Math. Ann. 310, 447–471 (1998)

Mathematische Annalen

Computing a Selmer group of a Jacobian using functions on the curve

Edward F. Schaefer

Department of Mathematics, Santa Clara University, Santa Clara, CA 95053, USA
(e-mail: eschaefer@scuacc.scu.edu)

Received 22 July 1996 / Revised version 17 March 1997

Mathematics Subject Classification (1991): 11G30, 11D25, 11G10, 14G25, 14H25, 14H40, 14H45

1 Introduction

Several algorithms have been developed for computing Selmer groups for the Jacobians of curves. Typically, one is interested in computing a Selmer group in order to bound a Mordell-Weil rank or study a part of a Tate-Shafarevich group (see, for example, [Kr]). For curves of genera 1 and 2, algorithms using homogeneous spaces have been developed for computing Selmer groups ([BSD, GG]). Already in the genus 2 case, the homogeneous spaces are quite difficult to describe. For that reason, these tend to be somewhat unwieldy to implement. Other algorithms use functions on the curve to compute a Selmer group ([BK, Ca, CF, Fd, FPS, KS, Mc, PS, Sc1, Tp]). These tend to be far easier. Their success, however, seems to be based on two assumptions. These assumptions have been satisfied in the examples presented, so far, but should not be expected to be satisfied in all cases. In this paper, we attempt to provide a framework for the study and development of algorithms for computing Selmer groups using functions on the curve. In particular, we consider the assumptions they are based on.

Let C be a curve defined over the number field K and let J be its Jacobian. We standardly identify J with $\mathrm{Pic}^0(C(\overline{K}))$ which we will denote $\mathrm{Pic}^0(C)$. Let A be an abelian variety defined over K and let $\phi : A \to J$ be an isogeny defined over K. Let $A[\phi]$ denote the kernel of ϕ. For most practical purposes (such as descent), it is really only useful to work with an isogeny whose kernel has a prime-power exponent. So we assume that $A[\phi]$ has exponent $q = p^l$ for some prime number p.

In Sect. 2 we provide a framework for developing an algorithm for computing the ϕ-Selmer group for A over K. For the sake of clarity, we first describe a straightforward way of creating such an algorithm. The assumptions that such an algorithm is based on are discussed in Sect. 2.4. All but one algorithm in the literature, that the author is aware of, fits into the framework described. In Sect. 2.5, we discuss how this framework can be extended in special cases to encompass this and other algorithms.

The strength of this approach is that it allows us to develop an algorithm tailored to the data at hand. We give several examples. In Sect. 3 we describe an algorithm for computing a Selmer group for curves of the form $y^p = f(x)$ where p is a prime not dividing the degree of f. We do three examples. Let ζ_p denote a primitive pth root of unity. In the first, we find the Mordell-Weil ranks of the Jacobian of $y^3 = (x^2+1)(x^2-4x+1)$ over $\mathbf{Q}(\zeta_3)$ and $\mathbf{Q}$. In the second we describe all solutions of $y^2 = x^5+1$ in fields of degree 2 or less over $\mathbf{Q}$. In the third we describe all solutions of $y^3 = x(x-1)(x-2)(x-3)$ in fields of degree 3 or less over $\mathbf{Q}$. In the latter two examples, the Mordell-Weil ranks of the Jacobians are 0 over $\mathbf{Q}(\zeta_5)$ and $\mathbf{Q}(\zeta_3)$ respectively. In Sect. 4 we compute the 2-Selmer group and Mordell-Weil rank, over $\mathbf{Q}$, of the Jacobian of a smooth plane quartic curve, using bitangents of the curve.

In Sect. 5 we give a review of the literature in which algorithms for curves of genus greater than 1 are discussed.

2 The algorithm

Let us define the Selmer group. Let J, K, A, ϕ, q and p be as in Sect. 1. Let S be a finite set of primes of K that includes primes over p, primes dividing the conductor of A, and if $p = 2$, includes real primes also. For any $\mathrm{Gal}(\overline{K}/K)$-module M let $M(K)$ denote the $\mathrm{Gal}(\overline{K}/K)$-invariants of M and $H^1(K,M)$ denote $H^1(\mathrm{Gal}(\overline{K}/K),M)$. Let $H^1(K,A[\phi];S)$ denote the subgroup of $H^1(K,A[\phi])$ of cocycle classes that are unramified outside S. Let δ be the map from $J(K)$ to $H^1(K,A[\phi])$ arising from the long exact sequence of Galois cohomology attached to the short exact sequence

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

The kernel of δ is $\phi A(K)$. Similarly, for any prime $\mathfrak{s} \in S$ we have a coboundary map $\delta_\mathfrak{s}$ from $J(K_\mathfrak{s})$ to $H^1(K_\mathfrak{s},A[\phi])$ with kernel $\phi A(K_\mathfrak{s})$. Let $\alpha_\mathfrak{s}$ be the restriction map from $H^1(K,A[\phi])$ to $H^1(K_\mathfrak{s},A[\phi])$. The following is a commutative diagram.

$$\begin{array}{ccc} J(K)/\phi A(K) & \xhookrightarrow{\delta} & H^1(K,A[\phi];S) \\ \downarrow & & \downarrow \prod \alpha_\mathfrak{s} \\ \prod\limits_{\mathfrak{s}\in S} J(K_\mathfrak{s})/\phi A(K_\mathfrak{s}) & \xhookrightarrow{\prod \delta_\mathfrak{s}} & \prod\limits_{\mathfrak{s}\in S} H^1(K_\mathfrak{s},A[\phi]) \end{array}$$

Define the Selmer group, $S^{\phi}(K,A)$, to be the intersection of the groups $\alpha_{\mathfrak{s}}^{-1}(\delta_{\mathfrak{s}}(J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})))$ for all $\mathfrak{s} \in S$. This is equivalent to the usual definition (see [Mi3, p. 92]).

In Sect. 2.1, we find a finitely generated K-algebra L and a map F, derived from functions on C, so that F maps $J(K)/\phi A(K)$ to L^*/L^{*q}. In Sect. 2.2 we find a map ι from $H^1(K,A[\phi])$ to L^*/L^{*q} so that $F = \iota \circ \delta$. The map ι will be induced from a Weil pairing and a Kummer map. Let $L_{\mathfrak{s}} = L \otimes_K K_{\mathfrak{s}}$. We will similarly be able to define maps $F_{\mathfrak{s}}$ and $\iota_{\mathfrak{s}}$ so that $F_{\mathfrak{s}} = \iota_{\mathfrak{s}} \circ \delta_{\mathfrak{s}}$. Once these maps are defined, the following will be a commutative diagram where the $\beta_{\mathfrak{s}}$'s are natural maps.

$$\begin{array}{ccccc} J(K)/\phi A(K) & \overset{\delta}{\hookrightarrow} & H^1(K,A[\phi];S) & \overset{\iota}{\hookrightarrow} & L^*/L^{*q} \\ \downarrow & & \downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \beta_{\mathfrak{s}} \\ \prod\limits_{\mathfrak{s}\in S} J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}}) & \overset{\prod \delta_{\mathfrak{s}}}{\hookrightarrow} & \prod\limits_{\mathfrak{s}\in S} H^1(K_{\mathfrak{s}},A[\phi]) & \overset{\prod \iota_{\mathfrak{s}}}{\hookrightarrow} & \prod\limits_{\mathfrak{s}\in S} L_{\mathfrak{s}}^*/L_{\mathfrak{s}}^{*q} \end{array}$$

We finish that section by making an assumption causing ι and $\iota_{\mathfrak{s}}$ and hence F and $F_{\mathfrak{s}}$ to be injective. In Sect. 2.3, we show how to use the maps F and $F_{\mathfrak{s}}$ to compute the Selmer group.

In order for the maps F and $F_{\mathfrak{s}}$ to be derived from functions on C, we need to make the following assumption. We will denote $\mathrm{Div}^0(C(\overline{K}))$ by $\mathrm{Div}^0(C)$.

Assumption I: For $\mathscr{K} = K$ or $K_{\mathfrak{s}}$, with $\mathfrak{s} \in S$, every element of $J(\mathscr{K})/\phi A(\mathscr{K})$ is represented by a divisor class containing an element of $\mathrm{Div}^0(C)(\mathscr{K})$, the divisors of C of degree 0 defined over $\mathscr{K}$.

2.1 The choice of F and L

Since we will be dealing with a Weil pairing, we need to consider the dual isogeny to ϕ. Let $\hat{\phi} : \hat{J} \to \hat{A}$ be the dual isogeny to ϕ and $\hat{J}[\hat{\phi}]$ be the kernel of $\hat{\phi}$. Let $\lambda : J \to \hat{J}$ be the canonical principal polarization of J with respect to C. Since C is defined over K, the principal polarization λ is also (see [Mi1, p. 186]). Let $\Psi = \lambda^{-1}(\hat{J}[\hat{\phi}])$; we know Ψ is contained in $J[q]$.

Step 1. Determine the subgroup of $J[q]$ that is Ψ.

If ϕ is the multiplication by q map, then $\Psi = J[q]$. For non-trivial examples, see Proposition 3.1 and Sect. 5.

Step 2. Choose some suitable $\mathrm{Gal}(\overline{K}/K)$-invariant set of divisors in $\mathrm{Div}^0(C)$ whose classes span Ψ.

We denote the linear equivalence class of the degree-0 divisor D in $\mathrm{Pic}^0(C)$ by $[D]$. We choose $\{D_1,\ldots,D_n\}$ to be a $\mathrm{Gal}(\overline{K}/K)$-invariant set of degree-0 divisors of C for which the divisor classes $\{[D_i]\}$ span Ψ. As we will see, the choice of spanning set determines the map F and the K-algebra L. Typically one wants a minimal, Galois-invariant spanning set. We also want to pick a spanning set so that the second assumption holds, if possible. This is discussed in Sect. 2.4.

Step 3. Determine the map F and the finitely generated K-algebra L based on the divisors chosen in Step 2.

First we define the finitely generated K-algebra L. Let

$$L' = \prod_{i=1}^{n} \overline{K_i}$$

with $K_i = K$. Let us define an action of $\mathrm{Gal}(\overline{K}/K)$ on L'. If $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then let $\overline{\sigma} \in S_n$ be defined such that if ${}^{\sigma}D_i = D_j$, then $\overline{\sigma} i = j$. Let

$${}^{\sigma}(a_1, \ldots, a_n) = ({}^{\sigma}a_{\overline{\sigma}^{-1}1}, \ldots, {}^{\sigma}a_{\overline{\sigma}^{-1}n})$$

for $a_i \in \overline{K_i}$. Define L to be the $\mathrm{Gal}(\overline{K}/K)$-invariants in L'.

Let us find a more practical description of L. Let Λ be a subset of $\{1, 2, \ldots, n\}$ such that the set $\{D_j\}_{j \in \Lambda}$ contains one representative of each $\mathrm{Gal}(\overline{K}/K)$-orbit of $\{D_i\}$. Let $L_j = K(D_j)$ be the minimal field of definition of D_j. Then we can find an isomorphism

$$L \cong \prod_{j \in \Lambda} L_j.$$

Let us describe that isomorphism. For simplicity, assume that $\mathrm{Gal}(\overline{K}/K)$ acts transitively on the $\{D_i\}$ and let $\Lambda = 1$. We have $L_1 = K(D_1)$. Let $\{\sigma_i\}$ be elements of $\mathrm{Gal}(\overline{K}/K)$ such that

$$\mathrm{Gal}(\overline{K}/K) = \coprod_i \sigma_i \, \mathrm{Gal}(\overline{K}/L_1)$$

and ${}^{\sigma_i}D_1 = D_i$. We have

$$L_1 \cong L \text{ by } l \in L_1 \mapsto ({}^{\sigma_1}l, \ldots, {}^{\sigma_n}l) \in \prod_{i=1}^{n} \overline{K_i}.$$

If there are several orbits, then we can extend this isomorphism by concatenation.

Let us define the map F. Let $qD_i = (f_i)$ where f_i is defined over $K(D_i)$. Such f_i's exist over $K(D_i)$ by Hilbert's Theorem 90. Let $\mathrm{Supp}(D_i)$ be the support of the divisor D_i.

Definition. *The avoidance set is the set of points* $\cup \mathrm{Supp}(D_i)$ *in* $C(\overline{K})$.

Define $F = (f_1, \ldots, f_n)$ from the complement of the avoidance set to L'. By abuse of notation we use P_L to denote the n-tuples of divisors and divisor classes $(D_1, \ldots, D_n)$ and $([D_1], \ldots, [D_n])$. Let $\hat{P}_L$ denote the n-tuple of elements $(\lambda[D_1], \ldots, \lambda[D_n])$ of $\hat{J}[\hat{\phi}]$.

2.2 Equivalence of maps

In this subsection we show that F induces a well-defined homomorphism from $J(K)/\phi A(K)$ to L^*/L^{*q} and that F is related to cohomological maps used to define a Selmer group. We will return to the algorithm in Subsect. 2.3.

Definition. *A good divisor is a divisor of C of degree 0, defined over K (or K_s), whose support does not intersect the avoidance set.*

From Assumption I, every element of $J(K)/\phi A(K)$ is represented by a divisor class containing a divisor of degree 0, defined over K. From [La, Lemma 3, p. 166], every divisor class that contains a divisor defined over K, contains a divisor defined over K, whose support does not intersect any given finite set, in particular, the avoidance set. So every element of $J(K)/\phi A(K)$ is represented by a good divisor.

Let g be a K-defined function from C to $\overline{K}$. Let $R = \sum n_i R_i$ be a divisor of C of degree 0, defined over K, whose support does not intersect the support of (g). We define

$$g(R) = \prod (g(R_i))^{n_i} \in K^*.$$

By abuse of notation we define the map F from good divisors to L^* in an analogous way.

The map F on good divisors, composed with the isomorphism of L with $\prod_{j\in\Lambda} L_j$, is the map $\prod_{j\in\Lambda} f_j$. In examples, we will often denote $\prod_{j\in\Lambda} L_j$ by L and this composition by F, since they are more practical.

Lemma 2.1. *The map F induces a homomorphism from the subgroup of $J(K)/qJ(K)$ represented by divisor classes containing good divisors to L^*/L^{*q}.*

Proof. The good divisors form a subgroup of $\mathrm{Div}^0(C)(K)$. The map F is a homomorphism from good divisors to L^*. Let D and D' be linearly equivalent good divisors. We would like to show that $F(D - D')$ is in L^{*q}. Let h be a K-defined function with $(h) = D - D'$. From Weil reciprocity, we have the following equalities of n-tuples

$$F(D - D') = F((h)) = h((F)) = h(qP_L) = (h(P_L))^q \in L^*.$$

Since P_L is fixed by $\mathrm{Gal}(\overline{K}/K)$ we know $h(P_L)$ is in L^*. So $F(D - D')$ is in L^{*q}. □

At this point let us relate the map F to the maps derived from cohomology which are traditionally used to compute a Selmer group. First let us recall the definition of the Weil pairing. Let τ be an isogeny of abelian varieties from B to V and $\hat{\tau}$ be the dual isogeny from $\hat{V}$ to $\hat{B}$. Let $P \in B[\tau]$ and $Q \in \hat{V}[\hat{\tau}]$ and D be a divisor on $\hat{B}$ representing P. There is a function g on $\hat{V}$ with divisor $\hat{\tau}^{-1}D$. Then $e_\tau(P, Q) = g(X + Q)/g(X)$ for any $X \in \hat{V}$ for which the right hand side of the equation is defined.

Let $\mu_q(L')$ be the qth roots of unity in L'. We have

$$\mu_q(L') \cong \mu_q(\overline{K_1}) \times \ldots \times \mu_q(\overline{K_n}).$$

Let $e_\phi(P, Q)$ denote the ϕ-Weil pairing of $P \in A[\phi]$ and $Q \in \hat{J}[\hat{\phi}]$. Define the map w from $A[\phi]$ to $\mu_q(L')$ by

$$w(P) = e_\phi(P, \hat{P}_L) = (e_\phi(P, \lambda[D_1]), \ldots, e_\phi(P, \lambda[D_n])).$$

Proposition 2.2. *The map w from $A[\phi]$ to $\mu_q(L')$ is injective and defined over K.*

Proof. Since the elements of the n-tuple $\hat{P}_L$ span $\hat{J}[\hat{\phi}]$, the map w is injective from the non-degeneracy of the Weil pairing. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We would like to show that ${}^\sigma w(P) = w({}^\sigma P)$. We have

$$w({}^\sigma P) = (e_\phi({}^\sigma P, \lambda[D_1]), \ldots, e_\phi({}^\sigma P, \lambda[D_n]))$$

and

$$\begin{aligned} {}^\sigma w(P) &= {}^\sigma(e_\phi(P, \lambda[D_1]), \ldots, e_\phi(P, \lambda[D_n])) \\ &= ({}^\sigma e_\phi(P, \lambda[D_{\overline{\sigma}^{-1}1}]), \ldots, {}^\sigma e_\phi(P, \lambda[D_{\overline{\sigma}^{-1}n}])) \\ &= (e_\phi({}^\sigma P, \lambda[{}^\sigma D_{\overline{\sigma}^{-1}1}]), \ldots, e_\phi({}^\sigma P, \lambda[{}^\sigma D_{\overline{\sigma}^{-1}n}])) \\ &= (e_\phi({}^\sigma P, \lambda[D_1]), \ldots, e_\phi({}^\sigma P, \lambda[D_n])). \end{aligned}$$

□

The map w induces a map from $H^1(K, A[\phi])$ to $H^1(K, \mu_q(L'))$ which we also call w. From [Se, p. 152], $H^1(K, \mu_q(L')) \cong L^*/L^{*q}$ by a map we call k. The map k sends the cocycle class containing $(\sigma \mapsto {}^\sigma(\sqrt[q]{l})/\sqrt[q]{l})$ to $l \in L^*$.

Theorem 2.3. *The maps F and $k \circ w \circ \delta$ are the same as maps from $J(K)/\phi A(K)$ to L^*/L^{*q}.*

Proof. Let δ_q be the coboundary map from $J(K)/qJ(K)$ to $H^1(K, J[q])$. Let w_q be the map from $J[q]$ to $\mu_q(L')$ that sends $R \in J[q]$ to $e_q(R, \hat{P}_L)$. For clarity we redenote δ and w by δ_ϕ and w_ϕ. We first show that the map F is the same as the composition $k \circ w_q \circ \delta_q$ on the subgroup of $J(K)/qJ(K)$ of elements represented by divisor classes containing good divisors. Let P be a good divisor representing such an element of $J(K)/qJ(K)$. From Lemma 2.1, the choice of such a P is unimportant. From [La, Lemma 3, p. 166], we can pick a degree 0 divisor Q, whose support does not intersect the avoidance set, and for which qQ is linearly equivalent to P. The class of cocycles $\delta_q([P])$ includes the cocycle $(\sigma \mapsto [{}^\sigma Q - Q])$ with $\sigma \in \mathrm{Gal}(\overline{K}/K)$. So $w_q \circ \delta_q([P])$ is the class of cocycles that includes $(\sigma \mapsto e_q([{}^\sigma Q - Q], \hat{P}_L))$. Let $e_q^\lambda(S, T) = e_q(S, \lambda T)$ for $S, T \in J[q]$. The e_q^λ-Weil pairing can be defined as follows. If h_1 and h_2 are functions on C with divisors qE_1 and qE_2 respectively, with disjoint supports, then $e_q^\lambda([E_1], [E_2]) = h_2(E_1)/h_1(E_2)$. Let $(g) = qQ - P$ with g defined over $K(Q)$. We have $({}^\sigma g) = q\,{}^\sigma Q - P$ and so $({}^\sigma g/g) = q\,{}^\sigma Q - qQ$. Recall $(f_i) = qD_i$. We have

$$e_q^\lambda([{}^\sigma Q - Q], [D_i]) = \frac{f_i({}^\sigma Q - Q)}{{}^\sigma g/g(D_i)}.$$

Thus we have the following equalities of n-tuples

$$e_q([{}^\sigma Q - Q], \hat{P}_L) = \frac{F({}^\sigma Q - Q)}{{}^\sigma g / g(P_L)} = \frac{{}^\sigma \beta}{\beta}$$

where $\beta = F(Q)/g(P_L)$. So we have

$$k \circ w_q \circ \delta_q([P]) \equiv \beta^q \equiv \frac{F(qQ)}{g(qP_L)} \equiv \frac{F(qQ)}{F(qQ - P)} \equiv F(P) \bmod L^{*q}.$$

Let us show that F and $k \circ w_\phi \circ \delta_\phi$ are the same as maps from $J(K)/\phi A(K)$ to L^*/L^{*q}. It follows from Assumption I that every element of $J(K)/\phi A(K)$ is represented by a good divisor. There is an isogeny $\tau : J \to A$ with $\phi \circ \tau = q$. From the commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & J[q] & \to & J(\overline{K}) & \stackrel{q}{\to} & J(\overline{K}) & \to & 0 \\ & & \downarrow \tau & & \downarrow \tau & & \downarrow 1 & & \\ 0 & \to & A[\phi] & \to & A(\overline{K}) & \stackrel{\phi}{\to} & J(\overline{K}) & \to & 0 \end{array}$$

we get the following commutative diagram by taking $\mathrm{Gal}(\overline{K}/K)$-invariants.

$$\begin{array}{ccc} J(K)/qJ(K) & \stackrel{\delta_q}{\to} & H^1(K, J[q]) \\ \downarrow & & \downarrow \tau \\ J(K)/\phi A(K) & \stackrel{\delta_\phi}{\to} & H^1(K, A[\phi]) \end{array}$$

From the compatibility of Weil pairings we have $e_q(R, \hat{P}_L) = e_\phi(\tau(R), \hat{P}_L)$. Thus the triangle of the following diagram commutes and so the whole diagram commutes.

$$\begin{array}{ccccc} J(K)/qJ(K) & \stackrel{\delta_q}{\to} & H^1(K, J[q]) & \searrow w_q & \\ \downarrow & & \downarrow \tau & & H^1(K, \mu_q(L')) \stackrel{k}{\to} L^*/L^{*q} \\ J(K)/\phi A(K) & \stackrel{\delta_\phi}{\to} & H^1(K, A[\phi]) & \nearrow w_\phi & \end{array}$$

From commutivity, F must factor through $\phi A(K)$ and F and $k \circ w_\phi \circ \delta_\phi$ are the same as maps from $J(K)/\phi A(K)$ to L^*/L^{*q}. □

Inspiration for this proof can be found in [Li] and [Mc, Lemma 2.2].

Note that Lemma 2.1 and Theorem 2.3 hold if we replace K and L' by any field $\mathscr{K}$ (containing K) and $L' \otimes_K \mathscr{K}$. Let $\mathfrak{s} \in S$ and $L_\mathfrak{s} = L \otimes_K K_\mathfrak{s}$. The map F induces a map $F_\mathfrak{s}$ from $J(K_\mathfrak{s})/\phi A(K_\mathfrak{s})$ to $L_\mathfrak{s}^*/L_\mathfrak{s}^{*q}$. In order to compute the Selmer group, we want the maps F and $F_\mathfrak{s}$ to be injective. The maps δ, $\delta_\mathfrak{s}$, k and $k_\mathfrak{s}$ are injective automatically. Let us make an assumption that makes w and $w_\mathfrak{s}$ injective also.

Let $\mathscr{K}$ be any field containing K and $\overline{\mathscr{K}}$ be an algebraic closure. Let coker be defined to make the following an exact sequence of $\mathrm{Gal}(\overline{\mathscr{K}}/\mathscr{K})$-modules.

$$0 \to A[\phi] \stackrel{w}{\to} \mu_q(L') \to \mathrm{coker} \to 0$$

In addition, let $\mathscr{K}'$ denote the minimal field of definition, over $\mathscr{K}$, of the D_i's.

We have

$$H^1(\mathscr{K}, A[\phi]) \xrightarrow{w} H^1(\mathscr{K}, \mu_q(L')) \text{ is injective}$$

$$\Leftrightarrow \mu_q(L')(\mathscr{K}) \to \text{coker}(\mathscr{K}) \text{ is surjective}$$

$$\Leftrightarrow H^1(\text{Gal}(\mathscr{K}'/\mathscr{K}), A[\phi]) \xrightarrow{w} H^1(\text{Gal}(\mathscr{K}'/\mathscr{K}), \mu_q(L')) \text{ is injective.}$$

Assumption II: The maps $H^1(G, A[\phi]) \xrightarrow{w} H^1(G, \mu_p(L'))$ are injective for $G = \text{Gal}(K'/K)$ and $G = \text{Gal}(K'_{\mathfrak{s}}/K_{\mathfrak{s}})$ with $\mathfrak{s} \in S$.
This assumption guarantees that the maps F and $F_{\mathfrak{s}}$ are injections.

2.3 Computing the Selmer group

Step 4. Find a set S.

The set of primes of K denoted S must include the primes dividing the conductor of A, the primes over p, and if $p = 2$, the real primes. The primes dividing the conductor of A are the same as those dividing the conductor of J. These are a subset of the primes at which the reduction of C is singular. It is easier, in general, to determine the primes at which the reduction of C is singular (see [Ha, chap. 1, Sect. 5]), than the primes dividing the conductor of J. So, for simplicity, we can include in S all of the primes at which the reduction of C is singular.

Step 5. Determine the image of $H^1(K, A[\phi]; S)$ in L^*/L^{*q} and find generators of that image.

We have $L \cong \prod_{j \in \Lambda} L_j$ where the L_j are fields. Thus L^*/L^{*q} is isomorphic to $\prod_{j \in \Lambda} L_j^*/L_j^{*q}$.

Definition. *Let $L_j(S, q)$ be the subgroup of L_j^*/L_j^{*q} of elements with the property that if we adjoin the qth root of a representative to L_j, that we get an extension unramified outside of primes over primes of S. Let $L(S, q) = \prod_{j \in \Lambda} L_j(S, q)$.*

Since we are making Assumption II, we have

$$H^1(K, A[\phi]) \cong \ker : H^1(K, \mu_q(L')) \to H^1(K, \text{coker})$$

and

$$\begin{aligned} H^1(K, A[\phi]; S) &\cong \ker : H^1(K, \mu_q(L'); S) \to H^1(K, \text{coker}) \\ &\cong \ker : L(S, q) \to H^1(K, \text{coker}). \end{aligned}$$

By abuse of notation, we refer to the subgroup of $L(S, q)$ above as $H^1(K, A[\phi]; S)$. Let $\beta_{\mathfrak{s}}$ be the natural map from L^*/L^{*q} to $L_{\mathfrak{s}}^*/L_{\mathfrak{s}}^{*q}$. The image of $J(K)/\phi A(K)$ in $H^1(K, A[\phi])$ actually lies in $H^1(K, A[\phi]; S)$ and the following diagram commutes (see [Mi3, p. 92]).

$$\begin{array}{ccc} J(K)/\phi A(K) & \overset{F}{\hookrightarrow} & H^1(K, A[\phi]; S) \\ \downarrow & & \downarrow \prod \beta_{\mathfrak{s}} \\ \prod_{\mathfrak{s}\in S} J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}}) & \overset{\prod F_{\mathfrak{s}}}{\hookrightarrow} & \prod_{\mathfrak{s}\in S} L_{\mathfrak{s}}^*/L_{\mathfrak{s}}^{*q} \end{array}$$

From Theorem 2.3 and the injectivity of $k \circ w$ the Selmer group, $S^{\phi}(K, A)$, is isomorphic to the intersection of the groups $\beta_{\mathfrak{s}}^{-1}(F_{\mathfrak{s}}(J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})))$ for all $\mathfrak{s} \in S$.

Step 6. Find generators for $J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})$ and their images under $F_{\mathfrak{s}}$, in $L_{\mathfrak{s}}^*/L_{\mathfrak{s}}^{*q}$, for all $\mathfrak{s} \in S$.

For representatives, we find $K_{\mathfrak{s}}$-rational, degree 0 divisors. It may be necessary to shift their supports so that we have good divisors. To check if the classes of good divisors are independent in $J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})$, it is easiest to check if their images under the injective map $F_{\mathfrak{s}}$ are independent in $L_{\mathfrak{s}}^*/L_{\mathfrak{s}}^{*q}$. A deterministic algorithm for finding such generators for the Jacobians of curves of genus 2 and the multiplication by 2 map is given in [St1].

We need to know how many generators are needed. Let C have genus g and $\mathfrak{s}$ be a finite prime of K. Recall $q = p^l$.

Proposition 2.4. *If $\mathfrak{s}|p$, then $\#J(K_{\mathfrak{s}})/qJ(K_{\mathfrak{s}}) = q^{g[K_{\mathfrak{s}}:\mathbf{Q}_p]} \cdot \#J(K_{\mathfrak{s}})[q]$. If $\mathfrak{s} \not| p$, then $\#J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}}) = \#A(K_{\mathfrak{s}})[\phi]$.*

Both statements can be shown using the snake lemma and the fact that $J(K_{\mathfrak{s}})$ contains a subgroup of finite index isomorphic to g copies of the ring of integers in $K_{\mathfrak{s}}$ (see [Ma] and [Sc2, Lemma 3.8, Proposition 3.9]). Of course, $\#J(\overline{K_{\mathfrak{s}}})[q] = q^{2g}$. If ϕ is not a multiplication by q map, and $\mathfrak{s}$ lies over p, then the computation of $\#J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})$ is not always trivial. This is discussed in [Sc2, Sect. 3], where an algorithm is given, in the case that J is an elliptic curve. In certain other cases it can be accomplished, as in Corollary 3.6.

If $p = 2$, then S includes real primes.

Proposition 2.5. *If $q = 2^l$ and J is defined over $\mathbf{R}$, then $\#J(\mathbf{R})/qJ(\mathbf{R}) = q^{-g} \cdot \#J(\mathbf{R})[q]$.*

For the proof, simply replace 2 by $q = 2^l$ in [Sc2, Proposition 5.4] where one can find discussions of more general isogenies of even degree at real primes.

Step 7. Find the intersection in $H^1(K, A[\phi]; S)$ of $\beta_{\mathfrak{s}}^{-1}(F_{\mathfrak{s}}(J(K_{\mathfrak{s}})/\phi A(K_{\mathfrak{s}})))$ for all $\mathfrak{s} \in S$.

At this point we have accomplished our goal of computing the Selmer group. One reason that Selmer groups are computed is for the purpose of bounding the Mordell-Weil rank. The group $J(K)$ is called the Mordell-Weil group of J over K. It is a finitely generated abelian group and its free $\mathbf{Z}$-rank is called the Mordell-Weil rank of J over K. In order to find the Mordell-Weil rank, we need to find elements of $J(K)/\phi A(K)$ and map them to L^*/L^{*q}. One can save time by doing this before Step 6 since elements of $J(K)/\phi A(K)$ map to

elements in each $J(K_\mathfrak{s})/\phi A(K_\mathfrak{s})$. Let $Ш(K,A)[\phi]$ denote the ϕ-torsion of the Tate-Shafarevich group for A over K. We hope to generate all of the kernel from $S^\phi(K,A)$ to $Ш(K,A)[\phi]$ (assuming you know what $Ш(K,A)[\phi]$ is!) This kernel is isomorphic to $J(K)/\phi A(K)$. If we have success, then we can attempt to compute the Mordell-Weil rank of $J(K)$.

Let ϕ' be an isogeny from J to A for which $\phi \circ \phi' = \tau$ and $\tau^t = mu$ for some unit u in End(J), and integers t and $m = q^j$. In addition, assume that we are able to compute $A(K)/\phi' J(K)$ (at this point it would be helpful if A were a Jacobian). The following proposition contains an exact sequence which helps combine the sizes of these groups to find the size of $J(K)/mJ(K)$.

Proposition 2.6. *Let B and D be abelian groups and let $f : B \to D$ and $g : D \to B$ be homomorphisms. The following is an exact sequence*

$$0 \to B[f]/g(D[fg]) \to B/gD \xrightarrow{f} D/fgD \to D/fB \to 0.$$

Proof. The proposition follows from the diagram below, which commutes from the snake lemma applied to the middle two exact sequences.

$$\begin{array}{ccccccccc}
0 & \to & g(D[fg]) & \to & B[f] & \to & B[f]/g(D[fg]) & \to & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & gD & \to & B & \to & B/gD & \to & 0 \\
 & & \downarrow f & & \downarrow f & & \downarrow f & & \\
0 & \to & fgD & \to & D & \to & D/fgD & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \to & 0 & \to & D/fB & \to & D/fB & \to & 0
\end{array}$$

□

If f and g are isogenies of abelian varieties, then the group $B[f]/g(D[fg])$ will be a quotient of torsion groups, hence computeable. Replacing f and g by ϕ and ϕ', from $J(K)/\phi A(K)$ and $A(K)/\phi' J(K)$ we can compute $J(K)/\tau J(K)$ using the exact sequence. By replacing f and g by τ^i, $1 \le i \le t-1$, and τ, we can compute the size of $J(K)/mJ(K)$. If r is the Mordell-Weil rank of J over K, then $J(K)/mJ(K) \cong (\mathbf{Z}/m\mathbf{Z})^r \oplus J(K)[m]$.

On the other hand, ϕ-Selmer groups have many interesting uses beyond computing $J(K)/mJ(K)$. For example, in [We], Wetherell provides a method of bounding the number of rational points on a curve C when the Mordell-Weil rank is at least as large as the genus. This is the case that effective Chabauty (see [Co]) does not help with. In order to do this, he considers a set of covers of the curve parametrized by elements of a ϕ-Selmer group, where ϕ is any isogeny from an abelian variety to the Jacobian of C.

2.4 Assumptions

Let us consider the two assumptions that we made.

Let $d = \gcd\{[K^\dagger : K] \mid K \subseteq K^\dagger \subset \overline{\mathbf{Q}},\ C(K^\dagger) \neq \emptyset\}$. Recall that the exponent of $A[\phi]$ is $q = p^l$.

Proposition 2.7. *If $p \not| d$, then Assumption I is satisfied.*

Proof. Let $K^\dagger$ be a field of degree $d^\dagger$ over K with $C(K^\dagger) \neq \emptyset$. From [Mi1, p. 168], every element of $J(K^\dagger)$ is represented by a degree 0 divisor of C defined over $K^\dagger$. Let N denote any map induced by the norm map from $K^\dagger$ to K. The following is a commutative diagram.

$$\begin{array}{ccccc} \mathrm{Div}^0(C)(K^\dagger) & \to & J(K^\dagger) & \to & 0 \\ \downarrow N & & \downarrow N & & \downarrow N \\ \mathrm{Div}^0(C)(K) & \to & J(K) & \to & \mathrm{coker} \end{array}$$

The composition of the natural inclusion of $\mathrm{Div}^0(C)(K)$ in $\mathrm{Div}^0(C)(K^\dagger)$ with the norm map to $\mathrm{Div}^0(C)(K)$ is the multiplication by $d^\dagger$ map. So $d^\dagger$ kills the cokernel. The cokernel is thus killed by d, the greatest common divisor of the $d^\dagger$'s. Since q is relatively prime to d, we know that every element of $J(K)/\phi A(K)$ is represented by a divisor class that contains a divisor of C defined over K.

Fix a prime $\mathfrak{s} \in S$. Since $p \not| d$, there is a completion of $K^\dagger$ at a prime over $\mathfrak{s}$ whose degree over $K_\mathfrak{s}$ is prime to p. The same argument as above shows that every element of $J(K_\mathfrak{s})/\phi A(K_\mathfrak{s})$ is represented by a divisor class that contains a divisor of C defined over $K_\mathfrak{s}$. □

Now let us consider Assumption II. If the induced map w on cohomology groups is an injection for some given spanning set then we have an injection for any spanning set containing the given one. To test whether there exists a spanning set satisfying Assumption II, it suffices to use the entire set Ψ. For any given spanning set, the following provides a simplification. Let K' be the minimal field of definition of the $D_i's$. Let $L'_j = \prod \overline{K}_{i_j}$ where i_j ranges over all those l such that D_l is in the same $\mathrm{Gal}(K'/K)$-orbit as D_j. We let L'_j inherit its $\mathrm{Gal}(K'/K)$-module structure from L'. We have $L' \cong \prod_{j\in\Lambda} L'_j$. The group $H^1(\mathrm{Gal}(K'/K), \mu_q(L'))$ is isomorphic to $\oplus_{j\in\Lambda} H^1(\mathrm{Gal}(K'/K), \mu_q(L'_j))$. Let Stab_j be the stabilizer in $\mathrm{Gal}(K'/K)$ of D_j. The latter sum is isomorphic to $\oplus_{j\in\Lambda} H^1(\mathrm{Stab}_j, \mu_q)$ from Shapiro's lemma (see [AW, p. 99]). We can make an analogous statement by replacing K with $K_\mathfrak{s}$.

2.5 Extension of the algorithm

Let f be a polynomial of degree 2d over the number field K with distinct roots in $\overline{K}$. Let C be the normalization of the curve given by the affine equation $y^2 = f(x)$ and let J be its Jacobian. Let $\{\alpha_i\}$ be the set of roots of f. Then the divisor classes in $P_L = ([(\alpha_1, 0) - (\alpha_1, 0)], [(\alpha_2, 0) - (\alpha_1, 0)], \ldots, [(\alpha_{2d}, 0) - (\alpha_1, 0)])$ span $J[2]$. We can let $L = K[T]/(f(T))$, and $L' = \overline{K}[T]/(f(T))$ where $\mathrm{Gal}(\overline{K}/K)$ acts trivially on T. Note $\overline{K}[T]/(f(T)) \cong \prod \overline{K}[T]/(T - \alpha_i) \cong \prod \overline{K_i}$ by $T \mapsto (T, \ldots, T) \mapsto (\alpha_1, \ldots, \alpha_{2d})$. The map w', given by $P \mapsto e_2(P, \hat{P}_L)$, sends $J[2]$ to $\mu_2(L')$. However this map may not be defined over K. The group G generated by the set $\{(\sigma - 1)(w'(P)) \mid P \in J[2], \sigma \in \mathrm{Gal}(\overline{K}/K)\}$ is contained in $\pm 1 \subset \mu_2(L')$.

Thus the induced map from $J[2]$ to $\mu_2(L')/\pm 1$ is defined over K; it is also injective. The map this induces on cohomology may not be injective, but the kernel is sufficiently under control so that Mordell-Weil ranks can nevertheless sometimes be computed. In this case, the map F is $x - T$ and its image is in $L^*/L^{*2}K^*$. This case is far more complicated than those that fit into the framework given earlier. It is discussed in [Ca], [FPS], [PS] and [St1].

We can try to use this technique in general. We can pick some spanning set and quotient out by a group like G. But then we can not typically expect the induced map on cohomology to be close enough to injective to be useful.

3 Curves of the form $y^p = f(x)$

Let K be a field of characteristic 0. Let $f(x)$ be a monic polynomial over K of degree d with distinct roots in $\overline{K}$. Let C be the normalization of the projective curve defined by the affine equation $y^p = f(x)$, where p is a prime that does not divide d. (The case where p does divide d is described in [PS]). From [Tw, Sect. 1], the genus of C is $g = (p-1)(d-1)/2$. Since $p \neq d$ there is a single point on the line at infinity. If $d \neq p \pm 1$, then the projective curve will be singular at ∞. Also from [Tw, Sect. 1], since $p \not| d$, the normalization has a single rational point over the point on the line at infinity which we denote ∞. Since we chose f to have distinct roots, the projective curve given by $y^p = f(x)$ can be singular nowhere else.

Consider the map τ on C, that on the affine part sends $(x, y) \mapsto (x, \zeta_p y)$. The map τ induces an automorphism of J. The group J is generated by divisor classes of the form $[P - \infty]$ where P is an affine point on C. The divisor of the function $x - x(P)$ is $\tau^{p-1}P + \ldots + \tau P + P - p\infty$. Consider the subring $\mathbf{Z}[\tau]$ in End(J). The minimal polynomial of τ over $\mathbf{Z}$ is $t^{p-1} + \ldots + t + 1$. Thus τ acts as a primitive pth root of unity in End(J); so by abuse of notation we rename it ζ_p. Let $\phi = 1 - \zeta_p$ in End(J).

For $1 \leq i \leq p-1$, the quotient of the numbers $(1 - \zeta_p^i)$ and $(1 - \zeta_p)$ is a unit. Thus the subgroup $J[\phi]$ of J is fixed by Gal$(\overline{K}/K)$. The abelian variety $J/J[\phi]$, however, will typically not be a Jacobian over K unless K contains ζ_p. Thus it will be difficult to compute the Mordell-Weil rank of $J(K)$ directly for the reasons presented at the end of Sect. 2.3. For that reason, we assume that K contains ζ_p so ϕ is a K-defined endomorphism.

Here is one case where the quotient is a Jacobian. Let C be $y^3 = x^2 - k$ and C' be $y^3 = x^2 + 27k$ with $k \in K^*$ (and K not necessarily containing ζ_p) and let E and E' be their Jacobians (elliptic curves). Let $\phi = 1 - \zeta_3$ on E and $\phi' = 1 - \zeta_3$ on E'. Then there are isogenies $\tau : E \to E/E[\phi] \cong E'$ and $\tau' : E' \to E'/E'[\phi'] \cong E$ defined over K with $\tau' \circ \tau = 3$. In [Tp], Top describes the computation of the τ- and τ'-Selmer groups along the lines of Sect. 2.

Let us show that $\Psi = \lambda^{-1}\hat{J}[\hat{\phi}] = J[\phi]$.

Proposition 3.1. *Let λ be the canonical principal polarization from J to $\hat{J}$ with respect to C. We have $\lambda^{-1}\hat{J}[\hat{\phi}] = J[\phi]$.*

Proof. Let $(1-\zeta_p)^\dagger$ denote the image in End(J) of $1-\zeta_p$ under the Rosati involution. By definition, the following diagram commutes.

$$\begin{array}{ccc} J & \stackrel{\lambda}{\to} & \hat{J} \\ (1-\zeta_p)^\dagger \uparrow & & \uparrow \widehat{1-\zeta_p} \\ J & \stackrel{\lambda}{\to} & \hat{J} \end{array}$$

From [Mi2, p. 139], we have $\zeta_p^\dagger = \zeta_p^{-1}$. Thus we have

$$\Psi = \lambda^{-1}\hat{J}[\widehat{1-\zeta_p}] = J[(1-\zeta_p)^\dagger] = J[1-\zeta_p^\dagger] = J[1-\zeta_p^{-1}] = J[1-\zeta_p] = J[\phi]$$

since the quotient of $1-\zeta_p^{-1}$ and $1-\zeta_p$ is a unit. □

We know $(\phi)^{p-1} = u \cdot p$ where u is a unit in End(J).

Definition. *Let* $\dim M$ *denote the dimension of an* $\mathbf{F}_p$*-vector space* M.

We also know $\dim J[p] = 2g = (p-1)(d-1)$, so $\dim J[\phi] = d-1$. We need to choose a Galois-invariant spanning set of $J[\phi]$. Let $\{\alpha_i\}$ be the set of roots of f.

Proposition 3.2. *The divisor classes* $[(\alpha_1, 0) - \infty], \ldots, [(\alpha_{d-1}, 0) - \infty]$ *form a basis for* $J[\phi]$.

Proof. The following proof was suggested by Michael Stoll. Let $\overline{K}(C)$ be the function field of C over $\overline{K}$ and let Princ denote the principal divisors. The following sequences are both exact.

$$0 \to \overline{K}^* \to \overline{K}(C)^* \stackrel{\text{div}}{\to} \text{Princ} \to 0$$

$$0 \to \text{Princ} \to \text{Div}^0(C) \to J \to 0$$

Let τ, as before, be the automorphism of C given on the affine part by $\tau(x,y) = (x, \zeta_p y)$. By extending τ from points to divisors, the map τ induces maps on Princ, $\text{Div}^0(C)$ and J. We can let τ act on $\overline{K}(C)$ by fixing $\overline{K}(x)$ and sending y to $\zeta_p^{-1}y$. Let $G = \langle\tau\rangle$. Under these actions, both are exact sequences of $\mathbf{Z}[G]$-modules.

Under G-cohomology we have the following exact sequence.

$$0 = H^1(G, \overline{K}(C)^*) \to H^1(G, \text{Princ}) \to H^2(G, \overline{K}^*) = \overline{K}^*/\overline{K}^{*p} = 1$$

To get the first equality, we can identify G with $\text{Gal}(\overline{K}(C)/\overline{K}(x))$ and use Hilbert's theorem 90. The next-to-last equality comes from the fact that G is a finite cyclic group and so $H^2(G, \overline{K}^*) \cong \ker(1-\tau)/\text{image(Norm)}$, where Norm $= 1 + \ldots + \tau^{p-1}$. Therefore $H^1(G, \text{Princ}) = 0$ and hence the map from $\text{Div}^0(C)^G$ to $J^G = J[\phi]$ is surjective. So $J[\phi]$ is generated by G-invariant divisors. The group $\text{Div}^0(C)^G$ is generated by divisors of the form $P - \infty$ where $P \in C^G$ and by those of the form $\text{Norm}(P-\infty)$ for arbitrary $P \in C \setminus \infty$. Each such $\text{Norm}(P-\infty) = \text{div}(x - x(P))$ and so is principal. Thus $J[\phi]$ is generated

by divisors of the form $P - \infty$ where $P \in C^G$ but the only points fixed by G are those with y-coordinate 0 and ∞.

We have already seen that $\dim J[\phi] = d - 1$ and that the sum of all d divisor classes $[(\alpha_i, 0) - \infty]$ is 0, so the result follows. □

Therefore $P_L = ((\alpha_1, 0) - \infty, \ldots, (\alpha_d, 0) - \infty)$ is a Galois-invariant set whose divisor classes span $J[\phi]$. Thus we can set $L = K[T]/(f(T))$ and

$$\begin{aligned} L' = \overline{K}[T]/(f(T)) &\cong \prod_{i=1}^{d} \overline{K}[T]/(T - \alpha_i) \\ &\cong \prod_{i=1}^{d} \overline{K}_i \text{ by } T \mapsto (T, \ldots, T) \mapsto (\alpha_1, \ldots, \alpha_d) \end{aligned}$$

where $\mathrm{Gal}(\overline{K}/K)$ acts trivially on T. Therefore we can let $F = x - T$ where if $R = \sum n_i R_i$ is a good divisor, then

$$(x - T)(R) = \prod (x(R_i) - T)^{n_i} \in L^*.$$

When composed with the isomorphism of L' and $\prod \overline{K}_i$, the map $x - T$ becomes the d-tuple of functions $(x - \alpha_1, \ldots, x - \alpha_d)$, whose divisors are pP_L.

It is often convenient to work with divisors of the form $D - r\infty$ where D is a K-rational, effective divisor of degree r. Let us consider the image of the divisor class containing such a divisor under the map $x - T$. The following proposition holds even when K does not contain ζ_p.

Proposition 3.3. *Any element of $J(K)$ can be represented by a divisor of degree 0 which is defined over K and whose support does not include ∞ or points with y-coordinate 0. In particular, let $D = {}^{\sigma_1}Q + \ldots + {}^{\sigma_r}Q - r\infty$ where the ${}^{\sigma_i}Q$ are the r conjugates over K of the point Q of C and $y(Q) \neq 0$. We have*

$$(x - T)([D]) \equiv \prod_{i=1}^{r} (x({}^{\sigma_i}Q) - T) (\mathrm{mod}\, L^{*p}).$$

Let $D = (\alpha_1, 0) + \ldots + (\alpha_r, 0) - r\infty$ where the α_i are conjugate over K, possibly renumbered, and $r < d$. We have

$$(x - T)([D]) \equiv \prod_{i=r+1}^{d} (\alpha_i - T)^{-1} + \prod_{i=1}^{r} (\alpha_i - T) \pmod{L^{*p}}.$$

Proof. Assume p is odd. Since C has a K-rational point, namely ∞, the first sentence follows from Proposition 2.7. Let $Q = (x_0, y_0)$ be a point of C defined over a finite extension of K and fix a set $\{\sigma_i\}$ of embeddings of $K(Q)$ in $\overline{K}$, such that ${}^{\sigma_1}Q, \ldots, {}^{\sigma_r}Q$ are the conjugates of Q over K. Let

$$D = (\sum_{i=1}^{r} {}^{\sigma_i}Q) - r\infty.$$

Any degree 0 divisor defined over K can be written as the sum and difference of such divisors (possibly with different sets of $\{\sigma_i\}$).

First we assume that $y_0 \neq 0$. Let $a, b \in K^*$ with $f(a) \neq 0$. Let (a, c), $(a, \zeta_p c)$, $\ldots, (a, \zeta_p^{p-1} c)$ be the p affine points on the line $x = a$ and let $(g_1, b), \ldots, (g_d, b)$ be the d affine points on the line $y = b$; the latter d points are not necessarily distinct. Since p does not divide d we can find integers n and m such that $nd + m(d-p) = 1$. The divisor of the function $(x-a)^{mr}(y-b)^{-nr-mr}$ is

$$r\infty + rm(a,c) + \ldots + rm(a,\zeta_p^{p-1}c) - r(n+m)(g_1,b) - \ldots - r(n+m)(g_d,b).$$

When we add D to this principal divisor we get a divisor without ∞ or points with y-coordinate 0 in its support. Therefore we have

$$\begin{aligned}(x-T)([D]) &= \frac{(a-T)^{prm}(x(^{\sigma_1}Q)-T)\cdot\ldots\cdot(x(^{\sigma_r}Q)-T)}{((g_1-T)\cdot\ldots\cdot(g_d-T))^{r(n+m)}} \\ &= \frac{(a-T)^{prm}(x(^{\sigma_1}Q)-T)\cdot\ldots\cdot(x(^{\sigma_r}Q)-T)}{((-1)^d(f(T)-b^p))^{r(n+m)}} \\ &\equiv (x(^{\sigma_1}Q)-T)\cdot\ldots\cdot(x(^{\sigma_r}Q)-T)(\mathrm{mod}\, L^{*p}).\end{aligned}$$

Let $D = (\alpha_1, 0) + \ldots + (\alpha_r, 0) - r\infty$ where the α_i are conjugate over K and $r < d$. We can let $r < d$ since $\sum(\alpha_i, 0) - d\infty$ is principal. Let $g = y - \prod_{i=1}^{r}(x-\alpha_i)$. We have

$$(g) = (\alpha_1, 0) + \ldots + (\alpha_r, 0) + \sum_{j=1}^{m'} P_j - (m'+r)\infty$$

where $m' = \max\{d-r, r(p-1)\}$ and $P_j = (x_j, y_j)$ with $y_j \neq 0$ and the x_j's are the roots of the polynomial

$$\prod_{i=r+1}^{d}(x-\alpha_i) - \prod_{i=1}^{r}(x-\alpha_i)^{p-1}.$$

We have

$$D - (g) = m'\infty - \sum_{i=1}^{m'} P_i$$

which is the negative of a divisor of the form we handled in the first part of the theorem. Therefore we have

$$(x-T)([D]) \equiv (\prod_{i=1}^{m'}(x_i - T))^{-1} \equiv (\prod_{i=1}^{m'}(T-x_i))^{-1}$$

$$\equiv (\prod_{i=r+1}^{d}(T-\alpha_i) - \prod_{i=1}^{r}(T-\alpha_i)^{p-1})^{-1}(\mathrm{mod}\, L^{*p}).$$

Let us consider L to be a product of number fields or to be contained in $\prod \overline{K_i}$. In either case, one of the two products in the above formula will be 0 at each factor. Thus we have

$$(x-T)([D]) \equiv \prod_{i=r+1}^{d}(\alpha_i - T)^{-1} + \prod_{i=1}^{r}(\alpha_i - T) \pmod{L^{*p}}.$$

For the $p = 2$ case, see [Sc1, Lemma 2.2]. □

The upshot of the first formula in the above lemma is that you can basically ignore the appearance of ∞ in such a divisor.

The following proposition shows that the map w induces on cohomology is injective and describes $H^1(K, J[\phi]; S)$.

Proposition 3.4. *Let K be a number field containing ζ_p. The groups $H^1(K, J[\phi]; S)$ and* $\ker : L(S,p) \overset{\text{norm}}{\to} K^*/K^{*p}$ *are isomorphic via $k \circ w$.*

Proof. First we show that the following is a split exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to J[\phi] \overset{w}{\to} \mu_p(L') \overset{N}{\to} \mu_p(\overline{K}) \to 0$$

where N is the norm map. The dimensions of the three $\mathbf{F}_p$-vector spaces are $d-1$, d and 1 respectively. The divisor of the function y is $(\alpha_1, 0) + \ldots + (\alpha_d, 0) - d\infty$. So the sum of the d divisor classes $[(\alpha_i, 0) - \infty]$ is trivial. Then since $\zeta_p \in K$, the Weil pairing is linear and the image of w is therefore equal to the kernel of the norm. Let Δ be the diagonal embedding of $\mu_p(\overline{K})$ in $\mu_p(L')$. Let b be a positive residue of $d^{-1} (\mathrm{mod}\ p)$. Then the composition of Δ^b and the norm is the identity, so the exact sequence splits.

Since this short exact sequence splits, the following is a split exact sequence

$$0 \to H^1(K, J[\phi]) \overset{w}{\to} H^1(K, \mu_p(L')) \overset{N}{\to} H^1(K, \mu_p(\overline{K})) \to 0.$$

The group $H^1(K, \mu_p(L'))$ is isomorphic to L^*/L^{*p} by the map we call k. The group $H^1(K, \mu_p(\overline{K}))$ is isomorphic to K^*/K^{*p} by a Kummer map also. So $k \circ w$ induces an isomorphism of $H^1(K, J[\phi])$ with the kernel of the norm from L^*/L^{*p} to K^*/K^{*p} and of $H^1(K, J[\phi]; S)$ with the kernel of the norm from $L(S,p)$ to K^*/K^{*p}. □

The following proposition has two corollaries for a number field K. The first gives the size of $J(K_\mathfrak{s})/\phi J(K_\mathfrak{s})$ for $\mathfrak{s}$ a finite prime. The second shows how to find the Mordell-Weil rank of $J(K)$ from $J(K)/\phi J(K)$ and knowledge of torsion.

Proposition 3.5. *Let $\mathscr{K}$ be a number field or the completion of a number field at a finite prime, that contains ζ_p. Then* $\dim J(\mathscr{K})/pJ(\mathscr{K}) - \dim J(\mathscr{K})[p]$ *is the same as* $(p-1)(\dim J(\mathscr{K})/\phi J(\mathscr{K}) - \dim J(\mathscr{K})[\phi])$.

Proof. For each $n \geq 1$, the following is an exact sequence from Proposition 2.6 where $B = D = J(\mathscr{K})$ and $g = \phi$ and $f = \phi^n$.

$$0 \to \frac{J(\mathscr{K})[\phi^n]}{\phi(J(\mathscr{K})[\phi^{n+1}])} \to \frac{J(\mathscr{K})}{\phi J(\mathscr{K})} \overset{\phi^n}{\to} \frac{J(\mathscr{K})}{\phi^{n+1}J(\mathscr{K})} \to \frac{J(\mathscr{K})}{\phi^n J(\mathscr{K})} \to 0$$

Therefore

$$\dim J(\mathscr{K})/pJ(\mathscr{K}) = \dim J(\mathscr{K})/\phi^{p-1}J(\mathscr{K})$$

$$= (p-1)\dim J(\mathscr{K})/\phi J(\mathscr{K}) - \sum_{i=1}^{p-2} \dim J(\mathscr{K})[\phi^i] + \sum_{i=1}^{p-2} \dim \phi(J(\mathscr{K})[\phi^{i+1}]).$$

Thus

$$\dim J(\mathscr{K})/pJ(\mathscr{K}) - \dim J(\mathscr{K})[p] = (p-1)\dim J(\mathscr{K})/\phi J(\mathscr{K}) - \sum_{i=1}^{p-1} \dim J(\mathscr{K})[\phi^i] + \sum_{j=1}^{p-1} \dim \phi(J(\mathscr{K})[\phi^j]).$$

For each $j \geq 1$, the following is an exact sequence.

$$0 \to J(\mathscr{K})[\phi] \to J(\mathscr{K})[\phi^j] \xrightarrow{\phi} \phi J(\mathscr{K})[\phi^j] \to 0$$

Thus

$$\begin{aligned} \dim J(\mathscr{K})/pJ(\mathscr{K}) - \dim J(\mathscr{K})[p] &= (p-1)\dim J(\mathscr{K})/\phi J(\mathscr{K}) \\ &\quad -(p-1)\dim J(\mathscr{K})[\phi]. \end{aligned}$$

□

Corollary 3.6. *Let $K_\mathfrak{s}$ be a finite extension of $\mathbf{Q}_s$ containing ζ_p and let $r = \mathrm{ord}_p(s)$. In addition let g be the genus of C. Then* $\dim J(K_\mathfrak{s})/\phi J(K_\mathfrak{s}) = gr[K_\mathfrak{s} : \mathbf{Q}_s(\zeta_p)] + \dim J(K_\mathfrak{s})[\phi]$.

Proof. If $s \neq p$, then $r = 0$ and this follows from Proposition 2.4. Let $\mathfrak{s}$ lie over p; so $r = 1$. From Proposition 2.4, we have

$$\dim J(K_\mathfrak{s})/pJ(K_\mathfrak{s}) = g[K_\mathfrak{s} : \mathbf{Q}_p] + \dim J(K_\mathfrak{s})[p].$$

Using Proposition 3.5 we have

$$g[K_\mathfrak{s} : \mathbf{Q}_p] = (p-1)(\dim J(K_\mathfrak{s})/\phi J(K_\mathfrak{s}) - \dim J(K_\mathfrak{s})[\phi])$$

$$g[K_\mathfrak{s} : \mathbf{Q}_p(\zeta_p)] = \dim J(K_\mathfrak{s})/\phi J(K_\mathfrak{s}) - \dim J(K_\mathfrak{s})[\phi].$$

□

Corollary 3.7. *Let K be a number field containing ζ_p. The Mordell-Weil rank of $J(K)$ is* $(p-1)(\dim J(K)/\phi J(K) - \dim J(K)[\phi])$.

This follows immediately from Proposition 3.5.

We conclude with a proposition suggested independently by Armand Brumer, Michael Stoll and the referee. The proof appears after [PS, Lemma 13.4].

Proposition 3.8. *Let C be defined over K, a number field not necessarily containing ζ_p. The Mordell-Weil rank of $J(K)$ is the quotient of the Mordell-Weil rank of $J(K(\zeta_p))$ by $[K(\zeta_p) : K]$.*

3.1 Example where not all elements of Ψ are rational

Proposition 3.9. *Let C be the projective curve given by the affine equation $y^3 = (x^2+1)(x^2-4x+1)$ and let J be its Jacobian. The group $J(\mathbf{Q})$ has Mordell-Weil rank 1 and the group $J(\mathbf{Q}(\zeta_3))$ has Mordell-Weil rank 2.*

Proof. Let $K = \mathbf{Q}(\zeta_3)$ and $f(x) = (x^2+1)(x^2-4x+1)$. Let $\phi = 1-\zeta_3$. We first compute $J(K)/\phi J(K)$. The roots of f are $\pm i$ and $2\pm\sqrt{3}$. We have $L = K[T]/(f(T)) \cong K(i)\times K(i)$ by $T \mapsto (i, 2+\sqrt{3})$ and L^*/L^{*3} is isomorphic to $(K(i)^*/K(i)^{*3})^2$. In $K(i) = \mathbf{Q}(\zeta_{12})$, we fix $\zeta_3 = (-1+\sqrt{-3})/2$ and $\sqrt{3} = i\sqrt{-3}$. The bad primes of C over $\mathbf{Q}$ are 2 and 3. There is one prime of $K(i)$ over 2 generated by $(1+i)$; it is inert in K and ramifies in $K(i)$. There is one prime $\mathfrak{q}$ of $K(i)$ over 3; it ramifies in K and then is inert up to $K(i)$. We will denote the restriction of these primes to K by 2 and $\mathfrak{q}$. Since $K(i)$ is a totally imaginary extension of the rationals, it has unit rank 1. We note that $i-\zeta_3$ is a fundamental unit. The class group of the field $K(i)$ is trivial. Thus $K(i)(S,3)$ is $\langle i-\zeta_3, \zeta_3, 1+i, \sqrt{-3}\rangle$.

From Proposition 3.4, the group $H^1(K, J[\phi]; S)$ is the kernel of the norm from $L(S,3) \cong K(i)(S,3)^2$ to K^*/K^{*3}. The number $\zeta_3(i-\zeta_3)$ generates the kernel of the norm from $K(i)(S,3)$ to K^*/K^{*3}. Thus $H^1(K, J[\phi]; S) = \langle (i-\zeta_3, (i-\zeta_3)^2), (\zeta_3, \zeta_3^2), (1+i, (1+i)^2), (\sqrt{-3}, \sqrt{-3}^2), (1, \zeta_3(i-\zeta_3))\rangle$. The group $S^{\phi}(K, J)$ is the intersection of the groups $\beta_{\mathfrak{s}}^{-1}(F_{\mathfrak{s}}(J(K_{\mathfrak{s}})/\phi J(K_{\mathfrak{s}})))$ for the primes $\mathfrak{s} = 2$ and $\mathfrak{q}$ of K.

At this point let us find the images of the known elements of $J(K)$ by the map $x-T$. The group $J(K)[\phi]$ has order 3 and is generated by the divisor class $[(i,0)+(-i,0)-2\infty]$. In $J(K)$ there is also the divisor class $[(0,1)-\infty]$. In the following table we present the images of these two classes in $H^1(K, J[\phi]; S)$ by the map $x-T$. Above each coordinate is written $x-\alpha$ to remind us how to compute that coordinate. We use Proposition 3.3 to compute the images of $[(0,1)-\infty]$ and $[(i,0)+(-i,0)-2\infty]$.

$$\begin{array}{rcccc} & & x-i & & x-(2+\sqrt{3}) \\ [(i,0)+(-i,0)-2\infty] & \mapsto & (1+i)^2 & & \zeta_3^2(i-\zeta_3)^2(1+i) \\ [(0,1)-\infty] & \mapsto & 1 & & \zeta_3^2(i-\zeta_3)^2 \end{array}$$

From the first exact sequence in the proof of Proposition 3.5, we know $J(K)[\phi]/\phi(J(K)[3])$ injects into $J(K)/\phi J(K)$ which injects into L^*/L^{*3}. Thus we know that $J(K)[3] = J(K)[\phi]$ and is generated by $[(i,0)+(-i,0)-2\infty]$ since its image is not trivial. In addition we see that the image of $[(0,1)-\infty]$ is independent of the image of torsion and so the divisor class has infinite order. We will show that $S^{\phi}(K, J)$ is generated by the images of $[(i,0)+(-i,0)-2\infty]$ and $[(0,1)-\infty]$.

Let us describe the groups $J(K_{\mathfrak{q}})/\phi J(K_{\mathfrak{q}})$ and $L_{\mathfrak{q}}^*/L_{\mathfrak{q}}^{*3} \cong (K_{\mathfrak{q}}(i)^*/K_{\mathfrak{q}}(i)^{*3})^2$. The group $K_{\mathfrak{q}}(i)^*/K_{\mathfrak{q}}(i)^{*3}$ is $\langle\sqrt{-3}, 1+\sqrt{-3}, 1+i\sqrt{-3}, 1+\sqrt{-3}^2, 1+i\sqrt{-3}^2, 1+\sqrt{-3}^3\rangle$. Let us rename those numbers $\langle A, B, E, \Gamma, \Phi, \Delta\rangle$, to agree with the notation in [KS]. Multiplicatively, anything that is 1 modulo

9 is a cube, as are $1 \pm i\sqrt{-3}^3$ and -1. We have $[i - \zeta_3, \zeta_3, 1 + i, \sqrt{-3}] \equiv [BE, B^2\Gamma, \Gamma^2, A] \bmod K_\mathfrak{q}(i)^{*3}$. Thus the kernel of $\beta_\mathfrak{q}$ is trivial. From Corollary 3.6 we know $\dim J(K_\mathfrak{q})/\phi J(K_\mathfrak{q})$ is the sum of $3[K_\mathfrak{q} : \mathbf{Q}_3(\zeta_3)]$, which is 3, and $\dim J(K_\mathfrak{q})[\phi]$, which is 1 since $K_\mathfrak{q} \cap K(J[\phi]) = K$, for a total of 4. In the following table we list generators of $J(K_\mathfrak{q})/\phi J(K_\mathfrak{q})$ and their images in $L_\mathfrak{q}^*/L_\mathfrak{q}^{*3} \cong (K_\mathfrak{q}(i)^*/K_\mathfrak{q}(i)^{*3})^2$.

		$x - i$	$x - (2 + \sqrt{3})$
$[(i, 0) + (-i, 0) - 2\infty]$	$\mapsto$	Γ	ΓE^2
$[(0, 1) - \infty]$	$\mapsto$	1	$\Gamma^2 E^2$
$[(4, y_1) - \infty]$	$\mapsto$	Φ	ΓE
$[(\frac{1+\sqrt{-3}^3}{\sqrt{-3}^3}, y_2) - \infty]$	$\mapsto$	Δ	Δ^2

A small amount of linear algebra shows that $\beta_\mathfrak{q}^{-1}(F_\mathfrak{q}(J(K_\mathfrak{q})/\phi J(K_\mathfrak{q})))$ is the same as the group generated by the images of $[(i, 0) + (-i, 0) - 2\infty]$ and $[(0, 1) - \infty]$. So that is the Selmer group and those two divisor classes generate $J(K)/\phi J(K)$. We do not even need $J(K_2)/\phi J(K_2)$. Thus, from Corollary 3.7, the Mordell-Weil rank of $J(K)$ is 2. One can verify that the divisor classes $[(0, 1) - \infty]$ and $[(0, \zeta_3) - \infty]$ have infinite order and are independent. From Proposition 3.8, the Mordell-Weil rank of $J(\mathbf{Q})$ is 1. □

Using a straightforward computation in the number field gotten by adjoining to $\mathbf{Q}$ the root of the characteristic polynomial of Frobenius of J over $\mathbf{F}_7$, Michael Stoll has shown that J is absolutely simple. This type of argument appears in the proof of [PS, Proposition 14.4].

3.2 Examples with Mordell-Weil rank 0

In this section we find solutions of two diophantine equations over infinitely many number fields. First let us state two propositions. Each follows from the Riemann-Roch theorem and results in [Mi1, Sect. 5] and is well-known.

Proposition 3.10. *Let $f(x)$ be a polynomial of degree 5 or 6, defined over a field K of characteristic other than 2 with distinct roots in $\overline{K}$. Let C be the normalization of the curve whose affine equation is $y^2 = f(x)$. Every element of* $\mathrm{Pic}^2(C)$ *has a unique representation by an effective divisor, with the exception of the canonical class. In addition, every K-rational divisor class of degree 2 can be represented by an effective K-rational divisor.*

Proposition 3.11. *Let C be a smooth plane quartic curve defined over a field K. Every element of* $\mathrm{Pic}^3(C)$ *has a unique representation by an effective divisor unless the divisor class contains $P_1 + P_2 + P_3$ where the three P_i's are collinear. In the latter case $[P_1 + P_2 + P_3] = [Q_1 + Q_2 + Q_3]$ if and only if there are lines L_1 and L_2 and a point R such that $L_1.C = P_1 + P_2 + P_3 + R$ and $L_2.C = Q_1 + Q_2 + Q_3 + R$. Assume, in addition, that C has a K-rational point. Every K-rational divisor class of degree 3 contains an effective K-rational divisor.*

From these follow special cases of the fact that when C has a K-rational point and the group $J(K)$ is finite, then we can describe all points on C over fields of degree over K, less than or equal to the genus. Though we can describe all such points, it is a more difficult problem to pick one of the fields and decide which of those points are defined over that field. We present examples using each of the previous propositions.

Proposition 3.12. *The only* $\mathbf{Q}$*-rational points on the curve* C *given by* $y^2 = x^5+1$ *are* ∞, $(0,\pm1)$ *and* $(-1,0)$. *The only other points on* C *rational over quadratic extensions are* $(1+i,\pm(1-2i))$, $(1-i,\pm(1+2i))$ *and those with* $x \in \mathbf{Q}$.

Note that we could compute a 2-Selmer group or a $(1-\zeta_5)$-Selmer group. We will do the latter, as there are already examples of the former in the literature.

Proof. We can rewrite the curve as $x^5 = (y+1)(y-1)$ and let $K = \mathbf{Q}(\zeta_5)$. We use the endomorphism $\phi = 1-\zeta_5$ of J, the Jacobian of C. The bad primes are the single prime over 2, which we also denote by 2, and the single prime $\mathfrak{p} = 1-\zeta_5$ over 5. The field K has class number 1 and unit rank 1, with fundamental unit $1+\zeta_5$. Thus $K(S,5) = \langle \zeta_5, 1+\zeta_5, 2, 1-\zeta_5\rangle$ and $H^1(K, J[\phi]; S)$ is the kernel of the norm from $L(S,5) = K(S,5)^2$ to K^*/K^{*5}.

We have $K_\mathfrak{p}^*/K_\mathfrak{p}^{*5} = \langle \mathfrak{p}, 1+\mathfrak{p}, 1+\mathfrak{p}^2, 1+\mathfrak{p}^3, 1+\mathfrak{p}^4, 1+\mathfrak{p}^5\rangle$. Let us rename those elements of $K_\mathfrak{p}$ by $\langle a,b,c,d,e,f\rangle$. Any element that is 1 modulo $\mathfrak{p}^6$ is a fifth power, as are the fourth roots of unity. The vectors $[\zeta_5, 1+\zeta_5, 2, 1-\zeta_5] \equiv [b^4c^4e^4, b^2c^4d^2e^4, e^3f, a] \bmod K_\mathfrak{p}^{*5}$. Thus the kernel of $\beta_\mathfrak{p}$ is trivial. From Corollary 3.6, $J(K_\mathfrak{p})/\phi J(K_\mathfrak{p})$ has dimension 3. In the following table we list generators of $J(K_\mathfrak{p})/\phi J(K_\mathfrak{p})$ and their images in $L_\mathfrak{p}^*/L_\mathfrak{p}^{*5}$.

	$y+1$	$y-1$
$[(x_1,\mathfrak{p}^3)-\infty] \mapsto$	d	d^4
$[(x_2,\mathfrak{p}^4)-\infty] \mapsto$	e	e^4
$[(x_3,\mathfrak{p}^5)-\infty] \mapsto$	f	f^4

We see that $\beta_\mathfrak{p}^{-1}$ of the image of $J(K_\mathfrak{p})/\phi J(K_\mathfrak{p})$ is the group generated by the image of $[(0,1)-\infty]$. So that is the Selmer group and $J(K)/\phi J(K)$ is generated by that divisor class. We do not even need $J(K_2)/\phi J(K_2)$. From Corollary 3.7, we see that $J(K)$ has Mordell-Weil rank 0.

Now $\#J(\mathbf{Q})$ is at least 10 since $J(\mathbf{Q})$ contains $[(0,1)-\infty]$ of order 5 and $[(-1,0)-\infty]$ of order 2. By computing $\#J(\mathbf{F}_p)$ for a few primes we can prove that the order of $J(\mathbf{Q})$ divides 10 so it is equal to 10. Let $D = [(0,1)+(-1,0)-2\infty]$. Then $2D = [2(0,1)-2\infty]$, $3D = [(1+i,1-2i)+(1-i,1+2i)-2\infty]$, $4D = [(0,-1)+\infty-2\infty]$, $5D = [(-1,0)+\infty-2\infty]$, $6D = [(0,1)+\infty-2\infty]$, $7D = [(1+i,-1+2i)+(1-i,-1-2i)-2\infty]$, $8D = [2(0,-1)-2\infty]$, $9D = [(0,-1)+(-1,0)-2\infty]$, $10D = [2\infty-2\infty] = 0$.

We have a bijection of the sets $J(\mathbf{Q})$ and $\mathrm{Pic}^2(C)(\mathbf{Q})$ by $[P+Q-2\infty] \mapsto [P+Q]$. From Proposition 3.10, if P is a $\mathbf{Q}$-rational point of C, then $[P+\infty-2\infty]$ must appear in the above list. If P is defined over a quadratic extension of $\mathbf{Q}$ and $\overline{P}$ is its conjugate, then $[P+\overline{P}-2\infty]$ must appear in the above list, unless

$[P + \overline{P} - 2\infty]$ is the canonical class. A simple calculation shows that if that is the case then $x(P) \in \mathbf{Q}$. □

Since J has complex multiplication by a cyclic, quartic, totally imaginary field it is absolutely simple. See [St2] for more discussion of the Mordell-Weil ranks of the Jacobians of curves of the form $y^2 = x^l + k$ where l is an odd prime.

Proposition 3.13. *The only* $\mathbf{Q}$*-rational points on the curve* C *given by* $y^3 = x(x-1)(x-2)(x-3)$ *are* ∞ *and those on* $y = 0$*. The only other points over quadratic extensions of* $\mathbf{Q}$ *are those on* $y = -1$ *and* $y = 2$*. There are 12 conjugate triples of points over cubic extensions that are not collinear. All other points over cubic extensions can be obtained by finding the other three points of intersection of a* $\mathbf{Q}$*-rational line with a point of* $C(\mathbf{Q})$*.*

Proof. We can use $\phi = 1 - \zeta_3$ and the techniques in earlier examples, to show that J has trivial Mordell-Weil rank over $\mathbf{Q}(\zeta_3)$ and hence over $\mathbf{Q}$. Let us compute $J(\mathbf{Q})$. We already have all of $J[\phi]$ rational over $\mathbf{Q}$. The line $y = -1$ is bitangent to C and meets the curve at $2(x_1, -1) + 2(x_2, -1)$ where the x_i are the roots of $x^2 - 3x + 1$. A line L is a bitangent of C if the intersection divisor of L with C is $L.C = 2P + 2Q$ for points P and Q of C (not necessarily distinct). We have a bijection of the sets $J(\mathbf{Q})$ and $\mathrm{Pic}^3(C)(\mathbf{Q})$ by $[P + Q + R - 3\infty] \mapsto [P + Q + R]$. From Proposition 3.11, the order of $[(x_1, -1) + (x_2, -1) + \infty - 3\infty]$ is 2.

The primes of bad reduction over $\mathbf{Q}$ are 2 and 3. The characteristic polynomial of the Frobenius of J over $\mathbf{F}_5$ is $f_5(t) = t^6 - 3t^4 - 15t^2 + 125$ which factors over $\mathbf{Q}$ into irreducible quadratic and quartic factors. Thus J is isogenous over $\mathbf{Q}$ to the sum of the elliptic curve E given by $y^3 = (\hat{x} - 9/4)(\hat{x} - 1/4)$ (where $\hat{x} = (x - \frac{3}{2})^2$) and a 2-dimensional abelian variety which is simple over $\mathbf{Q}$. In addition $\#J(\mathbf{F}_5) = f_5(1) = 4 \cdot 27$. The divisor of $y + 1$ is $4(-1, -1) - 4\infty$ over $\mathbf{F}_5$. From Proposition 3.11, the order of $[(-1, -1) + 2\infty - 3\infty]$ is 4 in $J(\mathbf{F}_5)$. So the 2-power part of $J(\mathbf{F}_5)$ is a cyclic group of order 4.

We have $\#J(\mathbf{F}_{19}) = 16 \cdot 27 \cdot 13$. The curve has 10 rational bitangents over $\mathbf{F}_{19}$. They are the line at infinity, $uy = -1$, $uy = 4x + 10$ and $uy = 10x + 2$ where $u^3 = 1$. This gives us 9 divisor classes of the form $[P_1 + P_2 + \infty - 3\infty]$ where $2P_1 + 2P_2$ is the intersection divisor of C with one of the $\mathbf{F}_{19}$-rational bitangents which is not the line at infinity. Each of these 9 divisor classes is different and has order 2, from Proposition 3.11. The 2-power part of $J(\mathbf{F}_{19})$ has 16 elements and at least 9 have order 2. Thus the 2-power part has exponent 2. Putting together the information from the reductions at 5 and 19, we see that $J(\mathbf{Q}) \cong (\mathbf{Z}/3\mathbf{Z})^3 \oplus \mathbf{Z}/2\mathbf{Z}$. By comparison $E(\mathbf{Q}) \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

We can find an effective representative of each divisor class in $\mathrm{Pic}^3(C)(\mathbf{Q})$. They are supported on the point ∞, the four points on $y = 0$, the two points on the bitangent $y = -1$, the four points on $y = 2$ (each is quadratic over $\mathbf{Q}$), and 12 triples of non-collinear conjugate cubic points. The proposition then follows from Proposition 3.11.

Of course $E(\mathbf{Q})$ gives us the $\mathbf{Q}$-rational points. But it does not give the points defined over quadratic and cubic extensions. □

4 A 2-descent for the Jacobian of a smooth plane quartic curve using bitangents

Let C be the curve over $\mathbf{Q}$ defined by the equation $592900X^4 + (-1609300Y + 1829520Z)X^3 + (1253725Y^2 - 244420ZY + 1648504Z^2)X^2 + (-219450Y^3 - 220390ZY^2 + 58564Z^2Y + 365904Z^3)X + (11025Y^4 + 6510ZY^3 - 31379Z^2Y^2 - 9548Z^3Y + 23716Z^4) = 0$ and let J be its Jacobian. The lines $X = 0$, $Y = 0$, $Z = 0$, $X + Y + Z = 0$, $X - Y - 2Z = 0$, $2X - Y + Z = 0$, and $X - 3Y + 2Z = 0$ are all bitangents of C (see the proof of Proposition 3.13 for the definition of bitangent). The curve C is a smooth plane quartic curve and so has genus 3. We will work over $K = \mathbf{Q}$ and use the multiplication by 2 map from J to itself as our isogeny. In this case $\Psi = \lambda^{-1}\hat{J}[\hat{2}] = J[2]$, where λ is the canonical principal polarization of J with respect to C. The curve C has the property that every element of $J[2]$ is defined over $\mathbf{Q}$. This fact simplifies the example and makes Assumption II hold.

Away from the line $Z = 0$ we let $x = X/Z$ and $y = Y/Z$ and denote points by their affine, (x, y)-coordinates. The divisors of the functions x, y, $x + y + 1$, $y - x + 2$, $y - 2x - 1$ and $x - 3y + 2$ are doubles of divisors, all of whose images have order two in J; in fact they form a basis for $J[2]$. Thus we can let $L = \mathbf{Q}^6$ and $F = (x, y, x+y+1, y-x+2, y-2x-1, x-3y+2)$. The group $H^1(\mathbf{Q}, J[2])$ is isomorphic to $L^*/L^{*2} \cong (\mathbf{Q}^*/\mathbf{Q}^{*2})^6$ by the map $k \circ w$. The map F is an injection from $J(\mathbf{Q})/2J(\mathbf{Q})$ to $(\mathbf{Q}^*/\mathbf{Q}^{*2})^6$. The set $C(\mathbf{Q})$ contains $(-7/5, 0)$ and $(-1/7, 0)$ (coming from the intersection with $y = 0$) and $(1/5, 8/5)$ so Assumption I holds from Proposition 2.7.

It is a straightforward exercise to show that this curve has nonsingular reduction at all finite primes greater than 17 and singular reduction at the others; thus we can let $S = \{\infty, 2, 3, 5, 7, 11, 13, 17\}$. The image of $J(\mathbf{Q})$ under F in $(\mathbf{Q}^*/\mathbf{Q}^{*2})^6$ is contained in the image of $H^1(\mathbf{Q}, J[2]; S)$. Recall from Step 5 that $\mathbf{Q}(S, 2) = \langle -1, 2, 3, 5, 7, 11, 13, 17\rangle \subset \mathbf{Q}^*/\mathbf{Q}^{*2}$. Under the identification of $H^1(\mathbf{Q}, J[2])$ with $(\mathbf{Q}^*/\mathbf{Q}^{*2})^6$, the group $H^1(\mathbf{Q}, J[2]; S)$ gets sent to $L(S, 2) = \mathbf{Q}(S, 2)^6$.

In the following table, we show the images in $L(S, 2)$, under F, of the six elements of $J[2]$ and two other rational divisor classes. Along the top of the table, we list the component functions of F. When we write $\frac{1}{2}(x)$, for example, we mean the divisor whose double is the divisor of x.

	x	y	$x+y+1$	$y-x+2$	$y-2x-1$	$x-3y+2$
$[\frac{1}{2}(x)] \mapsto$	5	$3 \cdot 7$	$2 \cdot 5 \cdot 7$	$2 \cdot 7$	$-2 \cdot 3 \cdot 5 \cdot 7$	$3 \cdot 7$
$[\frac{1}{2}(y)] \mapsto$	$-3 \cdot 7$	$2 \cdot 5 \cdot 11$	$2 \cdot 7$	$2 \cdot 3 \cdot 5 \cdot 7$	-7	$-5 \cdot 7$
$[\frac{1}{2}(x+y+1)] \mapsto$	$-2 \cdot 5 \cdot 7$	$-2 \cdot 7$	$-2 \cdot 5$	7	$-3 \cdot 5 \cdot 7$	-7
$[\frac{1}{2}(y-x+2)] \mapsto$	$-2 \cdot 7$	$-2 \cdot 3 \cdot 5 \cdot 7$	-7	$2 \cdot 5 \cdot 17$	$-2 \cdot 7$	$-3 \cdot 5 \cdot 7$
$[\frac{1}{2}(y-2x-1)] \mapsto$	$2 \cdot 3 \cdot 5 \cdot 7$	7	$3 \cdot 5 \cdot 7$	$2 \cdot 7$	1	$3 \cdot 5 \cdot 7$
$[\frac{1}{2}(x-3y+2)] \mapsto$	$-3 \cdot 7$	$5 \cdot 7$	7	$3 \cdot 5 \cdot 7$	$-3 \cdot 5 \cdot 7$	-13
$[(-7/5, 0) - (-1/7, 0)] \mapsto$	5	-7	$-3 \cdot 5 \cdot 7$	$3 \cdot 7 \cdot 17$	-7	$3 \cdot 5 \cdot 7 \cdot 13$
$[(1/5, 8/5) - (-1/7, 0)] \mapsto$	$-5 \cdot 7$	$3 \cdot 11$	$3 \cdot 5$	$3 \cdot 7 \cdot 17$	-7	$-5 \cdot 7$

The images of all eight divisor classes are independent. Since the images of the six divisor classes of order two are independent, they form a basis for $J[2]$. As the images of the other two divisors are independent of the image of $J[2]$, and of each other in $J(\mathbf{Q})/2J(\mathbf{Q})$, they each have infinite order and are independent in the Mordell-Weil group.

We can compute $S^2(\mathbf{Q}, J)$ in a manner similar to previous examples. The only difference is that we need to compute the intersection of all eight groups $\beta_s^{-1}(F_s(J(\mathbf{Q}_s)/2J(\mathbf{Q}_s)))$ for $s \in S$. The intersection has dimension 8 as an $\mathbf{F}_2$-vector space and a basis is the image of the eight rational divisors in the table. Thus $\dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q}) = 8$ and $\dim_{\mathbf{F}_2} J(\mathbf{Q})[2] = 6$ and so the Mordell-Weil rank is exactly 2.

Proposition 4.1. *The Mordell-Weil group over* $\mathbf{Q}$ *of the Jacobian of the smooth plane quartic curve* C*, which is bitangent to* $X = 0$, $Y = 0$, $Z = 0$, $X + Y + Z = 0$, $X - Y - 2Z = 0$, $2X - Y + Z = 0$, *and* $X - 3Y + 2Z = 0$, *has rank 2.*

Just computing the characteristic polynomial of Frobenius at $p = 19$ seemed infeasible and so we do not know the splitting behavior of J.

5 Examples in the literature for genus higher than 1

In [Sc2], a 2-Selmer group is used to show that the Mordell-Weil rank over $\mathbf{Q}$ of the Jacobian of $y^2 = f(x)$, where $f(x) = x^5 + 16x^4 - 274x^3 + 817x^2 + 178x + 1$, is 7. Let $L = \mathbf{Q}[T]/(f(T))$ and $\mathrm{Cl}(L)$ denote the class group of the field L. The fact that $\dim \mathrm{C}(L)/\mathrm{Cl}(L)^2$ is 4 was exploited. In [Sc1], a 2-Selmer group is used to show that the Mordell-Weil rank of the Jacobian of $y^2 = x(x-2)(x-3)(x-4)(x-5)(x-7)(x-10)$ over $\mathbf{Q}$ is 2. In [St2], Stoll computed both 2-Selmer groups and $(1-\zeta_5)$-Selmer groups for the Jacobians of some curves of the form $y^2 = x^5 + k$. Using information from both, some were shown to have non-trivial 2-parts of their Tate-Shafarevich groups.

In each of these cases, the hyperelliptic curve is of the form described in Sect. 3, namely $y^2 = f(x)$ where f has odd degree. As discussed in Sect. 2.5, there is a way of bounding the Mordell-Weil rank of the Jacobians of hyperelliptic curves of the form $y^2 = f(x)$, where f has even degree; see [Ca, FPS, PS]. The author has used this to show that the Mordell-Weil rank over $\mathbf{Q}$ of the Jacobian of a curve of Colin Stahlke's given by $y^2 = f(x)$ where $f(x) = 121x^6 - 138x^5 + 183x^4 + 370x^3 + 104x^2 - 112x + 1$ is exactly 12. Let $L = \mathbf{Q}[T]/(f(T))$ and $\mathrm{Cl}(L)$ denote the class group of the field L. The fact that $\dim \mathrm{Cl}(L)/\mathrm{Cl}(L)^2$ is 9 was exploited. In [FPS], the Mordell-Weil rank over $\mathbf{Q}$ of the Jacobian of $y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$ is shown to be 1. This is used to show that there are no $\mathbf{Q}$-rational quadratic polynomials with rational periodic points of period 5. In [PS] the algorithm is extended further to curves of the form $y^p = f(x)$ where the prime p divides the degree of f. In addition, the Mordell-Weil rank over $\mathbf{Q}$ of the Jacobian of $y^3 = (x^2 - x + 6)^2(x^8 + 3x + 3)$ is shown to be 2. This example required working in a number field of degree 16 over $\mathbf{Q}$.

Flynn has a technique for bounding the Mordell-Weil rank of the Jacobian J of a hyperelliptic curve C of genus 2 over a number field K, that is the best one available for certain cases (see [Fl, CF]). Let us describe how it fits into our framework and how it can be extended. Assume $J[2]$ has a rational subgroup of order 4 which is isotropic with respect to the 2-Weil pairing. In most cases, the quotient of J by that subgroup is again the Jacobian J' of a genus 2 curve C'. The induced isogeny is called a Richelot's isogeny. We denote it by ϕ. There is similarly a Richelot's isogeny ϕ' from J' to J such that $\phi' \circ \phi = 2$. Because of the isotropy, $\lambda^{-1}\hat{J}[\hat{\phi}'] = J[\phi]$ for the canonical principal polarization λ of J with respect to C (see [Mi2, prop. 16.8]). In [CF], Cassels and Flynn present a method for computing $S^{\phi}(K, J)$ and $S^{\phi'}(K, J')$ assuming that all elements of $J[\phi]$ are rational. They use the method described in Sect. 2. The kernel of a Richelot's isogeny is isomorphic to V_4, the Klein-4 group. The group $H^1(G, V_4)$ is trivial for all $G \subseteq \mathrm{Aut}(V_4)$. Thus for all possible Galois actions on $J[\phi]$ or $J'[\phi']$, Assumption II holds and we can do a descent using a Richelot's isogeny.

There are a few examples in the literature like those in Sect. 3 where $p \neq 2$. In [KS], the Mordell-Weil rank of the Jacobian of $y^3 = x^4 - 1$ over $\mathbf{Q}(\zeta_{12})$ is shown to be 0. Fadeev and McCallum describe a map F for quotients of the pth Fermat curve given by $y^p = x^a(1-x)^b$ with $0 < a, b < p$; see [Fd, Mc].

Acknowledgements. The author is supported by the National Security Agency grant MDA904-95-H-1051. The author is grateful to Gerhard Frey and the Institut für experimentelle Mathematik for their hospitality during the preparation of part of this paper and to Joseph Wetherell and the referee for helpful comments on the manuscript. The author also had useful discussions with Victor Flynn, Everett Howe, Matthew Klassen and Michael Stoll and made much use of the program GP-PARI.

References

[AW] Wall, C.T.C., Atiyah, M.F.: Cohomology of groups. In: Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic number theory, (pp. 94–115) London: Academic Press 1967

[BSD] Birch, B.J., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves I. J. Reine Angew. Math. **212**, 7–25 (1963)

[BK] Brumer, A., Kramer, K.: The rank of elliptic curves. Duke Math. J. **44**, 715–743 (1977)

[Ca] Cassels, J.W.S.: The Mordell-Weil group of curves of genus 2. In: Artin, M., Tate, J. (eds.): Arithmetic and geometry I, (pp. 27–60) Boston: Birkhäuser 1983

[CF] Cassels, J.W.S., Flynn, E.V.: Prolegomena to a middlebrow arithmetic of curves of genus 2. (London Math. Soc., Lecture Notes) Cambridge: Cambridge University Press 1996

[Co] Coleman, R.F.: Effective Chabauty. Duke Math. J. **52**, 765–780 (1985)

[Fd] Faddeev, D.K.: Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in an l-adic cyclotomic field. Tr. Mat. Inst. Steklova **64**, 284–293 (1961)

[Fl] Flynn, E.V.: Descent via isogeny in dimension 2. Acta Arithm. **66**, 23–43 (1994)

[FPS] Flynn, E.V, Poonen, B., Schaefer, E.F.: Cycles of quadratic polynomials and rational points on a genus-two curve. To appear in Duke Math. J.

[GG] Gordon, D., Grant, D.: Computing the Mordell-Weil rank of Jacobians of curves of genus 2. Trans. Amer. Math. Soc. **337**, 807–824 (1993)

[Ha] Hartshorne, R.: Algebraic geometry. Berlin Heidelberg New York: Springer 1977

[KS] Klassen, M.J., Schaefer, E.F.: Arithmetic and geometry of the curve $1+y^3 = x^4$. Acta Arithm. **74** 241–257 (1996)

[Kr] Kramer, K.: A family of semistable elliptic curves with large Tate-Shafarevitch groups. Proc. Amer. Math. Soc. **89**, 379-386 (1983)

[La] Lang, S.: Abelian varieties. New York: Interscience Publishers, 1959
[Li] Lichtenbaum, S.: Duality theorems for curves over P-adic fields. Invent. Math. **7**, 120–136 (1969)
[Ma] Mattuck, A.: Abelian varieties over p-adic ground fields. Ann. of Math. **62**, 92–119 (1955)
[Mc] McCallum, W.G.: On the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve. Invent. Math. **93**, 637–666 (1988)
[Mi1] Milne, J.S.: Jacobian varieties. In: Cornell, G., Silverman, J.H. (eds.): Arithmetic geometry, (pp. 167–212) Berlin Heidelberg New York: Springer 1986
[Mi2] Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.): Arithmetic geometry, (pp. 103–150) Berlin Heidelberg New York: Springer 1986
[Mi3] Milne, J.S.: Arithmetic duality theorems. Orlando: Academic Press, 1986
[PS] Poonen, B., Schaefer, E.F.: Explicit descent for Jacobians of cyclic covers of the projective line. To appear in J. Reine Angew. Math.
[Sc1] Schaefer, E.F.: 2-descent on the Jacobians of hyperelliptic curves. J. Number Theory **51**, 219–232 (1995)
[Sc2] Schaefer, E.F.: Class groups and Selmer groups. J. Number Theory **56**, 79–114 (1996)
[Se] Serre, J.P.: Local fields. Berlin Heidelberg New York: Springer 1979
[St1] Stoll, M.: Implementing 2-descent in genus 2. Preprint
[St2] Stoll, M.: On the Mordell-Weil rank of certain CM curves. Preprint
[Tp] Top, J.: Descent by 3-isogeny and 3-rank of quadratic fields. In: Gouvea, F., Yui, N. (eds.): Advances in number theory (pp. 303–317) Oxford: Clarendon Press 1993
[Tw] Towse, C.: Weierstrass points on cyclic covers of the projective line. To appear in Trans. Amer. Math. Soc. (1996)
[We] Wetherell, J.L.: Bounding the number of rational points through the arithmetic of covers. Preprint