GENERALIZED EXPLICIT DESCENT AND ITS APPLICATION TO CURVES OF GENUS 3

NILS BRUIN, BJORN POONEN, AND MICHAEL STOLL

ABSTRACT. We introduce a common generalization of essentially all known methods for explicit computation of Selmer groups, which are used to bound the ranks of abelian varieties over global fields. We also simplify and extend the proofs relating what is computed to the cohomologically-defined Selmer groups. Selmer group computations have been practical for many Jacobians of curves over \( \mathbb{Q} \) of genus up to 2 since the 1990s, but our approach is the first to be practical for general curves of genus 3. We show that our approach succeeds on some genus-3 examples defined by polynomials with small coefficients.

1. Introduction

1.1. Background. The Mordell–Weil theorem [Mor22, Wei29] states that for any abelian variety \( J \) over a number field \( k \), the abelian group \( J(k) \) is finitely generated. One of the main steps of the proof involves showing the finiteness of \( J(k)/nJ(k) \) for some \( n \geq 2 \). And there is essentially only one known proof of this finiteness, based on a vast generalization of Fermat's method of infinite descent. In modern terms, the proof embeds \( J(k)/nJ(k) \) into a Selmer group \( \text{Sel}^n(J) \), a finite group that is computable in principle.

But the Selmer group is defined as a subgroup of a Galois cohomology group \( H^1(k, J[n]) \), and 1-cocycles for the absolute Galois group \( \mathcal{G} \) of \( k \) are not objects that a computer can deal with directly. Fortunately, sometimes one can find more concrete representations for elements of \( H^1(k, J[n]) \). For example, if \( J \) is an elliptic curve with \( J[2] \subseteq J(k) \), then \( J[2] \) is isomorphic to \( \mu_2 \times \mu_2 \) as \( \mathcal{G} \)-module, and the Kummer sequence yields \( H^1(k, J[2]) \simeq k^\times/k^\times \times k^\times/k^\times \times k^\times/k^\times \).

In many higher-dimensional situations, however, the number field over which all the points of \( J[n] \) become rational is too large for the required computations. Instead one tries to find exact sequences relating \( J[n] \) to modules induced from \( \mathbb{Z}/n\mathbb{Z} \) or \( \mu_n \), since cohomology of induced modules can be computed by Shapiro's lemma [AW67, §4, Proposition 2]. For example, if \( J \) is the Jacobian of a hyperelliptic curve \( y^2 = f(x) \) with \( \deg f \) odd, and \( \Delta \) is the \( \mathcal{G} \)-set of Weierstrass points not including the one at infinity, then elements of \( J[2] \) are represented by degree-0 divisors supported on \( \Delta \cup \{ \infty \} \), and we obtain a split exact sequence

\[
0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \left( \mathbb{Z}/2\mathbb{Z} \right)^\Delta \rightarrow J[2] \rightarrow 0
\]
in which \((\mathbb{Z}/2\mathbb{Z})^\Lambda\) is a direct sum of induced modules: this was exploited in [Sch95]. For \(y^2 = f(x)\) with \(\text{deg } f\) even, there is still a relationship between \(J[2]\) and induced modules, but it is more involved, and it becomes much harder to relate \(H^1(k, J[2])\) to concrete objects: this problem, together with its generalization to \(y^p = f(x)\) for larger primes \(p\), was addressed in [PS97]. The situations of the two previous sentences were called true descent and fake descent, respectively, in [PS97].

1.2. Goal of this article. The main goal of this article is to develop a practical generalization of true and fake descent that contains essentially all previous instantiations of explicit descent. Our generalization is broad enough to suggest an explicit approach for Jacobians of arbitrary curves, using the \(G\)-set of odd theta characteristics. We demonstrate its practicality by computing the rank of \(J(\mathbb{Q})\) for the Jacobian of a non-hyperelliptic curve genus-3 curve \(X\) with no special property beyond having small discriminant: see Section 12.9.1. This is the first time that Selmer group computations for “general” genus-3 Jacobians have been possible.

Remark 1.1. Practical Selmer group calculations rely on the computation of class groups of number fields, and this is usually the bottleneck, except in situations where the \(G\)-action on certain torsion points is much smaller than expected for a general curve. For a general genus-3 curve over \(\mathbb{Q}\), our method requires the class group of a number field of degree 28; this seems to be the smallest possible, given that 28 is the smallest index of a proper subgroup of \(\text{Sp}_6(\mathbb{F}_2)\). For general genus-4 curves, the corresponding index is 120, which is likely to remain outside the realm of practical computation for some time.

Setting the computational advantages of our approach aside, the main theoretical advances in our article are as follows.

- Our approach of taking Cartier duals before taking cohomology (Sections 6.2.2 and 6.3.1) leads quickly to concrete results on groups such as \(H^1(k, J[2])\) over any field of characteristic not 2; this approach has already found outside applications: see [BGW13, Section 4]. In particular, our approach eliminates the use of generalized Jacobians and the group scheme \(J_m\) in [PS97], a significant simplification even in the setting of hyperelliptic curves.
- The introduction of the middle rows in (5) and (11) provides short proofs of the comparison theorems relating the cohomological and explicit definitions of descent maps.
- Appendix A shows how to augment the explicit descent maps to produce an explicit description of the Selmer group itself instead of a “fake” approximation to it.

Remark 1.2. For certain Jacobians \(J\), there is also a representation-theoretic approach to understanding \(J[2]\) and its Galois cohomology, based on Vinberg theory, whose relevance for arithmetic problems was first pointed out by Benedict Gross. Namely, Jack Thorne has shown very generally how, starting from a simple split algebraic group \(G\) of type \(A, D,\) or \(E\) over a field \(k\) of characteristic 0, one can produce a family of curves for which \(J[2]\) can be identified with the stabilizers for an action of the subgroup \(G^\theta\) fixed by an involution \(\theta\) in a particular canonical \(G^{ad}(k)\)-conjugacy class of involutions of \(G\), and from this one can obtain information about \(H^1(k, J[2])\). In particular, when \(G\) is of type \(E_6\) (resp. \(E_7\)), Thorne’s construction yields the universal family of non-hyperelliptic genus-3 curves with a marked hyperflex (resp., a marked flex that is not a hyperflex). See [Tho12]; the families
of genus-3 curves appear explicitly in Theorem 4.8 there. In the $E_6$ case, $\text{Gal}(k(J[2])/k)$ is generically $W(E_6)$, isomorphic to an index-28 subgroup of the group $\text{Sp}_6(\mathbb{F}_2)$ that arises for a general genus-3 curve. In the $E_7$ case, $\text{Gal}(k(J[2])/k)$ is generically $W(E_7)/\{\pm 1\}$, isomorphic to the full group $\text{Sp}_6(\mathbb{F}_2)$. It is reasonable to hope that it will eventually be possible to use Thorne’s work to study $\text{Sel}^2(J)$ for any non-hyperelliptic genus-3 curve with a rational flex.

1.3. Road map to the rest of the article. The first few sections are preliminary. Section 2 introduces the notation to be used throughout the rest of the article; much of it is standard. Section 3 introduces twisted powers, a slight generalization of induced modules and permutation modules. Section 4 uses Lang reciprocity to relate various definitions of Weil pairings. Section 5 reviews and develops the combinatorics of theta characteristics on a curve.

Section 6 introduces the key notions of the paper. First it axiomatizes the settings to which our explicit approach applies, formalizing them into the notions of true descent setup and fake descent setup, which are general enough to handle various isogenies $\phi: A \to J$ over a global field $k$. Given a true descent setup, we define a homomorphism

$$J(k)/\phi A(k) \to L^x/L^{xn}$$

that acts as a computation-friendly substitute for the connecting homomorphism

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

appearing in the definition of the actual $\phi$-Selmer group. In fact, the homomorphism (1) can be defined in two ways, either by using cohomology (good for comparing it to the homomorphism (2) used to define the actual $\phi$-Selmer group) or by evaluating explicit rational functions on 0-cycles (good for computing the homomorphism). Using our work on Weil pairings, we prove that the two definitions agree. A more complicated argument establishes compatibility of analogous definitions for a fake descent setup; here $L^x/L^{xn}$ is replaced by $L^x/L^{xn}k^x$.

Section 7 identifies the computation-friendly analogue of the subgroup of classes in $H^1(k, A[\phi])$ unramified outside a finite set of places, which is essential for making the computations finite. Section 9 defines a computation-friendly analogue of the $\phi$-Selmer group, called the true or fake Selmer group, and defines an analogue for a variety $X$ whose Albanese variety is $J$. Section 10 uses the notion of Shafarevich–Tate group from Section 8 to prove results that often enable one to pass from knowledge of the true or fake Selmer group to the actual $\phi$-Selmer group. A more elaborate method that always succeeds in calculating the $\phi$-Selmer group is presented in an appendix, but in some situations it may be impractical.

Section 11 provides details on how to compute true and fake Selmer groups. Section 12 specializes the approach to the case of non-hyperelliptic genus-3 curves, and ends with several examples.

2. Notation

If $S$ is a set and $n \in \mathbb{Z}_{\geq 0}$, let $\binom{S}{n}$ denote the set of $n$-element subsets of $S$. For each field $k$, choose a separable closure $k_s$ (compatibly, when possible), and let $\mathcal{G} = G_k = \text{Gal}(k_s/k)$. In general, for an object $X$ over $k$, we denote by $X_s$ its base extension to $k_s$. If $k$ is a global
field, let $\Omega_k$ be the set of nontrivial places of $k$. For $v \in \Omega_k$, let $k_v$ be the completion of $k$ at $v$; if moreover $v$ is non-archimedean, let $\mathcal{O}_v$ be the valuation ring in $k_v$, let $\mathbb{F}_v$ be the residue field, and let $k_{v,u}$ be the maximal unramified extension of $k_v$ inside a separable closure $k_{v,s}$.

All $\mathcal{G}$-sets and $\mathcal{G}$-modules are given the discrete topology, and the $\mathcal{G}$-action is assumed to be continuous. If $M$ is a $\mathcal{G}$-module, then $M^\mathcal{G}$ or $M(k)$ denotes the subgroup of $\mathcal{G}$-invariant elements, and $H^n(\mathcal{G}, M)$ denotes profinite group cohomology.

If $X$ is an integral $k$-scheme, then $k(X)$ is its function field. More generally, if $X$ is a disjoint union of integral $k$-schemes $X_i$, let $k(X)$ be the product of the $k(X_i)$; equivalently, $k(X)$ is the ring of global sections of the sheaf of total quotient rings (see [Har77, p.141]). Let $\mathcal{O} = \mathcal{O}_X$ be the structure sheaf.

Call a variety nice if it is smooth, projective, and geometrically integral. Curves will be assumed nice unless otherwise specified. For a nice variety $X$, let $\text{Div} X$ (resp. $\text{Div}^0 X$) be the group of divisors (resp. divisors algebraically equivalent to 0) on $X$ over $k$, let $\mathcal{Z}(X)$ (resp. $\mathcal{Z}^0(X)$) be the group of 0-cycles (resp. 0-cycles of degree 0), and define $\text{Pic} X$ as in [Har77, II. §6]; if $X$ is a curve, also define $\text{Pic}^0 X := \ker(\text{Pic} X \to \mathbb{Z})$. Alternatively, if $\text{Princ} X$ is the group of principal divisors, then $\text{Pic} X = \text{Div} X / \text{Princ} X$. If $f \in k(X)^*$ and $z = \sum n_P P \in \mathcal{Z}(X)$ is such that no closed point $P$ appearing in $z$ is a zero or pole of $f$, let $f(z) = \prod(P(N_{k(P)}(f(P))^nP) \in k^*$. Let $J := \text{Alb}_X$ be the Albanese variety of $X$, so $J$ is an abelian variety. Then the Picard variety of $X$ (i.e., the reduced subgroup scheme associated to the connected component of the Picard scheme of $X/k$) may be identified with the dual abelian variety $\hat{J}$. If $X$ is a curve, then both $J$ and $\hat{J}$ are the Jacobian $\text{Jac} X$. Let $\mathcal{J}^0(X)$ be the kernel of the natural map $\mathcal{Z}^0(X) \to J(k)$, and let $J(k)_{\circ}$ be the image of this map. More generally, if $G$ is a subgroup of $J(k)$, let $(J(k)/G)_{\circ}$ be the image of $\mathcal{Z}^0(X) \to J(k)/G$.

3. Twisted powers

Fix a field $k$.

Definition 3.1. Given a $\mathcal{G}$-module $M$, and a finite $\mathcal{G}$-set $\Delta$, the twisted power $M^\Delta$ is the $\mathcal{G}$-module of maps from $\Delta$ to $M$.

Remark 3.2. The $\mathcal{G}$-action on maps is the usual one: if $\sigma \in \mathcal{G}$ and $P \mapsto m_P$ is an element $m \in M^\Delta$, then $^\sigma m$ is the map $P \mapsto \sigma(m_{\sigma^{-1}P})$.

Remark 3.3. Applying the construction to $\mathbb{Z}$ with trivial action yields $\mathbb{Z}^\Delta$. Then $M^\Delta = \text{Hom}\mathbb{Z}(\mathbb{Z}^\Delta, M)$ for any $\mathcal{G}$-module $M$.

Remark 3.4. If $G$ is a commutative group scheme over $k$, we also use $G$ to denote the $\mathcal{G}$-module $G(k_s)$, and define $G^\Delta$ (at least as a $\mathcal{G}$-module). Similarly, a finite étale $k$-scheme $\Delta$ can be identified with a finite $\mathcal{G}$-set.

Definition 3.5. If $M$ is a $\mathcal{G}$-module and $\Delta$ is a finite $\mathcal{G}$-set, there is a homomorphism $\text{deg}: M^\Delta \to M$ that sums the coordinates, and we let $M^\Delta_{\text{deg}0}$ be its kernel.

Definition 3.6. Given a finite $\mathcal{G}$-module $M$ of size not divisible by char $k$, the Cartier dual of $M$ is the $\mathcal{G}$-module $M^\vee := \text{Hom}\mathbb{Z}(M, k^*_s)$. (This is compatible with the notion for finite commutative group schemes.)

Remark 3.7. For fixed $\Delta$, the functor $M \mapsto M^\Delta$ is exact.
Remark 3.8. For a finite $G$-module $M$ of size not divisible by char $k$, and a finite $G$-set $\Delta$, we have $(M^\Delta)^\vee \simeq (M^\vee)^\Delta$.

Each finite étale $k$-scheme $\Delta$ is Spec $L$ for some étale $k$-algebra $L$. Define the étale $k_s$-algebra $L_s := L \otimes_k k_s$. Thus $\mathbb{G}_a^\Delta(k) = L$ and $\mathbb{G}_a^\Delta(k_s) = L_s$. Assume char $k \nmid n$. Then $\mu_n^\Delta(k_s) = \mu_n(L_s)$. The group $H^1(\mathbb{G}_m^\Delta) = H^1(G, L_s^\times)$ is trivial by a generalization of Hilbert’s theorem 90 [Ser79, p. 152, Exercise 2], so $H^1(\mu_n^\Delta) = L^\times/L^{\times n}$.

4. Weil pairings

Let $k$ be a field. Let $n$ be a positive integer with char $k \nmid n$.

In this section we review Lang’s construction of the Weil pairing between Albanese varieties. Let $V$ and $W$ be nice $k$-varieties and let $\mathcal{D} \in \text{Div}(V \times W)$. The divisor $\mathcal{D}$ induces partial maps

$$\mathcal{D}: \mathcal{Z}^0(V_s) \to \text{Div}^0 W_s \quad \text{and} \quad \mathcal{D}^\dagger: \mathcal{Z}^0(W_s) \to \text{Div}^0 V_s.$$ 

Summation of 0-cycles in $\text{Alb}_V(k_s)$ gives rise to the exact sequence

$$0 \to \mathcal{Y}^0(V_s) \to \mathcal{Z}^0(V_s) \to \text{Alb}_V(k_s) \to 0.$$ 

By [Lan83, III, Theorem 4, Corollary 2], $\mathcal{D}(\mathcal{Y}^0(V_s)) \subset \text{Princ} W_s$. In particular, if $v \in \mathcal{Z}^0(V_s)$ maps to an $n$-torsion point $[v] \in \text{Alb}_V[n](k_s)$, then $nv \in \mathcal{Y}^0(V_s)$, and $\mathcal{D}(nv) = \text{div}(f_{nv})$ for some $f_{nv} \in k_s(W)$. Define $f_{nw} \in k_s(V)$ symmetrically. Define

$$e_{\mathcal{D}, n}: \text{Alb}_V[n](k_s) \times \text{Alb}_W[n](k_s) \to \mu_n(k_s)$$

$$[v], [w] \mapsto \frac{f_{nw}(v)}{f_{nw}(w)}$$

where $v \in \mathcal{Z}^0(V_s)$ mapping to $[v]$ and $w \in \mathcal{Z}^0(W_s)$ mapping to $[w]$ are chosen so that the evaluations make sense. See [Lan83, VI, §4] for the proof that $e_{\mathcal{D}, n}$ is well-defined, bilinear, and Galois-equivariant.

Remark 4.1. Let $A$ be an abelian variety, let $\hat{A}$ be the dual abelian variety, and continue to suppose that char $k \nmid n$. Take $V = A$ and $W = \hat{A}$, and let $\mathcal{D}$ be a Poincaré divisor. Since $\text{Alb}_A = A$ and $\text{Alb}_\hat{A} = \hat{A}$, we obtain a pairing $e_n: A[n] \times \hat{A}[n] \to \mu_n$. It is nondegenerate (see [Lan83, VI, VII]), so we obtain an identification of $\hat{A}[n]$ with $A[n]^\vee$.

4.2. The Albanese-Picard definition. Let $X$ be a nice $k$-variety. Let $J := \text{Alb}_X$. Let $\mathfrak{P}$ be a Poincaré divisor in $\text{Div}(J \times \hat{J})$. Fix a base point in $X_s$ to obtain a map $\iota: X_s \to J_s$. The functoriality of taking Albanese varieties yields $\iota(\mathcal{Y}^0(X_s)) \subset \mathcal{Z}^0(J_s)$. Define $\mathfrak{P}_0 := (\iota \times \text{id}_{\hat{J}})^* \mathfrak{P} \in \text{Div}(X_s \times \hat{J}_s)$. If $y \in \mathcal{Y}^0(X_s)$ and $z \in \mathcal{Z}^0(J_s)$, then $\mathfrak{P}_0(y)$ (if defined) is the divisor of some rational function on $\hat{J}_s$, which can be evaluated on $z$ (if the supports are disjoint) to obtain a value $\mathfrak{P}_0(y, z) \in k_s^\times$. Given $D \in \text{Div}^0(X_s)$, we may find $z \in \mathcal{Z}^0(J_s)$ summing to $[D] \in \text{Pic}^0(X_s) = \hat{J}_s(k_s)$, which means that $D - \mathfrak{P}_0(z) = \text{div}(g_{D, z})$ for some $g_{D, z} \in k_s(X)^\times$, and we obtain a partially-defined pairing

$$[\cdot, \cdot]: \mathcal{Y}^0(X_s) \times \text{Div}^0(X_s) \to k_s^\times$$

$$y, D \mapsto g_{D, z}(y) \mathfrak{P}_0(y, z)$$
See [PS99, Section 3.2] for a proof that this pairing is independent of the choices made, using Lang reciprocity and the seesaw principle. If \( g \in k_s(X)^\times \), then \([y, \text{div}(g)] = g(y)\) since the choice \( z = 0 \) yields \( g_{D,z} = g \).

Finally, define
\[
e_{X,n} : J[n] \times \widehat{J}[n] \to \mu_n(k_s) \\
([x], [D]) \mapsto \frac{f_{nD}(x)}{[nx, D]},
\]
where \( x \in \mathcal{Z}^0(X_s) \) represents an element of \( J[n](k_s) \), and \( D \in \text{Div}^0 X_s \) represents an element of \( \widehat{J}[n](k_s) \), and \( f_{nD} \in k_s(X)^\times \) has divisor \( nD \), and all these are chosen so that everything is defined.

Let us check that \( e_{X,n} \) is well-defined, i.e., independent of the choices of \( x \) and \( D \). Changing \( x \) means adding some \( y \in \mathcal{Y}^0(X_s) \) to it, and we have
\[
e_{X,n}([y], D) = \frac{f_{nD}(y)}{[ny, D]} = \frac{f_{nD}(y)}{[y, nD]} = \frac{f_{nD}(y)}{f_{nD}(y)} = 1.
\]
Changing \( D \) means adding \( \text{div}(f) \) to it for some \( f \in k_s(X)^\times \), and we have
\[
e_{X,n}(x, \text{div}(f)) = \frac{f^n(x)}{[nx, \text{div}(f)]} = \frac{f(x)^n}{f(x)^n} = 1.
\]

4.3. Functoriality. Let \( \iota : X \to X' \) be a morphism of nice varieties. Let \( x \in \mathcal{Y}^0(X_s) \) and \( D \in \text{Div}^0(X'_s) \). It is straightforward to check that
\[
[x, \iota^*D] = [\iota(x), D]
\]
whenever both sides are defined. It follows that for \([x] \in \text{Alb}_{X_s}[n]\) and \([D] \in (\text{Pic} X_s)[n]\) we have
\[
e_{X,n}([x], \iota^*[D]) = e_{X',n}([\iota(x)], [D]).
\]

4.4. Equality of the pairings. Let \( J := \text{Alb}_X \). We now have three pairings
\[
e_{X,n}, e_{J,n}, e_n : J[n] \times \widehat{J}[n] \to \mu_n,
\]
where the first two are from Section 4.2 and the third is from Remark 4.1.

**Proposition 4.2.** The pairings \( e_{X,n}, e_{J,n}, \) and \( e_n \) are equal.

**Proof.** Functoriality with respect to an Albanese embedding \( X_s \to \text{Alb}_{X_s} \) shows that \( e_{X,n} = e_{J,n} \).

Now we prove that \( e_{J,n} = e_n \). Suppose that \( a \in J[n](k_s) \) and \( a' \in \widehat{J}[n](k_s) \) are represented by appropriate \( z \in \mathcal{Z}^0(J_s) \) and \( z' \in \mathcal{Z}^0(\widehat{J}_s) \). Let \( D = \mathfrak{P}^l z' \in \text{Div}^0(J_s) \). By definition, \( f_{nz'} = f_{nD} \) and
\[
e_{J,n}(a, a') = \frac{f_{nD}(z)}{[nz, D]} = \frac{f_{nz'}(z)}{\mathfrak{P}_0(nz, z')} = \frac{f_{nz'}(z)}{f_{nz}(nz')} = e_n(a, a'). \]

5. **Odd theta characteristics**

Assume \( \text{char } k \neq 2 \). Let \( X \) be a nice curve of genus \( g \) over \( k \). Let \( \omega \) be its canonical bundle, and let \( J := \text{Jac } X \).
5.1. **Theta characteristics.** A **theta characteristic** on $X$ is a line bundle $\vartheta$ on $X$ such that $\vartheta^\otimes 2 \simeq \omega$. A theta characteristic $\vartheta$ is called **odd** if the nonnegative integer $h^0(\vartheta) := \dim H^0(X, \vartheta)$ is odd. The isomorphism classes of theta characteristics on $X$ form a set $\mathcal{T}$ of size $2^{2g}$, and the odd ones form a subset $\mathcal{T}_{\text{odd}}$ of size $2^{g-1}(2^g - 1)$ (cf. [Mum71]).

5.2. **Theta characteristics and quadratic forms.** Given a symplectic pairing $e$ on an $\mathbb{F}_2$-vector space $V$, a **quadratic form** associated to $e$ is a map of sets $q: V \to \mathbb{F}_2$ such that $q(x + y) - q(x) - q(y) = e(x, y)$ for all $x, y \in V$.

**Theorem 5.1** (Riemann-Mumford). Suppose that $k$ is separably closed and $\text{char } k \neq 2$. View the Weil pairing $e_2$ as a symplectic pairing on $J[2]$ with values in $\mathbb{F}_2 \simeq \{\pm 1\}$.

(a) For each theta characteristic $\vartheta$,

$$q_\vartheta : J[2] \to \mathbb{F}_2$$

$$\mathcal{L} \mapsto (h^0(\vartheta \otimes \mathcal{L}) + h^0(\vartheta)) \mod 2$$

is a quadratic form associated to $e_2$.

(b) The map

$$\mathcal{T} \to \{\text{quadratic forms on } J[2] \text{ associated to } e_2\}$$

$$\vartheta \mapsto q_\vartheta,$$

is a bijection.

(c) A theta characteristic $\vartheta$ is odd if and only if the Arf invariant of $q_\vartheta$ is 1.

**Proof.** See [Mum71] and [GH04, §4].

Combining Theorem 5.1 with the following lemma will help us understand the relations between the odd theta characteristics in the $\mathbb{F}_2$-vector space $\text{Pic} \frac{X}{\langle \omega \rangle}[2]$: see Corollary 5.3.

**Lemma 5.2.** Let $f$ be in the space $\mathbb{F}_2[x_1, \ldots, x_n]_{\leq 2}$ of polynomials of total degree at most 2. Let $f_2$ be its homogeneous part of degree 2.

(i) If $f$ vanishes on $\mathbb{F}_2^n$, then $f_2$ is a square.

(ii) If $n$ is even, and $f_2$ is nondegenerate (as a quadratic form), and $V \subseteq \mathbb{F}_2^n$ is a coset of a linear subspace of dimension at least $n/2 + 1$, then $f(v) = 0$ for some $v \in V$.

(iii) If $n$ is even and $n \geq 4$ and $v \in \mathbb{F}_2^n$, and $f_2$ is nondegenerate, then there exists $x \in \mathbb{F}_2^n$ with $f(x) = f(x + v) = 0$.

(iv) If $n$ is even and $n \geq 6$ and $v_1, v_2 \in \mathbb{F}_2^n$, and $f_2$ is nondegenerate, then there exists $x \in \mathbb{F}_2^n$ with $f(x) = f(x + v_1) = f(x + v_2) = 0$.

**Proof.**

(i) If $f_2$ is not a square, it contains a monomial $x_i x_j$ with $i \neq j$, and then restricting to the span of the $x_i$- and $x_j$-axes lets us reduce to the case $n = 2$, which is easy.

(ii) Replacing $f(x)$ by $f(x + v)$ lets us assume that $V$ is a subspace. Let $e$ be the symmetric bilinear pairing associated to $f_2$. Since $e$ is nondegenerate, $e|_V$ has kernel of size at most $n - \dim V < \dim V$, so $e|_V \neq 0$. Hence $f_2|_V$ is not a square. Apply (i) to $f + 1$.

(iii) If $v \neq 0$, let $V \subseteq \mathbb{F}_2^n$ be the codimension-1 coset defined by $f(x + v) - f(x) = 0$; if $v = 0$, let $V = \mathbb{F}_2^n$. Apply (ii).

(iv) By (iii), we may assume that $v_1, v_2$ are distinct and nonzero. Let $V$ be the codimension-2 coset defined by $f(x + v_1) - f(x) = 0$ and $f(x + v_2) - f(x) = 0$. Apply (ii).
In the rest of Section 5.2 except in Corollary 5.5, we assume that \( k \) is a separably closed field of characteristic not 2, and that \( X \) is a nice curve of genus \( g \geq 2 \) over \( k \).

**Corollary 5.3.**

(a) If \( g \geq 2 \), then every class in \( J[2] \subset \Pic_{(\omega)}X[2] \) has the form \( \vartheta_1 + \vartheta_2 \) (modulo \( \omega \)) with \( \vartheta_1, \vartheta_2 \in \mathcal{T}_{\text{odd}} \).

(b) If \( g \geq 3 \), and \( \vartheta_1, \ldots, \vartheta_6 \in \mathcal{T}_{\text{odd}} \) sum to 0 in \( \Pic_{(\omega)}X[2] \), then there exist \( \vartheta_{12}, \vartheta_{34}, \vartheta_{56} \in \mathcal{T}_{\text{odd}} \) such that

\[
\begin{align*}
\vartheta_1 + \vartheta_2 + \vartheta_{34} + \vartheta_{56} &= 0 \\
\vartheta_3 + \vartheta_4 + \vartheta_{12} + \vartheta_{56} &= 0 \\
\vartheta_5 + \vartheta_6 + \vartheta_{12} + \vartheta_{34} &= 0
\end{align*}
\]

in \( \Pic_{(\omega)}X[2] \).

**Proof.** Fix \( \vartheta \in \mathcal{T}_{\text{odd}} \). By Theorem 5.1, there is an identification \{zeros of \( q_\vartheta \) in \( J[2] \)\} \( \to \mathcal{T}_{\text{odd}} \) given by \( x \mapsto \vartheta + x \). Identify \( J[2] \) with \( \mathbb{F}_2^{2g} \), and \( q_\vartheta \) with a polynomial \( f \).

(a) Apply Lemma 5.2(iii) with \( v \) the class in \( J[2] \). Then \( x \) corresponds to the desired \( \vartheta_1 \), and \( x + v \) to \( \vartheta_2 \).

(b) Apply Lemma 5.2(iv) with \( v_1 = \vartheta_1 + \vartheta_2 \) and \( v_2 = \vartheta_3 + \vartheta_4 \) to get \( x \). Then \( x \) corresponds to the desired \( \vartheta_{56} \), \( x + v_1 \) corresponds to the desired \( \vartheta_{34} \), and \( x + v_2 \) corresponds to the desired \( \vartheta_{12} \). The first two relations are then satisfied, and the third is the sum of the first two.

By an incidence structure, we will mean a pair \((\Delta, \Sigma)\), where \( \Delta \) is a set and \( \Sigma \) is a collection of subsets of \( \Delta \). An isomorphism \((\Delta, \Sigma) \to (\Delta', \Sigma')\) is a bijection \( \Delta \to \Delta' \) under which \( \Sigma \) and \( \Sigma' \) correspond.

Let \( \Sigma \) be the set of 4-element subsets of \( \mathcal{T}_{\text{odd}} \) that sum to 0 in \( \Pic_{(\omega)}X[2] \).

**Proposition 5.4.** The following structures have the same automorphism group \( \text{Sp}_{2g}(\mathbb{F}_2) \):

1. The \( \mathbb{F}_2 \)-vector space \( \Pic_{(\omega)}X[2] \) equipped with \( \mathcal{T}_{\text{odd}} \) (viewed as a subset).
2. The \( \mathbb{F}_2 \)-vector space \( J[2] \) with the Weil pairing \( e_2 \).
3. The incidence structure \((\mathcal{T}_{\text{odd}}, \Sigma)\).

**Proof.** The automorphism group of (2) is \( \text{Sp}_{2g}(\mathbb{F}_2) \), so it suffices to show how to build each structure canonically in terms of the others.

1\( \to \)2: By Corollary 5.3(a), we can recover \( J[2] \) as the subgroup of \( \Pic_{(\omega)}X[2] \) generated by \( \vartheta_1 + \vartheta_2 \) with \( \vartheta_1, \vartheta_2 \in \mathcal{T}_{\text{odd}} \). The subset \( \mathcal{T}_{\text{odd}} \) determines the function \( h_0 \mod 2 \) on the nontrivial coset \( \mathcal{T} \) of \( J[2] \) in \( \Pic_{(\omega)}X[2] \). Choose \( \vartheta \in \mathcal{T}_{\text{odd}} \); from \( h_0 \mod 2 \), we can recover \( q = q_\vartheta \) and hence \( e_2(x, y) = q(x + y) - q(x) - q(y) \).

2\( \to \)1: Take the space of functions \( q: J[2] \to \mathbb{F}_2 \) such that \( (x, y) \mapsto q(x + y) - q(x) - q(y) \) is a multiple of \( e_2 \). Inside this we have the subset of \( q \) for which the multiple is \( e_2 \) itself and for which the Arf invariant is 1.

1\( \to \)3: Clear.

3\( \to \)1: If \( g = 2 \), take the \( \mathbb{F}_2 \)-vector space \( P \) with generator set \( \mathcal{T}_{\text{odd}} \) and with one relation saying that the sum of the generators is 0. If \( g \geq 3 \), take the \( \mathbb{F}_2 \)-vector space \( P \) with generator set \( \mathcal{T}_{\text{odd}} \) and with relations given by the elements of \( \Sigma \).
To show that the map $\epsilon: P \to \text{Pic}_{X}(\omega)[2]$ sending each basis element to the corresponding $\vartheta$ is an isomorphism, it suffices to show that its restriction $\epsilon_0: P_0 \to J[2]$ is an isomorphism, where $P_0$ is the codimension-1 subspace of $P$ spanned by pairs. Corollary 5.3(a) shows that $\epsilon_0$ induces a bijection $(\mathcal{S}_{\vartheta})/\sim \to [2] - \{0\}$, where $\{\vartheta_1, \vartheta_2\} \sim \{\vartheta_3, \vartheta_4\}$ means $\sum_{i=1}^{4} \vartheta_i = 0$ in $\text{Pic}_{X}(\omega)[2]$. In particular, $\epsilon_0$ is surjective. If $g = 2$, then $\epsilon_0$ is injective too, because $\dim P_0 = 4 = \dim J[2]$. To prove injectivity for $g \geq 3$, it suffices to prove that every relation
\[(\vartheta_1 + \vartheta_2) + (\vartheta_3 + \vartheta_4) = (\vartheta_5 + \vartheta_6)\]
in $\text{Pic}_{X}(\omega)[2]$ is a consequence of 4-term relations. But that is true, by Corollary 5.3(b).

**Corollary 5.5.** Let $k$ be any field of characteristic not 2. The action of $\mathcal{G}$ on $J[2]$, on the set of theta characteristics of $X_s$ or on the set of odd theta characteristics of $X_s$, factors through the standard action of $\text{Sp}_{2g}(\mathbb{F}_2)$ on $J[2]$.

**Remark 5.6.** It follows from the connectedness of the moduli space of genus-$g$ curves [DM69] that the isomorphism type of each structure in Proposition 5.4 depends only on $g$, and not on $k$ or $X$.

**Proposition 5.7.** For $g \geq 2$, we have $\#\Sigma = \frac{2g-3}{3}(2^{2g-1})(2^{2g-2} - 1)(2^{g-1} - 1)$.

**Proof.** Since $\text{Sp}_{2g}(\mathbb{F}_2)$ acts transitively on $J[2] - \{0\}$, all fibers of the summing map $(\mathcal{S}_{\vartheta})/\sim \to J[2] - \{0\} \subseteq \text{Pic}_{X}(\omega)[2]$ have the same size, namely $(2^{g-1} - 1)/2 = 2^{2g-3} - 2^{g-2}$. Hence the number of pairs of pairs such that the two pairs have the same image in $J[2] - \{0\}$ is $(2^{2g-1} - 1)(2^{g-3} - 2^{g-2})$. Each such pair of pairs consists of disjoint pairs, since $x + y = x + z$ would imply $y = z$. Thus each pair of pairs corresponds to a 4-element subset of $\mathcal{S}_{\vartheta}$ summing to 0 with a partition into two pairs. Each 4-element subset can be partitioned in 3 ways, so
\[
\#\Sigma = \frac{1}{3}(2^{2g-1} - 1)\left(\frac{2^{2g-3} - 2^{g-2}}{2}\right) = \frac{2^{g-3}}{3}(2^{2g-1} - 1)(2^{2g-2} - 1)(2^{g-2} - 1).
\]

5.3. Representing odd theta characteristics by divisors over the ground field.

**Proposition 5.8.** An odd theta characteristic $\vartheta$ on $X_s$ whose class lies in $(\text{Pic}_{X_s})^G$ is represented by an element of $\text{Div} X$.

**Proof.** The $k$-scheme parametrizing effective divisors whose class equals $\vartheta$ is a Brauer-Severi variety, a twisted form of $\mathbb{P}^{h^0(\vartheta) - 1}$, corresponding to a central simple algebra of dimension $h^0(\vartheta)^2$ and hence of index dividing $h^0(\vartheta)$ [GS06, Theorems 5.2.1 and 2.4.3], so the associated Brauer class $\tau \in \text{Br} k$ is killed by the odd integer $h^0(\vartheta)$ [GS06, Proposition 4.5.13(1)]. On the other hand, the Hochschild-Serre spectral sequence yields an exact sequence
\[\text{Pic} X \to (\text{Pic} X_s)^G \to \text{Br} k\]
under which the second map sends $\vartheta$ to $\tau$ and $\omega$ to 0, so $2\tau = 0$. Thus $\tau = 0$. So $\vartheta$ comes from an element of $\text{Pic} X$, or, equivalently, from an element of $\text{Div} X$. 

9
6. Generalized explicit descent

6.1. The setting. Suppose that $X$ is a nice variety over $k$. Let $J := \text{Alb}_X$.

6.2. True descent. To motivate the definition of a true descent setup, we recall the following:

**Example 6.1.** Assume $\text{char } k \neq 2$. Let $F(x) \in k[x]$ be a non-constant separable polynomial of odd degree $2g + 1$. Let $X$ be the smooth projective model of the curve $y^2 = F(x)$, so $X$ is a hyperelliptic curve of genus $g$. Let $\infty$ be the unique point at infinity on $X$, and let $\Delta \subset X$ be the 0-dimensional $k$-scheme such that $\Delta(k_s)$ consists of the $2g + 1$ Weierstrass points not equal to $\infty$. Then there is a surjection $(\mathbb{Z}/2\mathbb{Z})^\Delta \to \tilde{J}[2]$ sending each basis element $P \in \Delta(k_s)$ to the divisor class $[P - \infty]$ (see [Mum84, Lemma 2.4 and Corollary 2.11]). The family of divisors $P - \infty$ indexed by $P \in \Delta(k_s)$ may be viewed as a single divisor $\beta$ on $X \times \Delta$.

**Definition 6.2.** A true descent setup for $X$ consists of a triple $(n, \Delta, \mathcal{L})$, where $n$ is a positive integer not divisible by char $k$, $\Delta = \text{Spec } L$ is a finite étale $k$-scheme, and $\mathcal{L}$ is a line bundle on $X \times \Delta$ such that $\mathcal{L}^\otimes n \simeq \mathcal{O}$. In more concrete terms, if we choose $\beta \in \text{Div}(X \times \Delta)$ representing $\mathcal{L}$, the condition on $\beta$ is that $n\beta$ is principal; i.e., there is a function $f \in k(X \times \Delta)^\times$ such that $\text{div}(f) = n\beta$.

**Remark 6.3.** Given $\beta$, for each $P \in \Delta(k_s)$, we have the fiber $\beta_P \in \text{Div}_X$. In fact, we may think of $\beta$ as the family of divisors $\beta_P$ depending $\mathcal{G}$-equivariantly on $P$. Similarly, $f$ may be thought of as a family of functions $f_P \in k(X_s)^\times$.

Given $(n, \Delta, \mathcal{L})$, we will define a homomorphism

$$C: J(k) \to \frac{L_x}{L \times n}$$

using cohomology, and relate it to a more explicit homomorphism.

6.2.1. Cohomological definition. Take cohomology of

$$0 \to J[n] \to J \xrightarrow{n} J \to 0$$

to obtain $J(k) \to H^1(J[n])$. The condition on $\mathcal{L}$ (or $\beta$) implies that it induces a map $\Delta \to \tilde{J}[n]$, and hence a homomorphism $(\mathbb{Z}/n\mathbb{Z})^\Delta \to \tilde{J}[n]$. Taking the Cartier dual and applying Remark 3.8 yields $\alpha: J[n] \to \mu^\Delta_n$. Composition yields a homomorphism

$$C: J(k) \to H^1(J[n]) \xrightarrow{\alpha} H^1(\mu^\Delta_n) \simeq \frac{L_x}{L \times n}. \quad (3)$$

6.2.2. Explicit definition. Choose $\beta$ and $f$ as in Definition 6.2. Let $X^{\text{good}}$ be the largest open subscheme of $X$ such that $f$ is an invertible regular function on $X^{\text{good}} \times \Delta$. Then $f$ defines a morphism $X^{\text{good}} \times \Delta \to \mathbb{G}_m$, and hence a morphism $X^{\text{good}} \to \mathbb{G}^\Delta_m$. Evaluating on closed points and taking norms (this is necessary if the closed point is of degree greater than 1), we obtain a homomorphism $\mathcal{Z}(X^{\text{good}}) \to L^\times$. This induces $\mathcal{Z}^0(X^{\text{good}}) \to L^\times/L^{\times n}$. If we change $(\beta, f)$ to $(\beta', f')$, then $\beta' - \beta$ is the divisor of some $g \in k(X)^\times$, and $f' = cg^n f$ for some $c \in k^\times$. If we evaluate on any $z \in \mathcal{Z}^0(X)$ that is good for both $f$ and $f'$, then the value of the homomorphism in $L^\times/L^{\times n}$ is unchanged (the value of $g$ gives an $n^{\text{th}}$ power, and the
value of \( c \) is \( c^{\deg z} = 1 \). Given any \( z \in \mathcal{Z}^0(X) \), we can move \( \beta \) to avoid \( z \), so the compatible homomorphisms glue to give a homomorphism

\[
\tilde{C} : \mathcal{Z}^0(X) \to \frac{L^*}{L^*}.
\]

6.2.3. Compatibility of the two definitions.

**Proposition 6.4.** The maps \( C \) and \( \tilde{C} \) are compatible in the sense that the following diagram commutes:

\[
\begin{array}{ccc}
\mathcal{Z}^0(X) & \xrightarrow{\tilde{C}} & \frac{L^*}{L^*} \\
\downarrow & & \downarrow \\
J(k) & \xrightarrow{\alpha} & H^1(J[n]) \xrightarrow{\sim} \frac{L^*}{L^*}
\end{array}
\]

**Proof.** We may fix \((\beta, f)\) and consider \( \mathcal{Z}^0(X)_{\text{good}} \) instead of \( \mathcal{Z}^0(X) \). Let \( \mathcal{Z}^0 = \mathcal{Z}^0(X)_{\text{good}} \) and let \( \mathcal{Y}^0 \) be the Albanese kernel in the exact sequence of \( \mathcal{G} \)-modules

\[
0 \to \mathcal{Y}^0 \to \mathcal{Z}^0 \to J(k_s) \to 0.
\]

We will construct the following commutative diagram of \( \mathcal{G} \)-modules with exact rows (we write \( J \) for \( J(k_s) \), and so on):

\[
\begin{array}{ccc}
0 & \to & J[n] \\
\downarrow & & \downarrow \\
\mathcal{Z}^0 & \xrightarrow{\alpha} & \mathcal{Z}^0 \times \mathcal{Y}^0 \xrightarrow{nz+y} \mathcal{Z}^0 \to 0 \\
\downarrow & & \downarrow \\
0 & \to & \mathcal{G}_m^n \\
\end{array}
\]

The top and bottom rows are familiar. Surjectivity of the map \( \mathcal{Z}^0 \times \mathcal{Y}^0 \to \mathcal{Z}^0 \) given by \((z, y) \mapsto nz + y\) follows from surjectivity of multiplication by \( n \) on \( J(k_s) = \mathcal{Z}^0/\mathcal{Y}^0 \); let \( \widetilde{J}[n] \) be the kernel of the \( nz + y \) map. We have

\[
\widetilde{J}[n] = \{(z, -nz) \in \mathcal{Z}^0 \times \mathcal{Y}^0 : [z] \in J[n](k_s)\}.
\]

All the upward maps are induced by \( \mathcal{Z}^0 \to J(k_s) \), so commutativity of the top part of the diagram is straightforward.

The middle and rightmost downward maps in (5) are given by

\[
\begin{array}{c}
\mathcal{Z}^0 \times \mathcal{Y}^0 \\
\downarrow \quad y \\
\mathcal{G}_m^\Delta
\end{array}
\]

\[
\begin{array}{c}
f(z) \quad [y, \beta] \\
\downarrow \quad \\
\mathcal{G}_m^\Delta
\end{array}
\]

The bottom right square commutes since

\[
(f(z) \cdot [y, \beta])^n = f(nz) \cdot [y, n\beta] = f(nz)f(y) = \tilde{C}(nz + y).
\]

The leftmost downward vertical map is obtained by restricting the middle one.
Finally, we check that \( \alpha \) and the vertical maps in the first column form a commutative triangle. Since \( \alpha \) sends \( P \) to \( [\beta P] \), Remark 4.1 and the Albanese-Picard definition of \( e_n \) show that for any \( [z] \in J[n] \),
\[
\alpha([z]) = e_n([z], [\beta]) = \frac{f(z)}{[nz, \beta]} = f(z) \cdot [-nz, \beta],
\]
so the images of an element \( (z, -nz) \in \widetilde{J}[n] \) under the two paths to \( \mu_n^\Delta \) are equal. This completes the construction of (5).

Taking cohomology of (5) yields
\[
\begin{array}{c}
J(k) \xrightarrow{n} J(k) \xrightarrow{\alpha} H^1(J[n]) \\
\bigg\downarrow \quad \bigg\downarrow \quad \bigg\downarrow \\
Z^0(X^{\text{good}}) \xrightarrow{\tilde{C}} H^1(\widetilde{J}[n]) \xrightarrow{\alpha} H^1(\mu_n^\Delta).
\end{array}
\]

Equality of the compositions from \( Z^0(X^{\text{good}}) \) to \( H^1(\mu_n^\Delta) \) is the desired result.

**Remark 6.5.** If \( U \) is a dense open subscheme of \( X \), then by a moving lemma, \( Z^0(U) \) and \( Z^0(X) \) have the same image in \( J(k) \). (Proof: It suffices to prove that any closed point \( x \) of \( X \) is rationally equivalent to a 0-cycle supported on \( U \). Pick a closed point \( u \in U \). By a classical Bertini theorem, or [Poo04, Corollary 3.4] if \( k \) is finite, we can find a nice curve \( C \subseteq X \) through \( x \) and \( u \), and hence reduce to the case in which \( X \) is a curve. In this case, it suffices to apply weak approximation to find a rational function on \( X \) with prescribed valuations at the points of \( X - U \).)

**Corollary 6.6.** The explicit homomorphism \( \tilde{C} \) in (4) induces a homomorphism
\[
\tilde{C} : \left( \begin{array}{c}
J(k) \\
nJ(k)
\end{array} \right) \xrightarrow{\circ} \frac{L^x}{L^{x n}}.
\]

6.3. **Fake descent.** For computations using true descent setups to be practical, the degrees of the components of \( \Delta \) (i.e., the degrees of the field extensions \( L_i \) whose product is \( L \)) should be not too large. A fake descent setup will be a variant of the true descent setup, a variant that may allow a simpler \( \Delta \) to be used, at the expense of giving less direct information about Selmer groups. In Section 6.5 we show that the true descent setup can be viewed as a special case of the fake descent setup.

**Definition 6.7.** A fake descent setup for \( X \) consists of a triple \((n, \Delta, \mathcal{L})\), where \( n \) is a positive integer not divisible by \( \text{char } k \), \( \Delta = \text{Spec } L \) is a nonempty finite étale \( k \)-scheme, and \( \mathcal{L} \) is a line bundle on \( X \times \Delta \) such that \( \mathcal{L}^\otimes n \) is the pullback of a line bundle on \( X \). Equivalently, in terms of a divisor \( \beta \in \text{Div}(X \times \Delta) \) representing \( \mathcal{L} \), the condition is that there exists \( D \in \text{Div } X \) such that \( n\beta - (D \times \Delta) \) is principal; i.e., there is a function \( f \in k(X \times \Delta)^\times \) such that \( \text{div}(f) = n\beta - (D \times \Delta) \).

**Remark 6.8.** On the fibers, the last condition says that \( \text{div}(f_P) = n\beta_P - D \) for all \( P \in \Delta(k_s) \). Subtracting shows that \( [\beta_P - \beta_Q] \in \widetilde{J}[n] \) for all \( P, Q \in \Delta(k_s) \).
Examples 6.9. Definition 6.7 is motivated by the following examples of fake descent setups for curves.

(i) Assume char \( k \neq 2 \). Let \( \pi : X \to \mathbb{P}^1_k \) be a (ramified) degree-2 cover, so \( X \) is a hyperelliptic curve. Let \( n = 2 \), let \( \Delta \subset X \) be the ramification locus of \( \pi \), and let \( \beta \) be the diagonal copy of \( \Delta \) in \( X \times \Delta \). Then we can take \( D = \pi^*(y) \) for some \( y \in \mathbb{P}^1(k) \) (cf. [FPS97]). See Example 10.19 for more about this case.

(ii) The previous example generalizes to other geometrically generically cyclic covers \( \pi : X \to \mathbb{P}^1_k \) (cf. [PS97]). Let \( n \geq 2 \). Let \( k \) be a field with char \( k \nmid n \). Suppose that \( F(x) \in k[x] \) factors completely in \( k_s[x] \) and is not a \( p \)th power in \( k_s[x] \) for any \( p \mid n \). Let \( X \) be the smooth projective model of \( y^n = F(x) \). Let \( \pi : X \to \mathbb{P}^1 \) be the \( x \)-coordinate map. Let \( \Delta \) be the ramification locus of \( \pi \). Let \( \beta \) be the diagonal copy of \( \Delta \) in \( X \times \Delta \). Then we can take \( D = \pi^*(t) \) for some \( t \in \mathbb{P}^1(k) \).

(iii) Assume char \( k \notin \{2, 3, 7\} \). Let \( X \) be a twist of the Klein quartic curve \( x^3y + y^3z + z^3x = 0 \) in \( \mathbb{P}^2 \). Let \( n = 2 \), let \( \Delta \) correspond to the \( G \)-set of 8 triangles, as defined in [PSS07, §11.1], and let \( \beta \in \text{Div}(X \times \Delta) \) be the divisor of relative degree 3 over \( \Delta \) such that each \( \beta_P \) is the sum of the 3 points in the corresponding triangle. This gives a fake descent setup, provided that \( D \) can be found (as turned out to be the case for the curves of interest in [PSS07]).

(iv) Assume char \( k \neq 2 \). Let \( X \) be any curve of genus \( g \geq 2 \) over \( k \). Let \( n = 2 \). Let \( \Delta \) correspond to the \( G \)-set of odd theta characteristics on \( X_s \). Proposition 5.8 applied over the residue fields of each point of \( \Delta \) shows that one can find \( \beta \in \text{Div}(X \times \Delta) \) such that each \( \beta_P \) is the corresponding odd theta characteristic. Then one can take \( D \) to be a canonical divisor. This gives a fake descent setup that in principle can be used to perform a 2-descent on the Jacobian of \( X \). When \( g = 2 \), this specializes to Example (i).

A fake descent setup \((n, \Delta, \mathcal{L})\) will give rise to a cohomologically defined homomorphism

\[
C : J(k) \to H^1\left( \frac{\mu_n^\Delta}{\mu_n} \right)
\]

that we will relate to an explicit homomorphism

\[
\tilde{C} : Z^0(X) \to \frac{L^\times}{L^\times n_k^\times}.
\]

6.3.1. Cohomological definition. By the final statement in Remark 6.8, \( \mathcal{L} \) (or \( \beta \)) induces a homomorphism

\[
\alpha^\vee : (\mathbb{Z}/n\mathbb{Z})_{\deg 0}^\Delta \to \widehat{J}[n]
\]

Dualizing

\[
0 \to (\mathbb{Z}/n\mathbb{Z})_{\deg 0}^\Delta \to (\mathbb{Z}/n\mathbb{Z})^\Delta \to \mathbb{Z}/n\mathbb{Z} \to 0
\]

yields \((\mathbb{Z}/n\mathbb{Z})_{\deg 0}^\Delta\)^\vee \cong \mu_n^\Delta / \mu_n\), so the dual of \( \alpha^\vee \) is a homomorphism

\[
\alpha : J[n] \to \frac{\mu_n^\Delta}{\mu_n}.
\]

The composition

\[
J(k) \to H^1(J[n]) \xrightarrow{\alpha} H^1\left( \frac{\mu_n^\Delta}{\mu_n} \right)
\]

is the desired homomorphism \( C \).
6.3.2. **Explicit definition.** As in Section 6.2.2, \( f \) gives rise to a homomorphism \( \mathcal{Z}(X_{\text{good}}) \to L^\times \). If we change \((\beta, D, f)\) to \((\beta', D', f')\), then \( \beta' - \beta \) is the divisor of some \( g \in k(X \times \Delta)^\times \), \( D' - D \) is the divisor of some \( h \in k(X)^\times \), and \( f' = (cg^n/h)f \) for some \( c \in k(\Delta)^\times = L^\times \). If we evaluate on any \( z \in \mathcal{Z}(X) \) that is good for both \( f \) and \( f' \), then the value of the homomorphism in \( L^\times /L^\times n k^\times \) is unchanged (the value of \( g^n/h \) gives an element of \( L^\times n k^\times \), and the value of \( c \) is \( c^\deg z = c^0 = 1 \)). Thus we obtain (7).

6.3.3. **Compatibility of the two definitions.** Taking cohomology of

\[
0 \to \mu_n \to \mu_n^\Delta \to \frac{\mu_n^\Delta}{\mu_n} \to 0
\]

yields

\[
\frac{k^\times}{k^\times n} \to \frac{L^\times}{L^\times n} \to H^1\left(\frac{\mu_n^\Delta}{\mu_n}\right) \to \text{Br} k,
\]

so we may identify \( L^\times /L^\times n k^\times \) with a subgroup of \( H^1(\mu_n^\Delta/\mu_n) \).

**Proposition 6.10.** The two maps \( C \) and \( \tilde{C} \) are compatible in the sense that the following diagram commutes:

\[
\begin{array}{ccc}
\mathcal{Z}^0(X) & \xrightarrow{\beta} & J(k) \\
\downarrow & & \downarrow \\
J(k) & \xrightarrow{\alpha} & H^1(J[n]) \xrightarrow{\beta} H^1\left(\frac{\mu_n^\Delta}{\mu_n}\right) \xrightarrow{\alpha} L^\times /L^\times n k^\times
\end{array}
\]

**Proof.** We replace the pairing \([y, \beta]\) used in the true case with

\[
\mathcal{Y}^0 \to \frac{\mathbb{G}_m^\Delta(k_s)}{\mu_n(k_s)}
\]

\[
y \mapsto [y, \beta]_D := \frac{[y, \beta - H]}{h(y)^{1/n}}
\]

where \( H \in \text{Div}(X_s) \) and \( h \in k_s(X)^\times \) are chosen so that \( \text{div}(h) = D - nH \), and \( h(y)^{1/n} \) is a chosen \( n^\text{th} \) root of \( h(y) \) (and then \( H \) and \( h(y)^{1/n} \) are pulled back to \( (X \times \Delta)_s \); such \( H \) and \( h \) exist because one possibility is to take \( H = \beta_P \) for some \( P \in \Delta(k_s) \). If we change \( H \) to another choice \( H' \), then \( h \) is changed to \( h' \) where \( \text{div}(j) = nH - nH' \), so the value of (9) is multiplied by \([y, H - H']/j(y)^{1/n}\), which lies in \( \mu_n(k_s) \) since its \( n^\text{th} \) power equals \([y, \text{div}(j)]/j(y) = 1 \). Thus (9) is well-defined and Galois-equivariant. Also,

\[
[y, \beta]_D^n = \frac{[y, n\beta - nH]}{h(y)} = \frac{[y, \text{div}(fh)]}{h(y)} = \frac{(fh)(y)}{h(y)} = f(y).
\]
As in the proof of Proposition 6.4, we construct a commutative diagram with exact rows:

\[
\begin{array}{cccccccccccc}
0 & \longrightarrow & J[n] & \longrightarrow & J & \longrightarrow & J & \longrightarrow & 0 \\
& & \uparrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \tilde{J}[n] & \longrightarrow & \mathcal{Z}^0 \times \mathcal{Y}^0 & \longrightarrow & \mathcal{Z}^0[nz+y] & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mu_n^\Delta & \longrightarrow & G_m^\Delta[nz+y] & \longrightarrow & 0 \\
\end{array}
\]

The first two rows and the vertical maps between them are the same as in (5). The bottom row is a pushout of the bottom row of (5).

The middle downward map is

\[
\mathcal{Z}^0 \times \mathcal{Y}^0 \longrightarrow \frac{G_m^\Delta}{\mu_n}
\]

\[
z, y \mapsto f(z)[y, \beta]_D
\]

The rightmost downward map is

\[
\tilde{C}: \mathcal{Z}^0(X_{\text{good}}) \longrightarrow G_m^\Delta
\]

\[
z \mapsto f(z)
\]

The bottom right square commutes since (10) implies

\[
(f(z)[y, \beta]_D)^n = f(z)^n f(y) = f(nz + y).
\]

The leftmost downward vertical map is obtained by restricting the middle one.

Finally, we check that \(\alpha\) and the vertical maps in the first column form a commutative triangle. Any \((z, -nz) \in \tilde{J}[n]\) maps up to \([z] \in J[n]\), and maps right and down to \(f(z) \cdot [-nz, \beta]_D \in \frac{G_m^\Delta}{\mu_n}\). Remark 4.1 and the Albanese-Picard definition of \(e_n\) show that

\[
\alpha([z]) = e_n([z], [\beta - H]) = \frac{f(z)h(z)}{[nz, \beta - H]} = f(z) \cdot [-nz, \beta]_D \in \frac{G_m^\Delta}{\mu_n}.
\]

So the triangle commutes. This completes the construction of (11).

Taking cohomology of (11) yields

\[
\begin{array}{cccccccccccc}
J(k) & \longrightarrow & J(k) & \longrightarrow & H^1(J[n]) \\
& & \uparrow & & \downarrow & & \downarrow & & \\
\mathcal{Z}^0(X_{\text{good}}) & \longrightarrow & H^1(\tilde{J}[n]) & \longrightarrow & \tilde{C} & \longrightarrow & H^1(\frac{\mu_n^\Delta}{\mu_n}) \\
& & \downarrow & & \downarrow & & \downarrow & & \\
L^\times & \longrightarrow & H^1(\frac{\mu_n^\Delta}{\mu_n}) & \longrightarrow & 0.
\end{array}
\]

Equality of the compositions from \(\mathcal{Z}^0(X_{\text{good}})\) to \(H^1(\frac{\mu_n^\Delta}{\mu_n})\) is the desired result. \(\square\)
Corollary 6.11. The explicit homomorphism $\tilde{C}$ in (7) induces a homomorphism

$$\tilde{C}: \left( \frac{J(k)}{nJ(k)} \right) \to \frac{L^\times}{L^\times \times k^\times}.$$ 

Corollary 6.12. The homomorphism $\tilde{C}$, which a priori depends on $\beta$ and $D$, in fact is independent of $D$ and depends only on the linear equivalence class of $\beta$.

Proof. The linear equivalence class of $\beta$ is all that is needed to define $C$. □

Remark 6.13. By Corollary 6.12, we may move $\beta$ and $D$ within their linear equivalence classes and change $f$ accordingly in order to make $\text{div}(f)$ avoid any particular 0-cycle. Hence we may view $\tilde{C}$ as being defined on all of $\mathbb{Z}^0(X)$.

6.4. Isogenies associated to descent setups. Given a true or fake descent setup, we obtain a homomorphism $\alpha^\vee: E \to \hat{J}[n]$, where $E := (\mathbb{Z}/n\mathbb{Z})^\Delta$ for a true descent setup and $E := (\mathbb{Z}/n\mathbb{Z})_{\text{deg 0}}^\Delta$ for a fake descent setup.

In either case we obtain an isogeny $\hat{\phi}: \hat{J} \to \hat{A} := \hat{J}/\alpha^\vee(E)$, and $\hat{J}[\hat{\phi}] = \alpha^\vee(E)$. Let $A$ be the dual abelian variety of $\hat{A}$, and let $\phi: A \to J$ be the dual of $\hat{\phi}$. (For an early instance of relating the functions in a true descent setup to an isogeny between different abelian varieties, for the purpose of computing Selmer groups, see [Sch98].)

Proposition 6.14. The homomorphism $C: J(k) \to H^1(E^\vee)$ factors through the quotient $J(k)/\phi A(k)$.

Proof. By [Mum70, §III.15, Theorem 1], $A[\phi]^\vee \simeq \hat{J}[\hat{\phi}]$. Now $\alpha^\vee: E \to \hat{J}[n]$ factors through $\alpha^\vee(E) = \hat{J}[\hat{\phi}]$, and dualizing shows that $\alpha: J[n] \to E^\vee$ factors through $A[\phi]$. This explains the right triangle in the commutative diagram

$$\begin{array}{ccc}
\frac{J(k)}{nJ(k)} & \to & H^1(J[n]) \\
\downarrow & & \downarrow \\
\frac{J(k)}{\phi A(k)} & \to & H^1(A[\phi]),
\end{array}$$

while the square comes from functoriality of connecting homomorphisms. Since the top row gives $C$, the result follows. □

Corollary 6.15. The explicit homomorphism $\tilde{C}$ defined on $\mathbb{Z}^0(X)$ factors through not only $J(k)_o$ or $(J(k)/nJ(k))_o$, but also $(J(k)/\phi A(k))_o$.


Let $R := \ker \alpha^\vee$, so we have an exact sequence

$$0 \to R \to E \xrightarrow{\alpha^\vee} \hat{J}[\hat{\phi}] \to 0.$$  

Dualizing yields an exact sequence

$$0 \to A[\phi] \xrightarrow{\alpha} E^\vee \xrightarrow{q} R^\vee \to 0.$$
Take cohomology: for a true descent setup we obtain

\[ \begin{array}{ccccccccc}
0 & \longrightarrow & A[\phi](k) & \longrightarrow & E^\vee(k) & \longrightarrow & R^\vee(k) & \longrightarrow & H^1(A[\phi]) & \longrightarrow \quad (15)
\end{array} \]

\[ \begin{array}{ccccccccc}
0 & \longrightarrow & A[\phi](k) & \longrightarrow & E^\vee(k) & \longrightarrow & R^\vee(k) & \longrightarrow & H^1(A[\phi]) & \longrightarrow \quad (16)
\end{array} \]

and for a fake descent setup we obtain

The commutativity follows from Proposition 6.4 or Proposition 6.10.

6.5. Comparison of true and fake descent setups. A fake descent setup \((n, \Delta, \mathcal{L})\) in which there exists \(P \in \Delta(k)\) gives rise to a true descent setup \((n, \Delta', \mathcal{L}')\) as follows:

Let \(\Delta' = \Delta - \{P\}\) and define \(\beta'_Q = \beta_Q - \beta_P\) for each \(Q \in \Delta'.\) The étale algebras \(L, L'\) corresponding to \(\Delta, \Delta'\) satisfy \(L \simeq L' \times k.\) One can check that the fake diagram (11) maps to the true diagram (5) as follows: the first two rows map via the identity, and the third row maps via the homomorphisms induced by \((c_Q)_{Q \in \Delta} \mapsto (c_Q/c_P)_{Q \in \Delta'}\). Finally, the explicit true and fake homomorphisms are compatible in the sense that

\[ \begin{array}{ccccccccc}
\left( \begin{array}{c}
J(k) \\
\phi A(k)
\end{array} \right) & \longrightarrow & \left( \begin{array}{c}
L^x \\
L^n
\end{array} \right) \\
\text{true} & \text{fake} & \text{true} & \text{fake}
\end{array} \]

\[ \begin{array}{ccccccccc}
\left( \begin{array}{c}
J(k) \\
\phi A(k)
\end{array} \right) & \longrightarrow & \left( \begin{array}{c}
L^x \\
L^n k^x
\end{array} \right)
\end{array} \]

The commutativity follows from Proposition 6.4 or Proposition 6.10.

6.6. Notation. For our intended application, we are primarily interested in fake descent. To avoid having to state things twice, we let \(L^x/L^n k^x\) denote \(L^x/L^n\) in the context of a true descent setup, or \(L^x/L^n k^x\) in the context of a fake descent setup. If \(v \in \Omega_k\), let \(L_v := L \otimes_k k_v\) and define \(L^x_v/L^n_v k^x_v\) similarly. Decompose \(L\) as \(\prod L_i\) where each \(L_i\) is a field.

6.7. Restrictions on the image of \(\bar{C}\). Recall that \(R \subseteq E \subseteq (\mathbb{Z}/n\mathbb{Z})^\Delta.\)

**Lemma 6.16.** Suppose that the image of the diagonal \(\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\Delta\) is contained in \(R.\) Then the image of \(\bar{C}: \mathbb{Z}^0(X) \to L^x/L^n k^x\) is contained in the kernel of the homomorphism \(N: L^x/L^n k^x \to k^x/k^n\) induced by the norm map \(L^x \to k^x.\)
Proof. Dualizing the complex
\[ \mathbb{Z}/n\mathbb{Z} \hookrightarrow E \rightarrow \widehat{J}[\widehat{\phi}] \]
and applying $H^1$ yields a complex
\[ H^1(A[\phi]) \rightarrow H^1(E^v) \xrightarrow{\phi} \mathbb{F}_{k^n}. \]
The restriction of $\mathcal{N}$ to the subgroup $L^\times / L_v^\times k_v^\times$ equals $N$, because it is induced by dualizing $\mathbb{Z}/n\mathbb{Z} \rightarrow (\mathbb{Z}/n\mathbb{Z})^\Delta$ and taking cohomology. The result now follows from the commutative squares in (15) and (16).

7. Unramified classes

7.1. Local and global unramified classes. Let $k_v$ be a non-archimedean local field. If $M$ is any $G_{k_v}$-module, define the subgroup of unramified classes
\[ H^1(k_v, M)_{unr} := \ker \left( H^1(k_v, M) \rightarrow H^1(k_v, M_v, M) \right) \simeq H^1(\text{Gal}(k_v/k_v), (M(k_v, u)), \text{Gal}(k_v/k_v), M(k_v, u)), \]
where the isomorphism follows from the inflation-restriction sequence.

Now let $k$ be a global field, and let $\Omega_k$ be a subset of $\Omega_k$ containing the archimedean places. If $M$ is any $G_k$-module, define the subgroup of classes unramified outside $\Omega_k$, $H^1(k, M)_{\Omega_k}$, as the set of $\xi \in H^1(k, M)$ whose restriction in $H^1(k_v, M)$ lies in $H^1(k_v, M)_{unr}$ for all $v \notin \Omega_k$.

7.2. A Tamagawa number criterion. Let $k_v$ be a non-archimedean local field. Let $\phi: A \rightarrow J$ be a separable isogeny of abelian varieties over $k_v$. The short exact sequence
\[ 0 \rightarrow A[\phi] \rightarrow A \xrightarrow{\phi} J \rightarrow 0 \]
gives rise to a connecting homomorphism $\gamma_v: J(k_v) \rightarrow H^1(k_v, A[\phi])$. Let $J$ be the Néron model of $J$ over $O_v$. Let $J^0$ be the connected component of the identity in $J$. Let $\Phi$ be the group of connected components of the special fiber $J \times \mathbb{F}_v$, so $\Phi$ is a finite étale commutative $\mathbb{F}_v$-group scheme. The number $c_v(J) := \#\Phi(\mathbb{F}_v)$ is called the Tamagawa number of $J$ at $v$.

We use analogous notation for objects related to $A$.

Lemma 7.1. Let $\phi: A \rightarrow J$ be as above. Let $n$ be a positive integer such that $nA[\phi] = 0$ (one possibility is $n = \deg \phi$). If the residue characteristic $\text{char} \mathbb{F}_v$ does not divide $n$, and if $c_v(J)$ and $c_v(A)$ are coprime to $n$, then $\gamma_v(J(k_v)) = H^1(k_v, A[\phi]_{unr})$.

Proof. This is a straightforward generalization of the proof of [SS04, Lemma 3.1 and Proposition 3.2], which uses results from [Sch96, §3].

7.3. Unramified elements in the target of the descent map. Now suppose that $k$ is a global field and that we have a true or fake descent setup. From (15) or (16) applied to $k_v$ we obtain $L^\times / L_v^\times k_v^\times \hookrightarrow H^1(k_v, E^v)$. Call an element of $L^\times / L_v^\times k_v^\times$ unramified if its image in $H^1(k_v, E^v)$ is unramified.

Let $\mathcal{S}$ be a subset of $\Omega_k$ containing the archimedean places. Say that an element of $L^\times / L_v^\times k_v^\times$ is unramified outside $\mathcal{S}$ if its image in $L^\times / L_v^\times k_v^\times$ is unramified for each $v \notin \mathcal{S}$. Let $(L^\times / L_v^\times k_v^\times)_\mathcal{S}$ be the subgroup of such elements. Proposition 7.2 will provide an explicit description of $(L^\times / L_v^\times k_v^\times)_\mathcal{S}$. 

18
Given \( \ell \in L = \prod L_i \), let \( \ell_i \) be its image in \( L_i \). Let \( L(n, S) \) be the subgroup of \( L^x/L^{xn} \) consisting of elements represented by \( \ell \in L^x \) such that the prime-to-\( S \) part of the fractional ideal \((\ell_i)\) of \( L_i \) is an \( n^{th} \) power for all \( i \). In the true case, let \( \overset{\sim}{L}(n, S) = L(n, S) \); in the fake case, let \( \overset{\sim}{L}(n, S) \) be the subgroup of \( L^{x}/L^{xn}k^{x} \) consisting of elements represented by \( \ell \in L^{x} \) for which there exists a fractional ideal \( a \) of \( k \) such that the prime-to-\( S \) part of \( a \cdot (\ell_i) \) is an \( n^{th} \) power for all \( i \).

**Proposition 7.2.** Suppose that \( S \subseteq \Omega_k \) contains all archimedean places and all places of residue characteristic dividing \( n \). Then \((L^x/L^{xn}k^{x})_S = \overset{\sim}{L}(n, S)\).

**Proof.** The statement and proof are the same as for [PS97, Proposition 12.5]. \( \square \)

**Proposition 7.3.** The group \( \overset{\sim}{L}(n, S) \) is finite and computable.

**Proof.** Let \( O_S \) and \( O_{L,S} \) be the rings of \( S \)-integers in \( k \) and \( L \), respectively; then there are exact sequences

\[
0 \to \frac{O_{L,S}^{x}}{O_{L,S}^{xn}} \to L(n, S) \to \text{Cl}(O_{L,S})[n] \to 0
\]

and (in the fake case)

\[
k(n, S) \to L(n, S) \to \overset{\sim}{L}(n, S) \to \frac{\text{Cl}(O_S)}{n\text{Cl}(O_S)}.
\]

as in [PS97, Propositions 12.6 and 12.8], where these are constructed for prime \( n \). So the finiteness follows from the Dirichlet \( S \)-unit theorem and finiteness of the class groups, and the computability follows too since these are effective. \( \square \)

**Remark 7.4.** The computation of the unit groups and class groups typically dominates the running time in performing explicit descent.

**Proposition 7.5.** Let \( M \) be a finite \( G \)-module with \( \text{char } k \nmid \# M \). Let \( S \) be a finite set of places of \( k \) containing the archimedean places. Then \( H^1(k, M)_S \) is finite.

**Proof.** Using the inflation-restriction sequence lets us enlarge \( k \) to assume that \( G \) acts trivially on \( M \) and on the roots of unity of order dividing \( \# M \). Decomposing \( M \) as a product of cyclic groups lets us reduce to the case \( M = \mu_n \) where \( \text{char } k \nmid n \). Now \( H^1(k, \mu_n)_S \simeq (k^x/k^{xn})_S \), which, as in Proposition 7.3, is finite. \( \square \)

8. **Finite Galois modules and \( III^1 \)**

Let \( k \) be a global field, and let \( M \) be a finite \( G_k \)-module. If \( v \) is a place of \( k \), write \( H^1(k, M) \to H^1(k_v, M) \) for the restriction to a decomposition group associated to \( v \); if \( \xi \in H^1(k, M) \), let \( \xi_v \in H^1(k_v, M) \) be its restriction. As usual, define

\[
III^1(k, M) := \ker \left( H^1(k, M) \to \prod_{v \in \Omega_k} H^1(k_v, M) \right).
\]

**Lemma 8.1** (cf. [Mil06, Example I.4.11(i)]). If \( G_k \) acts trivially on \( M \), then \( III^1(k, M) = 0 \).
Proof. The hypothesis implies that $H^1(k, M) = \text{Hom}(G_k, M)$, where $\text{Hom}$ denotes the group of continuous homomorphisms. Chebotarev’s density theorem implies that the union of the decomposition groups $G_k_v$ is dense in $G_k$, so the map

$$\text{Hom}(G_k, M) \to \prod_v \text{Hom}(G_{k_v}, M)$$

is injective. This implies the result. □

Lemma 8.2. If $p$ is a prime not equal to $\text{char} \ k$, and $\Delta$ is any $G$-set, then $\Pi^1(k, \mu_p^\Delta) = 0$.

Proof. By Shapiro’s lemma, one reduces to proving that $\Pi^1(k, \mu_p) = 0$. The latter is the well-known fact that an element of $k^\times$ that is a $p$th power in every $k_v$ is a $p$th power in $k$. □

The following result allows us to compute $\Pi^1(k, M)$ using finite group cohomology.

Proposition 8.3. Let $k$ be a global field, let $M$ be a finite $G_k$-module, and let $K$ be a Galois splitting field of $M$. Let $G = \text{Gal}(K/k)$. For $v \in \Omega_k$, let $D_v \subset G$ denote a decomposition group. Then

$$\Pi^1(k, M) \simeq \ker \left( H^1(G, M) \to \prod_v H^1(D_v, M) \right).$$

In particular,

$$\Pi^1(k, M) \subseteq \bigcap_{\text{cyclic } H \leq G} \ker(H^1(G, M) \to H^1(H, M)).$$

Proof. For each nontrivial place $v$ of $k_s$, let $k_v$ and $K_v$ denote the corresponding completions of $k$ and $K$, and let $D_v$ be the corresponding decomposition group inside $G$. The products in the diagram below will be taken over all such $v$, instead of just the underlying places of $k$, but this does not affect the definitions of the Shafarevich–Tate groups, since in general, the kernel of a restriction map $H^1(G, M) \to H^1(H, M)$ is unchanged if $H \leq G$ is replaced by a conjugate subgroup. Inflation-restriction with respect to

$$1 \to G_K \to G_k \to G \to 1$$

and its local analogues yield the exactness of the last two rows in the commutative diagram

\[
\begin{array}{cccccc}
0 & \to & \Pi^1(G, M) & \to & \Pi^1(k, M) & \to & \Pi^1(K, M) \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & H^1(G, M) & \to & H^1(k, M) & \to & H^1(K, M) \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \prod_v H^1(D_v, M) & \to & \prod_v H^1(k_v, M) & \to & \prod_v H^1(K_v, M),
\end{array}
\]

and the groups in the top row are defined as the kernels of the vertical maps connecting the second and third rows. Lemma 8.1 yields $\Pi^1(K, M) = 0$, so $\Pi^1(k, M) \simeq \Pi^1(G, M)$, which is the first statement of the lemma. By the Chebotarev density theorem, every cyclic subgroup of $G$ occurs as a $D_v$; this implies the second statement. □
9. Definition of Selmer groups and sets

9.1. Selmer groups associated to isogenies.

**Definition 9.1.** Let $\phi: A \rightarrow J$ be an isogeny of abelian varieties over a global field $k$ such that $\text{char } k \nmid \deg \phi$. For each $v$, we obtain a connecting homomorphism $\gamma_v: J(k_v) \rightarrow H^1(k_v, A[\phi])$. Define

$$\text{Sel}^\phi(J) := \left\{ \delta \in H^1(k, A[\phi]) : \delta_v \in \text{im } \gamma_v \text{ for all } v \right\}.$$ 

**Proposition 9.2.** Let $S$ be a finite set of places of $k$ containing

- all archimedean places,
- all places where the residue characteristic divides $n$, and
- all places where the Tamagawa number of $J$ or $A$ is not coprime to $n$ (these form a subset of the places of bad reduction).

Then

(a) $\text{Sel}^\phi(J) = \{ \delta \in H^1(k, A[\phi])_S : \delta_v \in \text{im } \gamma_v \text{ for all } v \in S \}$.

(b) The group $H^1(k, A[\phi])_S$ is finite.

(c) The group $\text{Sel}^\phi(J)$ is finite.

**Proof.**

(a) Apply Lemma 7.1 to $k_v$ for each $v \notin S$.

(b) Finiteness of $H^1(k, A[\phi])_S$ is a special case of Proposition 7.5.

(c) This follows from (a) and (b). □

The image of $J(k)/\phi A(k) \hookrightarrow H^1(k, A[\phi])$ is contained in $\text{Sel}^\phi(J)$, by definition of the latter.

9.2. Selmer groups associated to descent setups. We define true and fake Selmer groups by replacing $H^1(k, A[\phi])$ by its explicit analogue $L^\times / L^\times n k^\times$, and by replacing $\gamma_v: J(k_v) \rightarrow H^1(k_v, A[\phi])$ by $C_v = \tilde{C}_v$, which is a homomorphism $J(k_v)^\circ \rightarrow L_v^\times / L_v^\times n k_v^\times$.

**Definition 9.3.** Given a true descent setup $(n, \Delta, \beta)$, define the true Selmer group

$$\text{Sel}_{\text{true}}^\alpha(J) := \left\{ \delta \in \frac{L^\times}{L^\times n k^\times} : \delta_v \in \text{im } (C_v) \text{ for all places } v \text{ of } k \right\}.$$ 

Given a fake descent setup $(n, \Delta, \beta)$, define the fake Selmer group

$$\text{Sel}_{\text{fake}}^\alpha(J) := \left\{ \delta \in \frac{L^\times}{L^\times n k^\times} : \delta_v \in \text{im } (C_v) \text{ for all places } v \text{ of } k \right\}.$$ 

To avoid having to state results twice, we use $\text{Sel}_{\text{true/fake}}^\alpha(J)$ to denote either $\text{Sel}_{\text{true}}^\alpha(J)$ or $\text{Sel}_{\text{fake}}^\alpha(J)$, depending on whether we are considering a true or a fake descent setup.
9.3. True and fake Selmer sets for $X$. Suppose that we have a true or fake descent setup for $X$, and that we fix $f \in k(X \times \Delta)^\times$ as in Definition 6.2 or 6.7, and define $X^{good}$ accordingly. Evaluation on closed points as in Section 6.2.2 or 6.3.2 defines a homomorphism $\tilde{C}_f : \mathcal{Z}(X^{good}) \to L^X/L^{xn}k^\times$. Since $\tilde{C}_f$ and $\tilde{C}$ agree on $\mathcal{Z}^0(X^{good})$, they have a common extension to the sum of their domains, $\mathcal{Z}(X^{good}) + \mathcal{Z}^0(X) = \mathcal{Z}(X)$. Then we may restrict to $X(k)$ to obtain a map of sets

$$C_f : X(k) \to L^X/L^{xn}k^\times.$$ 

Similarly, for each $v \in \Omega_k$, we obtain

$$C_{f,v} : X(k_v) \to L^\times_v/L^{xn}k_v^\times.$$ 

As the notation suggests, these maps depend on the choice of $f$.

**Definition 9.4.** Given a true or fake descent setup for $X$ and $f$, define

$$\mbox{Sel}^f_{\text{true/fake}}(X) := \left\{ \delta \in \frac{L^\times}{L^{xn}k^\times} : \delta_v \in \text{im}(C_{f,v}) \text{ for all places } v \text{ of } k \right\}.$$ 

**Lemma 9.5.** Suppose that the image of the diagonal $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\Delta$ is contained in $R$. Then there exists $c \in k^\times$ such that $\text{N}(\tilde{C}_f(z)) = c^{\deg z}$ in $k^\times/k^{xn}$ for all $z \in \mathcal{Z}(X)$. 

**Proof.** In the true case, the hypothesis on $R$ implies that $\sum_{P \in \Delta} \beta_P = \text{div}(r)$ for some $r \in k(X)^\times$. Then $\text{div}(\text{N}_{L/k}(f)) = n \sum_{P \in \Delta} \beta_P = \text{div}(r^n)$, so $\text{N}_{L/k}(f) = cr^n$ for some $c \in k^\times$. Evaluating on any $z \in \mathcal{Z}(X^{good})$ yields the result for such $z$. On the other hand, Lemma 6.16 yields the result for $z \in \mathcal{Z}^0(X)$. Together, these prove the result for any $z \in \mathcal{Z}(X^{good}) + \mathcal{Z}^0(X) = \mathcal{Z}(X)$.

In the fake case, the hypothesis on $R$ implies that $\#\Delta = nm$ for some $m \in \mathbb{Z}_{>0}$ and that $(\sum_{P \in \Delta} \beta_P) - mD = \text{div}(r)$ for some $r \in k(X)^\times$. Then $\text{div}(\text{N}_{L/k}(f)) = n (\sum_{P \in \Delta} \beta_P) - nmD = \text{div}(r^n)$, so $\text{N}_{L/k}(f) = cr^n$ for some $c \in k^\times$. The rest of the proof is as in the true case. 

10. Relations between various Selmer groups

In Sections 10.1–10.3, we will assume the following:

**Hypothesis 10.1.** The maps $J(k)_\circ \to J(k)/\phi A(k)$ and $J(k_v)_\circ \to J(k_v)/\phi A(k_v)$ are surjective for all places $v$ of $k$.

There are some common situations in which Hypothesis 10.1 is justified:

**Lemma 10.2.** Suppose that $X$ is a nice curve such that

(i) $X$ has a $k$-point (or more generally $H^0(k, \mbox{Pic } X_s) \rightarrow \mathbb{Z}$ is surjective), or

(ii) $k$ is a global field and $X$ has a $k_v$-point (or more generally $H^0(k_v, \mbox{Pic } X_{k_v,s}) \rightarrow \mathbb{Z}$ is surjective) for every $v \in \Omega_k$, or

(iii) $k$ is a global field of characteristic not 2 and $X$ is the smooth projective model of a hyperelliptic curve $y^2 = f(x)$ of even genus.

Then $J(k)_\circ = J(k)$. If moreover $k$ is a global field, then $J(k_v)_\circ = J(k_v)$ for every $v$, so Hypothesis 10.1 holds.
Proof. For (i) and (ii), see [PS97, Propositions 3.2 and 3.3]. For (iii) (generalized to superelliptic curves), see [PS97, end of §4]. □

Hypothesis 10.1 will let us define a map from the usual $\phi$-Selmer group into the Selmer group associated to our descent setup; without this map, not much could be said about how the groups relate. In Section 10.1 we study a local group $W_v$ that in a sense measures the difference between the local descent map $\gamma_v$ and our approximation $C_v$. In Section 10.3 we define a global group $K$ with a homomorphism $\kappa: K \to \prod_v W_v$ whose kernel and cokernel control the difference between the actual $\phi$-Selmer group and our explicit Selmer group $\text{Sel}^{\text{true/fake}}_\alpha(J)$.

10.1. **Local considerations.** We fix a place $v$ of $k$. Diagram (15) or (16) applied to $k_v$ yields

$$
\begin{align*}
\begin{aligned}
J(k_v) & \xrightarrow{\phi A(k_v)} J(k_v) \\
\gamma_v & \downarrow \\
E^v(k_v) & \xrightarrow{q} R^v(k_v) \to H^1(k_v, A[\phi]) \xrightarrow{\alpha_v} H^1(k_v, E^v) \to H^1(k_v, R^v)
\end{aligned}
\end{align*}
$$

in which the main row is exact. The group $\ker \alpha_v$ is hence isomorphic to $R^v(k_v)/qE^v(k_v)$, which is finite, and computable in terms of the actions of the decomposition group of $v$ on $E^v$ and $R^v$.

Since $C_v = \alpha_v \gamma_v$ in (19), we have an exact sequence

$$
\begin{align*}
\ker C_v & \to \ker \alpha_v \to \coker \gamma_v \to \coker C_v.
\end{align*}
$$

**Definition 10.3.** Let $W_v$ be either of the following naturally isomorphic groups obtained from (20):

(i) the cokernel of the first map $\ker C_v \to \ker \alpha_v$,

(ii) the image of the second map $\ker \alpha_v \to \coker \gamma_v$, or

(iii) the kernel of the third map $\coker \gamma_v \to \coker C_v$.

**Lemma 10.4.** For any $v \in \Omega_k$, the group $W_v$ is finite, and $\#W_v = \frac{\# \coker q \cdot \# \im C_v}{\# \im \gamma_v}$.

**Proof.** The group $\ker \alpha_v \simeq \coker q$ is finite. Separability of $\phi$ implies that $\phi A(k_v)$ is an open subgroup of the compact group $J(k_v)$, so the group $\im \gamma_v \simeq J(k_v)/\phi A(k_v)$ is finite too. By (19) and Definition 10.3(ii), we have exact sequences

$$
\begin{align*}
0 & \to \im \gamma_v \cap \ker \alpha_v \to \ker \alpha_v \to W_v \to 0 \\
0 & \to \im \gamma_v \cap \ker \alpha_v \to \im \gamma_v \to \im C_v \to 0,
\end{align*}
$$

which let us compute $\#W_v$. □

The following lemma will let us understand $W_v$ for most $v$.

**Lemma 10.5.** Let $v$ be a non-archimedean place of $k$ such that

(i) the residue characteristic of $v$ does not divide $n$, and

(ii) the Tamagawa numbers $c_v(J)$ and $c_v(A)$ are coprime to $n$.

Then

(a) $\im(C_v) \subseteq H^1(k_v, E^v)_{\text{unr}}$, and
(b) \( W_v = \text{im} \left( \frac{R^\vee(k_v)}{qE^\vee(k_v)} \to \frac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})} \right) \).

Proof. The commutative diagram

\[
\begin{array}{cccccc}
0 & \to & \frac{R^\vee(k_v)}{qE^\vee(k_v)} & \to & H^1(k_v, A[\phi]) & \to H^1(k_v, E^\vee) \\
\downarrow & & \downarrow \gamma_v & & \downarrow \alpha_v & \downarrow \\
0 & \to & \frac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})} & \to & H^1(k_{v,u}, A[\phi]) & \to H^1(k_{v,u}, E^\vee)
\end{array}
\]

has exact rows (cf. (19)). The central column is exact too, by (i), (ii), and Lemma 7.1.

(a) In (21), \( J(k_v)/\phi A(k_v) \) maps to 0 in \( H^1(k_{v,u}, E^\vee) \), so \( \text{im}(C_v) \subset H^1(k_v, E^\vee)_{\text{unr}} \).
(b) By Definition 10.3(ii),

\[
W_v = \text{im} (\ker \alpha_v \to \text{coker } \gamma_v)
= \text{im} \left( \frac{R^\vee(k_v)}{qE^\vee(k_v)} \to H^1(k_{v,u}, A[\phi]) \right)
= \text{im} \left( \frac{R^\vee(k_v)}{qE^\vee(k_v)} \to \frac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})} \right)
\]

Corollary 10.6. For all but finitely many \( v \), we have \( W_v = 0 \).

Proof. For all but finitely many \( v \), the residue characteristic of \( v \) does not divide \( n \), and \( J \) and \( A \) have good reduction at \( v \), so \( c_v(J) = c_v(A) = 1 \). If we also discard the finitely many \( v \) at which \( E^\vee \) is ramified, then for the remaining \( v \) the surjection \( E^\vee \to R^\vee \) of finite étale group schemes induces a surjection \( E^\vee(k_{v,u}) = E^\vee(k_{v,s}) \to R^\vee(k_{v,s}) = R^\vee(k_{v,u}) \), so Lemma 10.5(b) implies that \( W_v = 0 \).

Corollary 10.7. The product \( \prod_{v \in \Omega_k} W_v \) is a finite group.


Lemma 10.8. If \( v \) is complex, or if \( v \) is real and \( n \) is odd, then \( W_v = 0 \).

Proof. If \( v \) is complex, then \( \text{Gal}(k_{v,s}/k_v) = \text{Gal}(\mathbb{C}/\mathbb{C}) = \{1\} \). If \( v \) is real then \( \text{Gal}(k_{v,s}/k_v) = \text{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} \). Our assumptions assure that in either case, \( \text{Gal}(k_{v,s}/k_v) \) is annihilated by a unit modulo \( n \), so \( H^1(k_v, A[\phi]) = H^1(k_v, E^\vee) = 0 \). It follows that \( W_v = 0 \).
10.2. Finite description of true and fake Selmer groups. Let \( S \) be as in Proposition 9.2. Given another finite set of places \( T \), define

\[
S_T := \left\{ \delta \in \widehat{L(n, S)} : \delta \in \text{im}(C_v) \text{ for all } v \in T \right\}.
\]

**Theorem 10.9.** Let \( S \) and \( T \) be as above.

(a) We have \( \text{Sel}_{\text{true/fake}}^n(J) \subseteq S_T \).

(b) For each \( \delta \in \widehat{L(n, S)} \), fix a finite Galois extension \( k_\delta/k \) splitting \( R^\vee \) such that \( \delta \) maps to 0 in \( H^1(k_\delta, R^\vee) \). If \( T \) contains all places in \( S \), all places at which \( E^\vee \) ramifies, and enough places so that for each \( \delta \in \widehat{L(n, S)} \) the Frobenius elements \( \text{Frob}_v \) for \( v \in T \) unramified in \( k_\delta/k \) cover all conjugacy classes in \( \text{Gal}(k_\delta/k) \), then \( \text{Sel}_{\text{true/fake}}^n(J) = S_T \).

**Proof.**

(a) For \( v \notin S \), Lemma 10.5(a) proves that \( \text{Sel}_{\text{true/fake}}^n(J) \) consists of elements unramified at \( v \).

Proposition 7.2 now shows that \( \text{Sel}_{\text{true/fake}}^n(J) \subseteq \widehat{L(n, S)} \). The condition \( \delta \in \text{im}(C_v) \) in the definition of \( S_T \) is also in the definition of \( \text{Sel}_{\text{true/fake}}^n(J) \).

(b) Suppose that \( \delta \in S_T \). Given \( v \notin T \), we must show that \( \delta \in \text{im}(C_v) \). Choose \( w \in T \) unramified in \( k_\delta/k \) such that the conjugacy classes \( \text{Frob}_w \) and \( \text{Frob}_v \) in \( \text{Gal}(k_\delta/k) \) match. By definition of \( S_T \), we have \( \delta_w \in \text{im}(C_w) \). Then (19) for \( k_\delta \) shows that \( \delta \) maps to 0 in \( H^1(k_\delta, R^\vee) \). In other words, \( \delta \in H^1(\text{Gal}(k_\delta/k), R^\vee) \) restricts to 0 at \( w \). But the decomposition groups of \( v \) and \( w \) in \( \text{Gal}(k_\delta/k) \) are conjugate, so \( \delta \) maps to 0 in \( H^1(k_\delta, R^\vee) \) too. Thus the element \( \delta_v \in H^1(k_v, E^\vee) \) is the image of some \( \xi_v \in H^1(k_v, A[\phi]) \). Since \( v \notin S \), the element \( \delta_v \) is unramified; in particular, \( \xi_v \) maps to 0 in \( H^1(k_{v,u}, E^\vee) \). By hypothesis, \( E^\vee \) is unramified at \( v \), so \( E^\vee(k_{v,u}) \xrightarrow{\partial} R^\vee(k_{v,u}) \) is surjective, so the bottom row of (21) shows that \( H^1(k_{v,u}, A[\phi]) \rightarrow H^1(k_{v,u}, E^\vee) \) is injective. Thus \( \xi_v \) maps to 0 already in \( H^1(k_{v,u}, A[\phi]) \); i.e., \( \xi_v \in H^1(k_v, A[\phi])_{\text{unr}} \). By Lemma 7.1, \( \xi_v \) is in the image of \( J(k_v) \) under \( \gamma_v \). Thus \( \delta_v \) is in the image of \( J(k_v) \) under \( C_v \). \( \square \)

**Remark 10.10.** The idea to use an enlarged set \( T \) including places whose Frobenius elements cover the conjugacy classes was first used in [DSS00, Corollary 12].

**Remark 10.11.** Here we show how to compute a finite set \( T \) as in Theorem 10.9(b). A finite splitting field \( k_\Delta \) of \( \Delta \) will split \( R^\vee \). Given \( \delta \), represented by \( \ell = (\ell_i) \in L^x \), say, adjoining all \( n \)-th roots of the \( \ell_i \) to \( k_\Delta \) yields a candidate for \( k_\delta \). The Chebotarev density theorem guarantees that we can find enough \( v \) unramified in \( k_\delta/k \) to cover the conjugacy classes.

**Remark 10.12.** In practice, we may choose a smaller \( T \), one that does not satisfy the hypotheses in Theorem 10.9(b). Then we have only inclusions

\[
C(J(k)) \subseteq \text{Sel}_{\text{true/fake}}^n(J) \subseteq S_T.
\]

But if we find enough points in \( J(k) \) to show that \( C(J(k)) = S_T \), then we obtain \( \text{Sel}_{\text{true/fake}}^n(J) = S_T \) nevertheless. Often \( T = S \) suffices.
10.3. Comparison of the Selmer group associated to an isogeny with the Selmer group associated to a descent setup. In the following, we will study the relation between the Selmer group associated to a true or fake descent setup (which is an object we can hope to compute) and the Selmer group associated to the isogeny $\phi$ determined by the descent setup (which is the object we would like to compute). Theorem 10.14 will show that $\alpha$ induces a homomorphism from the latter to the former.

**Lemma 10.13.** We have an exact sequence

$$0 \rightarrow \text{Sel}^\alpha_{\text{true/fake}}(J) \rightarrow H^1(k, E^\vee) \rightarrow \prod_v \frac{H^1(k_v, E^\vee)}{\text{im } C_v}. $$

**Proof.** In the true case, $L^\times/L_n^\times k^\times = H^1(k, E^\vee)$, so this is just the definition of $\text{Sel}^\alpha_{\text{true}}(J)$. In the fake case, (8) for $k$ and its completions yields a commutative diagram

$$0 \rightarrow \Pi_v \frac{L^\times_{v}}{L_{v}^\times n_{v}^\times k_{v}^\times} \rightarrow \Pi_v H^1(k_v, E^\vee) \rightarrow \Pi_v \text{Br } k_v$$

with exact rows. An element $\delta \in H^1(k, E^\vee)$ mapping into $\text{im } C_v \subseteq L^\times_{v}/L_{v}^\times n_{v}^\times k_{v}^\times$ for all $v$ maps to 0 in $\text{Br } k_v$ for all $v$, so by the local-global property of the Brauer group, it also maps to 0 in $\text{Br } k$, so $\delta \in L^\times/L_n^\times k^\times$. Thus

$$\ker \left( H^1(k, E^\vee) \rightarrow \prod_v \frac{H^1(k_v, E^\vee)}{\text{im } C_v} \right) = \ker \left( \frac{L^\times_{v}}{L_{v}^\times n_{v}^\times k_{v}^\times} \rightarrow \prod_v \frac{H^1(k_v, E^\vee)}{\text{im } C_v} \right) = \text{Sel}^\alpha_{\text{fake}}(J).$$

Let $K$ be the kernel of the global map $\alpha: H^1(k, A[\phi]) \rightarrow H^1(k, E^\vee)$, which by (16) equals the (computable) cokernel of $q: E^\vee(k) \rightarrow R^\vee(k)$. Let $\kappa$ be the composition

$$K = \ker \alpha \rightarrow \prod_v \ker \alpha_v \rightarrow \prod_v \text{im}(\ker \alpha_v \rightarrow \text{coker } \gamma_v) = \prod_v W_v. $$

The following proposition gives a homomorphism $\text{Sel}^\phi(J) \rightarrow \text{Sel}^\alpha_{\text{true/fake}}(J)$ and provides information on its failure to be an isomorphism.

**Theorem 10.14.** We have an exact sequence

$$0 \rightarrow \ker \kappa \rightarrow \text{Sel}^\phi(J) \xrightarrow{\alpha \circ \gamma} \text{Sel}^\alpha_{\text{true/fake}}(J) \cap \alpha\left( H^1(k, A[\phi]) \right) \rightarrow \text{coker } \kappa.$$

**Proof.** By definition of $\kappa$, the diagram

$$0 \rightarrow K \rightarrow H^1(k, A[\phi]) \xrightarrow{\alpha \circ \gamma} \alpha\left( H^1(k, A[\phi]) \right) \rightarrow 0$$

$$0 \rightarrow \prod_v W_v \rightarrow \prod_v \frac{H^1(k_v, A[\phi])}{\text{im } \gamma_v} \rightarrow \prod_v \frac{H^1(k_v, E^\vee)}{\text{im } C_v}. $$

(23)
commutes. By definition of $K$ and Definition 10.3(iii) of $W_v$, the rows are exact. Apply the snake lemma and take the first four terms of the snake; Lemma 10.13 identifies the kernel of the third vertical map.

**Corollary 10.15.** We have $\# \ker (\text{Sel}^\alpha (J) \to \text{Sel}^\alpha_{\text{true/fake}} (J)) \leq R^\vee (k)/qE^\vee (k)$.

**Proof.** By Theorem 10.14, the kernel is isomorphic to $\ker \kappa \subseteq K \cong R^\vee (k)/qE^\vee (k)$. □

The following summarizes the best possible situation.

**Corollary 10.16.** Assume that $\text{Sel}^\alpha_{\text{true/fake}} (J) \subseteq \alpha (H^1 (k, A[\phi]))$ and that $W_v = 0$ for all places $v$ of $k$. Then we have an exact sequence

$$0 \to K \to \text{Sel}^\phi (J) \to \text{Sel}^\alpha_{\text{true/fake}} (J) \to 0.$$  

In particular, $\# \text{Sel}^\phi (J) = \# \alpha (H^1 (k, A[\phi]))$.

**Proof.** In Theorem 10.14, the homomorphism $\kappa : K \to \prod W_v$ is 0. □

We need a criterion that tells us when $\text{Sel}^\alpha_{\text{true/fake}} (J)$ is already contained in $\alpha (H^1 (k, A[\phi]))$.

Recall the discussion of $\text{III}^1$ in Section 8 and the exact sequence

$$0 \to A[\phi] \to E^\vee \xrightarrow{q} R^\vee \to 0.$$  

**Lemma 10.17.**

(a) There is an exact sequence

$$0 \to \text{Sel}^\alpha_{\text{true/fake}} (J) \cap \alpha (H^1 (k, A[\phi])) \to \text{Sel}^\alpha_{\text{true/fake}} (J) \xrightarrow{q} \text{III}^1 (k, R^\vee).$$

(b) In particular, if $\text{III}^1 (k, R^\vee) = 0$, then $\text{Sel}^\alpha_{\text{true/fake}} (J) \subseteq \alpha (H^1 (k, A[\phi]))$.

**Proof.** The last three terms in (15) or (16) for $k$ and the $k_v$ give rise to a commutative diagram with exact rows:

$$
\begin{array}{ccccccc}
0 & \to & \alpha (H^1 (k, A[\phi])) & \to & H^1 (k, E^\vee) & \xrightarrow{q} & H^1 (k, R^\vee) \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \prod \alpha_v (H^1 (k_v, A[\phi])) & \xrightarrow{\im C_v} & \prod \frac{H^1 (k_v, E^\vee)}{\im C_v} & \xrightarrow{\im C_v} & \prod \frac{H^1 (k, R^\vee)}{
\end{array}
$$

Take the kernels of the three vertical maps and apply Lemma 10.13. □

**Remark 10.18.** Results of Section 8 allow us to bound $\text{III}^1 (k, R^\vee)$ and to prove that it is 0 in many cases.

**Example 10.19.** We revisit the fake descent setup in Example 6.9(i) used for 2-descent on the Jacobian $J$ of a hyperelliptic curve $X$ with an even degree model $y^2 = f(x)$. Assume that $X$ has even genus or that $X(k_v) \neq \emptyset$ for all $v$; then Hypothesis 10.1 is satisfied, by Lemma 10.2. The $G_k$-set $\Delta$ is the set of Weierstrass points. The group $\mathbb{Z}/2\mathbb{Z}$ injects into $E = (\mathbb{Z}/2\mathbb{Z})^\Delta_{\text{deg}0}$, and $E^\vee = \mu_2^\Delta / \mu_2$. Since $\tilde{J} \simeq J$, exact sequence (13) is

$$0 \to \frac{\mathbb{Z}}{2\mathbb{Z}} \to E \to J[2] \to 0,$$
and its dual (14) is
\[ 0 \longrightarrow J[2] \xrightarrow{\alpha} E^\vee \xrightarrow{N} \mu_2 \longrightarrow 0 \]
where \( N \) is the norm. Cohomology (see (16)) gives
\[ 0 \longrightarrow \mathcal{K} \longrightarrow H^1(k, J[2]) \xrightarrow{\alpha} H^1(k, E^\vee), \]
where \( \mathcal{K} \simeq \mu_2(k)/N(E^\vee(k)) \). One can show (see [PS97, Theorem 11.3]) that the element of \( \mathcal{K} \) represented by \(-1 \in \mu_2(k)\) corresponds to the class \( \xi \) of the 2-covering \( \text{Pic}^1_{X/k} \to J \) in \( H^1(k, J[2]) \), where \( \text{Pic}^1_{X/k} \) is the Picard scheme component parametrizing line bundles of degree 1 on \( X \). For each \( v \), our assumption implies that \( \text{Pic}^1_{X/k} \) has a \( k_v \)-point, so \( \xi_v \) maps to 0 in \( H^1(k_v, J) \), so \( \xi_v \in \text{im} (C_v: J(k_v)/2J(k_v) \to H^1(k_v, J[2])) \). Since \( \xi_v \) generates \( \text{ker} \alpha_v \), we have \( W_v = 0 \) by Definition 10.3(ii). Also, \( \text{III}^1(k, \mu_2) = 0 \) by Lemma 8.1, so Lemma 10.17(b) applies, and Corollary 10.16 yields an exact sequence
\[ 0 \longrightarrow \mathcal{K} \longrightarrow \text{Sel}^2(J) \longrightarrow \text{Sel}^\alpha_{\text{true/fake}}(J) \longrightarrow 0. \]
Finally, since \( \mathcal{K} \simeq \mu_2(k)/N(E^\vee(k)) \), we have that \( \mathcal{K} = 0 \) if \( \Delta \) has a Galois-stable unordered partition into two sets of odd cardinality (a computable condition), and \( \mathcal{K} \simeq \mu_2(k) \) otherwise (cf. [PS97, Theorem 13.2]).

11. Computing true and fake Selmer groups

Choose \( S \) and \( T \) as in Section 10.2, and compute \( \hat{L}(n, S) \) as in Section 7.3. Because of Theorem 10.9, it remains to find an algorithm to test whether a given element of \( \hat{L}(n, S) \) is in the local image \( \text{im} C_v \) for a given \( v \). It is clear that this can be done in principle, but our goal here will be to describe a practical method, under an additional hypothesis:

**Hypothesis 11.1.** The variety \( X \) is a genus-\( g \) curve with a \( k_v \)-point \( x_0 \) (or more generally, a degree 1 divisor \( x_0 \) over \( k_v \)), and either \( \text{char } k_v = 0 \) or \( \text{char } k_v > g \).

We consider the non-archimedean and archimedean cases separately.

11.1. Computing the local image at a non-archimedean place. Fix a non-archimedean place \( v \) of \( k \). Let \( K \) be a finite extension of \( k_v \), say of degree \( d \), with valuation ring \( \mathcal{O} \), uniformizer \( \pi \), and maximal ideal \( m \). Let \( L_K := L \otimes_k K \). We have a map \( X(K) \to \mathbb{Z}^0(X_K) \) sending \( x \) to the class of the 0-cycle \( x - x_0 \), and following this with \( \bar{C}_K \) defines a continuous map
\[ \zeta_K: X(K) \to \frac{L_K^\times}{L_K^\times \mathbb{K}^\times}. \]
To define \( \zeta_K \) on all of \( X(K) \) requires using several functions \( f_1, \ldots, f_r \) with disjoint support, as in Remark 6.13. By perturbing \( x_0 \) in the smooth space \( X(k_v) \) (if \( x_0 \) is a point) or perturbing each component of \( x_0 \) in the space of points over its field of definition (if \( x_0 \) is a divisor), we may assume that the \( f_i \) can be evaluated at \( x_0 \).

We now explain how to compute a finite description of \( \zeta_K \). Choose a proper \( \mathcal{O} \)-scheme \( X \) with \( X_K \simeq X \). By the valuative criterion for properness, \( X(K) \simeq \mathcal{X}(\mathcal{O}) \simeq \lim \leftarrow_{m \geq 0} \mathcal{X}(\mathcal{O}/\pi^m) \).

By Hensel’s lemma, \( L_K^{\times n} \) has finite index in \( L_K^\times \), so \( L_K^{\times n}/L_K^{\times n} \mathbb{K}^\times \) is a finite discrete set, so \( \zeta_K \) is locally constant. Proceed as follows:
Start with \( m = 1 \).

On each remaining residue disk modulo \( \pi^m \) in \( X(K) \), check whether any \( f_i \) is such that \( f_i(x)/f_i(x_0) \) is constant in \( \frac{L_K^\times}{L_K^\times K^\times} \); if not, break the residue disk into residue disks modulo \( \pi^{m+1} \), and apply recursion.

Because the divisors of the \( f_i \) are disjoint, eventually this algorithm will terminate, with a partition of \( X(K) \) into residue disks on which \( c_K \) takes a known constant value.

Next, the diagram

\[
\begin{array}{ccc}
X(K) & \overset{x \to x - x_0}{\longrightarrow} & Z^0(X_K) \\
\downarrow \text{tr}_{K/k_v} & & \downarrow \text{tr}_{K/k_v} \\
Z^0(X_{k_v}) & \overset{\text{tr}_{K/k_v}}{\longrightarrow} & \frac{L_K^\times}{L_{K/v}^\times K_{k_v}^\times}
\end{array}
\]

commutes, so we can compute \( \widetilde{C} \) on elements of \( Z^0(k_v) \) of the form \( \text{tr}_{K/k_v} x - dx_0 \).

Lemma 11.2.

(a) There are only finitely many extensions \( K/k_v \) with \( [K : k_v] \leq g \) up to isomorphism, and we can list them all.

(b) As \( K \) ranges through these field extensions, and \( x \) ranges over \( X(K) \), the images of \( \text{tr}_{K/k_v} x - dx_0 \) generate \( J(k_v) \).

Proof.

(a) If \( \text{char} \ k_v = 0 \), see [PR01]. If \( \text{char} \ k_v > 0 \), the characteristic assumption in Hypothesis 11.1 guarantees that each \( K \) is tamely ramified over \( k_v \), so \( K \) is obtained by adjoining a single \( m \)th root of a uniformizer to a finite unramified extension of \( k_v \). We can compute representatives for the set of possible uniformizers up to \( m \)th powers.

(b) The Riemann-Roch theorem shows that every degree-0 divisor on \( X \) is linearly equivalent to \( E - gx_0 \) for some effective \( E \in \text{Div}^g X \). Writing \( E \) as a sum of closed points lets one express \( E - gx_0 \) as a sum of 0-cycles of the form \( \text{tr}_{K/k_v} x - dx_0 \) for various \( K \) of degree at most \( g \).

We can now compute \( \text{im} C_v \) as follows:

(i) Compute all extensions \( K \) as in Lemma 11.2(a).

(ii) For each, compute the image of \( c_K \), and apply \( N_{K/k_v} \) to find the image of \( C_v \) on 0-cycles of the form \( \text{tr}_{K/k_v} x - dx_0 \).

(iii) Compute the subgroup generated by all such images.

By Lemma 11.2, the result equals \( \text{im} C_v \).
11.2. Computing the local image at an archimedean place. For archimedean $v$ a similar method works, but instead of partitioning $X(K)$ into residue classes, we partition it into connected components, because a continuous map to the discrete set $L_K^*/L_v^*k_v^*$ is constant on connected components. If $K = \mathbb{C}$, then every point in $X(K)$ has the same image under $x \mapsto \text{tr}_{K/k_v} x - dx_0$ as $x_0$, which is 0. If $K = \mathbb{R}$, then we compute $f(x)/f(x_0)$ for one point $x$ in each connected component of $X(K)$, perturbing $x$ as necessary to ensure that $f$ is regular and nonvanishing at $x$.

11.3. Further comments on the computation of local images.

Remark 11.3. To find different $f$’s that can be used to compute $c_K$, we need to move $\beta$ (and/or $D$ in the fake case) within their linear equivalence classes. In the fake case, it is often more convenient to move $D$ in practice, since in many applications $\beta$ is the only effective divisor in its class.

Remark 11.4. Sometimes we can compute $c_K$ without moving $\beta$, as we now explain. Suppose that

- we have a true or fake descent setup, with a choice of $\beta$, $D$, and $f$;
- $f$ can be evaluated at $x_0$; where $x_0 \in X(K)$ or $x_0$ is a degree 1 divisor on $X$ over $K$,
  for some local field $K$;
- the supports of $\beta_P$ for $P \in \Delta$ are pairwise disjoint; and
- the image of the diagonal $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\Delta$ is contained in $R$.

Given $x \in X(K)$, the hypothesis on the $\beta_P$ implies that there is at most one $P$ such that $f_P$ has a zero or pole at $x$. We can evaluate $f_Q(x - x_0)$ for all $Q \neq P$, and the missing component of $c_K(x)$ can be recovered from the fact (Lemma 6.16) that $c_K(x)$ lies in the kernel of $N$.

Remark 11.5. Under the same hypotheses on $\beta$, $D$, $f$, $R$ as in Remark 11.4, we can evaluate $C_f$ at arbitrary $x \in X(k)$, using Lemma 9.5 instead of Lemma 6.16. Similarly, we can evaluate $C_{f,v}$.

Remark 11.6. Here we describe an alternative method that, when it succeeds, computes $\# \text{im } C_v$ much more quickly in practice. The method consists of two parts: computing an upper bound on $\# \text{im } C_v$ (or its exact value), and computing lower bounds on the group $\text{im } C_v$, and hoping that the sizes match. Suppose that $A = J$ and $\phi$ is multiplication-by-$n$ on $J$. To compute an upper bound on $\# \text{im } C_v$:

- First calculate the action of the decomposition group $\text{Gal}(k_{v,s}/k_v)$ on $\Delta$.
- Using this, compute the exact sequence
  \[ 0 \to J[n](k_v) \to E^\vee(k_v) \xrightarrow{q} R^\vee(k_v) \]
  of finite groups.
- From this, compute $\# J[n](k_v)$.
- Substitute this into the formula
  \[ \# \frac{J(k_v)}{nJ(k_v)} = \|n\|^{-\dim J} \# J[n](k_v), \]

where $\|n\|$ is the $v$-adic absolute value normalized so that $\|a\|_v = (\mathcal{O}_v : a\mathcal{O}_v)^{-1}$ for $a \in \mathcal{O}_v$ (this is a variant of [PS97, Proposition 12.10]).
- We obtain the bound $\# \text{im } C_v \leq \# J(k_v)/nJ(k_v)$, since $C_v$ factors through $J(k_v)/nJ(k_v)$.
• If \( q: E'(k_v) \to R'(k_v) \) is surjective, a condition that can be checked using (24), then (19) shows that \( \alpha_v \) is injective and \( \# \text{im} \ C_v = \# J(k_v)/nJ(k_v) \).

To compute lower bounds on \( \text{im} \ C_v \):

• Randomly select \( x \in X(k_v) \hookrightarrow J(k_v) \) and compute their images under \( C_v \) hoping that they generate a group of the right size. (Calculate \( N_{K/k_v}(\xi_K(x)) \) for \( x \in X(K) \) also for finite extensions \( K \) of \( k_v \) if it seems that the \( k_v \)-points are insufficient.)

12. Genus-3 curves

In this section we specialize to the case of a fake descent setup given by the bitangents of a smooth plane quartic. This is the non-hyperelliptic \( g = 3 \) case of Example 6.9(iv). Many of the results about smooth plane quartics we require were established already before 1900. See [Sal1879, p. 223 onwards] for a survey.

12.1. Bitangents of smooth plane quartics. Let \( k \) be a field of characteristic not 2. Let \( X \) be a non-hyperelliptic genus-3 curve over \( k \). The canonical map embeds \( X \) as a smooth quartic curve \( g(x, y, z) = 0 \) in \( \mathbb{P}^2 \). Conversely, every smooth quartic curve in \( \mathbb{P}^2 \) arises in this way. Let \( \hat{\mathbb{P}}^2 \) be the dual projective space, with homogeneous coordinates \( u, v, w \); its points correspond to lines in \( \mathbb{P}^2 \).

Definition 12.1. A bitangent to \( X \) is a line \( l \subset \mathbb{P}^2 \) such that the intersection \( l.X \) is \( 2\beta_l \) for some \( \beta_l \in \text{Div} X(k_v) \).

Given a bitangent \( l \), the line bundle \( \mathcal{L}_l \) associated to \( \beta_l \) is an odd theta characteristic on \( X \). The bitangents to \( X \) form a 28-element \( \mathcal{G} \)-set \( \Delta \) in bijection with the \( \mathcal{G} \)-set \( \mathcal{T}_{\text{odd}} \) of Section 5.1 [GH04, p. 289]. Alternatively, we may view \( \Delta \) as a finite étale subscheme of \( \hat{\mathbb{P}}^2 \), and the collection \( (\mathcal{L}_l) \) as a line bundle \( \mathcal{L} \) on \( X \times \Delta \). Then \( (2, \Delta, \mathcal{L}) \) is isomorphic to the fake descent setup in Example 6.9(iv) with \( g = 3 \). The isogeny \( \phi: A \to J \) of Section 6.4 is \( [2]: J \to J \).

12.2. Syzygetic quadruples.

Lemma 12.2. Let \( l_1, \ldots, l_4 \) be bitangents. Then the following are equivalent:

(i) The corresponding four odd theta characteristics sum to 0 in \( \text{Pic} X(k_v)/\langle \omega \rangle \) [2].

(ii) The divisor \( \beta_{l_1} + \cdots + \beta_{l_4} \) is linearly equivalent to 2 times a canonical divisor.

(iii) The divisor \( \beta_{l_1} + \cdots + \beta_{l_4} \) is an intersection \( Q.X \) for some (not necessarily irreducible) conic \( Q \subset \mathbb{P}^2 \).

Proof.

(i) \( \iff \) (ii): Considering degrees shows that the odd theta characteristics sum to 0 in \( \text{Pic} X(k_v)/\langle \omega \rangle \) [2] if and only if they sum to \( \omega \otimes 2 \) in \( \text{Pic} X \).

(iii) \( \implies \) (ii): Let \( l \) be any line in \( \mathbb{P}^2 \). Then \( Q \sim 2l \) on \( \mathbb{P}^2 \), so \( Q.X \sim 2l.X \) on \( X \), and \( l.X \) is a canonical divisor.

(ii) \( \implies \) (iii): Equivalently, we must show that \( \Gamma(\mathbb{P}^2, \mathcal{O}(2)) \to \Gamma(X, \mathcal{O}_X(2)) \) is surjective. This is true, since the cokernel is contained in \( H^1(\mathbb{P}^2, \mathcal{O}(-4 + 2)) = 0 \). \( \square \)
A 4-element set \( \{ l_1, \ldots, l_4 \} \) satisfying the conditions of Lemma 12.2 is called a **syzygetic quadruple**. Let \( \Sigma \subset \binom{\Delta}{4} \) be the set of syzygetic quadruples. This incidence structure \((\Delta, \Sigma)\) constructed above from bitangents is the same as that in Section 5.2 for \( g = 3 \). In particular, its isomorphism type is independent of \( X \) (see Remark 5.6). By Proposition 5.7, \#\( \Sigma \) = 315.

12.3. **Sp\(_6(\mathbb{F}_2)\)**-modules. If we chose a bijection between \( \Delta \) and \( \{1, \ldots, 28\} \), then the image \( G \), of \( G \to \text{Aut} \Delta \) would be identified with a subgroup of the symmetric group \( S_{28} \), and changing the bijection would change the subgroup up to \( S_{28} \)-conjugacy.

Instead we will choose an isomorphism between \((\Delta, \Sigma)\) and a fixed incidence structure \((\Delta, \Sigma)\), so that \( G \) is identified with a subgroup of \( \text{Aut}(\Delta, \Sigma) \), which by Proposition 5.4 is a specific copy of \( \text{Sp}_6(\mathbb{F}_2) \) in \( S_{28} \). Changing this isomorphism changes \( G \) only up to \( \text{Sp}_6(\mathbb{F}_2) \)-conjugacy. This more refined information will be needed to deduce the action of \( G \) on \( J[2], E^\vee, \) and \( R^\vee \).

The following lemma constructs our fixed \((\Delta, \Sigma)\) directly from the group \( \text{Sp}_6(\mathbb{F}_2)\):

**Lemma 12.3.**

(a) The group \( \text{Sp}_6(\mathbb{F}_2) \) has a unique index-28 subgroup \( H \), up to conjugacy. Let \( \Delta \) be the \( G \)-set \( G/H \). Identify \( \Delta \) with \( \{1, \ldots, 28\} \).

(b) There is a unique \( \text{Sp}_6(\mathbb{F}_2) \)-invariant subset of \( \binom{\Delta}{4} \) of size 315; call it \( \Sigma \).

**Proof.** Direct computation using Magma [Magma].

Let \( \Gamma \) be the image of the map

\[
\binom{\Delta}{2} \to \binom{\Delta}{12} \quad \pi \mapsto \bigcup \{ \sigma \in \Sigma : \pi \subset \sigma \}.
\]

In \( \mathbb{F}_2^\Delta \), let \( 1, \bar{J}, R, E \) be the \( \mathbb{F}_2 \)-spans of \( \{ \sum_{l \in \Delta} l \} \), \( \Gamma, \Sigma, \binom{\Delta}{2} \), respectively, where we identify subsets of \( \Delta \) with the sums of their elements in \( \mathbb{F}_2^\Delta \).

**Lemma 12.4.** The \( \text{Sp}_6(\mathbb{F}_2) \)-submodules of \( \mathbb{F}_2^\Delta \) are

\[
0 \subset 1 \subset \bar{J} \subset R \subset E \subset \mathbb{F}_2^\Delta,
\]

which have dimensions 0, 1, 7, 21, 27, 28, respectively.

**Proof.** The given modules obviously are submodules. Direct computation using Magma establishes that there are no others and that the dimensions are as stated.

**Corollary 12.5.** Let \( X \) be a smooth plane quartic. Let \( \Delta \) be its set of bitangents. Let \( \Sigma \) be its set of syzygetic quadruples. Construct \( E \) and \( R \) from the fake descent setup as in Section 6.3. Then there is an isomorphism \((\Delta, \Sigma) \cong (\Delta, \Sigma)\) of incidence structures, and any such isomorphism induces a homomorphism \( \rho: \bar{G} \to \text{Sp}_6(\mathbb{F}_2) \) and \( \bar{G} \)-equivariant isomorphisms \( E \cong E, R \cong R, \) and \( J[2] \cong \ker(E^\vee \to R^\vee) \), where \( \bar{G} \) acts on the \( \text{Sp}_6(\mathbb{F}_2) \)-modules via \( \rho \).
Proof. The isomorphism \((\Delta, \Sigma) \simeq (\Delta, \Sigma)\) exists because of the uniqueness in Lemma 12.3. The \(G\)-action on \(\Delta\) must respect \(\Sigma\), so we get
\[ \mathcal{G} \to \text{Aut}(\Delta, \Sigma) \simeq \text{Aut}(\Delta, \Sigma) = \text{Sp}_6(\mathbb{F}_2). \]
The induced isomorphism \(\mathbb{P}_2^\Delta \to \mathbb{P}_2^\Sigma\) sends \(E\) to \(E\) and \(R\) to \(R\) because by Lemma 12.4 there is at most one submodule of each dimension. By (14), we have
\[ J[2] \simeq \ker (E^\vee \to R^\vee) \simeq \ker (E^\vee \to R^\vee). \]

12.4. Computing bitangents and syzygetic quadruples.

Lemma 12.6. Let \(k\) be a field for which arithmetic operations can be computed. Suppose that \(g(x, y, z) \in k[x, y, z]\) is a degree-4 homogeneous polynomial defining a smooth curve \(X\) in \(\mathbb{P}^2\).

(a) We can compute \(\Delta\) as a subscheme in \(\mathbb{P}_k^2\).

(b) In the remaining parts, suppose that \(F\) is an explicit finite Galois extension of \(k\) over which \(\Delta\) splits completely, and write \(\Delta\) for \(\Delta(F)\). If we choose a bijection \(\Delta \to \{1, \ldots, 28\}\), then \(\Sigma\) can be determined as an explicit subset of \(\binom{\{1, \ldots, 28\}}{4}\).

(c) With notation as in (b), we can compute an isomorphism \((\Delta, \Sigma) \to (\Delta, \Sigma)\).

(d) If we have an explicit description of \(\text{Gal}(F/k)\) acting on \(F\), then the image of the homomorphism \(\rho: \mathcal{G}_k \to \text{Sp}_6(\mathbb{F}_2)\) of Corollary 12.5 can be computed.

Proof.

(a) We describe \(\Delta\) as a subscheme of \(\mathbb{P}_k^2\) by describing its intersection with each standard affine patch of \(\mathbb{P}_k^2\). For example, to compute the part of \(\Delta\) in the patch whose points correspond to lines \(l: ux + vy + wz = 0\) with \(w = 1\), substitute the parametrization \((s : t) \mapsto (s : t : -us - vt)\) of the line into \(g(x, y, z)\), set the result equal to \((a_0s^2 + a_1st + a_2t^2)^2\) for indeterminate \(a_0, a_1, a_2\), and eliminate \(a_0, a_1, a_2\) to find the conditions on \(u, v, w\) for \(l\) to be a bitangent.

(b) We use criterion (iii) in Lemma 12.2. Enumerate the 3-element subsets \(\{l_1, l_2, l_3\}\) of \(\Delta\). For each, use linear algebra over \(F\) to determine if there is a conic \(Q\) in \(\mathbb{P}^2\) such that \(Q.X \geq \beta_{l_1} + \beta_{l_2} + \beta_{l_3}\); if so, compute \(Q.X\) to check whether it equals \(\beta_{l_1} + \beta_{l_2} + \beta_{l_3} + \beta_{l_4}\) for some \(l_4 \in \Delta\). Record all such \(\{l_1, l_2, l_3\}\).

(c) Given (b), this is a matter of matching combinatorial data. A bijection \(\Delta \to \Delta'\) can be built one value at a time; we try all possibilities, checking as we go along that the distinguished 4-element subsets match so far.

(d) We compute equations for the bitangents, and hence compute the action of \(\text{Gal}(F/k)\) on \(\Delta\). Using (c), we translate this into an action of \(\text{Gal}(F/k)\) on \(\Delta\). The image of \(\text{Gal}(F/k) \to \text{Aut} \Delta\) is \(\text{im} \rho\). \(\square\)

12.5. Computing the discriminant of a ternary quartic form. The following is well-known.

Lemma 12.7. Fix positive integers \(n\) and \(d\). Let \(g(x_0, \ldots, x_n) \in \mathbb{Z}[x_0, \ldots, x_n]\) be a degree-\(d\) homogeneous polynomial with indeterminate coefficients \(c_1, \ldots, c_N\), so \(N = \binom{n + d}{d}\). Then there is a polynomial \(D(c_1, \ldots, c_N) \in \mathbb{Z}[c_1, \ldots, c_N]\), called the discriminant, such that whenever \(c_1, \ldots, c_N\) are specialized to elements of a field \(k\), the polynomial \(D\) vanishes if and only if the hypersurface \(g = 0\) in \(\mathbb{P}_k^n\) fails to be smooth of dimension \(n - 1\). Moreover, \(D\) is unique up to a sign.
Sketch of proof. Let $B = \mathbb{A}^N_\mathbb{Z}$, and let $X \subset \mathbb{P}^n \times B$ be the closed subscheme defined by $g = 0$, so $X \to B$ is the universal family of degree-$d$ hypersurfaces in $\mathbb{P}^n$. Let $S$ be the locus where $X \to B$ fails to be smooth of dimension $n - 1$. Then $S \to B$ is proper, so its image is a closed subscheme $V \subseteq \mathbb{A}^N_\mathbb{Z}$. On the other hand, analyzing the fibers of the other projection $S \to \mathbb{P}^n$ lets us show that $S$ and $V$ are integral (or empty) and lets us compute their dimensions. This eventually shows that $V$ is a hypersurface (possibly empty), so $V$ is cut out by a single equation, defined up to a unit of $\mathbb{Z}$.

We now restrict to the case $n = 2$ and $d = 4$, in which case $D$ is a polynomial of degree 27, denoted $I_{27}(g)$ in the notation of [Dix87]. We fix the sign by decreeing that $I_{27}(x^4 + y^4 + z^4) > 0$.

Over a ring in which $g$ is invertible, the discriminant of $g$ agrees, up to a unit, with the resultant $R(g)$ of $\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y}, \frac{\partial g}{\partial z}$ (cf. [GKZ08, Chapter 13, §1]), for which an algorithm is given in [Sal1876, §91]. Thus $I_{27}(g) = cR(g)$ for some $c \in \mathbb{Z}[1/2]^\times$ independent of $g$.

To determine the power of 2 in $c$, we compute $R(g)$ for a single $g \in \mathbb{Z}_2[x, y, z]$ for which $g = 0$ is smooth over $\mathbb{Z}_2$ (e.g., take $g = x^4 + y^z + z^2y$); for this $g$ we must have $cR(g) \in \mathbb{Z}_2^\times$. The sign of $c$ can be determined as the sign of $R(x^4 + y^4 + z^4)$. It turns out that $c = 2^{-14}$ (cf. [GKZ08, Chapter 13, Proposition 1.7] and [Dem12, §5, Definition 4 and Exemple 3]).

This algorithm was implemented by Christophe Ritzenthaler, and included by David Kohel in his Magma package Echidna [Koh]. We used this implementation (but negated the output to make the sign agree with our convention).

Remark 12.8. Given a smooth plane quartic curve $X$ over $\mathbb{Q}$ defined by $g = 0$, we can choose $g \in \mathbb{Z}[x, y, z]$ to minimize $|I_{27}(g)|$. But $I_{27}(-g) = -I_{27}(g)$, so the sign of $I_{27}(g)$ for such a minimizer $g$ is not uniquely determined by the curve $X$ in $\mathbb{P}^2_\mathbb{Q}$.

12.6. Computing fake Selmer groups of smooth plane quartics. We apply the procedure outlined in Section 11 to compute Sel$_{\text{fake}}^g(J)$ for the fake descent setup given in Section 12.1, under the assumption that $X_{k_v}$ has a divisor of degree 1 for all $v \in \Omega_k$. For simplicity and practicality, we assume that $k = \mathbb{Q}$. By multiplying the polynomial $g(x, y, z)$ defining $X$ in $\mathbb{P}^2$ by a positive integer, we may assume that $g$ has coefficients in $\mathbb{Z}$. We proceed with the following steps:

1. Determine $L$.
2. Determine the ring of integers $\mathcal{O}_L$ of $L$.
3. Determine a finite set $\mathcal{S} \subseteq \Omega_k$ containing the archimedean places, the places of residue characteristic 2, and the places $v$ where the Tamagawa number $c_v(J)$ is even.
4. Determine $L(2, \mathcal{S})$.
5. Determine the image $G$ of $\mathcal{G} \to \text{Aut } \Delta$ as a subgroup of $\text{Sp}_6(\mathbb{F}_2)$ up to $\text{Sp}_6(\mathbb{F}_2)$-conjugacy.
6. Choose a finite set $\mathcal{T} \subseteq \Omega_k$. For each $v \in \mathcal{T}$,
   a. Determine the decomposition group $D_v$ as a subgroup of $G$ up to $G$-conjugacy.
   b. Determine $\text{im } C_v$.
7. Compute $S'_\mathcal{T} = \{ \delta \in L(2, \mathcal{S}) : N_{L/k}(\delta) = 1 \in \kappa^*_{\kappa^*} \text{ and } \text{Res}_v \delta \in \text{im } C_v \text{ for all } v \in \mathcal{T} \}$.

Sections 12.6.1–12.6.7 elaborate on the implementation of the corresponding steps.

Lemma 6.16 and Theorem 10.9(a) imply Sel$_{\text{fake}}^g(J) \subseteq S'_\mathcal{T}$. So the result of the calculation is an upper bound $S'_\mathcal{T}$ for Sel$_{\text{fake}}^g(J)$, which by Theorem 10.9(b) can be guaranteed to
equal \text{Sel}_{\text{fake}}(J)$ by choosing $T$ appropriately large. (But as explained in Remark 10.12, in practice we will often not choose $T$ so large.)

12.6.1. **Determine $L$.** Our goal is to find a squarefree $h(t) \in k[t]$ of degree 28 such that $\Delta \simeq \text{Spec} L$ with $L := k[t]/h(t)$. First compute $\Delta$ as a subscheme of $\hat{\mathbb{P}}^2$ as in Lemma 12.6(a). Next, repeatedly choose a projection $\hat{\mathbb{P}}^2 \to \mathbb{P}^1$ (i.e., perform a change of variables, and then eliminate a variable) until one is found that maps $\Delta$ to an étale scheme $\Delta'$ of degree 28 with $\infty \notin \Delta'$. Then $\Delta'$ is the zero locus in $\mathbb{A}^1$ of the desired $h(t) \in k[t]$.

Let $\theta$ be the image of $t$ in $L$.

12.6.2. **Determine the ring of integers of $L$.** Here our task is to find a $\mathbb{Z}$-basis of $\mathcal{O}_L$, with each basis element expressed as a polynomial in $\theta$ of degree less than 28. This is a standard operation in algebraic number theory packages if $L$ is a field. If $L$ splits nontrivially as a product of fields, we just compute the integer rings of each constituent separately and piece the results together using the Chinese remainder theorem.

From the denominators of the coefficients of $h(x)$ we find $m \in \mathbb{Z}$ such that $m\theta$ is an algebraic integer. The standard approach for determining $\mathcal{O}_L$ would then be to compute the integral closure of $\mathcal{O} := \mathbb{Z}[m\theta]$ in $L$. But since $\theta$ was obtained by projecting a degree 28 subscheme of $\mathbb{P}^2$ onto $\mathbb{P}^1$, there are probably primes introduced into $\text{Disc} \mathcal{O}$ that do not divide $\text{Disc} \mathcal{O}_L$. In practice these primes can easily be of size $10^{100}$, so even finding them in $\text{Disc} \mathcal{O}$ may involve a challenging factorization.

Here are two ways to circumvent this problem:

1. Compute the discriminant $I_{27}(g)$ of the quartic form as in Section 12.5, and factor it. If $p$ is a prime not dividing the integer $I_{27}(g)$, then the 28 bitangents of $X$ reduce to the 28 distinct bitangents of the smooth plane quartic curve defined by $g(x, y, z) \mod p$, so $p \nmid \text{Disc} \mathcal{O}_L$. In other words, the set of prime factors of $I_{27}(g)$ is an upper bound for the set of primes dividing $\text{Disc} \mathcal{O}_L$. \textit{Magma}’s routine \texttt{MaximalOrder} accepts this upper bound as part of the input to help it remove extraneous factors via a lazy factorization.

2. Use a different projection to find a second order $\mathcal{O}'$. Then the order generated by $\mathcal{O}$ and $\mathcal{O}'$ is likely of small index in $\mathcal{O}_L$, in which case computing its integral closure in $L$ is much easier.

**Remark 12.9.** It is advisable to compute an LLL-reduced basis for $\mathcal{O}_L$ and use that to represent elements of $\mathcal{O}_L$ and $L$.

12.6.3. **Determine the set $\mathcal{S} \subset \Omega_k$.** Compute the integer $I_{27}(g)$ and factor it. If $p$ is a prime such that $p \nmid I_{27}(g)$, then $X$ has good reduction at $p$, from which it follows that $J$ has good reduction at $p$ and $c_p(J) = 1$. Therefore we may take the set $\mathcal{S}$ of Proposition 9.2 to be the set of prime divisors of $I_{27}(g)$, together with 2 and $\infty$.

**Remark 12.10.** Often we can use a smaller $\mathcal{S}$ by computing a proper regular model of $X$ over $\mathbb{Z}_p$ and using [BLR90, §9.6, Theorem 1] to compute $c_p(J)$. \textit{Magma} has an implementation by Steve Donnelly that can compute regular models of plane curves in many cases; there is also a function that extracts the component group $\Phi$; then $c_p(J) = \#\Phi(\mathbb{F}_p)$ is a divisor of $\#\Phi$, so this may let us prove that $c_p(J)$ is odd, in which case $p$ can be excluded from $\mathcal{S}$.

Here is a common special case in which no extra computation is required to exclude a prime:
Remark 12.11. Suppose that an odd prime $p$ appears with exponent 1 in the factorization of $J_2^2(g)$. Then $\text{Proj} \mathbb{Z}_p[x, y, z]/(g)$ is regular and its special fiber is an irreducible curve with multiplicity 1, with a single node. We deduce $c_p(J) = 1$, so we may exclude $p$ from $S$.

12.6.4. **Determine $\widetilde{L(2, S)}$.** Our goal here is to compute elements of $L^\times$ whose images in $L^\times/L^{x_2}k^\times$ form a basis for $\widetilde{L(2, S)}$.

We first compute $L(2, S)$. If we compute $L(2, S')$ for some $S' \supset S$, we can recover its subgroup $L(2, S)$ by performing linear algebra with the valuations in $S' - S$; thus we are free to enlarge $S$. If $S$ is enlarged enough that we can verify that $\text{Cl}(O_{L, S})[2] = 0$, then (17) implies that $L(2, S) = O_{L, S}^\times/O_{L, S}^{x_2}$.

Next, since $k = \mathbb{Q}$, we have $\text{Cl}(O_S) = 0$, so (18) implies $\widetilde{L(2, S)} = \text{coker}(O_S^\times/O_S^{x_2} \to O_{L, S}^\times/O_{L, S}^{x_2})$.

Thus we need only solve the following standard problems of algebraic number theory:

(A) find $S$ such that $\text{Cl}(O_{L, S})[2] = 0$, and

(B) compute bases for $O_S^\times/O_S^{x_2}$ and $O_{L, S}^\times/O_{L, S}^{x_2}$.

Current methods for solving problem (A) involve computing the whole class group $\text{Cl}(O_{L, S})$. Doing this unconditionally requires computation up to the Minkowski constants of the fields $L_i$ with product $L$, which requires running time polynomial in Disc $O_L$; in the case where $L$ is a degree 28 field, it is rare that Disc $O_L$ is small enough to make this practical. On the other hand, if we are willing to assume the Generalized Riemann Hypothesis for the $L_i$ of large degree, we can handle many more instances.

Problem (B) is less serious, once problem (A) has been solved. One can check whether an element of $O_{L, S}^\times$ is a square, by constructing the square root numerically to prove a positive answer and by reducing modulo primes to prove a negative answer. The Dirichlet $S$-unit theorem yields $\dim_{\mathbb{F}_2} O_{L, S}^\times/O_{L, S}^{\times_2} = \#S$ in advance, so if generators are constructed conditionally, they can be verified without difficulty.

**Remark 12.12.** **Magma** has a command to compute $L(2, S)$ when $k = \mathbb{Q}$.

12.6.5. **Choice of $T$.** Choose a finite set of places $T$, while keeping Remark 10.12 in mind. If it is necessary to get a better upper bound $S'_T$ on $\text{Sel}^\alpha_{\text{true/fake}}(J)$, we can enlarge $T$ later.

12.6.6. **Determine the global and local Galois actions on $\Delta$.** We have two goals:

(A) Describe the image $G$ of the homomorphism $\rho: G \to \text{Sp}_6(\mathbb{F}_2)$ in Corollary 12.5 as a subgroup of $\text{Sp}_6(\mathbb{F}_2)$ up to $\text{Sp}_6(\mathbb{F}_2)$-conjugacy. Since in Lemma 12.3(a) we fixed an embedding $\text{Sp}_6(\mathbb{F}_2) \hookrightarrow S_{28}$, the answer can be specified by giving explicit elements of $S_{28}$ that generate one such representative $G$ of its conjugacy class.

(B) For each $v \in T$, describe the decomposition group $D_v$ as a subgroup of the $G$ in (A) up to $G$-conjugacy. Each $D_v$ is to be specified by a list of elements of $G \subseteq S_{28}$ that generate $D_v$.

If (A) and (B) are done, then $E, R, J[2]$ with the actions of $G$ and $G_k$, can be computed as submodules and subquotients of $\mathbb{F}_2^\Delta$, as in Section 12.3.

**Magma** shows that there are 1397 conjugacy classes of subgroups in $\text{Sp}_6(\mathbb{F}_2)$ to distinguish. Here are some methods that can be applied (with varying degree of success) towards determining the image $G_K$ of $G_K \to \text{Sp}_6(\mathbb{F}_2)$ (up to $\text{Sp}_6(\mathbb{F}_2)$-conjugacy) for a field $K$:
• **Splitting field.** If a splitting field of $\Delta$ over $K$ is of small enough degree, then Lemma 12.6(d) is practical. But in the worst case, the splitting degree is $\# Sp_6(\mathbb{F}_2) = 1451520$.

• **Orbit sizes.** Factoring $h(x)$ over $K$ determines the orbit sizes of $G_K$; this already cuts the number of possibilities from 1397 down to at most 107 (there are 107 conjugacy classes with orbit size multiset $\{4, 8, 16\}$). Factoring $h(x)$ over the fields obtained by adjoining one root of (one factor of) $h(x)$ determines the orbit size multisets for the one-point stabilizers; these constrain $G_K$ further.

• **Decomposition subgroups.** If $K$ is a global field $k$, and we have computed decomposition subgroups $D_v$ in $Sp_6(\mathbb{F}_2)$ up to $Sp_6(\mathbb{F}_2)$-conjugacy for several $v$, then these constrain the possibilities for $G_K$.

Next we discuss the practicality of these methods for special types of fields $K$:

1. **Finite fields.** Here $G_K$ is cyclic. Magma shows that for each cyclic subgroup of $Sp_6(\mathbb{F}_2)$, either the orbit size multiset determines the conjugacy class uniquely, or the subgroup has size at most 6, in which case the splitting field method is practical. So $G_K$ is determined easily.

2. **Archimedean local fields.** The splitting field has degree at most 2, so use the splitting field method.

3. **Non-archimedean local fields.** If $X$ has good reduction, then we reduce to the case of a finite field. Otherwise, let $q = p^e$ be the size of the residue field (for $k = \mathbb{Q}$, $e = 1$); then we have normal subgroups $P \triangleleft I$ of $G_K$ (wild inertia and inertia) such that $G_K/I$ is cyclic of some order $f$, and $I/P$ is cyclic of order dividing $q^f - 1$ and $P$ is a $p$-group. If $p > 7$, then $p \nmid \# Sp_6(\mathbb{F}_2)$, so $P = \{1\}$, and $G_K$ is metacyclic; there are only 214 conjugacy classes of metacyclic subgroups of $Sp_6(\mathbb{F}_2)$, and the largest such subgroup has order 60, which is about the largest degree for which the splitting field method is easily practical. For $K = \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7$, the maximal size of $G_K$ is 2304, 432, 120, 60, respectively; if the splitting field method is impractical, we can eliminate possibilities by using the orbit size methods, and by using that the local Galois group must be contained in the global Galois group if the latter has been computed already.

4. **The global field $\mathbb{Q}$.** Determining the Galois group of a polynomial $h(t) \in \mathbb{Q}[t]$ is a standard problem in computational number theory: see [Sta73, GK00, Gei03]. A recent implementation by Claus Fieker and Jürgen Klüners in Magma chooses a prime $p$, labels the roots of $h$ in a splitting field $K_p/\mathbb{Q}_p$ by giving approximations to them, and computes the Galois group over $\mathbb{Q}$ as a subgroup of the permutations of the labels; in fact, by choosing an unramified prime $p$, the computations can be done in finite extensions of $\mathbb{F}_p$ instead of $\mathbb{Q}_p$. Once this is done for our $h$ of degree 28, the splitting field method can then compute $G$ in $Sp_6(\mathbb{F}_2)$ up to $Sp_6(\mathbb{F}_2)$-conjugacy.

An alternative to using the general-purpose implementation above is to use orbit sizes and decomposition subgroups to try to eliminate all possibilities except one. When this succeeds, which in practice seems to be almost always the case, it is often faster.

**Summary:** In practice we can always achieve goal (A). Goal (B) may be more difficult to reach, but the methods presented above often succeed. From now on, we assume that both goals have been reached.
12.6.7. **Determining the local images.** Given \( v \in \mathcal{T} \), our goal is to compute elements of \( L_v^\times \) whose images in \( L_v^\times / L_v^\times 2k_v^\times \) form a basis of \( \text{im} C_v \). We follow the approach in Section 11.

First let us explain how to compute the map \( c_K \) in Section 11.1, for any finite extension \( K \) of \( k_v \). Let \((u_0 : v_0 : w_0) \in \Delta(L)\) be the generic point of \( \Delta \) over \( k \); we perturb \( x_0 \) so that \( u_0x + v_0y + w_0z \) does not vanish at \((\text{points in the support of}) \ x_0 \). Given \( P \in X(K) \), choose a linear form \( u_0x + v_0y + w_0z \in K[x,y,z] \) not vanishing at \( P \) or \((\text{points in the support of}) \ x_0 \). If \( P \in X(K) \) does not lie on any bitangent, then evaluating the rational function

\[
\frac{u_0x + v_0y + w_0z}{u_0x + v_0y + w_0z}
\]

at \( P \) and \( x_0 \) give elements of \( L_K^\times ; \) their ratio mapped to \( L_K^\times / L_K^\times 2K^\times \) is \( c_K(P) \). If \( P \) does lie on a bitangent, then use Remark 11.4, which applies since the \( \beta \) are disjoint.

Now, to compute \( \text{im} C_v \), attempt to use Remark 11.6, in which for \( k_v = \mathbb{Q}_p \), (25) becomes

\[
\begin{cases}
\# J(k_v)/2J(k_v) & \text{if } v \neq 2 \\
8\# J[2](k_v) & \text{if } v = 2.
\end{cases}
\]

If the approach of Remark 11.6 fails, use the general approach of Section 11.1 or 11.2.

12.7. **Comparing \( \text{Sel}^\alpha_{\text{fake}}(J) \) with \( \text{Sel}^2(J) \).** Let notation be as in Section 12.6, where we computed a group \( S'_{\mathcal{T}} \) containing \( \text{Sel}^\alpha_{\text{fake}}(J) \), which Section 10.3 relates to \( \text{Sel}^2(J) \).

We review here the ways in which \( S'_{\mathcal{T}}, \text{Sel}^\alpha_{\text{fake}}(J) \), and \( \text{Sel}^2(J) \) can differ:

(i) \( S'_{\mathcal{T}} \) may be larger than \( \text{Sel}^\alpha_{\text{fake}}(J) \)
(ii) \( \text{Sel}^\alpha_{\text{fake}}(J) \) may fail to be contained in \( \alpha(H^1(k,J[2])) \) (both are subgroups of \( H^1(k,E^\vee) \)).
(iii) If \( \text{Sel}^\alpha_{\text{fake}}(J) \subseteq \alpha(H^1(k,J[2])) \), then \( \alpha \) induces a map \( \text{Sel}^2(J) \rightarrow \text{Sel}^\alpha_{\text{fake}}(J) \) (see Theorem 10.14), but it may fail to be injective and/or surjective.

And here are ways to detect or avoid these differences:

(i) Theorem 10.9(b) shows how to choose \( \mathcal{T} \) to ensure that \( \text{Sel}^\alpha_{\text{fake}}(J) = S_{\mathcal{T}} \), in which case both equal the group \( S'_{\mathcal{T}} \) sandwiched between them. But the amount of computation involved in implementing that strategy is probably prohibitive, so we may prefer to use the observation of Remark 10.12.

(ii) Lemma 10.17(b) shows that the containment \( \text{Sel}^\alpha_{\text{fake}}(J) \subseteq \alpha(H^1(k,J[2])) \) follows if \( \text{III}^1(k,R^\vee) = 0 \), and Proposition 8.3 gives an upper bound on \( \text{III}^1(k,R^\vee) \) that is often 0. More precisely, this upper bound is 0 for 1103 of the subgroup classes of \( \text{Sp}_6(\mathbb{F}_2) \). Even if we are unlucky enough to have \( G \) in the remaining 266 subgroup classes, there is hope since we find that there is a \( G \)-orbit in \( \Sigma \) of size at most 7, so the ideas of Appendix A are probably practical; and \( J[2] \) is reducible, so there are nontrivial isogenies available for descent computations.

(iii) In order to estimate the kernels and cokernels of \( \text{Sel}^2(J) \rightarrow \text{Sel}^\alpha_{\text{fake}}(J) \), we use Theorem 10.14. Assuming that we succeeded in computing global and local Galois groups as in Section 12.6.6, we have for each \( v \in \mathcal{T} \) an explicit description of

\[
\begin{align*}
0 \longrightarrow J[2](k_v) & \longrightarrow E^\vee(k_v) \overset{q}{\longrightarrow} R^\vee(k_v) \\
0 \longrightarrow J[2](k_v) & \longrightarrow E^\vee(k_v) \overset{q}{\longrightarrow} R^\vee(k_v).
\end{align*}
\]
Let $\kappa'_v$ be the map $K = \ker \alpha \to \ker \alpha_v$ implicit in (22), which can be identified with
\[
\frac{R^\vee(k)}{qE^\vee(k)} \to \frac{R^\vee(k_v)}{qE^\vee(k_v)},
\]
and hence computed. The map in (22) we are really interested in is the map
\[
\kappa_v : K = \ker \alpha \to W_v := \frac{\ker \alpha_v}{\ker \alpha_v \cap \im \gamma_v}.
\]
We computed $\# J(k_v)/2J(k_v)$ and $\# \im C_v$; dividing gives the size of $\ker C_v \simeq \gamma_v(\ker C_v) = \ker \alpha_v \cap \im \gamma_v$, so in some cases we may have sufficient information to deduce $\kappa_v$ and piece together $\kappa = \prod_v \kappa_v$ and its kernel and cokernel. Even if we can determine $\# \coker \kappa$, however, it is only an upper bound on $\# \coker(\text{Sel}^2(J) \to \text{Sel}^a_{\text{fake}}(J))$ (see Theorem 10.14).

12.8. Descent on the curve. Let $X$ be a smooth plane quartic over a global field $k$ of characteristic not 2. The fake descent setup described in Section 12.1 can be used also to perform a descent on the curve as described in Section 9.3. Let $u_\theta, v_\theta, w_\theta \in L$ be as in Section 12.6.7, and choose $f$ to be $(u_\theta x + v_\theta y + w_\theta z)/\ell$ for some linear form $\ell \in k[x, y, z]$.

To apply Remark 11.5, we need to find the $c$ and $r$ of Lemma 9.5. By interpolation, find a degree 14 form $r_{14} \in k[x, y, z]$ whose zero divisor on $X$ is $\sum_{P \in \Delta} \beta_P$; such a form is unique modulo $g$ and up to scalar multiple. Thus there exists $c \in k^\times$ such that
\[
N_{L[x, y, z]/k[x, y, z]}(u_\theta x + v_\theta y + w_\theta z) \equiv cr_{14}(x, y, z)^2 \pmod{g(x, y, z)}.
\]
Comparing coefficients lets us compute $c$. Then $c$ and $r := r_{14}/\ell^{14}$ are as in Lemma 9.5.

We can now evaluate $C_{f, v}(Q)$ for any $Q \in X(k_v)$, by using $f$; in fact, it suffices to evaluate $u_\theta x + v_\theta y + w_\theta z$ at any triple of homogeneous coordinates representing $Q$, since the value of $\ell$ on this triple will be in $k_v^\times$.

**Lemma 12.13.** Assume that the $u_\theta, v_\theta, w_\theta$ above are in $\mathcal{O}_L$. Let $S \subset \Omega_k$ be a finite set of places containing the archimedean places, the places of residue characteristic 2, the places of bad reduction of the model $g(x, y, z) = 0$ of $X$, and places lying under $\mathcal{O}_L$-primes dividing the $\mathcal{O}_L$-ideal $(u_\theta, v_\theta, w_\theta)$. Then $\im C_f \subset L(2, S)$.

**Proof.** Let $v \in \Omega_k \setminus S$. Then $L_v$ is a product of local fields, and we let $\mathcal{O}_{L_v}$ be the product of their valuation subrings. Suppose that $(x : y : z) \in X(k_v)$. Without loss of generality, $x, y, z \in \mathcal{O}_v$ and $(x, y, z)\mathcal{O}_v = \mathcal{O}_v$. The point $(u_\theta : v_\theta : w_\theta) \in \mathbb{P}^2(L)$ extends to a point in $\mathbb{P}^2(\mathcal{O}_{L_v})$. Given $Q \in \Delta(k_{v,u}) = \Delta(k_s)$, we can specialize $u_\theta$ to an element $u_Q$ in the valuation ring of $k_{v,u}$, and define $v_Q$ and $w_Q$ similarly; our hypothesis on $(u_\theta, v_\theta, w_\theta)$ implies that $\min(v(u_Q), v(v_Q), v(w_Q)) = 0$. On the reduction of $X$ at $v$, the 28 bitangents are distinct, so the reduction of $(x : y : z) \in X(k_v)$ lies on at most one bitangent, so
\[
v(u_Q x + v_Q y + w_Q z) > 0
\]
for at most one $Q$. On the other hand, (27) and our hypothesis on $(u_\theta, v_\theta, w_\theta)$ imply that $2 \mid v(c)$, so
\[
2 \mid v(N_{L_v/k_v}(u_\theta x + v_\theta y + w_\theta z)) = v\left(\prod_Q (u_Q x + v_Q y + w_Q z)\right).
\]
Combining the previous two sentences shows that $2 \mid v(u_Q x + v_Q y + w_Q z)$ for all $Q$, and hence $u_Q x + v_Q y + w_Q z$ is a square in $L \otimes k_{v,u}$. \hfill \Box

By breaking up $X(k_v)$ as in Section 11.1, we can compute $C_{f,v}(X(k_v))$ for any $v$. (Note that in contrast to Section 11.1, we do not need to work with extensions of $k_v$.) For a finite set $T \subset \Omega_k$, we compute

$$S'_T := \{ \delta \in L(2, \mathcal{S}) : N(\delta) \in c k^{x_2} \text{ and } \delta_v \in C_{f,v}(X(k_v)) \text{ for all } v \in T \} ,$$

which contains $\text{Sel}_{f, \text{fake}}^f(X)$. In particular, if $S'_T$ is empty, then $X$ has no $k$-rational points.

On the other hand, the following may be useful in proving the existence of local points:

**Lemma 12.14.** Let $k_v$ be a nonarchimedean local field with valuation ring $\mathcal{O}_v$ and residue field $\mathbb{F}_v$ of size at least 37. If $X_{k_v}$ is a smooth plane quartic, and $X_{\mathbb{F}_v}$ is geometrically irreducible, then $X(k_v)$ is nonempty.

*Proof.* Removing the singularities from $X_{\mathbb{F}_v}$ yields a smooth curve of genus $g$ with at most $6 - 2g$ punctures, for some $g \in \{0, 1, 2, 3\}$. In all four cases, the Hasse-Weil bound implies the existence of a smooth $\mathbb{F}_v$-point. By Hensel’s lemma, it lifts to an $\mathcal{O}_v$-point, which gives a $k_v$-point. \hfill \Box

12.9. **Examples.** Denis Simon kindly supplied us with a list of smooth plane quartics with small integer coefficients and small discriminant. These serve as test cases for the methods outlined in Section 12.6. In the first three examples, we use fake descent to determine the structure of $J(\mathbb{Q})$, which in the first two examples lets us determine $X(\mathbb{Q})$. In the fourth example, we use descent on the curve to prove that $X(\mathbb{Q}) = \emptyset$.

12.9.1. A genus 3 curve with $J(\mathbb{Q}) \simeq \mathbb{Z}/51\mathbb{Z}$. Let $X$ be the curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by

$$x^3y - x^2y^2 - x^2z^2 - xy^2z + xz^3 + y^3z = 0 .$$

(This is isomorphic to the curve of smallest discriminant in Simon’s list.)

*Steps 1 and 2.* The algebra $L = \mathbb{Q}[t]/(h(t))$ turns out to be a degree 28 number field over $\mathbb{Q}$. It follows that $\mathcal{G}_L$ acts transitively on the bitangents. We compute $\mathcal{O}_L$ and find that $\text{Disc} \mathcal{O}_L = 2^{42} \cdot 29^6 \cdot 163^9$.

*Step 3.* We find that $I_{27} = 4727 = 29 \cdot 163$. By Remark 12.11, we may take $\mathcal{S} = \{2, \infty\}$.

*Step 4.* The class group of $\mathcal{O}_L$ is generated by primes of norm below the Minkowski bound, which is 36,984,868, remarkably small for a degree-28 number field. We can prove unconditionally that the class group of $\mathcal{O}_L$ is trivial, and we can find explicit generators of $L(2, \mathcal{S})$. We find $L(2, \mathcal{S}) \simeq (\mathbb{Z}/2\mathbb{Z})^{17}$ and $\widetilde{L(2, \mathcal{S})} \simeq (\mathbb{Z}/2\mathbb{Z})^{15}$.

*Step 5.* By computing the Frobenius action at 3 and 5, we find that $G$ is either the full group $\text{Sp}_6(\mathbb{F}_2)$ or the unique index-36 subgroup up to conjugacy. The larger group acts doubly transitively on the bitangents, whereas the smaller does not. If we factor $h(t)$ over $L$, we find factors of degrees 1, 12, 15, so $G$ is the smaller group. With this information we can check that

$$0 \longrightarrow J[2](\mathbb{Q}) \longrightarrow E^\vee(\mathbb{Q}) \longrightarrow R^\vee(\mathbb{Q}) \longrightarrow 0$$

$$\begin{array}{c|c|c}
0 & 0 & \mathbb{F}_2 \\
\end{array}$$

(28)
Step 6. Taking $\mathcal{T} = \emptyset$ (i.e., doing no local computations with $X$) yields the upper bound $S_0' \simeq (\mathbb{Z}/2\mathbb{Z})^{13}$ on $\text{Sel}^g_{\text{fake}}(J)$. To obtain a better bound, we next try $\mathcal{T} = \{2\}$; it will turn out that this suffices.

Step 6a. We check that $h$ is irreducible over $\mathbb{Q}_2$, so $D_2$ acts transitively on $\Delta$. This, together with the general constraints on a decomposition subgroup at 2, leaves only two candidates for $D_2$ up to conjugacy: a group $G_{56}$ of order 56 and a group $G_{168}$ of order 168. We can distinguish these by the number of points fixed by their one-point stabilizers: $G_{56}$ leaves 4 points fixed and $G_{168}$ leaves 1 point fixed. We find that $h$ has 4 roots in $\mathbb{Q}_2(\theta)$, so $D_2 = G_{56}$.

Actually, the distinction is unimportant, because for either group we have

$$\text{Step 6b.} \quad \text{From } J[2](\mathbb{Q}_2) = 0 \text{ and (26), we deduce } \# \text{ im } \gamma_2 = 8. \quad \text{Embed } X_{\mathbb{Q}_2} \text{ in } J_{\mathbb{Q}_2} \text{ using } x_0 = (0 : 0 : 1) \in X(\mathbb{Q}_2); \quad \text{we find points in } X(\mathbb{Q}_2) \text{ whose images under } C_2 \text{ generate a group of size } 8. \quad \text{Thus the inequality } \# \text{ im } C_2 \leq \# \text{ im } \gamma_2 \text{ is an equality; i.e., } \# \text{ im } C_2 = 8. \quad \text{By Lemma 10.4 and its proof, we obtain}

$$W_2 \simeq \ker \alpha_2 \simeq \frac{R^\vee(\mathbb{Q}_2)}{qE^\vee(\mathbb{Q}_2)} \simeq \mathbb{Z}/2\mathbb{Z},$$

by (29).

Step 7. Given that we have explicit generators for $\widetilde{L(2,S)}$, we can compute the map

$$\widetilde{L(2,S)} \rightarrow \frac{(L \otimes \mathbb{Q}_2)^\times}{(L \otimes \mathbb{Q}_2)^\times \otimes \mathbb{Q}_2^\times}.$$ 

In Step 6b, we computed $\text{im } C_2$, so we can compute $S_2'$ for $\mathcal{T} = \{2\}$. We find $S_2' = 0$. Thus $\text{Sel}^g_{\text{fake}}(J) = 0$.

By (28) and Corollary 10.15, $\text{Sel}^2(J)$ is either 0 or $\mathbb{Z}/2\mathbb{Z}$. We can decide which by computing $\ker \kappa$ in Theorem 10.14. By (30), the map $K \rightarrow W_2$ is $R^\vee(\mathbb{Q})/qE^\vee(\mathbb{Q}) \rightarrow R^\vee(\mathbb{Q}_2)/qE^\vee(\mathbb{Q}_2)$, which is an isomorphism, so $\kappa$ is injective; thus $\text{Sel}^2(J) = 0$ by Theorem 10.14.

Remark 12.15. The situation can be reinterpreted as follows: the kernel $K$ of the map $\alpha : H^1(Q, J[2]) \rightarrow H^1(Q, E^\vee)$ has a non-trivial element $\delta$, but its restriction $\delta_2 \in H^1(\mathbb{Q}_2, J[2])$ is not in $\text{im } \gamma_2$. (This is because $0 \neq \delta_2 \in \ker \alpha_2$, while $\text{im } \gamma_2 \cap \ker \alpha_2 = 0$: see Step 6b above.) In classical language, $\delta$ corresponds to a 2-covering of $J$ that has no $\mathbb{Q}_2$-point, so $\delta \notin \text{Sel}^2(J)$.

Proposition 12.16. If $X$ is the curve

$$x^3 y - x^2 y^2 - x^2 z^2 - xy^2 z + xz^3 + y^3 z = 0$$
in $\mathbb{P}^2_Q$, then $J(\mathbb{Q}) = \langle (x : y : z) \rangle \simeq \mathbb{Z}/51\mathbb{Z}$ and

$$X(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 0 : 1), (1 : 0 : 0), (1 : 0 : 1), (1 : 1 : 0), (1 : 1 : 1)\}.$$

Proof. Since $\text{Sel}^2(J) = 0$, the group $J(\mathbb{Q})$ is finite and of odd order. Reduction modulo 3 injects $J(\mathbb{Q})_{\text{tors}}$ into $J(\mathbb{F}_3)$, which, according to Magma, is of order 51. (We use $J(\mathbb{F}_3)$ to denote the group of $\mathbb{F}_3$-points on the reduction.) On the other hand, Magma shows that $\langle (0 : 1 : 0) - (0 : 0 : 1) \rangle$ is of exact order 51 in $J(\mathbb{Q})$. Thus $J(\mathbb{Q}) \simeq \mathbb{Z}/51\mathbb{Z}$. 

\[ \text{Page 41} \]
Finally, we determine $X(\mathbb{Q})$. The Abel-Jacobi map $X \rightarrow J$ given by $P \mapsto [P - (0 : 0 : 1)]$ injects $X(\mathbb{Q})$ into $J(\mathbb{Q})$. Magma determines which points in $J(\mathbb{Q})$ can be represented as $[P - (0 : 0 : 1)]$, and the result is as stated.$\square$

12.9.2. A positive rank example. Let $X$ be the curve in $\mathbb{P}^2_\mathbb{Q}$ defined by

$$x^2y^2 - xy^3 - x^3z - 2x^2z^2 + y^2z^2 - xz^3 + yz^3 = 0.$$ 

The group $J(\mathbb{Q})_{\text{tors}}$ injects into $J(\mathbb{F}_3)$, and its odd part injects into $J(\mathbb{F}_2)$ (the curve has good reduction at 2 and 3). We compute $J(\mathbb{F}_2) \simeq \mathbb{Z}/71\mathbb{Z}$ and $J(\mathbb{F}_3) \simeq \mathbb{Z}/85\mathbb{Z}$, so $J(\mathbb{Q})_{\text{tors}} = 0$. On the other hand, the divisor class

$$G := [(0 : 1 : -1) + (0 : 0 : 1) - 2(0 : 1 : 0)]$$

is nonzero since $X$ is not hyperelliptic. Thus $\text{rk}J(\mathbb{Q}) \geq 1$.

Steps 1 and 2. The algebra $L$ turns out to be a degree 28 number field. We find that $\text{Disc} \mathcal{O}_L = 2^{42} \cdot 41^5 \cdot 347^6$.

Step 3. We have $I_{27} = 41 \cdot 347$. By Remark 12.11, we may take $\mathcal{S} = \{2, \infty\}$.

Step 4. The Minkowski bound for $\mathcal{O}_L$ is $1008340641$. The truly dedicated enthusiast could probably verify unconditionally that the class group of $\mathcal{O}_L$ is trivial. We verified this only conditionally on the Generalized Riemann Hypothesis for $L$. Subject to this, we find explicit generators of $L(2, \mathcal{S}) \simeq (\mathbb{Z}/2\mathbb{Z})^{17}$ and $\overline{L(2, \mathcal{S})} \simeq (\mathbb{Z}/2\mathbb{Z})^{15}$.

Step 5. By computing the Frobenius action at 5 and 7, we find that $G \simeq \text{Sp}_6(\mathbb{F}_2)$. Thus $J[2](\mathbb{Q}) = E^\vee(\mathbb{Q}) = R^\vee(\mathbb{Q}) = 0$.

Step 6. It will turn out that taking $\mathcal{T} = \{2\}$ is enough to obtain the upper bound $S_{\mathcal{T}}' \simeq \mathbb{Z}/2\mathbb{Z}$ on $\text{Sel}_\text{fake}^2(J)$.

Step 6a,b. We check that $h$ is irreducible over $\mathbb{Q}_2$, so $D_2$ acts transitively on the bitangents. This leaves 6 possibilities for $D_2$ up to $\text{Sp}_6(\mathbb{F}_2)$-conjugacy, but for all of them we have $J[2](\mathbb{Q}_2) = E^\vee(\mathbb{Q}_2) = 0$. Following Remark 11.6, we obtain $\# \text{im} C_2 \leq \# J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 8$ (see (26)), but we also find enough points in $X(\mathbb{Q}_2)$ to show that $\# \text{im} C_2 \geq 8$, so $\# \text{im} C_2 = 8$.

Step 7. We can compute the map

$$\overline{L(2, \mathcal{S})} \rightarrow \frac{(L \otimes \mathbb{Q}_2)^\times}{(L \otimes \mathbb{Q}_2)^\times \mathbb{Q}_2^\times}$$

explicitly, and we have $\text{im} C_2$; from this we compute that $S_{\mathcal{T}}' \simeq \mathbb{Z}/2\mathbb{Z}$.

Since $R^\vee(\mathbb{Q}) = 0$, Corollary 10.15 implies that $\text{Sel}_2^2(J) \rightarrow \text{Sel}_\text{fake}^2(J)$ is injective. Thus

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow \text{Sel}_2^2(J) \hookrightarrow \text{Sel}_\text{fake}^2(J) \subset S_{\mathcal{T}}' \simeq \mathbb{Z}/2\mathbb{Z},$$

so $\text{rk} J(\mathbb{Q}) \leq 1$. Combining this with the earlier information yields $J(\mathbb{Q}) \simeq \mathbb{Z}$.

Proposition 12.17. Let $X$ be the curve

$$x^2y^2 - xy^3 - x^3z - 2x^2z^2 + y^2z^2 - xz^3 + yz^3 = 0$$

in $\mathbb{P}^2_\mathbb{Q}$. Assume the Generalized Riemann Hypothesis. Then $J(\mathbb{Q}) \simeq \mathbb{Z}$ and

$$X(\mathbb{Q}) = \{(1 : 1 : 0), (-1 : 0 : 1), (0 : -1 : 1), (0 : 1 : 0),$$

$$(1 : 1 : -1), (0 : 0 : 1), (1 : 0 : 0), (1 : 4 : -3)\}.$$
Step 4. The Minkowski bound for Step 3. We compute
\[ J = 13 \]
This curve has at least the following 7 rational points.

We check that \( \#X(\mathbb{F}_3) = 7 \), and that the set of 8 points in \( X(\mathbb{Q}) \) listed above surjects onto \( X(\mathbb{F}_3) \), with \( P_0 := (1 : 1 : 0) \) and \( P_1 := (1 : 4 : -3) \) reducing to the same point. Since \( \text{rk} J(\mathbb{Q}) = 1 \) and \( \dim J = 3 \), there is a 2-dimensional subspace \( V \subset H^0(X_{\mathbb{Q}_3}, \Omega^1) \) such that \( f_{P}^{\omega} \omega = 0 \) for all \( P, P' \in X(\mathbb{Q}) \) and \( \omega \in V \). Since \([P_1 - P_0] \) is nonzero in \( J(\mathbb{Q}) \), it is of infinite order, so \( V = \{ \omega : f_{P_0}^{\omega} = 0 \} \). We compute this integral (to some 3-adic precision) for \( \omega \) in a basis for \( H^0(X_{\mathbb{Q}_3}, \Omega^1) \) by evaluating the integral as a power series in a uniformizing parameter \( t \) at \( P_0 \); then algebra produces a basis for \( V \). Explicitly, if we identify each \( \omega \in H^0(X_{\mathbb{Q}_3}, \Omega^1) \) with a linear form \( ux + vy + wz \), a basis for \( V \) is given by \( \omega_1 \) corresponding to \((21262 + O(3^{10}))x - y \) and \( \omega_2 \) corresponding to \((1302 + O(3^{10}))x - z \).

For each point of \( X(\mathbb{F}_3) \), we need to find the rational points in the corresponding residue class in \( X(\mathbb{Q}_3) \). For each point \( Q \in X(\mathbb{F}_3) \) other than the reduction of \( P_0 \) (and \( P_1 \)), the mod 3 reduction of one of \( \omega_1, \omega_2 \) is nonvanishing at \( Q \), so by Proposition 6.3 in [Sto06], there is at most one rational point reducing to \( Q \), and we already know one. The rational points \( P \) in the residue class containing \( P_0 \) and \( P_1 \) satisfy \( f_{P_0}^{\omega_1} = f_{P_0}^{\omega_2} = 0 \); these give two power series equations over \( \mathbb{Q}_3 \) to be solved for \( t \in 3\mathbb{Z}_3 \). We calculate that each power series has three zeros in \( 3\mathbb{Z}_3 \), but the intersection is of size at most 2, so \( P_0 \) and \( P_1 \) are the only rational points in this residue class.

12.9.3. A modular curve of level 13. Let \( X_{\text{split}}(13) \) (resp. \( X_{\text{nonsplit}}(13) \)) be the modular curve of level 13 over \( \mathbb{Q} \) corresponding to the normalizer of a split (resp. nonsplit) Cartan subgroup of \( \text{SL}_2(\mathbb{Z}/13\mathbb{Z}) \). These are non-hyperelliptic curves of genus 3, and it turns out [Bar13,Bar12] that both are isomorphic to the smooth plane quartic curve
\[
X : x^3y + x^3z - 2x^2y^2 - x^2yz + xy^3 - xy^2z + 2xyz^2 - xz^3 - 2y^2z^2 + 3yz^3 = 0.
\]
This curve has at least the following 7 rational points.
\[
\{(0 : 1 : 0), (0 : 0 : 1), (-1 : 0 : 1), (1 : 0 : 0), (1 : 1 : 0), (0 : 3 : 2), (1 : 0 : 1)\}
\]
We compute \( J(\mathbb{F}_3) \simeq \mathbb{Z}/91\mathbb{Z} \) and \( J(\mathbb{F}_7) \simeq \mathbb{Z}/659\mathbb{Z} \). Since \( J(\mathbb{Q})_{\text{tors}} \) injects into both groups, \( J(\mathbb{Q})_{\text{tors}} = 0 \). This, with the fact that \( \#X(\mathbb{Q}) \geq 2 \), implies that \( \text{rk} J(\mathbb{Q}) > 0 \). One can verify that the divisor classes
\[
[(0 : 1 : 0) - (1 : 0 : 0)], [(0 : 0 : 1) - (1 : 0 : 0)], [(-1 : 0 : 1) - (1 : 0 : 0)] \in J(\mathbb{Q})
\]
generate a group containing all differences of the points listed above. Furthermore, the image in \( J(\mathbb{F}_3) \times J(\mathbb{F}_5) \times J(\mathbb{F}_{43}) \) is isomorphic to
\[
\mathbb{Z}/(7 \cdot 13 \cdot 29 \cdot 97)\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z},
\]
so \( \text{rk} J(\mathbb{Q}) \geq 3 \).

We apply the procedure in Section 12.6 to compute an upper bound on \( \text{rk} J(\mathbb{Q}) \).

Steps 1 and 2. The algebra \( L \) is a degree 28 number field with \( \text{Disc} \mathcal{O}_L = 2^{12} \cdot 13^{24} \).

Step 3. We have \( I_{27} = 13^6 \). The closed subscheme of \( \mathbb{P}^2_{\mathbb{Z}_{13}} \) defined by (31) is regular, and its special fiber is a geometrically integral curve of genus 0, so \( c_{13}(J) = 1 \). Therefore we can take \( \mathcal{S} = \{2, \infty\} \).

Step 4. The Minkowski bound for \( \mathcal{O}_L \) is 8158071456. The truly dedicated enthusiast could probably verify unconditionally that the class group of \( \mathcal{O}_L \) is trivial. We verified this only
conditionally on the Generalized Riemann Hypothesis for $L$. Subject to this, we find explicit generators of $L(2, S) \simeq (\mathbb{Z}/2\mathbb{Z})^{17}$ and $\overline{L}(2, S) \simeq (\mathbb{Z}/2\mathbb{Z})^{15}$.

Step 5. Since $L$ is a field, $G$ acts transitively on the bitangents. There are 18 subgroups of $\text{Sp}_6(\mathbb{F}_2)$ up to conjugacy with that property. The Fieker-Klüners implementation in Magma for finding Galois groups yields $\#G = 504$. This determines $G$ uniquely up to conjugacy.

This information allows us to compute:

$$
\begin{array}{c}
0 \longrightarrow J[2](\mathbb{Q}) \longrightarrow E^\vee(\mathbb{Q}) \longrightarrow R^\vee(\mathbb{Q}) \\
0 \longrightarrow 0 \longrightarrow \mathbb{F}_2^2.
\end{array}
$$

Steps 6 and 7. It will turn out that taking $T = \{2\}$ is enough to obtain the upper bound $S(2) \simeq \mathbb{Z}/2\mathbb{Z}$ on $\text{Sel}_{\text{fake}}^0(J)$. The fact that $L$ has only one prime above 2 shows that $D_2$ acts transitively. This together with the constraints on a decomposition group at 2 determines $D_2$ uniquely up to conjugacy in $\text{Sp}_6(\mathbb{F}_2)$. We obtain $\#D_2 = 56$ and

$$
\begin{array}{c}
0 \longrightarrow J[2](\mathbb{Q}_2) \longrightarrow E^\vee(\mathbb{Q}_2) \longrightarrow R^\vee(\mathbb{Q}_2) \\
0 \longrightarrow 0 \longrightarrow \mathbb{F}_2^2.
\end{array}
$$

Following Remark 11.6, we obtain $\# \text{im} C_2 \leq \# \text{im} \gamma_2 = #J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 2^3$ (see (26)). Further computation shows that $S_0 = (\mathbb{Z}/2\mathbb{Z})^{13}$ and that the homomorphism

$$
S_0^\prime \rightarrow \frac{(L \otimes \mathbb{Q}_2)^\times}{(L \otimes \mathbb{Q}_2)^\times \mathbb{Q}_2^\times}
$$

is injective. It follows that $\# S_0^\prime \leq \# \text{im} C_2 \leq 2^3$. Thus $\# \text{Sel}_{\text{fake}}^0(J) \leq 2^3$. By Corollary 10.15 and (32), this implies $\# \text{Sel}^2(J) \leq 2^5$, so $\text{rk} J(\mathbb{Q}) \leq 5$.

We now present two approaches to improve this to $\text{rk} J(\mathbb{Q}) \leq 3$. The first is to use the isomorphism $\text{End} J \simeq \mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ of [Bar12, Proposition 2.4] to obtain that $\text{rk} J(\mathbb{Q})$ is a multiple of 3, which improves the bound to $\text{rk} J(\mathbb{Q}) \leq 3$. The second is to follow Section 11.1 to compute that $\# \text{im} C_2 = 2$, which can be used as follows. By the same argument as in the previous paragraph, $\# \text{im} C_2 = 2$ implies $\# \text{Sel}_{\text{fake}}^0(J) \leq 2^3$ and $\# \text{Sel}^2(J) \leq 2^3$. On the other hand, $3 \leq \text{rk} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \text{Sel}^2(J)$, so equality holds everywhere in this paragraph. In particular, if $\text{III}(J)$ is the Shafarevich-Tate group of $J$, then $\text{III}(J)[2] = 0$. We have proved

**Proposition 12.18.** Let $X = X_{\text{split}}(13) \simeq X_{\text{nonsplit}}(13)$ over $\mathbb{Q}$. Assume the Generalized Riemann Hypothesis. Then $J(\mathbb{Q}) \simeq \mathbb{Z}^3$ and $\text{III}(J)[2] = 0$.

**Remark 12.19.** By (33) and Lemma 10.4, we have $W_2 = 0$. In particular, we are in the situation of Corollary 10.16.

12.9.4. A genus 3 curve violating the local-to-global principle. The fake descent setup presented in Section 12.1 allows us also to compute $\text{Sel}_{\text{fake}}^0(X)$ for a smooth plane quartic $X$.

**Proposition 12.20.** Let $X$ be the curve in $\mathbb{P}_\mathbb{Q}^2$ defined by

$$
x^4 + y^4 + x^2yz + 2xyz^2 - y^2z^2 + z^4 = 0.
$$

Then $X(\mathbb{R}) \neq \emptyset$ and $X(Q_p) \neq \emptyset$ for all $p$, but if the Generalized Riemann Hypothesis holds, then $X(\mathbb{Q}) = \emptyset$. 

44
Proof. We have \( I_{27} = -2^8 \cdot 5^2 \cdot 1361 \cdot 97103 \), so Lemma 12.14 implies \( X(\mathbb{Q}_p) \neq \emptyset \) for \( p \geq 37 \). A further calculation using Hensel’s lemma shows that \( X(\mathbb{Q}_p) \neq \emptyset \) for \( p < 37 \) too, and that \( X(\mathbb{R}) \neq \emptyset \).

To prove \( X(\mathbb{Q}) = \emptyset \), we apply Section 12.8 with \( S = \{ \infty, 2, 5, 1361, 97103 \} \). It is straightforward to find \((u_9, v_9, w_9)\) satisfying the hypotheses of Lemma 12.13 for \( S \). We find that \( \text{Disc}(O_L) = 2^{30} \cdot 5^{10} \cdot 1361^6 \cdot 97103^6 \) and that the Minkowski bound exceeds \( 10^{22} \), so determining \( \text{Cl}(O_{L,S}) \) unconditionally is out of the question. Conditional on the Generalized Riemann Hypothesis for \( L \), which we assume from now on, we find that \( \text{Cl}(O_{L,S}) = \mathbb{Z}/2\mathbb{Z} \) and we also find \( O_{L,S}^\times/O_{L,S}^{\times 2} \). This leads to explicit generators of \( L(2, S) \simeq (\mathbb{Z}/2\mathbb{Z})^{41} \) and \( L(2, S) \simeq (\mathbb{Z}/2\mathbb{Z})^{36} \). We compute \( c = -1 \). For \( T = \{ 2, 1361 \} \), we find \( S_T' = \emptyset \), so \( X(\mathbb{Q}) = \emptyset \). \( \square \)

Appendix A. Determining the \( \phi \)-Selmer group directly

We can modify our approach so that it computes \( \text{Sel}^\phi(J) \) directly, instead of computing \( \text{Sel}^\text{true/fake}(J) \) and hoping to control the difference.

The fundamental idea behind a true descent setup is to replace the Galois module \( \hat{J}[\phi] \) whose cohomology we want by a permutation module \((\mathbb{Z}/n\mathbb{Z})^\Delta \) whose cohomology we can compute. The discrepancies between \( \text{Sel}^\text{true/fake}(J) \) and \( \text{Sel}^\phi(J) \) come from the non-injectivity of \( (\mathbb{Z}/n\mathbb{Z})^\Delta \to \hat{J}[\phi] \). In this section we deal with the non-injectivity by finding another permutation module \((\mathbb{Z}/n\mathbb{Z})^{\Delta'} \) that surjects onto the kernel.

A.1. Correspondences. A correspondence \( \Delta \to \Delta' \) between finite \( \mathcal{G} \)-sets is a \( \mathcal{G} \)-homomorphism \( \mathbb{Z}^{\Delta} \to \mathbb{Z}^{\Delta'} \). Given a \( \mathcal{G} \)-module \( M \) and \( \Delta \to \Delta' \), we define homomorphisms \( \tau^*: M^{\Delta'} \to M^\Delta \) and \( \tau_*: M^\Delta \to M^{\Delta'} \) as follows. Restricting the composition pairing

\[
\text{Hom}_\mathbb{Z}(\mathbb{Z}^{\Delta'}, M) \times \text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'}) \to \text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, M)
\]

by setting the second argument to \( \tau \) yields a \( \mathcal{G} \)-homomorphism that with the identifications of Remark 3.3 becomes \( \tau^*: M^{\Delta'} \to M^\Delta \). Applying this construction to the \( \mathbb{Z} \)-dual of \( \tau \) yields \( \tau_* \).

Example A.1. Suppose that \( X \) is a nice \( k \)-variety. If we apply the previous remark to the \( \acute{e} \text{tale} \) group scheme \( M \) such that \( M(k_s) \) is the \( \mathcal{G}_k \)-module \( \text{Div}(X) \), then \( M^\Delta(k) = \text{Div}(X \times \Delta) \), and we obtain \( \tau_*: \text{Div}(X \times \Delta) \to \text{Div}(X \times \Delta') \). Similarly we obtain \( \tau_*: k(X \times \Delta)^\times \to k(X \times \Delta')^\times \).

Lemma A.2. Let \( M \) be a finite \( \mathcal{G} \)-module such that \( nM = 0 \).
(a) There exists a finite \( \mathcal{G} \)-set \( \Delta \) with a surjection \((\mathbb{Z}/n\mathbb{Z})^\Delta \to M \).
(b) There exists a finite \( \mathcal{G} \)-set \( \Delta \) with an injection \( M \hookrightarrow \mu_n^\Delta \) (here we assume \( \text{char } k \nmid n \)).

Proof. For (a), take \( \Delta = M \): the identity \( M \to M \) induces \( \mathbb{Z}^M \to M \), which factors through \((\mathbb{Z}/n\mathbb{Z})^M \) since \( nM = 0 \). Applying (a) to \( M^\times := \text{Hom}_\mathbb{Z}(M, k^*_s) \) and applying \( \text{Hom}_\mathbb{Z}(-, k^*_s) \) yields (b). \( \square \)

Lemma A.3. Each of the four homomorphisms

\[
\begin{align*}
\text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'}) & \xrightarrow{\tau^*} \text{Hom}_\mathbb{Z}((\mathbb{Z}/n\mathbb{Z})^\Delta, (\mathbb{Z}/n\mathbb{Z})^{\Delta'}) \\
\text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'}) & \xrightarrow{\tau^*} \text{Hom}_\mathbb{Z}((\mathbb{Z}/n\mathbb{Z})^{\Delta'}, (\mathbb{Z}/n\mathbb{Z})^\Delta) \\
\text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'}) & \xrightarrow{\tau^*} \text{Hom}_\mathbb{Z}(\mu_n^\Delta, \mu_n^{\Delta'}) \\
\text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'}) & \xrightarrow{\tau^*} \text{Hom}_\mathbb{Z}(\mu_n^{\Delta'}, \mu_n^\Delta)
\end{align*}
\]
is surjective with kernel $n \text{Hom}_\mathbb{Z}(\mathbb{Z}^\Delta, \mathbb{Z}^{\Delta'})$ (in the last two we assume $\text{char } k \nmid n$).

**Proof.** The statements do not involve the $G$-action, so each reduces to an easy statement about abelian groups. □

### A.2. Determining the Selmer group.

Set $\widehat{G}_m^\Delta := G_m^\Delta$ for a true descent setup, and $\widehat{G}_m^{\Delta'} := G_m^{\Delta'}/\mu_n$ for a fake descent setup.

Recall that $R = \ker(\alpha^\vee: E \to \hat{J}(\hat{\phi}))$. Fix a finite étale scheme $\Delta' = \text{Spec } L'$ with a surjection $(\mathbb{Z}/n\mathbb{Z})^{\Delta'} \to R$ (one such choice is $\Delta' = R$). By definition of $R$, we have an exact sequence

$$
(34) \quad (\mathbb{Z}/n\mathbb{Z})^{\Delta'} \to E \to \hat{J}(\hat{\phi}) \to 0
$$

and its dual

$$
(35) \quad 0 \to A[\phi] \to E^\vee \to \mu_n^{\Delta'}
$$
in which the image of the last map is $R^\vee$.

**Remark A.4.** Define $Q$ and $q'$ by the exact sequence

$$
(36) \quad 0 \to R^\vee \to \mu_n^{\Delta'} \to q' \to Q \to 0.
$$

If $Q(k) = q'(\mu_n(L'))$ and $\Pi^1(k, \mu_n^{\Delta'}) = 0$ (the latter holds if $n$ is prime, by Lemma 8.2), then $\Pi^1(k, R^\vee) = 0$, so the first assumption in Corollary 10.16 is satisfied. This gives a simple way of showing that $\Pi^1(k, R^\vee)$ vanishes, but the criterion can be weaker than that coming from Section 8.

By Lemma A.3, the composition

$$
(37) \quad (\mathbb{Z}/n\mathbb{Z})^{\Delta'} \to R \to E \to (\mathbb{Z}/n\mathbb{Z})^\Delta
$$

is $\tau^*$ for some correspondence $\Delta \cdots \to \Delta'$. We use $\tau_*$ to denote any of several homomorphisms induced by $\tau$; the context will make the meaning clear. In the fake case, $\tau_*: \mu_n^{\Delta} \to \mu_n^{\Delta'}$ kills the diagonal $\mu_n$, because taking duals in (37) shows that $\tau_*$ factors through $E^\vee = \mu_n^{\Delta}/\mu_n$. Thus $\tau_*: G_m^\Delta \to G_m^{\Delta'}$ induces $\tau_*: \widehat{G}_m^\Delta \to \widehat{G}_m^{\Delta'}$ in both cases.
Let $U$ be the image of $(\tau_n, n): G_m^\Delta \to G_m^\Delta \times G_m^\Delta$. The last map in (35) is induced by $\tau_n: \mu_n^\Delta \to \mu_n^{\Delta'}$, so we have a commutative diagram with exact rows and columns

\[
\begin{array}{ccccccc}
0 & & & & & & 0 \\
\downarrow & & & & & & \downarrow \\
0 & \longrightarrow & A[\phi] & \longrightarrow & \widetilde{G_m^\Delta}^{(\tau_n, n)} & \longrightarrow & U & \longrightarrow & 0 \\
\downarrow & & & & & & \downarrow \text{pr}_2 \\
0 & \longrightarrow & E' & \longrightarrow & \widetilde{G_m^\Delta} & \longrightarrow & \widetilde{G_m^\Delta} & \longrightarrow & 0,
\end{array}
\]

(38)

in which \(\ker \text{pr}_2\) is identified as \(E'\) by the snake lemma. Taking cohomology, we obtain

\[
\begin{array}{ccccccc}
R^{\tau}(k) & & & & & & R^{\tau}(k) \\
\downarrow & & & & & & \downarrow \\
(G_m^\Delta(k))^{(\tau_n, n)} & \longrightarrow & U(k) & \longrightarrow & H^1(k, A[\phi]) & \longrightarrow & H^1(k, \widetilde{G_m^\Delta}) \\
\downarrow & & & & & & \downarrow \text{pr}_2 \\
E'(k) & \longrightarrow & (G_m^\Delta(k)) & \longrightarrow & L & \longrightarrow & H^1(k, E') & \longrightarrow & H^1(k, \widetilde{G_m^\Delta}).
\end{array}
\]

(39)

**Lemma A.5.** There is a finite étale \(k\)-scheme \(\Delta''\) and a correspondence \(\Delta' \cdots \Delta''\) such that

\[
\mu_n^\Delta \rightarrow_{\tau_n} \mu_n^{\Delta'} \rightarrow_{\tau_n} \mu_n^{\Delta''}
\]

is exact. There is another correspondence \(\Delta' \cdots \Delta''\) such that \(\tau' \circ \tau = n\tau''\). Then

\[
U = \ker\left( G_m^{\Delta'} \times G_m^\Delta \longrightarrow G_m^{\Delta'} \times G_m^{\Delta''}, \quad (\ell', \ell) \mapsto \left( \frac{\ell'^n}{\ell}, \frac{\tau'_n(\ell')}{\tau''_n(\ell')} \right) \right).
\]

**Proof.** Lemma A.2(b) applied to the cokernel of \(\tau_n\) yields \(\Delta''\) and \(\tau'\). By Lemma A.3, \(\tau' \circ \tau\) is \(n\) times some \(\tau''\). Direct computation shows that \(U\) is contained in the kernel. To see the other inclusion, let \((\ell', \ell)\) be in the kernel. Let \(\lambda \in G_m^{\Delta}(k_n)\) be such that \(\lambda^n = \ell\), and let \(\zeta' = \ell' / \tau_n(\lambda)\). Then \(\zeta'^n = \ell'^n / \tau_n(\lambda^n) = \ell'^n / \tau_n(\ell) = 1\), so \(\zeta' \in \mu_n^\Delta\). Also,

\[
\tau_n'(\zeta') = \frac{\tau'_n(\ell')}{\tau'_n(\lambda)} = \frac{\tau'_n(\ell')}{(n\tau'')_n(\lambda)} = \frac{\tau'_n(\ell')}{\tau''_n(\ell)} = 1,
\]

which implies that \(\zeta' = \tau_n(\zeta)\) for some \(\zeta \in \mu_n^\Delta\). Then \((\ell', \ell) = (\tau_n(\zeta), (\zeta)\lambda^n) \in U. \) \qed
Corollary A.6. Keeping the notation from Lemma A.5, we have

\[ U(k) = \{(\ell', \ell) \in L'^\times \times L^\times : \tau_*(\ell) = \ell'^n, \tau_*''(\ell) = \tau_*'(\ell') \}. \]

In this paragraph, suppose that we are in the fake case. The map \( \tau_* : \mu_{nD}^\Delta \to \mu_{nD'}^\Delta \) factors through \( E' = \mu_{nD}/\mu_n \), so it kills the diagonal image of \( \mu_n \). Let \( \iota : \mathbb{Z} \to \mathbb{Z}^\Delta \) be the diagonal embedding; the previous sentence shows that \((\tau \circ \iota)_* : \mu_n \to \mu_{nD'}^\Delta \) is trivial. By Lemma A.3, \( \tau \circ \iota = n\theta \) for some correspondence \( \theta \). The image of \( a \in k^\times \) under \( \theta_* : \mathbb{G}_m \to \mathbb{G}_m^{\Delta'} \) in each component of \( (L')^\times \) is a fixed power of \( a \).

Lemma A.7.

(a) In the true case, \( \overline{\mathbb{G}_m}(k) \) is mapped by \( \overline{\mathbb{G}_m} \) to \( L^\times \subseteq L^\times \) and by \( (\tau_*, n) \) to

\[ (\tau_*(\ell), \ell^n) : \ell \in L^\times \subseteq U(k). \]

(b) In the fake case, \( \overline{\mathbb{G}_m}(k) \) is mapped by \( \overline{\mathbb{G}_m} \) to \( L^\times k^\times \subseteq L^\times \) and by \( (\tau_*, n) \) to

\[ (\tau_*(\ell)\theta_*(a), \ell^n a) : \ell \in L^\times, a \in k^\times \subseteq U(k). \]

Proof. The true case is immediate from the definitions, so assume that we are in the fake case. We have an exact sequence

\[ 0 \to \mathbb{G}_m \to \mathbb{G}_m^\Delta \times \mathbb{G}_m \xrightarrow{j} \overline{\mathbb{G}_m} \to 0 \]

with maps induced by \( \ell \mapsto (\ell, \ell^{-n}) \) and \( (\ell, a) \mapsto \ell a^{1/n} \) (the \( n \)th root is well-defined modulo \( \mu_n \)). Taking cohomology shows that \( j \) induces a surjection \( L^\times \times k^\times \to \overline{\mathbb{G}_m}(k) \). Following \( j \) by \( \overline{\mathbb{G}_m} \) yields \( (\ell, a) \mapsto \ell^n a \), whose image on \( k \)-points is \( L^\times k^\times \). Following \( j \) by \( \overline{\mathbb{G}_m} \) yields \( (\ell, a) \mapsto (\tau_*(\ell)\theta_*(a), \ell^n a) \), whose image on \( k \)-points is \( V \). \( \square \)

Remark A.8. The definition of \( j \) in the proof of Lemma A.7(b) shows that in (41), it suffices to let \( a \) run over a set of representatives of \( k^\times/k^\times n \).

Define \( V := \text{im} \left( \overline{\mathbb{G}_m}(k) \xrightarrow{(\tau_*, n)} U(k) \right) \), so \( V \) is given by (40) or (41).

Lemma A.9. Suppose that we have a true (respectively, fake) descent setup \( (n, \Delta, \mathbb{Z}) \). Choose \( \beta \) as in Definition 6.2 (respectively, \( \beta \) and \( D \) as in Definition 6.7). Then \( \tau_* (\beta) \) (respectively, \( \tau_* (\beta) - \theta_*(D) \)) is a principal divisor on \( X \times \Delta' \).

Proof. In the true case, the composition

\[ (\mathbb{Z}/n\mathbb{Z})^\Delta \xrightarrow{\tau_*} (\mathbb{Z}/n\mathbb{Z})^\Delta \xrightarrow{\alpha^\vee} \widehat{J} [\phi] \subseteq \text{Pic } X_s \]

is 0 by (34), and it sends a basis element \( P' \) to the class of the divisor \( \tau_* (\beta)|_{X \times \{P'\}} \).

In the fake case, we use the following diagram:

\[
\begin{array}{ccc}
\mathbb{Z}^\Delta & \xrightarrow{\tau_*} & (\mathbb{Z}/n\mathbb{Z})^\Delta \\
\downarrow \quad \downarrow & & \downarrow \quad \downarrow \\
\langle (nP, 1) : P \in \Delta \rangle & \xrightarrow{(\beta, -D)} & \text{Pic } X_s \\
\end{array}
\]

(42)
Here the middle vertical map sends $\sum P\bar{a}_P$ (where $a_P \in \mathbb{Z}$ reduces to $a_P \in \mathbb{Z}/n\mathbb{Z}$) to $(\sum_P a_P \bar{P}, \sum_P a_P \bar{P})/n$. The map $(\beta, -D)$ sends $(\sum a_P \bar{P}, b)$ to the class of $\sum a_P \beta_P - bD$, so $(nP, 1)$ goes to the class of $nP - D$, which is trivial by the definitions of $\beta$ and $D$. Both paths from $\mathbb{Z}^{\Delta'}$ to $(\sum P \bar{a}_P)_{\mathbb{Z}^{\Delta}}$ send a basis element $P'$ to $\sum_P \tau_{P', P} P, \sum_P \tau_{P', P}$, which is the desired result.

Problem. If $\phi_{*}(\beta) = \beta$ is the coefficient of $\bar{P}$, then the composition along the top row is zero, which is the desired result.

Lemma A.9 shows that there is a function $r = (r_{P'})_{P' \in \mathcal{D}} \in k(X \times \Delta')^\times$ such that

$$\text{div}(r) = \begin{cases} \tau_{*}(\beta), & \text{in the true case,} \\
\tau_{*}(\beta) - \theta_{*}(D), & \text{in the fake case.} \end{cases}$$

Recall from Definitions 6.2 and 6.7 the function $f \in k(X \times \Delta)$ satisfying

$$\text{div}(f) = \begin{cases} n\beta, & \text{in the true case,} \\
n\beta - D & \text{in the fake case.} \end{cases}$$

Lemma A.10. We have $\tau_{*}(f) \equiv r^n \pmod{(L')^\times}$. If $y \in \mathcal{Y}^0(X^\text{good})$, then $\tau_{*}([y, \beta]) = [y, \div(r)]$.

Proof. Since $\text{div}(\tau_{*}(f)) = n\tau_{*}(\beta) = \text{div}(r^n)$, the congruence holds. In the true case,

$$\tau_{*}([y, \beta]) = [y, \tau_{*}(\beta)] = [y, \div(r)] = r(y) \in \mathbb{G}_m(k_s).$$

In the fake case, define $[y, \beta]_D$ using $H$ and $h$ as in (9); then

$$\tau_{*}([y, \beta]_D) = \frac{[y, \tau_{*}(\beta - \tau_{*}H)]}{\tau_{*}(\tau_{*}(h)(y))} = \frac{[y, \tau_{*}(\beta) - \theta_{*}(nH)]}{\theta_{*}(h)(y)} = \frac{[y, \div(r \cdot \theta_{*}(h))] - r(y)}{\theta_{*}(h)(y)} = r(y).$$

In the following diagram with exact rows, the first, second, and fourth rows are as in (5) or (11), except that the first is a pushout by $J[n] \rightarrow A[\phi]$. The third and fourth rows are the same as in $\sum \alpha$. The two maps from $\mathbb{Z}^0 \times \mathcal{Y}^0$ to $U$ coincide by Lemma A.10. Thus the diagram below commutes:

\begin{align*}
\begin{array}{ccccccccc}
0 & \rightarrow & A[\phi] & \rightarrow & A & \rightarrow & J & \rightarrow & 0 \\
0 & \rightarrow & \bar{J}[n] & \rightarrow & \mathbb{Z}^0 \times \mathcal{Y}^0 & \rightarrow & \mathbb{Z}^0 & \rightarrow & 0 \\
0 & \rightarrow & A[\phi] & \rightarrow & \mathbb{G}_m^{\Delta} & \rightarrow & U & \rightarrow & 0 \\
0 & \rightarrow & E^{\nabla} & \rightarrow & \mathbb{G}_m^{\Delta} & \rightarrow & \mathbb{G}_m^{\Delta} & \rightarrow & 0 \\
\end{array}
\end{align*}

(43)
Applying cohomology to the first, third and fourth rows and using Lemma A.7(b), we obtain the following diagram with exact rows:

\[
\begin{array}{ccc}
0 & \xrightarrow{J(k)} & J(k) \\
\phi(A(k)) & \xrightarrow{\gamma} & H^1(k, A[\phi]) \\
\mathbb{Z}^0(X_{\text{good}}^k) & \xrightarrow{(r,f)} & \mathbb{Z}^0(X_{\text{good}}^k) \\
0 & \xrightarrow{U(k)} & H^1(k, A[\phi]) \\
\mathbb{Z}^0(X_{\text{good}}^k) & \xrightarrow{pr'_2} & H^1(k, A[\phi]) \\
0 & \xrightarrow{L^\times_{k}} & H^1(k, E^\vee) \\
\end{array}
\]

(44)

We write \( H := \frac{U(k)}{V} \) and \( \rho_v : H \rightarrow H_v \), where \( H_v \) is the local analogue of \( H \).

**Lemma A.11.** \( \varPi^1(k, \mathbb{G}_m^\Delta) = 0 \).

**Proof.** In the true case, \( H^1(k, \mathbb{G}_m^\Delta) = 0 \) (see the end of Section 3). In the fake case, taking cohomology of

\[
0 \rightarrow \mu_n \rightarrow \mathbb{G}_m^\Delta \rightarrow \mathbb{G}_m^\Delta \rightarrow 0
\]

yields an injection \( H^1(k, \mathbb{G}_m^\Delta) \hookrightarrow H^2(k, \mu_n) \), which restricts to an injection \( \varPi^1(k, \mathbb{G}_m^\Delta) \hookrightarrow \varPi^2(k, \mu_n) \). But \( \varPi^2(k, \mu_n) = 0 \) by the local-global property for the Brauer group.

**Proposition A.12.** Assume Hypothesis 10.1. Then the injection \( H \hookrightarrow H^1(k, A[\phi]) \) in the third row of (44) identifies

\[
\{ h \in H : \rho_v(h) \in (r, f)(\mathbb{Z}^0(X_{k_v}^\text{good})) \text{ for all places } v \}
\]

with \( \text{Sel}^\phi(J) \).

**Proof.** Hypothesis 10.1 shows that the image of \( J(k_v)/\phi(A(k_v)) \) in \( H^1(k_v, A[\phi]) \) equals the image of \( \mathbb{Z}^0(X_{k_v}^\text{good}) \), which in (44) for \( k_v \) maps to 0 in \( H^1(k_v, \mathbb{G}_m^\Delta) \). Thus the image of \( \text{Sel}^\phi(J) \subseteq H^1(k, A[\phi]) \) in \( H^1(k, \mathbb{G}_m^\Delta) \) lies in \( \varPi^1(k_v, \mathbb{G}_m^\Delta) \), which is 0 by Lemma A.11, so \( \text{Sel}^\phi(J) \subseteq H \) by (44). For \( h \in H \), the element \( \rho_v(h) \) is in the image of \( J(k_v)/\phi(A(k_v)) \) (or \( \mathbb{Z}^0(X_{k_v}^\text{good}) \) as above) if and only if it is in the image of \( (r, f)(\mathbb{Z}^0(X_{k_v}^\text{good})) \), by (44).

We now describe the fibers of the map \( pr'_2 \) in (44). This will help us obtain a computable description of \( \text{Sel}^\phi(J) \): see Proposition A.15 below.

Recall the exact sequence (cf. Remark A.4)

\[
0 \rightarrow A[\phi] \rightarrow E^\vee \xrightarrow{\tau_*} \mu_n^{\Delta'} \xrightarrow{q'} Q \rightarrow 0.
\]

**Lemma A.13.** Let \( \ell \in L^\times \) and let \( \xi \) be its image in \( H^1(k, E^\vee) \).

(a) If \( \xi \) lifts to \( H^1(k, A[\phi]) \), then \( \tau_* (\ell) \) is an \( n \)th power in \( L' \).
(b) Conversely, suppose that \( \tau_*(\ell) \) is an \( n \)th power in \( L' \), say \( \tau_*(\ell) = u^n \). Let \( \lambda \in L_s^\times \) be such that \( \lambda^n = \ell \). Then:

1. The element \( w := q'(\tau_*(\lambda)/u) \in Q \) is \( G \)-invariant,
2. Let \( Z := \{ \zeta \in \mu_n(L') : q'(\zeta) = w \} \). Then \( (\zeta, u, \ell) \in U(k) \) if and only if \( \zeta \in Z \).
3. The set of elements of \( H^1(k, A[\phi]) \) mapping to \( \xi \) is the image of \( \{ (\zeta, u, \ell) : \zeta \in Z \} \) under \( U(k) \rightarrow H^1(k, A[\phi]) \).
4. Two such pairs \( (\zeta u, \ell) \) and \( (\zeta' u, \ell) \) have the same image in \( H^1(k, A[\phi]) \) if and only if \( \zeta'/\zeta \in \tau_*(E^\vee(k)) \).

(c) In particular, if \( \mu_n(L') \) surjects onto \( Q(k) \), then \( \xi \) lifts to \( H^1(k, A[\phi]) \) if and only if \( \tau_*(\ell) \) is an \( n \)th power in \( L' \).

\textbf{Proof.} In \((39)\), the image of \( pr_2^{-1}(\ell) \) under \( U(k) \rightarrow H^1(k, A[\phi]) \) equals the set \( \alpha^{-1}(\xi) \) of lifts of \( \xi \).

(a) If \( \xi \) lifts, then there is a pair \( (u, \ell) \in U(k) \). By Lemma A.5, \( \tau_*(\ell) = u^n \).
(b) 1. Note that \( \tau_*(\lambda)/u \in \mu_n \), since

\[
\left( \frac{\tau_*(\lambda)}{u} \right)^n = \frac{\tau_*(\lambda^n)}{u^n} = \frac{\tau_*(\ell)}{u^n} = 1.
\]

For \( \sigma \in G \),

\[
\frac{\sigma w}{w} = \frac{\sigma q'(\tau_*(\lambda)/u)}{q'(\tau_*(\lambda)/u)} = q'\left( \frac{\sigma \tau_*(\lambda)}{\tau_*(\lambda)} \right) = q'\left( \frac{\tau_*(\lambda)}{\lambda} \right) = 1,
\]

since \( q' \circ \tau_* \) is trivial and \( u \) is \( G \)-invariant.
2. By part (a), the elements of \( pr_2^{-1}(\ell) \subset U(k) \) have the form \( (\zeta u, \ell) \) with suitable \( \zeta \in \mu_n(L') \). By definition of \( U \), the condition on \( \zeta \) is that there exists \( \tilde{\lambda} \in L_s^\times \) such that \( \tau_*(\tilde{\lambda}) = \zeta u \) and \( \tilde{\lambda}^n = \ell \). Equivalently, writing \( \tilde{\lambda} = \tilde{\zeta} \lambda \), there exists \( \tilde{\zeta} \in \mu_n(L_s) \) such that \( \tau_*(\tilde{\zeta}) = \zeta u/\tau_*(\lambda) \). By \((45)\), \( \tau_*(\mu_n(L_s)) = \ker(q') \), so this in turn is equivalent to \( q'(\zeta) = q'(\tau_*(\lambda)/u) = w \).
3. This follows from 2. and the first sentence of this proof.
4. In \((39)\), the intersection of \( \ker \cdot \cdot \cdot \) with the kernel of \( U(k) \rightarrow H^1(k, A[\phi]) \) is \( (\tau_*, n)(E^\vee(k)) = \tau_*(E^\vee(k)) \times \{1\} \).

(c) This follows from part (b). \( \square \)

\textbf{Remark A.14.} We can compute \( w \in Q(k) \) by working over a finite field. Let \( v \) be a finite place of \( k \) such that the characteristic of its residue field \( \mathbb{F}_v \) does not divide \( n \) and such that \( \ell \) is a unit at \( v \). The formula in Lemma A.13(b)1., applied over \( \mathbb{F}_v \) to the mod \( v \) reductions of \( \ell \) and \( u \), computes an element of \( Q(\mathbb{F}_v) \) that is the image in \( Q(\mathbb{F}_v) \) of the desired \( w \). Since the reduction map \( Q(k) \rightarrow Q(\mathbb{F}_v) \) is injective, we can recover \( w \) in \( Q(k) \).

Proposition A.12 involves an infinite group \( H \). Imposing the condition that elements are unramified at all places outside a finite set \( S \) lets us replace \( H \) by a finite subgroup \( H_S \), this will reduce the determination of \( \text{Sel}^\phi(J) \) to a finite computation. Let \( H^1(k, A[\phi])_S \) be the group of classes unramified outside \( S \), as in Section 7.1.

\textbf{Proposition A.15.} Assume Hypothesis 10.1. Let \( S \) be a finite set of places of \( k \) containing the set of places in Proposition 9.2 and the places at which \( E^\vee \) is ramified. Let \( H_S \) be the preimage in \( H = U(k)/V \) of \( L(\pi, S) \subset L^\times/L^\times \) under the map \( pr'_2 \) in \((44)\). Then
the injection \( H \hookrightarrow H^1(k, A[\phi]) \) in the third row of (44) identifies the subgroup \( H_S \) with \( H^1(k, A[\phi])_S \cap \text{im}(H \to H^1(k, A[\phi])) \), and identifies

\[
\{ h \in H_S : \rho_v(h) \in (r, f)(\mathcal{Z}^0(X_{k_v}^{\text{good}})) \text{ for all } v \in S \}
\]

with \( \text{Sel}^\phi(J) \).

**Proof.** Let \( v \notin S \) be a place of \( k \). Since \( E^\vee \) is unramified at \( v \), we have \( E^\vee(k_{v,u}) = E^\vee(k_s) \), so the first map in

\[
E^\vee(k_{v,u}) \to R^\vee(k_{v,u}) \to H^1(k_{v,u}, A[\phi]) \xrightarrow{\alpha} H^1(k_{v,u}, E^\vee)
\]

is surjective. This shows that for \( \xi \in H^1(k, A[\phi]) \), \( \xi \) is unramified outside \( S \) if and only if \( \alpha(\xi) \) is unramified outside \( S \). On the other hand, Proposition 7.2 shows that \( H_S \) equals the set of \( h \in H \) whose image \( \text{pr}_2(h) \) in \( L^x/L^{x \times k^x} \) is unramified outside \( S \). By (44), the previous two sentences yield the first identification. Combining this with Proposition 9.2(a) and the last sentence of the proof of Proposition A.12 yields the second identification. \( \square \)

We now sketch an algorithm for computing \( \text{Sel}^\phi(J) \), using the explicit description given in Proposition A.15. First compute \( \widehat{L(n, S)} \). Lemma A.13 lets us compute its inverse image \( H_S \) under the map \( \text{pr}_2 \) in (44). To perform the computations required by Lemma A.13, we need to be able to evaluate \( \tau_* : L^x \to L'^x \) and extract \( n^\text{th} \) roots in \( L' \); the remaining computations use only finite Galois modules like \( E^\vee, \mu_n', \) or \( Q \), so they are not difficult.

Similarly, for each \( v \in S \), first compute \( L^x_v/L^{x \times k_v^x} \), and use Lemma A.13 (over \( k_v \)) to obtain a description of \( H_v \). The map \( H_S \to H_v \) is induced by the inclusion \( U(k) \hookrightarrow U(k_v) \), so it too is easily described. Next, assuming that we can evaluate \( r \) and \( f \) on \( \mathcal{Z}^0(X_{k_v}^{\text{good}}) \), we can determine the image of \( J(k_v) \) in \( H_v \). Using all this, the second identification in Proposition A.15 lets us compute \( \text{Sel}^\phi(J) \).

We summarize this discussion as follows.

**Theorem A.16.** Given a true or fake descent setup with associated isogeny \( \phi : A \to J \), we can compute the Selmer group \( \text{Sel}^\phi(J) \) if we can do the following:

- **Compute in the algebras** \( L \) and \( L' \) and their completions (this includes the ability to take \( n^\text{th} \) roots).
- **Determine a set** \( S \) of places of \( k \) as in Proposition A.15.
- **Compute** \( k(n, S) \) and \( L(n, S) \).
- **Evaluate** \( \tau_* \) on \( L^x \) and \( L^x_v \) for \( v \in S \), and on finite residue fields.
- **Evaluate** \( f \) and \( r \) on \( \mathcal{Z}^0(X_{k_v}^{\text{good}}) \) for \( v \in S \).

**Example A.17.** Consider the case of 2-descent on Jacobians of non-hyperelliptic genus-3 curves \( X \), as in Section 12. For generic \( X \), the smallest usable set \( \Delta' \) is the set of syzygetic quadruples, which has size 315. We have not had the need to implement the approach of this appendix on such examples, but it is likely that this could be done if required.
A.3. Determining the Selmer group in special situations. In some cases, the computation of \( \text{Sel}^\phi(J) \) as described in Section A.2 can be simplified. In particular, in the following proposition, the set \( S \) is potentially smaller than that required in Proposition A.15.

**Proposition A.18.** In the situation of Section A.2, let \( S \) be a set of places of \( k \) containing the set of places in Proposition 9.2. Assume that the map \( E^\nu(k') \rightarrow R^\nu(k') \) is surjective for all field extensions \( k' \) of \( k \) and that the map \( q' : \mu_n(L') \rightarrow Q(k) \) is surjective. Then

\[
\text{Sel}^\phi(J) \simeq \{ \delta = [\ell] \in \widehat{L(n,S)} : \tau_*(\ell) \in L'^{\times n} \text{ and } \delta_v \in \text{im} C_v \text{ for all } v \in S \}.
\]

**Proof.** Since \( E^\nu(k) \rightarrow R^\nu(k) \) is surjective, the map \( H^1(k,A[\phi]) \xrightarrow{\alpha} H^1(k,E^\nu) \) is injective. So the map \( \text{pr}_2 \) in (44) identifies \( H \) with a subgroup of \( L^\times/L_v^\times k_v^\times \), and similarly identifies \( H_v \) with a subgroup of \( L_v^\times/L_v^\times k_v^\times \), for each \( v \). Also \( E^\nu(k_{v,u}) \rightarrow R^\nu(k_{v,u}) \) is surjective for each \( v \), so the proof of Proposition A.15 shows that \( H_S \) is the subgroup of elements of \( H \) unramified outside \( S \). Since \( \mu_n(L') \rightarrow Q(k) \) is surjective, Lemma A.13(c) yields

\[
(47) \quad H_S \simeq \{ [\ell] \in \widehat{L(n,S)} : \tau_*(\ell) \in L'^{\times n} \}.
\]

In (44), \( C_v = \text{pr}_2 \circ (r,f) \), so \( (r,f)(Z_0(X_{k_v}^{\text{good}})) = \text{im} C_v \). Substituting this and (47) into (46) completes the proof. \( \square \)

**Remark A.19.** In contrast with Theorem A.16, Proposition A.18 lets us determine \( \text{Sel}^\phi(J) \) without evaluating \( \tau_* \) on \( L_v \) and without evaluating (or even constructing) \( r \).

**Remark A.20.** The surjectivity assumptions in Proposition A.18 can be checked by a finite computation. This is clear for the statements over \( k \), since they involve only the \( k \)-points of some finite Galois modules. To check surjectivity of \( E^\nu(k') \rightarrow R^\nu(k') \) for all extension fields \( k' \) of \( k \), let \( \Gamma \) be the (finite) Galois group over \( k \) of the splitting field of \( E^\nu \); then the action of \( G_v \) on \( E^\nu \) (and therefore also \( R^\nu \)) factors through a subgroup \( \Gamma' \leq \Gamma \). The surjectivity of \( E^\nu(k') \rightarrow R^\nu(k') \) is determined by \( \Gamma' \), so it suffices to check it for each \( \Gamma' \); in fact, we need only consider one \( \Gamma' \) in each conjugacy class of subgroups.

**Remark A.21.** Suppose that \( n \) is prime, and that the surjectivity assumptions in Proposition A.18 hold. Then \( \text{III}^1(k,R^\nu) = 0 \) by Remark A.4, and \( W_v = 0 \) for all \( v \) by Lemma 10.5(b), and \( K = 0 \) by its second definition (preceding (22)). So by Lemma 10.17(b) and Corollary 10.16, we actually have

\[
\text{Sel}^\phi(J) \simeq \text{Sel}^\phi_{\text{true/fake}}(J).
\]

The advantage of computing \( \text{Sel}^\phi(J) \) using Proposition A.18 instead of computing \( \text{Sel}^\phi_{\text{true/fake}}(J) \) using Theorem 10.9(b) is that the former requires local computations at only the places in \( S \) instead of the places in the potentially much larger set \( T \) of Theorem 10.9(b). This improvement is possible because of the additional condition \( \tau_*(\ell) \in L'^{\times n} \): Proposition A.18 says that \( \text{Sel}^\phi(J) \simeq S_S \cap \{ [\ell] \in \widehat{L(n,S)} : \tau_*(\ell) \in L'^{\times n} \} \), which by Lemma A.13(c) equals \( S_S \cap \alpha(H^1(k,A[\phi])) \) under the assumptions made. In other words, enlarging \( S \) to a \( T \) large enough that \( S_T = \text{Sel}^\phi_{\text{true/fake}}(J) \) has the effect of intersecting \( S_S \) with \( \alpha(H^1(k,A[\phi])) \).

**Example A.22.** We consider 3-descent on an elliptic curve \( J \), as in [SS04]. Let \( \Delta = J[3] - \{0\} \), and let \( \beta \) be the graph of the map \( \Delta \rightarrow \text{Div}^0 J_\delta \) sending \( P \) to \( (P) - (O) \). This defines a true descent setup, for which \( A[\phi] = J[3] \) and \( L \) is an étale algebra of degree 8. Fix a Weierstrass
equation for \( J \); then let \( \Delta' \) be the set of eight lines in \( \mathbb{P}^2 \) passing through three of the points in \( \Delta \), together with the four vertical lines passing through two of them and the origin of \( J \). Let the correspondence \( \tau \) be given by incidence. A finite computation as in Remark A.20 shows that the maps \( \mu_3(L') \to Q(k) \) and \( \mu_3(L) \to \overline{R}(k) \) are surjective over any field. So Proposition A.18 gives us a way to determine \( \text{Sel}^3(J) \), if we can compute \( L(3, S) \).

The approach described here and in Section A.2 has advantages and disadvantages compared to computing \( \text{Sel}_{\text{true/fake}}^a(J) \) as in Section 11. One obvious advantage is that it computes the Selmer group directly. Also, as in Remark A.21, it requires local computations at only the places in \( S \) instead of the places in a potentially much larger set \( T \). So whenever this direct approach is feasible (as in the example above), one should use it.

On the other hand, the direct approach requires not only information on \( (S-)\text{-class} \) and unit groups of \( L \), but also a presentation of \( L' \), the map \( \tau_*: L^\times \to L'^\times \), and possibly the function \( r \), which is defined over \( L' \).

### A.4. Passing from a true or fake Selmer group to the actual Selmer group.

Recall the exact sequence

\[
0 \to \ker \kappa \to \text{Sel}^a(J) \to \text{Sel}_{\text{true/fake}}^a(J) \cap \alpha(H^1(k, A[\phi])) \to \text{coker} \kappa.
\]

from Theorem 10.14. Assuming that we have computed \( \text{Sel}_{\text{true/fake}}^a(J) \), we can determine the order of \( \text{Sel}^a(J) \) if we can

- find the order of \( \ker \kappa \);
- for any given \( \xi \in \text{Sel}_{\text{true/fake}}^a(J) \) check if \( \xi \in \alpha(H^1(k, A[\phi])) \);
- and if so, find its image in \( \text{coker} \kappa \).

In this subsection, we will explain why this seems no easier than computing \( \text{Sel}^a(J) \) directly using the approach of Section A.2.

Lemma A.13 implies the following.

**Corollary A.23.** If we can evaluate the map \( \tau_* \) explicitly on \( L^\times \) and if we can extract \( n^{th} \) roots in \( L' \), then we can determine whether any given element in the image of \( L^\times \) in \( H^1(k, E^\nu) \) lies in \( \alpha(H^1(k, A[\phi])) \).

This takes care of the second point in the list above.

For the other two points, we need to find the groups \( W_v \) and the map \( \kappa: K \to \prod_v W_v \).

The group \( K = R^\nu(k)/q E^\nu(k) \) can be found by a finite computation, using the inclusion \( R^\nu(k) \hookrightarrow \mu_n(L') \) arising from (36) to represent elements of \( R^\nu(k) \). For the finitely many \( v \) for which the proof of Corollary 10.6 does not guarantee \( W_v = 0 \), we use the following to compute \( W_v \):

**Lemma A.24.** Fix \( v \).

(a) The map

\[
\ker C_v \xrightarrow{\gamma_v} \ker \alpha_v \simeq R^\nu(k_v)/q E^\nu(k_v)
\]

can be described explicitly as follows. Given \( [z] \in \ker C_v \subseteq J(k_v)/\phi A(k_v) \), represented by some \( z \in T_0(X_k^{\text{good}}) \), the image \( \gamma_v([z]) \) is represented by \( \zeta \in R^\nu(k_v) \subseteq \mu_n(L'_v) \) defined as follows:

In the true case, \( f(z_0) = \ell^n \) for some \( \ell \in L^\times_v \); set \( \zeta := r(z)/\tau_*(\ell) \).

In the fake case, \( f(z_0) = \ell^n a \) for some \( \ell \in L^\times_v \) and \( a \in k_v^\times \); set \( \zeta := r(z)/(\tau_*(\ell)\theta_*(a)) \).
(b) Assume Hypothesis 11.1. If we know \( \#(J(k_v)/\phi A(k_v)) \) and we can compute the functions \( f \) and \( r \) on \( Z^0(X_{k_v}^{\text{good}}) \) and \( \tau_* \) on \( L_v^\times \), then we can compute \( W_v \) in the course of the computation of \( \text{im} C_v \) as in Remark 11.6 as follows:

1. Search for points on \( X \) over finite extensions of \( k_v \) until a 0-cycle \( x_0 \) of degree 1 on \( X_{k_v} \) is found.

2. Randomly generate elements \( z := \text{tr}_{K/k_v}(x) - dx_0 \in Z^0(X_{k_v}^{\text{good}}) \) as in Remark 11.6, let \( J \) be the subgroup of \( J(k_v)/\phi A(k_v) \) they generate so far, compute \( I := C_v(J) \subseteq L_v^\times /L_v^\times k_v^\times \), and compute \( G := \gamma_v(\ker(C_v|J)) \subseteq R^\times(k_v)/qE^\times(k_v) \), until \( \#I \cdot \#G = \#(J(k_v)/\phi A(k_v)) \).

3. When equality occurs, \( I = \text{im} C_v \) and \( W_v \simeq (R^\times(k_v)/qE^\times(k_v))/G \).

**Proof.**

(a) In the true case, \( C_v([z]) = 0 \) means that \( f(z) = \ell^u \) for some \( \ell \in L_v^\times \). Let \( V_v \) be the local analogue of \( V \). Dividing \( (r(z), f(z)) \in U(k_v) \) by \( (\tau_*(\ell), \ell^u) \in V_v \) (cf. Lemma A.7) yields \( (\zeta, 1) \in U(k_v) \), so Corollary A.6 implies \( \zeta \in \mu_n(L') \). In the fake case, divide instead by \( (\tau_*(\ell)\theta_\ell(a), \ell^u a) \in V_v \). Lemma A.13(b)2. applied with \( \ell = 1, u = 1, \lambda = 1 \), and hence \( w = 1 \), yields \( \zeta \in \ker(q_{|[V_n(V')]}) = R^\times(k_v) \) (see (36)).

(b) We have \( \#I \cdot \#G = \#J \leq \#(J(k_v)/\phi A(k_v)) \) with equality if and only if \( J = J(k_v)/\phi A(k_v) \). When equality occurs, \( I = \text{im} C_v \) and \( G = \gamma_v(\ker C_v) \), and Definition 10.3(i) yields \( W_v \simeq (R^\times(k_v)/qE^\times(k_v))/G \). □

**Remark A.25.** By computing \( \#J = \#I \cdot \#G \) as the algorithm in Lemma A.24(b) progresses, we can detect when \( J = J(k_v)/\phi A(k_v) \). This stopping rule can help make our computation more efficient.

Once we know \( W_v \) as a quotient of \( R^\times(k_v) \) for all \( v \) for which \( W_v \) might be nonzero, the map \( \kappa: K \to \prod_v W_v \), with \( K = R^\times(k)/qE^\times(k) \), is induced by the maps \( R^\times(k) \to R^\times(k_v) \) and hence is computable. In particular, we can find the size of \( \ker \kappa \), which takes care of the first point in our list.

The following lemma deals with the last point.

**Lemma A.26.** Under the assumptions in Corollary A.23 and Lemma A.24(b), given an element \( \xi \in \text{Sel}_{\text{true/fake}}(J) \cap \alpha(H^1(k, A[\phi])) \), represented by some explicit \( \ell \in L^\times \), we can find the image of \( \xi \) in \( \text{coker} \kappa \).

**Proof.** Use Lemma A.24 (and the sentence preceding it) to compute \( W_v \) for all \( v \). Compute \( \kappa \) as in the sentences preceding Lemma A.26. Our task is to compute the image of \( \xi \) under the snake map implied by (23). To do this, we do a parallel diagram chase in the more computation-friendly diagram

\[
\begin{array}{ccccccc}
0 & \longrightarrow & R^\times(k) & \longrightarrow & U(k) & \overset{\text{pr}_2}{\longrightarrow} & L^\times \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_v R^\times(k_v) & \longrightarrow & \prod_v U(k_v) & \overset{\text{pr}_2}{\longrightarrow} & \prod_v L^\times
\end{array}
\]

(48)

(with exact rows from (39)), which maps to (23).

55.
Use Lemma A.13 to compute $u$ such that $(u, \ell) \in U(k)$, i.e., such that $\tau_*(\ell) = u^n$. For the places $v$ for which $W_v = 0$, set $\zeta_v := 1 \in R^\ell(k_v)$. For the finitely many remaining $v$, we have $\xi_v = C_v([z_v])$ for some $z_v \in Z^0(X^\text{good}_v)$ found during the local image computation; then $f(z_v) \equiv \ell$ in $L^\times_v/L^\times_v k_v^\times$. Dividing $(u, \ell) \in U(k_v)$ by $(r(z_v), f(z_v))$ and then by an element of $V_v$ as in Lemma A.7 yields an element $(\zeta_v, 1) \in U(k_v)$ with the same image as $(u, \ell)$ in the group $H^1(k_v, A[\phi]) / \text{im} \gamma_v$ in the corresponding position of (23). By exactness of the second row of (48), we have $\zeta_v \in R^\ell(k_v)$. Then $(\zeta_v) \in \prod R^\ell(k_v)$ maps to an element of $\prod W_v$ in (23), which represents the image of $\xi$ in $\text{coker} \kappa$. □

We conclude that in order to find (the order of) $\text{Sel}^\phi(J)$ from $\text{Sel}^\alpha_{\text{true/fake}}(J)$, we need to be able to lift a given $\ell \in L^\times$ to $(u, \ell) \in U(k)$ (or show that such a lift does not exist), and to evaluate $r$ and $\tau_*$ locally at the places with potentially nontrivial $W_v$. But if we can do all this, then we can also compute $\text{Sel}^\phi(J)$ directly as described in Theorem A.16.

Acknowledgments

Our research project was begun at the Mathematical Sciences Research Institute in 2006, and continued over several years at several institutions: Banff International Research Station, Institute for Computational and Experimental Research in Mathematics, Jacobs University, Massachusetts Institute for Technology, Mathematisches Forschungsinstitut Oberwolfach, Pacific Institute for the Mathematical Sciences, and Universit"at Bayreuth. We thank them all for their hospitality. We thank also David Kohel and Christophe Ritzenthaler for comments on discriminants of ternary quartic forms, Benedict Gross and Jack Thorne for the content of Remark 1.2, and Edward Schaefer for suggestions of references.

References


[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)


[Sta73] Richard P. Stauduhar, The determination of Galois groups, Math. Comp. 27 (1973), 981–996. MR0327712 (48 #6054)


DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BC V5A 1S6, CANADA

E-mail address: nbruin@sfu.ca

URL: http://www.cecm.sfu.ca/~nbruin/

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/

MATHEMATHISCHES INSTITUT, UNIVERSITÄT BAYREUTH, 95440 BAYREUTH, GERMANY

E-mail address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/