

GENERALIZED JACOBIANS AND EXPLICIT DESCENTS

BRENDAN CREUTZ

ABSTRACT. We develop a cohomological description of explicit descents in terms of generalized Jacobians, generalizing the known description for hyperelliptic curves. Specifically, given an integer n dividing the degree of some reduced, effective and base point free divisor \mathfrak{m} on a curve C , we show that multiplication by n on the generalized Jacobian $J_{\mathfrak{m}}$ factors through an isogeny $\varphi : A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ whose kernel is dual to the Galois module of divisor classes D such that nD is linearly equivalent to some multiple of \mathfrak{m} . By geometric class field theory, this corresponds to an abelian covering of $C_{\bar{k}} := C \times_{\text{Spec } k} \text{Spec }(\bar{k})$ of exponent n unramified outside \mathfrak{m} . We show that the n -coverings of C parameterized by explicit descents are the maximal unramified subcoverings of the k -forms of this ramified covering. We present applications to the computation of Mordell-Weil ranks of nonhyperelliptic curves.

1. INTRODUCTION

Suppose $f(x, y)$ is a binary form of degree d over a field k of characteristic not equal to 2. Pencils of quadrics with discriminant form $f(x, y)$ have been studied in [BSD63, Cas62, Cre01, BG13, Wan18, BGW15, BGW17]. When d is even, the $\text{SL}_d(k)/\mu_2$ -orbits of pairs (A, B) with discriminant form $f(x, y)$ correspond to a collection of 2-coverings of the hyperelliptic curve $C : z^2 = f(x, y)$. When $k = \mathbb{Q}$ these coverings are used in [Bha] and [BGW17] to compute the average size of the 2-Selmer set of C , and of the torsor J^1 parameterizing divisor classes of degree 1, respectively, from which they deduce the fantastic result that most hyperelliptic curves over \mathbb{Q} have no rational points.

The same collection of coverings can also be described in terms of the k -algebra $L := k[x]/f(x, 1)$. This description was used in [BS09] and [Cre13] to compute 2-Selmer sets of C and J^1 , respectively, for individual hyperelliptic curves. A key step in both [Cre13] and [BGW17] is to check that this collection of coverings is large enough to contain the locally soluble 2-coverings (under suitable hypotheses on C). In [BGW17] this is achieved by identifying these coverings as the unramified subcoverings of k -forms of the maximal abelian covering of exponent 2 unramified outside the pair of points at infinity on the affine model $z^2 = f(x, y)$, a characterization that is quite natural in light of the use of generalized Jacobians in [PS97].

Meanwhile the theory of explicit descents has expanded to incorporate computable descriptions of certain approximations to Selmer sets, called fake Selmer sets, for all curves. This is developed for nonhyperelliptic curves of genus at least 2 in [BPS16] and for curves of genus 1 in [Cre14]. In this paper we provide geometric and cohomological descriptions of these descents in terms of generalized Jacobians, generalizing the description for hyperelliptic curves given in [PS97, BGW17]. Specifically, given an integer n dividing the degree of some reduced effective and base point free divisor \mathfrak{m} on a curve C , we show that multiplication by n on the generalized Jacobian $J_{\mathfrak{m}}$ factors through an isogeny of semiabelian varieties $\varphi : A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ whose kernel is naturally the dual of the Galois module of classes of

divisors D on $C_{\bar{k}} := C \times_{\text{Spec } k} \text{Spec}(\bar{k})$ such that nD is linearly equivalent to a multiple of \mathfrak{m} . By geometric class field theory, this corresponds to an abelian covering of exponent n and conductor \mathfrak{m} . We show that the fake descents mentioned above have a natural interpretation in terms of the k -forms of this ramified covering, which we call φ -coverings. The main result in this direction is Theorem 4.4, from which we deduce Corollaries 4.6 and 4.7 giving an interpretation of the descents on C and J^1 in terms of those n -coverings which arise as maximal unramified subcoverings of the k -forms of this ramified covering.

This description unifies the methods of explicit descent described in [MSS96, BS09, Cre13, Cre14, BPS16] and allows a more natural interpretation of some of the objects that arise. Moreover, it yields a number of applications to explicit descent and the arithmetic of curves described in the following subsections.

1.0.1. *Applications to explicit descent on J .* The fake descent presented in [BPS16] proceeds by substituting the connecting homomorphism $d : J(k) \rightarrow H^1(k, J[n])$ in the Kummer sequence with a more computationally amenable homomorphism $f : \text{Pic}^0(C) \rightarrow L^\times/k^\times L^{\times n}$, for some étale k -algebra L . Here $\text{Pic}(C)$ denotes the group of k -rational divisors on C modulo linear equivalence and $\text{Pic}^0(C)$ denotes the subgroup of classes of degree 0. In order to obtain information about the Selmer group from this, they require some hypothesis (e.g., [BPS16, Hypothesis 10.1]) to ensure that $\text{Pic}^0(C) = J(k)$ globally and locally. In general one has an injective map $\text{Pic}^0(C) \rightarrow \text{Pic}^0(\bar{C})^{\text{Gal } k} = J(k)$ which need not be surjective. We show how such hypotheses can be omitted in a number of relevant cases (cf. Theorem 5.6). In Theorem 6.3 we use this to determine the Mordell-Weil rank of a Jacobian J of a plane quartic curve C for which $\text{Pic}^0(C) \neq J(k)$.

1.0.2. *Application to explicit descent on C and J^1 .* In [BPS16] a ‘fake Selmer set’ of a non-hyperelliptic curve C over a global field is introduced. Using the machinery of [BPS16] we introduce a fake Selmer set of the torsor J^1 parameterizing divisor classes of degree 1 (see Definition 5.1). It is easy to see that C and J^1 cannot have any rational points if the corresponding fake Selmer set is empty. Our interpretation in terms of generalized Jacobians allows us to verify that the obstruction coming from these fake descents is indeed a finite abelian descent obstruction in the sense of [Sko01, Section 5.3] and, consequently, that such counterexamples to the Hasse principle are explained by the Brauer-Manin obstruction (cf. [Sko01, Theorem 6.1.2]). This is given in Theorem 5.2 and 5.3 below.

Particularly in the case of J^1 , this allows us to obtain deeper knowledge than would otherwise be obtained from simply knowing that $J^1(k)$ is empty. Indeed, we are able to tap into results in arithmetic duality which would otherwise only be possible conditionally on deep conjectures concerning finiteness of the Tate-Shafarevich group $\text{III}(J)$. In Section 6.1 we give an example of a nonhyperelliptic genus 3 curve over \mathbb{Q} with absolutely simple Jacobian J for which the fake 2-Selmer set of J^1 is empty. Theorem 5.3 is then used to prove that $\text{III}(J)[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and consequently to determine that the Mordell-Weil rank is 1. Without making use of Theorem 5.3 we would only obtain the weaker conclusion that $1 \leq \text{rank}(J(\mathbb{Q})) \leq 2$ and $1 \leq \dim_{\mathbb{F}_2} \text{III}(J)[2] \leq 2$.

1.0.3. *Applications to descent on genus 1 curves.* The results of [Cre14] describe n -descents on genus 1 curves of degree n when n is prime. The results just mentioned extend aspects of this to general n . Namely, for such a curve we have a computable fake Selmer set whose emptiness implies that the curve is not divisible by n in the Tate-Shafarevich group of its

Jacobian. This is potentially practical in the case $n = 4$, enabling 16-descent on elliptic curves.

1.0.4. *Application to Galois descent of unramified abelian coverings of exponent 2.* The results of this paper are used in [Cre16] to prove that if C is an everywhere locally solvable curve of genus $g \geq 2$ over a global field of characteristic different from 2 and that the Galois action on $J[2]$ is generic (i.e., $\text{Gal}(k(J[2])/k)$ is isomorphic to S_{2g+2} or $\text{GSp}_{2g}(\mathbb{F}_2)$ correspondingly as C is or is not hyperelliptic), then the maximal unramified abelian covering of $C_{\bar{k}}$ of exponent 2 descends to k .

The obstruction to Galois descent for the φ -covering mentioned above and its maximal unramified subcovering are elements of the Galois cohomology groups $H^2(k, A_m[\varphi])$ and $H^2(k, J[2])$, respectively. The proof proceeds by showing that, generically, the locally trivial subgroup $\text{III}^2(k, A_m[\varphi])$ is trivial, which implies that the ramified covering and, hence also, its unramified subcovering descend to k . The use of φ -coverings here seems unavoidable (and the result all the more surprising) given that the group $\text{III}^2(k, J[2])$ can be nontrivial even when the Galois action on $J[2]$ is generic. In fact, this occurs whenever C has no rational theta characteristics and all of the decomposition groups of $\text{Gal}(k(J[2])/k)$ are cyclic, since in this case the torsor parameterizing theta characteristics gives a nontrivial element of $\text{III}^1(k, J[2])$ (see [Ati71] and [PR11, Remark 3.18]) and $\text{III}^2(k, J[2]) \simeq \text{III}^1(k, J[2])$ by Tate's duality theorem. Moreover, there are examples of locally solvable curves of genus ≥ 2 for which the maximal unramified abelian covering of exponent 2 does not descend to k (see [CV15, Theorem 6.7]).

1.0.5. *Potential application to average sizes of Selmer sets.* We expect our interpretation may also be of relevance to future efforts to compute these Selmer sets *on average*. Namely, it should be possible to identify the collection $\text{Cov}_m^n(J^1)$ with the orbits in some coregular representation (as is done in [BGW17] for the hyperelliptic case). The results in Theorems 3.8 and 7.1 would then have implications for the structure of the space of orbits. Thorne has recently made progress understanding the situation for nonhyperelliptic genus 3 curves with a marked rational point [Tho15, Tho]. It is our hope that the results of this paper may shed light on the corresponding situation when there are no rational points.

1.1. **Notation.** Throughout this paper n is an integer and k is a field of characteristic not divisible by n , with separable closure \bar{k} and absolute Galois group $\text{Gal}_k = \text{Gal}(\bar{k}/k)$. We will use C to denote a *nice curve* over k , i.e. a smooth, projective and geometrically integral k -variety of dimension 1. For a nonempty finite étale k -scheme $\Delta = \text{Spec}(L)$ we use $\text{Res}_\Delta = \text{Res}_{L/k}$ to denote the restriction of scalars functor taking L -schemes to k -schemes. For a commutative étale k -group scheme G , we use $H^i(G)$ to denote the Galois cohomology group $H^i(\text{Gal}_k, G(\bar{k}))$. For k a global field, equivalence classes of absolute values on k (whether archimedean or not) will be referred to as primes.

Acknowledgements. I would like to thank: Michael Stoll and Bjorn Poonen for comments and discussions concerning the material in this article and Nils Bruin for providing me with Magma code for a number of the algorithms described in [BPS16]. In developing the algorithms and examples in Section 6 I have made use of a list quartic curves of small discriminant provided by Denis Simon as well as the database [Sut18] developed by Andrew

Sutherland. Computations were performed using the Magma Computer Algebra System described in [BCP97].

2. THE MODULUS SETUP

Definition 2.1. *Let C be a nice curve over k . A **modulus setup** for C is a pair (n, \mathfrak{m}) consisting of a positive integer n not divisible by the characteristic of k , and a reduced, effective and base point free divisor $\mathfrak{m} \in \text{Div}(C)$ of degree m , with n dividing m .*

Given a modulus setup (n, \mathfrak{m}) we define $\ell := \deg(\mathfrak{m})/n$. We are primarily interested in the following examples.

- M.1** Suppose $\pi : C \rightarrow \mathbb{P}^1$ is a double cover which is not ramified over $\infty \in \mathbb{P}^1$. Let $n = 2$ and $\mathfrak{m} = \pi^*\infty$.
- M.2** Suppose C is a genus 1 curve of degree m in \mathbb{P}^{m-1} . Take \mathfrak{m} to be any reduced hyperplane section and take $n = m$.
- M.3** Suppose C is any nice nonhyperelliptic curve of genus at least 3, $n = 2$ and \mathfrak{m} is a canonical divisor. Then $m = 2g - 2$ and $\ell = g - 1$.

2.1. The generalized Jacobian associated to a modulus setup. Let C be a nice curve over k with a modulus setup (n, \mathfrak{m}) . We may view \mathfrak{m} as a finite étale subscheme $\mathfrak{m} = \text{Spec } M \subset C$, or as a **modulus** in the sense of geometric class field theory (see [Ser88]). Let $C_{\mathfrak{m}}$ denote the singular curve associated to \mathfrak{m} as in [Ser88, IV.4]. Let Pic_C and $\text{Pic}_{C_{\mathfrak{m}}}$ be the commutative group schemes over k representing the Picard functors of C and $C_{\mathfrak{m}}$. There is an exact sequence of commutative group schemes over k ,

$$(2.1) \quad 1 \rightarrow T \rightarrow \text{Pic}_{C_{\mathfrak{m}}} \rightarrow \text{Pic}_C \rightarrow 0,$$

where T is an algebraic torus. The restriction of (2.1) to the identity components is an exact sequence of semiabelian varieties,

$$(2.2) \quad 1 \rightarrow T \rightarrow J_{\mathfrak{m}} \rightarrow J \rightarrow 0,$$

where $J_{\mathfrak{m}}$ is the generalized Jacobian of C associated to the modulus \mathfrak{m} and J is the usual Jacobian of C .

Let \mathbb{G}^{\times} denote the multiplicative group scheme.¹

Lemma 2.2. *$T \simeq \text{Res}_{\mathfrak{m}} \mathbb{G}^{\times} / \mathbb{G}^{\times}$ is isomorphic to the quotient of $\text{Res}_{\mathfrak{m}} \mathbb{G}^{\times}$ by the diagonal embedding of \mathbb{G}^{\times} , and there is an exact sequence of finite group schemes*

$$1 \longrightarrow \frac{\text{Res}_{\mathfrak{m}}^1 \mu_n}{\mu_n} \longrightarrow T[n] \longrightarrow \mu_n \longrightarrow 1,$$

where $\text{Res}_{\mathfrak{m}}^1 \mu_n$ is the kernel of the norm map $N : \text{Res}_{\mathfrak{m}} \mu_n \rightarrow \mu_n$.

Proof. The first statement, that $T = \text{Res}_{\mathfrak{m}} \mathbb{G}^{\times} / \mathbb{G}^{\times}$, follows from well known results on the structure of generalized Jacobians (see [Ser88, §V Prop. 7]). Let $\text{Res}_{\mathfrak{m}}^1 \mathbb{G}^{\times}$ denote the kernel of the norm map $\text{Res}_{\mathfrak{m}} \mathbb{G}^{\times} \rightarrow \mathbb{G}^{\times}$. The inclusion map $\text{Res}_{\mathfrak{m}}^1 \mathbb{G}^{\times} \rightarrow \text{Res}_{\mathfrak{m}} \mathbb{G}^{\times}$ induces a

¹In conjunction with our use of \mathfrak{m} for the modulus and m for its degree, the standard notation \mathbb{G}_m for the multiplicative group might lead to confusion.

surjective map onto $\text{Res}_m \mathbb{G}^\times / \mathbb{G}^\times$ with kernel μ_m . This gives the middle rows of the following commutative and exact diagram.

$$\begin{array}{ccccccc}
& \mu_n & \longrightarrow & \text{Res}_m^1 \mu_n & \longrightarrow & T[n] & \\
& \downarrow & & \downarrow & & \downarrow & \\
1 & \longrightarrow & \mu_m & \longrightarrow & \text{Res}_m^1 \mathbb{G}^\times & \longrightarrow & \frac{\text{Res}_m \mathbb{G}^\times}{\mathbb{G}^\times} \longrightarrow 1 \\
& & \downarrow n & & \downarrow n & & \downarrow n \\
1 & \longrightarrow & \mu_m & \longrightarrow & \text{Res}_m^1 \mathbb{G}^\times & \longrightarrow & \frac{\text{Res}_m \mathbb{G}^\times}{\mathbb{G}^\times} \longrightarrow 1 \\
& & \downarrow m/n & & \downarrow & & \\
& & \mu_n & \longrightarrow & 1 & &
\end{array}$$

The exact sequence in the statement of the lemma follows by applying the snake lemma. \square

2.2. The isogeny associated to a modulus setup.

Lemma 2.3. *Given a modulus setup (n, \mathfrak{m}) there is a commutative group scheme \mathfrak{A} over k and isogenies $\psi : \text{Pic}_{C_{\mathfrak{m}}} \rightarrow \mathfrak{A}$ and $\varphi : \mathfrak{A} \rightarrow \text{Pic}_{C_{\mathfrak{m}}}$ such that $\ker(\psi) = \frac{\text{Res}_m^1 \mu_n}{\mu_n} \subset T[n]$ and $\varphi \circ \psi = [n]$. Moreover, we have a commutative and exact diagram*

$$\begin{array}{ccccccc}
1 & \longrightarrow & T' & \longrightarrow & \mathfrak{A} & \longrightarrow & \text{Pic}_C \longrightarrow 0 \\
& & \downarrow \varphi & & \downarrow \varphi & & \downarrow n \\
1 & \longrightarrow & T & \longrightarrow & \text{Pic}_{C_{\mathfrak{m}}} & \longrightarrow & \text{Pic}_C \longrightarrow 0.
\end{array}$$

where T' is a torus and $T'[\varphi] \simeq \mu_n$.

Proof. By Lemma 2.2, $\text{Pic}_{C_{\mathfrak{m}}}$ contains a finite group scheme isomorphic to $\text{Res}_m^1 \mu_n / \mu_n$. The quotient of $\text{Pic}_{C_{\mathfrak{m}}}$ by this subgroup scheme yields an isogeny $\psi : \text{Pic}_{C_{\mathfrak{m}}} \rightarrow \mathfrak{A}$. The existence of φ follows from the fact that $\ker(\psi)$ is contained in the kernel of multiplication by n . Since $\ker(\psi) \subset T$, \mathfrak{A} is an extension of Pic_C . The assertion that $T'[\varphi] \simeq \mu_n$ follows from Lemma 2.2. \square

Remark 2.4. *When $n = m = \deg(\mathfrak{m}) = 2$, we have that $T[n] \simeq \mu_n$. Hence ψ is the identity map on $\mathfrak{A} = \text{Pic}_{C_{\mathfrak{m}}}$ and φ is multiplication by 2.*

2.3. Description using divisor classes. A function $f \in k(C)^\times$ that is regular on \mathfrak{m} gives, by restriction, an element $f|_{\mathfrak{m}} \in M$, where $\text{Spec}(M) = \mathfrak{m}$. We use $\text{Div}_{\mathfrak{m}}(C)$ to denote the divisors of C that have support disjoint from \mathfrak{m} .

Lemma 2.5. *Let \mathfrak{A} be as defined in Lemma 2.3. Then*

$$\begin{aligned}
\text{Pic}_C(\bar{k}) &= \text{Div}(C_{\bar{k}}) / \{\text{div}(f) : f \in \bar{k}(C_{\bar{k}})^\times\}, \\
\text{Pic}_{C_{\mathfrak{m}}}(\bar{k}) &= \text{Div}_{\mathfrak{m}}(C_{\bar{k}}) / \{\text{div}(f) : f \in \bar{k}(C_{\bar{k}})^\times, f|_{\mathfrak{m}} = 1\}, \\
\mathfrak{A}(\bar{k}) &= \text{Div}_{\mathfrak{m}}(C_{\bar{k}}) / \{\text{div}(f) : f \in \bar{k}(C_{\bar{k}})^\times, f|_{\mathfrak{m}} \in \text{Res}_m^1 \mu_n\}.
\end{aligned}$$

Moreover, $\varphi : \mathfrak{A} \rightarrow \text{Pic}_{C_{\mathfrak{m}}}$ is induced by multiplication by n on $\text{Div}_{\mathfrak{m}}(C_{\bar{k}})$.

Proof. The first two statements are well known (see [Ser88]; note that $f|_{\mathfrak{m}} = 1$ if and only if $f \equiv 1 \pmod{\mathfrak{m}}$, since \mathfrak{m} is reduced). The \bar{k} -points of the subgroup $T = \text{Res}_{\mathfrak{m}} \mathbb{G}^{\times} / \mathbb{G}^{\times} \subset \text{Pic}_{C_{\mathfrak{m}}}$ are represented by divisors of functions which do not vanish on \mathfrak{m} ,

$$T(\bar{k}) = \frac{\{\text{div}(f) : f \in \bar{k}(C_{\bar{k}})^{\times}, f|_{\mathfrak{m}} \in \overline{M}^{\times}\}}{\{\text{div}(f) : f \in \bar{k}(C_{\bar{k}})^{\times}, f|_{\mathfrak{m}} = 1\}}.$$

The description of $\mathfrak{A}(\bar{k})$ in the statement then follows from the fact that \mathfrak{A} is the quotient of $\text{Pic}_{C_{\mathfrak{m}}}$ by the image of $\text{Res}_{\mathfrak{m}}^1 \mu_n$ in T . The final statement follows easily from the fact that $\varphi \circ \psi$ is multiplication by n on $\text{Pic}_{C_{\mathfrak{m}}}$. \square

2.4. Component groups. The component groups of $\text{Pic}_{C_{\mathfrak{m}}}$, Pic_C and \mathfrak{A} are all isomorphic to \mathbb{Z} , the isomorphism being given by the degree map on divisor classes. The degree 0 component of \mathfrak{A} is a semiabelian variety $A_{\mathfrak{m}}$ fitting into an exact sequence,

$$(2.3) \quad 1 \rightarrow T' \rightarrow A_{\mathfrak{m}} \rightarrow J \rightarrow 0.$$

In particular, $A_{\mathfrak{m}}$ is geometrically connected. We label the components

$$(2.4) \quad \text{Pic}_C = \bigsqcup_{i \in \mathbb{Z}} J^i, \quad \text{Pic}_{C_{\mathfrak{m}}} = \bigsqcup_{i \in \mathbb{Z}} J_{\mathfrak{m}}^i, \quad \mathfrak{A} = \bigsqcup_{i \in \mathbb{Z}} A_{\mathfrak{m}}^i,$$

so that the superscripts denote the image under the degree map. To ease notation we also denote the degree 0 components by $J = J^0$, $J_{\mathfrak{m}} = J_{\mathfrak{m}}^0$ and $A_{\mathfrak{m}} = A_{\mathfrak{m}}^0$. For any $i \in \mathbb{Z}$, J^i and $J_{\mathfrak{m}}^i$ are torsors under J and $J_{\mathfrak{m}}$, respectively.

Let $\mathfrak{m}' \in \text{Div}_{\mathfrak{m}}(C)$ be an effective reduced k -rational divisor linearly equivalent to and with disjoint support from \mathfrak{m} (which exists by Bertini's theorem, provided k has sufficiently many elements). Then \mathfrak{m}' determines classes in Pic_C , $\text{Pic}_{C_{\mathfrak{m}}}$ and \mathfrak{A} , which generate, in each, a subgroup scheme isomorphic to the constant group scheme \mathbb{Z} . Let \mathcal{J} , $\mathcal{J}_{\mathfrak{m}}$ and $\mathcal{A}_{\mathfrak{m}}$ denote the corresponding quotient group schemes, which exist since the category of commutative algebraic groups is abelian. We have,

$$(2.5) \quad \mathcal{J} := \frac{\text{Pic}_C}{\mathbb{Z}\mathfrak{m}'} = \bigsqcup_{i=0}^{m-1} J^i, \quad \mathcal{J}_{\mathfrak{m}} := \frac{\text{Pic}_{C_{\mathfrak{m}}}}{\mathbb{Z}\mathfrak{m}'} = \bigsqcup_{i=0}^{m-1} J_{\mathfrak{m}}^i, \quad \mathcal{A}_{\mathfrak{m}} := \frac{\mathfrak{A}}{\mathbb{Z}\mathfrak{m}'} = \bigsqcup_{i=0}^{m-1} A_{\mathfrak{m}}^i,$$

where we have abused notation slightly by writing \mathfrak{m}' to also denote its class in Pic_C , $\text{Pic}_{C_{\mathfrak{m}}}$ and \mathfrak{A} , respectively.

Remark 2.6. *It is not generally true that all effective divisors linearly equivalent to and disjoint from \mathfrak{m} give the same class in $\text{Pic}_{C_{\mathfrak{m}}}$, so the quotient maps $\text{Pic}_{C_{\mathfrak{m}}} \rightarrow \mathcal{J}_{\mathfrak{m}}$ and $\mathfrak{A} \rightarrow \mathcal{A}_{\mathfrak{m}}$ may depend on the choice for \mathfrak{m}' . However, the map $\text{Pic}_C \rightarrow \mathcal{J}$ depends only on \mathfrak{m} .*

The maps ψ and φ of Lemma 2.3 induce maps $\psi : \mathcal{J}_{\mathfrak{m}} \rightarrow \mathcal{A}_{\mathfrak{m}}$ and $\varphi : \mathcal{A}_{\mathfrak{m}} \rightarrow \mathcal{J}_{\mathfrak{m}}$ whose composition is multiplication by n . The map φ induces a morphism of exact sequences of group schemes,

$$(2.6) \quad \begin{array}{ccccccc} 0 & \longrightarrow & T' & \longrightarrow & \mathcal{A}_{\mathfrak{m}} & \longrightarrow & \mathcal{J} \longrightarrow 0 \\ & & \downarrow \varphi & & \downarrow \varphi & & \downarrow n \\ 0 & \longrightarrow & T & \longrightarrow & \mathcal{J}_{\mathfrak{m}} & \longrightarrow & \mathcal{J} \longrightarrow 0, \end{array}$$

6

and in particular an isogeny of semiabelian varieties,

$$(2.7) \quad \varphi : A_m \longrightarrow J_m .$$

Lemma 2.7. *There is a commutative and exact diagram,*

$$(2.8) \quad \begin{array}{ccccc} \mu_n & \xlongequal{\quad} & \mu_n & & \\ \downarrow & & \downarrow & & \\ A_m[\varphi] & \hookrightarrow & \mathcal{A}_m[\varphi] & \xrightarrow{\frac{1}{\ell} \deg} & \mathbb{Z}/n\mathbb{Z} \\ \downarrow & & \downarrow & & \parallel \\ J[n] & \hookrightarrow & \mathcal{J}[n] & \xrightarrow{\frac{1}{\ell} \deg} & \mathbb{Z}/n\mathbb{Z} . \end{array}$$

Proof. The first and second columns are, respectively, the kernels of the morphism of exact sequences appearing in Lemma 2.3 and Diagram (2.6). They are exact by the snake lemma, since $\varphi : T' \rightarrow T$ is an epimorphism. By Lemma 2.5, a divisor $D \in \text{Div}_m(C_{\bar{k}})$ represents a class in $\mathcal{A}_m[\varphi]$ if and only if $nD = a\mathbf{m}' + \text{div}(f)$, for some $a \in \mathbb{Z}$ and $f \in k(C_{\bar{k}})^\times$ with $f|_{\mathbf{m}} \in \text{Res}_{\mathbf{m}}^1 \mu_n$. In particular, $n \deg(D) = \deg(nD) = \deg(a\mathbf{m}') = an\ell$. So ℓ divides $\deg(D)$. As every class in \mathcal{A}_m can be represented by a divisor of degree $1 \leq d \leq m$ this shows that the maps in the first row are well defined. By definition, $A_m[\varphi]$ is the intersection of the kernels of the maps φ and \deg on \mathcal{A}_m . Surjectivity in the middle row follows from the fact that A_m is a divisible group. Namely, there exists $\mathbf{n}' \in \text{Div}(\bar{C})$, necessarily of degree ℓ , such that the class of $n\mathbf{n}'$ is equal to that of \mathbf{m}' in $\mathfrak{A}(\bar{k})$. By Lemma 2.5, $\varphi([\mathbf{n}']) = [n\mathbf{n}'] = [\mathbf{m}'] = 0$ in \mathcal{A}_m . Thus the middle row is exact. The same argument (applied to \mathcal{J} in place of \mathcal{A}_m) shows the same for the bottom row. \square

2.5. Extended Weil pairings. We now define a bilinear pairing

$$e : \mathcal{J}_m[n] \times \mathcal{J}_m[n] \rightarrow \mu_n .$$

Fix $f \in k(C)^\times$ such that $\text{div}(f) = \mathbf{m}' - \mathbf{m}$. Given $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_m[n]$, choose representative divisors $D_1, D_2 \in \text{Div}_m(C_{\bar{k}})$, and let $d_i = \deg(D_i)/\ell$, where we remind the reader that $\ell := m/n$. There exist unique functions $h'_i \in k(C_{\bar{k}})^\times$ such that $nD_i = \text{div}(h'_i) + d_i\mathbf{m}'$ and $h'_i|_{\mathbf{m}} = 1$. Set $h_i = f^{d_i} h'_i$, so that $nD_i = \text{div}(h_i) + d_i\mathbf{m}$. Define:

$$(2.9) \quad e(\mathcal{D}_1, \mathcal{D}_2) = (-1)^{d_1 d_2} \prod_{P \in C(\bar{k})} (-1)^{n(\text{ord}_P D_1)(\text{ord}_P D_2)} \frac{h_2^{\text{ord}_P D_1}}{h_1^{\text{ord}_P D_2}}(P) \in \bar{k}^\times .$$

We note that when D_1 and D_2 have disjoint support, this can be written as

$$(2.10) \quad e(\mathcal{D}_1, \mathcal{D}_2) = (-1)^{d_1 d_2} \frac{h_2(D_1)}{h_1(D_2)} .$$

Proposition 2.8. *The pairing e is Galois equivariant and induces, via the surjective map $\psi : \mathcal{J}_m[n] \rightarrow \mathcal{A}_m[\varphi]$ and the maps in (2.8), nondegenerate Galois equivariant pairings*

$$\begin{aligned} e : \mathcal{A}_m[\varphi] \times \mathcal{A}_m[\varphi] &\rightarrow \mu_n , \\ e : \mathcal{A}_m[\varphi] \times \mathcal{J}[n] &\rightarrow \mu_n , \\ e : \mathcal{J}[n] \times \mathcal{J}[n] &\rightarrow \mu_n . \end{aligned}$$

Moreover, the pairing on $\mathcal{J}[n] \times \mathcal{J}[n]$ coincides with the Weil pairing.

Remark 2.9. *The definition of e given above depends on the choice of \mathbf{m}' in (2.5) and the function f with $\text{div}(f) = \mathbf{m}' - \mathbf{m}$. However, as shown in the proof below, the induced pairings on $A_{\mathbf{m}}[\varphi] \times \mathcal{J}[n]$ and $J[n] \times J[n]$ do not depend on these choices.*

Proof. One can check that the pairing $e : \mathcal{J}_{\mathbf{m}}[n] \times \mathcal{J}_{\mathbf{m}}[n] \rightarrow \mu_n$ is Galois equivariant exactly as is done in [PS97, Section 7] where the situation of Example M.1 is considered (one need only replace the function x there with the function f in the definition above).

We will show that the orthogonal complements of $\text{Res}_{\mathbf{m}}^1 \mu_n / \mu_n$ and $T[n]$ with respect to e are $\mathcal{J}_{\mathbf{m}}[n]$ and $J_{\mathbf{m}}[n]$, respectively. This is enough to ensure that e induces the pairings stated. The pairing induced on $J[n]$ is evidently the Weil pairing (see [How96, Theorem 1]), which is known to be nondegenerate. Nondegeneracy of the other pairings follows from the exactness of (2.8). Alternatively, Lemma 3.5 below gives an alternative description of this pairing using class field theory which is readily seen to be nondegenerate.

Let $\mathcal{D}_1 \in T[n]$. Then \mathcal{D}_1 is represented by $D_1 = \text{div}(f)$ for some $f \in k(C_{\bar{k}})^\times$ with $f|_{\mathbf{m}} \in \text{Res}_{\mathbf{m}} \mu_n$. Since $nD_1 = \text{div}(f^n)$ and $f^n|_{\mathbf{m}} = 1$ we must use $h_1 = f^n$ in the definition of the pairing. Suppose $\mathcal{D}_2 \in \mathcal{J}[n]$ and let D_2, h_2, d_2 be as in the definition of the pairing. Then we have

$$\begin{aligned}
e(\mathcal{D}_1, \mathcal{D}_2) &= \prod_{P \in C(\bar{k})} (-1)^{n(\text{ord}_P f)(\text{ord}_P D_2)} \frac{h_2^{\text{ord}_P f}}{f^{n \text{ord}_P D_2}}(P) \\
&= \prod_{P \in C(\bar{k})} (-1)^{(\text{ord}_P f)(\text{ord}_P h_2 + d_2 \text{ord}_P \mathbf{m})} \frac{h_2^{\text{ord}_P f}}{f^{\text{ord}_P h_2 + d_2 \text{ord}_P \mathbf{m}}}(P) \quad (\text{since } nD_2 = \text{div}(h_2) + d_2 \mathbf{m}.) \\
&= \prod_{P \in C(\bar{k})} (-1)^{d_2(\text{ord}_P f)(\text{ord}_P \mathbf{m})} f^{-d_2 \text{ord}_P \mathbf{m}}(P) \quad (\text{by Weil reciprocity}) \\
&= \prod_{P \in C(\bar{k})} f^{-d_2 \text{ord}_P \mathbf{m}}(P) \quad (\text{since } f|_{\mathbf{m}} \text{ is invertible}) \\
&= N(f|_{\mathbf{m}})^{-d_2},
\end{aligned}$$

where N denotes the induced norm $\text{Res}_{\mathbf{m}} \mathbb{G}^\times \rightarrow \mathbb{G}^\times$. From this one easily sees that $\text{Res}_{\mathbf{m}}^1 \mu_n / \mu_n$ lies in the kernel of the pairing and that $T[n]$ pairs trivially with the degree 0 subgroup, $J_{\mathbf{m}}[n] \subset \mathcal{J}_{\mathbf{m}}[n]$. \square

Taking Galois cohomology of (2.8) yields a commutative and exact diagram

$$(2.11) \quad \begin{array}{ccccc}
& & k^\times / k^{\times n} & \xlongequal{\quad} & k^\times / k^{\times n} \\
& & \downarrow & & \downarrow \\
\mathbb{Z}/n\mathbb{Z} & \xrightarrow{\partial'} & H^1(A_{\mathbf{m}}[\varphi]) & \longrightarrow & H^1(\mathcal{A}_{\mathbf{m}}[\varphi]) \xrightarrow{\frac{1}{2} \text{deg}} H^1(\mathbb{Z}/n\mathbb{Z}) \\
\parallel & & \downarrow & & \downarrow & \parallel \\
\mathbb{Z}/n\mathbb{Z} & \xrightarrow{\partial} & H^1(J[n]) & \longrightarrow & H^1(\mathcal{J}[n]) \xrightarrow{\frac{1}{2} \text{deg}} H^1(\mathbb{Z}/n\mathbb{Z}) \\
& & \downarrow \gamma & & \downarrow \gamma' \\
& & \text{Br}(k)[n] & \xlongequal{\quad} & \text{Br}(k)[n]
\end{array}$$

Lemma 2.10. *The images of $\partial(1)$ and $\partial'(1)$ in $H^1(J)$ and $H^1(A_m)$ are the classes of J^ℓ and A_m^ℓ , respectively. The maps Υ and Υ' are given by*

$$\begin{aligned}\Upsilon(\xi) &= \xi \cup_e \partial(1), \text{ and} \\ \Upsilon'(\xi) &= \xi \cup_e \partial'(1),\end{aligned}$$

where \cup_e denotes the cup product pairings

$$\begin{aligned}\cup_e : H^1(J[n]) \times H^1(J[n]) &\rightarrow H^2(\mu_n) = \text{Br}(k)[n], \text{ and} \\ \cup_e : H^1(\mathcal{J}[n]) \times H^1(A_m[\varphi]) &\rightarrow H^2(\mu_n) = \text{Br}(k)[n]\end{aligned}$$

determined by the e -pairings of Proposition 2.8 (cf. [NSW08, page 38]).

Proof. At the level of cocycles, $\partial(1)$ is represented by $\text{Gal}_k \ni \sigma \mapsto [\sigma(D) - D] \in J[n]$, where $D \in \text{Div}(\overline{C})$ is such that nD is linearly equivalent to \mathfrak{m}' and the square parentheses denote the class of a divisor in $\text{Pic}(\overline{C})$. The divisor D necessarily has degree $m/n = \ell$, so the image of this cocycle in $H^1(J)$ represents J^ℓ . The claim that $\partial'(1)$ represents A_m^ℓ is established similarly.

The e -pairings of Proposition 2.8 give commutative diagrams of pairings

$$(2.12) \quad \begin{array}{ccccc} \mu_n & \times & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mu_n \\ \downarrow & & \uparrow & & \parallel \\ A_m[\varphi] & \times & \mathcal{J}[n] & \rightarrow & \mu_n \\ \downarrow & & \uparrow & & \parallel \\ J[n] & \times & J[n] & \rightarrow & \mu_n \end{array} \quad \begin{array}{ccccc} \mu_n & \times & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mu_n \\ \downarrow & & \uparrow & & \parallel \\ A_m[\varphi] & \times & A_m[\varphi] & \rightarrow & \mu_n \\ \downarrow & & \uparrow & & \parallel \\ \mathcal{J}[n] & \times & A_m[\varphi] & \rightarrow & \mu_n. \end{array}$$

Since the maps Υ and Υ' are coboundary maps from the first columns and the maps ∂ and ∂' are coboundary maps from the second columns we may apply [NSW08, Corollary 1.4.5] once to each of the diagrams in (2.12) to deduce that $\Upsilon(\xi) = \xi \cup_e \partial(1)$ and $\Upsilon'(\xi) = \xi \cup_e \partial'(1)$. \square

2.6. Brauer class of a k -rational divisor class. Given a nice curve C , there is a well known exact sequence

$$(2.13) \quad 0 \rightarrow \text{Pic}(C) \longrightarrow \text{Pic}_C(k) \xrightarrow{\Theta_C} \text{Br}(k)$$

(see [Lic69]). The map Θ_C gives the obstruction to a k -rational divisor class being represented by a k -rational divisor.

Lemma 2.11. *Let $d : J(k) \rightarrow H^1(J[n])$ denote the connecting homomorphism in the Kummer sequence. For any $x \in J(k)$ we have $\Upsilon \circ d(x) = \ell \cdot \Theta_C(x)$.*

Proof. The image of d is isotropic with respect to the Weil-pairing cup product \cup_e . This gives a commutative diagram of pairings

$$\begin{array}{ccccc} \cup_e : & H^1(J[n]) & \times & H^1(J[n]) & \rightarrow & \text{Br}(k) \\ & d \uparrow & & \downarrow & & \parallel \\ \langle \cdot, \cdot \rangle : & J(k) & \times & H^1(J) & \rightarrow & \text{Br}(k) \end{array}$$

By a result of Lichtenbaum (see the proof of [Lic69, Corollary 1]) we have that $\langle x, [J^1] \rangle = \Theta_C(x)$. By the previous lemma we have

$$\Upsilon \circ d(x) = d(x) \cup_e \partial(1) = \langle x, [J^\ell] \rangle = \ell \cdot \langle x, [J^1] \rangle = \ell \cdot \Theta_C(x).$$

□

Let $J(k)_\bullet$ denote the kernel of the composition $\Upsilon \circ d : J(k) \rightarrow H^1(J[n]) \rightarrow \text{Br}(k)$. Then $\text{Pic}^0(C) \subset J(k)_\bullet \subset J(k)$ and, in general, any of these containments can be proper. Lemma 2.11 shows that $\text{Pic}^0(C) = J(k)_\bullet$ when $\ell = 1$ (e.g., for the modulus setups of Example M.1 and Example M.2) while the following corollary shows that $J(k)_\bullet = J(k)$ when k is a local or global field and C has a modulus setup as in Example M.3.

Corollary 2.12. *If*

- (1) *the period of C divides ℓ , or*
- (2) *k is a local or global field and $\gcd(m, g - 1)$ divides ℓ ,*

then $\Upsilon \circ d = 0$.

Proof. The image of $\Theta_C : J(k) \rightarrow \text{Br}(k)$ is isomorphic to the cokernel of $\text{Pic}^0(C) \rightarrow J(k)$, which is annihilated by the period of C ([PS97, Prop. 3.2]). Over a local field, the period of C divides $g - 1$ ([PS97, Prop. 3.4]). Since the period also divides $m = \deg(\mathfrak{m})$, (2) implies that ℓ is divisible by the period locally. Hence $\Upsilon \circ d = 0$ locally. This must also be true globally by the local-global principle for $\text{Br}(k)$. □

We recall that the situation for $\text{Pic}_{C_{\mathfrak{m}}}$ is different.

Lemma 2.13. *The natural map $\text{Div}_{\mathfrak{m}}(C) \rightarrow \text{Pic}_{C_{\mathfrak{m}}}(k)$ is surjective. In particular, for any $i \geq 1$, $\text{Div}^i(C) \neq \emptyset$ if and only if $J_{\mathfrak{m}}^i(k) \neq \emptyset$.*

Proof. The first statement follows from [PS97, Lemma 3.5]. The second follows from the first by the moving lemma. □

3. n -COVERINGS, φ -COVERINGS AND THE DESCENT SETUP

3.1. n -coverings and φ -coverings.

Definition 3.1. *Suppose $\phi : A \rightarrow B$ is an isogeny of semiabelian varieties over k and V is a B -torsor. We say $\pi : V' \rightarrow V$ is a ϕ -covering of V if there exist isomorphisms a, b of \bar{k} -varieties such that a is compatible with the torsor structure of V , fitting into a commutative diagram*

$$\begin{array}{ccc} V'_k & \xrightarrow{b} & A_{\bar{k}} \\ \downarrow \pi & & \downarrow \phi \\ V_k & \xrightarrow{a} & B_{\bar{k}} \end{array}$$

Let $\text{Cov}^\phi(V)$ denote the set of isomorphism classes of ϕ -covering of V , considered as objects in the category of V -schemes.

To say that a is compatible with the torsor structure means that $a(x + y) = a(x) + y$. Note that the isomorphism b endows V' with the structure of a torsor under A by the rule $x + y = b^{-1}(b(x) + y)$. The classes of these torsors satisfy $\phi_*[V'] = [V] \in H^1(B)$. When nonempty, $\text{Cov}^\phi(V)$ is a principal homogeneous space for the group $H^1(\ker(\phi))$ acting by twisting. The isogenies $\varphi : A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ and $n : J \rightarrow J$ give distinguished points in $\text{Cov}^\varphi(J_{\mathfrak{m}})$ and $\text{Cov}^n(J)$, endowing these sets with the structure of an abelian group and isomorphisms to $H^1(A_{\mathfrak{m}}[\varphi])$ and $H^1(J[n])$, respectively.

Suppose (n, \mathfrak{m}) is a modulus setup for a nice curve C over k . The isogenies $\varphi : A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ and $n : J \rightarrow J$ give rise to the notions of φ -coverings of $J_{\mathfrak{m}}^i$ and n -coverings of J^i for each $i \geq 0$. The pullback of a φ -covering $V \rightarrow J_{\mathfrak{m}}^1$ along the canonical map $(C - \mathfrak{m}) \rightarrow J_{\mathfrak{m}}^1$ sending a geometric point x to the class of the divisor x in $J_{\mathfrak{m}}^1(\bar{k}) \subset \text{Pic}_{C_{\mathfrak{m}}}(\bar{k})$ yields an unramified covering of $(C - \mathfrak{m})$. Corresponding to this is a unique (up to isomorphism) morphism $\pi : Y \rightarrow C$ of smooth projective curves over k which is unramified outside \mathfrak{m} .

Definition 3.2. *Suppose (n, \mathfrak{m}) is a modulus setup for a nice curve C over k . A morphism $\pi : Y \rightarrow C$ of nice curves is a φ -covering of C if it is the unique extension of the pullback of a φ -covering of $J_{\mathfrak{m}}^1$ along the canonical map $(C - \mathfrak{m}) \rightarrow J_{\mathfrak{m}}^1$. A morphism $\pi : X \rightarrow C$ is an n -covering of C if it is the pullback of an n -covering of J^1 along the canonical map $C \rightarrow J^1$. Let $\text{Cov}^n(C)$ and $\text{Cov}^{\varphi}(C)$ denote, respectively, the sets of isomorphism classes of n -coverings and φ -coverings of C (considered as objects in the category of C -schemes).*

Proposition 3.3. *An n -covering of C is a k -form of the maximal unramified abelian covering of C of exponent n . A φ -covering of C is an abelian covering of exponent n and conductor \mathfrak{m} whose maximal unramified subcovering is an n -covering.*

Proof. Any unramified abelian extension of $\bar{k}(\bar{C})$ of exponent n is obtained by adjoining n -th roots of functions $f \in \bar{k}(\bar{C})$ with $\text{div}(f) = nD \in n\text{Div}(\bar{C})$. For any such function, the class of the divisor D lies in $J[n]$. For the (unique up to isomorphism) n -covering $\pi : C' \rightarrow \bar{C}$ we have $J[n](\bar{k}) = \ker(\pi^* : \text{Pic}^0(\bar{C}) \rightarrow \text{Pic}^0(C'))$. Thus $\bar{k}(C')$ contains n -th roots of all functions f as above. This proves the first statement.

Similarly, the field extension of $\bar{k}(C_{\bar{k}})$ corresponding to a φ -covering is the compositum of the extensions corresponding to the index n subgroups of $A_{\mathfrak{m}}[\varphi]$, or equivalently, to the points of order n in the Cartier dual $\mathcal{J}[n]$ (the duality is given by Proposition 2.8). If $D \in \text{Div}(C_{\bar{k}})$ represents a point of order n in $\mathcal{J}[n]$, then there exists a function $h_D \in \bar{k}(C_{\bar{k}})^{\times}$ such that $\text{div}(h_D) = nD - d\mathfrak{m}$ for some $d \in \mathbb{Z}$. The corresponding extension of $\bar{k}(C_{\bar{k}})$ is obtained by adjoining an n -th root of h_D . Such extensions are of conductor \mathfrak{m} . The maximal unramified subextension is obtained by adjoining n -th roots only of those h_D for which $\text{div}(h_D) - nD = d\mathfrak{m}$ with $d \equiv 0 \pmod{n}$. These correspond to points in $J[n]$ showing that the maximal unramified subcover of a φ -covering is an n -covering. □

When nonempty, the sets $\text{Cov}^n(C)$ and $\text{Cov}^{\varphi}(C)$ are principal homogeneous spaces for $H^1(J[n])$ and $H^1(A_{\mathfrak{m}}[n])$, respectively, acting by twisting. By geometric class field theory the canonical pullback maps $p : \text{Cov}^n(J^1) \rightarrow \text{Cov}^n(C)$ and $p_{\mathfrak{m}} : \text{Cov}^{\varphi}(J_{\mathfrak{m}}^1) \rightarrow \text{Cov}^{\varphi}(C)$ are bijections that are equivariant for the actions by $H^1(J[n])$ and $H^1(A_{\mathfrak{m}}[n])$. By Proposition 3.3 there is a canonical map $u : \text{Cov}^{\varphi}(C) \rightarrow \text{Cov}^n(C)$, which associates to a φ -covering of C the maximal unramified intermediate covering of C . Let $\text{Cov}_{\mathfrak{m}}^n(C)$ denote the image of u .

Given a φ -covering $\pi : F_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}^i$, the torsor structures restrict to actions of the tori $T' \subset A_{\mathfrak{m}}$ and $T \subset J_{\mathfrak{m}}$ on $F_{\mathfrak{m}}$ and $J_{\mathfrak{m}}^i$, respectively. The quotients $F = F_{\mathfrak{m}}/T'$ and $J^i = J_{\mathfrak{m}}^i/T$ are torsors under $J = A_{\mathfrak{m}}/T' = J_{\mathfrak{m}}/T$. The existence of these quotients in the category of varieties follows from [Gro95, Theoreme 7.2], while the induced torsor structure can be established as in the proof of [Bor96, Lemma 3.1]. Since the actions of T' and T are equivariant with respect to π , there is an induced map $\pi' : F \rightarrow J^i$ which is a torsor under $A_{\mathfrak{m}}[\varphi]/T'[\varphi] = J[n]$. This induces a map $q : \text{Cov}^{\varphi}(J_{\mathfrak{m}}^i) \rightarrow \text{Cov}^n(J^i)$. Let $\text{Cov}_{\mathfrak{m}}^n(J^i)$ denote the image of q . We record the following.

Lemma 3.4.

- (1) The isomorphism $\text{Cov}^n(J) \simeq H^1(J[n])$ restricts to $\text{Cov}_m^n(J) \simeq \ker(\Upsilon)$.
- (2) The maps defined above fit into a commutative diagram,

$$\begin{array}{ccc} \text{Cov}^\varphi(J_m^1) & \xrightarrow{p_m} & \text{Cov}^\varphi(C) \\ \downarrow q & & \downarrow u \\ \text{Cov}^n(J^1) & \xrightarrow{p} & \text{Cov}^n(C). \end{array}$$

In particular, p restricts to give a bijection $p : \text{Cov}_m^n(J) \rightarrow \text{Cov}_m^n(C)$.

Proof. The first statement follows from exactness in (2.11). The second follows from the universal property of the fibered product. \square

Using φ -coverings we can give an alternative description of the e -pairing on $A_m[\varphi] \times \mathcal{J}[n]$ given in Proposition 2.8. Let (Y, π) be a φ -covering of $C_{\bar{k}}$. Let $M = \bar{k}(Y)$ and $K = \bar{k}(C_{\bar{k}})$, which we identify with the subfield $\pi^*(K) \subset M$. There are canonical isomorphisms $r : A_m[\varphi] \simeq \text{Gal}(M/\pi^*K)$ and $s : \mathcal{J}[n] \simeq (K^\times \cap M^{\times n})/K^{\times n}$. The latter sends the class of a divisor D to the class of a function $h \in K$ such that $\text{div}(h) = nD - d\mathfrak{m}$, for some integer d . Kummer theory gives a bilinear pairing $\kappa : \text{Gal}(M/K) \times (K^\times \cap M^{\times n})/K^{\times n} \rightarrow \mu_n$.

Lemma 3.5. For $\mathcal{D}_1 \in A_m[\varphi]$ and $\mathcal{D}_2 \in \mathcal{J}[n]$ we have $e(\mathcal{D}_1, \mathcal{D}_2) = \kappa(r(\mathcal{D}_1), s(\mathcal{D}_2))$.

Proof. The analogous statement for the induced pairing on $J[n] \times J[n]$ is the main result of [How96]. As described in Section 4 of op. cit. it suffices to prove the statement when k is a finite field. Let $\mathcal{D}_1 \in A_m[\varphi](\bar{k})$ and $\mathcal{D}_2 \in \mathcal{J}[n](\bar{k})$. By possibly enlarging k if necessary we can arrange that the \mathcal{D}_i are represented by k -rational divisors D_i and, moreover, that $J_m[n](k) = J_m[n](\bar{k})$. Take $g \in k(C)^\times$ such that $\text{div}(g) = nD_2 - d\mathfrak{m}$. Then, as seen in the proof of Proposition 3.3, $g \in M^{\times n}$. Let $F : J_m \rightarrow J_m$ be the k -Frobenius. Then $J_m[n](k) \subset \ker(F - 1)$, so $F - 1$ factors through multiplication by n , and hence through φ . Moreover, the extension M/K extends to a Galois extension N/K with $\text{Gal}(N/K) \simeq J_m[F - 1] \simeq J_m(k)$.

All of this fits into a commutative diagram

$$\begin{array}{ccccc} J_m(k) & \xrightarrow{\simeq} & \text{Gal}(N/K) & & \\ \downarrow (F-1)/n & \searrow (F-1)/\varphi & \downarrow & & \\ J_m(k)[n] & \xrightarrow{\psi} & A_m[\varphi](k) & \xrightarrow{\simeq_r} & \text{Gal}(M/K) \\ & \searrow \kappa(r(\cdot), s(\mathcal{D}_2)) & \downarrow & & \downarrow \\ & & \mu_n(k) & \xleftarrow{\simeq} & \text{Gal}(K(g^{1/n})/K). \end{array}$$

The map from the top left to the bottom right is given by the Artin map of class field theory and, hence, the composition $I^0(k) \rightarrow J_m(k) \rightarrow \mu_n(k)$ from the k -idèles of K to $\mu_n(k)$ can be computed with Hilbert norm residue symbols (see [Ser88, §6.30, p. 150]). Take $a \in I^0(k)$ to be an idèle whose divisor class is equal to the class of D_1 in $J_m(k)$ and $b \in I^0(k)$ such that $(F - 1)/n[b] = [a]$ in $J_m(k)$. To prove the lemma amounts to checking that $e(\mathcal{D}_1, \mathcal{D}_2)$ is equal to the product of the Hilbert norm residue symbols, $\prod_{P \in C(\bar{k})} (g, b)_P$. This can be verified exactly as in the calculation of [How96, Section 3]. \square

3.2. Soluble coverings. For an isogeny $\phi: A \rightarrow B$ of semiabelian varieties and V a torsor under B , let $\text{Cov}_{\text{sol}}^{\phi}(V)$ denote the set of isomorphism classes of ϕ -coverings $U \rightarrow V$ with $U(k) \neq \emptyset$. When k is a global field, let $\text{Sel}^{\phi}(V)$ denote the set of isomorphism classes of ϕ -coverings of V that are soluble everywhere locally. Define similarly $\text{Cov}_{\text{sol}}^n(C)$, $\text{Cov}_{\text{sol}}^{\varphi}(C)$, $\text{Sel}^n(C)$ and $\text{Sel}^{\varphi}(C)$.

Recall that for a nice curve C over k with modulus setup (n, \mathfrak{m}) , $J(k)_{\bullet}$ denotes the kernel of the composition $\Upsilon \circ d: J(k) \rightarrow H^1(J[n]) \rightarrow \text{Br}(k)$.

Lemma 3.6. $\text{Cov}_{\mathfrak{m}}^n(J) \cap \text{Cov}_{\text{sol}}^n(J) = d(J(k)_{\bullet})$.

Proof. $\text{Cov}_{\text{sol}}^n(J) = d(J(k))$ and $\text{Cov}_{\mathfrak{m}}^n(J) = \ker(\Upsilon)$ by Lemma 3.4. \square

The reciprocity law in the Brauer group yields the following.

Corollary 3.7. *If k is a global field and $J(k_v)_{\bullet} = J(k_v)$ for all but at most one prime v , then $\text{Sel}^n(J) \subset \text{Cov}_{\mathfrak{m}}^n(J)$.*

This corollary shows that the subgroup $\text{Cov}_{\mathfrak{m}}^n(J) \subset \text{Cov}^n(J)$ is large enough to be useful for arithmetic applications. We will derive analogous results for $\text{Cov}_{\mathfrak{m}}^n(C)$ and $\text{Cov}_{\mathfrak{m}}^n(J^i)$ as corollaries to the following theorem.

Theorem 3.8. *The group $H^1(J[n])$ acts on the sets $\text{Cov}^n(J^i)$ by twisting. This gives rise to simply transitive actions of:*

- (1) $H^1(J[n])$ on $\text{Cov}^n(J^i)$, when $[J^i]$ is divisible by n in $H^1(J)$;
- (2) $H^1(J[n])$ on $\text{Cov}^n(C)$, when $[J^i]$ is divisible by n in $H^1(J)$;
- (3) $\ker(\Upsilon)$ on $\text{Cov}_{\mathfrak{m}}^n(J^i)$, when $[J_{\mathfrak{m}}^i] \in \varphi_*(H^1(A_{\mathfrak{m}})) \subset H^1(J_{\mathfrak{m}})$;
- (4) $\ker(\Upsilon)$ on $\text{Cov}_{\mathfrak{m}}^n(C)$, when $[J_{\mathfrak{m}}^1] \in \varphi_*(H^1(A_{\mathfrak{m}})) \subset H^1(J_{\mathfrak{m}})$;
- (5) $J(k)/nJ(k)$ on $\text{Cov}_{\text{sol}}^n(J^i)$, when $J^i(k) \neq \emptyset$;
- (6) $d(J(k)_{\bullet})$ on $\text{Cov}_{\text{sol}}^n(J^i) \cap \text{Cov}_{\mathfrak{m}}^n(J^i)$, when $J_{\mathfrak{m}}^i(k) \neq \emptyset$;

and, assuming k is a global field, of

- (7) $\text{Sel}^n(J)$ on $\text{Sel}^n(J^i)$, when $[J^i] \in n\text{III}(J)$;
- (8) $\text{Sel}^n(J)$ on $\text{Sel}^n(J^i) \cap \text{Cov}_{\mathfrak{m}}^n(J^i)$, when $[J^i] \in n\text{III}(J)$ and for all but at most one prime v of k we have $J(k_v)_{\bullet} = J(k_v)$ and $J_{\mathfrak{m}}^i(k_v) \neq \emptyset$.

Proof.

- (1) First note that n -coverings are $J[n]$ -torsors. As in [Sko01, Section 2.2], the low degree terms of the Hochschild-Serre spectral sequence give an exact sequence

$$0 \rightarrow H^1(\text{Gal}_k, J[n]) \rightarrow H_{\text{ét}}^1(J^i, J[n]) \rightarrow H^0(\text{Gal}_k, H_{\text{ét}}^1(J_k^i, J[n])) \xrightarrow{\partial} H^2(\text{Gal}_k, J[n]).$$

There exists an n -covering of J_k^i and the image of its class under ∂ is the obstruction to the existence of an n -covering of J^i . This obstruction coincides with the coboundary of $[J^i]$ arising from the exact sequence $0 \rightarrow J[n] \rightarrow J \rightarrow J \rightarrow 0$ (see [Sko01, Lemma 2.4.5]). In particular, if $[J^i]$ is divisible by n , then $\text{Cov}^n(J^i) \neq \emptyset$. In this case $H^1(J[n])$ acts simply transitively on $\text{Cov}^n(J^i)$ by exactness of the sequence above.

- (2) It follows from geometric class field theory that the map $\text{Cov}^n(J^1) \rightarrow \text{Cov}^n(C)$ given by pullback is a bijection which respects the action of $H^1(J[n])$, so (1) \Rightarrow (2).

- (3) As in the proof of (1), the condition $[J_m^i] \in \varphi_*(H^1(A_m)) \subset H^1(J_m)$ ensures that $\text{Cov}^\varphi(J_m^i)$ is nonempty, and hence is a principal homogeneous space for $H^1(A_m[\varphi])$. The map $q : \text{Cov}^\varphi(J_m^i) \rightarrow \text{Cov}^n(J^i)$ is a map of principal homogeneous spaces, compatible with the homomorphism $s : H^1(A_m[\varphi]) \rightarrow H^1(J[n])$ coming from the cohomology of the exact sequence $1 \rightarrow T'[\varphi] \rightarrow A_m[\varphi] \rightarrow J[n] \rightarrow 0$. The image of q is $\text{Cov}_m^n(J^i)$, while the image of s is $\ker(\Upsilon)$.
- (4) This follows from (3) by pullback.
- (5) If $J^i(k) \neq \emptyset$, then $\text{Cov}_{\text{sol}}^n(J^i) \neq \emptyset$ (since in this case $[J^i] = 0$ in $H^1(J)$ is divisible by n). The difference of any two soluble n -coverings has trivial image in $H^1(J)$, hence must lie in the image of the Kummer map $d : J(k)/nJ(k) \hookrightarrow H^1(J[n])$.
- (6) By assumption $J_m^i(k) \neq \emptyset$, so $\text{Cov}_{\text{sol}}^\varphi(J_m^i) \neq \emptyset$. Then $q(\text{Cov}_{\text{sol}}^\varphi(J_m^i)) \subset \text{Cov}_m^n(J^i) \cap \text{Cov}_{\text{sol}}^n(J)$ is nonempty. The result now follows from (3) and (5) since $d(J(k)_\bullet) = d(J(k)/nJ(k)) \cap \ker(\Upsilon)$.
- (7) Since $[J^i] \in n\text{III}(J)$, we have that $\text{Sel}^n(J^i) \neq \emptyset$. One then argues as in (5) (everywhere locally) to see that the difference of two locally soluble n -coverings of J^i gives an element of $\text{Sel}^n(J)$.
- (8) First we claim that $\text{Cov}^\varphi(J_m^i)$ and, hence, $\text{Cov}_m^n(J^i)$ are nonempty. As in the proof of (1), there exists a φ -covering of $(J_m^i)_{\bar{k}}$ and the obstruction to Galois descent is an element $o \in H^2(A_m[\varphi])$. There is an exact sequence $\text{Br}(k)[n] = H^2(T'[\varphi]) \rightarrow H^2(A_m[\varphi]) \rightarrow H^2(J[n])$ and the image of o in $H^2(J[n])$ is the obstruction to the existence of an n -covering of J^i . We have assumed $[J^i] \in n\text{III}(J)$, so o is the image of an element from $\text{Br}(k)$. However, o must vanish everywhere locally since we have assumed J_m^i is locally soluble. So o is trivial by the local-global principle for the Brauer group.

Now suppose $(F, \pi) \in \text{Sel}^n(J^i)$. By (1) there exists some $\xi \in H^1(J[n])$ such that the twist $\xi \cdot (F, \pi)$ lies in $\text{Cov}_m^n(J^i)$. We will show that $\xi \in \ker(\Upsilon)$ which, in light of (3), shows that $(F, \pi) \in \text{Cov}_m^n(J^i)$. Thus, $\text{Sel}^n(J^i) \subset \text{Cov}_m^n(J^i)$ and the conclusion of (8) follows from (7).

Let v be a prime such that $J(k_v)_\bullet = J(k_v)$. Together (5) and (6) show that $\text{Cov}_{\text{sol}}^n(J_{k_v}^i) \subset \text{Cov}_m^n(J_{k_v}^i)$. Since $\text{res}_v(F, \pi) \in \text{Cov}_{\text{sol}}^n(J_{k_v}^i)$, (3) implies that $\text{res}_v(\xi) \in \ker(\Upsilon)$. Since $J(k_v)_\bullet = J(k_v)$ for all but at most one prime, the reciprocity law in the Brauer group gives that $\xi \in \ker(\Upsilon)$.

□

Corollary 3.9. $\text{Cov}_{\text{sol}}^n(C) \subset \text{Cov}_m^n(C)$ and if k is a global field, then $\text{Sel}^n(C) \subset \text{Cov}_m^n(C)$.

Proof. For the first statement we may assume $\text{Cov}_{\text{sol}}^n(C) \neq \emptyset$. Then $C(k) \neq \emptyset$ and, hence, $J_m^1(k), J^1(k) \neq \emptyset$ and $J(k)_\bullet = J(k)$. So (5) and (6) show that $\text{Cov}_{\text{sol}}^n(J^1) \subset \text{Cov}_m^n(J^1)$. Then $\text{Cov}_{\text{sol}}^n(C) \subset p(\text{Cov}_{\text{sol}}^n(J^1)) \subset p(\text{Cov}_m^n(J^1)) = \text{Cov}_m^n(C)$. To prove the second statement we may assume $\text{Sel}^n(C)$ is nonempty. Then the hypothesis of Theorem 3.8(8) in case $i = 1$ is satisfied, so this together with Theorem (3.8)(7) shows that $\text{Sel}^n(J^1) \subset \text{Cov}_m^n(J^1)$. The result now follows by applying the pullback map as in the proof of the first statement. □

Corollary 3.10. If $J(k)_\bullet = J(k)$ and $\text{Div}^i(C) \neq \emptyset$, then $\text{Cov}_{\text{sol}}^n(J^i) \subset \text{Cov}_m^n(J^i)$. If k is a global field and for all but at most one prime v of k , $\text{Div}^i(C_{k_v}) \neq \emptyset$ and $J(k_v)_\bullet = J(k_v)$. Then $\text{Sel}^n(J^i) \subset \text{Cov}_m^n(J^i)$.

Proof. If $\text{Sel}^n(J^i) = \emptyset$ there is nothing to prove. Otherwise, the hypotheses of (8) is satisfied since our assumption $\text{Div}^i(C_{k_v}) \neq \emptyset$ implies $J_{\mathfrak{m}}^i(k_v) \neq \emptyset$ by Lemma 2.13. Together (7) and (8) give the result. \square

4. THE DESCENT SETUP

We recall the following definition from [BPS16] (where the defined object is referred to as a *fake descent setup*).

Definition 4.1. *Let C be a nice curve over k . A **descent setup** for C is a triple (n, Δ, β) consisting of a positive integer n not divisible by the characteristic of k , a nonempty finite étale k -scheme $\Delta = \text{Spec } L$, and a divisor $\beta \in \text{Div}(C \times \Delta)$ such that $n\beta = \mathfrak{m} \times \Delta + \text{div}(f_{\mathfrak{m}})$ for some $\mathfrak{m} \in \text{Div}(C)$ and $f_{\mathfrak{m}} \in k(C \times \Delta)^\times$.*

If the divisor \mathfrak{m} appearing in the definition is effective, reduced and base point free, then (n, \mathfrak{m}) is a modulus setup, which we say is **associated to** (n, Δ, β) . For each $\delta \in \Delta(\bar{k})$, $\beta_\delta \in \text{Div}(C_{\bar{k}})$ is a divisor such that $n\beta_\delta - \mathfrak{m}$ is principal. So the class of β_δ in \mathcal{J} lies in $\mathcal{J}[n]$. This gives rise to a map $\text{Res}_\Delta \mathbb{Z}/n\mathbb{Z} \rightarrow \mathcal{J}[n]$ sending $\sum_{\delta \in \Delta(\bar{k})} c_\delta$ to the class of $\sum c_\delta \beta_\delta$. There is trace map $\text{Tr} : \text{Res}_\Delta \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ whose kernel we denote by $\text{Res}_\Delta^0 \mathbb{Z}/n\mathbb{Z}$. This fits into a commutative and exact diagram,

$$(4.1) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \text{Res}_\Delta^0 \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \text{Res}_\Delta \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\text{Tr}} & \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \parallel \\ 0 & \longrightarrow & J[n] & \longrightarrow & \mathcal{J}[n] & \xrightarrow{\frac{1}{n} \text{deg}} & \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \end{array}$$

Definition 4.2. *We say that (n, Δ, β) is an **n -descent setup** if the vertical maps in (4.1) are surjective and the divisors $\beta_\delta \in \text{Div}(C_{\bar{k}})$ are effective and have no common support.*

We note that if (n, Δ, β) is an n -descent setup, then the divisor \mathfrak{m} appearing in the definition is base point free, as it is linearly equivalent to each of the $n\beta_\delta$, which by assumption have no common support. Thus (n, \mathfrak{m}) is a modulus setup.

The following examples show that all of the modulus setups considered in Section 2 are associated to an n -descent setup. Details for Example D.1 and Example D.3 may be found in [BPS16, Examples 6.9], while Example D.2 is considered in [Cre14].

D.1 Suppose C is a double cover of \mathbb{P}^1 which is not ramified over ∞ . Let $\Delta(\bar{k})$ be the set of ramification points and take β to be the diagonal embedding of Δ in $C \times \Delta$. Then $(2, \Delta, \beta)$ is a 2-descent setup. Taking \mathfrak{m} be the pullback of $\infty \in \text{Div}(\mathbb{P}^1)$ we recover the modulus setup in Example M.1.

D.2 Suppose C is a genus 1 curve of degree n in \mathbb{P}^{n-1} (or equivalently, a genus 1 curve together with the linear equivalence class of a k -rational divisor of degree n). We obtain an n -descent setup by taking Δ to be the set of n^2 flex points (i.e. points $x \in C(\bar{k})$ such that $n \cdot x$ is a hyperplane section) and β to be the diagonal embedding of Δ in $C \times \Delta$. Taking \mathfrak{m} to be a generic hyperplane section recovers the modulus setup in Example M.2.

D.3 Suppose C is a nonhyperelliptic curve of genus ≥ 2 . We obtain a 2-descent setup for C by taking Δ to be the Gal_k -set of odd theta characteristics. A theta characteristic

is a line bundle θ on C whose square is the canonical bundle. By definition θ is odd if $h^0(X, \theta) \equiv 1 \pmod{2}$, which implies in particular that θ may be represented by an effective divisor. By [BPS16, Proposition 5.8] there is some effective $\beta \in \text{Div}(C \times \Delta)$ such that $[\beta_\delta] = \delta$ for $\delta \in \Delta(\bar{k})$. We can take \mathfrak{m} to be an effective canonical divisor and thus recover the modulus setup in Example M.3.

4.1. Descent maps. Let C be a nice curve over k with an n -descent setup (n, Δ, β) and associated modulus setup (n, \mathfrak{m}) . Let L denote the étale algebra corresponding to Δ , i.e., $\Delta = \text{Spec } L$. Call a divisor on C **good** if its support is disjoint from \mathfrak{m} and all β_δ .

Lemma 4.3. *Let $f_{\mathfrak{m}} \in k(C \times \Delta)^\times$ be as in Definition 4.1. Evaluation of $f_{\mathfrak{m}}$ at good divisors induces homomorphisms*

$$f_{\mathfrak{m}} : \text{Pic}_{C_{\mathfrak{m}}}(k) \rightarrow L^\times/L^{\times n}, \quad \text{and} \quad f_{\mathfrak{m}} : \text{Pic}(C) \rightarrow L^\times/k^\times L^{\times n}.$$

Proof. By Lemma 2.13 and the moving lemma, all elements of $\text{Pic}_{C_{\mathfrak{m}}}(k)$ can be represented by a good k -rational divisor and $\text{Pic}(C)$ is the image of $\text{Pic}_{C_{\mathfrak{m}}}(k)$. Suppose D is a good k -rational divisor and $D = \text{div}(g)$ for some $g \in k(C)^\times$. By Weil reciprocity $f_{\mathfrak{m}}(D) = g(\text{div}(f_{\mathfrak{m}})) = g(n\beta - \mathfrak{m} \times \Delta) = N(g|_{\mathfrak{m}})^{-1}g(\beta)^n \in k^\times L^{\times n}$. This shows that the second map is well defined. If the class of D is trivial in $\text{Pic}_{C_{\mathfrak{m}}}(k)$, then there is such a g with $g|_{\mathfrak{m}} = 1$ (cf. Lemma 2.5), so that $f_{\mathfrak{m}}(D) \in L^{\times n}$. \square

Dualizing (4.1) and taking Galois cohomology yields a commutative and exact diagram,

$$(4.2) \quad \begin{array}{ccccccc} \mathrm{H}^1(T'[\varphi]) & \longrightarrow & \mathrm{H}^1(A_{\mathfrak{m}}[\varphi]) & \longrightarrow & \mathrm{H}^1(J[n]) & \xrightarrow{\Upsilon} & \mathrm{H}^2(T'[\varphi]) \\ \parallel & & \downarrow \alpha_{\mathfrak{m}} & & \downarrow \alpha & & \parallel \\ k^\times/k^{\times n} & \longrightarrow & L^\times/L^{\times n} & \longrightarrow & \mathrm{H}^1\left(\frac{\text{Res}_\Delta \mu_n}{\mu_n}\right) & \longrightarrow & \text{Br}(k)[n] \end{array}$$

This is related to the maps in Lemma 4.3 and φ -coverings as follows.

Theorem 4.4. *For $i \in \{0, 1\}$ there is an $\alpha_{\mathfrak{m}}$ -equivariant map $\alpha_{\mathfrak{m}}^i : \text{Cov}^\varphi(J_{\mathfrak{m}}^i) \rightarrow L^\times/L^{\times n}$, functorial in k and such that for any $(F_{\mathfrak{m}}, \pi) \in \text{Cov}^\varphi(J_{\mathfrak{m}}^i)$ and $P \in \pi(F_{\mathfrak{m}}(k))$ we have $\alpha_{\mathfrak{m}}(F_{\mathfrak{m}}, \pi) = f_{\mathfrak{m}}(P)$.*

We prove the cases $i = 0$ and $i = 1$ separately below, after making some remarks and stating two corollaries that will be used in the following section. Proofs of the corollaries follow the proof of the theorem.

Remark 4.5. *The set of rational points on $J_{\mathfrak{m}}^i$ may be partitioned as*

$$J_{\mathfrak{m}}^i(k) = \coprod_{(F_{\mathfrak{m}}, \pi) \in \text{Cov}^\varphi(J_{\mathfrak{m}}^i)} \pi(F_{\mathfrak{m}}(k)).$$

The theorem says that the map $f_{\mathfrak{m}} : \text{Pic}_{C_{\mathfrak{m}}}^i(k) = J_{\mathfrak{m}}^i(k) \rightarrow L^\times/L^{\times n}$ is constant on each of the sets appearing in this partition and that the value on each is equal to the image of the corresponding covering under $\alpha_{\mathfrak{m}}^i$.

Corollary 4.6. *For $i \in \{0, 1\}$ there is an α -equivariant map $\alpha^i : \text{Cov}_{\mathfrak{m}}^n(J^i) \rightarrow L^\times/k^\times L^{\times n}$, functorial in k and such that for any $(F, \pi) \in \text{Cov}_{\mathfrak{m}}^n(J^i)$ and $P \in \pi(F(k)) \cap \text{Pic}^i(C)$ we have $\alpha^i(F, \pi) = f_{\mathfrak{m}}(P)$.*

Corollary 4.7. *There is an α -equivariant map $\alpha^1 : \text{Cov}_m^n(C) \rightarrow L^\times/k^\times L^{\times n}$, functorial in k and such that for any $(X, \pi) \in \text{Cov}_m^n(C)$ and $P \in \pi(X(k))$ we have $\alpha^1(X, \pi) = f_m(P)$.*

Remark 4.8. *There are partitions of the sets of rational points*

$$C(k) = \coprod_{(X, \pi) \in \text{Cov}_m^n(C)} \pi(X(k)) \quad \text{and} \quad J^i(k) = \coprod_{(F, \pi) \in \text{Cov}_m^n(C)} \pi(F(k))$$

By Corollary 3.9, $\text{Cov}_{\text{sol}}^n(C) \subset \text{Cov}_m^n(C)$, so Corollary 4.7 says that the map $f_m : C(k) \rightarrow L^\times/k^\times L^{\times n}$ is constant on each of the sets appearing in this partition and that the value on each is equal to the image of the corresponding covering under the descent map. A similar statement holds for J^i , provided $\text{Pic}^i(C) = J^i(k)$, in which case $\text{Cov}_{\text{sol}}^n(J^i) \subset \text{Cov}_m^n(J^i)$ by Lemma 3.6 and Corollary 3.10.

Remark 4.9. *The subgroup $J(k)_\bullet = \ker(\Upsilon \circ d) \subset J(k)$ is the largest subgroup of $J(k)$ on which one can define a homomorphism $f : J(k)_\bullet \rightarrow L^\times/k^\times L^{\times 2}$ such that f agrees with f_m on $\text{Pic}^0(C)$ and $f \circ d$ agrees with $\alpha^0 \circ d$ as in Corollary 4.6. This follows from a diagram chase in (4.2). Corollary 2.12 shows that $J(k)_\bullet = J(k)$ when C is a nonhyperelliptic curve defined over a local or global field and has 2-descent setup as in Example D.3. This is rather surprising given that it is not generally true that $J(k) = \text{Pic}^0(C)$ and, moreover, that $J(k)_\bullet = \text{Pic}^0(C)$ for a hyperelliptic curve with 2-descent setup as in Example D.1 (see [PS97, Corollary 10.6]). It would be very interesting to determine how this extended map f could be computed explicitly over, say, a local field.*

Proof of Theorem 4.4 in the case $i = 0$. Let $d_m : J_m(k) \rightarrow H^1(A_m[\varphi])$ denote the connecting homomorphism from the exact sequence $0 \rightarrow A_m[\varphi] \rightarrow A_m \rightarrow J_m \rightarrow 0$. Under the identification $H^1(A_m[\varphi]) = \text{Cov}^\varphi(J_m)$, the coboundary map d_m sends $P \in J_m(k)$ to the class of the φ -covering $A_m \rightarrow J_m$ given by $Q \mapsto \varphi(Q) + P$. So the following lemma proves Theorem 4.4 in the case $i = 0$. \square

Lemma 4.10. *The composition $J_m(k) \xrightarrow{d_m} H^1(A_m[\varphi]) \xrightarrow{\alpha} L^\times/L^{\times n}$ is equal to f_m .*

Proof. Let $D \in \text{Div}_m(C)$ be a good divisor representing $P \in J_m(k)$. Choose a good divisor $E \in \text{Div}_m(C_{\bar{k}})$ such that $nE - D = \text{div}(g)$ for some $g \in \bar{k}(C_{\bar{k}})^\times$ with $g|_m = 1$. This is possible since $J_m(\bar{k})$ is a divisible group. Then $d_m(P)$ is represented by the 1-cocycle $\xi_\sigma = [\sigma E - E] \in A_m[\varphi]$. Note that $\text{div}(\sigma g/g) = n(\sigma E - E)$. The image of ξ under $\alpha : H^1(A_m[\varphi]) \rightarrow H^1(\text{Res}_\Delta \mu_n)$ is represented by $e(\xi_\sigma, \beta)$, where e is the pairing defined in Proposition 2.8. From the definition of the e pairing we have

$$e(\xi_\sigma, \beta) = f_m(\sigma E - E)/(\sigma g/g)(\beta) = \sigma b/b,$$

where $b = f_m(E)/g(\beta)$. Thus, the image of $\alpha(\xi)$ under $H^1(\text{Res}_\Delta \mu_n) \simeq L^\times/L^{\times n}$ is represented by $b^n = f_m(nE)/g(n\beta) = f_m(D + \text{div}(g))/g(\mathfrak{m} \times \Delta + \text{div}(f_m)) = f_m(D)/g(\mathfrak{m} \times \Delta) = f_m(D)$, where the last two equalities follow from Weil reciprocity and the fact that $g|_m = 1$, respectively. \square

Proof of Theorem 4.4 in the case $i = 1$. Given $(F_m, \rho) \in \text{Cov}^\varphi(J_m^1)$, let $(Y, \pi) \in \text{Cov}^\varphi(C)$ be its image under the pullback map. As in the proof of Proposition 3.3 the extension $\bar{k}(Y_{\bar{k}})$ contains n -th roots g_δ of $f_{m, \delta}$ for each $\delta \in \Delta(\bar{k})$. Evidently $\text{div}(\sigma(g_\delta)) = \text{div}(g_{\sigma(\delta)})$ for any $\sigma \in \text{Gal}_k$, so by Hilbert's Theorem 90 there is a function $h \in k(Y \times \Delta)^\times$ such that $\text{div}(g_\delta) = \text{div}(h_\delta)$. Then $\pi^* f_m/h^n \in k(Y \times \Delta)^\times$ has trivial divisor, so must equal some

constant function $c \in L^\times = k(\Delta)^\times$. The class of c in $L^\times/L^{\times n}$ is independent of the choice for h . Thus we have a well defined map $\alpha^1 : \text{Cov}^\varphi(J_m^1) \rightarrow L^\times/L^{\times n}$ sending (F_m, ρ) to the class of c .

Now suppose $D \in \text{Div}^1(C)$ is a good divisor. For each $P \in C(\bar{k})$ in the support of D choose some $P' \in Y(\bar{k})$ such that $\pi(P') = P$ and set $D' = \sum_P \text{ord}_P(D)P' \in \text{Div}(\bar{Y})$. Let $\sigma \in \text{Gal}_k$. Since D is k -rational we can write ${}^\sigma(D') = \sum_P \text{ord}_P(D)P'_\sigma$ with $\pi(P'_\sigma) = P$. The restriction of π to the open subscheme $Y_0 = Y - \pi^{-1}(\mathfrak{m})$ is an $A_m[\varphi]$ -torsor over $C_0 = C - \mathfrak{m}$. Thus, for each $P \in \text{Supp}(D)$ and $\sigma \in \text{Gal}_k$ there is a unique $\gamma_{P,\sigma} \in A_m[\varphi](\bar{k})$ such that $\gamma_{P,\sigma} \cdot P' = P'_\sigma$. Set $\gamma_\sigma = \sum_P \text{ord}_P(D)\gamma_{P,\sigma}$, which we interpret as a 1-cocycle taking values in $A_m[\varphi]$. Since $\pi(D') = D$, γ_σ represents the class in $H^1(A_m[\varphi])$ of the torsor $\rho^{-1}([D]) \subset F_m$.

From the relation defining c we have $f_m(D)/c = f_m \circ \pi(D')/c = h(D')^n$. This represents a class in $H^1(\text{Res}_\Delta \mu_n)$ given by the 1-cocycle

$$\eta_\sigma = {}^\sigma(h(D'))/h(D') = h({}^\sigma D')/h(D') = \prod_P [h(\gamma_{P,\sigma} \cdot P')/h(P')]^{\text{ord}_P(D)}.$$

By Lemma 3.5 this can be expressed in terms of the extended Weil pairing of Proposition 2.8 as

$$\eta_\sigma = \prod_P e(\gamma_{P,\sigma}, \beta)^{\text{ord}_P(D)} = e(\gamma_\sigma, \beta).$$

This also represents the image of γ_σ under the map $\alpha : H^1(A_m[\varphi]) \rightarrow H^1(\text{Res}_\Delta \mu_n)$. Thus, $f_m(D)/c = f_m(D)/\alpha^1(F_m, \rho)$ is equal to $\alpha(\rho^{-1}([D]))$. In particular, $f_m(D) = \alpha^1(F_m, \rho)$ whenever the fiber $\rho^{-1}([D])$ contains a k -point. This is the property stated in the theorem.

Let us show that α_m^1 is α_m -equivariant. Suppose (Y_ξ, π_ξ) is the twist of (Y, π) by $\xi \in H^1(k, A_m[\varphi])$. By definition there is an isomorphism $\psi : (Y_\xi)_{\bar{k}} \rightarrow Y_{\bar{k}}$ such that $\pi \circ \psi = \pi_\xi$ and ${}^\sigma \psi(x) = \xi_\sigma \cdot \psi(x)$ for any $\sigma \in \text{Gal}_k$, where $\xi_\sigma \in A_m[\varphi] \simeq \text{Aut}(Y_{\bar{k}}/C_{\bar{k}})$. Let h, c and h_ξ, c_ξ be as in the definition of α_m^1 . We must show that c_ξ/c and $\alpha(\xi)$ give the same class in $L^\times/L^{\times n} \simeq H^1(\text{Res}_\Delta \mu_n)$. We have $c_\xi h_\xi^n = \pi_\xi^* f_m = (\pi \circ \psi)^* f_m = c(h \circ \psi)^n$. Thus, $c_\xi/c = (h(\psi(Q))/h_\xi(Q))^n$, for any $Q \in Y_\xi(\bar{k})$ where this expression is defined and nonzero. So the class of c_ξ/c in $L^\times/L^{\times n} \simeq H^1(\text{Res}_\Delta \mu_n)$ is represented by the 1-cocycle

$$\begin{aligned} \nu_\sigma &= {}^\sigma \left(\frac{h(\psi(Q))}{h_\xi(Q)} \right) \left(\frac{h_\xi(Q)}{h(\psi(Q))} \right) = \left(\frac{h(\xi_\sigma \cdot \psi(\sigma Q))}{h(\psi(Q))} \right) \left(\frac{h_\xi(Q)}{h_\xi(\sigma Q)} \right) \\ &= \left(\frac{h(\xi_\sigma \cdot \psi(\sigma Q))}{h(\psi(\sigma Q))} \right) \underbrace{\left(\frac{h(\psi(\sigma Q))}{h_\xi(\sigma Q)} \right)}_{c_\xi/c} \underbrace{\left(\frac{h_\xi(Q)}{h(\psi(Q))} \right)}_{c/c_\xi} = \left(\frac{h(\xi_\sigma \cdot \psi(\sigma Q))}{h(\psi(\sigma Q))} \right) \\ &= e(\xi_\sigma, \beta) = \alpha(\xi_\sigma), \end{aligned}$$

where the final line follows from Lemma 3.5 as above. \square

Proof of Corollary 4.6. If two elements of $\text{Cov}^\varphi(J_m^i)$ have the same image in $\text{Cov}_m^n(J^i)$, then their images under α_m^i differ by an element in $k^\times/(L^{\times n} \cap k^\times)$. This follows from the exactness of (4.2) and α_m -equivariance of α_m^i . Thus there is a unique map α^i fitting into the

commutative diagram

$$\begin{array}{ccccc}
J_m^i(k) & \xrightarrow{d_m} & \text{Cov}^\varphi(J_m^i) & \xrightarrow{\alpha_m^i} & L^\times/L^{\times n} \\
\downarrow s & & \downarrow q & & \downarrow \\
\text{Pic}^i(C) & \xrightarrow{d} & \text{Cov}_m^n(J^i) & \xrightarrow{\alpha^i} & L^\times/k^\times L^{\times n}
\end{array}$$

Here the maps d_m and d are defined by $d_m(P) = [A_m \ni Q \mapsto \varphi(Q) + P \in J^i]$ and $d(P) = [J \ni Q \mapsto nQ + P \in J^i]$. Note that in the case $i = 0$ these agree with the usual connecting homomorphisms. The map s is induced by the canonical map $\text{Pic}_{C_m}(k) \rightarrow \text{Pic}_C(k)$, and is surjective by Lemma 2.13. Theorem 4.4 shows that the composition along the top row is the map f_m of Lemma 4.3. Hence, the same is true of the bottom row. Thus α^i has all of the required properties. \square

Proof of Corollary 4.7. The pullback map $p : \text{Cov}_m^n(J^1) \rightarrow \text{Cov}_m^n(C)$ is a bijection by Lemma 3.4. Define $\alpha^1(X, \pi) = \alpha^1(F, \pi)$ where (X, π) is the pullback of (F, π) . The required properties follow immediately from Corollary 4.6. \square

5. FAKE SELMER SETS

When k is a global field with completions k_v the map f_m induces a commutative diagram,

$$(5.1) \quad \begin{array}{ccc}
\text{Pic}(C) & \xrightarrow{f_m} & \frac{L^\times}{k^\times L^{\times n}} \\
\downarrow & & \downarrow \prod \text{res}_v \\
\prod_v \text{Pic}(C_{k_v}) & \xrightarrow{\prod f_{m,v}} & \prod \frac{(L \otimes k_v)^\times}{k_v^\times (L \otimes k_v)^{\times n}}
\end{array}$$

Definition 5.1. *Suppose k is a global field. For any integer i , the fake Selmer set of J^i is the set*

$$\text{Sel}_{\text{fake}}^{f_m}(J^i) := \{ l \in L^\times/k^\times L^{\times n} : \text{res}_v(l) \in f_{m,v}(\text{Pic}^i(C_{k_v})), \text{ for all } v \}.$$

The fake Selmer set of C is the set

$$\text{Sel}_{\text{fake}}^{f_m}(C) := \{ l \in L^\times/k^\times L^{\times n} : \text{res}_v(l) \in f_{m,v}(C(k_v)), \text{ for all } v \}.$$

Theorem 5.2. *Suppose C is defined over a global field. If $\text{Sel}_{\text{fake}}^{f_m}(C) = \emptyset$, then $\text{Sel}^n(C) = \emptyset$.*

Proof. By Corollary 3.9, $\text{Cov}_{\text{sol}}^n(C_{k_v}) \subset \text{Cov}_m^n(C_{k_v})$ for each v and $\text{Sel}^n(C) \subset \text{Cov}_m^n(C)$. By Corollary 4.7 we have $f_m(C(k_v)) = \alpha^1(\text{Cov}_{\text{sol}}^n(C_{k_v}))$. Thus $\alpha^1(\text{Sel}^n(C)) \subset \text{Sel}_{\text{fake}}^{f_m}(C)$. \square

Theorem 5.3. *Suppose C is defined over a global field and $\text{Div}^1(C_{k_v}) \neq \emptyset$ for all primes v of k . If $\text{Sel}_{\text{fake}}^{f_m}(J^1) = \emptyset$, then $\text{Sel}^n(J^1) = \emptyset$.*

Proof. As noted in the proof of Lemma 2.11 we have $\Theta_C(x) = \langle x, [J^1] \rangle$. So the assumption on $\text{Div}^1(C_{k_v})$ implies that $\text{Pic}^0(C_{k_v}) = J(k_v)_\bullet = J(k_v)$. Thus the hypothesis of Corollary 3.10 is satisfied and so $\text{Sel}^n(J^1) \subset \text{Cov}_m^n(J^1)$. The property of α^1 given in Theorem 4.4 together with Corollary 3.10 gives that $f_{m,v}(\text{Pic}^1(C_{k_v})) = \alpha^1(\text{Cov}_{\text{sol}}^n(J_{k_v}^1))$. It follows that $\alpha^1(\text{Sel}^n(J)) \subset \text{Sel}_{\text{fake}}^{f_m}(J^1)$, which gives the result. \square

Remark 5.4. *The conclusion of the theorem implies that J^1 represents a nontrivial element in $\text{III}(J)/n\text{III}(J)$, not just in $\text{III}(J)$. Together with well known properties of the Cassels-Tate pairing this allows one to deduce better lower bounds for $\text{III}(J)$ and hence better upper bounds for the rank of $J(k)$. This is illustrated in the example in Section 6.1.*

Remark 5.5. *When C has a descent setup as in Example D.1 and Example D.2 a proof of Theorem 5.3 can be found in [Cre13, Prop. 5.4] and [Cre14, Theorem 5.2], respectively.*

5.1. Descent on J . The results of [BPS16, Section 10] show that from knowledge of $\text{Sel}_{\text{fake}}^{f_m}(J)$ one can often determine $\text{Sel}^n(J)$. For this to work one must at least have that $\alpha(\text{Sel}^n(J))$ is contained in the image of $L^\times/k^\times L^{\times n}$ (cf. (4.2)) or, equivalently, $\text{Sel}^n(J) \subset \ker(\Upsilon) = \text{Cov}_m^n(J)$. This can be ensured by imposing hypotheses on C such as [BPS16, Hypothesis 10.1] that the map $\text{Pic}^0(C) \rightarrow J(k)/nJ(k)$ is surjective both globally and locally. The results of Section 2 allow us to extract information concerning $\text{Sel}^n(J)$ in a number of cases where [BPS16, Hypothesis 10.1] does not hold.

Theorem 5.6. *Suppose C is defined over a global field k and $J^2(k) \neq \emptyset$. Let N be the number of primes v such that $\text{coker}(\text{Pic}^0(C_{k_v}) \rightarrow J(k_v)/2J(k_v)) \neq 0$. Suppose that either of the following holds*

- (1) *C is a nonhyperelliptic curve with a 2-descent setup as in Example D.3, or*
- (2) *C is a hyperelliptic curve with a 2-descent setup as in Example D.1 and $N \leq 1$.*

Then

$$\dim_{\mathbb{F}_2}(\alpha(\text{Sel}^2(J))) \leq \dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}^{f_m}(J) + \max\{0, N - 1\}.$$

Remark 5.7. *The kernel of $\alpha : \text{H}^1(J[2]) \rightarrow \text{H}^1(\text{Res}_\Delta \mu_2/\mu_2)$ can be computed from the Galois action on Δ , thus allowing us to extract upper bounds for $\dim_{\mathbb{F}_2}(\text{Sel}^2(J))$ as well.*

Proof. For each prime v , let $M_v := \text{coker}(\text{Pic}^0(C_{k_v}) \rightarrow J(k_v)/2J(k_v))$ and let T be the (finite) set of primes where M_v is nontrivial. In the nonhyperelliptic case we have $\ell = g - 1$ by Corollary 2.12, so $J(k_v)_\bullet = J(k_v)$ for all primes v . In the hyperelliptic case the assumption $N \leq 1$ implies $J(k_v)_\bullet = J(k_v)$ fails for at most one prime v . In both cases $\text{Sel}^n(J) \subset \text{Cov}_m^n(J)$ by Corollary 3.7.

For $v \notin T$ we have $\text{Pic}^0(C_{k_v}) = J(k_v)_\bullet = J(k_v)$ and $f_m(\text{Pic}^0(C_{k_v})) = \alpha^0(\text{Cov}_{\text{sol}}^n(J_{k_v}))$ by Lemma 3.6 and Theorem 4.6. So if $T = \emptyset$, then we have $\alpha(\text{Sel}^n(J)) \subset \text{Sel}_{\text{fake}}^{f_m}(J)$ and the result holds.

Let us assume $N = \#T > 0$. Let $K_v := \alpha(d(J(k_v)))$, $\Lambda_v := f_m(\text{Pic}^0(C_{k_v}))$. Identifying $J(k_v)/2J(k_v)$ with its image under d and using Lemma 4.10 we obtain a commutative diagram of \mathbb{F}_2 -linear maps

$$\begin{array}{ccccc} \text{Sel}^2(J) & \longrightarrow & \bigoplus_{v \in T} J(k_v)/2J(k_v) & \longrightarrow & \bigoplus_{v \in T} M_v \\ \downarrow \alpha & & \downarrow \alpha & & \downarrow \alpha \\ \alpha(\text{Sel}^2(J)) & \longrightarrow & \bigoplus_{v \in T} K_v & \longrightarrow & \bigoplus_{v \in T} K_v/\Lambda_v \end{array}$$

The maps $\Theta_{C_{k_v}}$ of (2.13) induce an isomorphism $\bigoplus M_v \rightarrow \bigoplus \text{Br}(k_v)[2] \simeq \mathbb{F}_2^N$. Since $J^2(k) \neq \emptyset$, $[J^1] \in \text{H}^1(J)[2]$. Therefore, there is a lift η of $[J^1]$ to $\text{H}^1(J[2])$. Given $\xi \in \text{Sel}^2(J)$ let $b = \xi \cup_e \eta \in \text{Br}(k)$ and for $v \in T$ let $x_v \in J(k_v)$ be such that $d(x_v) = \text{res}_v(\xi)$. Compatibility of the Tate pairing with the Weil pairing cup product (as noted in the proof of Lemma 2.11)

gives $\text{res}_v(b) = \langle d(x_v), [(J^1)_{k_v}] \rangle = \Theta_{C_{k_v}}(x_v)$. Therefore global reciprocity in $\text{Br}(k)$ implies that the image of $\text{Sel}^2(J)$ in $\bigoplus M_v \simeq \mathbb{F}_2^N$ is contained in a hyperplane. Since the vertical map on the right is surjective, this shows that the rank of the composition along the bottom row of the diagram is at most $N - 1$. On the other hand, the kernel is $\text{Sel}_{\text{fake}}^{\text{fm}}(J)$. \square

Here is an instance where we can prove that $J(k_v) \neq \text{Pic}^0(C_{k_v})$.

Lemma 5.8. *Suppose that C is a curve of genus g and either*

- (1) *k is a local field such that $J^1(k) = \emptyset$, or*
- (2) *C is defined over a global field K and $k = K_v$ is the unique completion of K such that $\text{Pic}^1(C_k) = \emptyset$. Assume further that $\text{Div}^{g-1}(C_{K_v}) \neq \emptyset$ for all primes v .*

Then $\text{coker}(\text{Pic}^0(C_k) \rightarrow J(k)/2J(k)) \neq 0$.

Proof. The map Θ_C is related to the Tate pairing by the rule $\Theta_C(x) = \langle x, [J^1] \rangle$. The assumption in (1) is that $[J^1]$ is nontrivial in $H^1(J)$, so the result follows from nondegeneracy of the Tate pairing. In case (2), the second assumption implies that the Cassels-Tate pairing is alternating by [PS99, Corollary 11]. If $J^1(k) \neq \emptyset$, then $J^1 \in \text{III}(J)$ and [PS99, Theorem 11] shows that J^1 pairs nontrivially with itself, a contradiction. Hence the hypothesis of (1) is satisfied. \square

6. EXAMPLES

Computations in this section were performed with the Magma Computer Algebra System described in [BCP97].

6.1. Example of explicit descent on J^1 .

Theorem 6.1. *Let C denote the genus 3 curve in $\mathbb{P}_{\mathbb{Q}}^2$ given by the vanishing of*

$$x^4 + 5x^3y + 9x^3z + 9x^2y^2 + 9x^2yz + xy^3 - 8xy^2z - 8xz^3 - 6y^4 - 3y^3z - 8y^2z^2 - 2yz^3 - 3z^4$$

and let J be the Jacobian of C . Then, assuming the generalized Riemann hypothesis, $J(\mathbb{Q}) \simeq \mathbb{Z}$ and $\text{III}(J)[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Furthermore, the curve C has points everywhere locally, but has no \mathbb{Q} -rational divisors of odd degree.

Remark 6.2. *There are examples of smooth plane quartics having points everywhere locally, but no rational divisors of odd degree given in [Bre86]. These examples exploit the fact that the plane quartic in question admits a finite morphism to a genus 1 curve. As the Jacobian of the curve in Theorem 6.1 is absolutely simple, such techniques do not apply.*

Proof of Theorem 6.1. C has real points and the polynomial defining C has good reduction at all primes other than $q = 760567$. The point $(0 : 1948 : 1) \in C(\mathbb{F}_q)$ is smooth, and for all other primes p , $C(\mathbb{F}_p) \neq \emptyset$ (for $p > 37$ this follows from the Weil bounds). So by Hensel's lemma C and, hence, J^1 have points everywhere locally. This implies that $\text{Pic}^d(C) = J^d(\mathbb{Q})$ and $\text{Pic}^d(C_{\mathbb{Q}_p}) = J^d(\mathbb{Q}_p)$ for all primes p and $d \geq 0$.

Using Magma we compute that $|J(\mathbb{F}_2)| = 25$ and $|J(\mathbb{F}_3)| = 57$. Since these orders are relatively prime, we have $J(\mathbb{Q})_{\text{tors}} = 0$. A search for points of small height on C over $\mathbb{Q}(\sqrt{2})$ yields

$$D_1 = (\sqrt{2} - 2 : -\sqrt{2} + 1 : 1) \quad \text{and} \quad D_2 = (-1 : \sqrt{2}/2 : 1)$$

Then $D = \text{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(D_1 - D_2)$ is a \mathbb{Q} -rational divisor of degree 0 on C representing a point $P \in J(\mathbb{Q})$. The image of P under the reduction map $J(\mathbb{Q}) \rightarrow J(\mathbb{F}_7)$ is nontrivial. So P has infinite order and, hence, $J(\mathbb{Q})$ has rank at least 1.

To proceed further we compute $\text{Sel}_{\text{fake}}^{f_m}(J^0)$ and $\text{Sel}_{\text{fake}}^{f_m}(J^1)$ for the descent setup and modulus setup as in Example D.3 and Example M.3, taking Δ to be the set of bitangents to C and β to be the diagonal embedding of Δ into $\text{Div}(\overline{C}) \times \Delta$. The algebra L has degree 28 and, moreover, its Galois group is isomorphic to $\text{GSp}_6(\mathbb{F}_2)$, showing that the representation $\text{Gal}_{\mathbb{Q}} \rightarrow \text{GSp}(J[2])$ is surjective. A Magma computation (assuming GRH) gives that \mathcal{O}_L has trivial class group. The function f_m can be written as a ratio of linear forms $f_m = l/l_0$, with $l \in L[x, y, z]$ and $l_0 \in \mathbb{Q}[x, y, z]$. Since \mathcal{O}_L has trivial class group, we can scale l by an element of L^\times such that the coefficients of l are integral and generate the unit ideal in \mathcal{O}_L .

By [BPS16, Theorem 10.9], $\text{Sel}_{\text{fake}}^{f_m}(J)$ is contained in $L(\mathcal{S}, 2)$, the unramified outside \mathcal{S} subgroup of $L^\times/\mathbb{Q}^\times L^{\times 2}$ for $\mathcal{S} = \{2, 760567, \infty\}$. Since L has class number 1, we can determine representatives in L^\times for $L(\mathcal{S}, 2)$ from the \mathcal{S} -unit group of L (cf. [BPS16, Proposition 7.3]). The order of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ can be computed from the splitting of p in L . This gives an upper bound for the size of the image of $J(\mathbb{Q}_p)$ under f_m . For both nonarchimedean primes $p \in \mathcal{S}$, the differences of images of points in $C(\mathbb{Q}_p)$ already generate a subgroup whose order meets the upper bound, hence must be the image of $J(\mathbb{Q}_p)$. The subgroup of $L(\mathcal{S}, 2)$ mapping into the images of $J(\mathbb{Q}_p)$ for $p \in \mathcal{S}$ has \mathbb{F}_2 -dimension 3 and contains $\text{Sel}_{\text{fake}}^{f_m}(J)$. Since the representation $\text{Gal}_{\mathbb{Q}} \rightarrow \text{GSp}(J[2])$ is surjective, [BPS16, Theorem 10.14] gives the inequality $\dim_{\mathbb{F}_2} \text{Sel}^2(J) \leq \dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}(J) \leq 3$.

The local image $f_m(C(\mathbb{Q}_p))$ is unramified for p outside \mathcal{S} by [BPS16, Lemma 12.13]. Since f_m is a homomorphism, the local image $f_m(J^1(\mathbb{Q}_p))$ is the coset of $f_m(J(\mathbb{Q}_p))$ containing $f_m(C(\mathbb{Q}_p))$. It follows that $\text{Sel}_{\text{fake}}^{f_m}(J^1) \subset L(\mathcal{S}, 2)$. Moreover, $f_m(J^1(\mathbb{Q}_p))$ for $p \in \mathcal{S}$ are easily obtained by translating the $f_m(J(\mathbb{Q}_p))$ already computed. It turns out that the image of $L(\mathcal{S}, 2)$ in $(L \otimes \mathbb{Q}_2)^\times/\mathbb{Q}_2^\times(L \otimes \mathbb{Q}_2)^{\times 2}$ does not intersect $f_m(J^1(\mathbb{Q}_2))$. Hence, $\text{Sel}_{\text{fake}}^{f_m}(J^1) = \emptyset$. By Theorem 5.3 we have $\text{Sel}^2(J^1) = \emptyset$. In particular, the computation shows that there are no 2-coverings of J^1 with \mathbb{Q}_2 -points and \mathbb{Q}_p -points for all p outside \mathcal{S} .

Since C has points everywhere locally, the Cassels-Tate pairing on $\text{III}(J)$ is alternating by [PS99, Corollary 12]. It induces a nondegenerate alternating pairing on the finite group $\frac{\text{III}(J)[2]}{2\text{III}(J)[4]}$, which consequently has square order (see, for example, [Cre13, Corollary 4.6]). The $\mathbb{Q}(\sqrt{2})$ -points on C above show that $J^2(\mathbb{Q}) \neq \emptyset$. Since $2[J^1] = [J^2]$ in $\text{III}(J)$, we conclude that $[J^1] \in \text{III}(J)[2]$. The fact that $\text{Sel}^2(J^1) = \emptyset$ implies, moreover, that $[J^1]$ gives a nontrivial element of $\frac{\text{III}(J)[2]}{2\text{III}(J)[4]}$ (cf. Theorem 3.8(7)). We conclude that $\text{III}(J)[2^\infty]$ admits a direct summand isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. From the exact sequence

$$0 \rightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow \text{Sel}^2(J) \rightarrow \text{III}(J)[2] \rightarrow 0$$

we therefore obtain that $J(\mathbb{Q}) \simeq \mathbb{Z}$ and $\text{III}(J)[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. \square

6.2. Descent on J . The following theorem gives an example where we compute $\text{Sel}^2(J)$, despite the fact that [BPS16, Hypothesis 10.1] does not hold.

Theorem 6.3. *The genus 3 curve $C \subset \mathbb{P}_{\mathbb{Q}}^2$ defined by the vanishing of*

$$x^4 + 2x^3y + 2x^3z + 4x^2y^2 + 2x^2yz + 4x^2z^2 + 3xy^3 + 2xy^2z + 4xyz^2 + 3xz^3 + 2y^4 + 5y^2z^2 + yz^3 + 2z^4$$

has the following properties.

- (1) $C(\mathbb{Q}_p) \neq \emptyset$ for all $p \neq 3, \infty$.
- (2) $\text{Pic}^{\text{odd}}(C_{\mathbb{Q}_3}) = \emptyset$.
- (3) $\text{Pic}^{\text{odd}}(C_{\mathbb{R}}) = \emptyset$.
- (4) $J = \text{Jac}(C)$ has $\text{rank}(J(\mathbb{Q})) = 1$.

Proof. The verification of (1) is straightforward. To show $\text{Pic}^{\text{odd}}(C_{\mathbb{Q}_p}) = \emptyset$ for $p = 3, \infty$ it suffices to check that C has no points over \mathbb{Q}_p or any extension of \mathbb{Q}_p of degree 3. For this we simply list the finitely many extensions and check locally solubility over each. We use the descent setup and modulus setup as in Example D.3 and Example M.3, taking Δ to be the set of bitangents to C and β to be the diagonal embedding of Δ into $\text{Div}(\overline{C}) \times \Delta$. The algebra L has degree 28 and splits as a product of 2 quadratic fields (both isomorphic to $\mathbb{Q}(\sqrt{-15})$) and 3 octic fields. Let $R^\vee = \text{coker}(J[2] \rightarrow \text{Res}_\Delta \mu_2/\mu_2)$. As described in [BPS16, 12.6.6] we compute the Galois action on the bitangents, from which we find that $\dim_{\mathbb{F}_2} J[2](\mathbb{Q}) = \dim_{\mathbb{F}_2} R^\vee(\mathbb{Q}) = 2$ and $\dim_{\mathbb{F}_2}(\text{Res}_\Delta \mu_2/\mu_2)(\mathbb{Q}) = 4$. From the exact sequence

$$0 \rightarrow J[2](\mathbb{Q}) \rightarrow (\text{Res}_\Delta \mu_2/\mu_2)(\mathbb{Q}) \rightarrow R^\vee(\mathbb{Q}) \rightarrow H^1(\mathbb{Q}, J[2]) \xrightarrow{\alpha} H^1(\mathbb{Q}, \text{Res}_\Delta \mu_2/\mu_2)$$

we conclude that α is injective over \mathbb{Q} .

There are points $P_1 = (\eta : 1 : 0)$, $P_2 = (\eta : 0 : 1) \in C(\mathbb{Q}(\eta))$, where η is a primitive cube root of unity. The torsion subgroup of $J(\mathbb{Q})$ is 2-primary, as can be seen by computing $\#J(\mathbb{F}_p)$ for small primes of good reduction. The divisor $D := \text{Tr}_{\mathbb{Q}(\eta)/\mathbb{Q}}(P_1 - P_2)$ represents a point $[D] \in J(\mathbb{Q})$ which maps to an element of order 18 in $J(\mathbb{F}_7)$, showing that $[D]$ has infinite order. Thus we have a lower bound $3 \leq \dim_{\mathbb{F}_2} \text{Sel}^2(J)$. Moreover, the points P_i show that $\text{Div}^2(C) \neq \emptyset$ and so the conditions of Theorem 5.6 are satisfied.

The curve C has good reduction outside $\mathcal{S}_1 := \{3, 5, 1613\}$ so by [BPS16, Theorem 10.9], $\text{Sel}_{\text{fake}}^f(J)$ is contained in $L(\mathcal{S}, 2)$, the unramified outside \mathcal{S} subgroup of $L^\times/k^\times L^{\times 2}$ for $\mathcal{S} = \{2, 3, 5, 1613, \infty\}$. We compute $L(\mathcal{S}, 2)$ as described in [BPS16, Proposition 7.3]. Since the largest discriminant of a factor of L is of order 10^{28} , this can be done without assuming GRH. For $p \in \mathcal{T} = \{2, 5, 1613\}$ we compute the local images $f_m(\text{Pic}^0(C_{\mathbb{Q}_p})) = f_m(J(\mathbb{Q}_p))$ following the strategy of [BPS16, Remark 11.6] (i.e., compute the images of random points until the dimension of the subgroup they generate meets an upper bound determined in advance from the action of the decomposition group on the bitangents). The subgroup $S_{\mathcal{T}} \subset L(\mathcal{S}, 2)$ satisfying these local conditions at all primes in \mathcal{T} has dimension 5.

From the action of the decomposition group at $p = 3$ on the bitangents we determine that $J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ and its image under $\alpha \circ d$ have dimension 3. However, computing the images of differences of random elements of $\text{Pic}^2(C_{\mathbb{Q}_3})$ under f_m we are only able to generate a subgroup H_3 of dimension 2. The subgroup $S_{\mathcal{T}, H_3}$ of $S_{\mathcal{T}}$ restricting to H_3 has dimension 2.

We now consider two cases. If the map $\text{Pic}^0(C_{\mathbb{Q}_3}) \rightarrow J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ is surjective, then H_3 has codimension 1 in $f_m(\text{Pic}^0(C_{\mathbb{Q}_3}))$, so $\dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}^f(J) \leq \dim_{\mathbb{F}_2} S_{\mathcal{T}, H_3} + 1 = 3$ and Theorem 5.6 applies with $N \leq 1$ to give $\dim_{\mathbb{F}_2} \text{Sel}^2(J) \leq \dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}^f(J) \leq 3$. If the map $\text{Pic}^0(C_{\mathbb{Q}_3}) \rightarrow J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)$ is not surjective, then $H_3 = f_m(\text{Pic}^0(C_{\mathbb{Q}_3}))$, so $\dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}^f(J) \leq \dim_{\mathbb{F}_2} S_{\mathcal{T}, H_3} = 2$ and Theorem 5.6 applies with $N \leq 2$ to give the upper bound $\dim_{\mathbb{F}_2} \text{Sel}^2(J) \leq \dim_{\mathbb{F}_2} \text{Sel}_{\text{fake}}^f(J) + 1 \leq 3$.

In either case we have the upper bound $\dim_{\mathbb{F}_2} \text{Sel}^2(J) \leq 3$ which coincides with the lower bound obtained from the point search. Thus $\text{rank}(J(\mathbb{Q})) = 1$. \square

Remark 6.4. *The computation outlined in the proof above shows that the maps $\text{Pic}^0(C_{\mathbb{Q}_p}) \rightarrow J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ are either surjective for all p , or fail to be surjective for both $p = 3$ and $p = \infty$. In fact the latter is the case. To prove this one can compute $f_{\mathfrak{m}}(\text{Pic}^0(C_{\mathbb{Q}_p}))$ algorithmically as described in [BPS16, Section 11.1] for either $p = 3$ or $p = \infty$. This shows that the set $S_{\mathcal{T}, H_3} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ computed is equal to $\text{Sel}_{\text{fake}}^{f_{\mathfrak{m}}}(J)$. Since $J(\mathbb{Q})/2J(\mathbb{Q})$ has dimension 3 and injects into $\text{Sel}^2(J)$ we conclude that $J(\mathbb{Q}) \neq \text{Pic}^0(C)$.*

7. THE SET $\text{Cov}_{\mathfrak{m}}^n(C)$ FOR GENUS 1 AND HYPERELLIPTIC CURVES

Suppose C is a nice curve over k with a modulus setup (n, \mathfrak{m}) associated to an n -descent setup. In this section we show how the sets $\text{Cov}_{\mathfrak{m}}^n(C)$ and $\text{Cov}_{\mathfrak{m}}^n(J^1)$ generalize known constructions in the situations of Example D.1 and Example D.2. For genus 1 curves this allows us to relate the existence of φ -coverings to the period-index problem.

7.1. Existence of φ -coverings. The following theorem gives, for a modulus setup associated to an n -descent setup, several conditions that are equivalent to the existence of an element in $\text{Cov}_{\mathfrak{m}}^n(C)$.

Theorem 7.1. *Suppose (n, \mathfrak{m}) is a modulus setup for C associated to an n -descent setup (n, Δ, β) and let $\varphi : A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ be the isogeny in (2.7). The following are equivalent.*

- (1) *The class of $J_{\mathfrak{m}}^1$ in $H^1(J_{\mathfrak{m}})$ is divisible by φ .*
- (2) *There exists a φ -covering of $J_{\mathfrak{m}}^1$.*
- (3) *There exists a φ -covering of C .*
- (4) $\text{Cov}^{\varphi}(C) \neq \emptyset$.
- (5) $\text{Cov}_{\mathfrak{m}}^n(C) \neq \emptyset$.
- (6) $\text{Cov}_{\mathfrak{m}}^n(J^1) \neq \emptyset$.
- (7) *There exists an n -covering $\pi : X \rightarrow C$ with the property that $\pi^*\beta_{\delta}$ is linearly equivalent to a k -rational divisor, for some $\delta \in \Delta(\bar{k})$.*
- (8) *The maximal unramified abelian covering of $C_{\bar{k}}$ of exponent n descends to k and the image of the k -rational divisor class $\pi^*\beta_{\delta}$ in $\text{Br}(k)$ under the map Θ_X of (2.13) lies in the image of the map Υ of (2.11), for every maximal unramified abelian covering $\pi : X \rightarrow C$ of exponent n and every $\delta \in \Delta(\bar{k})$.*

Before giving the proof we state and prove two lemmas.

Lemma 7.2. *Suppose (n, \mathfrak{m}) is a modulus setup associated to an n -descent setup (n, Δ, β) and that $\pi : X \rightarrow C$ is an n -covering. The class of (X, π) in $\text{Cov}^n(C)$ lies in $\text{Cov}_{\mathfrak{m}}^n(C)$ if and only if $\pi^*\beta_{\delta}$ is linearly equivalent to a k -rational divisor, for some $\delta \in \Delta(\bar{k})$.*

Proof. Suppose $\pi : X \rightarrow C$ lifts to a φ -covering $Y \rightarrow C$. The subfield $k(X) \subset k(Y)$ corresponds to the subgroup $\mu_n = T'[\varphi] \subset A_{\mathfrak{m}}[\varphi]$. The extension $k(X) \subset k(Y)$ is therefore obtained by adjoining to $k(X)$ an n -th root of a function f such that $\text{div}(f) = nD - \pi^*d\mathfrak{m}$, for some $d \in \mathbb{Z}$ and $f \in k(X)^{\times}$. Furthermore, we can arrange that $d = 1$. Indeed, we must have $\text{gcd}(n, d) = 1$, otherwise there would be a proper unramified intermediate extension of $k(X) \subset k(Y)$. Hence $\pi^*\mathfrak{m} = nD + \text{div}(f)$ for some $D \in \text{Div}(X)$ and $f \in k(X)^{\times}$. Recall that $n\beta - \mathfrak{m} \times \Delta = \text{div}(f_{\mathfrak{m}})$. So, for any $\delta \in \Delta(\bar{k})$, the function $h := f/\pi^*(f_{\mathfrak{m}, \delta}) \in \bar{k}(X_{\bar{k}})^{\times}$ has divisor $n(D - \pi^*\beta_{\delta})$. Since adjoining an n th root of h to $\bar{k}(X_{\bar{k}})$ gives an unramified

intermediate field of $\bar{k}(X_{\bar{k}}) \subset \bar{k}(Y_{\bar{k}})$, we must have $h \in \bar{k}(X_{\bar{k}})^{\times n}$. This shows that $D - \pi^* \beta_\delta$ is principal.

For the other direction, suppose $D \in \text{Div}(X)$ is a k -rational divisor linearly equivalent to $\pi^* \beta_\delta$. Then $\text{div}(\pi^* f_{\mathfrak{m}, \delta}) = n\pi^* \beta_\delta - \pi^* \mathfrak{m} = nD - \pi^* \mathfrak{m} + \text{div}(f)$, for some $f \in \bar{k}(X_{\bar{k}})^\times$. Thus, the divisor $nD - \pi^* \mathfrak{m} \in \text{Div}(X)$ is principal and k -rational. By Hilbert's Theorem 90 it is the divisor of some k -rational function $g \in k(X)^\times$. Let $Y \rightarrow X$ be the covering obtained by adjoining an n -th root of g to $k(X)$. Over \bar{k} we see that $\bar{k}(Y)$ is the compositum of $\bar{k}(X_{\bar{k}})$ and $\bar{k}(C_{\bar{k}})(\sqrt[n]{f_{\mathfrak{m}, \delta}})$, so $Y \rightarrow C$ is a φ -covering of C . \square

Lemma 7.3. *Suppose $\pi : X \rightarrow C$ is an n -covering and $\pi_z : X_z \rightarrow C$ is the twist by the cocycle $z \in Z^1(J[n])$. Let Θ_X and Θ_{X_z} denote the maps from (2.13) and let Υ denote the map in (2.11). For any $\delta \in \Delta(\bar{k})$,*

$$\Upsilon([z]) = \Theta_{X_z}(\pi_z^* \beta_\delta) - \Theta_X(\pi^* \beta_\delta).$$

Proof. There is an isomorphism of coverings $\rho : \bar{X}_z \rightarrow \bar{X}$ with the property that ${}^\sigma \rho \circ \rho^{-1} = T_{z_\sigma} \in \text{Aut}(\bar{X}/C_{\bar{k}})$ is translation by $z_\sigma \in J[n]$, for every $\sigma \in \text{Gal}_k$. Let $W = \pi_z^* \beta_\delta$ and $W' := \rho^*(W) = \pi^* \beta_\delta$. These represent Galois invariant divisor classes, hence, for any $\sigma \in \text{Gal}_k$ there are functions $f_\sigma \in \bar{k}(X_z)^\times$ and $g_\sigma \in \bar{k}(X)^\times$ with $\text{div}(f_\sigma) = {}^\sigma W - W$ and $\text{div}(g_\sigma) = {}^\sigma W' - W'$. The classes in $\text{Br}(k)$ of W and W' are given by the 2-cocycles

$$a_{(\sigma, \tau)} = \frac{{}^\sigma f_\tau \cdot f_\sigma}{f_{\sigma\tau}} \quad \text{and} \quad a'_{(\sigma, \tau)} = \frac{{}^\sigma g_\tau \cdot g_\sigma}{g_{\sigma\tau}},$$

both of which take values in \bar{k}^\times . Since $f_\sigma / \rho^* g_\sigma \in \bar{k}^\times$, the computation

$$\frac{a_{(\sigma, \tau)}}{a'_{(\sigma, \tau)}} = \frac{a_{(\sigma, \tau)}}{\rho^*(a'_{(\sigma, \tau)})} = \underbrace{\sigma \left(\frac{f_\tau}{\rho^* g_\tau} \right) \cdot \frac{f_\sigma}{\rho^* g_\sigma} \cdot \frac{\rho^* g_{\sigma\tau}}{f_{\sigma\tau}} \cdot \frac{{}^\sigma(\rho^* g_\tau)}{\rho^*({}^\sigma g_\tau)}}{\text{coboundary}}$$

shows that $\Theta_{X_z}(W) - \Theta_X(W')$ is represented by the 2-cocycle $\eta \in Z^2(\text{Gal}_k, \bar{k}^\times)$ defined by

$$\eta_{(\sigma, \tau)} = \frac{{}^\sigma(\rho^* g_\tau)}{\rho^*({}^\sigma g_\tau)} = \frac{{}^\sigma g_\tau \circ {}^\sigma \rho}{{}^\sigma g_\tau \circ \rho}.$$

Using that $(\rho^{-1})^*$ is the identity on $\bar{k} \subset \bar{k}(Y)$ and that ${}^\sigma \rho \circ \rho^{-1} = T_{z_\sigma}$ we have $\eta_{(\sigma, \tau)} = \frac{{}^\sigma g_\tau \circ T_{z_\sigma}}{{}^\sigma g_\tau}$. We recognize this as the Weil pairing $\eta_{(\sigma, \tau)} = e_n({}^\sigma P_\tau, z_\sigma)$, where $P_\tau \in J[n]$ is the class represented by the divisor ${}^\tau \beta_\delta - \beta_\delta$ (see Lemma 3.5). The cocycle $P_\tau \in Z^1(\text{Gal}_k, J[n])$ represents $\partial(1)$ where ∂ is the coboundary map in (2.11). So $\eta_{(\sigma, \tau)}$ represents the e -pairing cup product $\partial(1) \cup_e [z] = [z] \cup_e \partial(1) = \Upsilon([z])$ by Lemma 2.10. \square

Proof of Theorem 7.1. There exists a φ -covering of $(J_{\mathfrak{m}}^1)_{\bar{k}}$. The Galois descent obstruction to defining this over k is the image in $H^2(k, A_{\mathfrak{m}}[\varphi])$ of the class of this covering under the map

$$H^0(\text{Gal}_k, H^1((J_{\mathfrak{m}}^1)_{\bar{k}}, A_{\mathfrak{m}}[\varphi])) \rightarrow H^2(\text{Gal}_k, A_{\mathfrak{m}}[\varphi])$$

from the Hochschild-Serre spectral sequence (cf. [Sko01, Section 2.2]). This class coincides with the image of $[J_{\mathfrak{m}}^1]$ under the coboundary map arising from the exact sequence

$$0 \rightarrow A_{\mathfrak{m}}[\varphi] \rightarrow A_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}} \rightarrow 0$$

(see [Sko01, Lemma 2.4.5]). This proves the equivalence of (1) and (2), while the equivalence of (2) and (3) follows from geometric class field theory. The equivalences (3) \Leftrightarrow (4) \Leftrightarrow (5) \Leftrightarrow (6) follow immediately from the definitions, and (3) \Leftrightarrow (7) is given by Lemma 7.2.

It remains to prove (7) \Leftrightarrow (8). An n -covering $\pi : X \rightarrow C$ is a k -form of the maximal unramified abelian covering of exponent n , which we may assume exists. Then, for any $\delta, \delta' \in \Delta(\bar{k})$ the divisors $\pi^*\beta_\delta$ and $\pi^*\beta_{\delta'}$ are linearly equivalent. Indeed $\beta_\delta - \beta_{\delta'}$ represents a class in $J[n]$. It follows that the class of $\pi^*\beta_\delta$ in $\text{Pic}(X_{\bar{k}})$ is fixed by Gal_k . The image of this class in $\text{Br}(k)$ is trivial if and only if the class can be represented by a k -rational divisor. Since the set of all isomorphism classes of n -coverings of C is a principal homogeneous space for $H^1(J[n])$ under the action of twisting, the equivalence of (7) and (8) follows from Lemma 7.3. \square

7.2. Hyperelliptic curves. Suppose $(2, \mathbf{m})$ is a modulus setup for $C : z^2 = f(x, y)$, a double cover of \mathbb{P}^1 as in Example D.1.

- (1) Given a pair of symmetric bilinear forms (A, B) such that $\text{disc}(Ax - By) = f(x, y)$ the Fano variety of maximal linear subspaces contained in the base locus of the pencil of quadrics generated by (A, B) may be given the structure of a 2-covering of J^1 . Theorem 22 and the discussion of Section 5 in [BGW17] shows that the isomorphism classes of 2-coverings of J^1 that arise in this way are precisely those in $\text{Cov}_{\mathbf{m}}^2(J^1)$.
- (2) Section 3 of [BS09] gives an explicit construction of a collection of 2-coverings of C from the set H_k (notation as in [BS09]). Comparing Lemma 7.2 with the proof of [BS09, Theorem 3.4] shows that the collection of coverings they produce is precisely $\text{Cov}_{\mathbf{m}}^2(C)$.
- (3) In [Cre13, Section 6] a set $\text{Cov}_{\text{good}}(J^1/k)$ is defined; from that definition and point (2) above it follows that this set coincides with $\text{Cov}_{\mathbf{m}}^2(J^1)$. See also [Cre18, Lemma 2.3] for a direct proof that $\text{Cov}_{\text{good}}(J^1/k)$ coincides with the set described in (1) above.

7.3. Genus 1 curves. For a genus 1 curve C there is a natural identification $C = J^1$, and C can be endowed with the structure of a torsor under its Jacobian J . We define the **index** of C to be the least positive degree of a k -rational divisor on C and the **period** of C to be the order of the class $[C]$ in $H^1(E)$. The index I and period P of C are known to satisfy $P \mid I \mid P^2$, and over number fields all pairs of integers (P, I) satisfying these relations are known to occur [CS10]. The following result gives an interpretation of the equivalent conditions of Theorem 7.1 in terms of period and index of the n -coverings of C .

The proof of the following theorem is given at the end of this section.

Theorem 7.4. *Let $[C]$ be a torsor under an elliptic curve E with underlying curve C . The following are equivalent.*

- (1) *There exists a torsor $[C'] \in H^1(E)$ of index dividing n^2 such that $n[C'] = [C]$.*
- (2) *The curve C admits a modulus setup (n, \mathbf{m}) with $n = \deg(\mathbf{m})$ such that $[J_{\mathbf{m}}^1]$ is divisible by φ in $H^1(J_{\mathbf{m}})$.*

Remark 7.5. *In [Cre16] it is shown that condition (2) is satisfied when C is a locally soluble curve over a global field k and the action of Gal_k on $J[n]$ is sufficiently generic. In particular, when $k = \mathbb{Q}$, it holds when $n = p^r$ is any prime power with $p > 7$.*

From the proof one extracts the following, which shows that the set $\text{Cov}_{\mathbf{m}}^n(C)$ of this paper coincides with the set $\text{Cov}_0^n(C)$ defined in [Cre14, Definition 3.3].

Corollary 7.6. *Let C be a genus 1 curve with a modulus setup (n, \mathbf{m}) with $n = \deg(\mathbf{m})$. The set $\text{Cov}_{\mathbf{m}}^n(C)$ consists of those n -coverings $D \rightarrow C$ such that the index of D divides n^2 .*

Our proof of Theorem 7.4 will make use of the following interpretation of the elements of $H^1(E[n])$ taken from [CFO⁺08].

Definition 7.7. *A torsor divisor class pair (T, Z) consists of a E -torsor T and a k -rational divisor class $Z \in \text{Pic}_T(k)$. Two torsor divisor class pairs (T, Z) and (T', Z') are isomorphic if there is an isomorphism of torsors $s : T \rightarrow T'$ such that $s^*Z' = Z$.*

The automorphism group of the pair $(E, n \cdot 0_E)$ can be identified with $E[n]$, and every pair (T, Z) with $\deg(Z) = n$ can be viewed as a twist of $(E, n \cdot 0_E)$ ([CFO⁺08, Lemmas 1.7 and 1.8]). It follows that the torsor divisor class pairs of degree n , viewed as twists of $(E, n \cdot 0_E)$, are parameterized by the group $H^1(E[n])$.

Lemma 7.8. *Suppose (T', Z') is a torsor divisor class pair representing a lift of the class of (T, Z) under the map $n_* : H^1(E[n^2]) \rightarrow H^1(E[n])$. The Brauer classes associated to the k -rational divisor classes Z' and Z satisfy $n[Z'] = [Z]$ in $\text{Br}(k)$. In particular, Z is represented by a k -rational divisor if Z' is.*

Proof. Suppose the class of (T', Z') is represented by a 1-cocycle $\xi_\sigma \in Z^1(E[n^2])$. Let $f_\sigma, g_\sigma \in \bar{k}(E)^\times$ be functions such that $\text{div}(f_\sigma) = \tau_{\xi_\sigma}^*[n]^*0_E - [n]^*0_E$ and $\text{div}(g_\sigma) = \tau_{n\xi_\sigma}^*n \cdot 0_E - n \cdot 0_E$. Comparing divisors we see that we may scale by a constant to arrange that $f_\sigma^n = g_\sigma \circ [n]$. Moreover, using that ξ_σ is a cocycle, we see that the coboundaries of the 1-cochains $(\sigma \mapsto f_\sigma)$ and $(\sigma \mapsto g_\sigma)$ give 2-cocycles $F, G \in Z^2(\bar{k}^\times)$ satisfying $F^n = G$.

To prove the lemma one shows that F and G represent the Brauer classes corresponding to Z' and Z , respectively. By [CFO⁺08, Prop. 1.32], the pair $(g_\sigma, n\xi_\sigma)$ denotes a lift of $n\xi_\sigma$ to the theta group corresponding to the torsor divisor class pair $(E, n \cdot 0_E)$. Then [CFO⁺08, Prop. 2.2] shows that $[G] = [Z]$. In the same way we see that (f_σ, ξ_σ) gives a lift of ξ_σ to the theta group corresponding to $(E, [n]^*0_E) \simeq (E, n^2 \cdot 0_E)$ and so $[F] = [Z']$. \square

Proof of Theorem 7.4. We may assume $n > 1$.

(1) \Rightarrow (2). Suppose (1) holds and let $Z' \in \text{Pic}^{n^2}(C')$. Consider the torsor divisor class pair $([C'], Z')$. The image of this class under $n_* : H^1(E[n^2]) \rightarrow H^1(E[n])$ is represented by a pair $([C], Z)$. By Lemma 7.8, $Z \in \text{Pic}^n(C)$. By Riemann-Roch Z determines a map $C \rightarrow \mathbb{P}^{n-1}$ (which is an embedding for $n > 2$ and a double cover for $n = 2$). By Bertini the divisor class Z contains a reduced and effective and base point free divisor \mathbf{m} of degree n . Then (n, \mathbf{m}) is a modulus setup for C with $n = \deg(\mathbf{m})$. Let $\Delta := \{x \in C(\bar{k}) : n \cdot x \sim \mathbf{m}\}$ and take β to be the diagonal embedding of Δ in $C \times \Delta$. Then (n, \mathbf{m}) is associated to the n -descent setup (n, Δ, β) , which agrees with that described in Example D.2.

The pair (C', Z') corresponds to an n^2 -covering of E , which we may assume factors through the n -covering of E determined by (C, Z) . In particular, there is a commutative diagram

$$\begin{array}{ccccc} C' & \xrightarrow{\pi'} & C & \xrightarrow{\pi} & E \\ \downarrow s' & & \downarrow s & & \parallel \\ E & \xrightarrow{n} & E & \xrightarrow{n} & E \end{array}$$

where s and s' are isomorphisms defined over \bar{k} which determine the E -torsor structures on C and C' . Now $[\mathbf{m}] = Z = [s^*n \cdot 0_E]$, so we must have $s^*0_E = \beta_\delta$ for some $\delta \in \Delta(\bar{k})$. On

the other hand, Z' is the class of $s'^*n^2.0_E = s'^*[n]^*0_E = \pi'^*s^*0_E = \pi'^*\beta_\delta$. As this class is represented by a k -rational divisor, Theorem 7.1 shows that $[J_{\mathfrak{m}}^1]$ is divisible by φ .

(2) \Rightarrow (1). Then \mathfrak{m} is ample and base point free and, hence, determines a model of C as a degree n curve in \mathbb{P}^{n-1} . Let (n, Δ, β) be the n -descent setup as in Example D.2. By Theorem 7.1 there is an n -covering $\pi : C' \rightarrow C$ such that $\pi^*\beta_\delta$ is linearly equivalent to a k -rational divisor for some $\delta \in \Delta(\bar{k})$. The genus 1 curve C' is endowed with a torsor structure so that $n[C'] = [C]$ in $H^1(E)$. Moreover, the index of $[C']$ divides $\deg(\pi^*\beta_\delta) = n^2$. \square

REFERENCES

- [Ati71] Michael F. Atiyah, *Riemann surfaces and spin structures*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 47–62.
- [Bha] Manjul Bhargava, *Most hyperelliptic curves over \mathbb{Q} have no rational points*, available at [arXiv:1308.0395](https://arxiv.org/abs/1308.0395).
- [BG13] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L -functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91.
- [BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over \mathbb{Q} have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser.
- [BGW15] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits*, Representations of reductive groups, Progr. Math., vol. 312, Birkhäuser/Springer, Cham, 2015, pp. 139–171.
- [BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.
- [Bor96] Mikhail Borovoi, *The Brauer-Manin obstructions for homogeneous spaces with connected or abelian stabilizer*, J. Reine Angew. Math. **473** (1996), 181–194.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
- [Bre86] Andrew Bremner, *Some quartic curves with no points in any cubic field*, Proc. London Math. Soc. (3) **52** (1986), no. 2, 193–214.
- [BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum of Mathematics, Sigma **4** (2016), e6 80 pages.
- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370.
- [Cas62] J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.
- [CS10] Pete L. Clark and Shahed Sharif, *Period, index and potential. III*, Algebra Number Theory **4** (2010), no. 2, 151–174.
- [Cre01] J. E. Cremona, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1-2, 71–87. Computational algebra and number theory (Milwaukee, WI, 1996).
- [CFO⁺08] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit n -descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155.
- [Cre10] Brendan Creutz, *Explicit second p -descent on elliptic curves* (2010). Ph.D. thesis, Jacobs University.
- [Cre13] Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, Algorithmic number theory: Proceedings of the 10th Biennial International Symposium (ANTS-X) held in San Diego, July 9–13, 2012 (Everett W. Howe and Kiran S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Science Publishers, 2013, pp. 295–315.
- [Cre14] Brendan Creutz, *Second p -descents on elliptic curves*, Math. Comp. **83** (2014), no. 285, 365–409.

- [Cre16] Brendan Creutz, *Most binary forms come from a pencil of quadrics*, Proc. Amer. Math. Soc. Ser. B **3** (2016), 18–27.
- [Cre18] Brendan Creutz, *Improved rank bounds from 2-descent on hyperelliptic Jacobians*, Int. J. Number Theory **14** (2018), no. (6), 1709–1713.
- [CV15] Brendan Creutz and Bianca Viray, *Two torsion in the Brauer group of a hyperelliptic curve*, Manuscripta Math. **147** (2015), no. 1-2, 139–167.
- [Gro95] Alexander Grothendieck, *Techniques de construction et théorèmes d’existence en géométrie algébrique. III. Préschemas quotients*, Séminaire Bourbaki, Vol. 6, Soc. Math. France, Paris, 1995, pp. Exp. No. 212, 99–118 (French).
- [How96] Everett W. Howe, *The Weil pairing and the Hilbert symbol*, Math. Ann. **305** (1996), no. 2, 387–392.
- [Lic69] Stephen Lichtenbaum, *Duality theorems for curves over p -adic fields*, Invent. Math. **7** (1969), 120–136.
- [MSS96] J. R. Merriman, S. Siksek, and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **77** (1996), no. 4, 385–404.
- [Mil86a] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
- [Mil86b] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
- [Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.
- [NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.
- [PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318.
- [PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.
- [PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.
- [Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. Translated from the French.
- [Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.
- [Sut18] Andrew Sutherland, *A database of nonhyperelliptic genus 3 curves over \mathbb{Q}* (2018), available at [arXiv:1806.06289](https://arxiv.org/abs/1806.06289).
- [Tho15] Jack A. Thorne, *E_6 and the arithmetic of a family of nonhyperelliptic curves of genus 3*, Forum Math. Pi **3** (2015), e1, 41.
- [Tho] Jack A. Thorne, *On the 2-Selmer groups of plane quartic curves with a marked point*. (preprint).
- [Wan18] Xiaoheng Wang, *Maximal linear spaces contained in the based loci of pencils of quadrics*, Algebr. Geom. **5** (2018), no. 3, 359–397.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800, CHRISTCHURCH 8140, NEW ZEALAND

E-mail address: brendan.creutz@canterbury.ac.nz