

# Class Groups and Selmer Groups


EDWARD F. SCHAEFER

*Santa Clara University, Department of Mathematics, Santa Clara, California 95053*

*Communicated by K. Rubin*

Received May 19, 1994

... metadata, citation and similar papers at [core.ac.uk](http://core.ac.uk)

brought to you by  CORE

provided by Elsevier - Publisher Connector

their intersection. In this paper we compute the two groups and their intersection explicitly in the local case and put together the local information to get sharp upper bounds in the global case. The techniques in this paper can be used for arbitrary abelian varieties, isogenies and number fields assuming a frequently occurring condition. Several examples are worked out for the Jacobians of elliptic and hyperelliptic curves. © 1996 Academic Press, Inc.

## 1. INTRODUCTION

It has been known for some time that a Selmer group of an abelian variety and a group related to an ideal class group can often be embedded into the same cohomology group. Ideally, the images of the two groups are almost the same and we can compute one from the other. In order to do this we need to find how close the intersection is to each of the groups. In the past, this has been done for special cases of elliptic curves and with the Jacobians of Fermat curves. Using techniques from Galois cohomology, we will see that we can do this in much greater generality.

Let  $A$  and  $A'$  be abelian varieties of the same dimension  $g$ , defined over  $K$ , an algebraic number field, and let  $\phi$  be a  $K$ -defined isogeny from  $A$  onto  $A'$  (see Cornell and Silverman [6], Lang [12] or Mumford [18] as general references on abelian varieties and Silverman [27] for elliptic curves). The field  $L$ , which is the minimal field of definition of the points in  $A[\phi]$ , the kernel of  $\phi$ , is Galois over  $K$ . If  $H^1(\text{Gal}(L/K), A[\phi])$  is trivial, then the Selmer group  $S^\phi(K, A)$  can be embedded into the group  $\text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi])$  (see Section 2 for a description of these objects). Consider the subgroup of the homomorphism group of homomorphisms that factor through the Galois group of a totally unramified extension of  $L$ ; call this group  $C^\phi(K, A)$ . From class field

theory, this group is related to the ideal class group of  $L$ . Denote by  $I^\phi(K, A)$  the intersection of the group  $C^\phi(K, A)$  and the Selmer group. We would like to compute  $S^\phi(K, A)/I^\phi(K, A)$  and  $C^\phi(K, A)/I^\phi(K, A)$  as accurately as possible so as to relate the groups  $S^\phi(K, A)$  and  $C^\phi(K, A)$ . We do this with local computations.

Let  $\mathfrak{p}$  be a prime of  $K$  and  $K_{\mathfrak{p}}$  be the completion of  $K$  at that prime. Denote by  $S^\phi(K_{\mathfrak{p}}, A)$  the group  $A'(K_{\mathfrak{p}})/\phi A(K_{\mathfrak{p}})$ . We shall assume that  $H^1(G, A[\phi])$  is trivial for all  $G \subseteq \text{Gal}(L/K)$ . This condition occurs frequently and we will see some examples in section 5. Under this assumption we can embed  $S^\phi(K_{\mathfrak{p}}, A)$  into the group  $\text{Hom}_{G(LK_{\mathfrak{p}}/K_{\mathfrak{p}})}(\text{Gal}(\overline{LK}_{\mathfrak{p}}/LK_{\mathfrak{p}}), A[\phi])$ . Let  $C^\phi(K_{\mathfrak{p}}, A)$  be the subgroup of the homomorphism group of homomorphisms that factor through the Galois group of an unramified extension of  $LK_{\mathfrak{p}}$ . Denote by  $I^\phi(K_{\mathfrak{p}}, A)$  the intersection of the groups  $C^\phi(K_{\mathfrak{p}}, A)$  and  $S^\phi(K_{\mathfrak{p}}, A)$ .

Under the assumption that  $H^1(G, A[\phi]) = 0$  for all  $G \subseteq \text{Gal}(L/K)$ , we have the following injections of groups

$$S^\phi(K, A)/I^\phi(K, A) \hookrightarrow \prod_{\mathfrak{p}} S^\phi(K_{\mathfrak{p}}, A)/I^\phi(K_{\mathfrak{p}}, A)$$

$$C^\phi(K, A)/I^\phi(K, A) \hookrightarrow \prod_{\mathfrak{p}} C^\phi(K_{\mathfrak{p}}, A)/I^\phi(K_{\mathfrak{p}}, A)$$

where  $\mathfrak{p}$  ranges over the primes of  $K$ . We will show in Section 4 that for each finite prime  $\mathfrak{p}$  of  $K$  that does not divide the conductor of  $A$  or the degree of  $\phi$ , the groups  $S^\phi(K_{\mathfrak{p}}, A)$ ,  $I^\phi(K_{\mathfrak{p}}, A)$ ,  $C^\phi(K_{\mathfrak{p}}, A)$  and  $A(K_{\mathfrak{p}})[\phi]$  are isomorphic.

We will also see along the way that the orders of the groups  $S^\phi(K_{\mathfrak{p}}, A)$ ,  $C^\phi(K_{\mathfrak{p}}, A)$ , and  $I^\phi(K_{\mathfrak{p}}, A)$  can often be easily computed. Computing the sizes of  $S^\phi(K_{\mathfrak{p}}, A)$  and  $C^\phi(K_{\mathfrak{p}}, A)$  is standard. The substantial contribution here is the computation of  $I^\phi(K_{\mathfrak{p}}, A)$  where  $\mathfrak{p}$  is a finite prime that divides the conductor of  $A$ . This is the computation that has caused others trouble in the past. For elliptic curves, these computations are greatly facilitated by the algorithm of Tate [28]. These injections then give us upper bounds on the index of the group  $I^\phi(K, A)$  in the Selmer group and the group related to the ideal class group. We are most interested when the intersection is close to each of the groups, because then we can often compute one group from the other or at least bound the size of one given the size of the other.

Selmer groups hold key information about the group of rational points of an abelian variety over an algebraic number field, known as the Mordell–Weil group. Since neither Mordell–Weil groups nor class groups are well understood currently, any connection between them is helpful. On the lighter side, part of the lore of number theory is that high-rank elliptic

curves can produce record-breaking class groups. The practicalities of this were first worked out by Mestre [15]. Several papers have appeared recently where techniques were presented for computing one of these groups from the other. Eisenbeis, Frey and Ommerborn [7] studied elliptic curves of the form  $Y^2 = X^3 + k$  over  $\mathbf{Q}$  with the multiplication by 2 map (from now on the 2-map) and the 2-rank of the class groups of pure cubic fields. The same curves have a rational 3-isogeny, and Satgé [22] and Quer [20] have studied these and the 3-rank of the class groups of quadratic fields. Washington [30] studied the 2-map for curves of the form  $Y^2 = X^3 + mX^2 - (m+3)X + 1$  over  $\mathbf{Q}$  and the 2-rank of the class groups of the simplest cubic fields (see Cohn [5] or Shanks [26]). Brumer and Kramer [4] produced techniques for computing the connection in a more general domain. They studied the 2-map and cubic extensions for elliptic curves, defined over number fields that are unramified over  $\mathbf{Q}$  at 2, at primes of good or multiplicative reduction. McCallum [14] has studied the Jacobians of the  $p$ th Fermat curves and quotients of Fermat curves using  $p$ -isogenies and the  $p$ -part of the class group of  $\mathbf{Q}(\zeta_p)$ .

In the following we produce techniques that work in far greater generality. In Section 2 we give a global description of the Selmer group and the group related to an ideal class group. In Section 3 we present results that are useful for computing these groups and their intersection over local fields. In Section 4 we put these local results together to get upper bounds for the index of the global intersection in the Selmer group and in the group related to an ideal class group. In Section 5 we closely analyze the 2-map. We first give criteria for the cohomological triviality of  $J[2]$  as a  $\text{Gal}(L/K)$ -module where  $J$  is the Jacobian of a hyperelliptic curve. When  $J[2]$  is cohomologically trivial we can relate  $C^2(K, J)$  to the 2-parts of the class groups of a collection of subfields of  $L$ . We finish this section by presenting three examples. In the first example we show how to use a curve of Mestre's to produce a non-cyclic cubic extension of the rationals whose class group has 2-rank at least 13. Then we look at the Jacobian of a hyperelliptic curve whose 2-torsion is defined over a simplest quintic field and whose Mordell–Weil rank over the rationals is 7. Lastly, we see that the group related to the ideal class group is not always contained in the Selmer group as it seems to be in all published examples.

## 2. SELMER GROUPS AND CLASS GROUPS

Let  $K$  be a number field; this shall always mean that  $K$  is a finite extension of  $\mathbf{Q}$ . Let  $A$  and  $A'$  be abelian varieties defined over  $K$  of the same dimension  $g$  and let  $\phi$  be a  $K$ -defined isogeny of  $A$  onto  $A'$ . Let  $\text{Gal}(\bar{K}/K)$

denote the absolute Galois group of  $K$ . By taking  $\text{Gal}(\bar{K}/K)$ -invariants of the groups in the short exact sequence

$$0 \rightarrow A[\phi] \rightarrow A(\bar{K}) \xrightarrow{\phi} A'(\bar{K}) \rightarrow 0$$

we obtain the following long exact sequence. The symbol  $[\phi]$  after a group denotes its subgroup sent to 0 by  $\phi$ , and the expression  $H^1(K, M)$  denotes  $H^1(\text{Gal}(\bar{K}/K), M)$  for some  $\text{Gal}(\bar{K}/K)$ -module  $M$ .

$$0 \rightarrow A(K)[\phi] \rightarrow A(K) \xrightarrow{\phi} A'(K) \rightarrow H^1(K, A[\phi]) \rightarrow H^1(K, A(\bar{K})) \xrightarrow{\phi} \dots$$

This gives us the short exact sequence

$$0 \rightarrow A'(K)/\phi A(K) \rightarrow H^1(K, A[\phi]) \rightarrow H^1(K, A(\bar{K}))[\phi] \rightarrow 0.$$

See Atiyah and Wall [2] as a reference on group cohomology.

Let  $\mathfrak{p}$  be a prime of  $K$ , finite or infinite, and  $K_{\mathfrak{p}}$  be the completion of  $K$  at the prime  $\mathfrak{p}$ . For each prime  $\mathfrak{p}$  of  $K$  we obtain similar short exact sequences

$$0 \rightarrow A[\phi] \rightarrow A(\bar{K}_{\mathfrak{p}}) \xrightarrow{\phi} A'(\bar{K}_{\mathfrak{p}}) \rightarrow 0$$

and

$$0 \rightarrow A'(K_{\mathfrak{p}})/\phi A(K_{\mathfrak{p}}) \rightarrow H^1(K_{\mathfrak{p}}, A[\phi]) \rightarrow H^1(K_{\mathfrak{p}}, A(\bar{K}_{\mathfrak{p}}))[\phi] \rightarrow 0.$$

Since the group  $\text{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$  is isomorphic to a decomposition group for  $\mathfrak{p}$  in  $\text{Gal}(\bar{K}/K)$ , we can restrict cocycles in  $\text{Gal}(\bar{K}/K)$  to cocycles in  $\text{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ . This induces the restriction map

$$H^1(K, A[\phi]) \rightarrow H^1(K_{\mathfrak{p}}, A[\phi]).$$

We present the following commutative diagram in order to define the  $\phi$ -Selmer group for  $A$  over  $K$

$$\begin{array}{ccccccc} 0 & \longrightarrow & A'(K)/\phi A(K) & \longrightarrow & H^1(K, A[\phi]) & \longrightarrow & H^1(K, A(\bar{K}))[\phi] \longrightarrow 0 \\ & & \downarrow & & \downarrow & \searrow \beta & \downarrow \\ 0 & \longrightarrow & \prod_{\mathfrak{p}} A'(K_{\mathfrak{p}})/\phi A(K_{\mathfrak{p}}) & \longrightarrow & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, A[\phi]) & \longrightarrow & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, A(\bar{K}_{\mathfrak{p}}))[\phi] \longrightarrow 0 \end{array}$$

where  $\mathfrak{p}$  ranges over the primes of  $K$ . The  $\phi$ -Selmer group for  $A$  over  $K$  is the kernel of  $\beta$  and is denoted  $S^{\phi}(K, A)$ . The Selmer group clearly contains  $A'(K)/\phi A(K)$ .

The group of rational points  $A(K)$ , is often called the Mordell–Weil group; it is a finitely generated abelian group. Since the torsion of an abelian variety is computable, one could find the free  $\mathbf{Z}$ -rank of  $A(K)$  if one

could compute the group  $A(K)/nA(K)$  for some integer  $n$  greater than 1. So one often takes  $\phi$  to be a multiplication by  $n$  map. If  $\phi$  is a map from  $A'$  to  $A$  and  $\phi'$  is a map from  $A'$  to  $A$  with the property that  $\phi' \circ \phi = [n]$  then the following is an exact sequence of groups

$$0 \rightarrow \frac{A'(K)[\phi']}{\phi(A(K)[n])} \rightarrow \frac{A'(K)}{\phi A(K)} \xrightarrow{\phi'} \frac{A(K)}{nA(K)} \rightarrow \frac{A(K)}{\phi' A'(K)} \rightarrow 0.$$

If one could compute  $A'(K)/\phi A(K)$  and  $A(K)/\phi' A'(K)$ , then one could compute  $A(K)/nA(K)$ . There is no known algorithm to effectively compute the group  $A'(K)/\phi A(K)$  however. A Selmer group is the closest known approximation to  $A'(K)/\phi A(K)$  that is effectively computable, which is why they were originally of interest.

The field  $L$ , which is the minimal field of definition of the points in  $A[\phi]$ , is Galois over  $K$ . Restricting cocycles in  $H^1(K, A[\phi])$  to the subgroup  $\text{Gal}(\bar{L}/L)$  induces the following exact sequence of groups, called an inflation-restriction sequence

$$0 \rightarrow H^1(\text{Gal}(L/K), A[\phi]) \rightarrow H^1(K, A[\phi]) \rightarrow \text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi])$$

where  $\text{Hom}_{G(L/K)}$  denotes the  $\text{Gal}(L/K)$ -invariant homomorphisms. Assuming that  $H^1(\text{Gal}(L/K), A[\phi])$  is trivial, we have

$$H^1(K, A[\phi]) \hookrightarrow \text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi]).$$

We also assume that  $H^1(G, A[\phi])$  is trivial for all groups  $G$  contained in  $\text{Gal}(L/K)$ , so for each prime  $\mathfrak{p}$  of  $K$  we also have

$$H^1(K_{\mathfrak{p}}, A[\phi]) \hookrightarrow \text{Hom}_{G(LK_{\mathfrak{p}}/K_{\mathfrak{p}})}(\text{Gal}(\overline{LK}_{\mathfrak{p}}/LK_{\mathfrak{p}}), A[\phi]).$$

Let  $m$  be the exponent of  $A[\phi]$  and let  $\text{Cl}(L)$  denote the ideal class group of  $L$ . From class field theory, the dual of the group  $\text{Cl}(L)/\text{Cl}(L)^m$  is naturally isomorphic to the group  $\text{Hom}(\text{Gal}(H(L)/L), \mathbf{Z}/m\mathbf{Z})$  where  $H(L)$  is the maximal unramified abelian extension of  $L$ , its Hilbert class field. The group  $C^{\phi}(K, A)$  is the subgroup of  $\text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi])$  of homomorphisms that factor through the Galois group of a totally unramified extension of  $L$ . This subgroup is isomorphic to the group  $\text{Hom}_{G(L/K)}(\text{Gal}(H(L)/L), A[\phi])$  and so it is related to the group  $\text{Cl}(L)/\text{Cl}(L)^m$ . We will describe this relation for the 2-map and the Jacobians of hyperelliptic curves in Theorem 5.3. We will call any homomorphism that factors through the Galois group of a totally unramified extension an unramified homomorphism.

The group  $S^{\phi}(K, A)$  is the group of all elements of  $\text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi])$  that map to the image of  $A'(K_{\mathfrak{p}})/\phi A(K_{\mathfrak{p}})$  for all primes  $\mathfrak{p}$  of  $K$ . The

group  $C^\phi(K, A)$  is the group of all elements that map to unramified homomorphisms in  $\text{Hom}_{G(LK_p/K_p)}(\text{Gal}(\overline{LK_p}/LK_p), A[\phi])$  for all primes  $p$  of  $K$  since  $L$  is normal over  $K$ . These groups are the same locally for almost all primes, as we will see in the next section.

### 3. LOCAL COMPUTATIONS

In this section we describe the group  $A'(K_p)/\phi A(K_p)$ , the group of unramified homomorphisms in  $\text{Hom}_{G(LK_p/K_p)}(\text{Gal}(\overline{LK_p}/LK_p), A[\phi])$  and the subgroup of  $A'(K_p)/\phi A(K_p)$  that maps to unramified homomorphisms. If  $H^1(G, A[\phi]) = 0$  for all  $G \subseteq \text{Gal}(L/K)$  then these are the groups  $S^\phi(K_p, A)$ ,  $C^\phi(K_p, A)$  and  $I^\phi(K_p, A)$ . However, we will lift the restriction that  $H^1(G, A[\phi]) = 0$  for all  $G \subseteq \text{Gal}(L/K)$  until we discuss infinite primes. Since all computations will be local, and subscripts are annoying, we will omit them. We deal with finite primes first.

Let  $A$  and  $A'$  be abelian varieties of the same dimension  $g$  defined over  $K$ , the completion of a number field at a finite prime. Let  $\phi$  be an isogeny from  $A$  onto  $A'$  that is defined over  $K$ . Again define  $L$  to be the field  $K(A[\phi])$ .

From the short exact sequence

$$0 \rightarrow A[\phi] \rightarrow A \rightarrow A' \rightarrow 0$$

we obtain the following injection of groups by taking  $\text{Gal}(\overline{K}/K)$ -invariants

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

From the restriction map from cohomology there is a homomorphism

$$H^1(K, A[\phi]) \rightarrow \text{Hom}_{G(L/K)}(\text{Gal}(\overline{L}/L), A[\phi]).$$

We are first interested in describing the group of unramified homomorphisms in  $\text{Hom}_{G(L/K)}(\text{Gal}(\overline{L}/L), A[\phi])$  and the subgroup of  $A'(K)/\phi A(K)$  that maps to those unramified homomorphisms.

**LEMMA 3.1.** *The subgroup of unramified homomorphisms in  $\text{Hom}_{G(L/K)}(\text{Gal}(\overline{L}/L), A[\phi])$  is isomorphic to the group  $A(K)[\phi]$ .*

*Proof.* Let  $L^{\text{unr}}$  be the maximal unramified extension of  $L$  in the given algebraic closure. The group  $\text{Hom}(\text{Gal}(L^{\text{unr}}/L), A[\phi])$  is isomorphic to the group  $A[\phi]$  by the map  $f \mapsto f(\text{Frob}_L)$ . This map respects the  $\text{Gal}(L/K)$ -action on each module. Taking  $\text{Gal}(L/K)$ -invariants of both groups provides the result. ■

Now let us consider the subgroup of  $A'(K)/\phi A(K)$  that maps to unramified homomorphisms. We still need not assume that  $H^1(G, A[\phi]) = 0$  for  $G \subseteq \text{Gal}(L/K)$ . The connecting homomorphism from cohomology sends  $P \in A'(K)$  to the class of cocycles in  $H^1(K, A[\phi])$  consisting of cocycles  $\xi$  where  $\xi(\sigma) = \sigma Q - Q$  for  $\sigma \in \text{Gal}(\bar{K}/K)$  and  $Q \in A$  where  $\phi Q = P$ . The point  $P$  maps to an unramified homomorphism if and only if its inverse images under the map  $\phi$  are all defined over an unramified extension of  $L$ . Since  $L = K[A[\phi]]$ , if one is defined over an unramified extension of  $L$ , then they all are. Let  $A(K)[\phi]$  have exponent  $m$ . From the previous lemma, it is clear that if  $P$  maps to an unramified homomorphism, then these preimages will be defined over the unramified extension of  $L$  of degree  $m$ .

Let  $L'$  be the maximal unramified subextension of  $L$  over  $K$ . Let  $M$  be the unramified extension of  $L'$  of degree  $m$  and let  $\tau$  generate  $\text{Gal}(M/K)$ . The field  $ML$  is the unramified extension of  $L$  of degree  $m$ . These fields are displayed in Fig. 1.

LEMMA 3.2. *Let the group  $H^1(\text{Gal}(L/L'), A[\phi])$  be trivial. Let  $Q \in A(ML)$  and assume  $\phi Q = P$ , where  $P \in A'(K)$ . There exists a  $Q' \in A(M)$  such that  $\phi Q' = P$ .*

*Proof.* Since  $H^1(\text{Gal}(L/L'), A[\phi])$  is trivial, so is  $H^1(\text{Gal}(ML/M), A[\phi])$ . Thus  $H^1(M, A[\phi])$  injects into  $H^1(ML, A[\phi])$  and so  $A'(M)/\phi A(M)$  injects into  $A'(ML)/\phi A(ML)$ . So if  $P$  is in  $\phi A(ML)$  then  $P$  is in  $\phi A(M)$ . ■

LEMMA 3.3. *The elements of  $A(M)[\phi]$  are in the kernel of the norm from  $M$  to  $K$ .*

*Proof.* If  $T \in A(M)[\phi]$  then  $T \in A(L')[\phi]$ . Since  $N_{L'/K}(A(L')[\phi]) \subseteq A(K)[\phi]$ , it is clear that  $N_{M/K} = m \cdot N_{L'/K}$  on  $A(M)[\phi]$ . Since  $m$  is the exponent of  $A(K)[\phi]$ , all of  $A(M)[\phi]$  is in the kernel of  $N_{M/K}$ . ■

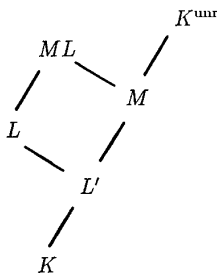


FIG. 1. Subfield diagram.

**THEOREM 3.4.** *Let  $K$  be the completion of a number field at a finite prime and let  $\phi$  be a  $K$ -defined isogeny from  $A$  to  $A'$ , which are  $K$ -defined abelian varieties. Let  $L = K(A[\phi])$  and let  $L'$  be the maximal unramified extension of  $K$  contained in  $L$ . Let  $m$  be the exponent of  $A(K)[\phi]$ , and  $M$  be the unramified extension of  $L'$  of degree  $m$  and  $\tau$  generate  $\text{Gal}(M/K)$ . Assume that the group  $H^1(\text{Gal}(L/L'), A[\phi])$  is trivial. The subgroup of  $A'(K)/\phi A(K)$  that maps to unramified homomorphisms in  $\text{Hom}_{\text{Gal}(\bar{L}/L)}(\text{Gal}(\bar{L}/L), A[\phi])$  is isomorphic to the following group*

$$\frac{A(M)[\phi] \cap (\tau - 1) A(M)}{(\tau - 1)A(M)[\phi]}$$

by the map  $P \mapsto \tau Q - Q$  where  $P \in A'(K)$ ,  $Q \in A(M)$  and  $\phi Q = P$ .

*Proof.* We chose  $M$  to have degree  $m$  over  $L'$  so that  $ML$  is the unramified extension of  $L$  of degree  $m$ . A point  $P$  in  $A'(K)$  maps to the homomorphism  $\sigma \mapsto \sigma(\phi^{-1}(P)) - \phi^{-1}(P)$  in  $\text{Hom}(\text{Gal}(\bar{L}/L), A[\phi])$ . A point  $P$  maps to an unramified homomorphism if the preimages,  $\phi^{-1}(P)$ , are defined over  $ML$ . From Lemma 3.2, such a point has a preimage defined over  $M$ . Therefore the subgroup of  $A'(K)/\phi A(K)$  that maps to unramified homomorphisms is  $(\phi A(M) \cap A'(K))/\phi A(K)$ . From the short exact sequence

$$0 \rightarrow A(M)[\phi] \rightarrow A(M) \xrightarrow{\phi} \phi A(M) \rightarrow 0.$$

we obtain the following exact sequence by taking  $\text{Gal}(M/K)$ -invariants

$$\begin{aligned} 0 \rightarrow (\phi A(M) \cap A'(K))/\phi A(K) &\rightarrow H^1(\text{Gal}(M/K), A(M)[\phi]) \\ &\xrightarrow{\gamma} H^1(\text{Gal}(M/K), A(M)). \end{aligned}$$

Since  $\text{Gal}(M/K)$  is cyclic, generated by  $\tau$ , we have

$$H^1(\text{Gal}(M/K), A(M)[\phi]) \cong \frac{\ker N_\tau: A(M)[\phi] \rightarrow A(M)[\phi]}{(\tau - 1) A(M)[\phi]}.$$

From Lemma 3.3, all of  $A(M)[\phi]$  is in the kernel of the norm. The subgroup of  $A'(K)/\phi A(K)$  that maps to unramified homomorphisms is isomorphic to the kernel of  $\gamma$  by the map  $P \mapsto \tau Q - Q$  where  $P \in \phi A(M) \cap A'(K)$ ,  $Q \in A(M)$  and  $\phi Q = P$ . The kernel of  $\gamma$  is the group of elements that map to coboundaries in  $H^1(\text{Gal}(M/K), A(M))$ . So the kernel of  $\gamma$  is isomorphic to

$$\frac{A(M)[\phi] \cap (\tau - 1) A(M)}{(\tau - 1)A(M)[\phi]}. \quad \blacksquare$$



Let us refer to this group as the intersection quotient. Because of the proof, the theorem holds when replacing  $M$  by any unramified extension of  $M$ . Notice that if all of  $A(M)[\phi]$  is contained in  $(\tau - 1)(A(M))$ , then the intersection quotient has the same order as  $A(K)[\phi]$  and so has the same order as the group of unramified homomorphisms.

Let us discuss the computation of the intersection quotient. The group  $A(M)[\phi]$  and the action of  $\tau$  on it should be easy to find. So we need to find which elements of  $A(M)[\phi]$  are in  $(\tau - 1)(A(M))$ . The following two lemmas bring this problem from the infinite to the finite as the group  $A(M)/A_0(M)$  is finite. Let  $NA$  be the Néron model of  $A$  over  $\mathcal{O}$ , the ring of integers in  $M$ . Define  $NA^0$  to be the open subgroup scheme of  $NA$  whose generic fiber is isomorphic to  $A$  over  $M$  and whose special fiber is the identity component of the closed fiber of  $NA$ . The group  $NA^0(\mathcal{O})$  is isomorphic to a subgroup of  $A(M)$  which we are denoting by  $A_0(M)$ .

LEMMA 3.5. *The groups  $H^i(\text{Gal}(M/K), A_0(M))$  are trivial for all  $i$ .*

*Proof.* In [17], Milne shows that if  $W$  is the completion of a number field at a finite prime, then  $H^i(\text{Gal}(W^{\text{unr}}/W), A_0(W^{\text{unr}}))$  is trivial for all  $i \geq 1$  where  $W^{\text{unr}}$  is the maximal unramified extension of  $W$  in a given algebraic closure of  $W$ . Since the Néron model is stable under unramified base extensions (see [1, p. 214]), we know that as  $M$  is an unramified extension of  $K$ , that the set of  $\text{Gal}(K^{\text{unr}}/M)$ -invariants of  $A_0(K^{\text{unr}})$  is  $A_0(M)$ . This is not necessarily the case otherwise. Since  $M^{\text{unr}} = K^{\text{unr}}$ , we have  $H^i(\text{Gal}(K^{\text{unr}}/M), A_0(K^{\text{unr}})) = 0$  for all  $i \geq 1$ . From [2, Prop. 5], it follows that the sequence

$$\begin{aligned} 0 \rightarrow H^i(\text{Gal}(M/K), A_0(M)) &\xrightarrow{\text{inf}} H^i(\text{Gal}(K^{\text{unr}}/K), A_0(K^{\text{unr}})) \\ &\xrightarrow{\text{res}} H^i(\text{Gal}(K^{\text{unr}}/M), A_0(K^{\text{unr}})) \end{aligned}$$

is exact and we are done. ■

LEMMA 3.6. *A point  $T$  of  $A(M)[\phi]$  is in  $(\tau - 1)(A(M))$  if and only if the image of  $T$  in  $A(M)/A_0(M)$  is in  $(\tau - 1)(A(M)/A_0(M))$ .*

*Proof.* We have the following short exact sequence of  $\text{Gal}(M/K)$ -modules

$$0 \rightarrow A_0(M) \rightarrow A(M) \rightarrow A(M)/A_0(M) \rightarrow 0.$$

We take  $\text{Gal}(M/K)$ -invariants and see from Lemma 3.5 that  $H^i(\text{Gal}(M/K), A_0(M))$  is trivial for all  $i$ . So we have

$$H^1(\text{Gal}(M/K), A(M)) \cong H^1(\text{Gal}(M/K), A(M)/A_0(M)).$$

Since  $\text{Gal}(M/K)$  is cyclic, each of these groups is isomorphic to the kernel of the norm modulo the image of  $(\tau - 1)$  on the appropriate Galois-module. From Lemma 3.3, the elements of  $A(M)[\phi]$  are in the kernel of the norm from  $M$  to  $K$ . The result follows from the fact that the image of  $T$  is trivial in one group if and only if it is trivial in the other. ■

We see that points in  $A(M)[\phi]$  (which equals  $A(L')[\phi]$ ) that are in  $A_0(M)$  are automatically in  $(\tau - 1)(A(M))$ . For points of  $A(M)[\phi]$  that are not in  $A_0(M)$  one must determine which have images that are in  $(\tau - 1)(A(M)/A_0(M))$ .

For elliptic curves, the possible groups  $E(M)/E_0(M)$  have been completely determined by the classification of Kodaira [11] and Néron [19]. If we take for  $E$  a minimal Weierstrass model, then the group  $E_0(M)$  is the subgroup of points of  $E(M)$  with non-singular reduction. In the following theorem we present an algorithm for determining if a point  $P$  in  $E(M)[\phi]$  with singular reduction is in  $(\tau - 1)(E(M))$ . This is accomplished in conjunction with Tate's algorithm [28]. We must first determine whether or not  $\tau$  acts non-trivially on  $E(M)/E_0(M)$ . If it does, then in most cases it is simply a matter of determining whether or not  $2 \mid \#\text{Gal}(L'/K)$  or if the image of  $P$  in  $E(M)/E_0(M) \cong \mathbf{Z}/n\mathbf{Z}$  is even.

**THEOREM 3.7.** *Let  $E$  be defined by a minimal Weierstrass equation over  $K$  and let  $\phi$  be a  $K$ -defined isogeny from  $E$  onto  $E'$ . Let  $L' = K(E[\phi]) \cap K^{\text{unr}}$ , let  $M$  be a finite unramified extension of  $L'$  and  $\tau$  generate  $\text{Gal}(M/K)$ . A point  $P$  in  $E(L')[\phi]$  with singular reduction will be in  $(\tau - 1)(E(M))$  in exactly the following cases. Otherwise it will not be in  $(\tau - 1)(E(M))$ .*

1.  $E$  has type  $I_v$  reduction (multiplicative) with  $v$  odd,  $\tau$  acts as  $-1$  on  $E(M)/E_0(M)$  and  $2 \mid \#\text{Gal}(L'/K)$ .

2.  $E$  has type  $I_v$  reduction with  $v$  even,  $\tau$  acts as  $-1$  on  $E(M)/E_0(M)$  and the image of  $P$  in  $E(M)/E_0(M) \cong \mathbf{Z}/v\mathbf{Z}$  is even.

3.  $E$  has type  $IV$  or  $IV^*$  reduction,  $\tau$  acts as  $-1$  on  $E(M)/E_0(M)$  and  $2 \mid \#\text{Gal}(L'/K)$ .

4.  $E$  has type  $I_v^*$  reduction with  $v$  odd,  $\tau$  acts as  $-1$  on  $E(M)/E_0(M)$  and the image of  $P$  in  $E(M)/E_0(M) \cong \mathbf{Z}/4\mathbf{Z}$  is 2.

5.  $E$  has type  $I_v^*$  reduction with  $v$  even (including  $v=0$ ), and either the action of  $\tau$  on  $E(M)/E_0(M)$  has order 2 and fixes  $P$  modulo  $E_0(M)$  or the action of  $\tau$  on  $E(M)/E_0(M)$  has order 3.

*Proof.* See Néron [19] or Tate [28] as a reference on the reduction types. Since  $E$  is given by a minimal Weierstrass equation, the points of

non-singular reduction are the same as the points of  $E_0$ . Let  $E$  have type  $I_\nu$  reduction (multiplicative) over  $K$ . The group  $E(K^{\text{unr}})/E_0(K^{\text{unr}})$  is isomorphic to the cyclic group of  $\nu$  components of the special fiber of the minimal regular projective 2-dimensional scheme  $\mathcal{E}$  whose generic fiber is isomorphic over  $K$  to  $E$ . The scheme  $\mathcal{E}$  is the minimal model for  $E$  as a curve, not as a group variety. The minimal model for  $E$  as a group variety is the Néron minimal model (see [27, p. 358]). The components form a loop with each component crossing the two adjacent components. The group  $\text{Gal}(K^{\text{unr}}/K)$  acts on the group of components and preserves its structure. Therefore, the group  $\text{Gal}(K^{\text{unr}}/K)$  must act as  $\pm 1$ . When  $\text{Gal}(K^{\text{unr}}/K)$  acts as  $+1$ , then  $E$  is said to have split multiplicative reduction over  $K$  and  $E(K)/E_0(K) \cong \mathbf{Z}/\nu\mathbf{Z}$ . When  $\text{Gal}(K^{\text{unr}}/K)$  acts as  $-1$ , then  $E$  is said to have non-split multiplicative reduction over  $K$  and  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z}$  when  $\nu$  is even and  $E(K)/E_0(K)$  is trivial when  $\nu$  is odd. If  $\nu$  is odd and  $E(K)/E_0(K) \neq 0$  then  $E(K)/E_0(K) \cong \mathbf{Z}/\nu\mathbf{Z} \cong E(M)/E_0(M)$  and so  $\tau$  acts trivially on  $E(M)/E_0(M)$ . Therefore  $P$  cannot be in the image of  $\tau - 1 = 0$ . If  $\nu$  is odd and  $E(K)/E_0(K) = 0$  but 2 does not divide  $\#\text{Gal}(L'/K)$ , then  $E(L')/E_0(L') = 0$  and so there is no  $P$ . When  $\nu$  is odd and  $E(K)/E_0(K) = 0$  and 2 divides  $\#\text{Gal}(L'/K)$ , we have  $E(L')/E_0(L') \cong \mathbf{Z}/\nu\mathbf{Z}$ . Since  $\tau$  acts as  $-1$ ,  $\tau - 1$  acts as multiplication by  $-2$  and so all points of  $E(L')$  are in the image of  $\tau - 1$ .

If  $\nu$  is even and  $E(K)/E_0(K) \not\cong \mathbf{Z}/2\mathbf{Z}$  then  $E(K)/E_0(K) \cong \mathbf{Z}/\nu\mathbf{Z} \cong E(M)/E_0(M)$  and so  $\tau$  acts trivially on  $E(M)/E_0(M)$ . If  $\nu \equiv 2 \pmod{4}$ ,  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z}$  and 2 does not divide  $\#\text{Gal}(L'/K)$ , then  $E(L')/E_0(L') \cong \mathbf{Z}/2\mathbf{Z}$ . If 2 does not divide  $\#\text{Gal}(M/L')$  either then  $E(M)/E_0(M) \cong \mathbf{Z}/2\mathbf{Z}$  and  $\tau$  acts trivially. Even if 2 divides  $\#\text{Gal}(M/L')$  then the image of  $\tau - 1$  will be points whose image in  $E(M)/E_0(M) \cong \mathbf{Z}/\nu\mathbf{Z}$  are even. The point  $P$  being in  $E(L')/E_0(L') \cong \mathbf{Z}/2\mathbf{Z}$ , will have image  $\frac{1}{2}\nu$  in  $\mathbf{Z}/\nu\mathbf{Z}$  which is odd so it is not in the image of  $\tau - 1$ . When 2 divides  $\#\text{Gal}(L'/K)$ , we have  $E(L')/E_0(L') \cong \mathbf{Z}/\nu\mathbf{Z}$ . Since  $\tau$  acts as  $-1$ , the points whose images in  $E(L')/E_0(L') \cong \mathbf{Z}/\nu\mathbf{Z}$  are even are in the image of  $\tau - 1$ . If  $\nu \equiv 0 \pmod{4}$ ,  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z}$ , and 2 does not divide  $\#\text{Gal}(M/K)$ , then  $E(M)/E_0(M) \cong \mathbf{Z}/2\mathbf{Z}$  and  $\tau$  acts trivially. If 2 divides  $\#\text{Gal}(M/K)$ , but 2 does not divide  $\#\text{Gal}(L'/K)$ , then  $E(L')/E_0(L') \cong \mathbf{Z}/2\mathbf{Z}$  and so  $2P$  has non-singular reduction. Notice that since  $\tau - 1$  acts as multiplication by  $-2$ , that  $P$  is in the image of  $\tau - 1$ . When 2 divides  $\#\text{Gal}(L'/K)$ , we have  $E(L')/E_0(L') \cong \mathbf{Z}/\nu\mathbf{Z}$ . Thus the elements of  $E(L')[\phi]$  whose images in  $E(M)/E_0(M) \cong \mathbf{Z}/\nu\mathbf{Z}$  are even are in the image of  $\tau - 1$ .

Let  $E$  have type  $II$  or  $II^*$  reduction. The group  $E(K^{\text{unr}})/E_0(K^{\text{unr}})$  is trivial so  $E(M)/E_0(M)$  is also and so there could not be a  $P$ . Let  $E$  have type  $III$  or  $III^*$  reduction. The group  $E(K^{\text{unr}})/E_0(K^{\text{unr}})$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z}$ . Since the automorphism group of  $\mathbf{Z}/2\mathbf{Z}$  is trivial, we see that the action of  $\tau$  is trivial.

Let  $E$  have type  $IV$  or  $IV^*$  reduction. The group  $E(K^{\text{unr}})/E_0(K^{\text{unr}})$  is isomorphic to  $\mathbf{Z}/3\mathbf{Z}$ . The automorphism group of  $\mathbf{Z}/3\mathbf{Z}$  is isomorphic to  $\mathbf{Z}/3\mathbf{Z}^*$ . If  $E(K)/E_0(K) \neq 0$  then  $E(K)/E_0(K) \cong E(M)/E_0(M)$  and so  $\tau$  acts trivially. If  $E(K)/E_0(K) = 0$  and 2 does not divide  $\#\text{Gal}(L'/K)$  then there is no  $P$ . When  $E(K)/E_0(K) = 0$  and 2 divides  $\#\text{Gal}(L'/K)$  we have a  $P$  defined over  $L'$  and  $\tau - 1$  acts as an automorphism on  $E(M)/E_0(M)$  and so  $P$  is in the image of  $\tau - 1$ .

Let  $E$  have type  $I_v^*$  reduction. If  $v$  is odd then we have  $E(K^{\text{unr}})/E_0(K^{\text{unr}}) \cong \mathbf{Z}/4\mathbf{Z}$ . The automorphism group of  $\mathbf{Z}/4\mathbf{Z}$  is isomorphic to  $\mathbf{Z}/4\mathbf{Z}^*$ . Therefore  $E(K)/E_0(K)$  has 2 or 4 elements. If  $E(K)/E_0(K) \cong \mathbf{Z}/4\mathbf{Z}$ , then  $E(K)/E_0(K) \cong E(M)/E_0(M)$  and so  $\tau$  acts trivially. If  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z}$ , then  $P \in E(L')[\phi]$  is in the image of  $\tau - 1$  if  $2P$  has non-singular reduction and 2 divides  $\#\text{Gal}(M/K)$ .

If  $v$  is even, then we have  $E(K^{\text{unr}})/E_0(K^{\text{unr}}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . When  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ , we have  $E(K)/E_0(K) \cong E(M)/E_0(M)$  and so  $\tau$  acts trivially. When  $E(K)/E_0(K) \cong \mathbf{Z}/2\mathbf{Z}$  the action of  $\text{Gal}(K^{\text{unr}}/K)$  on  $E(M)/E_0(M)$  has order 2. Therefore,  $P$  could only be in the image of  $\tau - 1$  if  $\tau$  fixes  $P$  modulo  $E_0(M)$  and 2 divides  $\#\text{Gal}(M/K)$ . When  $E(K)/E_0(K) = 0$ , the action of  $\text{Gal}(K^{\text{unr}}/K)$  on  $E(M)/E_0(M)$  has order 3. There will be no  $P$  unless 3 divides  $\#\text{Gal}(L'/K)$ . If that is the case, then  $\tau - 1$  is an automorphism on  $E(M)/E_0(M)$  and so all points  $P$  of  $E(L')$  will be in the image of the map  $\tau - 1$ . ■

Using the algorithm of Tate, one can quickly determine the reduction type of  $E$  over  $K$  and compute the group  $E(K)/E_0(K)$ . As we will see in examples in Section 5.2, it is easy to determine the action of  $\tau$  on  $E(M)/E_0(M)$ . So in practice, it is easy to determine which elements of  $E(M)[\phi]$  are in the image of the map  $\tau - 1$  on  $E(M)$ . So for elliptic curves, we have an algorithm for computing the size of the intersection quotient.

At this point we compute the order of the group  $A'(K)/\phi A(K)$ . Now let  $\mathcal{O}$  be the ring of integers in  $K$ . For  $i \geq 1$  there is a natural homomorphism

$$NA^0(\mathcal{O}) \rightarrow NA^0(\mathcal{O}/\mathfrak{p}^i)$$

where we use  $\mathfrak{p}$  to denote the maximal ideal in  $\mathcal{O}$ . The kernel of this homomorphism is often denoted  $NA^i(\mathcal{O})$  and it is isomorphic to a subgroup of the group  $A_0(K)$  which we shall denote by  $A_i(K)$ . If  $p$  is the characteristic of the residue class field of  $K$ , then the group  $A_1(K)$  is a pro- $p$ -group which is isomorphic to the underlying group of a formal group (see [17, p. 56]).

There is some  $m$  such that for all  $n \geq m$ , the groups  $A_n(K)$  and  $A'_n(K)$  are isomorphic, as the underlying groups of formal groups, to the product of  $g$  copies of the additive group of  $\mathcal{O}$  where  $g$  is the dimension of  $A$  and of

$A'$  (see [13]). As  $\phi$  is a  $K$ -defined isogeny of algebraic groups we can write  $\phi$  as a  $g$ -tuple of power series in  $g$ -variables in some neighborhoods  $A_l(K)$  and  $A'_l(K)$  of the 0-points for some  $l \geq m$ . If  $k$  is in  $K$ , then let  $|k|$  be its normalized absolute value, by which if  $\pi$  is a prime element of  $K$  and  $q$  is the order of the residue class field we have  $|\pi| = q^{-1}$ . Let  $|\phi'(0)|$  be the normalized absolute value of the determinant of the Jacobian matrix of partials of  $\phi$  evaluated at the 0-point. The value of  $|\phi'(0)|$  does not depend on the choice of parameters.

LEMMA 3.8. *The order of the group  $A'(K)/\phi A(K)$  is*

$$\frac{|\phi'(0)|^{-1} \cdot \# A(K)[\phi] \cdot \# A'(K)/A'_0(K)}{\# A(K)/A_0(K)}$$

*Proof.* From the snake lemma, we have the following commutative diagram

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & A(K)[\phi] & \longrightarrow & H_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_l(K) & \longrightarrow & A(K) & \longrightarrow & A(K)/A_l(K) & \longrightarrow & 0 \\ & & \downarrow \phi & & \downarrow \phi & & \downarrow \phi & & \\ 0 & \longrightarrow & A'_l(K) & \longrightarrow & A'(K) & \longrightarrow & A'(K)/A'_l(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & \longrightarrow & A'_l(K)/\phi A_l(K) & \longrightarrow & A'(K)/\phi A(K) & \longrightarrow & H_2 & \longrightarrow & 0 \end{array}$$

with  $l$  as above. So we have

$$\begin{aligned} \# A'(K)/\phi A(K) &= \# A(K)[\phi] \cdot \# A'_l(K)/\phi A_l(K) \cdot \frac{\# H_2}{\# H_1} \\ &= \# A(K)[\phi] \cdot \# A'_l(K)/\phi A_l(K) \cdot \frac{\# A'(K)/A'_l(K)}{\# A(K)/A_l(K)}. \end{aligned}$$

Let us first compute  $\# A'_l(K)/\phi A_l(K)$ . Fix isomorphisms of  $A_l(K)$  and  $A'_l(K)$  with  $\mathcal{O}^g$ . Let  $\mu_A$  be the Haar measure on  $A_m(K)$  which is induced by the product of the Haar measures on  $\mathcal{O}$  which have the property that  $\mu(\mathcal{O}) = 1$  and  $\mu(\mathfrak{p}^i) = |\pi|^i$  for  $i \geq 0$ . Define  $\mu_{A'}$  similarly. The isogeny  $\phi$  extends

to a morphism of the Néron models which respects the maps from  $NA(\mathcal{O})$  to  $NA(\mathcal{O}/\mathfrak{p}^n)$  and also these maps for  $A'$ . We have

$$\int_{A'_l(K)} d\mu_{A'} = \int_{A_l(K)} d\mu_A = \int_{\phi A_l(K)} |\phi'(0)|^{-1} d\mu_{A'} = |\phi'(0)|^{-1} \int_{\phi A_l(K)} d\mu_{A'}.$$

If  $H \subseteq G$  are subgroups of  $A'_m(K)$  then  $[G:H] = \mu_{A'}(G)/\mu_{A'}(H)$ . Therefore

$$\# A'_l(K)/\phi A_l(K) = |\phi'(0)|^{-1}.$$

Now let us compute  $\# A(K)/A_l(K)$  and also for  $A'$ . For all  $i \geq 1$  the quantities  $\# A_i(K)/A_{i+1}(K)$ ,  $\# A'_i(K)/A'_{i+1}(K)$  and  $q^g$  are the same. Since  $A$  and  $A'$  are isogenous, we also have  $\# A_0(K)/A_1(K)$  equals  $\# A'_0(K)/A'_1(K)$ . Therefore the quotient of  $\# A'(K)/A'_l(K)$  by  $\# A(K)/A_l(K)$  equals the quotient of  $\# A'(K)/A'_0(K)$  by  $\# A(K)/A_0(K)$ . ■

If  $A$  and  $A'$  are elliptic curves  $E$  and  $E'$ , then one can use Tate's algorithm to compute the orders of  $E'(K)/E'_0(K)$  and  $E(K)/E_0(K)$ . The quantity  $|\phi'(0)|^{-1}$  is simply the leading coefficient of the power series representation of  $\phi$ . We can compute that using the following method. First write  $\phi$  explicitly as coordinate functions  $\phi(x, y) = (x', y')$  (see [29]). Then make the substitutions  $z = -x/y$  and  $z' = -x'/y'$  and start to write  $z'$  as a power series in  $z$  (see [27, Chapt. IV]).

For arbitrary abelian varieties, if the residue characteristic  $p$  does not divide the degree of the isogeny, then  $|\phi'(0)|$  is 1, since the neighborhoods of the 0-points are pro- $p$ -groups. This follows from the last equation in the above proof. If  $A$  has good reduction over  $K$  then  $A(K) = A_0(K)$  and also  $A'(K) = A'_0(K)$ . If  $A$  does not have good reduction over  $K$  then it is not always the case that the size of  $A(K)/A_0(K)$  is equal to the size of  $A'(K)/A'_0(K)$ . As an example, let  $E$  be the elliptic curve defined by the equation  $Y^2 = X^3 - 189X + 1269$  over  $\mathbf{Q}_{31}$  and let  $\phi$  be the rational 3-isogeny gotten by dividing out by the 0-point and the points  $(3, \pm 27)$ . The discriminant of  $E$  is  $\Delta_E = -2^4 \cdot 3^{12} \cdot 31$ . This curve has split multiplicative reduction over  $\mathbf{Q}_{31}$ . The order of the group  $E(\mathbf{Q}_{31})/E_0(\mathbf{Q}_{31})$  is the same as the valuation of the discriminant for curves of split multiplicative reduction. So the order of the group  $E(\mathbf{Q}_{31})/E_0(\mathbf{Q}_{31})$  is 1. The curve  $E' = E/E[\phi]$  has Weierstrass equation  $Y^2 = X^3 + 1431X - 12339$ . This curve has discriminant  $\Delta_{E'} = -2^4 \cdot 3^{12} \cdot 31^3$  and also has split multiplicative reduction over  $\mathbf{Q}_{31}$ . Thus the order of the group  $E'(\mathbf{Q}_{31})/E'_0(\mathbf{Q}_{31})$  is 3.

The size of the group  $A'(K)/\phi A(K)$  is much easier to compute if  $\phi$  is a multiplication by  $n$  map because then we can take  $A = A'$ .

**PROPOSITION 3.9.** *If  $K$  is a finite extension of  $\mathbf{Q}_p$  and  $A$  has dimension  $g$  and if  $r = \text{ord}_p(n)$  then  $\# A(K)/nA(K) = p^{gr[K:\mathbf{Q}_p]} \cdot \# A(K)[n]$ .*

*Proof.* Let  $A_m(K)$  be isomorphic to  $\mathcal{O}^g$ . Then we have

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A(K)[n] & \longrightarrow & H_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & A_m(K) & \longrightarrow & A(K) & \longrightarrow & A(K)/A_m(K) \longrightarrow 0 \\
 & & \downarrow [n] & & \downarrow [n] & & \downarrow [n] \\
 0 & \longrightarrow & A_m(K) & \longrightarrow & A(K) & \longrightarrow & A(K)/A_m(K) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & \longrightarrow & A_m(K)/nA_m(K) & \longrightarrow & A(K)/nA(K) & \longrightarrow & H_2 \longrightarrow 0.
 \end{array}$$

It is clear that  $H_1$  and  $H_2$  have the same size and that  $\# A_m(K)/nA_m(K) = p^{gr[K: \mathbb{Q}_p]}$ . ■

To close this section, let us discuss what happens for the completion of a number field at an infinite prime.

**LEMMA 3.10.** *Let  $K$  be the completion of a number field at an infinite prime. Let  $\phi$  be a  $K$ -defined isogeny from  $A$  onto  $A'$ , abelian varieties which are defined over  $K$ . Let  $L = K(A[\phi])$  and  $H^1(\text{Gal}(L/K), A[\phi]) = 0$ . The group of unramified homomorphisms in  $\text{Hom}_{\text{Gal}(\bar{L}/L)}(\text{Gal}(\bar{L}/L), A[\phi])$  is trivial. If  $K \cong \mathbb{C}$  then  $A'(K)/\phi A(K) = 0$ . If  $K \cong \mathbb{R}$  and the degree of  $\phi$  is odd, then  $A'(K)/\phi A(K) = 0$ . If  $K \cong \mathbb{R}$  and there are points of  $A[\phi]$  that are not defined over  $\mathbb{R}$  then  $A'(K)/\phi A(K) = 0$ . Otherwise  $A'(K)/\phi A(K)$  has exponent 2 and we have  $\# A'(K)/\phi A(K) \leq 2^g$ .*

*Proof.* Since  $\mathbb{R}$  and  $\mathbb{C}$  have no non-trivial unramified extensions, the only homomorphism from  $\text{Gal}(\bar{L}/L)$  to  $A[\phi]$  which is unramified is the trivial homomorphism. If  $K \cong \mathbb{C}$  then  $\phi$  maps onto  $A'(K)$  so  $A'(K)/\phi A(K) = 0$ . Let  $K \cong \mathbb{R}$ . If the degree of  $\phi$  is odd, then  $A'(K)/\phi A(K)$  embeds into  $H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), A[\phi])$  which is trivial since  $[\mathbb{C}: \mathbb{R}]$  is coprime to the order of  $A[\phi]$  (see [2, p. 105]). If there are points of  $A[\phi]$  that are not defined over  $\mathbb{R}$  then  $L \cong \mathbb{C}$  and so  $H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), A[\phi])$  is trivial by assumption.

The only other case is that  $K \cong \mathbb{R}$ , the degree of  $\phi$  is even and all of the points of  $A[\phi]$  are defined over  $\mathbb{R}$ . We would like to show that  $A'(\mathbb{R})$  has at most  $2^g$  components. Let  $\mathbb{C}^g$  denote the tangent space to  $A'(\mathbb{C})$  at the 0-point of  $A'(\mathbb{C})$ . Since  $A'$  is defined over  $\mathbb{R}$  there is a  $2g$ -dimensional lattice  $A$  fixed by the action of  $\text{Gal}(\mathbb{C}/\mathbb{R})$  with  $A'(\mathbb{C})$  isomorphic to the quotient of  $\mathbb{C}^g$  by  $A$  (see [21]). We can look at this as an exact sequence of  $\text{Gal}(\mathbb{C}/\mathbb{R})$ -modules

$$0 \rightarrow A \rightarrow \mathbb{C}^g \rightarrow A'(\mathbb{C}) \rightarrow 0.$$

By taking  $\text{Gal}(\mathbf{C}/\mathbf{R})$ -invariants, we get the following exact sequence of groups, where  $\mathbf{R}^g$  denotes the tangent space to  $A'(\mathbf{R})$  at its 0-element.

$$0 \rightarrow A \cap \mathbf{R}^g \rightarrow \mathbf{R}^g \rightarrow A'(\mathbf{R}) \rightarrow H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) \rightarrow 0.$$

Since  $H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), \mathbf{C}^g) = 0$  (see [25, p. 152]), we get a 0 at the right end of that exact sequence. Let  $\sigma$  generate  $\text{Gal}(\mathbf{C}/\mathbf{R})$ . We have

$$H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) \cong \frac{\ker(\sigma + 1): A \rightarrow A}{(\sigma - 1)A}.$$

Now the kernel of  $\sigma + 1$  on  $\mathbf{C}^g$  is a  $g$ -dimensional vector space over  $\mathbf{R}$  so the kernel of  $\sigma + 1$  on  $A$  is a lattice of dimension  $g$ . Since 2 annihilates the cohomology group (see [2, p. 105]), the cohomology group has size at most  $2^g$ . The image of  $\mathbf{R}^g$  is connected, so  $A'(\mathbf{R})$  has at most  $2^g$  components.

The isogeny  $\phi$  takes components onto components and so the size of the group  $A'(\mathbf{R})/\phi A(\mathbf{R})$  is at most  $2^g$ . The group  $A'(\mathbf{R})/\phi A(\mathbf{R})$  embeds into  $H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A[\phi])$  which 2 annihilates, so  $A'(\mathbf{R})/\phi A(\mathbf{R})$  has exponent 2. ■

If  $A$  and  $A'$  are elliptic curves  $E$  and  $E'$ , then we can compute the size of  $E'(K)/\phi E(K)$  exactly. If  $K \cong \mathbf{R}$  we can write down a Weierstrass equation of the form  $Y^2 = f$  where  $f \in \mathbf{R}[X]$ . The discriminant of the Weierstrass equation is 16 times the discriminant of  $f$ . If  $f$  has 3 real roots then these discriminants are positive. If  $f$  has 2 imaginary roots then these discriminants are negative. When the discriminant is positive we can write down a Weierstrass equation of the form  $Y^2 = (X - a)(X - b)(X - c)$  where  $a, b, c$  are real and  $a < b < c$ .

**PROPOSITION 3.11.** *Let  $K$  be the completion of a number field at an infinite prime. Let  $E$  and  $E'$  be elliptic curves defined over  $K$  and let  $\phi$  be a  $K$ -defined isogeny of  $E$  onto  $E'$ . Let  $L = K(E[\phi])$  and  $H^1(\text{Gal}(L/K), E[\phi]) = 0$ . The group  $E'(K)/\phi E(K)$  is trivial unless  $K \cong \mathbf{R}$ , the degree of  $\phi$  is even, all of the points of  $E[\phi]$  are defined over  $K$  and we are in one of the following cases when the group will have order 2.*

- The discriminant of  $E$  is negative.
- The discriminant of  $E$  is positive and the 2-torsion point  $(a, 0)$  is contained in  $E[\phi]$ .

*Proof.* The only thing left to do after the proof of Lemma 3.10 is show the size of the group  $E'(K)/\phi E(K)$  in the case that  $K \cong \mathbf{R}$ , the degree of  $\phi$  is even and all of the points of  $E[\phi]$  are defined over  $K$ . To ease notation we will say that  $K = \mathbf{R}$ .



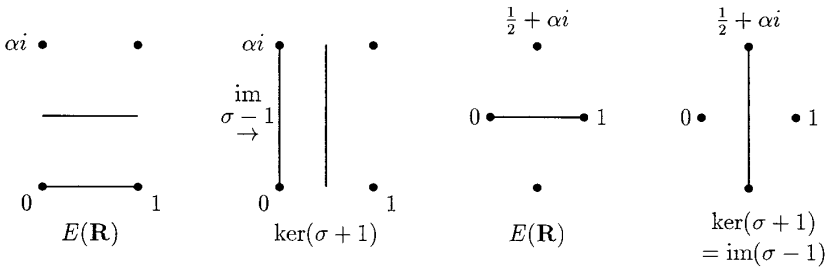


FIG. 2.  $E$  as a quotient of the complex plane.

Since  $E$  is defined over  $\mathbf{R}$ , the group of points of  $E$  over the complex numbers is isomorphic to the complex numbers modulo a lattice generated by 1 and  $\alpha i$  when ( $\Delta_E > 0$ ) or  $1/2 + \alpha i$  (when  $\Delta_E < 0$ ) where  $\alpha$  is a positive real number (see [27, Chap. VI]).

In the first case,  $E(\mathbf{R})$  is made up of two components with imaginary parts 0 and  $\alpha/2$  in the given fundamental domain. In the second case,  $E(\mathbf{R})$  is the subgroup of the given fundamental domain with imaginary part 0; see Fig. 2. We have the following exact sequence

$$0 \rightarrow E'(\mathbf{R})/\phi E(\mathbf{R}) \rightarrow H^1(\mathbf{R}, E[\phi]) \rightarrow H^1(\mathbf{R}, E(\mathbf{C}))[\phi] \rightarrow 0.$$

Let  $\sigma$  generate  $\text{Gal}(\mathbf{C}/\mathbf{R})$  and let the discriminant of  $E$  be positive. On  $E(\mathbf{C})$ , the kernel of the norm,  $\sigma + 1$ , has two components, the set of points with real part  $1/2$  and the set of points with real part 0. The image of  $\sigma - 1$  is just the set of points with real part 0. Thus the group  $H^1(\mathbf{R}, E(\mathbf{C}))$  has order 2 and is generated by the component with real part  $1/2$ . To determine the order of  $H^1(\mathbf{R}, E(\mathbf{C}))[\phi]$ , we just need to check whether or not an element of the kernel of  $\phi$  is on the component with real part  $1/2$ . The points in the kernel of  $\phi$  are all in  $E(\mathbf{R})$  and the points of  $E(\mathbf{R})$  intersect the component with real part  $1/2$  only at 2-torsion points. Therefore if there is a 2-torsion point in  $E[\phi]$  with real part  $1/2$ , then all of  $H^1(\mathbf{R}, E(\mathbf{C}))$  is  $\phi$ -torsion. By graphing  $E(\mathbf{R})$  we see that the 2-torsion point  $(c, 0)$  is on the component of  $E(\mathbf{R})$  that includes the identity and so maps to the point  $1/2$  in the fundamental domain. A quick computation with 2-isogenies (see [27, p. 74]) shows that by dividing out  $E$  by the subgroup generated by the 2-torsion point  $(b, 0)$ , that the quotient curve has negative discriminant, and so the point  $(b, 0)$  must map to the point  $(1 + \alpha i)/2$ . Therefore the point  $(a, 0)$  must map to the point  $\alpha i/2$ . If all of  $E[2]$  is contained in  $E[\phi]$  then the points  $(b, 0)$  and  $(c, 0)$  are in  $E[\phi]$  so the group  $H^1(\mathbf{R}, E(\mathbf{C}))[\phi]$  has order 2. The group  $H^1(\mathbf{R}, E[\phi]) = \text{Hom}(\text{Gal}(\mathbf{C}/\mathbf{R}), E[\phi])$  will have order 4 so the group  $E'(\mathbf{R})/\phi E(\mathbf{R})$  will have order 2. If  $E[2]$  is not contained in  $E[\phi]$  then the group

$H^1(\mathbf{R}, E[\phi])$  will have order 2. If the non-trivial 2-torsion point in  $E[\phi]$  is  $(a, 0)$  then the group  $H^1(\mathbf{R}, E(\mathbf{C}))[\phi]$  will be trivial and have order 2 otherwise. Therefore the group  $E'(\mathbf{R})/\phi E(\mathbf{R})$  will have order 2 if  $(a, 0)$  is the 2-torsion point in  $E[\phi]$  and will be trivial otherwise.

If the discriminant is negative, then we see that the kernel of  $\sigma + 1$  on  $E(\mathbf{C})$  is the same as the image of  $\sigma - 1$ ; it is the subgroup of the fundamental domain with real part equal to  $1/2$ . Thus the group  $H^1(\mathbf{R}, E(\mathbf{C}))[\phi]$  is trivial. Since the discriminant of  $E$  is negative, the group  $E(\mathbf{R})[2]$  has order 2 so the group  $H^1(\mathbf{R}, E[\phi])$  has order 2. Therefore  $E'(\mathbf{R})/\phi E(\mathbf{R})$  has order 2.

#### 4. GLOBAL COMPUTATIONS

In this section we will bring together the local results from the previous section to prove a theorem giving upper bounds for the index of the global intersection in the Selmer group and in the group related to an ideal class group. Let  $A$  and  $A'$  be abelian varieties of the same dimension  $g$ , defined over  $K$ , an algebraic number field, and let  $\phi$  be a  $K$ -defined isogeny from  $A$  onto  $A'$ . Let  $L$  be the minimal field of definition of the points in  $A[\phi]$  and assume that  $H^1(G, A[\phi])$  is trivial for all  $G \subseteq \text{Gal}(L/K)$ . Let  $S^\phi(K, A)$  be the  $\phi$ -Selmer group of  $A$  over  $K$ . Let  $C^\phi(K, A)$  be the subgroup of unramified homomorphisms in  $\text{Hom}_{G(L/K)}(\text{Gal}(\bar{L}/L), A[\phi])$  and let  $I^\phi(K, A)$  be the intersection of  $C^\phi(K, A)$  and  $S^\phi(K, A)$ .

Let  $\mathfrak{p}$  be a prime of  $K$ . Denote by  $S^\phi(K_\mathfrak{p}, A)$  the group  $A'(K_\mathfrak{p})/\phi A(K_\mathfrak{p})$ . Let  $C^\phi(K_\mathfrak{p}, A)$  be the subgroup of unramified homomorphisms in  $\text{Hom}_{G(LK_\mathfrak{p}/K_\mathfrak{p})}(\text{Gal}(\overline{LK}_\mathfrak{p}/LK_\mathfrak{p}), A[\phi])$  and let  $I^\phi(K_\mathfrak{p}, A)$  be the intersection of  $S^\phi(K_\mathfrak{p}, A)$  and  $C^\phi(K_\mathfrak{p}, A)$ .

Fix  $\mathfrak{p}$ , a finite prime, and let  $m_\mathfrak{p}$  be the exponent of the group  $A(K_\mathfrak{p})[\phi]$ . Denote by  $M_\mathfrak{p}$  the intersection of the maximal unramified extension of  $K_\mathfrak{p}$  and the unramified extension of  $LK_\mathfrak{p}$  of degree  $m_\mathfrak{p}$ . The extension  $M_\mathfrak{p}/K_\mathfrak{p}$  is unramified and so the group  $\text{Gal}(M_\mathfrak{p}/K_\mathfrak{p})$  is cyclic which we shall say is generated by  $\tau_\mathfrak{p}$ .

Let  $NA$  and  $NA'$  be the Néron models of  $A$  and  $A'$  over  $\mathcal{O}$ , the ring of integers in  $K_\mathfrak{p}$ . Define  $NA^0$  to be the open subgroup scheme of  $NA$  whose generic fiber is isomorphic to  $A$  over  $K_\mathfrak{p}$  and whose special fiber is the identity component of the closed fiber of  $NA$ . The group  $NA^0(\mathcal{O})$  is isomorphic to a subgroup of  $A(K_\mathfrak{p})$  which we shall denote by  $A_0(K_\mathfrak{p})$ ; define  $A'_0$  similarly. If we compare at the 0-points of  $A$  and  $A'$ , then  $\phi$  can be written as a  $g$ -tuple of power series in  $g$  variables. Let  $|\phi'(0)|$  be the normalized absolute value of the determinant of the Jacobian matrix of partials for  $\phi$  evaluated at the 0-point.

**THEOREM 4.1.** *Let  $H^1(G, A[\phi]) = 0$  for all  $G \subseteq \text{Gal}(L/K)$ . We have the following injections of groups*

$$S^\phi(K, A)/I^\phi(K, A) \hookrightarrow \prod_{\mathfrak{p}} S^\phi(K_{\mathfrak{p}}, A)/I^\phi(K_{\mathfrak{p}}, A)$$

$$C^\phi(K, A)/I^\phi(K, A) \hookrightarrow \prod_{\mathfrak{p}} C^\phi(K_{\mathfrak{p}}, A)/I^\phi(K_{\mathfrak{p}}, A)$$

where  $\mathfrak{p}$  ranges over the primes of  $K$ . For each finite prime  $\mathfrak{p}$  of  $K$  that does not divide the conductor of  $A$  or the degree of  $\phi$ , the groups  $S^\phi(K_{\mathfrak{p}}, A)$ ,  $I^\phi(K_{\mathfrak{p}}, A)$ ,  $C^\phi(K_{\mathfrak{p}}, A)$  and  $A(K_{\mathfrak{p}})[\phi]$  are isomorphic.

The group  $C^\phi(K_{\mathfrak{p}}, A)$  is trivial if  $\mathfrak{p}$  is infinite, and isomorphic to  $A(K_{\mathfrak{p}})[\phi]$  otherwise. The group  $I^\phi(K_{\mathfrak{p}}, A)$  is trivial if  $\mathfrak{p}$  is infinite, and isomorphic to

$$\frac{A(M_{\mathfrak{p}})[\phi] \cap (\tau_{\mathfrak{p}} - 1)A(M_{\mathfrak{p}})}{(\tau_{\mathfrak{p}} - 1)A(M_{\mathfrak{p}})[\phi]}$$

otherwise. The group  $S^\phi(K_{\mathfrak{p}}, A)$  is trivial if  $\mathfrak{p}$  is infinite unless  $\mathfrak{p}$  is a real prime, the degree of  $\phi$  is even, and the points in  $A[\phi]$  are defined over  $K_{\mathfrak{p}}$ , in which case the group has exponent 2 and has size at most  $2^g$ . The group  $S^\phi(K_{\mathfrak{p}}, A)$  has order

$$\frac{|\phi'(0)|^{-1} \cdot \#A(K_{\mathfrak{p}})[\phi] \cdot \#A'(K_{\mathfrak{p}})/A'_0(K_{\mathfrak{p}})}{\#A(K_{\mathfrak{p}})/A_0(K_{\mathfrak{p}})}$$

when  $\mathfrak{p}$  is finite.

*Proof.* The injections are clear from the definitions of the groups involved. What happens at the infinite primes follows from Lemma 3.10. Let  $\mathfrak{p}$  be a finite prime. From Lemma 3.1 we see that the group  $C^\phi(K_{\mathfrak{p}}, A)$  is isomorphic to  $A(K_{\mathfrak{p}})[\phi]$ . Since  $H^1(G, A[\phi]) = 0$  for all  $G \subseteq \text{Gal}(L/K)$ , the group  $I^\phi(K_{\mathfrak{p}}, A)$  is defined and is isomorphic to the intersection quotient from Theorem 3.4. The order of the group  $S^\phi(K_{\mathfrak{p}}, A)$  comes from Lemma 3.8.

Let  $\mathfrak{p}$  be a finite prime that does not divide the conductor of  $A$  or the degree of  $\phi$ . Since  $\mathfrak{p}$  does not divide the conductor we have  $A(M_{\mathfrak{p}}) = A_0(M_{\mathfrak{p}})$ . So from Lemma 3.6, all of the elements of  $A(M_{\mathfrak{p}})[\phi]$  are in  $(\tau_{\mathfrak{p}} - 1)A(M_{\mathfrak{p}})$ . Thus the group  $I^\phi(K_{\mathfrak{p}}, A)$  has the same order as  $A(K_{\mathfrak{p}})[\phi]$  and so is equal to  $C^\phi(K_{\mathfrak{p}}, A)$ . We also have  $A(K_{\mathfrak{p}}) = A_0(K_{\mathfrak{p}})$  and  $A'(K_{\mathfrak{p}}) = A_0(K_{\mathfrak{p}})$ . In addition, since  $\mathfrak{p}$  does not divide the degree of  $\phi$ , we have  $|\phi'(0)| = 1$ . Therefore, the order of  $S^\phi(K_{\mathfrak{p}}, A)$  will be the same as the order of  $A(K_{\mathfrak{p}})[\phi]$ . So the image of  $S^\phi(K_{\mathfrak{p}}, A)$  in  $\text{Hom}_{G(LK_{\mathfrak{p}}/K_{\mathfrak{p}})}(\text{Gal}(\overline{LK}_{\mathfrak{p}}/LK_{\mathfrak{p}}), A[\phi])$  is the same as  $C^\phi(K_{\mathfrak{p}}, A)$ , which is isomorphic to  $A(K_{\mathfrak{p}})[\phi]$ . ■

For elliptic curves, all of the local groups are easy to compute. Use Theorem 3.4, Lemma 3.6 and Theorem 3.7 to compute the order of the intersection quotient. Theorem 3.7 requires a minimal Weierstrass equation at the prime  $\mathfrak{p}$  which we may not have, but that does not matter. We can just replace our Weierstrass equation with a minimal one at  $\mathfrak{p}$  so as to be able to apply Theorem 3.7 since the order of the intersection does not depend on the embedding. Use Tate's algorithm to compute the orders of  $E'(K_{\mathfrak{p}})/E'_0(K_{\mathfrak{p}})$  and  $E(K_{\mathfrak{p}})/E_0(K_{\mathfrak{p}})$ . As noted after proving Lemma 3.8, the quantity  $|\phi'(0)|^{-1}$  can be computed easily using [29] and [27, Chap. IV]. In the infinite case use Proposition 3.11 to compute the size of  $E'(K_{\mathfrak{p}})/\phi E(K_{\mathfrak{p}})$ . The group  $E(K_{\mathfrak{p}})[\phi]$  is trivial to compute also.

## 5. THE 2-MAP

The 2-map has been the most studied because it is usually the easiest isogeny to work with that is always defined over the field of definition of an abelian variety. In addition, one does not have to work with two different abelian varieties. For these reasons, 2-Selmer groups are frequently used when trying to compute the free  $\mathbf{Z}$ -rank of a Mordell–Weil group. Birch and Swinnerton-Dyer [3] created an algorithm for computing 2-Selmer groups for elliptic curves and this has been implemented as a computer program by John Cremona. Recently, algorithms have been introduced for computing 2-Selmer groups for the Jacobians of hyperelliptic curves that work in special cases. For hyperelliptic curves of genus 2 there are the algorithms of Flynn [8], and of Gordon and Grant [9], and for arbitrary genus see [23]. The algorithms of Flynn and of Gordon and Grant have also been implemented as computer programs. As mentioned in the introduction, the 2-map has been studied in connection with its relation to the 2-rank of the class group of cubic extensions of  $\mathbf{Q}$ . We will see why in Subsection 5.1

In this section we first show how the group  $C^2(K, J)$  is related to the 2-parts of class groups when  $J$  is the Jacobian of an elliptic or a hyperelliptic curve. We then present some examples of computing the local intersection  $I^2(K_{\mathfrak{p}}, E)$  for elliptic curves. Then we come up with simpler upper bounds for the sizes of  $S^2(K, A)/I^2(K, A)$  and  $C^2(K, A)/I^2(K, A)$ . Lastly we do explicit computations for three examples of Jacobians of elliptic and hyperelliptic curves.

### 5.1. The Group $C^2(K, J)$ for the Jacobians of Elliptic and Hyperelliptic Curves

Let  $C$  be the projective elliptic or hyperelliptic curve defined over  $K$ , a number field, by the equation  $Y^2 = f$  where  $f$  is a separable polynomial of odd degree  $d \geq 3$ . Let  $J$  be the Jacobian of the normalization of  $C$  and let

$\infty$  denote the point at infinity of the normalization of  $C$ . The genus of the curve  $C$  and the dimension of  $J$  are both  $(d-1)/2$ . Let  $L = K(J[2])$ , and let  $G_2$  be a 2-Sylow subgroup of  $\text{Gal}(L/K)$ . We will see below that when  $H^1(G_2, J[2])$  is trivial that we have

$$H^1(K, J[2]) \cong \text{Hom}_{\text{Gal}(L/K)}(\text{Gal}(\bar{L}/L), J[2]).$$

By abuse of notation we will denote the preimage in  $H^1(K, J[2])$  of  $C^2(K, J)$  also by  $C^2(K, J)$ .

Let  $F$  be the algebra defined by  $F = K[T]/f(T)$  and let  $\bar{F}$  be  $\bar{K}[T]/f(T)$ . In [23] the author presented an isomorphism of  $H^1(K, J[2])$  and the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$ . Any subset with  $d-1$  elements of the set of  $(\alpha_i, 0) - \infty$ , where  $f(\alpha_i) = 0$ , forms a basis for  $J[2]$ . Let  $w$  be the Weil-pairing of an element of  $J[2]$  with all  $d$  of the points  $(\alpha_i, 0) - \infty$ ; then  $w$  is a map from  $J[2]$  to  $\mu_2(\bar{F})$ . The map  $w$  induces an injective map from  $H^1(K, J[2])$  to  $H^1(K, \mu_2(\bar{F}))$ . The latter cohomology group is isomorphic to  $F^*/F^{*2}$  by a Kummer map (see [25, p. 152]). Composing the Kummer isomorphism and the Weil-pairing induces the desired isomorphism.

Let us define unramified elements in the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$ . We can write  $F \cong F_1 \times \dots \times F_r$ , where each  $F_i$  is a field and we have

$$F^*/F^{*2} \cong F_1^*/F_1^{*2} \times \dots \times F_r^*/F_r^{*2}.$$

For an arbitrary number field  $W$ , let us define the unramified elements of  $W^*/W^{*2}$  to be those which have the property that if one adjoins the square root of a representative to  $W$ , one gets a totally unramified extension of  $W$ . We will say an element of  $F^*/F^{*2}$  is unramified if its image in each  $F_i^*/F_i^{*2}$  is unramified. The group  $C^2(K, J)$  injects into the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$ . We will show that its image is the same as the subgroup of unramified elements.

LEMMA 5.1. *Let  $f$  be a separable polynomial of odd degree  $d \geq 3$ , defined over  $K$  a field of characteristic 0. Let  $C$  be the curve defined by  $Y^2 = f$  and let  $J$  be the Jacobian of the normalization of  $C$ . Let  $L = K(J[2])$  and  $G_2$  be a 2-Sylow subgroup of  $\text{Gal}(L/K)$ . Then the following are equivalent.*

1. *The group  $H^1(G_2, J[2])$  is trivial.*
2. *The group  $J[2]$  is cohomologically trivial as a  $G_2$ -module.*
3. *The group  $J[2]$  is cohomologically trivial as a  $\text{Gal}(L/K)$ -module.*
4. *Let  $W$  be the field fixed by  $G_2$ . In  $W[X]$ , the polynomial  $f$  is the product of one linear factor and  $(d-1)/\#G_2$  irreducible factors, each of degree  $\#G_2$ .*

5. Let  $\alpha_i$  for  $1 \leq i \leq d$  be the roots of  $f$ . For  $i$  not equal to  $j$ , the degree of  $L$  over  $K(\alpha_i, \alpha_j)$  is odd.

*Proof.* From [2, Thm. 6], (1) is equivalent to (2) and from [2, Prop. 8], (2) is equivalent to (3). To prove that (4) implies (5) we note that (4) implies that if  $\sigma \in G_2$  fixes two different  $\alpha_i$ 's then  $\sigma$  is the identity. Let  $i$  not equal  $j$  and let  $\hat{G} = \text{Gal}(L/K(\alpha_i, \alpha_j))$ . Let  $\hat{H}$  be a 2-Sylow subgroup in  $\hat{G}$ . The group  $\hat{H}$  can be extended to a 2-Sylow subgroup of  $\text{Gal}(L/K)$ , which we will call  $G_2$ . Elements of  $\hat{H}$  are in  $G_2$  and fix two different  $\alpha_i$ 's so  $\hat{H}$  is trivial. Thus the degree of  $L$  over  $K(\alpha_i, \alpha_j)$  is odd. To prove that (5) implies (4) we note that (5) implies that  $L$  is of odd degree over  $W(\alpha_i, \alpha_j)$  when  $i$  is not equal to  $j$ . So  $L$  equals  $W(\alpha_i, \alpha_j)$ . Since the degree of  $f$  is odd, one of its roots must be in  $W$  and each of the rest generates  $L$ , which is (4).

Now let us prove that (1) and (4) are equivalent. Let  $X$  be the  $G_2$ -set of roots of  $f$ . Let  $G_2$  act trivially on  $\mathbf{F}_2$  and let  $\mathbf{F}_2^X$  be the  $G_2$ -maps from  $X$  to  $\mathbf{F}_2$ . Recall that any subset of the set of  $(\alpha_i, 0) - \infty$  with  $d-1$  elements forms a basis for  $J[2]$ . It is easy to check that the kernel of the norm from  $\mathbf{F}_2^X$  to  $\mathbf{F}_2$  is isomorphic as a  $G_2$ -module to  $J[2]$ . In addition, since  $d$  is odd, the composition of the diagonal embedding of  $\mathbf{F}_2$  in  $\mathbf{F}_2^X$  with the norm is the identity map so the exact sequence

$$0 \rightarrow J[2] \rightarrow \mathbf{F}_2^X \xrightarrow{\text{norm}} \mathbf{F}_2 \rightarrow 0$$

splits. Therefore the exact sequence

$$0 \rightarrow H^1(G_2, J[2]) \rightarrow H^1(G_2, \mathbf{F}_2^X) \rightarrow H^1(G_2, \mathbf{F}_2) \rightarrow 0$$

also splits. Because these groups are finite, condition (1) is equivalent to  $H^1(G_2, \mathbf{F}_2^X) \cong H^1(G_2, \mathbf{F}_2)$ . Now  $X$  is isomorphic as a  $G_2$ -set to the disjoint union of its orbits and so to  $\coprod G_2/H_j$  for some set of subgroups  $H_j$  of  $G_2$ . Thus

$$\mathbf{F}_2^X \cong \bigoplus_j \mathbf{F}_2^{G_2/H_j}$$

as  $G_2$ -modules. So we have

$$H^1(G_2, \mathbf{F}_2^X) \cong H^1(G_2, \mathbf{F}_2^{G_2/H_1}) \oplus \cdots \oplus H^1(G_2, \mathbf{F}_2^{G_2/H_n})$$

for some  $n$ . Now from Shapiro's lemma (see [2, Prop. 2]), condition (1) is equivalent to

$$H^1(G_2, \mathbf{F}_2) \cong H^1(H_1, \mathbf{F}_2) \oplus \cdots \oplus H^1(H_n, \mathbf{F}_2).$$

Now  $X$  has odd cardinality and  $G_2$  is a 2-Sylow subgroup, so there is an orbit of cardinality one. Without loss of generality we will let  $H_1 = G_2$ . So

(1) is equivalent to all of the groups  $H^1(H_j, \mathbf{F}_2)$  being trivial for  $j > 1$ . Since  $H_j$  acts trivially on  $\mathbf{F}_2$  we know that such cohomology groups are trivial only when  $H_j$  is trivial. So (1) is true if and only if  $X$  has one orbit with a single element and otherwise consists of orbits with the same cardinality as  $G_2$ . In other words,  $f$  is the product of one linear factor and  $(d-1)/\#G_2$  irreducible factors each of degree  $\#G_2$ , which is condition (4). ■

Condition (5) is always true for elliptic curves, and for curves of the form  $y^2 = x^p + a$  where  $p$  is an odd prime.

LEMMA 5.2. *Let  $W$  be a finite extension of  $K$ , fields of characteristic 0. The norm from  $W^*/W^{*2}$  to  $K^*/K^{*2}$  sends unramified elements to unramified elements.*

*Proof.* Let  $W_1$  be any finite extension of  $K$ , and let  $W_i$ , for  $i = 1$  to  $s$ , be the  $s$  conjugates of  $W_1$  over  $K$ . Let  $\alpha_1 \in W_1$  and let  $\alpha_i$  be the image of  $\alpha_1$  in each  $W_i$ . Let  $W_1(\sqrt{\alpha_1})$  be a totally unramified extension of  $W_1$ . We will abbreviate totally unramified with unramified. Then  $W_i(\sqrt{\alpha_i})$  is an unramified extension of  $W_i$  for all  $i$ . Let  $E$  be the normal closure of  $W_1(\sqrt{\alpha_1})$  over  $K$ . We want to prove that  $K(\sqrt{N_{W_1/K}(\alpha_1)})$  is an unramified extension of  $K$ . Let  $I \subseteq \text{Gal}(E/K)$  be an inertia group and pick  $\sigma \in I$ . We want to prove that  $\sigma$  fixes  $\sqrt{N_{W_1/K}(\alpha_1)} = \sqrt{\alpha_1 \cdot \dots \cdot \alpha_s}$ . Pick an orbit of the set of  $\alpha_i$ 's under the action of the group generated by  $\sigma$  and number them  $\alpha_1, \dots, \alpha_j$  where  $\sigma(\alpha_i) = \alpha_{i+1}$  with the subscripts computed modulo  $j$ . We have  $\sigma(\sqrt{\alpha_i}) = \pm \sqrt{\alpha_{i+1}}$  and if we compute these for  $i$  from 1 to  $j$  then the number of minus signs must be even. If it were odd, then  $\sigma^j(\sqrt{\alpha_1}) = -\sqrt{\alpha_1}$  and so  $\sigma^j(\alpha_1) = \alpha_1$  and so  $\sigma^j$  would be in  $\text{Gal}(E/W_1)$ . Since  $W_i(\sqrt{\alpha_i})$  is an unramified extension of  $W_i$  we know that  $\sigma^j \in I$  would also fix  $\sqrt{\alpha_i}$ , a contradiction. Thus there are an even number of minus signs and so  $\sigma$  fixes the square root of the product of the elements of each orbit and so  $\sigma$  fixes  $\sqrt{\alpha_1 \cdot \dots \cdot \alpha_s}$ . ■

If the element  $a$  of  $F$  has image  $(a_1, \dots, a_r)$  in  $\prod F_i$ , then  $N_{F/K}(a)$  is the same as the product of the  $N_{F_i/K}(a_i)$ . We see that the norm from  $F^*/F^{*2} = \prod F_i^*/F_i^{*2}$  to  $K^*/K^{*2}$  takes unramified elements to unramified elements.

THEOREM 5.3 *Let  $f$  be a separable polynomial of odd degree  $d \geq 3$ , defined over  $K$ , a number field. Let  $C$  be the curve defined by  $Y^2 = f$ , let  $J$  be the Jacobian of the normalization of  $C$  and let  $F = K[T]/f(T)$ . Let  $L = K(J[2])$  and  $G_2$  be a 2-Sylow subgroup of  $\text{Gal}(L/K)$ . If the group  $H^1(G_2, J[2])$  is trivial then the group  $C^2(K, J)$  is isomorphic to the kernel of the norm from the unramified elements in  $F^*/F^{*2}$  to the unramified elements in  $K^*/K^{*2}$ .*

*Proof.* From Lemma 5.1, since  $H^1(G_2, J[2])$  is trivial, we know  $J[2]$  is cohomologically trivial as a  $\text{Gal}(L/K)$ -module. So  $H^i(\text{Gal}(L/K), J[2])$  is trivial for all  $i$ . From the extended inflation-restriction sequence (see [10, p. 30]) we then have

$$H^1(K, J[2]) \cong \text{Hom}_{\text{Gal}(L/K)}(\text{Gal}(\bar{L}/L), J[2]).$$

By abuse of notation we will denote the preimage in  $H^1(K, J[2])$  of  $C^2(K, J)$  also by  $C^2(K, J)$ . Thus,  $C^2(K, J)$  is the subgroup of  $H^1(K, J[2])$  consisting of classes of cocycles which, when restricted to  $\text{Gal}(\bar{L}/L)$ , factor through  $\text{Gal}(H(L)/L)$  where  $H(L)$  is the Hilbert class field of  $L$ .

We have seen that the group  $H^1(K, J[2])$  is isomorphic to the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$ . An element  $a$  of the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$  is in the image of  $C^2(K, J)$  exactly when its image  $(a_1, \dots, a_r)$  in  $\prod [F_i^*/F_i^{*2}]$  has the property that for each  $i$ , the field  $L(\sqrt{a_i})$  is unramified over  $L$  with the  $F_i$ 's properly embedded in  $L$ . That is, for each  $K$ -algebra homomorphism  $\sigma$  from  $F$  to  $L$ , the field  $L(\sqrt{\sigma(a)})$  is unramified over  $L$ . An element  $a$  in the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$  is in the subgroup of unramified elements exactly when for each  $K$ -algebra homomorphism  $\sigma$  from  $F$  to  $L$ , the field  $\sigma(F)(\sqrt{\sigma(a)})$  is unramified over  $\sigma(F)$ . We are trying to show that these two subgroups of  $F^*/F^{*2}$  are the same. It is clear that the latter subgroup is contained in the former.

Let us prove that the former subgroup is contained in the latter. Let  $a$  be an element of  $F^*$  with  $N_{F/K}(a)$  in  $K^{*2}$  and with the property that for every  $K$ -algebra homomorphism  $\sigma$  from  $F$  to  $L$  that  $L(\sqrt{\sigma(a)})$  is unramified over  $L$ . We have assumed condition (1) of lemma 5.1 and so we have condition (4). First we will assume that  $K=W$ , where  $W$  is the fixed field of  $G_2$ , a 2-Sylow subgroup of  $\text{Gal}(L/K)$ . Under this assumption, the algebra  $F$  is isomorphic to the direct product of  $K$  and  $(d-1)/\#\text{Gal}(L/K)$  copies of  $L$ . Let the image of  $a$  in this direct product be  $(a_1, \dots, a_r)$ . We need to show that  $K(\sqrt{a_1})$  is an unramified extension of  $K$  and that  $L(\sqrt{a_i})$  is an unramified extension of  $L$  for each  $i > 1$ . The latter statement is part of the assumption. Now  $N_{F/K}(a)$  is equal to  $a_1 N_{L/K}(a_2) \cdot \dots \cdot N_{L/K}(a_r)$  and is in  $K^{*2}$ . Thus  $a_1$  is congruent to  $N_{L/K}(a_2 \cdot \dots \cdot a_r)$  modulo  $K^{*2}$ . By hypothesis,  $L(\sqrt{a_i})$  for  $i > 1$  is an unramified extension of  $L$ . By Lemma 5.2, the field  $K(\sqrt{a_1})$  must be an unramified extension of  $K$ . So for every  $K$ -algebra homomorphism  $\sigma$  from  $F$  to  $L$  we have  $\sigma(F)(\sqrt{\sigma(a)})$  is unramified over  $\sigma(F)$ .

Now we will no longer assume that  $K=W$  and reduce to that case. Assume  $a$  is in  $F^*$  with  $N_{F/K}(a)$  in  $K^{*2}$  and assume for every  $K$ -algebra homomorphism  $\sigma$  from  $F$  to  $L$  that  $L(\sqrt{\sigma(a)})$  is unramified over  $L$ . Let  $F \otimes_K W$  be isomorphic to the product of fields  $\prod E_i$ . We have  $\sum [E_i : F] = [W : K]$  which is odd so without loss of generality, let the



degree of  $E_1$  over  $F$  be odd. There is some homomorphism  $\gamma$  from  $W$  to  $L$  such that the homomorphism  $\sigma \otimes \gamma$  from  $F \otimes_K W$  to  $L$  factors through  $E_1$  and we can denote the induced map from  $E_1$  to its image by  $\rho$ . Now the map  $\rho$  from  $E_1$  to  $\rho(E_1)$  extends the map  $\sigma$  from  $F$  to  $\sigma(F)$ .

$$\begin{array}{ccc} \sigma \otimes \gamma: F \otimes_K W & \xrightarrow{\rho} & \rho(E_1) \subset L \\ & \cup & \cup \\ & F & \xrightarrow{\sigma} \sigma(F) \end{array}$$

The degree of  $E_1$  over  $F$  is odd, so the degree of  $\rho(E_1)$  over  $\sigma(F)$  is odd. From above, since  $\sigma \otimes \gamma$  is a homomorphism from  $F \otimes_K W$  to  $L$ , we know  $\rho(E_1)(\sqrt{\rho(a \otimes 1)})$  over  $\rho(E_1)$  is unramified. The only elements of inertia groups we have to worry about are of 2-power order. Since the degree of  $\rho(E_1)$  over  $\sigma(F)$  is odd and  $\rho$  extends  $\sigma$ , we know that  $\sigma(F)(\sqrt{\sigma(a)})$  is unramified over  $\sigma(F)$  also. Therefore the subgroup of the kernel of the norm from  $F^*/F^{*2}$  to  $K^*/K^{*2}$  of unramified elements is equal to the image of  $C^2(K, J)$ . ■

The group of unramified elements in  $F^*/F^{*2}$  is the product of the groups of unramified elements in each  $F_i^*/F_i^{*2}$ . If  $W$  is any field, such as  $K$  or an  $F^i$ , then the group of unramified elements in  $W^*/W^{*2}$  is isomorphic to the dual of  $\text{Cl}(W)/\text{Cl}(W)^2$  from Kummer theory and class field theory.

### 5.2. The Group $I^2(K_p, E)$ .

In this section we will see that for elliptic curves, the computation of  $I^2(K_p, E)$  is essentially a matter of finding the action of  $\text{Gal}(\bar{K}_p/K_p)$  on  $E[2]$  and using Tate’s algorithm over  $K_p$  to deduce the action of  $\text{Gal}(M_p/K_p)$  on  $E(M_p)/E_0(M_p)$ . This is facilitated by that fact that the possible groups  $E(M_p)/E_0(M_p)$  and the possible Galois actions on them are very limited.

Let  $E$  be an elliptic curve defined over a number field  $K$ . Condition (5) of Lemma 5.1 is satisfied for all elliptic curves so condition (3) holds. That says that  $H^1(G, E[2]) = 0$  for all groups  $G$  contained in  $S_3$ , where  $S_3$  is the automorphism group of  $E[2]$ . So the conditions of Theorems 4.1 and 3.4 hold. From Theorem 3.4 and Lemmas 3.1 and 3.6, the order of the local intersection,  $I^2(K_p, E)$ , is the same as the order of the local group of unramified homomorphisms,  $C^2(K_p, E)$ , if all of the points in  $E(M_p)[2]$  have non-singular reduction, which will happen if the elliptic curve has good reduction at  $p$ . So the only cases where something interesting can happen occur when  $E$  has bad reduction at  $p$ .

From Theorem 3.4, in order to compute the size of the local intersection, we need to find out how many elements of  $E(M_p)[2]$  are in  $(\tau - 1)E(M_p)$  and divide that quantity by the size of  $(\tau - 1)(E(M_p)[2])$ . We know from

Lemma 3.6 that the elements of  $E(M_p)[2]$  that are in  $(\tau - 1)E(M_p)$  are those with non-singular reduction and those with singular reduction which have the property that their image in  $E(M_p)/E_0(M_p)$  is in  $(\tau - 1)(E(M_p)/E_0(M_p))$ . From Theorem 3.7 we find that the only times that a 2-torsion point with singular reduction could possibly be in the image of  $\tau - 1$  are in the cases that  $E$  has type  $I_v$  reduction where  $4|v$  or type  $I_v^*$  reduction with  $v$  odd or even. As we will see, in each of these three cases, a 2-torsion point with singular reduction, may or may not be in the group  $(\tau - 1)E(M_p)$ . In the other cases, either  $E(K_p^{\text{unr}})/E_0(K_p^{\text{unr}})$  has no 2-torsion or a point with singular reduction generates the 2-part of  $E/E_0$  and can not be in the image of  $\tau - 1$ . Computations of the groups  $E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)$  were accomplished with Tate's algorithm [28].

1. *Examples of curves with type  $I_v$  reduction with  $4|v$  and 2-torsion points of singular reduction in and not in the image of  $\tau - 1$ .* The curves  $Y^2 = X^3 - 26X^2 + 135X - 567$  and  $Y^2 = X^3 + 26X^2 + 135X + 567$  have discriminant  $\Delta = -2^4 \cdot 3^4 \cdot 23^2 \cdot 239$ . Over  $\mathbf{Q}_3$  they each have type  $I_v$  reduction (multiplicative) with  $v=4$ . Each have two 2-torsion points with singular reduction defined over  $\mathbf{Q}_3$ . They differ by a 2-torsion point with non-singular reduction and so have the same image in  $E/E_0$ . For both curves, the group  $E(\mathbf{Q}_3^{\text{unr}})/E_0(\mathbf{Q}_3^{\text{unr}})$  is isomorphic to  $\mathbf{Z}/4\mathbf{Z}$ . The first curve has split multiplicative reduction over  $\mathbf{Q}_3$  and the second does not. Therefore the group  $E(\mathbf{Q}_3)/E_0(\mathbf{Q}_3)$  is isomorphic to  $\mathbf{Z}/4\mathbf{Z}$  for the first curve and  $\mathbf{Z}/2\mathbf{Z}$  for the second. The image of the 2-torsion points with singular reduction is the element of order 2 in both groups. All of the 2-torsion is defined over  $\mathbf{Q}_3$  for these curves, so  $M_3$  is the quadratic unramified extension of  $\mathbf{Q}_3$ . We have  $E(M_3)/E_0(M_3)$  isomorphic to  $\mathbf{Z}/4\mathbf{Z}$  for both curves. The automorphism  $\tau$  acts trivially on each element of  $E(M_3)/E_0(M_3)$  for the first curve and as  $-1$  for the second. The 2-torsion points with singular reduction are in the image of the map  $\tau - 1$  for the second curve, but not the first.

For both curves the size of  $E(M_3)[2]$  is 4 and  $\tau$  acts trivially on each element so  $(\tau - 1)(E(M_3)[2])$  is trivial. For both curves the size of  $E_0(M_3)[2]$  is 2 and from Lemma 3.6, those 2 points are automatically in  $(\tau - 1)(E(M_3))$ . From above, the two 2-torsion points with singular reduction on the first curve are not in the image of  $\tau - 1$ . Thus the size of  $(\tau - 1)E(M_3) \cap E(M_3)[2]$  is 2 and so the size of  $I^2(\mathbf{Q}_3, E)$  is 2. The two 2-torsion points with singular reduction on the second curve are in the image of  $\tau - 1$ . So  $(\tau - 1)E(M_3) \cap E(M_3)[2]$  and  $I^2(\mathbf{Q}_3, E)$  each have size 4.

2. *Examples of curves with type  $I_v^*$  reduction with  $v$  odd and 2-torsion points of singular reduction in and not in the image of  $\tau - 1$ .* The curves  $Y^2 = X^3 - 23^2X + 23^3$  and  $Y^2 = X^3 - 23^2X - 23^3$  have discriminant  $\Delta = -2^4 \cdot 23^7$ . Over  $\mathbf{Q}_{23}$  they each have type  $I_v^*$  reduction with  $v=1$ . For both

curves, two 2-torsion points are defined over a quadratic ramified extension of  $\mathbf{Q}_{23}$ . Each curve has one 2-torsion point defined over  $\mathbf{Q}_{23}$  with singular reduction. So the field  $M_{23}$  is the quadratic unramified extension of  $\mathbf{Q}_{23}$ . For the first curve, the groups  $E(\mathbf{Q}_{23})/E_0(\mathbf{Q}_{23})$  and  $E(M_{23})/E_0(M_{23})$  are both isomorphic to  $\mathbf{Z}/4\mathbf{Z}$ . For the second curve, the group  $E(\mathbf{Q}_{23})/E_0(\mathbf{Q}_{23})$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  and  $E(M_{23})/E_0(M_{23})$  is isomorphic to  $\mathbf{Z}/4\mathbf{Z}$ . For both curves,  $(\tau - 1)(E(M_{23})[2])$  is trivial and  $E(M_{23})[2]$  has order 2. The action of  $\tau$  on the groups  $E(M_{23})/E_0(M_{23})$  is identical to that in the last example. So  $(\tau - 1)E(M_{23}) \cap E(M_{23})[2]$  and  $I^2(\mathbf{Q}_{23}, E)$  are trivial for the first curve and have order 2 for the second curve.

3. *Examples of curves with type  $I_v^*$  reduction with  $v$  even and 2-torsion points of singular reduction in and not in the image of  $\tau - 1$ .* The curve  $Y^2 = X^3 + X^2 + 4X + 12$  has discriminant  $\Delta = -2^8 \cdot 3^2 \cdot 23$ . Over  $\mathbf{Q}_2$  it has type  $I_v^*$  reduction with  $v = 0$ . All of the 2-torsion points are defined over  $\mathbf{Q}_2$ . So the field  $M_2$  is the quadratic unramified extension of  $\mathbf{Q}_2$ . The group  $(\tau - 1)(E(M_2)[2])$  is trivial. Two points in  $E(M_2)[2]$  have non-singular reduction and so are in  $(\tau - 1)E(M_2)$ . Two of the 2-torsion points have singular reduction. They generate  $E(\mathbf{Q}_2)/E_0(\mathbf{Q}_2)$  where they have the same image; this group has two elements. The group  $E(\mathbf{Q}_2^{\text{unr}})/E_0(\mathbf{Q}_2^{\text{unr}})$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ . There are only 2 automorphisms of  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$  fixing a given subgroup of order 2. So the group  $E(M_2)/E_0(M_2)$  must be isomorphic to  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ . The image of  $\tau - 1$  on an element of  $E(M_2)/E_0(M_2)$  not fixed by  $\tau$  is the image of the 2 singular points in  $E(M_2)/E_0(M_2)$ . Thus the two 2-torsion points with singular reduction are also in  $(\tau - 1)E(M_2)$ , so  $I^2(\mathbf{Q}_2, E)$  has 4 elements.

The curve  $Y^2 = X^3 - 25X$  has discriminant  $\Delta = 2^6 \cdot 5^6$ . Over  $\mathbf{Q}_5$  it also has type  $I_v^*$  reduction with  $v = 0$ . All of the 2-torsion points are defined over  $\mathbf{Q}_5$ . This curve has three 2-torsion points with singular reduction. The group  $E(\mathbf{Q}_5)/E_0(\mathbf{Q}_5)$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$  as it is generated by the 2-torsion points. Since the group  $E(\mathbf{Q}_5^{\text{unr}})/E_0(\mathbf{Q}_5^{\text{unr}})$  has been realized over  $\mathbf{Q}_5$  it is impossible for these 2-torsion points to be in the image of  $\tau - 1$ . So the group  $I^2(\mathbf{Q}_5, E)$  is trivial.

The curve  $Y^2 = X^3 - 75X + 125$  has discriminant  $\Delta = 2^4 \cdot 3^4 \cdot 5^6$ . Over  $\mathbf{Q}_5$  it also has type  $I_v^*$  reduction with  $v = 0$ . This curve has three 2-torsion points with singular reduction and they are all defined over  $L_5$ , the cubic unramified extension of  $\mathbf{Q}_5$ . The group  $E(\mathbf{Q}_5)/E_0(\mathbf{Q}_5)$  is trivial. The group  $E(L_5)/E_0(L_5)$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$  and is generated by the 2-torsion points. The field  $M_5$  is the sextic unramified extension of  $\mathbf{Q}_5$ . The automorphism  $\tau$  permutes the three 2-torsion points with singular reduction. Though all of the 2-torsion points are in  $(\tau - 1)E(M_5)$ , they are also in  $(\tau - 1)E(M_5)[2]$  and so the group  $I^2(\mathbf{Q}_5, E)$  is trivial. This should be clear anyway as the group  $E(\mathbf{Q}_5)[2]$  is trivial, so the group of unramified homomorphisms is also.

### 5.3. The Groups $S^2(K, A)/I^2(K, A)$ and $C^2(K, A)/I^2(K, A)$

Let us return to arbitrary abelian varieties and derive more elegant upper bounds for the sizes of the quotients of the Selmer group and the group related to the class group by their intersection, for the 2-map. We can reformulate Theorem 4.1 with the following divisibility conditions.

PROPOSITION 5.4. *We have*

$$\#S^2(K, A)/I^2(K, A) \left| \prod_{\mathfrak{p} \in T} \frac{\#A(K_{\mathfrak{p}})[2]}{\#I^2(K_{\mathfrak{p}}, A)} \right.$$

and

$$\#C^2(K, A)/I^2(K, A) \left| \prod_{\mathfrak{p} | \mathfrak{f}} \frac{\#A(K_{\mathfrak{p}})[2]}{\#I^2(K_{\mathfrak{p}}, A)} \right.$$

where  $T$  is the set of primes of  $K$  consisting of the infinite primes and the primes that divide  $2\mathfrak{f}$ , where  $\mathfrak{f}$  is the conductor of  $A$ .

*Proof.* The second divisibility statement follows immediately from Theorem 4.1. Let us consider the group  $S^2(K, A)/I^2(K, A)$ . The given divisibility statement differs from what appears in Theorem 4.1 at the primes dividing 2 and the infinite primes since at all other primes we have  $|\phi'(0)| = 1$  as well as  $A = A'$ . Let us consider the order of the group  $A(K_{\mathfrak{p}})/2A(K_{\mathfrak{p}})$  where  $\mathfrak{p}$  is a prime of  $K$ , i.e.  $S^2(K_{\mathfrak{p}}, A)$ . First assume that  $\mathfrak{p}$  is a prime dividing 2. From proposition 3.9, we have

$$\#A(K_{\mathfrak{p}})/2A(K_{\mathfrak{p}}) = 2^{g[K_{\mathfrak{p}} : \mathbf{Q}_2]} \cdot \#A(K_{\mathfrak{p}})[2]$$

where  $g$  is the dimension of  $A$ .

If  $K_{\mathfrak{p}} \cong \mathbf{C}$ , then  $A(K_{\mathfrak{p}})/2A(K_{\mathfrak{p}})$  is a trivial group. Let  $K_{\mathfrak{p}} \cong \mathbf{R}$ . We have the following commutative diagram from the snake lemma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker & \longrightarrow & A(\mathbf{R})[2] & \longrightarrow & H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{R}^g/A \cap (\mathbf{R}^g) & \longrightarrow & A(\mathbf{R}) & \longrightarrow & H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) & \longrightarrow & 0 \\ & & \downarrow [2] & & \downarrow [2] & & \downarrow [2] & & \\ 0 & \longrightarrow & \mathbf{R}^g/A \cap (\mathbf{R}^g) & \longrightarrow & A(\mathbf{R}) & \longrightarrow & H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & \longrightarrow & 0 & \longrightarrow & A(\mathbf{R})/2A(\mathbf{R}) & \longrightarrow & H^1(\text{Gal}(\mathbf{C}/\mathbf{R}), A) & \longrightarrow & 0. \end{array}$$

The center two short exact sequences appeared in the proof of Lemma 3.10. The size of the kernel of the 2-map from  $\mathbf{R}^g/A \cap (\mathbf{R}^g)$  to itself is  $2^g$ . We see that the size of  $A(\mathbf{R})/2A(\mathbf{R})$  equals  $\#A(\mathbf{R})[2]/2^g$ . Notice that if  $K_p$  is isomorphic to  $\mathbf{C}$  or to  $\mathbf{R}$  that we have

$$\#A(K_p)/2A(K_p) = \#A(K_p)[2]/2^{g[K_p:\mathbf{R}]}$$

So the contribution from the infinite primes and the primes dividing 2 is the following

$$\begin{aligned} & \prod_{p|\infty} \frac{\#A(K_p)[2]}{2^{g[K_p:\mathbf{R}]}} \cdot \prod_{p|2} \frac{2^{g[K_p:\mathbf{Q}_2]} \cdot \#A(K_p)[2]}{\#I^2(K_p, A)} \\ &= \frac{2^{g[K:\mathbf{Q}]}}{2^{g[K:\mathbf{Q}]}} \cdot \prod_{p|\infty} \#A(K_p)[2] \cdot \prod_{p|2} \frac{\#A(K_p)[2]}{\#I^2(K_p, A)} \\ &= \prod_{\substack{p|2 \\ \text{or } \infty}} \frac{\#A(K_p)[2]}{\#I^2(K_p, A)} \end{aligned}$$

since  $I^2(K_p, A)$  is trivial for all infinite primes from Lemma 3.10.

### 5.4. Examples

EXAMPLE I. A cubic field whose class group has 2-rank at least 13.

Mestre [16] has produced an elliptic curve  $E$  of rank at least 14 over  $\mathbf{Q}$ . A Weierstrass equation for the curve  $E$  is given by

$$Y^2 + 357573631Y = X^3 + 2597055X^2 - 549082X - 19608054.$$

The discriminant is odd, square-free and negative. The primes of bad reduction are those that divide the conductor of  $E$  which are exactly the ones that divide the discriminant. There are no non-trivial 2-torsion points defined over  $\mathbf{Q}$ . Let us determine whether  $L = \mathbf{Q}(E[2])$  is an  $A_3$ - or an  $S_3$ -extension of  $\mathbf{Q}$ . Choose another Weierstrass equation for  $E$  of the form  $Y^2 = g$  where  $g \in \mathbf{Z}[X]$ ; the polynomial  $g$  will be irreducible. The quotient of the discriminants of the two Weierstrass equations will be a square. The discriminant of the second will be 16 times the discriminant of the cubic polynomial  $g$ . If  $g(\alpha) = 0$ , then  $(\alpha, 0)$  is a 2-torsion point. The field  $F = \mathbf{Q}(\alpha)$  is a cubic extension of  $\mathbf{Q}$  whose discriminant differs by a square from the discriminant of  $g$ . Thus the discriminant of the field  $F$  is not a square, so  $L$  is an  $S_3$ -extension of  $\mathbf{Q}$  and  $F$  is a non-Galois cubic extension of  $\mathbf{Q}$ .

Let  $p$  be an odd prime of bad reduction. The elliptic curve has type  $I_v$  reduction (multiplicative) at  $p$  with  $v = 1$ . So  $E(\mathbf{Q}_p^{\text{unr}})/E_0(\mathbf{Q}_p^{\text{unr}})$  is trivial and the 2-torsion points defined over unramified extensions of  $\mathbf{Q}_p$  are in  $E_0$ . From Lemma 3.6, all points of  $E(M_p)[2]$  are in  $(\tau - 1)(E(M_p))$ . From

Theorem 3.4, the group  $I^2(\mathbf{Q}_p, E)$  has the same size as  $E(\mathbf{Q}_p)[2]$ . From Lemma 3.1 and Proposition 3.9, the groups  $C^2(\mathbf{Q}_p, E)$  and  $S^2(\mathbf{Q}_p, E)$  also have the same size as  $E(\mathbf{Q}_p)[2]$  (which is 2). So  $C^2(\mathbf{Q}_p, E)$  and  $S^2(\mathbf{Q}_p, E)$  are equal.

At the prime 2, the curve has supersingular good reduction and the reduced curve has 5 points over  $\mathbf{F}_2$ . In fact the group  $E(\mathbf{Q}_2)[2]$  is trivial and so the group of unramified homomorphisms at the prime 2, namely  $C^2(\mathbf{Q}_2, E)$ , is trivial and  $E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)$ , or  $S^2(\mathbf{Q}_2, E)$ , has 2 elements. Since the discriminant is negative, we have  $L_\infty = \mathbf{R}(E[2]) \cong \mathbf{C}$  so from Proposition 3.11 the group  $E(\mathbf{R})/2E(\mathbf{R})$  is trivial. So the three local groups are all trivial for the infinite prime. Thus for all primes but 2, all three local groups are the same. For the prime 2, the group  $C^2(\mathbf{Q}_2, E)$  is contained in the group  $S^2(\mathbf{Q}_2, E)$  with index 2. Therefore, the group of globally unramified homomorphisms,  $C^2(\mathbf{Q}, E)$ , is contained in the 2-Selmer group,  $S^2(\mathbf{Q}, E)$ , with index at most 2. To show it has index 2, we need to find an element of the Selmer group that restricts to the image of the non-trivial element of  $E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)$  in  $H^1(\mathbf{Q}_2, E[2])$ . There is a rational point with  $X$ -coordinate  $-2561042$ . When multiplied by 5, one gets a point in the kernel of reduction. The valuation of the  $X$ -coordinate of this second point at the prime 2 is  $-2$  so it is in  $E_1(\mathbf{Q}_2)$  but not in  $E_2(\mathbf{Q}_2)$ . The group  $E_2(\mathbf{Q}_2)$  is isomorphic to the additive group of the ring of integers in  $\mathbf{Q}_2$  and  $E_1(\mathbf{Q}_2)/E_2(\mathbf{Q}_2)$  has 2 elements (see [27, Chapt. IV: Prop. 3.2 and Thm. 6.4]). Therefore this point cannot be in  $2E(\mathbf{Q}_2)$ . This point maps to a homomorphism ramified at 2. So we know that  $C^2(\mathbf{Q}, E)$  has rank at least 13. From Theorem 5.3, since  $\text{Cl}(\mathbf{Q})$  is trivial, the group  $C^2(\mathbf{Q}, E)$  is isomorphic to the dual of  $\text{Cl}(F)/\text{Cl}(F)^2$ . So using the generators that Mestre produced, we can show that the class group of  $F$  has 2-rank at least 13, but we cannot show it is any greater than that.

EXAMPLE II. A curve of genus 2 whose Jacobian has rank 7 over  $\mathbf{Q}$ .

Let  $C$  be the hyperelliptic curve defined over  $\mathbf{Q}$  by the equation  $Y^2 = f$  where  $f = X^5 + 16X^4 - 274X^3 + 817X^2 + 178X + 1$ . Let  $J$  be the Jacobian of the normalization of  $C$ . The characteristic polynomial of the Frobenius for  $J$  over  $\mathbf{F}_3$  is  $t^4 + t^3 + 3t^2 + 3t + 9$  which is irreducible over  $\mathbf{Q}$ , so  $J$  is simple over  $\mathbf{Q}$ . Let  $\{\alpha_i\}$  be the set of roots of  $f$ . A basis for  $J[2]$  is the set of points  $(\alpha_i, 0) - \infty$  for  $i = 1$  to 4. The point  $(\alpha_5, 0) - \infty$  is the sum of the other 4. The 2-torsion points are all defined over the splitting field of  $f$  which is the simplest quintic field  $L$  with discriminant  $941^4$  (see [24]). Simplest quintic fields are Galois over  $\mathbf{Q}$ . The polynomial  $f$  has discriminant  $941^4 191^2$ . The primes we have to worry about are  $\infty$ , 2, 191, and 941. We would like to show that  $J(\mathbf{Q})$  has rank 7.

We have  $L \cong F = \mathbf{Q}[T]/f(T)$  in the notation of Subsection 5.1. The group  $H^1(\mathbf{Q}, J[2])$  is isomorphic to the kernel of the norm from  $L^*/L^{*2}$

to  $\mathbf{Q}^*/\mathbf{Q}^{*2}$ . If we compose this isomorphism with the coboundary embedding from  $J(\mathbf{Q})/2J(\mathbf{Q})$  to  $H^1(\mathbf{Q}, J[2])$  we get a map which is identical to the map  $X - T$  which is defined as follows (see [23]). Pick a degree 0 divisor  $D = \sum n_i R_i$  of  $C$  defined over  $\mathbf{Q}$  whose support does not contain any point of  $C$  with  $Y = 0$  or the point  $\infty$ . Define

$$(X - T)(D) = \prod (X(R_i) - T)^{n_i}.$$

One can show that the image of a point  $(x, y) - \infty$  where  $y \neq 0$  is  $x - T$  by finding the image of an equivalent divisor whose support does not contain  $\infty$ . Let  $L_p = \mathbf{Q}_p[T]/f(T)$ . We similarly have embeddings of  $J(\mathbf{Q}_p)/2J(\mathbf{Q}_p)$  into  $L_p^*/L_p^{*2}$  by the map  $X - T$ . If the prime  $p$  of  $\mathbf{Q}$  splits in  $L$  then  $L_p$  is isomorphic to the product of 5 copies of  $\mathbf{Q}_p$  and the 2-torsion is rational over  $\mathbf{Q}_p$ . Then we have

$$L_p \cong \mathbf{Q}_p[T]/f(T) \cong \mathbf{Q}_p \times \cdots \times \mathbf{Q}_p \quad \text{by } T \mapsto (\alpha_1, \dots, \alpha_5).$$

Again by finding the image of an equivalent divisor one can show that the point  $(\alpha_i, 0) - \infty$  maps to  $\alpha_i - \alpha_j$  at the  $j$ th component of  $(\mathbf{Q}_p^*/\mathbf{Q}_p^{*2})^5$  for  $j \neq i$  and to the product of the other 4 entries at the  $i$ th component.

The 2-rank of the class group of  $L$  is 4 (see [24]). Since condition (5) of Lemma 5.1 is satisfied, the groups  $H^i(G, J[2])$  are trivial for all  $i$  and for all  $G$  contained in  $\text{Gal}(L/\mathbf{Q})$ . Therefore the group  $H^1(\mathbf{Q}, J[2])$  is isomorphic to both  $\text{Hom}_{\text{Gal}(L/\mathbf{Q})}(\text{Gal}(\bar{L}, L), J[2])$  and to the kernel of the norm from  $L^*/L^{*2}$  to  $\mathbf{Q}^*/\mathbf{Q}^{*2}$ . Thus, from Theorem 5.3, the group  $C^2(\mathbf{Q}, J)$  is isomorphic to the group of unramified elements in the kernel of the norm from  $L^*/L^{*2}$  to  $\mathbf{Q}^*/\mathbf{Q}^{*2}$ . Since  $\mathbf{Q}$  has a trivial class group, we know  $C^2(\mathbf{Q}, J)$  is isomorphic to exactly one copy of the dual of  $\text{Cl}(L)/\text{Cl}(L)^2$ . Therefore  $C^2(\mathbf{Q}, J)$  has rank 4. The roots of  $f$  are all real, one is in the interval  $(-28, -27)$ , two are in  $(-1, 0)$ , one in  $(5, 6)$  and one in  $(6, 7)$ . Since there are 3 negative roots and 2 positive roots and they are units, the narrow and wide class numbers of  $L$  are the same.

The points  $(-17, \pm 1223)$ ,  $(-9, \pm 557)$ ,  $(-6, \pm 317)$ ,  $(-2, \pm 73)$ ,  $(0, \pm 1)$  and  $(4, \pm 37)$  are all in  $C(\mathbf{Q})$ . The points  $((5 + \sqrt{177})/2, \pm 191)$  and  $(5 - \sqrt{177})/2, \pm 191)$  of  $C$  give conjugates over  $\mathbf{Q}$  and we will denote them by  $(\beta_1, \pm 191)$  and  $(\beta_2, \pm 191)$  respectively. In this example, the notation  $(n)$  will refer to the divisor  $(n, \sqrt{f(n)}) - \infty$  and its image in  $J(N)/2J(N)$  over the appropriate field  $N$ . Let us compute the local groups for the four interesting primes. We know from the proof of Proposition 5.4 that the size of  $J(\mathbf{R})/2J(\mathbf{R})$  is the same as  $\#J(\mathbf{R})[2]/2^2$  which is 4. If we map  $(-2)$  into  $(L_\infty^*/L_\infty^{*2})^5$ , which is isomorphic to  $(\mathbf{R}^*/\mathbf{R}^{*2})^5$ , we get  $(1, -1, -1, -1, -1)$  and if we map  $(0)$  we get  $(1, 1, 1, -1, -1)$ . So  $(-2)$  and  $(0)$  generate  $J(\mathbf{R})/2J(\mathbf{R})$ . Now the prime 2 is inert in  $L$  and so

TABLE I

Some Points of  $J(\mathbf{Q}_{191})/2J(\mathbf{Q}_{191})$  and Their Images in  $L_{191}^*/L_{191}^{*2}$ 

|                         | $x-5$ | $x-6$ | $x-37$ | $x-\alpha_4$ | $x-\alpha_5$ |
|-------------------------|-------|-------|--------|--------------|--------------|
| $(\alpha_1)$            | 1     | -1    | -1     | -1           | -1           |
| $(\alpha_2)$            | 1     | 1     | 1      | -1           | -1           |
| $(\alpha_3)$            | 1     | -1    | -1     | 1            | 1            |
| $(\alpha_4)$            | 1     | 1     | -1     | $\pi$        | $-\pi$       |
| $(\alpha_5)$            | 1     | 1     | -1     | $\pi$        | $-\pi$       |
| $(-17)$                 | 1     | -1    | -1     | 1            | 1            |
| $(-9)$                  | 1     | -1    | -1     | 1            | 1            |
| $(-6)$                  | 1     | -1    | -1     | 1            | 1            |
| $(-2)$                  | 1     | -1    | -1     | 1            | 1            |
| $(0)$                   | -1    | -1    | 1      | 1            | 1            |
| $(4)$                   | -1    | -1    | 1      | 1            | 1            |
| $(\beta_1) + (\beta_2)$ | 1     | -1    | 1      | $-\pi$       | $\pi$        |

$J(\mathbf{Q}_2)[2]$  is trivial. Thus the group  $C^2(\mathbf{Q}_2, J)$  is trivial and from Proposition 3.9, the group  $S^2(\mathbf{Q}_2, J)$  has rank 2. The prime 941 ramifies totally in  $L$  and so  $J(\mathbf{Q}_{941})[2]$  is trivial as are the groups  $S^2(\mathbf{Q}_{941}, J)$  and  $C^2(\mathbf{Q}_{941}, J)$  (and so this prime can be ignored).

We have

$$Y^2 = f = (X - \alpha_1) \cdots (X - \alpha_5) \equiv (X - 5)(X - 6)(X - 37)(X - 159)^2 \pmod{191}.$$

So the prime 191 splits in  $L$  and so  $C^2(\mathbf{Q}_{191}, J)$  and  $S^2(\mathbf{Q}_{191}, J)$  each have rank 4. In Table I we present a list of some rational points of  $J(\mathbf{Q}_{191})$  and their images in  $L_{191}^*/L_{191}^{*2}$  where  $\pi$  is a prime element and  $-1$  is a quadratic non-residue modulo 191. Along the top is written  $x - \alpha_i$  to remind us how to compute the  $i$ th component.

We see that  $(\alpha_1)$ ,  $(\alpha_4)$ ,  $(-2)$  and  $(0)$  form a basis for  $J(\mathbf{Q}_{191})/2J(\mathbf{Q}_{191})$  and that  $I^2(\mathbf{Q}_{191}, J)$  has rank 3. So our first estimates from Theorem 4.1 show that  $C^2(\mathbf{Q}, J)/I^2(\mathbf{Q}, J)$  has rank at most 1, from the prime 191, and  $S^2(\mathbf{Q}, J)/I^2(\mathbf{Q}, J)$  has rank at most 5, which is 2 from the infinite prime, 2 from the prime 2 and 1 from the prime 191. Using the fact that the narrow and wide class numbers are the same, we see that we cannot have a quadratic extension of  $L$  which is ramified only at  $\infty$  therefore  $S^2(\mathbf{Q}, J)/I^2(\mathbf{Q}, J)$  has rank at most 3. Since  $C^2(\mathbf{Q}, J)$  has rank 4, we see from Theorem 4.1 that the rank of  $S^2(\mathbf{Q}, J)$  is between 3 and 7.

At this point we will show that  $(-17)$ ,  $(-9)$ ,  $(-6)$ ,  $(-2)$ ,  $(0)$ ,  $(4)$  and  $(\beta_1) + (\beta_2)$  are all independent points of infinite order in  $J(\mathbf{Q})$ . The prime 37 splits in  $L$  and we have

$$Y^2 = f \equiv (X - 4)(X - 8)(X - 12)(X - 16)(X - 18) \pmod{37}.$$



TABLE II

Some Points of  $J(\mathbf{Q}_{37})/2J(\mathbf{Q}_{37})$  and Their Images in  $L_{37}^*/L_{37}^{*2}$

|                         | $x-4$ | $x-8$ | $x-12$ | $x-16$ | $x-18$ |
|-------------------------|-------|-------|--------|--------|--------|
| $(-17)$                 | 1     | 1     | 2      | 1      | 2      |
| $(-9)$                  | 2     | 2     | 1      | 1      | 1      |
| $(-6)$                  | 1     | 2     | 2      | 2      | 2      |
| $(0)$                   | 1     | 2     | 1      | 1      | 2      |
| $(-2)$                  | 2     | 1     | 2      | 2      | 2      |
| $(4)$                   | 1     | 1     | 2      | 1      | 2      |
| $(\beta_1) + (\beta_2)$ | 2     | 2     | 1      | 1      | 1      |

In Table II are the images of the given rational points in  $L_{37}^*/L_{37}^{*2}$ ; where 2 is a quadratic non-residue of 37.

Since none of the images of these points is trivial, none of them is a torsion point. Notice that  $(-17), (-9), (-6), (0)$  are all independent, and so are independent points of  $J(\mathbf{Q})$  of infinite order. We have the relations  $(-2) = (-9) + (-6), (4) = (-17)$  and  $(\beta_1) + (\beta_2) = (-9)$  in  $J(\mathbf{Q}_{37})/2J(\mathbf{Q}_{37})$ . The prime 73 also splits in  $L$  and we have

$$Y^2 = f \equiv (X + 26)(X + 19)(X + 2)(X - 13)(X - 18) \pmod{73}.$$

In Table III are the images of the given rational points in  $L_{73}^*/L_{73}^{*2}$ ; where 5 is a quadratic non-residue of 73. We see that  $(-2)$  is independent of  $(-17), (-9), (-6), (0)$ . Now if there is a dependence relation of  $(4)$  on  $(-17), (-9), (-6), (0)$  and  $(-2)$  in  $J(\mathbf{Q})/2J(\mathbf{Q})$  then the same relation holds in any  $J(\mathbf{Q}_p)/2J(\mathbf{Q}_p)$ . Over  $\mathbf{Q}_{37}$  the only such relations involving  $(4)$  are  $(4) = (-17)$  and  $(4) = (-17) + (-2) + (-9) + (-6)$ . Over  $\mathbf{Q}_{73}$  the only such relations involving  $(4)$  are  $(4) = (-9) + (-2)$  and  $(4) = (-17) + (-6) + (-2)$ . Since there is no intersection in relations locally, there is no

TABLE III

Some Points of  $J(\mathbf{Q}_{73})/2J(\mathbf{Q}_{73})$  and Their Images in  $L_{73}^*/L_{73}^{*2}$

|                         | $x+26$ | $x+19$ | $x+2$ | $x-13$ | $x-18$ |
|-------------------------|--------|--------|-------|--------|--------|
| $(-17)$                 | 1      | 1      | 5     | 5      | 1      |
| $(-9)$                  | 5      | 5      | 5     | 5      | 1      |
| $(-6)$                  | 5      | 5      | 1     | 1      | 1      |
| $(0)$                   | 5      | 1      | 1     | 5      | 1      |
| $(-2)$                  | 1      | 5      | 5     | 5      | 5      |
| $(4)$                   | 5      | 1      | 1     | 1      | 5      |
| $(\beta_1) + (\beta_2)$ | 1      | 5      | 1     | 5      | 1      |

relation globally. From its image in  $L_{191}^*/L_{191}^{*2}$ , it is clear that the point  $(\beta_1) + (\beta_2)$  is independent of the rest. Therefore the Mordell–Weil rank of  $J$  over  $\mathbf{Q}$  is at least 7. But the Selmer group has rank at most 7. Therefore the Mordell–Weil rank is exactly 7.

In this example, as in the last, we have  $C^2(\mathbf{Q}, J) = I^2(\mathbf{Q}, J)$ . It is a straightforward computation to show that the images of the four independent points  $(-2) + (-6)$ ,  $(-2) + (-9)$ ,  $(-2) + (-17)$ ,  $(0) + (4)$  are unramified at all primes.

EXAMPLE III.  $C^2(K, A)$  is not always contained in  $S^2(K, A)$ .

In the examples that have been worked out in the literature like the ones above, the group of unramified homomorphisms is always contained in the Selmer group; see [7, 20, 30] and [27, p. 321, 10.9(e)]. This is not always the case, however. Let  $L$  be a cyclic cubic extension of  $\mathbf{Q}$  with class number 4; such fields exist, like the one with conductor 163. Now  $C^2(\mathbf{Q}, E) = \text{Hom}_{\text{Gal}(L/\mathbf{Q})}(\text{Gal}(H(L)/L), E[2])$  where  $H(L)$  is the Hilbert class field of  $L$ . Since  $H^2(\text{Gal}(L/\mathbf{Q}), E[2]) = 0$ , there is only one possible Galois group  $\text{Gal}(H(L)/\mathbf{Q})$ . Since  $A_4$  contains  $V_4$  as a subgroup and the quotient acts on  $V_4$  as  $\text{Gal}(L/\mathbf{Q})$  acts on  $E[2]$ , we know that  $A_4$  must be that group. Let  $\mathfrak{p}$  be a prime of  $H(L)$  whose restriction to  $\mathbf{Q}$  is  $p$ , an odd prime, and assume that  $\mathfrak{p}$  is an unramified extension of  $p$  with a decomposition group of order two. By Tchebotarov's density theorem, there are infinitely many such primes. Choose a polynomial  $f \in \mathbf{Z}[X]$  whose roots generate  $L$  and assume  $p$  does not divide the discriminant of  $f$ . Let the following be the factorization of  $f$ :

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

and define  $g$  in the following way:

$$g = (X - p\alpha_1)(X - p\alpha_2)(X - p\alpha_3).$$

Let  $E$  be the elliptic curve defined by the equation  $Y^2 = g$ . The points  $T_i = (p\alpha_i, 0)$  are the non-trivial 2-torsion points. There are four  $\text{Gal}(L/\mathbf{Q})$ -invariant homomorphisms from  $\text{Gal}(H(L)/L)$  to  $E[2]$ ; these are the four elements of  $C^2(\mathbf{Q}, E)$ . They restrict onto the four unramified homomorphisms in  $\text{Hom}(\text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p), E[2])$ . The 2-torsion points are representatives for  $E(\mathbf{Q}_p)/2E(\mathbf{Q}_p)$ . These points are mapped to the homomorphisms that send an element  $\psi \in \text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$  to  $\psi \frac{1}{2}T_i - \frac{1}{2}T_i$  where  $\frac{1}{2}T_i$  is a 4-torsion point. The coordinates of the 4-torsion points lying over the point  $(p\alpha_1, 0)$  are

$$\begin{aligned} & (p\alpha_1 \pm p \sqrt{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}, \\ & \pm p \sqrt{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} (\sqrt{p(\alpha_1 - \alpha_2)} \pm \sqrt{p(\alpha_1 - \alpha_3)}) \end{aligned}$$

where the first and third  $\pm$  must agree. From the  $Y$ -coordinates, it is clear that the 4-torsion points are defined over a ramified extension of  $\mathbf{Q}_p$ . By symmetry, all three non-trivial 2-torsion points will map to ramified homomorphisms. So the sizes of  $S^2(\mathbf{Q}_p, E)$  and  $C^2(\mathbf{Q}_p, E)$  are each 4 and they have trivial intersection. One could also show this by noticing that  $E$  has type  $I_0^*$  reduction over  $\mathbf{Q}_p$  with  $E(\mathbf{Q}_p)/2E(\mathbf{Q}_p) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  and using Theorem 3.7. Since the group  $C^2(\mathbf{Q}, E)$  maps onto the group  $C^2(\mathbf{Q}_p, E)$ , which has trivial intersection with the group  $S^2(\mathbf{Q}_p, E)$ , the group  $C^2(\mathbf{Q}, E)$  cannot be contained in the 2-Selmer group.

#### ACKNOWLEDGMENTS

I thank Hendrik Lenstra for his support and guidance throughout the preparation of this paper and for suggesting the proofs of Lemma 5.1 and Theorem 5.3. I also thank Bas Edixhoven, Everett Howe, and Joseph Wetherell for their helpful advice.

#### REFERENCES

1. M. ARTIN, Néron models, in "Arithmetic Geometry" (G. Cornell and J. H. Silverman, Eds.), pp. 213–230, Springer-Verlag, New York, 1986.
2. M. F. ATIYAH AND C. T. C. WALL, Cohomology of groups, in "Algebraic Number Theory" (J. W. S. Cassels and A. Fröhlich, Eds.), pp. 94–115, Academic Press, London, 1967.
3. B. J. BIRCH AND H. P. F. SWINNERTON-DYER, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** (1963), 7–25.
4. A. BRUMER AND K. KRAMER, The rank of elliptic curves, *Duke Math. J.* **44** (1977), 715–743.
5. H. COHN, A device for generating fields of even class number, *Proc. Amer. Math. Soc.* **7** (1956), 595–598.
6. G. CORNELL AND J. SILVERMAN, (Eds.) "Arithmetic Geometry", Springer-Verlag, New York, 1986.
7. H. EISENBEIS, G. FREY, AND B. OMMERBORN, Computation of the 2-rank of pure cubic fields, *Math. Comp.* **32** (1978), 559–569.
8. E. V. FLYNN, Descent via isogeny in dimension 2, *Acta Arith.* **66** (1994), 23–43.
9. D. GORDON AND D. GRANT, Computing the Mordell–Weil rank of Jacobians of curves of genus two, *Trans. AMS* **337** (1993), 807–824.
10. H. KOCH, "Galoissche Theorie der  $p$ -Erweiterungen," VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
11. K. KODAIRA, On compact analytic surfaces II, *Ann. Math.* **77** (1963), 563–626.
12. S. LANG, "Abelian Varieties," Interscience, New York, 1959.
13. A. MATTUCK, Abelian varieties over  $p$ -adic ground fields, *Ann. Math.* **62** (1955), 92–119.
14. W. G. MCCALLUM, The arithmetic of Fermat curves, *Math. Ann.* **294** (1992), 503–511.
15. J. F. MESTRE, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, *J. Reine Angew. Math.* **343** (1983), 23–35.
16. J. F. MESTRE, Formules explicites et minorations de conducteurs, *Comp. Math.* **58** (1986), 209–232.

17. J. S. MILNE, "Arithmetic Duality Theorems," Academic Press, Orlando, FL, 1986.
18. D. MUMFORD, "Abelian Varieties," Oxford Univ. Press, Oxford, 1970.
19. A. NÉRON, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, *Publ. Math. Inst. Hautes Études Sci.* **21** (1964), 361–482
20. J. QUER, Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), 215–218.
21. M. ROSEN, Abelian Varieties over  $\mathbb{C}$ , in "Arithmetic Geometry" (G. Cornell and J. H. Silverman, Eds.), pp. 79–101, Springer-Verlag, New York, 1986.
22. P. SATGÉ, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986), 294–317.
23. E. SCHAEFER, 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995), 219–232.
24. R. SCHOOF AND L. C. WASHINGTON, Quintic polynomials and real cyclotomic fields, *Math. Comp.* **50** (1988), 543–556.
25. J. P. SERRE, "Local Fields," Springer-Verlag, New York, 1979.
26. D. SHANKS, The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.
27. J. H. SILVERMAN, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.
28. J. TATE, Algorithm for determining the type of a singular fiber in an elliptic pencil, in "Modular Functions of One Variable IV," Lecture Notes in Math., Vol. 476, pp. 33–52, Springer-Verlag, Berlin, 1975.
29. J. VÉLU, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A* **273** (1971), 238–241.
30. L. C. WASHINGTON, Class numbers of the simplest cubic fields, *Math. Comp.* **48** (1987), 371–384.