree hyperelliptic curves, $(1-\zeta_l)$-descent on degree l-cyclic covers of $\mathbb{P}^1$ ramified at ∞.

One can ask the following question regarding computation of the CTP in a true descent setup.

Question 7.2.2. *How can one compute the CTP using the Albanese-Albanese definition on the Selmer group corresponding to a true descent setup (n, Δ, D) of a curve C?*

If a, a' are the two elements of the Selmer group being paired, then using the methods developed in §4.3.1 and Chapter 6, one obtains a 3-cocycle η' from the 3-cocycle η, that factors through the field of definition K' of 1-cocycle α' representing a'. However, our contention is that if the Selmer group is coming from a true descent

set up, then it should be possible to make choices of Hilbert's Theorem 90 elements that are required during the reduction such that η' is trivial cocycle.

For the local part of the pairing, one can ask the following question (whose answer is probably yes).

Question 7.2.3. *Let $\psi : A \to J_C$ be an isogeny of degree n. Then* [BPS16, Lemma 7.1] *implies that if v is a prime of k such that the Tamagawa numbers $c_v(A)$ and $c_v(J_C)$ are coprime to n, and residue characteristic of k_v does not divide n, then $\delta_v(J_C(k_v)) = \mathrm{H}^1(\mathrm{Gal}(k_v^{\mathrm{nr}}/k_v), A[\psi])$. Can we show an analogue of Lemma 4.3.19 for v satisfying the above condition, and also show that the values taken by ε have trivial valuation at v?*

7.2.2 Algorithmic questions

We state some natural algorithmic questions that arise from this thesis.

Problem 7.2.4. Give an algorithm to compute the CTP for 2-Selmer groups of even-degree hyperelliptic curves unconditionally.

Problem 7.2.5. Recall from §7.1.1 that one can extend the method of computing CTP in §4.3.1 to the case of p-cyclic covers of $\mathbb{P}^1$ with ramification at ∞ over k containing μ_p. However, a hurdle to obtaining an algorithm is that in the local step where one needs to find a point $P_v \in J(\overline{k_v})$ for a place v of k which witnesses the triviality of the 1-cocycle representing the $(1-\zeta_p)$-Selmer element, that algorithmically amounts to solving the following problem: Given a point Q in the image of $1-\zeta_p$, find the point P such that $(1-\zeta_p)(P) = Q$. In $p = 2$ case, Stoll in [Sto17b] gives an algorithm to compute half of a point, given that one exists. Vishal Arul in [Aru20] solves the above problem when Q is in the image of the Abel-Jacobi map.

A probably simpler problem would be to invert an element in the image of $(1-\zeta_p)$ isogeny over local fields, where the theory of formal groups is available.

The following problem is a generalization of the above.

Problem 7.2.6. Let $\psi : A \to B$ be an isogeny of abelian varieties A and B over k. Let v be a place of k and $P \in B(k_v)$. Then compute $Q \in A(\overline{k_v})$ such that $\psi(Q) = P$.

The following problem asks if we can avoid solving the above two problems while computing the CTP.

Problem 7.2.7. Write an expression for the class $c_v \in \mathrm{Br}(k_v)$ obtained during the local part of the CTP just using the local point Q_v on the abelian variety. In essence, we want something in the direction of the case of 2-Selmer groups of elliptic curves.

7.2.3 Arithmetic statistics with the CTP

It would be interesting to study if one can determine the average size of $\ker(\langle\cdot,\cdot\rangle_{\mathrm{CT}})$ on $\mathrm{S}^{(2)}(E/\mathbb{Q})$. One of the toy examples to attack is the family of elliptic curves given by the equation of the form $y^2 = x(x^2 + ax + b)$ with $a, b \in \mathbb{Z}$. This family exhibits an isogeny ϕ of degree 2, and explicit formulas for the CTP on $\mathrm{S}^{(\phi)}(E/\mathbb{Q})$ are known. The idea would be to estimate the average size of the kernel of the CTP in this case first.

Bibliography

[Aru20] Vishal Arul, *Division by $1-\zeta$ on Superelliptic Curves and Jacobians*, International Mathematics Research Notices (2020).

[Bea00] Cheryl Beaver, *5-Torsion in the ShafarevichTate Group of a Family of Elliptic Curves*, Journal of Number Theory **82** (2000), 25-46.

[BFS23] Nils Bruin, Victor E. Flynn, and Ari Shnidman, *Genus two curves with full level $\sqrt{3}$-structure and Tate-Shafarevich groups*, Selecta Math. **29** (2023), no. 42.

[BFT14] Nils Bruin, Victor E. Flynn, and Damiano Testa, *Descent via (3,3)-isogeny on Jacobians of genus 2 curves*, Acta Arithmetica **165** (2014), 201–223.

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum of Mathematics, Sigma **4** (2016), e6.

[Bro82] Kenneth S. Brown, *Cohomology of Groups*, Springer-Verlag New York, 1982.

[Cas62] J.W.S. Cassels, *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung.*, Journal für die reine und angewandte Mathematik **1962** (1962), no. 211, 95 - 112.

[Cas98] J. W. S. Cassels, *Second descents for elliptic curves*, Journal für die reine und angewandte Mathematik **1998** (1998), no. 494, 101– 127.

[CF96] J.W.S. Cassels and Victor E. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996.

[CFO+08] J. E Cremona, T. A Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves, I. Algebra*, Journal für die reine und angewandte Mathematik **2008** (2008), no. 615, 121–155, DOI doi:10.1515/CRELLE.2008.012.

[Cor] David Corwin, *From Chabauty's method to Kim's non-abelian Chabauty's method.* available at https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf (downloaded on May 16, 2024).

[DGH21] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger, *Uniformity in Mordell-Lang for curves*, Ann. Math. **194** (2021), 237–298.

[EvdHT21] Tim Evink, Gert-Jan van der Heiden, and Jaap Top, *Two-descent on some genus two curves*, Indagationes Mathematicae (2021).

[Fie09] Claus Fieker, *Minimizing representations over number fields II: Computations in the Brauer group*, Journal of Algebra **322** (2009), 752-765.

[Fis22] Tom Fisher, *On binary quartics and the Cassels-Tate pairing*, Res. Number Theory **8** (2022), no. 74.

[Fla90] Matthias Flach, *A generalisation of the Cassels-Tate pairing.*, Journal für die reine und angewandte Mathematik **1990** (1990), 113 - 127.

[Fly94] Victor E. Flynn, *Descent via isogeny in dimension 2*, Acta Arithmetica **66** (1994), 23–43.

[FN14] Tom Fisher and Rachel Newton, *Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve*, International Journal of Number Theory **10** (2014), no. 07, 1881-1907.

[FSS10] Tom Fisher, Edward F. Schaefer, and Michael Stoll, *The yoga of the Cassels-Tate pairing*, LMS Journal of Computation and Mathematics **13** (2010), 451-460.

[FvB18] Tom Fisher and Monique van Beek, *Computing the Cassels-Tate pairing on 3-isogeny Selmer groups via cubic norm equations*, Acta Arithmetica **185** (2018), no. 4, 367–396.

[FY23] Tom Fisher and Jiali Yan, *Computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian*, 2023. Preprint available at https://arxiv.org/abs/2306.06011.

[Har77] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag New York, 1977.

[HS00] Marc Hindry and Joseph Silverman, *Diophantine Geometry*, Springer-Verlag New York, 2000.

[Jac96] Nathan Jacobson, *Finite-Dimensional Division Algebras over Fields*, Springer Berlin, Heidelberg, 1996.

[KRZB15] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank*, Duke Mathematical Journal **165** (2015), 3189-3240.

[Lan83] Serge Lang, *Abelian Varieties*, Springer-Verlag New York, 1983.

[LMF24] LMFDB, *The L-functions and modular forms database*, 2024. [Online; accessed 2 April 2024].

[Moo] Ben Moonen, *Abelian Varieties*. Draft of book on abelian varieties.

[Neu99] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag New York, 1999.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/NSW2.3.pdf. MR2392026

[Pan21] Anurag Pandey, *Variety Membership Testing in Algebraic Complexity Theory(Doctoral thesis)*, Universität des Saarlandes, 2021. (downloaded on May 16, 2024).

[Pat24] Ross Paterson, *The Failure of Galois Descent for p-Selmer Groups of Elliptic Curves*, Mathematical Proceedings of the Cambridge Philosophical Society **177** (2024), no. 1, 185218.

[Poo17] Bjorn Poonen, *Rational Points on Varieties*, Vol. 186, American Mathematical Society, 2017.

[Pre13] Thomas Preu, *Effective lifting of 2-cocycles for Galois cohomology*, Open Mathematics **11** (2013), no. 12, 2138–2149, DOI doi:10.2478/s11533-013-0319-4.

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, Journal für die reine und angewandte Mathematik **1997** (1997), 141 - 188.

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate Pairing on Polarized Abelian Varieties*, Annals of Mathematics **150** (1999), no. 3, 1109–1149.

[Sch96] Edward F. Schaefer, *Class Groups and Selmer Groups*, Journal of Number Theory **56** (1996), no. 1, 79-114.

[SD13] Peter Swinnerton-Dyer, 2^n*-descent on elliptic curves for all* n, Journal of the London Mathematical Society **87** (2013), no. 3, 707-723.

[Ser79] J.P. Serre, *Local Fields*, Springer-Verlag New York, 1979.

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag New York, 2009.

[Smi05] Benjamin Smith, *Explicit endomorphisms and correspondences (Doctoral thesis)*, University of Sydney, 2005.

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-Descent on an Elliptic Curve*, Transactions of the American Mathematical Society **356** (2004), no. 3, 1209–1231.

[SS23] Himanshu Shukla and Michael Stoll, *The Cassels-Tate pairing on 2-Selmer groups of elliptic curves*, 2023. Preprint available at https://arxiv.org/abs/2302.01640 (downloaded on May 16, 2024).

[Sto] Michael Stoll, *Arithmetic of Hyperelliptic curves*. Lecture notes available at https://mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2019/Skript-ArithHypCurves-pub-screen.pdf (downloaded on May 16, 2024).

[Sto98] ———, *On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians*, Journal für die reine und angewandte Mathematik **1998** (1998), 171-189.

[Sto01] ———, *Implementing 2–descent for Jacobians of hyperelliptic curves*, Acta Arithmetica **98** (2001), 245–277.

[Sto06] ———, *Independence of rational points on twists of a given curve*, Compositio Math. **142** (2006), 1201–1214.

[Sto12] Michael Stoll, *Descent on Elliptic Curves*, Panoramas et Synthèses **36** (2012), 151–179.

[Sto17a] Michael Stoll, *Selmer Groups and Descent*, 2017. Lecture notes from Workshop on Curves and L-functions, Trieste; available at https://people.maths.bris.ac.uk/~matyd/Trieste2017/Stoll.pdf (downloaded on May 16, 2024).

[Sto17b] ———, *Chabauty Without the Mordell-Weil Group*, Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, 2017, pp. 623–663.

[Sto19] ———, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, J. Eur. Math. Soc. **21** (2019), no. 3, 923–956.

[SvL13] Michael Stoll and Ronald van Luijk, *Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$*, Acta. Arith. **159** (2013), 133–14.

[Tat63] John Tate, *Duality theorems in Galois cohomology of number fields*, Proceedings of International Congress for Mathematicians (Stockholm) 1963, 1963, pp. 288–295.

[Wei38] André Weil, *Generalization of abelian functions*, J. Math. Pure Appl. (9) **17** (1938), 47–87.

[Yan21a] Jiali Yan, *Computing the Cassels-Tate Pairing for Genus Two Jacobians with Rational Two Torsion Points*, 2021. Preprint available at https://arxiv.org/abs/2109.08258 (downloaded on May 16, 2024).

[Yan21b] ———, *Computing the Cassels-Tate Pairing for Jacobian Varieties of Genus Two Curves (Doctoral thesis)*, University of Cambridge, 2021.

Index

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die von mir angegebenen Quellen und Hilfsmittel verwendet habe.

Weiterhin erkläre ich, dass ich die Hilfe von gewerblichen Promotionberatern bzw. -vermittlern oder ähnlichen Dienstleistern weder bisher in Anspruch genommen habe, noch künftig in Anspruch nehmen werde.

Zusätzlich erkläre ich hiermit, dass ich keinerlei frühere Promotionsversuche unternommen habe.

Bayreuth, den

Himanshu Shukla