EXPLICIT DESCENT FOR JACOBIANS OF CYCLIC COVERS OF THE PROJECTIVE LINE

BJORN POONEN AND EDWARD F. SCHAEFER

Abstract. We develop a general method for bounding Mordell-Weil ranks of Jacobians of arbitrary curves of the form $y^p = f(x)$. As an example, we compute the Mordell-Weil ranks over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-3})$ for a non-hyperelliptic curve of genus 8.

Contents

1. Introduction

The usual proofs of the Mordell-Weil Theorem for abelian varieties involve working over a field over which all the n-torsion is defined, for some $n \geq 2$. This is fine in theory, but from the computational point of view, it is disastrous already for Jacobians of genus 2 curves over $\mathbf{Q}$, since adjoining the coordinates of all 2-torsion points on such an abelian variety can result in a number field of degree 720.

For such curves, Cassels [7] outlined a possible solution to this problem. For J the Jacobian of $X : y^2 = f(x)$ with $f(x) \in \mathbf{Q}[x]$ of degree 5, he defined an explicit injective

Date: February 10, 1997.

The first author is supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. The second author is supported by National Security Agency grant MDA904-95-H-1051. The final version of this paper has appeared in *J. Reine Angew. Math.* **488** (1997), 141–188.

homomorphism[1]

$$(x-T) : J(\mathbf{Q})/2J(\mathbf{Q}) \hookrightarrow \ker\left(L^*/L^{*2} \xrightarrow{\text{Norm}} \mathbf{Q}^*/\mathbf{Q}^{*2}\right),$$

where $L = \mathbf{Q}[T]/(f(T))$. The first examples were worked out several years later, by Gordon and Grant [10], who solved the problem in the case where all the 2-torsion was defined over $\mathbf{Q}$ by writing down homogeneous spaces of J explicitly. The second author [17] later used the $(x-T)$ map more directly to handle cases without the assumption on the 2-torsion, and without having to write down homogeneous spaces of J. He also showed that the map $(x-T)$ was equivalent to the usual 2-descent map from Galois cohomology, and generalized to all hyperelliptic curves of odd degree. More recently [18], he generalized to curves of the form $y^p = f(x)$ where $f(x)$ had distinct roots, and $\deg f$ was prime to p.

The problem becomes much more complicated when p divides the degree of $f(x)$. For genus 2 curves X over $\mathbf{Q}$ of the form $y^2 = f(x)$ with $\deg f = 6$, Cassels defined a homomorphism

$$(x-T) : J(\mathbf{Q})/2J(\mathbf{Q}) \to \ker\left(L^*/L^{*2}\mathbf{Q}^* \xrightarrow{\text{Norm}} \mathbf{Q}^*/\mathbf{Q}^{*2}\right),$$

where $L = \mathbf{Q}[T]/(f(T))$ again, but this time the cohomological interpretation remained mysterious; this map could not literally be the 2-descent map from Galois cohomology, because as Cassels observed, the kernel of $(x-T)$ could be non-trivial in some cases! The first example was worked out in [9], which also gave a practical characterization of this kernel.

One of the main achievements of this paper is to find a cohomological description of this $(x-T)$ map by relating it to the descent map for a generalized Jacobian.[2] The cohomological description is necessary if one wants to compare the $(x-T)$ descent with the usual 2-descent from Galois cohomology. It also lets one systematically derive many properties of the homomorphism $(x-T)$ that are useful for carrying out the descent in practice.

In fact, we prove our theorems more generally for curves of the form $y^p = f(x)$ with $\deg f$ divisible by p. This class of curves includes Fermat curves, for example. Although it may seem as if the case where p divides $\deg f$ is special, in fact just the opposite is true: given a curve with model $y^p = f(x)$ over a ground field k of characteristic not p, with p *not* dividing f, one can always[3] apply an automorphism of $\mathbf{P}^1$ to x (and adjust y accordingly) in order to move all branch points of $x : X \to \mathbf{P}^1$ away from ∞, and this results in a new model $y^p = g(x)$ with $\deg g$ divisible by p. Conversely, however, given $X : y^p = f(x)$ over k with f a p-th power free polynomial of degree divisible by p, application of an automorphism of $\mathbf{P}^1$ to x can result in a curve $y^p = g(x)$ with p not dividing $\deg g$ only if f has a root in k. This is a somewhat rare event if k is a number field and f has large random coefficients, for instance.

[1] The name "$(x-T)$" for the homomorphism is borrowed from [17]. The reason for this name will be clear from the definition in Section 5.

[2] One can give an explanation for the appearance of this generalized Jacobian. Usually when performing a full or partial p-descent on the Jacobian of a curve, one needs functions whose divisors are p times a divisor representing a p-torsion divisor class, so that adjoining the p-th roots of these functions gives rise to unramified extensions. If f is a p-th power free polynomial of degree divisible by p, and α is a root of f, then the divisor of the function $x-\alpha$ on $y^p = f(x)$ does not have this property: adjoining a p-th root yields a covering ramified above the points at infinity, and such coverings are classified by a generalized Jacobian with modulus supported at these points at infinity.

[3] Actually this will be impossible over k in certain cases where k is a finite field.

After setting up some notation in Section 2, we will need to discuss some technical period-index questions, because we do not assume that our curves have k-rational points, or even k-rational divisor classes of degree 1. Sections 4 and 5 define the curves we will work with, and the various versions of the $(x-T)$ map. Sections 6, 7, and 8 culminate in Section 9, in which the cohomological description of the $(x-T)$ map is given.

Section 10 uses this description to explain why we should expect in general that the $(x-T)$ map will be definable only on the subgroup of $J(k)$ consisting of k-divisor classes representable by k-rational divisors. The cohomological description is then used in Section 11 to prove a rather curious characterization (Theorem 11.3) of the kernel of $(x-T)$, in Section 12 to derive restrictions on its image, and in Section 13 to relate the $(x-T)$ map to the usual Selmer and Shafarevich-Tate groups.

We then use the methods we have developed to compute the Mordell-Weil rank over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-3})$ of the Jacobian of a non-hyperelliptic curve of genus 8. As far as we know, no one has ever computed a Mordell-Weil rank for any curve of genus greater than 3 over a number field before, except for special curves, such as Fermat quotients[4] and modular curves, and curves whose Jacobians split. Combining the result of our computation with a result of Coleman [8], we show that our genus 8 curve has at most 12 rational points, and at most 36 points over $\mathbf{Q}(\sqrt{-3})$.

We conclude the paper with a number of open questions on average Mordell-Weil ranks.

2. Notation

Let k be a field, and let $G_k = \operatorname{Gal}(k^{\mathrm{sep}}/k)$. Throughout the paper we will use $H^i(A)$ as an abbreviation for the cohomology group $H^i(G_k, A)$. Let X be a smooth projective curve over k, and let $X^{\mathrm{sep}} = X \otimes_k k^{\mathrm{sep}}$ denote the same curve with the base field extended to k^{sep}. Let $\operatorname{Div}(X^{\mathrm{sep}})$ denote the group of divisors on X^{sep}, i.e., the free group on the points $X(k^{\mathrm{sep}})$. Let $k^{\mathrm{sep}}(X)$ denote the field of functions of X^{sep}. Let $\operatorname{Princ}(X^{\mathrm{sep}})$ denote the subgroup of principal divisors. Let $\operatorname{Div}(X) = H^0(\operatorname{Div}(X^{\mathrm{sep}}))$, and let $\operatorname{Princ}(X) = H^0(\operatorname{Princ}(X^{\mathrm{sep}}))$, which is also the group of divisors of functions in $k(X)$, the field of functions of X. Let $\operatorname{Pic}(X^{\mathrm{sep}}) = \operatorname{Div}(X^{\mathrm{sep}})/\operatorname{Princ}(X^{\mathrm{sep}})$ denote the group of divisors on X^{sep} modulo linear equivalence, and let $\operatorname{Pic}(X) = \operatorname{Div}(X)/\operatorname{Princ}(X)$. Although the map $\operatorname{Pic}(X) \to H^0(\operatorname{Pic}(X^{\mathrm{sep}}))$ is injective, it is not necessarily surjective; in other words there may exist k-rational divisor classes that do not contain k-rational divisors.

Let S be a finite G_k-stable subset of $X(k^{\mathrm{sep}})$. A *modulus* with support S is a G_k-stable divisor $\mathfrak{m} = \sum_{P\in S} m_P P \in \operatorname{Div}(X)$ with $m_P > 0$. A rational function φ on X^{sep} is said to be 1 mod $\mathfrak{m}$ if the valuation of $1-\varphi$ at each $P \in S$ satisfies $v_P(1-\varphi) \geq m_P$.

Let $\operatorname{Div}_{\mathfrak{m}}(X^{\mathrm{sep}})$ denote the subgroup of $\operatorname{Div}(X^{\mathrm{sep}})$ of divisors with support disjoint from $\mathfrak{m}$. Let $\operatorname{Princ}_{\mathfrak{m}}(X^{\mathrm{sep}})$ denote the subgroup of $\operatorname{Princ}(X^{\mathrm{sep}})$ consisting of divisors of functions on X^{sep} that are 1 mod $\mathfrak{m}$. Let $\operatorname{Div}_{\mathfrak{m}}(X) = H^0(\operatorname{Div}_{\mathfrak{m}}(X^{\mathrm{sep}}))$, and let $\operatorname{Princ}_{\mathfrak{m}}(X) = H^0(\operatorname{Princ}_{\mathfrak{m}}(X^{\mathrm{sep}}))$, which is also the group of divisors of k-rational functions on X that are 1 mod $\mathfrak{m}$. Let $\operatorname{Pic}_{\mathfrak{m}}(X^{\mathrm{sep}}) = \operatorname{Div}_{\mathfrak{m}}(X^{\mathrm{sep}})/\operatorname{Princ}_{\mathfrak{m}}(X^{\mathrm{sep}})$ and $\operatorname{Pic}_{\mathfrak{m}}(X) = \operatorname{Div}_{\mathfrak{m}}(X)/\operatorname{Princ}_{\mathfrak{m}}(X)$. Let $\operatorname{Div}^0(X^{\mathrm{sep}})$ denote the subgroup of $\operatorname{Div}(X^{\mathrm{sep}})$ of divisors of degree zero, and similarly define $\operatorname{Div}^0(X)$, $\operatorname{Pic}^0_{\mathfrak{m}}(X^{\mathrm{sep}})$, etc. as the degree zero parts of the corresponding groups. Finally let $\operatorname{Pic}^{(p)}(X^{\mathrm{sep}})$ denote the subgroup of divisor classes of degree divisible by p in $\operatorname{Pic}(X^{\mathrm{sep}})$. Similarly define $\operatorname{Div}^{(p)}(X^{\mathrm{sep}})$, $\operatorname{Pic}^{(p)}_{\mathfrak{m}}(X)$, etc.

[4] See [13] and the papers referenced there.

Let J be the Jacobian of X, so that $J(k^{\mathrm{sep}}) = \operatorname{Pic}^0(X^{\mathrm{sep}})$. Let $J_{\mathfrak{m}}$ be the generalized Jacobian (see [19]) of the pair $(X, \mathfrak{m})$, so that $J_{\mathfrak{m}}(k^{\mathrm{sep}}) = \operatorname{Pic}^0_{\mathfrak{m}}(X^{\mathrm{sep}})$. Then $J_{\mathfrak{m}}$ is a commutative algebraic group that fits in an exact sequence

$$0 \to \mathcal{T} \to J_{\mathfrak{m}} \to J \to 0 \tag{1}$$

where $\mathcal{T}$ is a connected commutative linear algebraic group.

We will specialize some of these definitions and make a few more in Section 4.

3. Period and index

The reader is invited to skip this section until the results here are referred to. This section considers questions of existence of rational divisor classes and rational divisors of given degree, and questions of representability of rational divisor classes by rational divisors. As mentioned in Section 2, the injection $\operatorname{Pic}(X) \to H^0(\operatorname{Pic}(X^{\mathrm{sep}}))$ is not always an isomorphism; in general there is an exact sequence

$$0 \to \operatorname{Pic}(X) \to H^0(\operatorname{Pic}(X^{\mathrm{sep}})) \xrightarrow{\theta} \operatorname{Br}(k) \to \operatorname{Br}(X) \to H^1(\operatorname{Pic}(X^{\mathrm{sep}})) \to H^3(k^{\mathrm{sep}*}), \tag{2}$$

where $\operatorname{Br}(k) = H^2(k^{\mathrm{sep}*})$ is the Brauer group of k, and $\operatorname{Br}(X)$ can be defined as the kernel of the natural homomorphism $H^2(k^{\mathrm{sep}}(X)^*) \to H^2(\operatorname{Div}(X^{\mathrm{sep}}))$ since X is a curve. (See [12].) There is also a pairing

$$\rho_0 : H^1(\operatorname{Pic}^0(X^{\mathrm{sep}})) \times H^0(\operatorname{Pic}^0(X^{\mathrm{sep}})) \to \operatorname{Br}(k). \tag{3}$$

The exact sequence

$$0 \longrightarrow \operatorname{Pic}^0(X^{\mathrm{sep}}) \longrightarrow \operatorname{Pic}(X^{\mathrm{sep}}) \xrightarrow{\deg} \mathbf{Z} \longrightarrow 0$$

gives rise to

$$H^0(\operatorname{Pic}(X^{\mathrm{sep}})) \xrightarrow{\deg} \mathbf{Z} \longrightarrow H^1(\operatorname{Pic}^0(X^{\mathrm{sep}})), \tag{4}$$

and we let $\mathfrak{c}$ denote the image of $1 \in \mathbf{Z}$ in $H^1(\operatorname{Pic}^0(X^{\mathrm{sep}}))$. Then for all $x \in H^0(\operatorname{Pic}^0(X^{\mathrm{sep}}))$,

$$\theta(x) = \rho_0(\mathfrak{c}, x), \tag{5}$$

as in the proof of Corollary 1 in [12][5].

The *index* of a curve X over a field k is the greatest common divisor of the degrees of all k-rational divisors. The *period* of a curve X over a field k is the greatest common divisor of the degrees of all k-rational divisor classes.

Proposition 3.1. *The cokernel of the injection* $\operatorname{Pic}(X) \to H^0(\operatorname{Pic}(X^{sep}))$ *is killed by the index I of X over k. In particular, if $I = 1$, then* $\operatorname{Pic}(X) \to H^0(\operatorname{Pic}(X^{sep}))$ *is an isomorphism.*

Proof. Let $D = \sum_P n_P P$ be a k-rational divisor of degree I. For each P occuring in D, choose a uniformizing parameter t_P defined over $k(P)$. Assume that the choices are made so that if P' is a G_k-conjugate of P, then $t_{P'}$ is the conjugate of t_P. Define a map

$$\begin{aligned} k^{\mathrm{sep}}(X)^* &\xrightarrow{\Phi} k^{\mathrm{sep}*} \\ f &\mapsto \prod_P \left(\frac{f}{t_P^{\operatorname{ord}_P f}}(P) \right)^{n_P}. \end{aligned}$$

[5] Corollary 1 in [12] is stated for k a p-adic field, but the part of the proof verifying this formula for θ does not use any properties of k.

The composition

$$k^{\mathrm{sep}*} \hookrightarrow k^{\mathrm{sep}}(X)^* \xrightarrow{\Phi} k^{\mathrm{sep}*}$$

is the I-th power map, so the kernel of

$$H^2(k^{\mathrm{sep}*}) \to H^2(k^{\mathrm{sep}}(X)^*)$$

is killed by I. This kernel is the same as the cokernel of $\mathrm{Pic}(X) \to H^0(\mathrm{Pic}(X^{\mathrm{sep}}))$, by (2). □

Proposition 3.2. *The cokernel of the injection* $\mathrm{Pic}^0(X) \to H^0(\mathrm{Pic}^0(X^{sep}))$ *is killed by the period P of X over k. In particular, if $P = 1$, then* $\mathrm{Pic}^0(X) \to J(k)$ *is an isomorphism.*

Proof. By (4), the order of $\mathfrak{c}$ is P. Thus by (5), $P \cdot \theta(x) = \rho_0(P\mathfrak{c}, x) = 0$ for all $x \in H^0(\mathrm{Pic}^0(X^{\mathrm{sep}}))$, as desired. □

If k is a global field[6], we let P_v denote the period of X over a completion k_v of k.

Proposition 3.3. *Suppose X is a curve over a global field k. If $P_v = 1$ for all places v of k, then the map* $\mathrm{Pic}^0(X) \to H^0(\mathrm{Pic}^0(X^{sep})) = J(k)$ *is an isomorphism.*

Proof. This follows from Proposition 3.2 and the fact that $\mathrm{Br}(k) \to \prod_v \mathrm{Br}(k_v)$ is injective. See also [15, p. 168] and [12, pp. 130–131] for the number field case. □

Proposition 3.4. *If k is a local field, then the period P of X over k divides $g - 1$.*

Proof. We will model our proof on the proof given by Lichtenbaum [12] when k was a finite extension of $\mathbf{Q}_p$. We retain the notation of the proof of Proposition 3.2. The homomorphism

$$\rho_0^* : H^1(\mathrm{Pic}^0(X^{\mathrm{sep}})) \to \mathrm{Hom}(H^0(\mathrm{Pic}^0(X^{\mathrm{sep}})), \mathrm{Br}(k))$$

induced by the pairing ρ_0 in (3) is an isomorphism, by [16, I.§3, Remark 3.7] for the archimedean case, [12, Theorem 2] or [16, I.§3, Corollary 3.4] for the unequal characteristic nonarchimedean case, and [16, III.§7, Theorem 7.8] for the equicharacteristic nonarchimedean case. The order of $\mathfrak{c}$ in $H^1(\mathrm{Pic}^0(X^{\mathrm{sep}}))$ is P. By (5), $\rho_0^*(\mathfrak{c}) = \theta$, so the group $\theta(H^0(\mathrm{Pic}^0(X^{\mathrm{sep}})))$ has exponent P (exactly). On the other hand,

$$(P + g - 1)\theta(H^0(\mathrm{Pic}^0(X^{\mathrm{sep}}))) = 0$$

as in the proof of Theorem 7 in [12]. Hence $P+g-1 \equiv 0 \pmod{P}$, which gives the result. □

In contrast with the situation with the usual Jacobian, k-rational points of generalized Jacobians are always represented by k-rational divisors, as we now prove.

Proposition 3.5. *If $\mathfrak{m}$ is nonzero, then the natural injection* $\mathrm{Pic}_{\mathfrak{m}}(X) \to H^0(\mathrm{Pic}_{\mathfrak{m}}(X^{sep}))$ *is an isomorphism.*

Proof. Let $k^{\mathrm{sep}}(X)_{\mathfrak{m}}$ denote the subgroup of $k^{\mathrm{sep}}(X)^*$ consisting of functions with no zeros or poles at points in $\mathfrak{m}$. Let $k^{\mathrm{sep}}(X)_{\mathfrak{m},1}$ denote the subgroup of functions that are 1 mod $\mathfrak{m}$. Define $k(X)_{\mathfrak{m}}$ and $k(X)_{\mathfrak{m},1}$ as the G_k-invariants of these groups. Let $\mathbf{Z}^{\mathfrak{m}}$ denote the free abelian group generated by the distinct points in $\mathfrak{m}$. We have an exact sequence of G_k-modules

$$1 \to k^{\mathrm{sep}}(X)_{\mathfrak{m}} \to k^{\mathrm{sep}}(X)^* \to \mathbf{Z}^{\mathfrak{m}} \to 1$$

[6] In this paper, a global field is a finite extension of $\mathbf{Q}$ or a finite extension of $\mathbf{F}_q(t)$ for some q. A local field is the completion of a global field at some place.

where the last map gives the $\mathfrak{m}$-part of the divisor of $h \in k^{\text{sep}}(X)^*$. Taking Galois cohomology, we obtain

$$k(X)^* \to H^0(\mathbf{Z}^{\mathfrak{m}}) \to H^1(k^{\text{sep}}(X)_{\mathfrak{m}}) \to H^1(k^{\text{sep}}(X)^*).$$

The first map is surjective, since standard approximation theorems let one find a k-rational function having prescribed orders of vanishing at a finite set of points whenever the orders of vanishing prescribed are equal at G_k-conjugate points. Also $H^1(k^{\text{sep}}(X)^*) = 0$ by Noether's generalization of Hilbert's Theorem 90. Therefore $H^1(k^{\text{sep}}(X)_{\mathfrak{m}}) = 0$.

Let $\mathcal{O}_P$ denote the local ring at P on X^{sep}, and let $\mathfrak{a}_P$ denote its maximal ideal. Let $R_{\mathfrak{m}} = \prod_{P \in S} (\mathcal{O}_P/\mathfrak{a}_P^{m_P})^*$. Then we have the exact sequence

$$1 \to k^{\text{sep}}(X)_{\mathfrak{m},1} \to k^{\text{sep}}(X)_{\mathfrak{m}} \to R_{\mathfrak{m}} \to 1$$

Taking Galois cohomology, we obtain

$$k(X)_{\mathfrak{m}} \to H^0(R_{\mathfrak{m}}) \to H^1(k^{\text{sep}}(X)_{\mathfrak{m},1}) \to H^1(k^{\text{sep}}(X)_{\mathfrak{m}}) = 0.$$

The first map is surjective, since standard approximation theorems let one find a k-rational function with prescribed residues modulo powers of the maximal ideal at a finite set of points, provided that the residues prescribed are G_k-conjugate at G_k-conjugate points. Thus $H^1(k^{\text{sep}}(X)_{\mathfrak{m},1}) = 0$.

Since $\mathfrak{m}$ is nonzero, the divisor map gives an isomorphism

$$k^{\text{sep}}(X)_{\mathfrak{m},1} \cong \operatorname{Princ}_{\mathfrak{m}}(X^{\text{sep}}).$$

Thus $H^1(\operatorname{Princ}_{\mathfrak{m}}(X^{\text{sep}})) = 0$ too. Taking Galois cohomology of

$$0 \to \operatorname{Princ}_{\mathfrak{m}}(X^{\text{sep}}) \to \operatorname{Div}_{\mathfrak{m}}(X^{\text{sep}}) \to \operatorname{Pic}_{\mathfrak{m}}(X^{\text{sep}}) \to 0$$

yields

$$0 \to \operatorname{Princ}_{\mathfrak{m}}(X) \to \operatorname{Div}_{\mathfrak{m}}(X) \to H^0(\operatorname{Pic}_{\mathfrak{m}}(X^{\text{sep}})) \to H^1(\operatorname{Princ}_{\mathfrak{m}}(X^{\text{sep}})) = 0,$$

which yields

$$\operatorname{Pic}_{\mathfrak{m}}(X) = \frac{\operatorname{Div}_{\mathfrak{m}}(X)}{\operatorname{Princ}_{\mathfrak{m}}(X)} \cong H^0(\operatorname{Pic}_{\mathfrak{m}}(X^{\text{sep}})),$$

as desired. □

4. Cyclic covers of the projective line

We retain the notation of Section 2, but now specialize to the types of curves we are interested in. Let p be a prime. From now on, we assume that the field k is *not* of characteristic p, and that k contains a primitive p-th root of unity ζ.[7] Let $\pi : X \to \mathbf{P}^1$ be a cyclic cover of $\mathbf{P}^1$ over k of degree p, such that all the branch points are in $\mathbf{P}^1(k^{\text{sep}})$.[8] Applying an automorphism of $\mathbf{P}^1$ if necessary, we may assume that X is unramified above the point $\infty \in \mathbf{P}^1$, at least if the cardinality of k is greater than the number of branch

[7] If we are interested in Mordell-Weil ranks over fields k not containing a primitive p-th root of unity, we can do all our computations over $k(\zeta)$ and at the end apply Lemma 13.4.

[8] We insist that the $\mathbf{P}^1$ actually be $\mathbf{P}^1$ over k, and not a twisted form. (Of course, we also want X and π to be defined over k.) It is possible to have cyclic covers of twists of $\mathbf{P}^1$, even if k is a number field: in fact there exist hyperelliptic curves of any odd genus g over k, that are not of the form $y^2 = f(x)$ over k. For instance, the space curve over $\mathbf{Q}$ defined by the equations $x^2 + z^2 = -1$ and $y^2 = (x-1)(x-2)(x-3)(x-4)$ is a double cover of the conic $x^2 + z^2 = -1$ ramified at 8 points, so it is a hyperelliptic curve of genus 3, but its quotient by the hyperelliptic involution $(x, y, z) \mapsto (x, -y, z)$ is the conic, which has no rational point.

points of π. (For simplicity, we will make this assumption.[9]) By Kummer theory, X has a (possibly singular) model $y^p = f(x)$ where $f(x) \in k[x]$ factors over k^{sep} as $c \prod_{i=1}^{d}(x-\alpha_i)^{n_i}$ with $1 \le n_i < p$. The degree of $f(x)$ must be divisible by p, since otherwise X would be ramified above ∞. Applying the Riemann-Hurwitz formula to π shows that the genus g of X equals $(d-2)(p-1)/2$.

We take as our modulus on X the divisor $\mathfrak{m} = \pi^*\infty \in \operatorname{Div}(X)$, which is a sum of p distinct points individually defined over $k(c^{1/p})$, where $c \in k^*$ is the leading coefficient of f. Now $\mathcal{T}$ is a $(p-1)$-dimensional torus, and the generalized Jacobian $J_{\mathfrak{m}}$ is a semiabelian variety. For example, if $p=2$, then $\mathcal{T}$ is the twist $\mathbf{G}_m(c)$ of $\mathbf{G}_m$ associated to the (at most) quadratic extension $k(\sqrt{c})/k$. We can also define a (disconnected) commutative algebraic group $\mathcal{J}_{\mathfrak{m}}$ over k such that $\mathcal{J}_{\mathfrak{m}}(k^{\mathrm{sep}}) = \operatorname{Pic}_{\mathfrak{m}}(X^{\mathrm{sep}})/(\mathbf{Z}\cdot\mathfrak{m}')$, where $\mathfrak{m}'$ denotes the class of π^*P in $\operatorname{Pic}_{\mathfrak{m}}(X^{\mathrm{sep}})$ for any $P \in \mathbf{A}^1(k) \subset \mathbf{P}^1(k)$.[10] This class is independent of the choice of P, because the functions $(x-a)/(x-b)$ are 1 mod $\mathfrak{m}$. We have an exact sequence

$$0 \longrightarrow J_{\mathfrak{m}} \longrightarrow \mathcal{J}_{\mathfrak{m}} \xrightarrow{\deg} \mathbf{Z}/p\mathbf{Z} \longrightarrow 0. \tag{6}$$

In abuse of notation, let ζ denote the automorphism $(x,y) \mapsto (x,\zeta y)$ of X. By extending linearly, we obtain a map $\zeta_* : \operatorname{Div}(X^{\mathrm{sep}}) \to \operatorname{Div}(X^{\mathrm{sep}})$. Let ϕ denote the formal sum $(1-\zeta) + \sum_{i=0}^{p-1}\zeta^i$ and let $\psi = \sum_{i=0}^{p-2}(p-1-i)\zeta^i$. Then we define maps ϕ_* and ψ_* on $\operatorname{Div}(X^{\mathrm{sep}})$ in the obvious way, and we have

$$\phi_*\psi_* D = pD + \frac{p^2-p-2}{2}(1+\zeta+\zeta^2+\cdots+\zeta^{p-1})_* D.$$

We should warn that $(1+\zeta+\zeta^2+\cdots+\zeta^{p-1})_*$ is not zero as a map on $\operatorname{Div}(X^{\mathrm{sep}})$ or $\operatorname{Pic}(X^{\mathrm{sep}})$. Nevertheless, for any affine point $Q \in X(k^{\mathrm{sep}})$, the divisor $Q + \zeta(Q) + \zeta^2(Q) + \cdots + \zeta^{p-1}(Q)$ is trivial in $\mathcal{J}_{\mathfrak{m}}$, so we obtain a well-defined action of the cyclotomic ring $\mathbf{Z}[\zeta]$ on J, $J_{\mathfrak{m}}$, and $\mathcal{J}_{\mathfrak{m}}$, and also on $\mathcal{T}$. In particular, ϕ and ψ act on all of these, and their composition $\phi\psi$ is simply multiplication-by-p. Note that ϕ acts on these simply as $1-\zeta$.[11]

In the remaining paragraph of this section, let us suppose k is a global field, and let us specialize some of the results of Section 3 to our situation. The existence of $\mathfrak{m}$ forces $P_v = 1$ or $P_v = p$ for each v. By Proposition 3.4, if $g \not\equiv 1 \pmod{p}$, then $P_v = 1$ for all v, so that $\operatorname{Pic}^0(X) \to J(k)$ is an isomorphism, by Proposition 3.3. In particular if X is the hyperelliptic curve $y^2 = f(x)$, and g is even, then $P_v = 1$ for all v. If $p \ge 3$, the condition $g \not\equiv 1 \pmod{p}$ is equivalent to $d \not\equiv 0 \pmod{p}$, since $g = (d-2)(p-1)/2$.

5. The $(x-T)$ maps

Let $f_0(x) = c_0 \prod_{i=1}^{d}(x-\alpha_i) \in k[x]$ be the radical of f, where c_0 may be chosen as any fixed nonzero element of k. (When working over number fields, it may be convenient to choose c_0 so as to clear any denominators arising from the possible non-integrality of the α_i.) Let L be the separable algebra $k[T]/(f_0(T))$, and let $L^{\mathrm{sep}} = L \otimes k^{\mathrm{sep}}$. It will sometimes be convenient to identify L^{sep} with $k^{\mathrm{sep}} \times k^{\mathrm{sep}} \times \cdots \times k^{\mathrm{sep}}$, with the image of T corresponding to $(\alpha_1, \alpha_2, \ldots, \alpha_d)$. We say a divisor is *good*[12] if its support is disjoint from $\mathfrak{m}$ and the

[9] If k is a very small finite field, we can replace k by a finite extension without doing too much damage.

[10] We would like to take $\mathfrak{m}'$ to be $\mathfrak{m}$ itself, but $\mathfrak{m}$ is not in $\operatorname{Div}_{\mathfrak{m}}(X^{\mathrm{sep}})$.

[11] The reason for not defining ϕ as $1-\zeta$ in the first place is that we will need $\phi : \operatorname{Pic}(X^{\mathrm{sep}}) \to \operatorname{Pic}^{(p)}(X^{\mathrm{sep}})$ to be a surjection with finite kernel. (See Section 9.)

[12] The terminology differs slightly from that in [9]: there a good divisor also had to be k-rational.

ramification points of π (the points where $y = 0$)[13]. When a divisor $D = \sum n_P P$ and the divisor of a function h have disjoint supports, recall that $h(D)$ is defined as $\prod_P h(P)^{n_P}$. We define $(x-T)(D)$ similarly, even though $(x-T)$ is not literally a rational function on X: if $D = \sum n_P P \in \operatorname{Div}(X^{\mathrm{sep}})$ is good, we define

$$(x-T)(D) = \prod_P (x_P - T)^{n_P} \in L^{\mathrm{sep}},$$

where x_P denotes the x-coordinate of the affine point P. Since each x_P is not a root of $f(x)$, $(x-T)(D) \in L^{\mathrm{sep}*}$. Moreover, if D is actually in $\operatorname{Div}(X)$, then by Galois theory, $(x-T)(D) \in L^*$.

Suppose $D = \operatorname{div} h \in \operatorname{Princ}(X)$ is a good k-rational divisor that is also principal. (Assume h is defined over k as well.) For each root α of $f(x)$, Weil reciprocity gives

$$(x-\alpha)(D) = (x-\alpha)(\operatorname{div} h) = h(\operatorname{div}(x-\alpha)) = \frac{h((\alpha,0))^p}{h(\mathfrak{m})},$$

so

$$(x-T)(D) = \frac{h((T,0))^p}{h(\mathfrak{m})} \in L^{*p}k^*.$$

If moreover $D \in \operatorname{Princ}_{\mathfrak{m}}(X)$, then $h(\mathfrak{m}) = 1$, so $(x-T)(D) \in L^{*p}$. By standard approximation theorems for valuations, every divisor in $\operatorname{Div}(X)$ is linearly equivalent to a good divisor in $\operatorname{Div}(X)$, and every divisor in $\operatorname{Div}_{\mathfrak{m}}(X)$ differs from a good divisor in $\operatorname{Div}_{\mathfrak{m}}(X)$ by a divisor in $\operatorname{Princ}_{\mathfrak{m}}(X)$, so from the above we obtain induced $(x-T)$ maps that fit into a commutative diagram:

$$\begin{tikzcd} \operatorname{Pic}_{\mathfrak{m}}(X) \arrow[r, "(x-T)"] \arrow[d] & L^*/L^{*p} \arrow[d] \\ \operatorname{Pic}(X) \arrow[r, "(x-T)"] & L^*/L^{*p}k^*. \end{tikzcd} \tag{7}$$

Remark. In Section 10, it will be explained why one cannot expect to extend $(x-T)$ to a map defined on all of $J(k)$, at least not if one wants a homomorphism taking values in $L^*/L^{*p}k^*$.

Proposition 5.1. *The kernel of $(x-T)$ contains $\phi \operatorname{Pic}_{\mathfrak{m}}(X)$ (resp. $\phi \operatorname{Pic}(X)$). It also contains $\mathfrak{m}'$ (resp. $\mathfrak{m}$). If there is a k-rational point ∞_1 on X above $\infty \in \mathbf{P}^1$, then it too is killed by the $(x-T)$ map on $\operatorname{Pic}(X)$.*

Proof. For any good k-rational divisor D, $(x-T)(\zeta_* D) = (x-T)(D)$ directly from the definition, since ζ preserves x-coordinates. Hence

$$(x-T)(\phi_* D) = \frac{(x-T)(D)}{(x-T)(D)}(x-T)(D)^p \in L^{*p}.$$

For the second statement, it suffices to show that if $E = \sum_P n_P P$ is any k-rational divisor on $\mathbf{P}^1$ with support away from ∞ and the branch points of π, then $(x-T)(\pi^* E)$ is trivial.

[13] It is not true in general that all Weierstrass points of X are ramification points of π, even when $g > 1$. See [22] for some quantitative statements.

Let x_P denote the coordinate of a point $P \in \mathbf{P}^1$. We find

$$(x-T)(\pi^* E) = \left(\prod_P (x_P - T)^{n_P} \right)^p \in L^{*p},$$

as desired.

If ∞_1 is k-rational, then we can write $f(x) = a^p x^{np} + \dots$ with $a \in k^*$. Choose i so that $y/(\zeta^i a x^n)$ has value 1 at ∞_1. Let $g(x) \in k[x]$ be a polynomial of degree $m \geq n$, with leading coefficient $\zeta^i a$ and such that the degree of $h(x) = g(x)^p - x^{(m-n)p} f(x)$ is $mp-1$ and such that $g(x)$ shares no roots with f. Write $h(x) = b \prod_{i=1}^{mp-1} (x - \beta_i)$. Choose $i(x), j(x) \in k[x]$ monic of degrees l and $l+m$ respectively, such that neither shares a root with f.[14] Denote the roots of $i(x)$ and $j(x)$ by γ_i and δ_i respectively. Define

$$\begin{aligned} D &:= \operatorname{div} \left(\frac{j(x)}{i(x)(g(x) - x^{m-n} y)} \right) \\ &= \sum_{i=1}^{l+m} \sum_{j=0}^{p-1} \left(\gamma_i, \zeta^j y_{\gamma_i} \right) - \sum_{i=1}^{l} \sum_{j=0}^{p-1} \left(\delta_i, \zeta^j y_{\delta_i} \right) - \infty_1 - \sum_{i=1}^{mp-1} \left(\beta_i, y_{\beta_i} \right). \end{aligned}$$

Note that $D + \infty_1$ is a k-rational good divisor. We have

$$\begin{aligned} (x-T)(\infty_1) &\equiv (x-T)(D + \infty_1) \\ &\equiv \frac{\left[(-1)^{l+m} j(T) \right]^p}{\left[(-1)^l i(T) \right]^p} \cdot \frac{b}{(-1)^{mp-1} \left[g(T)^p - T^{(m-n)p} f(T) \right]} \\ &\equiv \left[\frac{j(T)}{i(T) g(T)} \right]^p \cdot (-1)^s b \qquad \text{(for some } s\text{)} \\ &\equiv 1 \pmod{L^{*p} k^*}. \end{aligned}$$

□

If the natural injection $\operatorname{Pic}^0(X) \to J(k)$ is an isomorphism, we can rewrite the $(x-T)$ map on the degree zero part as

$$(x-T) : J(k)/\phi J(k) \to L^*/L^{*p} k^*. \tag{8}$$

The relationship between this map and the homomorphism originally defined by Cassels in [7] is easy to describe. By the final paragraph of Section 4, $\operatorname{Pic}^0(X) \to J(k)$ is an isomorphism in the special case ($p = 2$) of a genus 2 hyperelliptic curve $y^2 = f(x)$ with $f \in \mathbf{Q}[x]$ and $\deg f = 6$. Thus we obtain a map as in (8), and this coincides with Cassels' map

$$(x-T) : J(\mathbf{Q})/2J(\mathbf{Q}) \to L^*/L^{*2} \mathbf{Q}^*.$$

Remarks. Although it may seem that the definition of $(x-T)$ depends on the choice of parameter on $\mathbf{P}^1$, especially in light of the last part of Proposition 5.1, the dependence is mainly superficial. Suppose that $\alpha(x) = (ax+b)/(cx+d)$ is an automorphism of $\mathbf{P}^1$ over k, and that $\bar{\pi} = \alpha \circ \pi : X \to \mathbf{P}^1$ is another cyclic cover unramified above ∞. We then obtain a new model $y^p = \bar{f}(x)$, a new algebra $\bar{L} = k[\bar{T}]/\bar{f}(\bar{T})$, and a new map

$$(x - \bar{T}) : \operatorname{Pic}(X) \to \bar{L}^*/\bar{L}^{*p} k^*.$$

[14] We can always take $l = 0$ except in certain cases when k is a very small finite field.

But there is an isomorphism $\breve{\alpha} : \bar{L} \to L$ of k-algebras taking $\bar{T}$ to $(aT+b)/(cT+d)$, and one can easily check that

$$\breve{\alpha}((x-\bar{T})(\mathcal{D})) = (x-T)(\mathcal{D}) \tag{9}$$

at least for $\mathcal{D} \in \operatorname{Pic}^{(p)}(X)$. (It suffices to check this for $\alpha(x) = ax+b$ and $\alpha(x) = 1/x$, since such automorphisms generate $\operatorname{Aut}(\mathbf{P}^1)$.)

In Section 9 we will give an alternative description of $(x-T)$ using cohomology, that is valid only on $\operatorname{Pic}^{(p)}(X)$. The fact that (9) can fail for $\mathcal{D} \in \operatorname{Pic}(X) \setminus \operatorname{Pic}^{(p)}(X)$ explains why we should not expect such an ∞-independent description to extend to all of $\operatorname{Pic}(X)$.

6. Description of ϕ-torsion in terms of ramification points and L^{sep}

The purpose of this section is to give concrete descriptions of $J[\phi]$, $J_{\mathfrak{m}}[\phi]$ and $\mathcal{J}_{\mathfrak{m}}[\phi]$ in terms of the ramification points of π and the algebra L^{sep}. First let us compute their dimensions. Throughout this paper, $\dim V$ will denote the $\mathbf{F}_p$-dimension of V.

Lemma 6.1. *We have* $\dim J[\phi] = d-2$, $\dim \mathcal{T}[\phi] = 1$, $\dim J_{\mathfrak{m}}[\phi] = d-1$, *and* $\dim \mathcal{J}_{\mathfrak{m}}[\phi] = d$. *Moreover, ϕ is surjective as an endomorphism of $J(k^{sep})$, $\mathcal{T}(k^{sep})$, or $J_{\mathfrak{m}}(k^{sep})$.*

Proof. The endomorphism ζ on J satisfies $X^{p-1} + X^{p-2} + \cdots + 1 = 0$. Its characteristic polynomial $P(X)$ is a polynomial in $\mathbf{Z}[X]$ of degree $2g = (d-2)(p-1)$, so it can only be $(X^{p-1} + X^{p-2} + \cdots + 1)^{d-2}$. In particular the degree of $\phi = 1 - \zeta$ equals $P(1) = p^{d-2}$, so $\dim J[\phi] = d-2$. The endomorphism ϕ on J is an isogeny, so it is surjective on $J(k^{\text{sep}})$.

Over $k(c^{1/p})$, $\mathcal{T}$ becomes isomorphic to $(\mathbf{G}_m)^p/\mathbf{G}_m$, where the last $\mathbf{G}_m$ is embedded diagonally, and ζ acts by cyclically permuting the coordinates. Thus $\mathcal{T}[\phi]$ is one-dimensional, generated by $(1, \zeta, \zeta^2, \ldots, \zeta^{p-1})$, and $\phi : \mathcal{T}(k^{\text{sep}}) \to \mathcal{T}(k^{\text{sep}})$ is surjective. Applying the snake lemma to

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{T} \arrow[r] \arrow[d, "\phi"] & J_{\mathfrak{m}} \arrow[r] \arrow[d, "\phi"] & J \arrow[r] \arrow[d, "\phi"] & 0 \\
0 \arrow[r] & \mathcal{T} \arrow[r] & J_{\mathfrak{m}} \arrow[r] & J \arrow[r] & 0
\end{tikzcd}$$

shows that $\dim J_{\mathfrak{m}}[\phi] = \dim \mathcal{T}[\phi] + \dim J[\phi] = d-1$, and that $\phi : J_{\mathfrak{m}}(k^{\text{sep}}) \to J_{\mathfrak{m}}(k^{\text{sep}})$ is surjective. Applying the snake lemma to

$$\begin{tikzcd}
0 \arrow[r] & J_{\mathfrak{m}} \arrow[r] \arrow[d, "\phi"] & \mathcal{J}_{\mathfrak{m}} \arrow[r] \arrow[d, "\phi"] & \mathbf{Z}/p\mathbf{Z} \arrow[r] \arrow[d, "p"] & 0 \\
0 \arrow[r] & J_{\mathfrak{m}} \arrow[r] & \mathcal{J}_{\mathfrak{m}} \arrow[r] & \mathbf{Z}/p\mathbf{Z} \arrow[r] & 0
\end{tikzcd}$$

shows that $\dim \mathcal{J}_{\mathfrak{m}}[\phi] = \dim J_{\mathfrak{m}}[\phi] + 1 = d$. □

For $1 \le i \le d$, let W_i be the point $(\alpha_i, 0)$. Let $\mathfrak{W} = \oplus_{i=1}^d \mathbf{Z} \cdot W_i \subset \operatorname{Div}(X^{\text{sep}})$. Let $\mathfrak{W}^0$ be the kernel of the degree map $\mathfrak{W} \to \mathbf{Z}$, and let $\mathfrak{S} = \sum_{i=1}^d n_i W_i \in \mathfrak{W}$. (Recall that n_i is the multiplicity of $(x-\alpha)$ in $f(x)$.)

Proposition 6.2. *The map $\operatorname{Div}(X^{sep}) \to \mathcal{J}_{\mathfrak{m}}(k^{sep})$ induces an isomorphism of $\mathbf{Z}/p\mathbf{Z}$-graded G_k-modules $\mathfrak{W}/p\mathfrak{W} \to \mathcal{J}_{\mathfrak{m}}[\phi]$. Restricting to the degree zero parts gives $\mathfrak{W}^0/p\mathfrak{W}^0 \cong J_{\mathfrak{m}}[\phi]$. If $\mathfrak{T}$ is any fixed divisor of degree $(\deg f)/p$ in $\mathfrak{W}$, then $\mathfrak{S} - p\mathfrak{T}$ generates a subgroup of $\mathfrak{W}^0/p\mathfrak{W}^0$ corresponding under this isomorphism to the kernel $\mathcal{T}[\phi]$ of the surjection $J_{\mathfrak{m}}[\phi] \to J[\phi]$.*

Proof. Clearly $\phi(W_i) = \mathfrak{m}' = 0$ in $\mathcal{J}_\mathfrak{m}$, so $\mathfrak{W}$ maps into $\mathcal{J}_\mathfrak{m}[\phi]$, and $p\mathfrak{W}$ is in the kernel of the map, since $\mathcal{J}_\mathfrak{m}[\phi]$ is killed by p. Conversely, if $D \in \mathfrak{W}$ is in the kernel, then $\deg D$ must be divisible by p, and after adding a multiple of pW_1 (which is a form of $\mathfrak{m}'$), we may assume $D = \operatorname{div} h$ where h is 1 mod $\mathfrak{m}$. The automorphism ζ fixes D, so $D = \operatorname{div}(h \circ \zeta^{-1})$ also. Since h and $h \circ \zeta^{-1}$ are both 1 mod $\mathfrak{m}$, we have $h = h \circ \zeta^{-1}$, so $h = h_0(x)$ for some rational function h_0 of x. Then $D = \operatorname{div} h_0(x) \in p\mathfrak{W}$. Hence the map $\mathfrak{W}/p\mathfrak{W} \to \mathcal{J}_\mathfrak{m}[\phi]$ is injective. But $\dim \mathfrak{W}/p\mathfrak{W} = d = \dim \mathcal{J}_\mathfrak{m}[\phi]$ by Lemma 6.1, so the map must be an isomorphism.

Restricting to the degree zero parts gives $\mathfrak{W}^0/p\mathfrak{W}^0 \cong J_\mathfrak{m}[\phi]$. If $\mathfrak{T}$ is a divisor $\sum a_i W_i$ of degree $(\deg f)/p$, then $\mathfrak{S} - p\mathfrak{T}$ is the divisor of $y/\prod(x-\alpha_i)^{a_i}$. Therefore $\mathfrak{S} - p\mathfrak{T}$ corresponds under this isomorphism to an element of $J_\mathfrak{m}[\phi]$ that gets killed in $J[\phi]$. On the other hand, $\mathfrak{S} - p\mathfrak{T}$ is nonzero in $\mathfrak{W}^0/p\mathfrak{W}^0$, and the kernel $\mathcal{T}[\phi]$ of $J_\mathfrak{m}[\phi] \to J[\phi]$ is only 1-dimensional, by Lemma 6.1, so we are done. □

Since $0 < n_i < p$, we may define an isomorphism of G_k-modules

$$\begin{aligned} \epsilon : \mathfrak{W}/p\mathfrak{W} \cong \mathcal{J}_\mathfrak{m}[\phi] &\to \mu_p(L^{\text{sep}}) \\ W_i \qquad\qquad &\mapsto (1, \dots, 1, \zeta^{(n_i^{-1} \bmod p)}, 1, \dots, 1), \end{aligned}$$

with the ζ in the i-th component of L^{sep}.[15] It is designed so that $\epsilon(\mathfrak{S} - p\mathfrak{T})$ equals the diagonal embedding of ζ in $\mu_p(L^{\text{sep}})$.

For $\beta = (\beta_1, \dots, \beta_d) \in L^{\text{sep}*}$, define a "weighted norm" $N(\beta) = \prod_{i=1}^d \beta_i^{n_i} \in k^{\text{sep}*}$. Then N is a Galois-equivariant homomorphism $L^{\text{sep}*} \to k^{\text{sep}*}$. If all the n_i are 1 (which is automatic if $p = 2$), then N is simply the norm map. The following alternative definition of N is more suitable for computation. Let $f(x) = c \prod f_j(x)^{m_j}$ be the factorization of f over k into irreducibles, and let $L_j = k[T]/(f_j(T))$, so that $L = \prod L_j$ is the decomposition of L into fields, and let $L_j^{\text{sep}} = L_j \otimes_k k^{\text{sep}}$. Let $\beta_{(j)}$ denote the component in L_j^{sep} of $\beta \in L^{\text{sep}*}$, and define $N(\beta) = \prod \operatorname{Norm}_{L_j^{\text{sep}}/k^{\text{sep}}}(\beta_{(j)})^{m_j}$. If $\beta \in L^*$, then $N(\beta) = \prod \operatorname{Norm}_{L_j/k}(\beta_{(j)})^{m_j} \in k^*$.

The degree map $\mathfrak{W}/p\mathfrak{W} \to \mathbf{Z}/p\mathbf{Z}$ corresponds to $N : \mu_p(L^{\text{sep}}) \to \mu_p(k^{\text{sep}})$ under the isomorphisms $\epsilon : \mathfrak{W}/p\mathfrak{W} \to \mu_p(L^{\text{sep}})$ and $\mathbf{Z}/p\mathbf{Z} \to \mu_p(k^{\text{sep}})$, where the latter takes 1 to ζ. (This is the reason for defining N as above.) Thus $\mathfrak{W}^0/p\mathfrak{W}^0$ and $J_\mathfrak{m}[\phi]$ are isomorphic to the kernel of $\mu_p(L^{\text{sep}}) \xrightarrow{N} \mu_p(k^{\text{sep}})$. As mentioned before, $\mathfrak{S} - p\mathfrak{T} \in \mathfrak{W}^0/p\mathfrak{W}^0$ maps to $\zeta \in \mu_p(k^{\text{sep}}) \subset \mu_p(L^{\text{sep}})$ under this isomorphism, so by Proposition 6.2, we obtain the isomorphism

$$J[\phi] \cong \ker\left(\frac{\mu_p(L^{\text{sep}})}{\mu_p(k^{\text{sep}})} \xrightarrow{N} \mu_p(k^{\text{sep}})\right),$$

which we will again denote ϵ.

7. An extended Weil pairing

In this section we define a "Weil pairing"

$$e_p : \mathcal{J}_\mathfrak{m}[p] \times \mathcal{J}_\mathfrak{m}[p] \to \mu_p(k^{\text{sep}}),$$

and show that it is related to the isomorphism ϵ of the previous section. If one restricts this pairing e_p to the degree zero part, $J_\mathfrak{m}[p]$, then the subgroup $\mathcal{T}[p]$ is in the kernel on each side, and one recovers the usual Weil pairing on $J[p]$.

[15] The name ϵ is chosen in light of the results of the next section, where it is shown that ϵ can be related to the Weil pairing.

Given $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_\mathfrak{m}[p]$, choose representing divisors $D_1, D_2 \in \operatorname{Div}_\mathfrak{m}(X^{\text{sep}})$, and let $d_i = \deg D_i$. Then there are unique functions h_i such that $x^{-d_i} h_i$ is $1 \bmod \mathfrak{m}$ and $\operatorname{div}(h_i) = pD_i - d_i\mathfrak{m}$. Define

$$e_p(\mathcal{D}_1, \mathcal{D}_2) = e_p(D_1, D_2) = (-1)^{d_1 d_2} \prod_P (-1)^{p(\operatorname{ord}_P D_1)(\operatorname{ord}_P D_2)} \frac{h_2^{\operatorname{ord}_P D_1}}{h_1^{\operatorname{ord}_P D_2}}(P) \in k^{\text{sep}*}, \tag{10}$$

where the product is over all $P \in X(k^{\text{sep}})$. For a divisor D, $\operatorname{ord}_P D$ is defined to be the coefficient of P in D; when h is a function, $\operatorname{ord}_P h$ is defined to be $\operatorname{ord}_P(\operatorname{div} h)$. When D_1 and D_2 have disjoint supports, we have the simpler formula $e_p(D_1, D_2) = (-1)^{d_1 d_2} h_2(D_1)/h_1(D_2)$. If one considers only D_1 and D_2 of degree 0, we recover a well-known definition of the usual Weil pairing, and this will vindicate the claim made at the beginning of this section, once we show that e_p is a well-defined pairing on $\mathcal{J}_\mathfrak{m}[p]$.

First let us check that the definition does not depend on the choice of D_1. If $D_1' = D_1 + \operatorname{div} j$, where j is 1 mod $\mathfrak{m}$, then we must take $h_1' = h_1 j^p$, and we find

$$\begin{aligned}
\frac{e_p(D_1', D_2)}{e_p(D_1, D_2)} &= \prod_P (-1)^{p(\operatorname{ord}_P j)(\operatorname{ord}_P D_2)} \frac{h_2^{\operatorname{ord}_P j}}{j^{p \operatorname{ord}_P D_2}}(P) \qquad (\text{since } \deg \operatorname{div} j = 0) \\
&= \prod_P (-1)^{(\operatorname{ord}_P j)(\operatorname{ord}_P h_2 + d_2 \operatorname{ord}_P \mathfrak{m})} \frac{h_2^{\operatorname{ord}_P j}}{j^{\operatorname{ord}_P h_2}}(P) \qquad (\text{since } j \text{ is } 1 \bmod \mathfrak{m}) \\
&= \prod_P (-1)^{(\operatorname{ord}_P j)(d_2 \operatorname{ord}_P \mathfrak{m})} \qquad (\text{by Weil reciprocity}) \\
&= 1,
\end{aligned}$$

since the supports of $\operatorname{div} j$ and $\mathfrak{m}$ are disjoint. If $D_1' = D_1 + \mathfrak{m}'$ where we abuse notation by writing $\mathfrak{m}'$ for the particular divisor $\pi^*(0) = \mathfrak{m} + \operatorname{div} x = \sum_{i=0}^{p-1} \zeta^i Q$, where $Q = (0, f(0)^{1/p})$, then we must take $h_1' = x^p h_1$, and we find

$$\begin{aligned}
\frac{e_p(D_1', D_2)}{e_p(D_1, D_2)} &= (-1)^{pd_2} \prod_P (-1)^{p(\operatorname{ord}_P \mathfrak{m}')(\operatorname{ord}_P D_2)} \frac{h_2^{\operatorname{ord}_P \mathfrak{m}'}}{x^{p \operatorname{ord}_P D_2}}(P) \\
&= (-1)^{pd_2} \prod_P (-1)^{(\operatorname{ord}_P \mathfrak{m}')(d_2 \operatorname{ord}_P \mathfrak{m} + \operatorname{ord}_P h_2)} \frac{h_2^{\operatorname{ord}_P(\mathfrak{m} + \operatorname{div} x)}}{x^{\operatorname{ord}_P(d_2\mathfrak{m} + \operatorname{div} h_2)}}(P) \\
&\qquad (\text{by definition of } \mathfrak{m}' \text{ and } h_2) \\
&= (-1)^{pd_2} \prod_P (-1)^{d_2(\operatorname{ord}_P \mathfrak{m}')(\operatorname{ord}_P \mathfrak{m})} \prod_P (-1)^{(\operatorname{ord}_P \mathfrak{m}' - \operatorname{ord}_P x)(\operatorname{ord}_P h_2)} \\
&\qquad \times \prod_P \frac{h_2^{\operatorname{ord}_P \mathfrak{m}}}{x^{\operatorname{ord}_P(d_2\mathfrak{m})}}(P) \prod_P (-1)^{\operatorname{ord}_P h_2 \operatorname{ord}_P x} \frac{h_2^{\operatorname{ord}_P x}}{x^{\operatorname{ord}_P h_2}}(P).
\end{aligned}$$

The first product equals 1, since $\mathfrak{m}$ and $\mathfrak{m}'$ have disjoint supports. The second product equals

$$\prod_P (-1)^{(\operatorname{ord}_P \mathfrak{m})(\operatorname{ord}_P h_2)} = (-1)^{pd_2},$$

since $x^{-d_2}h_2$ is 1 mod $\mathfrak{m}$. The third product equals $(x^{-d_2}h_2)(\mathfrak{m}) = 1$, again since $x^{-d_2}h_2$ is 1 mod $\mathfrak{m}$. The fourth product equals 1 by Weil reciprocity. Hence we obtain

$$\frac{e_p(D_1', D_2)}{e_p(D_1, D_2)} = 1,$$

as desired. The same considerations show that the definition of e_p does not depend on the choice of D_2. Bilinearity of e_p is clear, and it follows that e_p takes values in μ_p. Directly from the definition, $e_p(\mathcal{D}_1, \mathcal{D}_2)e_p(\mathcal{D}_2, \mathcal{D}_1) = 1$, so e_p is skew-symmetric if $p > 2$, and symmetric if $p = 2$.

Proposition 7.1. *If $\mathcal{D} \in \mathcal{J}_{\mathfrak{m}}[p]$, then $\epsilon(\psi\mathcal{D}) = e_p(\mathcal{D}, (T, 0))$.*

Remark. The equality in the proposition is an abbreviation: what we mean is that for each i, the i-th component of the left hand side in $L^{\mathrm{sep}} = k^{\mathrm{sep}} \times k^{\mathrm{sep}} \times \cdots \times k^{\mathrm{sep}}$ equals $e_p(\mathcal{D}, (\alpha_i, 0))$. We will use similar abbreviations later in the paper, often without further mention. One can think of $(x - T)(D)$ as being another such abbreviation.

Proof. Let $D = \sum_P c_P P \in \operatorname{Div}(X^{\mathrm{sep}})$ be a good divisor representing the class $\mathcal{D}$, and let $d_1 = \deg D = \sum_P c_P$. Since $\phi\psi = p$ as an endomorphism of $\mathcal{J}_{\mathfrak{m}}$, $\psi\mathcal{D} \in \mathcal{J}_{\mathfrak{m}}[\phi]$, so by Proposition 6.2 there exists a divisor $E = \sum_{i=1}^d q_i W_i \in \mathfrak{W}$ and a function j on X such that j is 1 mod $\mathfrak{m}$ and $\psi_* D = E + \operatorname{div} j$. Applying $(1-\zeta)_*$ to both sides kills E, and we obtain

$$\left(p - \sum_{i=0}^{p-1} \zeta^i\right)_* D = (1-\zeta)_* \operatorname{div} j$$

$$pD - \sum_P c_P \sum_{i=0}^{p-1} \zeta^i(P) = \operatorname{div} j - \zeta_*(\operatorname{div} j)$$

$$pD - d_1\mathfrak{m} - \operatorname{div}\left(\prod_P (x - x_P)^{c_P}\right) = \operatorname{div}\left(\frac{j}{j \circ \zeta^{-1}}\right),$$

since $\zeta_*(\operatorname{div} j) = (\zeta^{-1})^* (\operatorname{div} j)$, where $(\zeta^{-1})^*$ is the pullback action on $\operatorname{Div}(X^{\mathrm{sep}})$ in the opposite direction coming from the automorphism $\zeta^{-1} : X \to X$. Hence $pD - d_1\mathfrak{m} = \operatorname{div} h_1$ where

$$h_1 = \left(\frac{j}{j \circ \zeta^{-1}}\right) \cdot \prod_P (x - x_P)^{c_P}.$$

Since j is 1 mod $\mathfrak{m}$, we find that $x^{-d_1}h_1$ is 1 mod $\mathfrak{m}$ also.

The function $h_2 = x - \alpha_i$ satisfies $\operatorname{div} h_2 = pW_i - \mathfrak{m}$, and $x^{-1}h_2$ is 1 mod $\mathfrak{m}$. By (the simple case of) the definition of e_p, we have

$$\begin{aligned} e_p(D, W_i) &= (-1)^{d_1} h_2(D)/h_1(W_i) \\ &= (-1)^{d_1} \frac{j \circ \zeta^{-1}}{j}(W_i) \ \ \frac{\prod_P (x_P - \alpha_i)^{c_P}}{\prod_P (\alpha_i - x_P)^{c_P}} \\ &= (-1)^{d_1} \frac{j \circ \zeta^{-1}}{j}(W_i) \ \ (-1)^{\sum_P c_P} \\ &= \frac{j \circ \zeta^{-1}}{j}(W_i). \end{aligned}$$

By definition of j, $\operatorname{ord}_{W_i}(j) = -q_i$. On the other hand, $\operatorname{ord}_{W_i}(y) = n_i$. Therefore the function $\ell = y^{q_i} j^{n_i}$ has no pole or zero at W_i. Using the fact that $\frac{y \circ \zeta^{-1}}{y}$ is the constant function with value $\zeta^{-1} \in k$, we obtain

$$\begin{aligned} e_p(D, W_i)^{n_i} &= \frac{j^{n_i} \circ \zeta^{-1}}{j^{n_i}}(W_i) \\ &= \frac{\ell(\zeta^{-1}(W_i))}{\ell(W_i)} \quad \frac{y^{-q_i} \circ \zeta^{-1}}{y^{-q_i}}(W_i) \\ &= \frac{\ell(W_i)}{\ell(W_i)} \quad \left(\zeta^{-1}\right)^{-q_i} \\ &= \zeta^{q_i}. \end{aligned}$$

Since $e_p(D, W_i) \in \mu_p(k^{\text{sep}})$, and $0 < n_i < p$, we find

$$e_p(D, W_i) = \zeta^{(n_i^{-1} \bmod p) q_i}$$

which by definition of ϵ and q_i equals the i-th component of $\epsilon(E) = \epsilon(\psi \mathcal{D})$, as desired. □

8. The main diagram

From the identifications of Section 6, we get the following commutative diagram (11) below with exact rows and columns. If we identify $\mathcal{T}[\phi]$ with $\mu_p(k^{\text{sep}})$ (as is possible by the proof of Lemma 6.1), the leftmost column becomes simply the exact sequence of ϕ-torsion in (1). Let q denote the quotient map $\mu_p(L^{\text{sep}}) \to \frac{\mu_p(L^{\text{sep}})}{\mu_p(k^{\text{sep}})}$.

(11)
$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mu_p(k^{\text{sep}}) \arrow[r, equal] \arrow[d] & \mu_p(k^{\text{sep}}) \arrow[d] & & \\
0 \arrow[r] & J_{\mathfrak{m}}[\phi] \arrow[r, "\epsilon"] \arrow[d] & \mu_p(L^{\text{sep}}) \arrow[r, "N"] \arrow[d, "q"] & \mu_p(k^{\text{sep}}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & J[\phi] \arrow[r, "\epsilon"] \arrow[d] & \frac{\mu_p(L^{\text{sep}})}{\mu_p(k^{\text{sep}})} \arrow[r, "N"] \arrow[d] & \mu_p(k^{\text{sep}}) \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

We now compute the long exact sequences of cohomology for all the rows and columns. Both $H^1(k^{\text{sep}*})$ and $H^1(L^{\text{sep}*})$ are 0 (the latter is Exercise 2 on page 152 in [20]), so $H^1(\mu_p(k^{\text{sep}})) = k^*/k^{*p}$ and similarly $H^1(\mu_p(L^{\text{sep}})) = L^*/L^{*p}$. Also, $H^2(\mu_p(k^{\text{sep}})) = \operatorname{Br}(k)[p]$, the p-torsion of the Brauer group of k. We obtain our main diagram (12), in which all rows and columns are exact.

(12)

$$\begin{tikzcd}
 & & k^*/k^{*p} \arrow[r, equal] \arrow[d] & k^*/k^{*p} \arrow[d] & \\
\mu_p(L) \arrow[r, "N"] \arrow[d] & \mu_p(k) \arrow[r, "\delta'"] \arrow[d, equal] & H^1(J_{\mathfrak{m}}[\phi]) \arrow[r, "\epsilon"] \arrow[d] & L^*/L^{*p} \arrow[r, "N"] \arrow[d, "q"] & k^*/k^{*p} \arrow[d, equal] \\
H^0\left(\dfrac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \arrow[r, "N"] & \mu_p(k) \arrow[r, "\delta"] & H^1(J[\phi]) \arrow[r, "\epsilon"] \arrow[d, "\Upsilon"] & H^1\left(\dfrac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \arrow[r] \arrow[d] & k^*/k^{*p} \\
 & & \mathrm{Br}(k)[p] \arrow[r, equal] & \mathrm{Br}(k)[p] &
\end{tikzcd}$$

We denote by δ', δ, and Υ the connecting homomorphisms in the diagram.

9. Cohomological reinterpretation of $(x - T)$

The map ϕ on $\mathrm{Pic}(X^{\mathrm{sep}})$ is not surjective, because it multiplies degrees by p. It is, however, surjective as an endomorphism of the degree zero part $J(k^{\mathrm{sep}})$, by Lemma 6.1, so the map $\phi : \mathrm{Pic}(X^{\mathrm{sep}}) \to \mathrm{Pic}^{(p)}(X^{\mathrm{sep}})$ is surjective. Its kernel is contained in the degree zero part, so we obtain

$$0 \to J[\phi] \longrightarrow \mathrm{Pic}(X^{\mathrm{sep}}) \xrightarrow{\phi} \mathrm{Pic}^{(p)}(X^{\mathrm{sep}}) \longrightarrow 0.$$

The corresponding long exact sequence of cohomology results in a map

$$\iota : H^0(\mathrm{Pic}^{(p)}(X^{\mathrm{sep}})) \to H^1(J[\phi]). \tag{13}$$

with kernel $\phi H^0(\mathrm{Pic}(X^{\mathrm{sep}}))$. Restricting to the degree zero part yields the more familiar ϕ-descent homomorphism

$$J(k)/\phi J(k) \to H^1(J[\phi]).$$

Taking the long exact sequences of cohomology associated with the rows of

$$\begin{tikzcd}
0 \arrow[r] & J[p] \arrow[r] \arrow[d, "\psi"] & J \arrow[r, "p"] \arrow[d, "\psi"] & J \arrow[r] \arrow[d, "1"] & 0 \\
0 \arrow[r] & J[\phi] \arrow[r] & J \arrow[r, "\phi"] & J \arrow[r] & 0
\end{tikzcd}$$

yields

(14)

$$\begin{tikzcd}
0 \arrow[r] & J(k)/pJ(k) \arrow[r] \arrow[d, "1"] & H^1(J[p]) \arrow[d, "\psi"] \\
0 \arrow[r] & J(k)/\phi J(k) \arrow[r, "\iota"] & H^1(J[\phi]),
\end{tikzcd}$$

the compatibility relation between ι on $J(k)$ and the usual p-descent map.

In exactly the same way, but remembering also Proposition 3.5, we obtain a map

$$\iota' : \mathrm{Pic}^{(p)}_{\mathfrak{m}}(X) \to H^1(J_{\mathfrak{m}}[\phi]), \tag{15}$$

whose restriction to the subgroup $J_{\mathfrak{m}}(k)$ has kernel $\phi J_{\mathfrak{m}}(k)$.

Lemma 9.1. *We have $\delta(\zeta) = \iota(\mathfrak{m})$ and $\delta'(\zeta) = \iota'(\mathfrak{m}')$. They are represented by the cocycle $\xi_\sigma = {}^\sigma W_i - W_i$ in $H^1(J[\phi])$ or $H^1(J_{\mathfrak{m}}[\phi])$, respectively.*

Proof. Let $\ell = (\zeta^{n_1^{-1} \bmod p}, 1, 1, \dots, 1) \in \mu_p(L^{\text{sep}})$. Then $N(\ell) = \zeta$, by definition of N, and $\delta(\zeta)$ is by definition represented by the cocycle $\sigma \mapsto \mathcal{D}_\sigma$ where $\epsilon(\mathcal{D}_\sigma) = {}^\sigma\ell/\ell$. But $\epsilon(W_1) = \ell$, so $\epsilon({}^\sigma W_1 - W_1) = {}^\sigma\ell/\ell$, which proves that ξ when $i = 1$ represents $\delta(\zeta)$.

On the other hand, for any i, $\phi W_i = pW_i$, which is equivalent to $\mathfrak{m}$ in $\operatorname{Pic}(X^{\text{sep}})$, so $\iota(\mathfrak{m})$ is by definition represented by ξ.

The same proof verifies the analogous statements for $J_\mathfrak{m}$ in place of J. □

Corollary 9.2. *The kernel of* $\epsilon : H^1(J[\phi]) \to H^1\left(\frac{\mu_p(L^{sep})}{\mu_p(k^{sep})}\right)$ *is generated by* $\iota(\mathfrak{m})$*. The kernel of* $\epsilon : H^1(J_\mathfrak{m}[\phi]) \to L^*/L^{*p}$ *is generated by* $\iota'(\mathfrak{m}')$*.*

Proof. By (12), the first kernel is generated by $\delta(\zeta)$, and the second kernel is generated by $\delta'(\zeta)$. Now use Lemma 9.1. □

Theorem 9.3. *The restriction of*

$$(x - T) : \operatorname{Pic}_\mathfrak{m}(X) \to L^*/L^{*p}$$

to $\operatorname{Pic}_\mathfrak{m}^{(p)}(X)$ *coincides with the composition*

$$\epsilon \circ \iota' : \operatorname{Pic}_\mathfrak{m}^{(p)}(X) \to L^*/L^{*p}.$$

Proof. By Proposition 5.1 and Corollary 9.2, both maps kill $\mathfrak{m}'$, so it suffices to show that the maps coincide on $\operatorname{Pic}_\mathfrak{m}^0(X) = J_\mathfrak{m}(k)$. Given an element of $J_\mathfrak{m}(k)$, let $D \in \operatorname{Div}_\mathfrak{m}^0(X)$ be a good divisor representing it. Choose a good divisor $E \in \operatorname{Div}_\mathfrak{m}^0(X^{\text{sep}})$ such that $pE - D = \operatorname{div} j$ for a function j that is 1 mod $\mathfrak{m}$. Then $\iota'(D)$ is the cohomology class of the cocycle $\sigma \mapsto \psi({}^\sigma E - E)$ in $H^1(J_\mathfrak{m}[\phi])$. By Proposition 7.1, $(\epsilon \circ \iota')(D)$ considered as an element of $H^1(\mu_p(L^{\text{sep}}))$ is the cohomology class of the cocycle $\xi_\sigma := e_p({}^\sigma E - E, (T, 0))$. We have $\operatorname{div}({}^\sigma j/j) = p({}^\sigma E - E)$ and $\operatorname{div}(x - T) = p(T, 0) - \mathfrak{m}$. Hence

$$\begin{aligned}
\xi_\sigma &= e_p({}^\sigma E - E, (T, 0)) \\
&= \frac{(x - T)({}^\sigma E - E)}{({}^\sigma j/j)((T, 0))} \qquad \text{(by the simple case of the definition of } e\text{)} \\
&= {}^\sigma\beta/\beta,
\end{aligned}$$

where $\beta := (x - T)(E)/j((T, 0)) \in L^{\text{sep}}$. Now

$$\begin{aligned}
\beta^p &= \frac{(x - T)(pE)}{j(p(T, 0))} \\
&= \frac{(x - T)(D + \operatorname{div} j)}{j(\mathfrak{m} + \operatorname{div}(x - T))} \\
&= (x - T)(D)\frac{(x - T)(\operatorname{div} j)}{j(\operatorname{div}(x - T))} \qquad \text{(since } j \text{ is 1 mod } \mathfrak{m}\text{)} \\
&= (x - T)(D),
\end{aligned}$$

by Weil reciprocity. It follows that the cohomology class of ξ coincides with the image of $(x - T)(D)$ under the Kummer identification $L^*/L^{*p} \to H^1(\mu_p(L^{\text{sep}}))$, which is what we needed. □

Theorem 9.4. *The restrictions of the maps*

$$q \circ (x - T) : \operatorname{Pic}(X) \to L^*/L^{*p}k^* \hookrightarrow H^1\left(\frac{\mu_p(L^{sep})}{\mu_p(k^{sep})}\right)$$

and

$$\epsilon \circ \iota : H^0(\mathrm{Pic}^{(p)}(X^{sep})) \to H^1\left(\frac{\mu_p(L^{sep})}{\mu_p(k^{sep})}\right)$$

to their common domain of definition $\mathrm{Pic}^{(p)}(X)$ *coincide.*

Proof. We have a commutative diagram (with non-exact rows)

$$\begin{tikzcd}
\mathrm{Pic}^{(p)}_{\mathfrak{m}}(X) \arrow[r, "\iota'"] \arrow[d] & H^1(J_{\mathfrak{m}}[\phi]) \arrow[r, "\epsilon"] \arrow[d] & L^*/L^{*p} \arrow[d, "q"] \\
\mathrm{Pic}^{(p)}(X) \arrow[r, "\iota"] & H^1(J[\phi]) \arrow[r, "\epsilon"] & H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)
\end{tikzcd} \tag{16}$$

and also the diagram (7). Since $\mathrm{Pic}^{(p)}_{\mathfrak{m}}(X) \to \mathrm{Pic}^{(p)}(X)$ is surjective, the desired result follows from Theorem 9.3. □

Corollary 9.5. *The composition*

$$\mathrm{Pic}^{(p)}(X) \xrightarrow{\iota} H^1(J[\phi]) \xrightarrow{\Upsilon} \mathrm{Br}(k)[\phi]$$

is zero.

Proof. This follows from Theorem 9.4 (and a diagram chase in (12)). □

10. The maximal domain of definition of $(x - T)$

The results of this section will not be needed in the rest of the paper, so it may be skipped on a first reading.

Originally the $(x - T)$ map was not defined on all of $J(k)$; instead it was defined (in the degree zero part) only on the subgroup $\mathrm{Pic}^0(X)$ of divisor classes represented by k-rational divisors. Of course, the map would be more useful if it could be defined on all of $J(k)$. Using Theorem 9.3 and viewing q as an identification of $L^*/L^{*2}k^*$ with a subgroup of $H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$, we can extend $(x - T)$ to the map

$$\epsilon \circ \iota : J(k) \longrightarrow H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right).$$

But if we want a homomorphism with values in $L^*/L^{*2}k^*$, we must restrict the domain of the function to the kernel of $\Upsilon \circ \iota$, as a diagram chase in (12) shows. In this section, we relate Υ to two pairings taking values in $\mathrm{Br}(k)$, and hence show that the kernel of $\Upsilon \circ \iota$ is exactly $\mathrm{Pic}^0(X)$. This explains why the original domain of definition $\mathrm{Pic}^0(X)$ is the largest subgroup H of $J(k)$ for which we can expect a natural homomorphism

$$(x - T) : H \to L^*/L^{*2}k^*.$$

The first pairing will be derived from the ϕ-Weil pairing on J. The automorphism ζ of J respects the natural principal polarization, because it comes from an automorphism of X. Therefore $\zeta^\dagger = \zeta^{-1}$ where † denotes the Rosati involution defined by this polarization (see [14, p. 139]). Hence $\phi^\dagger = 1 - \zeta^{-1} = \zeta^{-1}\phi$ in $\mathrm{End}\, J$. In particular, the kernel of the dual isogeny $\hat{\phi} : \hat{J} \to \hat{J}$ can be identified with $J[\phi]$. Thus the ϕ-Weil pairing is a map

$$e_\phi : J[\phi] \times J[\phi] \to \mu_p(k^{\mathrm{sep}}).$$

Lemma 10.1. *Let $a, b \in J[\phi]$. Then $e_\phi(a,b) = e_\phi(b,a)$.*

Proof. Let A and B be divisors of degree 0 such that $\psi_* A$ and $\psi_* B$ represent a and b in $J[\phi]$, respectively. We may assume that the x-coordinates of the points in the support of A differ from the x-coordinates of the points in the support of B. We have $pA = \mathrm{div} h$, $pB = \mathrm{div} j$ for some functions h and j. Also,

$$e_\phi(\psi_* A, \psi_* B) = e_p(A, \psi_* B) \text{ and } e_\phi(\psi_* B, \psi_* A) = e_p(B, \psi_* A).$$

Let $\psi^\dagger$ denote the endomorphism gotten by replacing ζ by ζ^{-1} in the definition of ψ. On J, the endomorphism $\psi^\dagger$ is the image of ψ under the Rosati involution. Note that $\psi^\dagger + \psi = p + (p-2)(1 + \ldots + \zeta^{p-1})$. In order to compute $e_p(A, \psi_* B)$, we need to find a function whose divisor is $p\psi_* B$. We have

$$p\psi_* B = \psi_* pB = \psi_* \mathrm{div} j = \mathrm{div}(j \circ \psi^\dagger)$$

where $j \circ \psi^\dagger$ is the function sending a point P of C to the image of j on the divisor $\psi^\dagger P$. Similarly, $p\psi_* A = \mathrm{div}(h \circ \psi^\dagger)$. Thus we have

$$\frac{e_\phi(a,b)}{e_\phi(b,a)} = \frac{e_p(A, \psi_* B)}{e_p(B, \psi_* A)} = \frac{j(\psi^\dagger_* A)}{h(\psi_* B)} \cdot \frac{j(\psi_* A)}{h(\psi^\dagger_* B)} = \frac{j((\psi^\dagger + \psi)_* A)}{h((\psi^\dagger + \psi)_* B)}$$

$$= \frac{j(pA + (p-2)(1 + \ldots + \zeta^{p-1})_* A)}{h(pB + (p-2)(1 + \ldots + \zeta^{p-1})_* B)} = \frac{j(\mathrm{div} h)}{h(\mathrm{div} j)} \left(\frac{j(\mathrm{div} \prod_{P \in A}(x - x_P))}{h(\mathrm{div} \prod_{P \in B}(x - x_P))} \right)^{p-2}$$

$$= \left(\frac{\prod_{P \in A}(x - x_P)(pB)}{\prod_{P \in B}(x - x_P)(pA)} \right)^{p-2} = \left(\frac{\prod_{P \in A}(x - x_P)(B)}{\prod_{P \in B}(x - x_P)(A)} \right)^{p(p-2)} = 1.$$

(In the product over $P \in A$, etc., we take P's with multiplicity.) □

The pairing e_ϕ induces a cup product pairing

$$\eta : H^1(J[\phi]) \times H^1(J[\phi]) \to H^2(\mu_p(k^{\mathrm{sep}})) = \mathrm{Br}(k)[p].$$

Explicitly, if $\{\alpha_\sigma\}$ and $\{\beta_\tau\}$ are cocycles representing elements of $H^1(J[\phi])$, then $\eta(\alpha, \beta)$ is represented by the 2-cocyle

$$(\sigma, \tau) \mapsto e_\phi\left(\alpha_\sigma, {}^\sigma\beta_\tau\right).$$

Lemma 10.2. *The cup product pairing η is anti-symmetric.*

Proof. This follows from Lemma 10.1 and a standard property of the cup product. (See [1, Proposition 9(ii)].) □

Proposition 10.3. *For all $x \in H^1(J[\phi])$, $\Upsilon(x) = \eta(x, \delta(\zeta))$.*

Proof. We will prove that $\Upsilon(x) = -\eta(\delta(\zeta), x)$. The result then follows from the anti-symmetry of η proven in Lemma 10.2. Let x be a 1-cocycle in $H^1(J[\phi])$. Let b_σ be the unique degree 0 divisor representing x_σ of the form

$$b_\sigma = \left(\sum_{1 \le j \le d-2} \alpha_j W_j \right) - (\sum \alpha_j) W_{d-1}$$

with $\alpha_j \in \{0, \ldots, p-1\}$. (The existence and uniqueness follows from Proposition 6.2.)

Recall that $\mathfrak{S} = \sum n_i W_i$ and $\mathfrak{T}$ is a divisor of degree $(\deg f)/p$ supported on the W_i. We have the short exact sequence[16]

$$0 \to \frac{\langle \mathfrak{S} - p\mathfrak{T}\rangle}{p\mathfrak{W}^0} \to \frac{\mathfrak{W}^0}{p\mathfrak{W}^0} \to J[\phi] \to 0.$$

The map Υ is the composition of the map from $H^1(J[\phi])$ to $H^2(\langle \mathfrak{S} - p\mathfrak{T}\rangle/p\mathfrak{W}^0)$ with the isomorphism from $H^2(\langle \mathfrak{S} - p\mathfrak{T}\rangle/p\mathfrak{W}^0)$ to $H^2(\mu_p(k^{\mathrm{sep}}))$ induced by ϵ. We see that x maps to the class in $H^2(\langle \mathfrak{S} - p\mathfrak{T}\rangle/p\mathfrak{W}^0)$ of the 2-cocycle $f_1(\sigma,\tau) = {}^\sigma\mathfrak{b}_\tau + \mathfrak{b}_\sigma - \mathfrak{b}_{\sigma\tau} \bmod p\mathfrak{W}^0$. The divisor ${}^\sigma\mathfrak{b}_\tau + \mathfrak{b}_\sigma - \mathfrak{b}_{\sigma\tau}$ is a principal divisor supported on the W_i. Note that the supports of $\mathfrak{b}_{\sigma\tau}$ and $\mathfrak{b}_\sigma$ do not contain W_d. Let $\gamma = \mathrm{ord}_{W_d}{}^\sigma\mathfrak{b}_\tau$. Then the number of $\mathfrak{S}$'s appearing in ${}^\sigma\mathfrak{b}_\tau + \mathfrak{b}_\sigma - \mathfrak{b}_{\sigma\tau}$ is $\gamma \cdot (n_d^{-1} \bmod p)$; call this product n. We have

$${}^\sigma\mathfrak{b}_\tau + \mathfrak{b}_\sigma - \mathfrak{b}_{\sigma\tau} \equiv n(\mathfrak{S} - p\mathfrak{T}) \bmod p\mathfrak{W}^0.$$

Thus the image $\Upsilon(x)$ of f_1 under ϵ in $H^2(\mu_p(k^{\mathrm{sep}}))$ is represented by $f_1'(\sigma,\tau) := \zeta^n$.

The element $-\eta(\delta(\zeta), x)$ of $H^2(\mu_p(k^{\mathrm{sep}}))$ is represented by the 2-cocycle

$$f_2(\sigma,\tau) = e_\phi({}^\sigma W_d - W_d, {}^\sigma\mathfrak{b}_\tau)^{-1} = e_\phi(W_d - {}^\sigma W_d, {}^\sigma\mathfrak{b}_\tau).$$

Let D be a good divisor of degree 0 and j a function that is 1 mod $\mathfrak{m}$ with $\psi_* D = W_d - {}^\sigma W_d + \mathrm{div}(j)$. We have

$$f_2(\sigma,\tau) = e_\phi(\psi_* D, {}^\sigma\mathfrak{b}_\tau) = e_p(D, {}^\sigma\mathfrak{b}_\tau).$$

We see

$$(1-\zeta)_*\psi_* D = (1-\zeta)_*\mathrm{div}(j),$$

hence

$$pD - (1 + \ldots + \zeta^{p-1})_*(D) = \mathrm{div}\frac{j}{j \circ \zeta^{-1}}.$$

The function

$$h = \left(\frac{j}{j\circ\zeta^{-1}}\right) \cdot \prod_{P\in D}(x - x_P)$$

is 1 mod $\mathfrak{m}$, and $\mathrm{div}(h) = pD$. (In the product over $P \in D$, we take P's with multiplicity.) From (10), we obtain

$$e_p(D, {}^\sigma\mathfrak{b}_\tau) = \frac{\prod_{P\in{}^\sigma\mathfrak{b}_\tau}(x - x_P)(D)}{\frac{j}{j\circ\zeta^{-1}}({}^\sigma\mathfrak{b}_\tau)\prod_{P\in D}(x - x_P)({}^\sigma\mathfrak{b}_\tau)} = \frac{j\circ\zeta^{-1}}{j}({}^\sigma\mathfrak{b}_\tau).$$

The supports of ${}^\sigma\mathfrak{b}_\tau$ and $\mathrm{div} j$ can only have W_d in common. Since $\mathrm{ord}_{W_d}(j) = -1$, the function $\ell = j^{n_d}y$ has no zero or pole at W_d. We have

$$\left(\frac{j\circ\zeta^{-1}}{j}(W_d)\right)^{n_d} = \frac{\ell\circ\zeta^{-1}(W_d)}{\ell(W_d)} \cdot \frac{y}{y\circ\zeta^{-1}}(W_d) = \zeta$$

as in the proof of Proposition 7.1. Hence

$$\frac{j\circ\zeta^{-1}}{j}(W_d) = \zeta^{n_d^{-1} \bmod p}.$$

If $i < d$ then

$$\frac{j\circ\zeta^{-1}}{j}(W_i) = \frac{j(\zeta^{-1}W_i)}{j(W_i)} = 1.$$

[16] In what follows, one should interpret $\langle \mathfrak{S} - p\mathfrak{T}\rangle$ as the 1-dimensional $\mathbf{F}_p$-vector space generated by the *image* of $\mathfrak{S} - p\mathfrak{T}$ in $\mathfrak{W}^0/p\mathfrak{W}^0$.

Since $\operatorname{ord}_{W_d} {}^\sigma b_\tau = \gamma$ we have

$$\frac{j \circ \zeta^{-1}}{j}({}^\sigma b_\tau) = \zeta^{\gamma \cdot n_d^{-1} \bmod p} = \zeta^n.$$

Thus the 2-cocycles f_1' and f_2 are the same in $H^2(\mu_p(k^{\mathrm{sep}}))$. □

Let $\nu : H^1(J[\phi]) \to H^1(J(k^{\mathrm{sep}})) = H^1(\operatorname{Pic}^0(X^{\mathrm{sep}}))$ be the map coming from the inclusion $J[\phi] \to J(k^{\mathrm{sep}})$. We next show that the pairing η is compatible with the pairing ρ_0.

Lemma 10.4. *For all $x \in H^1(J[\phi])$ and $y \in H^0(\operatorname{Pic}^0(X^{sep})) = J(k)$,*

$$\eta(x, \iota(y)) = \rho_0(\nu(x), y).$$

Proof. By Lemma 10.2, it suffices to prove $\eta(\iota(y), x) + \rho(\nu(x), y) = 0$. For each $\sigma \in G_k$, choose $b_\sigma \in \operatorname{Div}^0(X^{\mathrm{sep}})$ such that the divisor classes of the b_σ define a cocycle representing x. Then for each $\sigma, \tau \in G_k$, pb_σ and ${}^\sigma b_\tau - b_{\sigma\tau} + b_\sigma$ are the divisors of functions h_τ and $f_{\sigma,\tau}$, respectively. By comparing divisors, we find

$$(f_{\sigma,\tau})^p = \frac{h_\sigma \cdot {}^\sigma h_\tau}{h_{\sigma\tau}}$$

up to a constant in $k^{\mathrm{sep}*}$, and by changing each $f_{\sigma,\tau}$ we may assume the constant is 1.

Choose $F \in \operatorname{Div}^0(X^{\mathrm{sep}})$ such that y is represented by pF. Using the compatibility of the e_ϕ and e_p, and the compatibility of the ϕ-descent map ι with the p-descent map as in (14), we find that $\eta(\iota(y), x)$ is represented by the 2-cocycle

$$\begin{aligned}(\sigma, \tau) &\mapsto e_p({}^\sigma F - F, {}^\sigma b_\tau) \\ &= \frac{({}^\sigma h_\tau)\,({}^\sigma F - F)}{g_\sigma\,({}^\sigma b_\tau)} \qquad \text{(by definition of } e_p\text{)},\end{aligned}$$

where g_σ is a function with divisor $p\,({}^\sigma F - F)$. On the other hand, using the definition of ρ_0 in [12], we see that $\rho_0(\nu(x), y)$ is represented by the 2-cocycle

$$\begin{aligned}(\sigma, \tau) &\mapsto f_{\sigma,\tau}(pF) g_\sigma({}^\sigma b_\tau) \\ &= \frac{h_\sigma(F) \cdot ({}^\sigma h_\tau)\,(F)}{h_{\sigma\tau}(F)} g_\sigma\,({}^\sigma b_\tau)\,,\end{aligned}$$

so $\eta(\iota(y), x) + \rho_0(\nu(x), y)$ is represented by the 2-cocycle

$$\begin{aligned}(\sigma, \tau) &\mapsto \frac{h_\sigma(F) \cdot ({}^\sigma h_\tau)\,(F)}{h_{\sigma\tau}(F)} \cdot \frac{({}^\sigma h_\tau)\,({}^\sigma F)}{({}^\sigma h_\tau)\,(F)} \\ &= \frac{h_\sigma(F) \cdot {}^\sigma(h_\tau(F))}{h_{\sigma\tau}(F)},\end{aligned}$$

which is clearly a coboundary. □

Remark. At the bottom of page 54 in [16], Milne mentions that a compatibility result similar to Lemma 10.4 holds for abelian varieties in general.

Recall the map θ and the element $\mathfrak{c} \in H^1(\operatorname{Pic}^0(X^{\mathrm{sep}}))$ from Section 3.

Corollary 10.5. *The map $\Upsilon \circ \iota : J(k) \to \operatorname{Br}(k)[p]$ coincides with the restriction of $-\theta$ to $J(k)$, and its kernel is* $\operatorname{Pic}^0(X)$.

Proof. By definition, $\mathfrak{c}$ is represented by the 1-cocycle $c_\sigma := {}^\sigma\mathcal{D} - \mathcal{D}$ with values in $\operatorname{Pic}^0(X^{\mathrm{sep}})$, where $\mathcal{D}$ is any divisor class of degree 1 over k^{sep}. In particular, if we choose $\mathcal{D}$ to be the divisor class of W_i, and use Lemma 9.1, we find that $\mathfrak{c} = \nu(\delta(\zeta))$. If $P \in J(k)$, then

$$\begin{aligned}\Upsilon(\iota(P)) &= \eta(\iota(P), \delta(\zeta)) \qquad \text{(by Proposition 10.3)}\\ &= -\eta(\delta(\zeta), \iota(P)) \qquad \text{(by Lemma 10.2)}\\ &= -\rho_0(\nu(\delta(\zeta)), P) \qquad \text{(by Lemma 10.4)}\\ &= -\rho_0(\mathfrak{c}, P) \qquad \text{(by the remarks above)}\\ &= -\theta(P) \qquad \text{(by (5))}.\end{aligned}$$

The kernel of $\theta : J(k) \to \operatorname{Br}(k)$ is $\operatorname{Pic}^0(X)$, by (2). □

Corollary 10.6. *The group* $\operatorname{Pic}^0(X)$ *is the largest subgroup of* $J(k)$ *whose image under*

$$\epsilon \circ \iota : J(k) \longrightarrow H^1\left(\frac{\mu_p(L^{sep})}{\mu_p(k^{sep})}\right)$$

is contained in the subgroup $L^*/L^{*p}k^*$.

Proof. A diagram chase in (12) shows that this largest subgroup is exactly the kernel of $\Upsilon \circ \iota$. Now apply Corollary 10.5. □

Remark. Suppose that $p = 2$, $k = \mathbf{R}$, and X is (a nonsingular projective model of) the curve $y^2 = -x^4 - 1$. Let ∞_1 and ∞_2 denote the points on X above $x = \infty$ on $\mathbf{P}^1$. One can check that the divisor $\infty_1 - \infty_2$ represents a real (i.e., $\mathbf{R}$-rational) divisor class that does not contain any real divisor, so its image under θ is the non-trivial element of $\operatorname{Br}(\mathbf{R})$. For this curve over $\mathbf{R}$, one cannot expect to extend $(x - T)$ to all of $J(\mathbf{R})$ in a natural way. (Thanks to David Grant for mentioning to us this example of a degree zero k-rational divisor class without k-rational divisors.)

11. The kernel of $(x - T)$

In the following two sections, we indicate how the cohomological description of the $(x-T)$ maps given in the last section can be used to derive some of their properties. Here we describe the kernels.

Proposition 11.1. *The kernel of the map*

$$(x - T) : \operatorname{Pic}^{(p)}_{\mathfrak{m}}(X) \longrightarrow L^*/L^{*p}$$

is generated by $\phi \operatorname{Pic}_{\mathfrak{m}}(X)$ *and* $\mathfrak{m}'$. *The kernel of the map*

$$(x - T) : \operatorname{Pic}^{(p)}(X) \longrightarrow L^*/L^{*p}k^*$$

is generated by $\operatorname{Pic}^{(p)}(X) \cap \phi H^0(\operatorname{Pic}(X^{sep}))$ *and the divisor class of* $\mathfrak{m}$.

Proof. By Theorem 9.3, the first kernel is the same as the kernel of $\epsilon \circ \iota'$. The kernel of ι' is $\phi \operatorname{Pic}_{\mathfrak{m}}(X)$ by construction, and the kernel of ϵ is generated by $\iota'(\mathfrak{m}')$, by Corollary 9.2. This proves the first statement, and the second is proved in exactly the same way, using Theorem 9.4. □

Let us now concentrate on a more concrete description of the size of the kernel for the $(x - T)$ map on $\operatorname{Pic}^0(X)$.

Lemma 11.2. *The horizontal map* $N : H^0\left(\frac{\mu_p(L^{sep})}{\mu_p(k^{sep})}\right) \longrightarrow \mu_p(k)$ *in (12) is surjective if and only if*

a) $f(x)$ *has a factor in* $k[x]$ *of degree prime to* p

or

b) $p = 2$, g *is even, and* $f(x)$ *factors over some quadratic extension* K *of* k *as* $ch(x)\bar{h}(x)$ *where* $c \in k^*$, $h(x) \in K[x]$ *and* $\bar{h}(x)$ *is the* $\mathrm{Gal}(K/k)$*-conjugate of* $h(x)$*.*

Proof. If $f(x)$ has a factor in $k[x]$ of degree prime to p, then it must have an irreducible factor $h(x)$ of degree prime to p. The element ℓ of

$$L^{\mathrm{sep}} = k^{\mathrm{sep}} \times k^{\mathrm{sep}} \times \cdots \times k^{\mathrm{sep}}$$

that is ζ in each component corresponding to a root of $h(x)$ and 1 in every other component is in $\mu_p(L)$, and the image of ℓ in $H^0\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$ maps under N to $N(\ell) = \zeta^{n_h \deg h(x)}$, where n_h is the multiplicity with which $h(x)$ appears in the factorization of $f(x)$. Since $1 \le n_h \le p-1$, $N(\ell)$ is a non-trivial element of $\mu_p(k)$. Thus $N : H^0\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \longrightarrow \mu_p(k)$ is surjective.

Next suppose $p = 2$, g is even, K is a quadratic extension of k, and $f(x) = ch(x)\bar{h}(x)$ where $c \in k^*$, $h(x) \in K[x]$ and $\bar{h}(x)$ is the $\mathrm{Gal}(K/k)$-conjugate of $h(x)$. Let $\ell \in L^{\mathrm{sep}}$ be the element which is 1 in components corresponding to roots of $h(x)$ and -1 in components corresponding to roots of $\bar{h}(x)$. Although $\ell \notin L$, automorphisms in G_k at worst send ℓ to $-\ell$, so ℓ does correspond to an element of $H^0\left(\frac{\mu_2(L^{\mathrm{sep}})}{\mu_2(k^{\mathrm{sep}})}\right)$. We have $N(\ell) = (-1)^{\deg \bar{h}(x)} = (-1)^{(\deg f)/2}$. Since $p = 2$, the roots of $f(x)$ are distinct, and $\deg f = d = 2g + 2$, so $N(\ell) = (-1)^{g+1} = -1$. Thus $N : H^0\left(\frac{\mu_2(L^{\mathrm{sep}})}{\mu_2(k^{\mathrm{sep}})}\right) \longrightarrow \mu_2(k)$ is surjective.

Conversely, suppose $N : H^0\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \longrightarrow \mu_p(k)$ is surjective. Pick $\ell \in L^{\mathrm{sep}}$ corresponding to an element in $H^0\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$ such that $N(\ell) = \zeta$. Let $h_j(x) = \prod (x - \alpha_i)^{n_i}$ where the product is over all i for which the corresponding component of ℓ is ζ^j. Then

$$\zeta = N(\ell) = \prod_{j=0}^{p-1} (\zeta^j)^{\deg h_j}, \tag{17}$$

so there is some j for which $\deg h_j$ is prime to p. If $h_j(x) \in k[x]$, we are done. Otherwise, the action of G_k multiplies ℓ by non-trivial elements of $\mu_p(k)$, so G_k acts transitively on the h_j. In particular, $\deg h_j$ is independent of j, and the right hand side of (17) equals

$$\zeta^{\left(\sum_{j=0}^{p-1} j\right)(\deg h_0)} = \zeta^{\frac{1}{2}p(p-1)(\deg h_0)}.$$

If $p \ge 3$ or p divides $\deg h_0$, then the exponent on the right is divisible by p, contradicting (17). Thus $p = 2$, $\deg h_0$ is odd, and $f(x) = ch_0(x)h_1(x)$, with $c \in k^*$ the leading coefficient of $f(x)$, and with G_k acting transitively on $\{h_0, h_1\}$. Finally, $\deg f = 2g + 2$ as before, so $\deg h_0 = g + 1$, making g even. □

Recall from Proposition 3.2 that the existence of a k-rational divisor class of degree 1 is enough to guarantee that $\mathrm{Pic}^0(X) \to J(k)$ is an isomorphism. The following generalizes Proposition 5 in [9], which is the special case where $p = 2$, $g = 2$, and $X(k)$ is non-empty.

Theorem 11.3. *If X has no k-rational divisor class of degree 1, then*

$$(x-T): \frac{\operatorname{Pic}^0(X)}{\operatorname{Pic}^0(X) \cap \phi H^0(\operatorname{Pic}^0(X^{sep}))} \longrightarrow L^*/L^{*p}k^* \tag{18}$$

is injective. If X does *have a k-rational divisor class $\mathcal{D}$ of degree 1, then the kernel of*

$$(x-T): J(k)/\phi J(k) \longrightarrow L^*/L^{*p}k^*$$

is generated by $\mathfrak{m} - \phi\mathcal{D}$. This kernel has order

1 if a) $f(x)$ has a factor in $k[x]$ of degree prime to p,
or b) $p = 2$, g is even, and $f(x)$ factors over some quadratic extension K of k as $ch(x)\bar{h}(x)$ where $c \in k^*$, $h(x) \in K[x]$ and $\bar{h}(x)$ is the $\operatorname{Gal}(K/k)$-conjugate of $h(x)$.
p otherwise.

Proof. If $\mathcal{E}_0 \in \operatorname{Pic}^0(X)$ is in the kernel of $(x-T)$, then by Proposition 11.1, $\mathcal{E}_0 = \phi\mathcal{E} - r\mathfrak{m}$ for some $\mathcal{E} \in H^0(\operatorname{Pic}(X^{\text{sep}}))$ and $r \in \mathbf{Z}$. Taking degrees of both sides shows $\deg \mathcal{E} = r$. If X has no k-rational divisor class of degree 1, then X has no k-rational divisor class of degree prime to p (because $\deg \mathfrak{m} = p$), so $r \in p\mathbf{Z}$. In this case, $\mathcal{E}_0 = \phi(\mathcal{E} - (r/p)\mathfrak{m})$, so we see that (18) is injective.

From now on we assume that there *is* a k-rational divisor class $\mathcal{D}$ of degree 1. Then $\mathfrak{m} - \phi\mathcal{D}$ is in the kernel by Proposition 11.1. Moreover, any element $\mathcal{E}_0 \in J(k)$ of the kernel is of the form $\phi\mathcal{E} - r\mathfrak{m}$ with $\mathcal{E} \in H^0(\operatorname{Pic}(X^{\text{sep}}))$ and $r = \deg \mathcal{E}$ as above. We can always rewrite $\mathcal{E}_0$ as $\phi(\mathcal{E} - r\mathcal{D}) - r(\mathfrak{m} - \phi\mathcal{D})$, so $\mathfrak{m} - \phi\mathcal{D}$ generates the kernel (modulo $\phi J(k)$).

The group $J(k)/\phi J(k)$ is killed by p, so the order of $\mathfrak{m} - \phi\mathcal{D}$ in it is either 1 or p. The order is 1 if and only if $\iota(\mathfrak{m} - \phi D)$ is trivial. We have

$$\iota(\mathfrak{m} - \phi D) = \iota(\mathfrak{m}) = \delta(\zeta),$$

by Lemma 9.1. By (12), $\delta(\zeta)$ vanishes if and only if the map $N : H^0\left(\frac{\mu_p(L^{\text{sep}})}{\mu_p(k^{\text{sep}})}\right) \longrightarrow \mu_p(k)$ is surjective. Hence we obtain the criterion of Lemma 11.2. □

12. The image of $(x-T)$

Although we cannot realistically hope to find an effective description of the image of $(x-T)$ in general (this would let one compute Mordell-Weil ranks in many situations), we can use the cohomological description to derive some restrictions on the image. Some of these restrictions were previously known for the case $p = 2$ (see [9]).

Proposition 12.1. *The image of*

$$(x-T): \operatorname{Pic}^0(X) \longrightarrow L^*/L^{*p}k^*$$

is contained in the kernel of the map $N : L^*/L^{*p}k^* \to k^*/k^{*p}$.

Proof. This follows from Theorem 9.4 and the exactness of the rows in (12). □

If A is an abelian variety over a local field k of residue characteristic not p, and if A has good reduction, then the image of the usual p-descent map $A(k)/pA(k) \to H^1(A[p])$ is contained in the subgroup of cohomology classes that are *unramified*, meaning that their restrictions to $H^1(I, A[p])$ are trivial, where I is the inertia group. This facilitates the computation of the Selmer group for abelian varieties over global fields.

To prove an analogue for the $(x-T)$ map, we need a notion of unramified for elements of L^*/L^{*p} and $L^*/L^{*p}k^*$. Let k be a local field with ring of integers $\mathcal{O}_k$. An element of L^*/L^{*p} is said to be unramified if its image under the Kummer isomorphism $L^*/L^{*p} \to H^1(\mu_p(L^{\mathrm{sep}}))$ is an unramified cohomology class. Similarly, an element of $L^*/L^{*p}k^*$ is said to be unramified if its image under the injection $L^*/L^{*p}k^* \hookrightarrow H^1\left(\mu_p(L^{\mathrm{sep}})/\mu_p(k^{\mathrm{sep}})\right)$ induced by the map q of (12) is unramified.

Proposition 12.2. *Let k be a local field of finite residue characteristic not p, and suppose J has good reduction. Then the image of*

$$(x-T) : \mathrm{Pic}^0(X) \longrightarrow L^*/L^{*p}k^*$$

is unramified.

Proof. This is a corollary of Theorem 9.4 and the well-known fact that the image of $\iota : J(k)/\phi J(k) \to H^1(J[\phi])$ is unramified. □

In the next proposition, we give a more computable criterion for checking whether elements are unramified. Let $L \cong \prod L_i$ be the decomposition of L into fields L_i. Let $\mathcal{O}_{L_i}$ be the ring of integers of L_i. If $\ell \in L$, we denote by $\ell_i \in L_i$ the image of ℓ in L_i.

Proposition 12.3. *Let k be a local field of residue characteristic not p. An element of L^*/L^{*p} represented by $\ell \in L^*$ is unramified if and only if the fractional $\mathcal{O}_{L_i}$-ideal (ℓ_i) is a p-th power for all i. An element of $L^*/L^{*p}k^*$ represented by $\ell \in L^*$ is unramified if and only if there exists a fractional $\mathcal{O}_k$-ideal $\mathfrak{a}$ such that the fractional $\mathcal{O}_{L_i}$-ideal $\mathfrak{a} \cdot (\ell_i)$ is a p-th power for all i.*

Remark. Since $\mathcal{O}_k$ has class number 1, we could have made the final statement of Proposition 12.3 with an *element* $a \in k$ instead of an ideal. We have chosen the given formulation so as to conform more closely with Proposition 12.5 below, in which case this substitution *cannot* be made in general.

Proof. Let k^{unr} denote the maximal unramified extension of k, let I denote the inertia group $\mathrm{Gal}(k^{\mathrm{sep}}/k^{\mathrm{unr}})$, and let $L^{\mathrm{unr}} = L \otimes_k k^{\mathrm{unr}}$. We have the following commutative square with horizontal isomorphisms:

$$\begin{tikzcd} L^*/L^{*p} \arrow[r] \arrow[d] & H^1(\mu_p(L^{\mathrm{sep}})) \arrow[d] \\ L^{\mathrm{unr}*}/L^{\mathrm{unr}*p} \arrow[r] & H^1(I, \mu_p(L^{\mathrm{sep}})). \end{tikzcd} \tag{19}$$

Therefore the element of L^*/L^{*p} represented by $\ell \in L^*$ is unramified if and only if ℓ becomes trivial in $L^{\mathrm{unr}*}/L^{\mathrm{unr}*p}$. The residue field of each component of L^{unr} is separably closed of characteristic not p, so by Hensel's Lemma, an element of $L^{\mathrm{unr}*}$ is in $L^{\mathrm{unr}*p}$ if and only if its valuation in each component is divisible by p. This proves the first part.

Similarly we have a commutative square with horizontal injections:

$$\begin{tikzcd} L^*/L^{*p}k^* \arrow[r] \arrow[d] & H^1\left(\dfrac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \arrow[d] \\ L^{\mathrm{unr}*}/L^{\mathrm{unr}*p}k^{\mathrm{unr}*} \arrow[r] & H^1\left(I, \dfrac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \end{tikzcd} \tag{20}$$

An element of $L^*/L^{*p}k^*$ represented by $\ell \in L^*$ is unramified if and only if ℓ becomes trivial in $L^{\mathrm{unr}*}/L^{\mathrm{unr}*p}k^{\mathrm{unr}*}$; i.e., if and only if there exists $a \in k^{\mathrm{unr}*}$ such that $a\ell$ is in $L^{\mathrm{unr}*p}$. By Hensel's Lemma again, $k^{\mathrm{unr}*}/k^{\mathrm{unr}*p}$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ via the discrete valuation, so we may modify a by an element of $k^{\mathrm{unr}*p}$ to assume without loss of generality that $a \in k^*$. Then by the earlier part of this proof, $a\ell$ is in $L^{\mathrm{unr}*p}$ if and only if the fractional ideal $(a)(\ell_i)$ in L_i is a p-th power for all i. This proves the second part. □

From now on, we let k be a global field of characteristic not p. For each nonarchimedean place v of k, let k_v denote the completion. Let $G_v = \mathrm{Gal}(k_v^{\mathrm{sep}}/k_v)$ and $I_v = \mathrm{Gal}(k_v^{\mathrm{sep}}/k_v^{\mathrm{unr}})$ be the decomposition group and inertia group, respectively. Let $L_v = L \otimes k_v$, and let $L_v^{\mathrm{sep}} = L \otimes k_v^{\mathrm{sep}}$. Also let $L_v^{\mathrm{unr}} = L \otimes k_v^{\mathrm{unr}}$, where k_v^{unr} is the maximal unramified extension of the local field k_v. If S is a set of places of k including all the archimedean places, an element of L^*/L^{*p} or $L^*/L^{*p}k^*$ is said to be unramified outside S if it is unramified at each $v \notin S$.[17] Let $(L^*/L^{*p})_S$ and $(L^*/L^{*p}k^*)_S$ denote the subgroups of elements unramified outside S of L^*/L^{*p} and $L^*/L^{*p}k^*$, respectively.

Proposition 12.4. *Let S be a set of places of k containing all places of bad reduction for J, all the archimedean places, and all places of k above p. Then the image of*

$$(x - T) : \mathrm{Pic}^0(X) \longrightarrow L^*/L^{*p}k^*$$

is contained in $(L^*/L^{*p}k^*)_S$.

Proof. This is a corollary of Proposition 12.2. □

Remark. If v is a nonarchimedean place such that the coefficients of $f(x)$ are integral at v, the leading coefficient is a v-adic unit, and v does not divide p or the discriminant of $f(x)$, then J will have good reduction at v. One can let S be the set of archimedean places together with the nonarchimedean places violating one of the conditions in the previous sentence.

If one wishes to use Proposition 12.4 in practice, one needs a more concrete description of $(L^*/L^{*p}k^*)_S$. We devote the rest of this section to finding such a description.

Proposition 12.5. *Let S be a set of places of k including all the archimedean places and all places above p. An element of L^*/L^{*p} represented by $\ell \in L^*$ is unramified outside S if and only if the prime-to-S part of the ideal (ℓ_i) of L_i is a p-th power for all i. An element of $L^*/L^{*p}k^*$ represented by $\ell \in L^*$ is unramified outside S if and only if there exists an ideal $\mathfrak{a}$ of k such that the prime-to-S part of the ideal $\mathfrak{a} \cdot (\ell_i)$ of L_i is a p-th power for all i.*

Proof. This is a corollary of Proposition 12.3. □

Let $\mathcal{O}_S$ denote the ring of S-integers of k. Let $\mathcal{O}_{L_i,S}$ denote the ring of elements of L_i that are integral at all places above all places of k outside S. Let $\mathcal{O}_{L,S} = \prod \mathcal{O}_{L_i,S} \subset L$. For any Dedekind domain R, let $\mathrm{Cl}(R)$ denote the class group of R. Define $\mathrm{Cl}(\mathcal{O}_{L,S}) = \prod \mathrm{Cl}(\mathcal{O}_{L_i,S})$.

[17] For L^*/L^{*p}, this definition agrees with the definition given in [9] for the case $p = 2$. In [9], however, an element of $L^*/L^{*p}k^*$ was called unramified outside S if and only if it was the image of some element of L^*/L^{*p} unramified outside S. This older definition agrees with ours in the case where the ring $\mathcal{O}_S$ of S-integers of k has class number prime to p, but is less stringent in general. The present definition is superior in two regards: first, it is local in nature, and second, Proposition 12.4 (the generalization of Proposition 3 in [9]) is true for it, regardless of the class number of $\mathcal{O}_S$.

Proposition 12.6. *If S is a nonempty set of places of k including all the archimedean places and all places above p, then there is an exact sequence*

$$0 \to \mathcal{O}_{L,S}^*/\mathcal{O}_{L,S}^{*p} \to (L^*/L^{*p})_S \to \operatorname{Cl}(\mathcal{O}_{L,S})[p] \to 0.$$

Proof. We write $w|v$ if w is a valuation on some L_i extending v on k. Then we have an exact sequence

$$0 \longrightarrow \mathcal{O}_{L,S}^* \longrightarrow L^* \xrightarrow{\prod w} \prod_{w|v, v\notin S} \mathbf{Z} \longrightarrow \operatorname{Cl}(\mathcal{O}_{L,S}) \longrightarrow 0$$

By Proposition 12.5, we have also an exact sequence

$$0 \longrightarrow (L^*/L^{*p})_S \longrightarrow L^*/L^{*p} \xrightarrow{\prod w} \prod_{w|v, v\notin S} \mathbf{Z}/p\mathbf{Z}.$$

By applying the snake lemma to the middle two rows of

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \mathcal{O}_{L,S}^* \arrow[r, "p"] \arrow[d] & \mathcal{O}_{L,S}^* \arrow[r] \arrow[d] & (L^*/L^{*p})_S \arrow[d] & \\
 & L^* \arrow[r, "p"] \arrow[d, "\prod w"] & L^* \arrow[r] \arrow[d, "\prod w"] & L^*/L^{*p} \arrow[r] \arrow[d, "\prod w"] & 0 \\
0 \arrow[r] & \prod_{w|v,v\notin S} \mathbf{Z} \arrow[r, "p"] \arrow[d] & \prod_{w|v,v\notin S} \mathbf{Z} \arrow[r] \arrow[d] & \prod_{w|v,v\notin S} \mathbf{Z}/p\mathbf{Z} \arrow[r] \arrow[d] & 0 \\
 & \operatorname{Cl}(\mathcal{O}_{L,S}) \arrow[r, "p"] \arrow[d] & \operatorname{Cl}(\mathcal{O}_{L,S}) \arrow[r] \arrow[d] & \dfrac{\operatorname{Cl}(\mathcal{O}_{L,S})}{p\operatorname{Cl}(\mathcal{O}_{L,S})} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{21}$$

we obtain the desired exact sequence. □

Recall that $\dim V$ denotes the $\mathbf{F}_p$-dimension of V. By a valuation on L, we mean the composition of a projection $L \to L_i$ and a valuation of the field L_i.

Corollary 12.7. *Let S be a nonempty set of places of k including all the archimedean places and all places above p, and let W denote the set of valuations w on L such that $w|v$ for some $v \in S$. Then* $\dim(L^*/L^{*p})_S = \#W + \dim \operatorname{Cl}(\mathcal{O}_{L,S})[p]$.

Proof. If W_i denotes the set of valuations w of L_i above some v in S, then the rank of $\mathcal{O}_{L_i,S}^*$ is $\#W_i - 1$, and $\dim \mathcal{O}_{L_i,S}^*/\mathcal{O}_{L_i,S}^{*p} = \#W_i$, since the torsion subgroup of $\mathcal{O}_{L_i,S}^*$ is cyclic of order divisible by p. Sum over i to get $\dim \mathcal{O}_{L,S}^*/\mathcal{O}_{L,S}^{*p} = \#W$, and use Proposition 12.6. □

In fact, Proposition 12.6 gives us an algorithm for computing $(L^*/L^{*p})_S$. (As usual, S is a nonempty set of places of k including all the archimedean places and all places above p.) Let ζ_i be a root of unity in L_i of maximal order, or at least of index prime to p in the group of all roots of unity in L_i. If L_i is a number field, let $\mathcal{O}_i$ denote the ring of integers in L_i. If L_i is a function field, let $\mathcal{O}_i$ denote the ring of elements that are integral away from some fixed place w_i above some place in S. Let B_i be a basis for the free part of the unit group $\mathcal{O}_i^*$ of L_i if L_i is a number field, and let $B_i = \{\}$ if L_i is a function field. Let $\mathfrak{p}_{i,1}, \mathfrak{p}_{i,2}, \dots, \mathfrak{p}_{i,r}$ denote the prime ideals of $\mathcal{O}_{L_i,S}$ corresponding to the places of L_i above the finite $v \in S$, excluding w_i if L_i is a function field. For $j = 1, 2, \dots, r$, inductively take the smallest power of $\mathfrak{p}_{i,j}$ that is in the subgroup of $\mathrm{Cl}(\mathcal{O}_i)$ generated by $\mathfrak{p}_{i,1}, \dots, \mathfrak{p}_{i,j-1}$, and let $\beta_{i,j}$ be the generator of the corresponding principal ideal $\mathfrak{p}_{i,1}^{r_1}\mathfrak{p}_{i,2}^{r_2}\cdots\mathfrak{p}_{i,j}^{r_j}$. Then $B_i \cup \{\zeta_i\} \cup \{\beta_{i,j} : 1 \le j \le r\}$ is a basis for $\mathcal{O}_{L_i,S}^*/\mathcal{O}_{L_i,S}^{*p}$. For each element $\bar{\mathfrak{a}}_j$ of $\mathrm{Cl}(\mathcal{O}_{L_i,S})[p]$, choose a representing ideal $\mathfrak{a}_j$, and let γ_j be a generator of $\mathfrak{a}_j^p$. Then $B_i \cup \{\zeta_i\} \cup \{\beta_{i,j} : 1 \le j \le s\} \cup \{\gamma_j\}_j$ is a basis for $(L_i^*/L_i^{*p})_S$, and taking the union over i yields a basis for $(L^*/L^{*p})_S$.

We next develop a down-to-earth description for $(L^*/L^{*p}k^*)_S$. Let $(k^*/k^{*p})_S$ be defined in the obvious way, either as the subgroup of k^*/k^{*p} mapping into elements of $H^1(\mu_p(k^{\mathrm{sep}}))$ unramified outside S, or as the subgroup represented by elements $\beta \in k^*$ such that the prime-to-S part of the ideal of β is a p-th power. (The proof of Proposition 12.5 shows that these definitions are equivalent.) In applying Proposition 12.8 below, note that the criterion of Néron-Ogg-Shafarevich implies that if v is a nonarchimedean place of k not above p, and v ramifies in some L_i, then v is automatically a place of bad reduction for J, because $k(J[\phi])$ is the splitting field of $f(x)$ over k.

Proposition 12.8. *If S is a nonempty set of places of k including all places that ramify in some L_i, all the archimedean places, and all places above p, then there is an exact sequence*

$$(k^*/k^{*p})_S \to (L^*/L^{*p})_S \to (L^*/L^{*p}k^*)_S \to \frac{\mathrm{Cl}(\mathcal{O}_S)}{p\,\mathrm{Cl}(\mathcal{O}_S)} \to \frac{\mathrm{Cl}(\mathcal{O}_{L,S})}{p\,\mathrm{Cl}(\mathcal{O}_{L,S})}.$$

Proof. The valuation v induces an isomorphism

$$k_v^{\mathrm{unr}*}/k_v^{\mathrm{unr}*p} \cong \mathbf{Z}/p\mathbf{Z}.$$

Similarly

$$L_v^{\mathrm{unr}*}/L_v^{\mathrm{unr}*p} \cong \prod_{w|v} \mathbf{Z}/p\mathbf{Z}.$$

The rightmost column of (21) is thus the same as

$$0 \to (L^*/L^{*p})_S \to L^*/L^{*p} \to \prod_{v \notin S} L_v^{\mathrm{unr}*}/L_v^{\mathrm{unr}*p} \to \frac{\mathrm{Cl}(\mathcal{O}_{L,S})}{p\,\mathrm{Cl}(\mathcal{O}_{L,S})} \to 0.$$

Similarly we obtain

$$0 \to (k^*/k^{*p})_S \to k^*/k^{*p} \to \prod_{v \notin S} k_v^{\mathrm{unr}*}/k_v^{\mathrm{unr}*p} \to \frac{\mathrm{Cl}(\mathcal{O}_S)}{p\,\mathrm{Cl}(\mathcal{O}_S)} \to 0.$$

Also the map

$$k_v^{\mathrm{unr}*}/k_v^{\mathrm{unr}*p} \to L_v^{\mathrm{unr}*}/L_v^{\mathrm{unr}*p}$$

is injective for each v that is unramified in all the L_i. (In fact, it would suffice to have v unramified in one of the L_i.) Thus we may apply the snake lemma to the middle two rows of

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & (k^*/k^{*p})_S \arrow[r] \arrow[d] & (L^*/L^{*p})_S \arrow[r] \arrow[d] & (L^*/L^{*p}k^*)_S \arrow[d] & \\
 & k^*/k^{*p} \arrow[r] \arrow[d] & L^*/L^{*p} \arrow[r] \arrow[d] & L^*/L^{*p}k^* \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod k_v^{\mathrm{unr}*}/k_v^{\mathrm{unr}*p} \arrow[r] \arrow[d] & \prod L_v^{\mathrm{unr}*}/L_v^{\mathrm{unr}*p} \arrow[r] \arrow[d] & \prod L_v^{\mathrm{unr}*}/L_v^{\mathrm{unr}*p}k_v^{\mathrm{unr}*} \arrow[r] & 0 \\
 & \dfrac{\mathrm{Cl}(\mathcal{O}_S)}{p\,\mathrm{Cl}(\mathcal{O}_S)} \arrow[r] \arrow[d] & \dfrac{\mathrm{Cl}(\mathcal{O}_{L,S})}{p\,\mathrm{Cl}(\mathcal{O}_{L,S})} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd} \tag{22}$$

to obtain the desired exact sequence. □

We can use Proposition 12.8 to outline an algorithm for computing a basis for $(L^*/L^{*p}k^*)_S$. Compute a basis for $(L^*/L^{*p})_S$ as in the paragraph after Corollary 12.7. Similarly find a basis for $(k^*/k^{*p})_S$, and express the images in $(L^*/L^{*p})_S$ of these basis elements in terms of the previous basis. Compute a basis $\mathcal{B} \subset (L^*/L^{*p}k^*)_S$ for the quotient of $(L^*/L^{*p})_S$ by the image of $(k^*/k^{*p})_S$. Find ideals $\mathfrak{a}$ that represent a basis for the kernel of $\frac{\mathrm{Cl}(\mathcal{O}_S)}{p\,\mathrm{Cl}(\mathcal{O}_S)} \to \frac{\mathrm{Cl}(\mathcal{O}_{L,S})}{p\,\mathrm{Cl}(\mathcal{O}_{L,S})}$. For each $\mathfrak{a}$ and i, choose an ideal $\mathfrak{a}_i$ of $\mathcal{O}_{L_i,S}$ such that $\mathfrak{a}\mathfrak{a}_i^p$ is a principal fractional ideal of $\mathcal{O}_{L_i,S}$. Let $c_i \in L_i$ be a generator of this principal ideal, and let $c = (c_i)$ be the corresponding element of L^*. Then $\mathcal{B}$ and the c's associated to the $\mathfrak{a}$'s form a basis for $(L^*/L^{*p}k^*)_S$.

We conclude this section with two lemmas that are useful when computing the local images of $(x - T)$. Lemma 12.9 holds for both local and global fields.

Lemma 12.9. *Let n denote the number of distinct irreducible factors of $f(x)$ over k. Suppose that at least one of these factors has degree prime to p. Then* $\dim J(k)[\phi] = n - 2$.

Proof. By Proposition 6.2, $\dim J(k)[\phi] = \dim V - 1$, where V is the subspace of $\mathfrak{W}^0/p\mathfrak{W}^0$ represented by divisors $D \in \mathfrak{W}^0$ on which G_k acts by addition of multiples of $\mathfrak{S}$ modulo $p\mathfrak{W}^0$. (It is one less, because $\mathfrak{S} - p\mathfrak{T}$ is trivial in $J(k)[\phi]$.)

Let $f_1(x)$ be an irreducible factor of $f(x)$ of degree prime to p. If $\sigma \in G_k$, then in the cycle decomposition of σ acting on the roots of $f_1(x)$ there is a cycle of length m prime to p. Then σ^m fixes at least one root of $f_1(x)$, so it is impossible for $\sigma^m(D) - D$ to be a nonzero multiple of $\mathfrak{S}$ modulo $p\mathfrak{W}^0$. Since m is prime to p, and $\mathfrak{S}$ is G_k-stable, it follows that $\sigma(D) - D$ cannot be a nonzero multiple of $\mathfrak{S}$ modulo $p\mathfrak{W}^0$. Thus V is the subspace of G_k-invariants of $\mathfrak{W}^0/p\mathfrak{W}^0$.

The space of G_k-invariants of $\mathfrak{W}/p\mathfrak{W}$ has dimension n, and there is a G_k-invariant of degree prime to p, corresponding to $f_1(x)$, so $\dim V = n - 1$, whence the result. □

If k_v is the completion of a number field k with respect to a place v, we let $|\ |_v$ denote the corresponding absolute value, normalized so that it literally extends the usual or ℓ-adic absolute value on $\mathbf{Q}$. The following generalizes Corollary 4.7 in [18].

Lemma 12.10. *Let v be a place of the number field k, lying above the place ℓ of $\mathbf{Q}$. Then*

$$\#J(k_v)/\phi J(k_v) = |p|_v^{-g[k_v:\mathbf{Q}_\ell]/(p-1)} \#J(k_v)[\phi].$$

Proof. Since $J(k_v)$ is a compact Lie group over $\mathbf{Q}_\ell$ of dimension $g[k_v : \mathbf{Q}_\ell]$, multiplication-by-p locally multiplies Haar measure by $|p|_v^{g[k_v:\mathbf{Q}_\ell]}$. Since p equals ϕ^{p-1} up to an automorphism, multiplication-by-ϕ locally multiplies Haar measure by $|p|_v^{g[k_v:\mathbf{Q}_\ell]/(p-1)}$. Thus the Haar measure of the image $\phi(J(k_v))$ is

$$\frac{|p|_v^{g[k_v:\mathbf{Q}_\ell]/(p-1)}}{\#J(k_v)[\phi]}$$

times the Haar measure of $J(k_v)$, and

$$\#J(k_v)/\phi J(k_v) = |p|_v^{-g[k_v:\mathbf{Q}_\ell]/(p-1)} \#J(k_v)[\phi].$$

□

13. The Selmer and Shafarevich-Tate groups

In this section, we assume k is a global field of characteristic not p containing the p-th roots of unity, and that X has a k_v-rational divisor class of degree 1 for each place v of k. By Propositions 3.2 and 3.3, the latter hypothesis implies that $\operatorname{Pic}^0(X) \to J(k)$ is an isomorphism, and similarly over every completion. Also recall from the final paragraph of Section 4 that this hypothesis is automatically satisfied if $g \not\equiv 1 \pmod{p}$. Then we have a commutative diagram

$$\begin{tikzcd} J(k)/\phi J(k) \arrow[r, "(x-T)"] \arrow[d] & L^*/L^{*p}k^* \arrow[d] \\ \prod_v J(k_v)/\phi J(k_v) \arrow[r, "(x-T)"] & \prod_v L_v^*/L_v^{*p}k_v^*. \end{tikzcd} \tag{23}$$

We define the fake ϕ-Selmer group $\operatorname{Sel}^\phi_{\text{fake}}(J,k)$ to be the subgroup of elements of $L^*/L^{*p}k^*$ that map down in $L_v^*/L_v^{*p}k_v^*$ into the image of the local $(x-T)$ map for all v. First let us prove an analogue of Proposition 12.1 and Proposition 12.4 for $\operatorname{Sel}^\phi_{\text{fake}}(J,k)$.

Proposition 13.1. *Let S be a nonempty set of places of k containing all places of bad reduction for J, all the archimedean places, and all places of k above p. Then the group $\operatorname{Sel}^\phi_{\textit{fake}}(J,k)$ is contained in the kernel of*

$$N : (L^*/L^{*p}k^*)_S \to k^*/k^{*p}.$$

Proof. First we show that if $\ell \in \operatorname{Sel}^\phi_{\text{fake}}(J,k)$, then $N(\ell) \in k^{*p}$. If not, then by the Chebotarev Density Theorem applied to the Kummer extension $k(N(\ell)^{1/p})/k$, we would find $N(\ell) \notin k_v^{*p}$ for some v. On the other hand, $\ell = (x-T)(\mathcal{D})$ for some $\mathcal{D} \in J(k_v)$, so this would contradict Proposition 12.1 over k_v.

The fact that $\operatorname{Sel}^\phi_{\text{fake}}(J,k)$ is unramified at $v \notin S$ follows from Proposition 12.2. □

Remark. Given that we have an algorithm for computing $(L^*/L^{*p}k^*)_S$, it is easy to see from Proposition 13.1 that $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ is effectively computable. To make this practical, all one needs is a good algorithm for finding a basis for $J(k_v)/\phi J(k_v)$ for $v \in S$.

Recall that the actual Selmer group $\mathrm{Sel}^{\phi}(J,k)$ is the subgroup of elements of $H^1(J[\phi])$ that map in $H^1(G_v, J[\phi])$ into the image of $J(k_v)/\phi J(k_v) \to H^1(G_v, J[\phi])$ for all v.

Theorem 13.2. *Suppose X has a k_v-rational divisor class of degree 1 for each place v of k. Then there is an exact sequence*

$$\mu_p(k) \xrightarrow{\delta} \mathrm{Sel}^{\phi}(J,k) \xrightarrow{\epsilon} \mathrm{Sel}^{\phi}_{\mathit{fake}}(J,k) \longrightarrow 0. \tag{24}$$

The image of $\mu_p(k)$ in $\mathrm{Sel}^{\phi}(J,k)$ is trivial if and only if $f(x)$ has a factor in $k[x]$ of degree prime to p, or $p=2$, g is even, and $f(x)$ factors over some quadratic extension K of k as $ch(x)\bar{h}(x)$ where $c \in k^*$, $h(x) \in K[x]$, and $\bar{h}(x)$ is the conjugate of $h(x)$ under $\mathrm{Gal}(K/k)$.

Remark. The condition for the triviality of the image of $\mu_p(k)$ is the same as the condition for the triviality of the kernel of $(x-T)$ in Theorem 11.3 when X has a k-rational divisor class of degree 1. But the map $\mathrm{Sel}^{\phi}(J,k) \to \mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ may have a non-trivial kernel even if the map

$$(x-T) : J(k)/\phi J(k) \to \mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$$

is injective. (This will happen if the image of ζ in $\mathrm{Sel}^{\phi}(J,k)$ maps to a non-trivial element of the Shafarevich-Tate group.)

Proof. From (12) we have an exact sequence

$$H^0\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \xrightarrow{N} \mu_p(k) \xrightarrow{\delta} H^1(J[\phi]) \xrightarrow{\epsilon} H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \longrightarrow k^*/k^{*p}. \tag{25}$$

Let $\mathcal{D}_v$ denote a k_v-rational divisor class of degree 1. Then by Lemma 9.1,

$$\delta(\zeta) = \iota(\mathfrak{m}) = \iota(\mathfrak{m} - \phi\mathcal{D}_v) \in \iota(J(k_v)),$$

where we abusively use ι to denote the map analogous to (13) for k_v. Thus $\delta(\mu_p(k)) \in \mathrm{Sel}^{\phi}(J,k)$. The condition for its triviality follows from Lemma 11.2 and the exactness of (25).

Next let us show that if $\xi \in \mathrm{Sel}^{\phi}(J,k)$ then $\epsilon(\xi)$ is in $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$. (To make sense of this, we identify $L^*/L^{*p}k^*$ with a subgroup of $H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$ using the vertical map q in (12).) Since $\xi \in H^1(J[\phi])$ comes locally from a point in $J(k_v)/\phi J(k_v)$, it maps to zero in $\mathrm{Br}(k_v)[p]$ by Corollary 9.5. Since $\mathrm{Br}(k) \to \prod_v \mathrm{Br}(k_v)$ is injective, ξ maps to zero in $\mathrm{Br}(k)[p]$. By a diagram chase in (12), $\epsilon(\xi) \in H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$ comes from a (unique) element $\ell \in L^*/L^{*p}k^*$. Since ξ is in the image of the local ι map on $J(k_v)/\phi J(k_v)$, ℓ will be in the image of the local $(x-T)$ map, by Theorem 9.4. Thus $\ell \in \mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$.

The exactness of (24) in the middle follows from the exactness of (25) at the term $H^1(J[\phi])$. Finally let us show that $\mathrm{Sel}^{\phi}(J,k) \to \mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ is surjective. By Proposition 13.1, $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ is contained in the kernel of

$$N : L^*/L^{*p}k^* \subset H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right) \to k^*/k^{*p}$$

so by (25) any element in $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ comes from some $\xi \in H^1(J[\phi])$. For each v, its restriction $\xi_v \in H^1(G_v, J[\phi])$ maps under ϵ to $\epsilon(\iota(P_v)) \in H^1\left(\frac{\mu_p(L^{\mathrm{sep}})}{\mu_p(k^{\mathrm{sep}})}\right)$ for some $P_v \in J(k_v)/\phi J(k_v)$, by definition of $\mathrm{Sel}^\phi_{\mathrm{fake}}(J,k)$. Hence $\xi_v - \iota(P_v) \in \ker \epsilon$, and by the exactness of the local version of (25), we have $\xi_v - \iota(P_v) \in \delta(\mu_p(k_v))$. But $\delta(\mu_p(k_v)) \subseteq \iota(J(k_v)/\phi J(k_v))$ by the first part of this proof, so $\xi_v \in \iota(J(k_v)/\phi J(k_v))$ as well. This holds for all v, so $\xi \in \mathrm{Sel}^\phi(J,k)$. □

Let $Ш(J,k)$ denote the Shafarevich-Tate group of J over k. Recall that there is an exact sequence

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

By Lemma 9.1, $\iota(\mathfrak{m}) = \delta(\zeta) \in H^1(J[\phi])$, so $\iota(\mathfrak{m}) \in \mathrm{Sel}^\phi(J,k)$ by Theorem 13.2. By Lemma 9.1, the image of $\iota(\mathfrak{m})$ in $Ш(J,k)[\phi]$ equals the cohomology class of $\beta_\sigma = {}^\sigma W - W$ in $H^1(J(k^{\mathrm{sep}}))$, where W is any point in $X(k^{\mathrm{sep}})$. Hence this image also equals the element $\mathfrak{c} \in H^1(J(k^{\mathrm{sep}}))$, which is the homogeneous space $\mathrm{Pic}^1(X^{\mathrm{sep}})$ of J, defined in Section 3. The element $\mathfrak{c}$ is trivial if and only if X has a k-rational divisor of degree 1. Define $(Ш(J,k)[\phi])_{\mathrm{fake}} = Ш(J,k)[\phi]/\langle \mathfrak{c} \rangle$.[18]

Theorem 13.3. *Suppose X has a k_v-rational divisor class of degree 1 for each place v of k. Then we have an exact sequence*

$$J(k)/\phi J(k) \xrightarrow{(x-T)} \mathrm{Sel}^\phi_{\mathit{fake}}(J,k) \longrightarrow (Ш(J,k)[\phi])_{\mathit{fake}} \longrightarrow 0.$$

Proof. Take the cokernels of the vertical maps in

$$\begin{tikzcd}
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \mu_p(k) \arrow[r] \arrow[d] & \mu_p(k) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J(k)/\phi J(k) \arrow[r] & \mathrm{Sel}^\phi(J,k) \arrow[r] & Ш(J,k)[\phi] \arrow[r] & 0.
\end{tikzcd}$$

(The rightmost vertical map sends ζ to $\mathfrak{c}$.) □

Remarks. The kernel of $(x-T)$ is completely described by Theorem 11.3. It is tempting also to let $J(k)/\ker(x-T)$ be denoted by $(J(k)/\phi J(k))_{\mathrm{fake}}$!

Finally let us mention that if we are interested in computing the Mordell-Weil rank of one of our Jacobians over a global field k not necessarily containing a primitive p-th root of unity, a reasonable strategy is first to find the Mordell-Weil rank over $k(\zeta)$, and then to apply the following lemma, which was suggested to us independently by A. Brumer, M. Stoll, and the referee.

Lemma 13.4. *Let k be a global field of characteristic not p, not necessarily containing a primitive p-th root of unity $\zeta \in k^{sep}$. Let $f(x)$ be a p-th power-free polynomial with zeros in k^{sep}, and let J be the Jacobian of $y^p = f(x)$, as usual. Then*

$$\mathrm{rank}\, J(k) = \frac{\mathrm{rank}\, J(k(\zeta))}{[k(\zeta):k]}.$$

Proof. Let ζ_p be a primitive p-th root of unity in $\overline{\mathbf{Q}}$. Identify $\mathrm{Gal}(k(\zeta)/k)$ in the natural way with a subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$, and let K be the subfield of $\mathbf{Q}(\zeta_p)$ fixed by the corresponding subgroup G of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Because of the automorphism $(x,y) \mapsto (x,\zeta y)$ of the curve $y^p = f(x)$ over $k(\zeta)$, the group $V := J(k(\zeta)) \otimes \mathbf{Q}$ has a natural $\mathbf{Q}(\zeta_p)$-vector space structure. Moreover, $\mathrm{Gal}(k(\zeta)/k)$ acts on the group V, and we may reinterpret this action as an action

[18] We could have written $Ш_{\mathrm{fake}}(J,k)[\phi]$ instead, but this would have been very abusive of notation since there is no natural $Ш_{\mathrm{fake}}(J,k)$ of which it is the ϕ-torsion subgroup!

of G. This latter action respects the $\mathbf{Q}(\zeta_p)$-vector space structure in the following sense: if $\sigma \in G$ and $v \in V$, then $\sigma(\zeta_p v) = \sigma(\zeta_p)\sigma(v)$.

If we fix a $\mathbf{Q}(\zeta_p)$-basis for V, the action of G defines a 1-cocycle with values in $GL_r(\mathbf{Q}(\zeta_p))$, where $r = \dim_{\mathbf{Q}(\zeta_p)} V$. But $H^1(G, GL_r(\mathbf{Q}(\zeta_p))) = 0$ (see [20, Proposition 3, p. 151]), and it follows that some other choice of basis would have been G-stable; in other words, if V^G denotes the K-vector space of vectors in V fixed by G, then the $K[G]$-modules V and $V^G \otimes_K \mathbf{Q}(\zeta_p)$ are isomorphic. Hence

$$\operatorname{rank} J(k(\zeta)) = \dim_{\mathbf{Q}} V = [\mathbf{Q}(\zeta_p) : K] \cdot \dim_{\mathbf{Q}} \left(V^G\right) = [k(\zeta) : k] \cdot \operatorname{rank} J(k).$$

□

14. Example

In this section we will demonstrate the practicality of our methods by proving the following theorem.

Theorem 14.1. *Let J denote the Jacobian of the genus 8 curve*

$$X : y^3 = (x^2 - x + 6)^2(x^8 + 3x + 3)$$

over $\mathbf{Q}$. Then $J(\mathbf{Q})$ has rank 2 and $J(\mathbf{Q}(\sqrt{-3}))$ has rank 4.

All computations will be done using GP-PARI, except when explicitly stated otherwise. Before beginning the computation, let us make a few remarks about our choice of curve. Let $k = \mathbf{Q}(\zeta)$ where ζ is a primitive p-th root of unity; we will soon choose $p = 3$. To make the computation challenging, we wanted our curve to have the following properties:

(1) The curve X should not be hyperelliptic.
(2) None of the ramification points should be k-rational.
(3) The polynomial $f(x)$ should have a multiple factor.[19]
(4) One of the factors should define a field extension of k having class number divisible by p.
(5) One of the factors should have large Galois group over k.
(6) The endomorphism ring of the Jacobian J should be no larger than $\mathbf{Z}[\zeta]$.[20]

In hope of satisfying (1), we chose $p = 3$, so that $k = \mathbf{Q}(\sqrt{-3})$. To satisfy (2), we needed to make $\deg f$ divisible by 3, and to choose $f(x)$ with no linear factors over k. To satisfy (4), we chose one of the factors of $f(x)$ to be $x^2 - x + 6$, a root of which generates $\mathbf{Q}(\sqrt{-23})$ over $\mathbf{Q}$, the first quadratic imaginary number field of class number 3. The field $k(\sqrt{-23})$ has class number 3 also. To satisfy (3), we chose to make $x^2 - x + 6$ a repeated factor. To satisfy (5), we chose to have only one other irreducible factor, with the full symmetric group as Galois group over k. Thus we chose to set

$$f(x) = (x^2 - x + 6)^2 h(x)$$

where $\deg h(x)$ would be constrained to be 2 modulo 3. The computation would eventually require calculating the class group and fundamental units in the number field obtained by

[19] Although handling the multiple factor requires more thought, since for instance N is not simply the norm, the computation time is actually reduced because of it, since the degree of the largest number field we need to work in is less than it would have been otherwise.

[20] The reason for this restriction is that an exceptionally large endomorphism ring can in some cases simplify the computation of the Mordell-Weil group. We want to rule out such "cheats."

Prime ℓ	Characteristic polynomial
2	$X^{16}+X^{14}+X^{12}+X^{10}-20X^8+4X^6+16X^4+64X^2+256$
5	$X^{16}+14X^{14}+132X^{12}+963X^{10}+5340X^8+24075X^6+82500X^4+218750X^2+390625$
7	$X^{16}+6X^{15}+19X^{14}+84X^{13}+307X^{12}+792X^{11}+2497X^{10}+7074X^9+16759X^8+49518X^7+122353X^6+271656X^5+737107X^4+1411788X^3+2235331X^2+4941258X+5764801$

TABLE 1. The characteristic polynomials of Frobenius for J_ℓ over $\mathbf{F}_\ell$.

adjoining a root of h to k; in order that this not take an inordinate amount of time, we chose to have $\deg h = 8$, so that the large number field would have absolute degree 16.

We chose to set $h(x) = x^8 + ax + b$ for positive integers a and b. We chose a and b so that X would have bad reduction at at most three finite primes of $\mathbf{Q}$ other than 3.[21] The pair (a, b) of positive integers satisfying this condition with $a + b$ minimal was $(3, 3)$. Hence we took

$$f(x) = (x^2 - x + 6)^2(x^8 + 3x + 3).$$

The factorization of the discriminant of $f_0(x) = (x^2 - x + 6)(x^8 + 3x + 3)$ is $-3^9 \cdot 23 \cdot 553411^2 \cdot 14306587$. Let $S_0 = \{3, 23, 553411, 14306587\}$. Then X has bad reduction at most at the primes in S_0. (We did not have to add 3 to the list, since it already appeared in the discriminant. Without further work, however, we cannot say whether 3 actually is a prime of bad reduction.)

Proposition 14.2. *The curve X is not hyperelliptic.*

Proof. Let X' denote the image of the canonical map $X \to \mathbf{P}^{g-1}$. Let K and K' denote the function fields over k of X and X', respectively. We have $[K : K'] = 2$ if X is hyperelliptic, and $[K : K'] = 1$ otherwise. One can check that the differentials dx/y and $x\,dx/y$ on X are regular, so we have $k(x) \subseteq K' \subseteq K$. But $[K : k(x)] = 3$, so $[K : K']$ cannot be 2. □

Proposition 14.3. *The Galois group of $x^8 + 3x + 3$ over $k = \mathbf{Q}(\sqrt{-3})$ is the full symmetric group S_8.*

Proof. The program `galp` by M. Olivier and Y. Eichenlaub (available by anonymous ftp at `megrez.math.u-bordeaux.fr`) shows that the Galois group of $x^8 + 3x + 3$ over $\mathbf{Q}$ is S_8. Hence the Galois group of $x^8 + 3x + 3$ over k has order at least $8!/2$. But the only subgroup of S_8 of index 2 is A_8, and the Galois group cannot be A_8, because the discriminant of $x^8 + 3x + 3$ is $3^7 \cdot 14306587$, which is not a square in k. □

Table 1 gives the characteristic polynomial of Frobenius for the reduction J_ℓ of J modulo the first three primes ℓ of $\mathbf{Q}$ outside S_0. These were computed by exhausting over x-coordinates to count points on X over $\mathbf{F}_{\ell^i}$ for $1 \le i \le 8$.

Proposition 14.4. *The Jacobian J is absolutely simple, and* $\operatorname{End} J = \mathbf{Z}[\zeta]$.

Proof. We first use the recipe described in [23] to compute the decomposition of J_5 and J_7 into simple factors up to isogeny over $\overline{\mathbf{F}}_5$ and $\overline{\mathbf{F}}_7$, respectively.

[21] Having more primes of bad reduction would have made the computation more tedious, but without otherwise affecting the difficulty much.

From Table 1, we compute that the characteristic polynomial of J_5 over $\mathbf{F}_{25}$ is

$$P_{25}(X) = \left(X^8 + 14X^7 + 132X^6 + 963X^5 + 5340X^4 + 24075X^3 \\ +82500X^2 + 218750X + 390625\right)^2 .$$

The octic polynomial is irreducible, and the number field K_1 generated by a root π has one nontrivial subfield, according to the program `KASH`: the totally real quartic subfield F_1 fixed by the automorphism σ of K_1 sending π to $25/\pi$. If some power of π did not generate K_1 over $\mathbf{Q}$, it would be in the subfield F_1, and ${}^{\sigma}\pi/\pi$ would be a root of unity in K_1. The only roots of unity in K_1 are 1 and -1, and $({}^{\sigma}\pi/\pi)^2 \neq 1$, so $K_1 = \mathbf{Q}(\pi^n)$ for any $n \geq 1$. The simple abelian variety A over $\mathbf{F}_{25}$ corresponding to the Weil number π is hence absolutely simple, and its endomorphism algebra is an order in a division algebra E with center K_1. The invariant of E at a place v of K_1 equals $(f_v \operatorname{ord}_v \pi)/2 \bmod 1$ if v divides 5, and 0 otherwise, where f_v denotes the residue field degree of v, and ord_v is the $\mathbf{Z}$-valued discrete valuation at v. We compute that f_v or $\operatorname{ord}_v \pi$ is even at each v, so E is trivial in the Brauer group, A is 4-dimensional with $(\operatorname{End} A) \otimes \mathbf{Q} = K_1$, and J_5 is isogenous over $\mathbf{F}_{25}$ to $A \times A$.

The characteristic polynomial P_7 of J_7 over $\mathbf{F}_7$ factors over $\mathbf{Q}$ as

$$(X^2 + 5X + 7) \cdot (X^6 - 6X^5 + 24X^4 - 67X^3 + 168X^2 - 294X + 343) \\ \cdot (X^8 + 7X^7 + 25X^6 + 91X^5 + 295X^4 + 637X^3 + 1225X^2 + 2401X + 2401),$$

so J_7 is isogenous to $E_1 \times B \times C$ over $\mathbf{F}_7$, where E_1 is an elliptic curve with $j = 0$, and B and C are $\mathbf{F}_7$-simple abelian varieties of dimensions 3 and 4, respectively. To check that B is absolutely simple, we must show that powers of a root ρ of the sextic factor of P_7 generate the field $K_2 := \mathbf{Q}(\rho)$. The nontrivial subfields of K_2 are $\mathbf{Q}(\sqrt{-3})$ and the cubic field F_2 fixed by the automorphism $\rho \mapsto 7/\rho$. That no power of ρ lies in F_2 can be checked as above for π and F_1. Since ρ divides 7, if $\rho^n \in \mathbf{Q}(\sqrt{-3})$ for some $n \geq 1$, the vector of valuations of ρ at the primes of K_2 above 7 would have to be a $\mathbf{Q}$-linear combination of the corresponding vectors for $2 + \sqrt{-3}$ and $2 - \sqrt{-3}$ in K_2. We compute that this is not the case. Thus $\mathbf{Q}(\rho^n) = K_2$ for all $n \geq 1$, and B is absolutely simple. Similarly we prove that C is absolutely simple.

If J split up to isogeny over $\overline{\mathbf{Q}}$ at all, it would split as $D_1 \times D_2$, where each D_i was 4-dimensional, because of the splitting of J_5. If D_1 and D_2 were not isogenous, then the automorphism ζ of J would have to act on each independently, and then ζ would also act on the mod 5 reductions, which would both be A. This contradicts the fact that $\mathbf{Q}(\zeta)$ is not a subfield of K_1. Thus J would have to be isogenous to a square, but this is inconsistent with the splitting of J_7. Hence J is absolutely irreducible. Moreover, $\operatorname{End} J$ contains $\mathbf{Z}[\zeta]$ and maps into the endomorphism ring of E, so $\operatorname{End} J$ must equal $\mathbf{Z}[\zeta]$. □

Proposition 14.5. *The torsion subgroup $J(k)_{tors}$ is trivial.*

Proof. The prime-to-2 part of $J(k)_{\text{tors}}$ injects under reduction modulo 2 into $J(\mathbf{F}_4)$, and $\#J(\mathbf{F}_4) = 2^4 \cdot 3^8$, which we obtain using Table 1. The prime-to-7 part[22] of $J(k)_{\text{tors}}$ injects under reduction modulo $2+\sqrt{-3}$ into $J(\mathbf{F}_7)$, and $\#J(\mathbf{F}_7) = 3^2 \cdot 13^3 \cdot 787$, again obtained using Table 1. Hence it remains to show that there is no 3-power torsion. Since multiplication-by-3 on J equals ϕ^2 up to an automorphism, if there were a 3-torsion point in $J(k)$, there would also be a ϕ-torsion point. But $\dim J(k)[\phi] = 0$, by Lemma 12.9. □

[22] In fact the whole group $J(k)_{\text{tors}}$ injects into $J(\mathbf{F}_7)$, since the absolute ramification index of $2 + \sqrt{-3}$ is less than $7 - 1$.

Prime	(e,f)'s in L_1	(e,f)'s in L_2
3	$(2,1),(2,1)$	$(8,1),(8,1)$
23	$(2,2)$	$(1,2),(1,2),(1,2),(1,10)$
553411	$(1,1),(1,1),(1,1),(1,1)$	$(1,1),(1,1),(1,1),(1,1),(1,6),(1,6)$
14306587	$(1,1),(1,1),(1,1),(1,1)$	$(1,1),(1,1),(1,1),(1,1),(2,1),(2,1),(1,4),(1,4)$

TABLE 2. The splitting of primes in S_0 in L_1 and L_2.

The curve X has three points above $\infty \in \mathbf{P}^1$, and they can be distinguished by the value of the rational function y/x^4, which will be 1, ζ, or ζ^2. We name them ∞_1, ∞_2, and ∞_3, respectively. Only ∞_1 is defined over $\mathbf{Q}$; the other two are defined over k.

The only prime in S_0 that remains inert in k is 23. The others factor as follows: $3 = -p_3^2$, where $p_3 = \sqrt{-3}$; $553411 = p_{553411}\bar{p}_{553411}$, where $p_{553411} = -644 + 215\sqrt{-3}$ and $\bar{p}_{553411}$ is its conjugate; and $14306587 = p_{14306587}\bar{p}_{14306587}$, where $p_{14306587} = (-7475 - 671\sqrt{-3})/2$ and $\bar{p}_{14306587}$ is its conjugate. Let S be the set of primes of k above primes in S_0, together with the infinite place ∞. Thus we have $\#S = 7$, and Corollary 12.7 implies $\dim(k^*/k^{*3})_S = 7$, and we can easily find a basis using the algorithm given after that corollary.

Let $L_1 = k[T]/(T^2 - T + 6)$ and $L_2 = k[T]/(T^8 + 3T + 3)$ and $L = k[T]/f_0(T) = L_1 \times L_2$. Applying the PARI functions `compositum` and `initalgred` we find that L_1 is generated over $\mathbf{Q}$ by a root of

$$h_1(x) = x^4 - 4x^3 + 19x^2 - 30x + 39$$

and that L_2 is generated over $\mathbf{Q}$ by a root of

$$h_2(x) = x^{16} - 8x^{14} + 28x^{12} - 56x^{10} + 70x^8 - 56x^6 + 28x^4 - 5x^2 + 1.$$

The element $T \in L$ is represented by $(-1/10)x^3 + (3/10)x^2 - (21/10)x + 12/5$ in $\mathbf{Q}[x]/h_1(x)$ and $x^2 - 1$ in $\mathbf{Q}[x]/h_2(x)$.

Both L_1 and L_2 contain $\mathbf{Q}(\sqrt{-3})$, so they are totally complex, and their groups of units have ranks 1 and 7, respectively. The class groups have size 3 and 1, respectively; a prime $\mathfrak{p}_3$ of L_1 above 3 generates the class group of L_1. In particular, $\mathrm{Cl}(\mathcal{O}_{L,S})$ is trivial.

The ramification indices e and residue degrees f of the primes of L_1 and L_2 above the primes in S_0 are listed in Table 2. By Corollary 12.7, it follows that $\dim(L^*/L^{*3})_S = 41$. We find a basis for $(L^*/L^{*3})_S$ by using the algorithm given after that corollary, with help from the PARI function `isprincipalgen`, which can find generators of all the necessary ideals. We can compute the image of the basis of $(k^*/k^{*3})_S$ in $(L^*/L^{*3})_S$ (with respect to its basis), using the PARI functions `nfval` and `isunit`. Similarly we can compute the image of N on the basis of $(L^*/L^{*3})_S$, expressed in terms of the basis of $(k^*/k^{*3})_S$.

We find that the map $(k^*/k^{*3})_S \to (L^*/L^{*3})_S$ induced by the inclusion map is injective. Also, $\mathrm{Cl}(k)$ is trivial, so $\mathrm{Cl}(\mathcal{O}_S)$ is trivial. Hence by Proposition 12.8, $\dim(L^*/L^{*3}k^*)_S = 34$. The map $N : (L^*/L^{*3})_S \to (k^*/k^{*3})_S$, on the other hand, turns out to be surjective, so

$$\dim\ker\Big((L^*/L^{*3}k^*)_S \xrightarrow{N} (k^*/k^{*3})_S\Big) = 27,$$

and again we can compute representatives for a basis.

Table 2 also lets us compute the factorizations of $f(x)$ over each relevant completion k_v of k, and also the $\mathbf{F}_3$-dimensions of the groups $J(k_v)[\phi]$ and $J(k_v)/\phi J(k_v)$ for each place v of k. These are listed in Table 3. To obtain the k_v-factorizations from the information in Table 2, we need only note that $k/\mathbf{Q}$ is Galois, and that the primes 3, 23, 553411, and 14306587 of $\mathbf{Q}$

Place v	k_v-factorization of $f(x)$	$\dim J(k_v)[\phi]$	$\dim J(k_v)/\phi J(k_v)$
p_3	$1^2 \cdot 1^2 \cdot 4 \cdot 4$	2	10
23	$2^2 \cdot 1 \cdot 1 \cdot 1 \cdot 5$	3	3
p_{553411}	$1^2 \cdot 1^2 \cdot 1 \cdot 1 \cdot 6$	3	3
$\bar{p}_{553411}$	$1^2 \cdot 1^2 \cdot 1 \cdot 1 \cdot 6$	3	3
$p_{14306587}$	$1^2 \cdot 1^2 \cdot 1 \cdot 1 \cdot 2 \cdot 4$	4	4
$\bar{p}_{14306587}$	$1^2 \cdot 1^2 \cdot 1 \cdot 1 \cdot 2 \cdot 4$	4	4
∞	$1^2 \cdot 1^2 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$	8	0

Table 3. The degrees and multiplicities of the factors of $f(x)$ over k_v, and the $\mathbf{F}_3$-dimensions of $J(k_v)[\phi]$ and $J(k_v)/\phi J(k_v)$.

ℓ	$\dim \frac{(k \otimes \mathbf{Q}_\ell)^*}{(k \otimes \mathbf{Q}_\ell)^{*3}}$	$\dim \frac{(L_1 \otimes \mathbf{Q}_\ell)^*}{(L_1 \otimes \mathbf{Q}_\ell)^{*3}}$	$\dim \frac{(L_2 \otimes \mathbf{Q}_\ell)^*}{(L_2 \otimes \mathbf{Q}_\ell)^{*3}}$	$\dim \frac{(L \otimes \mathbf{Q}_\ell)^*}{(L \otimes \mathbf{Q}_\ell)^{*3}(k \otimes \mathbf{Q}_\ell)^*}$
3	4	8	20	24
23	2	2	8	8
553411	4	8	12	16
14306587	4	8	16	20

Table 4. Dimensions of cokernels of $z \mapsto z^3$ in some local multiplicative groups.

ramify, remain inert, split, and split in k, respectively. Lemmas 12.9 and 12.10 let us verify the remaining columns of Table 3.

To do computations in $L_v^*/L_v^{*3}k_v^*$, we work within L_v^*/L_v^{*3} and compute the image of a basis of k_v^*/k_v^{*3} in it. We group together v above the same prime $\ell \in S_0$; for example, we work within the group $(L \otimes \mathbf{Q}_{553411})^*/(L \otimes \mathbf{Q}_{553411})^{*3}$. Since $L = L_1 \times L_2$, we can work with each factor independently. To solve the "discrete logarithm problem" in $(L_2 \otimes \mathbf{Q}_{553411})^*/(L_2 \otimes \mathbf{Q}_{553411})^{*3}$, for example, given an element of L_2, we divide by powers of chosen generators of the ideals above 553411 to make it a unit (keeping track of the valuations modulo 3), and then use the PARI command `zideallog` applied to $(\mathcal{O}_{L_2}/(553411))^*$ to compute the discrete logarithm of the 553411-adic unit modulo 3. (For $\ell = 3$, we work in $(\mathcal{O}_{L_2}/(9))^*$, since a 3-adic unit that is 1 modulo 9 is a 3-adic cube.)

The dimensions of some of these groups are listed in Table 4. Note that for each ℓ,

$$\frac{(k \otimes \mathbf{Q}_\ell)^*}{(k \otimes \mathbf{Q}_\ell)^{*3}} \longrightarrow \frac{(L \otimes \mathbf{Q}_\ell)^*}{(L \otimes \mathbf{Q}_\ell)^{*3}}$$

turned out to be injective.

Since X has a $\mathbf{Q}$-rational point at infinity, and since $f(x)$ has a factor of degree prime to $p = 3$ even over $\mathbf{Q}$, Theorem 11.3 tells us that

$$J(k)/\phi J(k) \xrightarrow{(x-T)} L^*/L^{*3}k^*$$

is injective, and the corresponding maps over each completion of k are injective also.

The only part of the calculation that would be difficult to automate completely is the search for the generators of $J(k_v)/\phi J(k_v)$ for the bad places $v \in S$. Although we know the dimension *a priori*, and in theory could simply search the space of k_v-rational divisors systematically, to higher and higher v-adic precision until the right number of generators

ℓ	Basis for $\dfrac{J(k \otimes \mathbf{Q}_\ell)}{\phi J(k \otimes \mathbf{Q}_\ell)}$	Dimension
3	$3, 8, 9, 40, x^2+2x+5, x^2-2x+5, x^2-3x+4,$ $x^2+\frac{1}{2}(-9+\sqrt{-3})x+(-3-\sqrt{-3}), x^2+\frac{1}{2}(-9-\sqrt{-3})x+(-3+\sqrt{-3}),$ $x^4+(27+20\sqrt{-3})x^3+(48+14\sqrt{-3})x^2+(24+22\sqrt{-3})x+(15+14\sqrt{-3})$	10
23	$\frac{1}{2}(3+\sqrt{-3}), \frac{1}{2}(13+\sqrt{-3}), \frac{1}{2}(19+\sqrt{-3})$	3
553411	$3, 10, \frac{1}{2}(-29+\sqrt{-3}), \frac{1}{2}(-7+\sqrt{-3}), 665952, 665952+(2+\sqrt{-3})p_{553411}^2$	6
14306587	$0, 1, 6, 11, \frac{1}{2}(-11+\sqrt{-3}), \frac{1}{2}(27+\sqrt{-3}), \frac{1}{2}(31+\sqrt{-3}), \frac{1}{2}(41+\sqrt{-3})$	8

TABLE 5. Generators of $J(k \otimes \mathbf{Q}_\ell)/\phi J(k \otimes \mathbf{Q}_\ell)$ for $\ell \in S_0$.

was found, the time required for this could be prohibitive, especially in certain cases when v lies above a large prime of $\mathbf{Q}$ (such as 553411). If some of the required generators reduce to points on a non-identity component of the special fiber of the Néron model, they may be scrunched up in a tiny p-adic neighborhood of a point with singular reduction in our original model. In this case, we are better off looking at points in such a neighborhood, which is what we did to find some of the generators at 3 and at 553411. (For instance, note that the number 665952 in Table 5 is a common root modulo 553411 of $x^2 - x + 6$ and $x^8 + 3x + 3$.)

We list generators for $J(k \otimes \mathbf{Q}_\ell)/\phi J(k \otimes \mathbf{Q}_\ell)$ in Table 5, coded as follows: an element α of k represents the class of the divisor $P - \infty_1$, where $P \in X(k \otimes \mathbf{Q}_\ell)$ has x-coordinate α; a polynomial $h(x) \in k[x]$ represents the class of the divisor $D - (\deg D)\infty_1$, where D is a G_k-stable sum of $X(\overline{k} \otimes \mathbf{Q}_\ell)$ points whose x-coordinates are the roots of $h(x)$ in $\overline{k}$. To verify that these generate, we simply check for each ℓ that their images under $(x - T)$ generate an $\mathbf{F}_3$-vector space of the correct dimension inside $\dfrac{(L \otimes \mathbf{Q}_\ell)^*}{(L \otimes \mathbf{Q}_\ell)^{*3}(k \otimes \mathbf{Q}_\ell)^*}$.

For each $\ell \in S_0$, we compute the image of these generators and the image of the basis elements for $L^*/L^{*3}k^*$ in $\dfrac{(L \otimes \mathbf{Q}_\ell)^*}{(L \otimes \mathbf{Q}_\ell)^{*3}(k \otimes \mathbf{Q}_\ell)^*}$. It is then a matter of linear algebra over $\mathbf{F}_3$ to find $\mathrm{Sel}^\phi_{\text{fake}}(J, k)$, as a subgroup of $(L^*/L^{*3}k^*)_S$. It turns out that $\dim \mathrm{Sel}^\phi_{\text{fake}}(J, k) = 2$. By Theorem 13.2, we have an isomorphism

$$\mathrm{Sel}^\phi(J, k) \xrightarrow{\epsilon} \mathrm{Sel}^\phi_{\text{fake}}(J, k),$$

so $\dim \mathrm{Sel}^\phi(J, k) = 2$ also.

At this point, we hope to find elements in $J(k)$ whose images under $(x - T)$ generate $\mathrm{Sel}^\phi_{\text{fake}}(J, k)$. Define divisors

$$D_1 = (-1, 4) - \infty_1,$$
$$D_2 = \left(\frac{1+\sqrt{-23}}{2}, 0\right) + \left(\frac{1-\sqrt{-23}}{2}, 0\right) - 2\infty_1.$$

By Proposition 5.1, $(x - T)(D_1) = -1 - T$. We cannot compute $(x - T)(D_2)$ immediately from the definition and Proposition 5.1, since D_2 involves points with $y = 0$. Instead note that

$$\mathrm{div}(y - (x^2 - x + 6)) = 2D_2 + D_3 - (\text{a divisor supported at infinity}),$$

where D_3 is a k-rational sum of eight points whose x-coordinates are the roots of the octic polynomial

$$\frac{f(x)-(x^2-x+6)^3}{(x^2-x+6)^2} = x^8 - x^2 + 4x - 3,$$

which is relatively prime to $f(x)$. Hence, by Proposition 5.1,

$$(x-T)(D_2) = (x-T)(D_3) = (-1)^8(T^8 - T^2 + 4T - 3)$$

modulo cubes in L^*.

We check that $(x-T)(D_1)$ and $(x-T)(D_2)$ are in $\mathrm{Sel}^{\phi}_{\text{fake}}(J,k)$, as they should be. In fact, it turns out that they are independent, and hence form a basis for $\mathrm{Sel}^{\phi}_{\text{fake}}(J,k)$. From Theorem 13.3, it follows that $(Ш(J,k)[\phi])_{\text{fake}}$ and $Ш(J,k)[\phi]$ are trivial, and that $J(k)/\phi J(k)$ is 2-dimensional over $\mathbf{F}_3$, with the images of D_1 and D_2 being a basis.

By Proposition 14.5, $J(k)[\phi]$ is trivial, so $J(k)\otimes_{\mathbf{Z}}\mathbf{Q} = J(k)\otimes_{\mathbf{Z}[\zeta]} k$ is a 2-dimensional k-vector space with the images of D_1 and D_2 as a basis. In particular, $J(k)$ has rank 4 (over $\mathbf{Z}$). By Lemma 13.4, $J(\mathbf{Q})$ has rank 2, and indeed the divisor classes of D_1 and D_2 are independent points of infinite order. This completes the proof of Theorem 14.1.

Remark. The fact that the ranks over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-3})$ are 2 and 4, respectively, are not surprising once one realizes that X has rational points above $x=-1$ and $x=\infty$ on $\mathbf{P}^1$, and that $f(x)$ factors over $\mathbf{Q}$.

Corollary 14.6. *We have* $\#X(\mathbf{Q}) \le 12$ *and* $\#X(\mathbf{Q}(\sqrt{-3})) \le 36$.

Proof. Coleman's effective version [8] of Chabauty's argument proves that if X is a curve of genus g over a number field k with Mordell-Weil rank at most $g-1$, if $\mathfrak{p}$ is an unramified prime of k at which X has good reduction, and if the residue characteristic of $\mathfrak{p}$ is greater than $2g$, then

$$\#X(k) \le \#X(\mathbf{F}_{\mathfrak{p}}) + 2g - 2.$$

We take $k = \mathbf{Q}(\sqrt{-3})$ and $\mathfrak{p} = 4+\sqrt{-3}$. We find $\#X(\mathbf{F}_{19}) = 22$, so $\#X(\mathbf{Q}(\sqrt{-3})) \le 36$. To obtain the bound for $\#X(\mathbf{Q})$, note that each rational point on X gives rise to three $\mathbf{Q}(\sqrt{-3})$-rational points on X, by taking the orbit under the automorphism ζ. □

The truth is probably that the numbers of rational points over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-3})$ are much smaller; the upper bounds could probably be reduced substantially with further analysis.

We conclude this section with a few words on the computing time required for this example. The computations were done on a Sun SPARCstation-20. By far the most expensive part was the certification of the class group and units for the degree 16 number field L_2: it took PARI ten minutes of CPU time to compute these assuming GRH, but then 47 hours to check that the results were correct independent of GRH. The rest of the descent computations were done in well under an hour, and the time for them could probably have been reduced to a few minutes if we had taken care to optimize our code. The only other expensive part was the computation of the characteristic polynomial of J over $\mathbf{F}_7$ by naïvely enumerating points on X over $\mathbf{F}_{7^i}$ for $i = 1,\dots,8$. This took 44 hours, but it is worth mentioning that this computation was not needed in the descent; we used it only in order to demonstrate that the endomorphism ring was no larger than expected, and to completely determine the torsion subgroup of $J(k)$. Also, we probably could have reduced this time somewhat by writing a special-purpose program in C, say, instead of using the high-level language of GP-PARI.

15. Concluding remarks

It would be interesting to know what Mordell-Weil rank we can expect to find on average. More precisely, fix a number field k and a positive integer g, let S_h denote the set of k-isomorphism classes of g-dimensional abelian varieties over k having Faltings height at most h, and define the "average Mordell-Weil rank" as

$$f(k,g) := \lim_{h\to\infty} \frac{\sum_{A\in S_h} \operatorname{rank} A(k)}{\# S_h},$$

assuming that the limit exists. There are then many (well-known) questions one could ask:

Question 1. Can one determine $f(k,g)$ for any k and g (or even prove that it exists)?

Assuming standard conjectures, the sign of the functional equation of the L-series forces half the abelian varieties to have rank at least 1, so we can expect $f(k,g) \geq 1/2$ for every k and g. Brumer [3] proved under standard conjectures that $f(\mathbf{Q},1) \leq 2.3$, and he and Heath-Brown have improved this to $f(\mathbf{Q},1) \leq 2$.[23] Computer experiments seem to suggest that $f(\mathbf{Q},1) > 1/2$, but the evidence is not yet strong enough to say this with conviction. (See [5].) As for *unconditional* results, virtually nothing is known for number fields: even the possibilities $f(\mathbf{Q},1) = 0$ and $f(\mathbf{Q},1) = \infty$ have not been ruled out yet. On the other hand, Brumer and Heath-Brown's upper bounds mentioned above are proved unconditionally over the function field $\mathbf{F}_q(t)$.

Question 2. For fixed k, how does $f(k,g)$ grow as a function of g? For example, is it bounded, or is it perhaps $O(g)$ as $g \to \infty$?

If it were $o(g)$ as $g \to \infty$, this would be good news for the method of Chabauty and Coleman [8].

Question 3. For fixed g, is $f(k,g)$ independent of the number field k? If not, is it at least uniformly bounded as a function of k?

The answers may be entirely different if one restricts attention to Jacobians. There is good reason to expect different behavior for our cyclic covers when $p \geq 3$, since the endomorphism ring of the Jacobian is then larger than $\mathbf{Z}$. See also [4] for some results on the rank of $J_0(N)$ and for further musings on ranks.

One can ask similar questions about the Selmer groups and Shafarevich-Tate groups. Cassels [6], Bölling [2], and Kramer [11] have shown that the Shafarevich-Tate group can be arbitrarily large in certain families of elliptic curves over number fields. Wong [24] has given an asymptotic formula for the average rank of the 2-Selmer group in a family of twists of an elliptic curve with full rational 2-torsion over any number field with odd class number.

Of course, we cannot base any conjectures on our one example, but at least we have laid down some of the groundwork for more extensive numerical investigations.

Acknowledgements

We thank David Grant for the example at the end of Section 10. We thank also Michael Stoll for comments on an early draft of the paper. He obtained some of our results independently for the case $p = 2$, $\deg f = 6$, and he has begun implementing the algorithm in

[23] In these results, the elliptic curves are ordered by "naïve height" instead of by Faltings height, but this is a minor difference. Also, it is not shown that $f(k,1)$ actually exists: it is really a $\limsup$ that is bounded.

our paper for that case [21]. We thank Armand Brumer and Siman Wong for some interesting discussions regarding the concluding remarks. Finally we thank the referee for several worthwhile suggestions.

References

[1] Atiyah, M. F. and Wall, C. T. C., Cohomology of groups, Chapter IV in: J. W. S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967.

[2] Bölling, R., Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gross werden, *Math. Nachr.* **67** (1975), 157–179.

[3] Brumer, A., The average rank of elliptic curves I, *Invent. Math.* **109** (1992), no. 3, 445–472.

[4] Brumer, A., The rank of $J_0(N)$, Columbia University Number Theory Seminar (New York, 1992), *Astérisque* No. 228 (1995), 3, 41–68.

[5] Brumer, A. and McGuinness, O., The behavior of the Mordell-Weil group of elliptic curves, *Bull. Amer. Math. Soc. (N.S.)* **23** (1990), no. 2, 375–382.

[6] Cassels, J. W. S., Arithmetic on curves of genus 1. VI. The Tate-Šafarevič group can be arbitrarily large, *J. Reine Angew. Math.* **214/215** (1964), 65–70.

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

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

[9] Flynn, E. V., Poonen, B., and Schaefer, E., Cycles of quadratic polynomials and rational points on a genus 2 curve, to appear in *Duke Math. J.*

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

[11] Kramer, K., A family of semistable elliptic curves with large Tate-Shafarevitch groups, *Proc. Amer. Math. Soc.* **89** (1983), no. 3, 379–386.

[12] Lichtenbaum, S., Duality theorems for curves over p-adic fields, *Invent. Math.* **7** (1969), 120–136.

[13] McCallum, W., On the method of Coleman and Chabauty, *Math. Ann.* **299** (1994), 565–596.

[14] Milne, J. S., Abelian Varieties, in: Cornell, G., Silverman, J.H.(eds.), *Arithmetic geometry*, 103–150, Springer-Verlag, New York, 1986.

[15] Milne, J. S., Jacobian Varieties, in: Cornell, G., Silverman, J.H.(eds.), *Arithmetic geometry*, 167–212, Springer-Verlag, New York, 1986.

[16] Milne, J. S., *Arithmetic Duality Theorems*, Academic Press, Orlando, Fl., 1986.

[17] Schaefer, E. F., 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995) 219–232.

[18] Schaefer, E. F., Computing a Selmer group of a Jacobian using functions on the curve, to appear in *Math. Ann.*

[19] Serre, J.-P., *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1988.

[20] Serre, J.-P., *Local Fields*, Springer-Verlag, New York, 1979.

[21] Stoll, M., Implementing 2-descent in genus 2, in preparation.

[22] Towse, C., Weierstrass points on cyclic covers of the projective line, *Trans. Amer. Math. Soc.* **348** (1996), no. 8, 3355–3378.

[23] Waterhouse, W., Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* (4) **2** (1969), 521–560.

[24] Wong, S., On the Selmer groups of elliptic curves in quadratic twist families, Ph. D. thesis, M. I. T., 1995.

Department of Mathematics, Princeton University, Princeton, NJ 08544-1000, USA
E-mail address: `poonen@math.princeton.edu`

Santa Clara University, Santa Clara, CA 95053, USA
E-mail address: `eschaefer@scuacc.scu.edu`