Forum of Mathematics, Sigma (2016), Vol. 4, e6, 80 pages
doi:10.1017/fms.2016.1

GENERALIZED EXPLICIT DESCENT AND ITS APPLICATION TO CURVES OF GENUS 3

NILS BRUIN[1], BJORN POONEN[2] and MICHAEL STOLL[3]

[1] Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada;
email: nbruin@sfu.ca

[2] Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA;
email: poonen@math.mit.edu

[3] Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany;
email: Michael.Stoll@uni-bayreuth.de

Received 9 May 2015; accepted 8 January 2016

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.

2010 Mathematics Subject Classification: 11G30 (primary); 11G10, 14G25, 14H45 (secondary)

1. Introduction

1.1. Background. The Mordell–Weil theorem [23, 42] 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 $n \geqslant 2$. And there is essentially only one known proof of this finiteness, based on a vast generalization of Fermat's method of infinite descent.

© The Author(s) 2016. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

In modern terms, the proof embeds $J(k)/nJ(k)$ into a Selmer group $\mathrm{Sel}^n(J)$, 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 a $\mathcal{G}$-module, and the Kummer sequence yields $H^1(k, J[2]) \simeq k^\times/k^{\times 2} \times k^\times/k^{\times 2}$.

However, in many higher-dimensional situations, 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 μ_n, since cohomology of induced modules can be computed by Shapiro's lemma [1, Section 4, Proposition 2]. For example, if J is the Jacobian of a hyperelliptic curve $y^2 = f(x)$ with $\deg f$ odd, and Δ 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

$$0 \longrightarrow \frac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\Delta} \longrightarrow J[2] \longrightarrow 0$$

in which $(\mathbb{Z}/2\mathbb{Z})^\Delta$ is a direct sum of induced modules: this was exploited in [34]. For $y^2 = f(x)$ with $\deg f$ 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 [29]. The situations of the two previous sentences were called true descent and fake descent, respectively, in [29].

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 $\mathcal{G}$-set of odd theta characteristics. We demonstrate its practicality by computing the rank of $J(\mathbb{Q})$ for the Jacobians of several nonhyperelliptic genus 3 curves X, some of which have no special property beyond having a small discriminant; at least one of these curves can be handled unconditionally, without assuming the Generalized Riemann hypothesis (see Section 12.9). 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 $\mathcal{G}$-action on certain torsion points is much smaller than

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\mathrm{Sp}_6(\mathbb{F}_2)$. 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 [4, Section 4]). In particular, our approach eliminates the use of generalized Jacobians and the group scheme $\mathcal{J}_{\mathfrak{m}}$ in [29], 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^θ fixed by an involution θ in a particular canonical $G^{\mathrm{ad}}(k)$-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 (respectively E_7), Thorne's construction yields the universal family of nonhyperelliptic genus 3 curves with a marked hyperflex (respectively, a marked flex that is not a hyperflex). See [41]; the families of genus 3 curves appear explicitly in Theorem 4.8 there. In the E_6 case, $\mathrm{Gal}(k(J[2])/k)$ is generically $W(E_6)$, isomorphic to an index 28 subgroup of the group $\mathrm{Sp}_6(\mathbb{F}_2)$ that arises for a general genus 3 curve. In the E_7 case, $\mathrm{Gal}(k(J[2])/k)$ is generically $W(E_7)/\{\pm 1\}$, isomorphic to the full group $\mathrm{Sp}_6(\mathbb{F}_2)$. It is reasonable to hope that it will eventually be possible to use Thorne's work to study $\mathrm{Sel}^2(J)$ for any nonhyperelliptic genus 3 curve with a rational flex.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\phi\colon A \to J$ over a global field k. Given a true descent setup, which includes an étale k-algebra L, we define a homomorphism

$$\frac{J(k)}{\phi A(k)} \longrightarrow \frac{L^\times}{L^{\times n}} \tag{1}$$

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

$$\frac{J(k)}{\phi A(k)} \longrightarrow H^1(k, A[\phi]) \tag{2}$$

appearing in the definition of the actual ϕ-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 ϕ-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 $L^\times/L^{\times n}$ is replaced by $L^\times/L^{\times n}k^\times$.

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 ϕ-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 ϕ-Selmer group. A more elaborate method that *always* succeeds in calculating the ϕ-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 nonhyperelliptic genus 3 curves, and ends with several examples.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

2. Notation

If S is a set and $n \in \mathbb{Z}_{\geqslant 0}$, 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 $\mathcal{G} = \mathcal{G}_k = \mathrm{Gal}(k_s/k)$. 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 Ω_k be the set of nontrivial places of k. For $v \in \Omega_k$, let k_v be the completion of k at v; moreover, if v is nonarchimedean, 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 $H^n(M)$ or $H^n(k, M)$ or $H^n(\mathcal{G}, M)$ 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 [17, page 141]). Let $\mathscr{O} = \mathscr{O}_X$ 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 $\mathrm{Div}\, X$ (respectively $\mathrm{Div}^0 X$) be the group of divisors (respectively divisors algebraically equivalent to 0) on X over k, let $\mathcal{Z}(X)$ (respectively $\mathcal{Z}^0(X)$) be the group of 0-cycles (respectively 0-cycles of degree 0), and define $\mathrm{Pic}\, X$ as in [17, II. Section 6]; if X is a curve, also define $\mathrm{Pic}^0 X := \ker(\mathrm{Pic}\, X \xrightarrow{\deg} \mathbb{Z})$. Alternatively, if $\mathrm{Princ}\, X$ is the group of principal divisors, then $\mathrm{Pic}\, X = \mathrm{Div}\, X / \mathrm{Princ}\, X$. If $f \in k(X)^\times$ 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

$$f(z) = \prod_P (N_{k(P)/k} f(P))^{n_P} \in k^\times.$$

Let $J := \mathrm{Alb}_X$ be the Albanese variety of X, so J is an abelian variety. Then the Picard variety of X (that is, the reduced subgroup scheme associated to the connected component of the Picard scheme of X/k) may be identified with the dual abelian variety $\widehat{J}$. If X is a curve, then both J and $\widehat{J}$ are the Jacobian $\mathrm{Jac}\, X$. Let $\mathcal{Y}^0(X)$ 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.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

DEFINITION 3.1. Given a $\mathcal{G}$-module M, and a finite $\mathcal{G}$-set Δ, the *twisted power* M^Δ is the $\mathcal{G}$-module of maps from Δ 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 $M^\Delta = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^\Delta, M)$ 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^Δ (at least as a $\mathcal{G}$-module). Similarly, a finite étale k-scheme Δ can be identified with a finite $\mathcal{G}$-set.

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

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

REMARK 3.7. For fixed Δ, the functor $M \mapsto M^\Delta$ is exact.

REMARK 3.8. For a finite $\mathcal{G}$-module M of size not divisible by $\mathrm{char}\, k$, and a finite $\mathcal{G}$-set Δ, we have $(M^\Delta)^\vee \simeq (M^\vee)^\Delta$.

Each finite étale k-scheme Δ is $\mathrm{Spec}\, L$ 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 $\mathrm{char}\, k \nmid n$. Then $\mu_n^\Delta(k_s) = \mu_n(L_s)$. The group $H^1(\mathbb{G}_m^\Delta) = H^1(\mathcal{G}, L_s^\times)$ is trivial by a generalization of Hilbert's theorem 90 [38, page 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 $\mathrm{char}\, k \nmid n$.

4.1. The Albanese–Albanese definition. In this section, we review Lang's construction of the Weil pairing between Albanese varieties. Let V and W be

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

nice k-varieties and let $\mathfrak{D} \in \operatorname{Div}(V \times W)$. The divisor $\mathfrak{D}$ induces partial maps

$$\mathfrak{D}\colon \mathcal{Z}^0(V_s) \to \operatorname{Div}^0 W_s \text{ and } \mathfrak{D}^t\colon \mathcal{Z}^0(W_s) \to \operatorname{Div}^0 V_s.$$

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

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

By [19, III, Theorem 4, Corollary 2], $\mathfrak{D}(\mathcal{Y}^0(V_s)) \subset \operatorname{Princ} W_s$. In particular, if $v \in \mathcal{Z}^0(V_s)$ maps to an n-torsion point $[v] \in \operatorname{Alb}_V[n](k_s)$, then $nv \in \mathcal{Y}^0(V_s)$, and $\mathfrak{D}(nv) = \operatorname{div}(f_{nv})$ for some $f_{nv} \in k_s(W)^\times$. Define $f_{nw} \in k_s(V)^\times$ symmetrically. Define

$$\begin{aligned} e_{\mathfrak{D},n}\colon \operatorname{Alb}_V[n](k_s) \times \operatorname{Alb}_W[n](k_s) &\longrightarrow \mu_n(k_s) \\ [v], [w] &\longmapsto \frac{f_{nw}(v)}{f_{nv}(w)} \end{aligned}$$

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 [19, VI, Section 4] for the proof that $e_{\mathfrak{D},n}$ is well defined, bilinear, and Galois-equivariant.

REMARK 4.1. Let A be an abelian variety, let $\widehat{A}$ be the dual abelian variety, and continue to suppose that $\operatorname{char} k \nmid n$. Take $V = A$ and $W = \widehat{A}$, and let $\mathfrak{D}$ be a Poincaré divisor. Since $\operatorname{Alb}_A = A$ and $\operatorname{Alb}_{\widehat{A}} = \widehat{A}$, we obtain a pairing $e_n\colon A[n] \times \widehat{A}[n] \to \mu_n$. It is nondegenerate (see [19, VI, VII]), so we obtain an identification of $\widehat{A}[n]$ with $A[n]^\vee$.

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

$$\begin{aligned} [\,,\,]\colon \mathcal{Y}^0(X_s) \times \operatorname{Div}^0(X_s) &\longrightarrow k_s^\times \\ y, D &\longmapsto g_{D,z}(y)\mathfrak{P}_0(y, z). \end{aligned}$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

See [31, 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 $[y, \operatorname{div}(g)] = g(y)$ since the choice $z = 0$ yields $g_{D,z} = g$.

Finally, define

$$\begin{aligned} e_{X,n} \colon J[n] \times \widehat{J}[n] &\longrightarrow \mu_n(k_s) \\ ([x], [D]) &\longmapsto \frac{f_{nD}(x)}{[nx, D]}, \end{aligned}$$

where the 0-cycle $x \in \mathcal{Z}^0(X_s)$ represents an element of $J[n](k_s)$, the divisor $D \in \operatorname{Div}^0 X_s$ represents an element of $\widehat{J}[n](k_s)$, the rational function $f_{nD} \in k_s(X)^\times$ has divisor nD, and all these are chosen so that everything is defined.

Let us check that $e_{X,n}$ is well defined, that is, 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 $\operatorname{div}(f)$ to it for some $f \in k_s(X)^\times$, and we have

$$e_{X,n}(x, \operatorname{div}(f)) = \frac{f^n(x)}{[nx, \operatorname{div}(f)]} = \frac{f(x)^n}{f(x)^n} = 1.$$

4.3. Functoriality. Let $\iota \colon X \to X'$ be a morphism of nice varieties. Let $x \in \mathcal{Y}^0(X_s)$ and $D \in \operatorname{Div}^0(X'_s)$. We have $[x, \iota^* D] = [\iota(x), D]$ whenever both sides are defined (take $g_{i^*D, i^*z} = i^* g_{D,z}$ in the definition). It follows that for $[x] \in \operatorname{Alb}_{X_s}[n]$ and $[D] \in (\operatorname{Pic} X'_s)[n]$ we have $e_{X,n}([x], \iota^*[D]) = e_{X',n}([\iota(x)], [D])$.

4.4. Equality of the pairings. Let $J := \operatorname{Alb}_X$. We now have three pairings

$$e_{X,n}, e_{J,n}, e_n \colon J[n] \times \widehat{J}[n] \to \mu_n,$$

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 $X_s \to \operatorname{Alb}_{X_s}$ shows that $e_{X,n} = e_{J,n}$.

Now we prove that $e_{J,n} = e_n$. In the definition of $e_{J,n}$, we use $\mathfrak{P}_0 = \mathfrak{P}$. 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 $D = \mathfrak{P}^t(z') \in \operatorname{Div}^0(J_s)$. By definition, $f_{nz'} = f_{nD}$. Also, for

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

any $y \in \mathcal{Y}^0(J_s)$, we have $[y, D] = \mathfrak{P}(y, z')$ since in the definition we can take $z = z'$ and $g_{D,z} = 1$. Thus

$$e_{J,n}(a, a') = \frac{f_{nD}(z)}{[nz, D]} = \frac{f_{nz'}(z)}{\mathfrak{P}(nz, z')} = \frac{f_{nz'}(z)}{f_{nz}(z')} = e_n(a, a'). \qquad \square$$

5. Odd theta characteristics

Assume $\operatorname{char} k \neq 2$. Let X be a nice curve of genus g over k. Let ω be its canonical bundle, and let $J := \operatorname{Jac} X$.

5.1. Theta characteristics. A *theta characteristic* on X is a line bundle ϑ on X such that $\vartheta^{\otimes 2} \simeq \omega$. A theta characteristic ϑ 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_s form a set $\mathcal{T}$ of size 2^{2g}, and the odd ones form a subset $\mathcal{T}_{\mathrm{odd}}$ of size $2^{g-1}(2^g - 1)$ (cf. [25]).

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 $q\colon V \to \mathbb{F}_2$ 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* $\operatorname{char} k \neq 2$. *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 ϑ,*

$$\begin{aligned} q_\vartheta\colon J[2] &\to \mathbb{F}_2 \\ \mathscr{L} &\mapsto (h^0(\vartheta \otimes \mathscr{L}) + h^0(\vartheta)) \pmod 2 \end{aligned}$$

is a quadratic form associated to e_2.

(b) *The map*

$$\begin{aligned} \mathcal{T} &\longrightarrow \{\text{quadratic forms on } J[2] \text{ associated to } e_2\} \\ \vartheta &\longmapsto q_\vartheta, \end{aligned}$$

is a bijection.

(c) *A theta characteristic ϑ is odd if and only if the Arf invariant of q_ϑ is* 1.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. See [25] and [16, Section 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 $(\operatorname{Pic} X/\langle\omega\rangle)[2]$ (see Corollary 5.3).

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

(i) *If f vanishes everywhere 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 $n \geqslant 4$ 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 $n \geqslant 6$ 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 dimension 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 the equation $f(x + v) - f(x) = 0$; 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

$$f(x + v_1) - f(x) = 0 \quad \text{and} \quad f(x + v_2) - f(x) = 0.$$

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 $g \geqslant 2$ over k.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

COROLLARY 5.3.

(a) *If $g \geqslant 2$, then every class in $J[2] \subset (\operatorname{Pic} X/\langle\omega\rangle)[2]$ has the form $\vartheta_1 + \vartheta_2$ (modulo ω) with $\vartheta_1, \vartheta_2 \in \mathscr{T}_{\mathrm{odd}}$.*

(b) *If $g \geqslant 3$, and $\vartheta_1, \ldots, \vartheta_6 \in \mathscr{T}_{\mathrm{odd}}$ sum to 0 in $(\operatorname{Pic} X/\langle\omega\rangle)[2]$, then there exist $\vartheta_{12}, \vartheta_{34}, \vartheta_{56} \in \mathscr{T}_{\mathrm{odd}}$ such that*

$$\begin{aligned}\vartheta_1 + \vartheta_2 + \vartheta_{34} + \vartheta_{56} &= 0,\\ \vartheta_3 + \vartheta_4 + \vartheta_{12} + \vartheta_{56} &= 0,\\ \vartheta_5 + \vartheta_6 + \vartheta_{12} + \vartheta_{34} &= 0\end{aligned}$$

in $(\operatorname{Pic} X/\langle\omega\rangle)[2]$.

Proof. Fix $\vartheta \in \mathscr{T}_{\mathrm{odd}}$. The elements of $\mathscr{T}$ are $\vartheta + x$ for $x \in J[2]$, and $\vartheta + x$ is odd if and only if $q_\vartheta(x) = 0$, by the definitions of odd and q_ϑ. In other words, there is an identification

$$\begin{aligned}\{\text{zeros of } q_\vartheta \text{ in } J[2]\} &\longrightarrow \mathscr{T}_{\mathrm{odd}}\\ x &\longmapsto \vartheta + x.\end{aligned}$$

Identify $J[2]$ with $\mathbb{F}_2^{2g}$, and q_ϑ with a polynomial f.

(a) Apply Lemma 5.2(iii) with v the class in $J[2]$. Then x corresponds to the desired ϑ_1, and $x + v$ to ϑ_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 ϑ_{56}, $x + v_1$ corresponds to the desired ϑ_{34}, and $x + v_2$ corresponds to the desired ϑ_{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 (Δ, Σ), where Δ is a set and Σ is a collection of subsets of Δ. An *isomorphism* $(\Delta, \Sigma) \to (\Delta', \Sigma')$ is a bijection $\Delta \to \Delta'$ under which Σ and Σ' correspond.

Let Σ be the set of 4-element subsets of $\mathscr{T}_{\mathrm{odd}}$ that sum to 0 in $(\operatorname{Pic} X/\langle\omega\rangle)[2]$.

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

(1) *the $\mathbb{F}_2$-vector space $(\operatorname{Pic} X/\langle\omega\rangle)[2]$ equipped with $\mathscr{T}_{\mathrm{odd}}$ (viewed as a subset);*

(2) *the $\mathbb{F}_2$-vector space $J[2]$ with the Weil pairing e_2;*

(3) *the incidence structure $(\mathscr{T}_{\mathrm{odd}}, \Sigma)$.*

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. The automorphism group of (2) is $\mathrm{Sp}_{2g}(\mathbb{F}_2)$, 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 $(\mathrm{Pic}\, X/\langle\omega\rangle)[2]$ generated by $\vartheta_1 + \vartheta_2$ with $\vartheta_1, \vartheta_2 \in \mathscr{T}_{\mathrm{odd}}$. The subset $\mathscr{T}_{\mathrm{odd}}$ determines the function $h^0 \pmod 2$ on the nontrivial coset $\mathscr{T}$ of $J[2]$ in $(\mathrm{Pic}\, X/\langle\omega\rangle)[2]$. Choose $\vartheta \in \mathscr{T}_{\mathrm{odd}}$; from $h^0 \pmod 2$, 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 $q\colon J[2] \to \mathbb{F}_2$ such that the function $(x, y) \mapsto q(x+y)-q(x)-q(y)$ 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 $\mathscr{T}_{\mathrm{odd}}$ and with one relation saying that the sum of the generators is 0. If $g \geqslant 3$, take the $\mathbb{F}_2$-vector space P with generator set $\mathscr{T}_{\mathrm{odd}}$ and with relations given by the elements of Σ.

To show that the map $\epsilon\colon P \to (\mathrm{Pic}\, X/\langle\omega\rangle)[2]$ sending each basis element to the corresponding ϑ is an isomorphism, it suffices to show that its restriction $\epsilon_0\colon P_0 \to J[2]$ is an isomorphism, where P_0 is the codimension-1 subspace of P spanned by pairs. Corollary 5.3(a) shows that ϵ_0 induces a bijection

$$\binom{\mathscr{T}_{\mathrm{odd}}}{2}\Big/\sim \longrightarrow J[2] - \{0\},$$

where $\{\vartheta_1, \vartheta_2\} \sim \{\vartheta_3, \vartheta_4\}$ means $\sum_{i=1}^{4} \vartheta_i = 0$ in $(\mathrm{Pic}\, X/\langle\omega\rangle)[2]$. In particular, ϵ_0 is surjective. If $g = 2$, then ϵ_0 is injective too, because $\dim P_0 = 4 = \dim J[2]$. To prove injectivity for $g \geqslant 3$, it suffices to prove that every relation $(\vartheta_1 + \vartheta_2) + (\vartheta_3 + \vartheta_4) = (\vartheta_5 + \vartheta_6)$ in $(\mathrm{Pic}\, X/\langle\omega\rangle)[2]$ 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* $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ *on $J[2]$.*

REMARK 5.6. It follows from the connectedness of the moduli space of genus g curves [7] 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 $g \geqslant 2$, we have*

$$\#\Sigma = \frac{2^{g-3}}{3}(2^{2g} - 1)(2^{2g-2} - 1)(2^{g-2} - 1).$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. Since $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ acts transitively on $J[2]-\{0\}$, all fibers of the summing map

$$\binom{\mathscr{T}_{\mathrm{odd}}}{2} \longrightarrow J[2]-\{0\} \subseteq \frac{\mathrm{Pic}\, X}{\langle\omega\rangle}[2]$$

have the same size, namely $\binom{2^{g-1}(2^g-1)}{2}/(2^{2g}-1) = 2^{2g-3}-2^{g-2}$. Hence the number of *pairs* of pairs such that the two pairs have the same image in $J[2]-\{0\}$ is $(2^{2g}-1)\binom{2^{2g-3}-2^{g-2}}{2}$. 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 $\mathscr{T}_{\mathrm{odd}}$ summing to 0 with a partition into two pairs. Each 4-element subset can be partitioned in three ways, so

$$\#\Sigma = \frac{1}{3}(2^{2g}-1)\binom{2^{2g-3}-2^{g-2}}{2} = \frac{2^{g-3}}{3}(2^{2g}-1)(2^{2g-2}-1)(2^{g-2}-1). \qquad \square$$

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

PROPOSITION 5.8. *An odd theta characteristic ϑ on X_s whose class lies in* $(\mathrm{Pic}\, X_s)^{\mathcal{G}}$ *is represented by an element of* $\mathrm{Div}\, X$.

Proof. The k-scheme parametrizing effective divisors whose class equals ϑ 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 $h^0(\vartheta)$ [15, Theorems 5.2.1 and 2.4.3], so the associated Brauer class $\tau \in \mathrm{Br}\, k$ is killed by the odd integer $h^0(\vartheta)$ [15, Proposition 4.5.13(1)]. On the other hand, the Hochschild–Serre spectral sequence yields an exact sequence $\mathrm{Pic}\, X \to (\mathrm{Pic}\, X_s)^{\mathcal{G}} \to \mathrm{Br}\, k$ under which the second map sends ϑ to τ and ω to 0, so $2\tau = 0$. Thus $\tau = 0$. So ϑ comes from an element of $\mathrm{Pic}\, X$, or, equivalently, from an element of $\mathrm{Div}\, X$. $\square$

6. Generalized explicit descent

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

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

EXAMPLE 6.1. Assume $\mathrm{char}\, k \neq 2$. Let $F(x) \in k[x]$ be a nonconstant separable polynomial of odd degree $2g+1$. Let X be the smooth projective model of the

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

curve $y^2 = F(x)$, so X is a hyperelliptic curve of genus g. Let ∞ 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 ∞. Then there is a surjection $(\mathbb{Z}/2\mathbb{Z})^{\Delta} \to \widehat{J}[2]$ sending each basis element $P \in \Delta(k_s)$ to the divisor class $[P - \infty]$ (see [26, 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 β on $X \times \Delta$.

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

REMARK 6.3. Given β, for each $P \in \Delta(k_s)$, we have the fiber $\beta_P \in \operatorname{Div} X_s$. In fact, we may think of β as the family of divisors β_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 $(n, \Delta, \mathscr{L})$, we will define a homomorphism

$$C\colon J(k) \longrightarrow \frac{L^{\times}}{L^{\times n}}$$

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

6.2.1. Cohomological definition. Take cohomology of

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

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

$$C\colon J(k) \longrightarrow H^1(J[n]) \xrightarrow{\alpha} H^1(\mu_n^{\Delta}) \simeq \frac{L^{\times}}{L^{\times n}}. \tag{3}$$

6.2.2. Explicit definition. Choose β and f as in Definition 6.2. Let X^{good} be the largest open subscheme of X such that f is an invertible regular function on $X^{\mathrm{good}} \times \Delta$. Then f defines a morphism $X^{\mathrm{good}} \times \Delta \to \mathbb{G}_m$, and hence a morphism $X^{\mathrm{good}} \to \mathbb{G}_m^{\Delta}$. Evaluating on closed points and taking norms (this is necessary if the closed point is of degree greater than 1), we obtain a homomorphism $\mathcal{Z}(X^{\mathrm{good}}) \to L^{\times}$. This induces $\mathcal{Z}^0(X^{\mathrm{good}}) \to L^{\times}/L^{\times n}$. If we change (β, f) to

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

(β', 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 nth power, and the value of c is $c^{\deg z} = 1$). Given any $z \in \mathcal{Z}^0(X)$, we can move β to avoid z, so the compatible homomorphisms glue to give a homomorphism

$$\widetilde{C} : \mathcal{Z}^0(X) \longrightarrow \frac{L^\times}{L^{\times n}}. \tag{4}$$

6.2.3. Compatibility of the two definitions.

PROPOSITION 6.4. *The maps C and $\widetilde{C}$ are compatible in the sense that the following diagram commutes:*

$$\begin{tikzcd}
\mathcal{Z}^0(X) \arrow[d] \arrow[drrr, bend left, "\widetilde{C}"] & & & \\
J(k) \arrow[r] & H^1(J[n]) \arrow[r, "\alpha"] & H^1(\mu_n^\Delta) & \frac{L^\times}{L^{\times n}}. \arrow[l, "\sim"']
\end{tikzcd}$$

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

$$0 \longrightarrow \mathcal{Y}^0 \longrightarrow \mathcal{Z}^0 \longrightarrow J(k_s) \longrightarrow 0.$$

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

$$\begin{tikzcd}
0 \arrow[r] & J[n] \arrow[r] & J \arrow[r, "n"] & J \arrow[r] & 0 \\
0 \arrow[r] \arrow[uu, bend left, "\alpha"] & \widetilde{J[n]} \arrow[r] \arrow[u] \arrow[d] & \mathcal{Z}^0 \times \mathcal{Y}^0 \arrow[r, "nz+y"] \arrow[u] \arrow[d] & \mathcal{Z}^0 \arrow[r] \arrow[u] \arrow[d, "\widetilde{C}"] & 0 \\
0 \arrow[r] & \mu_n^\Delta \arrow[r] & \mathbb{G}_m^\Delta \arrow[r, "n"] & \mathbb{G}_m^\Delta \arrow[r] & 0.
\end{tikzcd} \tag{5}$$

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

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

$$\begin{array}{rcl} \mathcal{Z}^0 \times \mathcal{Y}^0 & \longrightarrow & \mathbb{G}_m^{\Delta} \\ z, y & \longmapsto & f(z)[y, \beta] := (f_P(z) \cdot [y, \beta_P])_{P \in \Delta(k_s)} \end{array}$$

$$\begin{array}{rcl} \widetilde{C} \colon \mathcal{Z}^0 & \longrightarrow & \mathbb{G}_m^{\Delta} \\ z & \longmapsto & f(z). \end{array}$$

The bottom right square commutes since

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

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

Finally, we check that α and the vertical maps in the first column form a commutative triangle. Since $\alpha^\vee$ 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 μ_n^{Δ} are equal. This completes the construction of (5).

Taking cohomology of (5) yields

$$\begin{tikzcd} J(k) \arrow[r, "n"] & J(k) \arrow[r] & H^1(J[n]) \arrow[dd, bend left, "\alpha"] \\ & \mathcal{Z}^0(X^{\mathrm{good}}) \arrow[u] \arrow[r] \arrow[d, "\widetilde{C}"] & H^1(\widetilde{J[n]}) \arrow[u] \arrow[d] \\ L^\times \arrow[r, "n"] & L^\times \arrow[r] & H^1(\mu_n^{\Delta}). \end{tikzcd}$$

Equality of the compositions from $\mathcal{Z}^0(X^{\mathrm{good}})$ 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, $\mathcal{Z}^0(U)$ and $\mathcal{Z}^0(X)$ 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 [28, 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 $X - U$.)

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

COROLLARY 6.6. *The explicit homomorphism* $\widetilde{C}$ *in* (4) *induces a homomorphism*

$$\widetilde{C}\colon \left(\frac{J(k)}{nJ(k)}\right)_{\circ} \longrightarrow \frac{L^{\times}}{L^{\times n}}.$$

6.3. Fake descent. For computations using true descent setups to be practical, the degrees of the components of Δ (that is, 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 Δ 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 $(n, \Delta, \mathscr{L})$, where n is a positive integer not divisible by $\operatorname{char} k$, $\Delta = \operatorname{Spec} L$ is a nonempty finite étale k-scheme, and $\mathscr{L}$ is a line bundle on $X \times \Delta$ such that $\mathscr{L}^{\otimes n}$ is the pullback of a line bundle on X. Equivalently, in terms of a divisor $\beta \in \operatorname{Div}(X \times \Delta)$ representing $\mathscr{L}$, the condition is that there exists $D \in \operatorname{Div} X$ such that $n\beta - (D \times \Delta)$ is principal; that is, there is a function $f \in k(X \times \Delta)^{\times}$ such that $\operatorname{div}(f) = n\beta - (D \times \Delta)$.

REMARK 6.8. On the fibers, the last condition says that $\operatorname{div}(f_P) = n\beta_P - D$ for all $P \in \Delta(k_s)$. Subtracting shows that $[\beta_P - \beta_Q] \in \widehat{J}[n]$ 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 $\operatorname{char} k \neq 2$. Let $\pi\colon X \to \mathbb{P}^1_k$ be a (ramified) degree 2 cover, so X is a hyperelliptic curve. Let $n = 2$, let $\Delta \subset X$ be the ramification locus of π, and let β be the diagonal copy of Δ in $X \times \Delta$. Then we can take $D = \pi^*(y)$ for some $y \in \mathbb{P}^1(k)$ (cf. [**11**]). See Example 10.19 for more about this case.

(ii) The previous example generalizes to other geometrically generically cyclic covers $\pi\colon X \to \mathbb{P}^1_k$ (cf. [**29**]). Let $n \geqslant 2$. Let k be a field with $\operatorname{char} k \nmid n$. Suppose that $F(x) \in k[x]$ factors completely in $k_s[x]$ and is not a pth power in $k_s[x]$ for any $p \mid n$. Let X be the smooth projective model of $y^n = F(x)$. Let $\pi\colon X \to \mathbb{P}^1$ be the x-coordinate map. Let Δ be the ramification locus of π. Let β be the diagonal copy of Δ in $X \times \Delta$. Then we can take $D = \pi^*(t)$ for some $t \in \mathbb{P}^1(k)$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

(iii) Assume $\operatorname{char} k \notin \{2, 3, 7\}$. 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 Δ correspond to the $\mathcal{G}$-set of 8 triangles, as defined in [30, Section 11.1], and let $\beta \in \operatorname{Div}(X \times \Delta)$ be the divisor of relative degree 3 over Δ such that each β_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 [30]).

(iv) Assume $\operatorname{char} k \neq 2$. Let X be any curve of genus $g \geqslant 2$ over k. Let $n = 2$. Let Δ correspond to the $\mathcal{G}$-set of odd theta characteristics on X_s. Proposition 5.8 applied over the residue fields of each point of Δ shows that one can find $\beta \in \operatorname{Div}(X \times \Delta)$ such that each β_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 $(n, \Delta, \mathscr{L})$ will give rise to a cohomologically defined homomorphism

$$C\colon J(k) \longrightarrow H^1\left(\frac{\mu_n^{\Delta}}{\mu_n}\right) \tag{6}$$

that we will relate to an explicit homomorphism

$$\widetilde{C}\colon \mathcal{Z}^0(X) \longrightarrow \frac{L^\times}{L^{\times n}k^\times}. \tag{7}$$

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

$$\alpha^\vee\colon (\mathbb{Z}/n\mathbb{Z})^{\Delta}_{\deg 0} \longrightarrow \widehat{J}[n].$$

Dualizing

$$0 \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\Delta}_{\deg 0} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\Delta} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

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

$$\alpha\colon J[n] \longrightarrow \frac{\mu_n^{\Delta}}{\mu_n}.$$

The composition

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

is the desired homomorphism C.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

6.3.2. Explicit definition. As in Section 6.2.2, f gives rise to a homomorphism $\mathcal{Z}(X^{\mathrm{good}}) \to L^\times$. If we change (β, D, f) to (β', D', f'), then $\beta' - \beta$ is the divisor of some $g \in k(X \times \Delta)^\times$, and $D' - D$ 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 $z \in \mathcal{Z}^0(X)$ 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

$$0 \longrightarrow \mu_n \longrightarrow \mu_n^\Delta \longrightarrow \frac{\mu_n^\Delta}{\mu_n} \longrightarrow 0$$

yields

$$\frac{k^\times}{k^{\times n}} \longrightarrow \frac{L^\times}{L^{\times n}} \longrightarrow H^1\left(\frac{\mu_n^\Delta}{\mu_n}\right) \longrightarrow \operatorname{Br} k, \tag{8}$$

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 $\widetilde{C}$ are compatible in the sense that the following diagram commutes:*

$$\begin{tikzcd}
\mathcal{Z}^0(X) \arrow[d] \arrow[rrr, bend left, "\widetilde{C}"] & & & \\
J(k) \arrow[r] & H^1(J[n]) \arrow[r, "\alpha"] & H^1\left(\frac{\mu_n^\Delta}{\mu_n}\right) & \frac{L^\times}{L^{\times n}k^\times} \arrow[l, hook']
\end{tikzcd}$$

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

$$\begin{aligned} \mathcal{Y}^0 &\longrightarrow \frac{\mathbb{G}_m^\Delta(k_s)}{\mu_n(k_s)} \\ y &\longmapsto [y, \beta]_D := \frac{[y, \beta - H]}{h(y)^{1/n}} \end{aligned} \tag{9}$$

where $H \in \operatorname{Div}(X_s)$ and $h \in k_s(X)^\times$ are chosen so that $\operatorname{div}(h) = D - nH$, and $h(y)^{1/n}$ is a chosen nth 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 hj where $\operatorname{div}(j) = nH - nH'$, so the value of (9) is multiplied by $[y, H - H']/j(y)^{1/n}$,

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

which lies in $\mu_n(k_s)$ since its nth power equals $[y, \operatorname{div}(j)]/j(y) = 1$. Thus, (9) is well defined and Galois-equivariant. Also,

$$[y, \beta]_D^n = \frac{[y, n\beta - nH]}{h(y)} = \frac{[y, \operatorname{div}(fh)]}{h(y)} = \frac{(fh)(y)}{h(y)} = f(y). \tag{10}$$

As in the proof of Proposition 6.4, we construct a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & J[n] \arrow[r] \arrow[dd, bend right, "\alpha"'] & J \arrow[r, "n"] & J \arrow[r] & 0 \\
0 \arrow[r] & \widetilde{J[n]} \arrow[r] \arrow[u] \arrow[d] & \mathcal{Z}^0 \times \mathcal{Y}^0 \arrow[r, "nz+y"] \arrow[u] \arrow[d] & \mathcal{Z}^0 \arrow[r] \arrow[u] \arrow[d, "\widetilde{C}"] & 0 \\
0 \arrow[r] & \dfrac{\mu_n^\Delta}{\mu_n} \arrow[r] & \dfrac{\mathbb{G}_m^\Delta}{\mu_n} \arrow[r, "n"] & \mathbb{G}_m^\Delta \arrow[r] & 0.
\end{tikzcd} \tag{11}$$

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

$$\begin{aligned} \mathcal{Z}^0 \times \mathcal{Y}^0 &\longrightarrow \frac{\mathbb{G}_m^\Delta}{\mu_n} \\ z, y &\longmapsto f(z)[y, \beta]_D \end{aligned}$$

and the rightmost downward map is

$$\begin{aligned} \widetilde{C} \colon \mathcal{Z}^0(X_s^{\text{good}}) &\longrightarrow \mathbb{G}_m^\Delta \\ z &\longmapsto f(z). \end{aligned}$$

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 α and the vertical maps in the first column form a commutative triangle. Any $(z, -nz) \in \widetilde{J[n]}$ maps up to $[z] \in J[n]$, and maps right and down to $f(z) \cdot [-nz, \beta]_D \in (\mathbb{G}_m^\Delta/\mu_n)$. Remark 4.1 and the Albanese–Picard definition of e_n show that

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

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Taking cohomology of (11) yields

$$\begin{tikzcd}
J(k) \arrow[r, "n"] & J(k) \arrow[r] & H^1(J[n]) \arrow[ddl, bend left, "\alpha"] \\
 & \mathcal{Z}^0(X^{\mathrm{good}}) \arrow[u] \arrow[r] \arrow[d, "\widetilde{C}"] & H^1(\widetilde{J[n]}) \arrow[u] \arrow[d] \\
 & L^\times \arrow[r] & H^1\left(\frac{\mu_n^\Delta}{\mu_n}\right).
\end{tikzcd}$$

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

COROLLARY 6.11. *The explicit homomorphism $\widetilde{C}$ in (7) induces a homomorphism*

$$\widetilde{C}\colon \left(\frac{J(k)}{nJ(k)}\right)_\circ \longrightarrow \frac{L^\times}{L^{\times n}k^\times}.$$

COROLLARY 6.12. *The homomorphism $\widetilde{C}$, which a priori depends on β and D, in fact is independent of D and depends only on the linear equivalence class of β.*

Proof. The linear equivalence class of β is all that is needed to define C. □

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

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

In either case, we obtain an isogeny $\widehat{\phi}\colon \widehat{J} \to \widehat{A} := \widehat{J}/\alpha^\vee(E)$, and $\widehat{J}[\widehat{\phi}] = \alpha^\vee(E)$. Let A be the dual abelian variety of $\widehat{A}$, and let $\phi\colon A \to J$ be the dual of $\widehat{\phi}$. (It was first explained in [36] that the generality in which one relates the functions in a true descent setup to an isogeny is for an isogeny whose image is a Jacobian.)

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. By [24, Section III.15, Theorem 1], $A[\phi]^\vee \simeq \widehat{J}[\widehat{\phi}]$. Now the homomorphism $\alpha^\vee\colon E \to \widehat{J}[n]$ factors through $\alpha^\vee(E) = \widehat{J}[\widehat{\phi}]$, and dualizing shows that $\alpha\colon J[n] \to E^\vee$ factors through $A[\phi]$. This explains the right triangle in the commutative diagram

$$\begin{tikzcd} \dfrac{J(k)}{nJ(k)} \arrow[r] \arrow[d] & H^1(J[n]) \arrow[r] \arrow[d] & H^1(E^\vee) \\ \dfrac{J(k)}{\phi A(k)} \arrow[r] & H^1(A[\phi]), \arrow[ur] & \end{tikzcd} \tag{12}$$

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

COROLLARY 6.15. *The explicit homomorphism $\widetilde{C}$ defined on $\mathcal{Z}^0(X)$ factors not only through $J(k)_\circ$ or $(J(k)/nJ(k))_\circ$, but also through $(J(k)/\phi A(k))_\circ$.*

Proof. Combine Proposition 6.14 with Proposition 6.4 or Proposition 6.10. □

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

$$0 \longrightarrow R \longrightarrow E \xrightarrow{\alpha^\vee} \widehat{J}[\widehat{\phi}] \longrightarrow 0. \tag{13}$$

Dualizing yields an exact sequence

$$0 \longrightarrow A[\phi] \xrightarrow{\alpha} E^\vee \xrightarrow{q} R^\vee \longrightarrow 0. \tag{14}$$

Take cohomology: for a true descent setup we obtain

$$\begin{tikzcd} & & \left(\dfrac{J(k)}{\phi A(k)}\right)_\circ \arrow[r, "\widetilde{C}"] \arrow[d, hook] \arrow[dr, "C"] & \dfrac{L^\times}{L^{\times n}} \arrow[d, equal] & \\ 0 \arrow[r] & A[\phi](k) \arrow[r, "\alpha"] & E^\vee(k) \arrow[r, "q"] & R^\vee(k) \arrow[r] & H^1(A[\phi]) \arrow[r, "\alpha"] & H^1(E^\vee) \arrow[r, "q"] & H^1(R^\vee) \end{tikzcd} \tag{15}$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

and for a fake descent setup we obtain

$$\begin{tikzcd}
 & & \left(\frac{J(k)}{\phi A(k)}\right)_\circ \arrow[r, "\tilde{c}"] \arrow[d, hook] \arrow[dr, "c"] & \frac{L^\times}{L^{\times n}k^\times} \arrow[d, hook] & \\
0 \arrow[r] & A[\phi](k) \arrow[r, "\alpha"] & E^\vee(k) \arrow[r, "q"] & R^\vee(k) \arrow[r] & H^1(A[\phi]) \arrow[r, "\alpha"] & H^1(E^\vee) \arrow[r, "q"] & H^1(R^\vee).
\end{tikzcd} \tag{16}$$

The commutativity follows from Proposition 6.4 or Proposition 6.10.

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

$$\begin{tikzcd}
\left(\frac{J(k)}{\phi A(k)}\right)_\circ \arrow[r, "\tilde{c}_{\text{true}}"] \arrow[dr, "\tilde{c}_{\text{fake}}"'] & \frac{(L')^\times}{(L')^{\times n}} \arrow[d, equal] \\
 & \frac{L^\times}{L^{\times n}k^\times}
\end{tikzcd}$$

commutes.

Moreover, every true descent setup can be obtained from some fake descent setup in this way, at least if k is infinite. Thus fake descent is a generalization of true descent.

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

6.7. Restrictions on the image of $\widetilde{C}$. 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 $\widetilde{C}\colon \mathcal{Z}^0(X) \to \widetilde{L^\times/L^{\times n}k^\times}$ is contained in the kernel of the homomorphism $N\colon \widetilde{L^\times/L^{\times n}k^\times} \to k^\times/k^{\times n}$ induced by the norm map $L^\times \to k^\times$.*

Proof. Dualizing the complex

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow E \to \widehat{J}[\widehat{\phi}]$$

and applying H^1 yields a complex

$$H^1(A[\phi]) \longrightarrow H^1(E^\vee) \xrightarrow{\mathcal{N}} \frac{k^\times}{k^{\times n}}.$$

The restriction of $\mathcal{N}$ to the subgroup $\widetilde{L^\times/L^{\times n}k^\times}$ equals N, because it is induced by dualizing $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^{\Delta}$ 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 nonarchimedean local field. If M is any $\mathcal{G}_{k_v}$-module, define the *subgroup of unramified classes*

$$\begin{aligned} H^1(k_v, M)_{\mathrm{unr}} &:= \ker\big(H^1(k_v, M) \to H^1(k_{v,u}, M)\big) \\ &\simeq H^1(\mathrm{Gal}(k_{v,u}/k_v), M(k_{v,u})), \end{aligned}$$

where the isomorphism follows from the inflation–restriction sequence.

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

7.2. A Tamagawa number criterion. Let k_v be a nonarchimedean local field. Let $\phi\colon A \to J$ be a separable isogeny of abelian varieties over k_v. The short exact sequence

$$0 \longrightarrow A[\phi] \longrightarrow A \xrightarrow{\phi} J \longrightarrow 0$$

gives rise to a connecting homomorphism

$$\gamma_v\colon J(k_v) \longrightarrow H^1(k_v, A[\phi]).$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Let $\mathcal{J}$ be the Néron model of J over $\mathcal{O}_v$. Let $\mathcal{J}^0$ be the connected component of the identity in $\mathcal{J}$. Let Φ be the group of connected components of the special fiber $\mathcal{J} \times \mathbb{F}_v$, so Φ 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 $\phi\colon A \to J$ be as above. Let n be a positive integer such that $nA[\phi] = 0$ (one possibility is $n = \deg\phi$). If the residue characteristic* $\operatorname{char}\mathbb{F}_v$ *does not divide n, and if $c_v(J)$ and $c_v(A)$ are coprime to n, then*

$$\gamma_v(J(k_v)) = H^1(k_v, A[\phi])_{\mathrm{unr}}.$$

Proof. This is a straightforward generalization of the proof of [37, Lemma 3.1 and Proposition 3.2], which uses results from [35, Section 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 $\widetilde{L_v^\times/L_v^{\times n}k_v^\times} \hookrightarrow H^1(k_v, E^\vee)$. Call an element of $\widetilde{L_v^\times/L_v^{\times n}k_v^\times}$ *unramified* if its image in $H^1(k_v, E^\vee)$ is unramified.

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

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

PROPOSITION 7.2. *Suppose that $\mathcal{S} \subseteq \Omega_k$ contains all archimedean places and all places of residue characteristic dividing n. Then $(\widetilde{L^\times/L^{\times n}k^\times})_{\mathcal{S}} = \widetilde{L(n, \mathcal{S})}$.*

Proof. The statement and proof are the same as for [29, Proposition 12.5]. □

PROPOSITION 7.3. *The group $\widetilde{L(n, \mathcal{S})}$ is finite and computable.*

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. Let $\mathcal{O}_{\mathcal{S}}$ and $\mathcal{O}_{L,\mathcal{S}}$ be the rings of $\mathcal{S}$-integers in k and L, respectively; then there are exact sequences

$$0 \longrightarrow \frac{\mathcal{O}_{L,\mathcal{S}}^{\times}}{\mathcal{O}_{L,\mathcal{S}}^{\times n}} \longrightarrow L(n,\mathcal{S}) \longrightarrow \mathrm{Cl}(\mathcal{O}_{L,\mathcal{S}})[n] \longrightarrow 0 \tag{17}$$

and (in the fake case)

$$k(n,\mathcal{S}) \longrightarrow L(n,\mathcal{S}) \longrightarrow \widetilde{L(n,\mathcal{S})} \longrightarrow \frac{\mathrm{Cl}(\mathcal{O}_{\mathcal{S}})}{n\,\mathrm{Cl}(\mathcal{O}_{\mathcal{S}})}, \tag{18}$$

as in [29, Propositions 12.6 and 12.8], where these are constructed for prime n. So the finiteness follows from the Dirichlet $\mathcal{S}$-unit theorem and finiteness of the class groups, and the computability follows too since these are effective. □

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

Proof. Using the inflation–restriction sequence lets us enlarge k to assume that $\mathcal{G}$ 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 $\operatorname{char} k \nmid n$. Now $H^1(k,\mu_n)_{\mathcal{S}} \simeq (k^{\times}/k^{\times n})_{\mathcal{S}}$, which, as in Proposition 7.3, is finite. □

8. Finite Galois modules and Ш[1]

Let k be a global field, and let M be a finite $\mathcal{G}_k$-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

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

LEMMA 8.1 (Cf. [22, Example I.4.11(i)]). *If $\mathcal{G}_k$ acts trivially on M, then* $Ш^1(k,M) = 0$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. The hypothesis implies that $H^1(k, M) = \mathrm{Hom}(\mathcal{G}_k, M)$, where Hom denotes the group of continuous homomorphisms. Chebotarev's density theorem implies that the union of the decomposition groups $\mathcal{G}_{k_v}$ is dense in $\mathcal{G}_k$, so the map

$$\mathrm{Hom}(\mathcal{G}_k, M) \longrightarrow \prod_v \mathrm{Hom}(\mathcal{G}_{k_v}, M)$$

is injective. This implies the result. □

LEMMA 8.2. *If p is a prime not equal to* $\mathrm{char}\, k$, *and Δ is any $\mathcal{G}$-set, then* $Ш^1(k, \mu_p^{\Delta}) = 0$.

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

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

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

$$Ш^1(k, M) \simeq \ker\Big(H^1(G, M) \to \prod_v H^1(D_v, M)\Big).$$

In particular,

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

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 $H \leqslant G$ is replaced by a conjugate subgroup. Inflation–restriction with respect to $1 \to \mathcal{G}_K \to \mathcal{G}_k \to G \longrightarrow 1$ and its local analogues yield the exactness of the last two rows in the commutative

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

diagram

$$\begin{tikzcd}
0 \arrow[r] & Ш^1(G, M) \arrow[r] \arrow[d] & Ш^1(k, M) \arrow[r] \arrow[d] & Ш^1(K, M) \arrow[d] \\
0 \arrow[r] & H^1(G, M) \arrow[r] \arrow[d] & H^1(k, M) \arrow[r] \arrow[d] & H^1(K, M) \arrow[d] \\
0 \arrow[r] & \prod_v H^1(D_v, M) \arrow[r] & \prod_v H^1(k_v, M) \arrow[r] & \prod_v H^1(K_v, M),
\end{tikzcd}$$

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 $Ш^1(K, M) = 0$, so $Ш^1(k, M) \simeq Ш^1(G, M)$, 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 $\phi\colon A \to J$ be an isogeny of abelian varieties over a global field k such that $\operatorname{char} k \nmid \deg \phi$. For each v, we obtain a connecting homomorphism $\gamma_v\colon J(k_v) \to H^1(k_v, A[\phi])$. Define

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

PROPOSITION 9.2. *Let $\mathcal{S}$ 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) $\mathrm{Sel}^{\phi}(J) = \{\delta \in H^1(k, A[\phi])_{\mathcal{S}} : \delta_v \in \operatorname{im} \gamma_v$ *for all* $v \in \mathcal{S}\}$.

(b) *The group* $H^1(k, A[\phi])_{\mathcal{S}}$ *is finite.*

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof.

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

(b) Finiteness of $H^1(k, A[\phi])_{\mathcal{S}}$ 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 $\mathrm{Sel}^{\phi}(J)$, 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 $\widetilde{L^\times/L^{\times n}k^\times}$, and by replacing $\gamma_v\colon J(k_v) \to H^1(k_v, A[\phi])$ by $\widetilde{C}_v\colon J(k_v)_\circ \to \widetilde{L_v^\times/L_v^{\times n}k_v^\times}$, which we shall henceforth denote by C_v.

DEFINITION 9.3. Given a true descent setup (n, Δ, β), define the *true Selmer group*

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

Given a fake descent setup (n, Δ, β), define the *fake Selmer group*

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

To avoid having to state results twice, we use $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)$ to denote either $\mathrm{Sel}^{\alpha}_{\mathrm{true}}(J)$ or $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$, depending on whether we are considering a true or a fake descent setup.

9.3. True and fake Selmer sets for X. The concept of a Selmer group associated to an isogeny $\phi\colon A \to J$ can be generalized to the situation of a finite étale cover $Y \to X$ of nice varieties, as a subset of $H^1(k, \mathrm{Aut}(Y_s/X_s))$. In general, it is just a finite set but it contains arithmetic information about X. For instance, if the Selmer set is empty, then so is $X(k)$. Like Selmer groups, Selmer sets are in theory computable, but often not efficiently. In this section, we consider more computationally amenable variants, generalizing the hyperelliptic setting in [6].

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.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Evaluation on closed points as in Sections 6.2.2 or 6.3.2 defines a homomorphism $\widetilde{C}_f\colon \mathcal{Z}(X^{\mathrm{good}}) \to \widetilde{L^\times/L^{\times n}k^\times}$. Since $\widetilde{C}_f$ and $\widetilde{C}$ agree on $\mathcal{Z}^0(X^{\mathrm{good}})$, they have a common extension to the sum of their domains, $\mathcal{Z}(X^{\mathrm{good}})+\mathcal{Z}^0(X) = \mathcal{Z}(X)$. Then we may restrict to $X(k)$ to obtain a map of sets

$$C_f\colon X(k) \longrightarrow \widetilde{L^\times/L^{\times n}k^\times}.$$

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

$$C_{f,v}\colon X(k_v) \longrightarrow \widetilde{L_v^\times/L_v^{\times n}k_v^\times}.$$

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

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

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 $N(\widetilde{C}_f(z)) = c^{\deg z}$ in $k^\times/k^{\times n}$ for all $z \in \mathcal{Z}(X)$.*

Proof. In the true case, the hypothesis on R implies that $\sum_{P\in\Delta} \beta_P = \mathrm{div}(r)$ for some $r \in k(X)^\times$. Then

$$\mathrm{div}(N_{L/k}(f)) = n\sum_{P\in\Delta} \beta_P = \mathrm{div}(r^n),$$

so $N_{L/k}(f) = cr^n$ for some $c \in k^\times$. Evaluating on any $z \in \mathcal{Z}(X^{\mathrm{good}})$ 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 $z \in \mathcal{Z}(X^{\mathrm{good}}) + \mathcal{Z}^0(X) = \mathcal{Z}(X)$.

In the fake case, the hypothesis on R implies that $\#\Delta = nm$ for some $m \in \mathbb{Z}_{>0}$ and that $\left(\sum_{P\in\Delta} \beta_P\right) - mD = \mathrm{div}(r)$ for some $r \in k(X)^\times$. Then

$$\mathrm{div}(N_{L/k}(f)) = n\sum_{P\in\Delta} \beta_P - nmD = \mathrm{div}(r^n),$$

so $N_{L/k}(f) = cr^n$ for some $c \in k^\times$. The rest of the proof is as in the true case. □

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $H^0(k, \operatorname{Pic} X_s) \xrightarrow{\deg} \mathbb{Z}$ is surjective); or*

(ii) *k is a global field and for every $v \in \Omega_k$ the curve X has a k_v-point (or more generally $H^0(k_v, \operatorname{Pic} X_{k_{v,s}}) \xrightarrow{\deg} \mathbb{Z}$ is surjective); 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 we have $J(k_v)_\circ = J(k_v)$ for every v, so Hypothesis 10.1 holds.

Proof. For (i) and (ii), see [**29**, Propositions 3.2 and 3.3]. For (iii) (generalized to superelliptic curves), see [**29**, end of Section 4]. □

Hypothesis 10.1 will let us define a map from the usual ϕ-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 γ_v and our approximation C_v. In Section 10.3, we define a global group $\mathcal{K}$ with a homomorphism $\kappa : \mathcal{K} \to \prod_v W_v$ whose kernel and cokernel control the difference between the actual ϕ-Selmer group and our explicit Selmer group $\operatorname{Sel}^{\alpha}_{\text{true/fake}}(J)$.

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

$$\begin{tikzcd}
 & \dfrac{J(k_v)}{\phi A(k_v)} \arrow[d, hook, "\gamma_v"'] \arrow[dr, "C_v"] & & & \\
E^\vee(k_v) \arrow[r, "q"] & R^\vee(k_v) \arrow[r] & H^1(k_v, A[\phi]) \arrow[r, "\alpha_v"] & H^1(k_v, E^\vee) \arrow[r] & H^1(k_v, R^\vee),
\end{tikzcd} \tag{19}$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

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

$$\ker C_v \longrightarrow \ker \alpha_v \longrightarrow \operatorname{coker} \gamma_v \longrightarrow \operatorname{coker} C_v. \tag{20}$$

DEFINITION 10.3. Let W_v be any 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 $\ker \alpha_v \to \operatorname{coker} \gamma_v$; or

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

LEMMA 10.4. *For any $v \in \Omega_k$, the group W_v is finite, and*

$$\#W_v = \frac{\#\operatorname{coker} q \cdot \#\operatorname{im} C_v}{\#\operatorname{im} \gamma_v}.$$

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

$$0 \longrightarrow \operatorname{im} \gamma_v \cap \ker \alpha_v \longrightarrow \ker \alpha_v \longrightarrow W_v \longrightarrow 0,$$
$$0 \longrightarrow \operatorname{im} \gamma_v \cap \ker \alpha_v \longrightarrow \operatorname{im} \gamma_v \longrightarrow \operatorname{im} C_v \longrightarrow 0,$$

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 nonarchimedean 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) $\operatorname{im}(C_v) \subseteq H^1(k_v, E^\vee)_{\mathrm{unr}}$, *and*

(b) $W_v = \operatorname{im}\left(\dfrac{R^\vee(k_v)}{qE^\vee(k_v)} \to \dfrac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})}\right)$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. The commutative diagram

$$\begin{tikzcd}
 & & \dfrac{J(k_v)}{\phi A(k_v)} \arrow[d, "\gamma_v"'] \arrow[dr, "C_v"] & \\
0 \arrow[r] & \dfrac{R^\vee(k_v)}{qE^\vee(k_v)} \arrow[r] \arrow[d] & H^1(k_v, A[\phi]) \arrow[r, "\alpha_v"] \arrow[d] & H^1(k_v, E^\vee) \arrow[d] \\
0 \arrow[r] & \dfrac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})} \arrow[r] & H^1(k_{v,u}, A[\phi]) \arrow[r] & H^1(k_{v,u}, E^\vee)
\end{tikzcd} \tag{21}$$

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 $\operatorname{im}(C_v) \subset H^1(k_v, E^\vee)_{\mathrm{unr}}$.

(b) By Definition 10.3(ii),

$$\begin{aligned} W_v &= \operatorname{im}(\ker \alpha_v \to \operatorname{coker} \gamma_v) \\ &= \operatorname{im}\left(\frac{R^\vee(k_v)}{qE^\vee(k_v)} \to H^1(k_{v,u}, A[\phi])\right) \\ &= \operatorname{im}\left(\frac{R^\vee(k_v)}{qE^\vee(k_v)} \to \frac{R^\vee(k_{v,u})}{qE^\vee(k_{v,u})}\right). \end{aligned}$$

□

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

$$E^\vee(k_{v,u}) = E^\vee(k_{v,s}) \xrightarrow{q} R^\vee(k_{v,s}) = R^\vee(k_{v,u}),$$

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.*

Proof. Combine Lemma 10.4 and Corollary 10.6. □

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\mathrm{Gal}(k_{v,s}/k_v) = \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\}$. If v is real then $\mathrm{Gal}(k_{v,s}/k_v) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$. Our assumptions assure that in either case, $\mathrm{Gal}(k_{v,s}/k_v)$ 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 $\mathcal{S}$ be as in Proposition 9.2. Given another finite set of places $\mathcal{T}$, define

$$S_{\mathcal{T}} := \left\{ \delta \in \widetilde{L(n, \mathcal{S})} : \delta_v \in \mathrm{im}(C_v) \text{ for all } v \in \mathcal{T} \right\}.$$

THEOREM 10.9. *Let $\mathcal{S}$ and $\mathcal{T}$ be as above.*

(a) *We have* $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \subseteq S_{\mathcal{T}}$.

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

Proof.

(a) For $v \notin \mathcal{S}$, Lemma 10.5(a) proves that $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)$ consists of elements unramified at v. Proposition 7.2 now shows that $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \subseteq \widetilde{L(n, \mathcal{S})}$. The condition $\delta \in \mathrm{im}\, C_v$ in the definition of $S_{\mathcal{T}}$ is also in the definition of $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)$.

(b) Suppose that $\delta \in S_{\mathcal{T}}$. Given $v \notin \mathcal{T}$, we must show that $\delta \in \mathrm{im}\, C_v$. Choose $w \in \mathcal{T}$ unramified in k_δ/k such that the conjugacy classes Frob_w and Frob_v in $\mathrm{Gal}(k_\delta/k)$ match. By definition of $S_{\mathcal{T}}$, we have $\delta_w \in \mathrm{im}\, C_w$. Then (19) for k_w shows that δ maps to 0 in $H^1(k_w, R^\vee)$. In other words, the element $\delta \in H^1(\mathrm{Gal}(k_\delta/k), R^\vee)$ restricts to 0 at w. But the decomposition groups of v and w in $\mathrm{Gal}(k_\delta/k)$ are conjugate, so δ maps to 0 in $H^1(k_v, R^\vee)$ too. Thus the localization $\delta_v \in H^1(k_v, E^\vee)$ is the image of some $\xi_v \in H^1(k_v, A[\phi])$. Since $v \notin \mathcal{S}$, the element δ_v is unramified; in particular, ξ_v maps to 0 in $H^1(k_{v,u}, E^\vee)$. By hypothesis, $E^\vee$ is unramified

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

at v, so $E^\vee(k_{v,u}) \xrightarrow{q} R^\vee(k_{v,u})$ is surjective, so the bottom row of (21) shows that $H^1(k_{v,u}, A[\phi]) \to H^1(k_{v,u}, E^\vee)$ is injective. Thus, ξ_v maps to 0 already in $H^1(k_{v,u}, A[\phi])$; that is, $\xi_v \in H^1(k_v, A[\phi])_{\mathrm{unr}}$. By Lemma 7.1, ξ_v is in the image of $J(k_v)$ under γ_v. Thus δ_v is in the image of $J(k_v)$ under C_v. □

REMARK 10.10. The idea to use an enlarged set $\mathcal{T}$ including places whose Frobenius elements cover the conjugacy classes was first used in [**10**, Corollary 12].

REMARK 10.11. Here we show how to compute a finite set $\mathcal{T}$ as in Theorem 10.9(b). A finite splitting field k_Δ of Δ will split $R^\vee$. Given δ, represented by $\ell = (\ell_i) \in L^\times$, say, adjoining all nth roots of the ℓ_i to k_Δ yields a candidate for k_δ. The Chebotarev density theorem guarantees that we can find enough v unramified in k_δ/k to cover the conjugacy classes.

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

$$C(J(k)) \subseteq \mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J) \subseteq S_{\mathcal{T}}.$$

But if we find enough points in $J(k)$ to show that $C(J(k)) = S_{\mathcal{T}}$, then we obtain $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J) = S_{\mathcal{T}}$ nevertheless. Often $\mathcal{T} = \mathcal{S}$ 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 ϕ determined by the descent setup (which is the object we would like to compute). Theorem 10.14 will show that α induces a homomorphism from the latter to the former.

LEMMA 10.13. *We have an exact sequence*

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

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{L^\times}{L^{\times n}k^\times} \arrow[r] \arrow[d] & H^1(k, E^\vee) \arrow[r] \arrow[d] & \operatorname{Br} k \arrow[d] \\
0 \arrow[r] & \prod_v \dfrac{L_v^\times}{L_v^{\times n}k_v^\times} \arrow[r] & \prod_v H^1(k_v, E^\vee) \arrow[r] & \prod_v \operatorname{Br} k_v
\end{tikzcd}$$

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

$$\begin{aligned}
\ker\left(H^1(k, E^\vee) \to \prod_v \frac{H^1(k_v, E^\vee)}{\operatorname{im} C_v}\right) &= \ker\left(\frac{L^\times}{L^{\times n}k^\times} \to \prod_v \frac{H^1(k_v, E^\vee)}{\operatorname{im} C_v}\right) \\
&= \operatorname{Sel}^\alpha_{\text{fake}}(J). \qquad \square
\end{aligned}$$

Let $\mathcal{K}$ be the kernel of the global map $\alpha\colon H^1(k, A[\phi]) \to H^1(k, E^\vee)$. By (16), $\mathcal{K}$ equals the (computable) cokernel of $q\colon E^\vee(k) \to R^\vee(k)$. Let κ be the composition

$$\mathcal{K} = \ker \alpha \to \prod_v \ker \alpha_v \twoheadrightarrow \prod_v \operatorname{im}(\ker \alpha_v \to \operatorname{coker} \gamma_v) = \prod_v W_v. \tag{22}$$

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

THEOREM 10.14. *We have an exact sequence*

$$0 \longrightarrow \ker \kappa \longrightarrow \operatorname{Sel}^\phi(J) \xrightarrow{\alpha} \operatorname{Sel}^\alpha_{\text{true/fake}}(J) \cap \alpha\big(H^1(k, A[\phi])\big) \longrightarrow \operatorname{coker} \kappa.$$

Proof. By definition of κ, the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{K} \arrow[r] \arrow[d, "\kappa"'] & H^1(k, A[\phi]) \arrow[r, "\alpha"] \arrow[d] & \alpha\big(H^1(k, A[\phi])\big) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v W_v \arrow[r] & \prod_v \dfrac{H^1(k_v, A[\phi])}{\operatorname{im} \gamma_v} \arrow[r] & \prod_v \dfrac{H^1(k_v, E^\vee)}{\operatorname{im} C_v} &
\end{tikzcd} \tag{23}$$

commutes. By definition of $\mathcal{K}$ 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. $\square$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

COROLLARY 10.15. *We have*

$$\#\ker\left(\mathrm{Sel}^{\phi}(J) \to \mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)\right) \leqslant \#R^{\vee}(k)/qE^{\vee}(k).$$

Proof. By Theorem 10.14, the kernel is isomorphic to

$$\ker\kappa \subseteq \mathcal{K} \simeq R^{\vee}(k)/qE^{\vee}(k). \qquad \square$$

The following summarizes the best possible situation.

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

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathrm{Sel}^{\phi}(J) \longrightarrow \mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \longrightarrow 0.$$

In particular, $\#\mathrm{Sel}^{\phi}(J) = \#\mathcal{K} \cdot \#\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)$.

Proof. In Theorem 10.14, the codomain of $\kappa : \mathcal{K} \to \prod_v W_v$ is 0. $\square$

We need a criterion that tells us when $\mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J)$ is already contained in $\alpha\big(H^1(k, A[\phi])\big)$. Recall the discussion of $Ш^1$ in Section 8 and the exact sequence

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

LEMMA 10.17.

(a) *There is an exact sequence*

$$0 \longrightarrow \mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \cap \alpha\big(H^1(k, A[\phi])\big) \longrightarrow \mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \xrightarrow{q} Ш^1(k, R^{\vee}).$$

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

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

$$\begin{tikzcd}
0 \arrow[r] & \alpha\left(H^1(k, A[\phi])\right) \arrow[r] \arrow[d] & H^1(k, E^{\vee}) \arrow[r, "q"] \arrow[d] & H^1(k, R^{\vee}) \arrow[d] \\
0 \arrow[r] & \prod_v \dfrac{\alpha_v\left(H^1(k_v, A[\phi])\right)}{\mathrm{im}\, C_v} \arrow[r] & \prod_v \dfrac{H^1(k_v, E^{\vee})}{\mathrm{im}\, C_v} \arrow[r] & \prod_v H^1(k, R^{\vee}).
\end{tikzcd}$$

Take the kernels of the three vertical maps and apply Lemma 10.13. $\square$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

REMARK 10.18. Results of Section 8 allow us to bound $Ш^1(k, R^\vee)$ 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 $\mathcal{G}_k$-set Δ is the set of Weierstrass points. The group $\mathbb{Z}/2\mathbb{Z}$ injects into $E = (\mathbb{Z}/2\mathbb{Z})^{\Delta}_{\deg 0}$, and $E^\vee = \mu_2^{\Delta}/\mu_2$. Since $\widehat{J} \simeq J$, exact sequence (13) is

$$0 \longrightarrow \frac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow E \longrightarrow J[2] \longrightarrow 0,$$

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 [29, Theorem 11.3]) that the element of $\mathcal{K}$ represented by $-1 \in \mu_2(k)$ corresponds to the class ξ of the 2-covering $\mathbf{Pic}^1_{X/k} \to J$ in $H^1(k, J[2])$, where $\mathbf{Pic}^1_{X/k}$ is the Picard scheme component parametrizing degree 1 line bundles on X. For each v, our assumption implies that $\mathbf{Pic}^1_{X/k}$ has a k_v-point, so ξ_v maps to 0 in $H^1(k_v, J)$, so

$$\xi_v \in \operatorname{im}\left(\gamma_v \colon J(k_v)/2J(k_v) \to H^1(k_v, J[2])\right).$$

Since ξ_v generates $\ker \alpha_v$, we have $W_v = 0$ by Definition 10.3(ii). We also have $Ш^1(k, \mu_2) = 0$ by Lemma 8.1, so Lemma 10.17(b) applies, and Corollary 10.16 yields an exact sequence

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathrm{Sel}^2(J) \longrightarrow \mathrm{Sel}^{\alpha}_{\mathrm{true/fake}}(J) \longrightarrow 0.$$

Finally, since $\mathcal{K} \simeq \mu_2(k)/N(E^\vee(k))$, we have that $\mathcal{K} = 0$ if Δ has a Galois-stable unordered partition into two sets of odd cardinality (a computable condition), and $\mathcal{K} \simeq \mu_2(k)$ otherwise (cf. [29, Theorem 13.2]).

11. Computing true and fake Selmer groups

Choose $\mathcal{S}$ and $\mathcal{T}$ as in Section 10.2, and compute $\widetilde{L(n, \mathcal{S})}$ as in Section 7.3. Because of Theorem 10.9, it remains to find an algorithm to test whether a given

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

element of $\widetilde{L(n,\mathcal{S})}$ is in the local image $\operatorname{im} C_v$ 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* $\operatorname{char} k_v = 0$ *or* $\operatorname{char} k_v > g$.

We consider the nonarchimedean and archimedean cases separately.

11.1. Computing the local image at a nonarchimedean place. Fix a nonarchimedean place v of k. Let K be a finite extension of k_v, say of degree d, with valuation ring $\mathcal{O}$, uniformizer π, and maximal ideal $\mathfrak{m}$. Let $L_K := L \otimes_k K$. We have a map $X(K) \to \mathcal{Z}^0(X_K)$ sending x to the 0-cycle $x - x_0$, and following this with $\widetilde{C}_K$ defines a continuous map

$$\mathfrak{c}_K : X(K) \longrightarrow \widetilde{\frac{L_K^\times}{L_K^{\times n} K^\times}}.$$

To define $\mathfrak{c}_K$ on all of $X(K)$ requires using several functions $f_1, \dots, f_r$ 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 $\mathfrak{c}_K$. Choose a proper $\mathcal{O}$-scheme $\mathcal{X}$ with $\mathcal{X}_K \simeq X_K$. By the valuative criterion for properness,

$$X(K) \simeq \mathcal{X}(\mathcal{O}) \simeq \varprojlim_{m \geqslant 0} \mathcal{X}(\mathcal{O}/\pi^m).$$

By Hensel's lemma, $L_K^{\times n}$ has finite index in $L_K^\times$, so $\widetilde{L_K^\times / L_K^{\times n} K^\times}$ is a finite discrete set, so $\mathfrak{c}_K$ is locally constant. Proceed as follows:

- Start with $m = 1$.
- On each remaining residue disk modulo π^m in $X(K)$, check whether any f_i is such that $f_i(x)/f_i(x_0)$ is constant in $(\widetilde{L_K^\times / (L_K^{\times n} K^\times)})$; if not, break the residue disk into residue disks modulo π^{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 $\mathfrak{c}_K$ takes a known constant value.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Next, the diagram

$$\begin{tikzcd}
X(K) \arrow[r, "x \mapsto x - x_0"] \arrow[dr, "x \mapsto \mathrm{tr}_{K/k_v}\, x - dx_0"'] & \mathcal{Z}^0(X_K) \arrow[r] \arrow[d, "\mathrm{tr}_{K/k_v}"] & \widetilde{\dfrac{L_K^\times}{L_K^{\times n} K^\times}} \arrow[d, "N_{K/k_v}"] \\
& \mathcal{Z}^0(X_{k_v}) \arrow[r] & \widetilde{\dfrac{L_v^\times}{L_v^{\times n} k_v^\times}}
\end{tikzcd}$$

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

LEMMA 11.2.

(a) *There are only finitely many extensions K/k_v with $[K : k_v] \leqslant g$ 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 $\mathrm{tr}_{K/k_v}\, x - dx_0$ generate $J(k_v)$.*

Proof.

(a) If $\operatorname{char} k_v = 0$, see [27]. If $\operatorname{char} k_v > 0$, 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 mth root of a uniformizer to a finite unramified extension of k_v. We can compute representatives for the set of possible uniformizers up to mth powers.

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

We can now compute $\operatorname{im} C_v$ as follows:

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

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

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

By Lemma 11.2, the result equals $\operatorname{im} C_v$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\widetilde{L_v^\times/L_v^{\times n}k_v^\times}$ is constant on connected components. If $K = \mathbb{C}$, then every point in $X(K)$ has the same image under $x \mapsto \mathrm{tr}_{K/k_v} x - dx_0$ 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 $\mathfrak{c}_K$, we need to move β (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 β is the only effective divisor in its class.

REMARK 11.4. Sometimes we can compute $\mathfrak{c}_K$ without moving β, as we now explain. Suppose that

- we have a true or fake descent setup, with a choice of β, 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 β_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 β_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 $\mathfrak{c}_K(x)$ can be recovered from the fact (Lemma 6.16) that $\mathfrak{c}_K(x)$ lies in the kernel of N.

REMARK 11.5. Under the same hypotheses on β, 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 $\mathrm{im}\, C_v$ much more quickly in practice. The method consists of two parts: computing an upper bound on $\#\,\mathrm{im}\, C_v$ (or its exact value), and computing lower bounds on the group $\mathrm{im}\, C_v$, and hoping that the sizes match. Suppose that $A = J$ and ϕ is multiplication-by-n on J. To compute an upper bound on $\#\,\mathrm{im}\, C_v$:

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

- Calculate the action of the decomposition group $\mathrm{Gal}(k_{v,s}/k_v)$ on Δ.
- Using this, compute the exact sequence

$$0 \longrightarrow J[n](k_v) \longrightarrow E^\vee(k_v) \xrightarrow{q} R^\vee(k_v) \tag{24}$$

  of finite groups.
- From this, compute $\#J[n](k_v)$.
- Substitute this into the formula

$$\#\frac{J(k_v)}{nJ(k_v)} = \|n\|_v^{-\dim J}\#J[n](k_v), \tag{25}$$

  where $\| \ \|_v$ is the v-adic absolute value normalized so that for all $a \in \mathcal{O}_v$ we have $\|a\|_v = (\mathcal{O}_v : a\mathcal{O}_v)^{-1}$ (this is a variant of [29, Proposition 12.10]).
- We obtain the bound $\#\operatorname{im} C_v \leqslant \#J(k_v)/nJ(k_v)$, since C_v factors through $J(k_v)/nJ(k_v)$.
- If $q\colon E^\vee(k_v) \to R^\vee(k_v)$ is surjective, a condition that can be checked using (24), then (19) shows that α_v is injective and $\#\operatorname{im} C_v = \#J(k_v)/nJ(k_v)$.

To compute lower bounds on $\operatorname{im} C_v$:

- 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 $N_{K/k_v}(\mathfrak{c}_K(x))$ 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 nonhyperelliptic $g = 3$ case of Example 6.9(iv). Many of the results about smooth plane quartics we require were established already before 1900. See [33, page 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 nonhyperelliptic 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 $\widehat{\mathbb{P}}^2$ be the dual projective space, with homogeneous coordinates u, v, w; its points correspond to lines in $\mathbb{P}^2$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

DEFINITION 12.1. A *bitangent* to X_s is a line $l \subset \mathbb{P}^2_{k_s}$ such that the intersection $l.X$ is $2\beta_l$ for some $\beta_l \in \operatorname{Div} X_{k_s}$.

Given a bitangent l, the line bundle $\mathscr{L}_l$ associated to β_l is an odd theta characteristic on X_s. The bitangents to X_s form a 28-element $\mathcal{G}$-set Δ in bijection with the $\mathcal{G}$-set $\mathscr{T}_{\mathrm{odd}}$ of Section 5.1 [**16**, page 289]. Alternatively, we may view Δ as a finite étale subscheme of $\widehat{\mathbb{P}}^2$, and the collection $(\mathscr{L}_l)$ as a line bundle $\mathscr{L}$ on $X \times \Delta$. Then $(2, \Delta, \mathscr{L})$ is isomorphic to the fake descent setup in Example 6.9(iv) with $g = 3$. The isogeny $\phi\colon A \to J$ of Section 6.4 is $[2]\colon J \to J$.

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* $(\operatorname{Pic} X_s/\langle\omega\rangle)[2]$.

(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) $\Longleftrightarrow$ (ii) Considering degrees shows that the odd theta characteristics sum to 0 in $(\operatorname{Pic} X_s/\langle\omega\rangle)[2]$ if and only if they sum to $\omega^{\otimes 2}$ in $\operatorname{Pic} X_s$.

(iii) $\Longrightarrow$ (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) $\Longrightarrow$ (iii) Equivalently, we must show that $\Gamma(\mathbb{P}^2, \mathscr{O}(2)) \to \Gamma(X, \mathscr{O}_X(2))$ is surjective. This is true, since the cokernel is contained in $H^1(\mathbb{P}^2, \mathscr{O}(-4+2))$, which is 0. $\square$

A 4-element set $\{l_1, \ldots, l_4\}$ satisfying the equivalent 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 (Δ, Σ) 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, $\#\Sigma = 315$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

12.3. $\mathbf{Sp_6(\mathbb{F}_2)}$-modules. If we chose a bijection between Δ and $\{1, \ldots, 28\}$, then the image G of $\mathcal{G} \to \operatorname{Aut} \Delta$ 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 (Δ, Σ) and a fixed incidence structure $(\boldsymbol{\Delta}, \boldsymbol{\Sigma})$, so that G is identified with a subgroup of $\operatorname{Aut}(\boldsymbol{\Delta}, \boldsymbol{\Sigma})$, which by Proposition 5.4 is a specific copy of $\mathrm{Sp}_6(\mathbb{F}_2)$ in S_{28}. Changing *this* isomorphism changes G only up to $\mathrm{Sp}_6(\mathbb{F}_2)$-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 $(\boldsymbol{\Delta}, \boldsymbol{\Sigma})$ directly from the group $\mathrm{Sp}_6(\mathbb{F}_2)$:

LEMMA 12.3.

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

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

Proof. Direct computation using `Magma` [20]. □

Let $\boldsymbol{\Gamma}$ be the image of the map

$$\begin{aligned} \binom{\boldsymbol{\Delta}}{2} &\longrightarrow \binom{\boldsymbol{\Delta}}{12} \\ \pi &\longmapsto \bigcup \{\sigma \in \boldsymbol{\Sigma} : \pi \subset \sigma\}. \end{aligned}$$

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

LEMMA 12.4. *The* $\mathrm{Sp}_6(\mathbb{F}_2)$*-submodules of* $\mathbb{F}_2^{\boldsymbol{\Delta}}$ *are*

$$0 \subset \mathbf{1} \subset \widetilde{\mathbf{J}} \subset \mathbf{R} \subset \mathbf{E} \subset \mathbb{F}_2^{\boldsymbol{\Delta}},$$

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. □

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

COROLLARY 12.5. *Let X be a smooth plane quartic. Let Δ be its set of bitangents. Let Σ be its set of syzygetic quadruples. Construct E and R from the fake descent setup as in Section 6.3. Then there exists an isomorphism $(\Delta, \Sigma) \simeq (\boldsymbol{\Delta}, \boldsymbol{\Sigma})$ of incidence structures, and any such isomorphism induces a homomorphism $\rho\colon \mathcal{G} \to \mathrm{Sp}_6(\mathbb{F}_2)$ and $\mathcal{G}$-equivariant isomorphisms $E \simeq \mathbf{E}$, $R \simeq \mathbf{R}$, and $J[2] \simeq \ker(\mathbf{E}^\vee \to \mathbf{R}^\vee)$, where $\mathcal{G}$ acts on the $\mathrm{Sp}_6(\mathbb{F}_2)$-modules via ρ.*

Proof. The isomorphism $(\Delta, \Sigma) \simeq (\boldsymbol{\Delta}, \boldsymbol{\Sigma})$ exists because of the uniqueness in Lemma 12.3. The $\mathcal{G}$-action on Δ must respect Σ, so we get

$$\mathcal{G} \longrightarrow \mathrm{Aut}(\Delta, \Sigma) \simeq \mathrm{Aut}(\boldsymbol{\Delta}, \boldsymbol{\Sigma}) = \mathrm{Sp}_6(\mathbb{F}_2).$$

The induced isomorphism $\mathbb{F}_2^{\Delta} \to \mathbb{F}_2^{\boldsymbol{\Delta}}$ sends E to $\mathbf{E}$ and R to $\mathbf{R}$ because by Lemma 12.4 there is at most one submodule of each dimension. By (14), we have

$$J[2] \simeq \ker\left(E^\vee \to R^\vee\right) \simeq \ker(\mathbf{E}^\vee \to \mathbf{R}^\vee). \qquad \square$$

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 Δ as a subscheme in $\widehat{\mathbb{P}}^2_k$.

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

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

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

Proof.

(a) We describe Δ as a subscheme of $\widehat{\mathbb{P}}^2$ by describing its intersection with each standard affine patch of $\widehat{\mathbb{P}}^2$. For example, to compute the part of Δ in the patch whose points correspond to lines $l\colon ux + vy + wz = 0$ 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 $(a_0 s^2 + a_1 st + a_2 t^2)^2$ for indeterminate

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 Δ. For each, the condition that a conic Q in $\mathbb{P}^2$ satisfies $Q.X \geqslant \beta_{l_1} + \beta_{l_2} + \beta_{l_3}$ amounts to linear conditions on the coefficients of a homogeneous equation of Q; if such a Q exists, it is unique and can be found by linear algebra over F, and we then 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 $\{l_1, \ldots, l_4\}$.

(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 $\mathrm{Gal}(F/k)$ on Δ. Using (c), we translate this into an action of $\mathrm{Gal}(F/k)$ on $\boldsymbol{\Delta}$. The image of $\mathrm{Gal}(F/k) \to \mathrm{Aut}\,\boldsymbol{\Delta}$ is $\mathrm{im}\,\rho$. □

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 $\mathbb{P}^n_k$ 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 [9]. We fix the sign by decreeing that $I_{27}(x^4 + y^4 + z^4) > 0$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Over a ring in which $\deg g$ is invertible, the discriminant of g agrees, up to a unit, with the resultant $R(g)$ of $\partial g/\partial x$, $\partial g/\partial y$, $\partial g/\partial z$ (cf. [14, Ch. 13, Section 1]), for which an algorithm is given in [32, Section 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 $\mathbb{Z}_2$ (for example, take $g = x^3y + y^3z + z^3x$); 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. [14, Ch. 13, Proposition 1.7] and [8, Section 5, Définition 4 and Exemple 3]).

An algorithm for computing $I_{27}(g)$ was implemented by Christophe Ritzenthaler, and included by D. Kohel in his `Magma` package `Echidna` [18]. 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 $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$ 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 $\mathcal{S} \subset \Omega_k$ 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 $\widetilde{L(2, \mathcal{S})}$.

(5) Determine the image G of $\mathcal{G} \to \mathrm{Aut}\,\Delta$ as a subgroup of $\mathrm{Sp}_6(\mathbb{F}_2)$ up to $\mathrm{Sp}_6(\mathbb{F}_2)$-conjugacy.

(6) Choose a finite set $\mathcal{T} \subset \Omega_k$. For each $v \in \mathcal{T}$,

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

(a) Determine the decomposition group D_v as a subgroup of G up to G-conjugacy.

(b) Determine $\operatorname{im} C_v$.

(7) Compute

$$S'_{\mathcal{T}} = \left\{ \delta \in \widetilde{L(2,\mathcal{S})} : N_{L/k}(\delta) = 1 \in \frac{k^\times}{k^{\times 2}} \text{ and } \operatorname{Res}_v \delta \in \operatorname{im} C_v \text{ for all } v \in \mathcal{T} \right\}.$$

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

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

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

Let θ 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 θ 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 θ was obtained by projecting a degree 28 subscheme of $\mathbb{P}^2$ onto $\mathbb{P}^1$, there are probably primes introduced into $\operatorname{Disc} \mathcal{O}$ that do not divide $\operatorname{Disc} \mathcal{O}_L$. In practice, these primes can easily be of size 10^{100}, so even finding them in $\operatorname{Disc} \mathcal{O}$ may involve a challenging factorization.

Here are two ways to circumvent this problem:

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

(1) Compute the discriminant $I_{27}(g)$ of the quartic form as in Section 12.5, and factor it. If p is an odd 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 $g(x, y, z) \pmod p$, so $p \nmid \operatorname{Disc} \mathcal{O}_L$. In other words, the set of odd prime factors of $I_{27}(g)$ is an upper bound for the set of odd prime factors of $\operatorname{Disc} \mathcal{O}_L$. `Magma`'s routine `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 ∞.

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 [**5**, Section 9.6, Theorem 1] to compute $c_p(J)$. `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 Φ; 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 $I_{27}(g)$. Then $\operatorname{Proj} \mathbb{Z}_p[x, y, z]/(g)$ 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 $\mathcal{S}$.

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

Next, since $k = \mathbb{Q}$, we have $\mathrm{Cl}(\mathcal{O}_{\mathcal{S}}) = 0$, so (18) implies

$$\widetilde{L(2,\mathcal{S})} = \operatorname{coker}\left(\mathcal{O}_{\mathcal{S}}^{\times}/\mathcal{O}_{\mathcal{S}}^{\times 2} \to \mathcal{O}_{L,\mathcal{S}}^{\times}/\mathcal{O}_{L,\mathcal{S}}^{\times 2}\right).$$

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

(A) find $\mathcal{S}$ such that $\mathrm{Cl}(\mathcal{O}_{L,\mathcal{S}})[2] = 0$; and

(B) compute bases for $\mathcal{O}_{\mathcal{S}}^{\times}/\mathcal{O}_{\mathcal{S}}^{\times 2}$ and $\mathcal{O}_{L,\mathcal{S}}^{\times}/\mathcal{O}_{L,\mathcal{S}}^{\times 2}$.

Current methods for solving problem (A) involve computing the whole class group $\mathrm{Cl}(\mathcal{O}_{L,\mathcal{S}})$. Doing this unconditionally requires computation up to the Minkowski constants of the fields L_i with product L, which requires running time polynomial in $\operatorname{Disc}\mathcal{O}_{L_i}$; in the case where L is a degree 28 field, it is rare that $\operatorname{Disc}\mathcal{O}_L$ 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 $\mathcal{O}_{L,\mathcal{S}}^{\times}$ 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 $\mathcal{S}$-unit theorem yields $\dim_{\mathbb{F}_2} \mathcal{O}_{L,\mathcal{S}}^{\times}/\mathcal{O}_{L,\mathcal{S}}^{\times 2} = \#\mathcal{S}$ in advance, so if generators are constructed conditionally, they can be verified without difficulty.

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

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

12.6.6. Determine the global and local Galois actions on Δ. We have two goals:

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

(B) For each $v \in \mathcal{T}$, 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 $\mathcal{G}$ and $\mathcal{G}_{k_v}$ can be computed as submodules and subquotients of $\mathbb{F}_2^{\Delta}$, as in Section 12.3.

`Magma` shows that there are 1369 conjugacy classes of subgroups in $\mathrm{Sp}_6(\mathbb{F}_2)$ to distinguish. Here are some methods that can be applied (with varying degrees of success) toward determining the image G_K of $\mathcal{G}_K \to \mathrm{Sp}_6(\mathbb{F}_2)$ (up to $\mathrm{Sp}_6(\mathbb{F}_2)$-conjugacy) for a field K:

- *Splitting field.* If a splitting field of Δ over K is of small enough degree, then Lemma 12.6(d) is practical. But in the worst case, the splitting degree is $\#\,\mathrm{Sp}_6(\mathbb{F}_2) = 1451520$.

- *Orbit sizes.* Factoring $h(x)$ over K determines the orbit sizes of G_K; this already cuts the number of possibilities from 1369 down to at most 107 (there are 107 conjugacy classes for which the orbit sizes are 4, 8, 16). Factoring $h(x)$ over the fields obtained by adjoining one root of (one factor of) $h(x)$ determines the orbit sizes 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 $\mathrm{Sp}_6(\mathbb{F}_2)$ up to $\mathrm{Sp}_6(\mathbb{F}_2)$-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 $\mathrm{Sp}_6(\mathbb{F}_2)$, 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) *Nonarchimedean 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 $p \nmid \#\,\mathrm{Sp}_6(\mathbb{F}_2)$, so $P = \{1\}$, and G_K is metacyclic; there are only 214 conjugacy classes of metacyclic subgroups of $\mathrm{Sp}_6(\mathbb{F}_2)$, and the largest such subgroup has order 60, which is about the largest degree for which the splitting field method is easily

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 [12, 13, 39]. 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 $\mathrm{Sp}_6(\mathbb{F}_2)$ up to $\mathrm{Sp}_6(\mathbb{F}_2)$-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 $L_v^\times/L_v^{\times 2}k_v^\times$ form a basis of $\operatorname{im} C_v$. We follow the approach in Section 11.

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

$$\frac{u_\theta x + v_\theta y + w_\theta z}{u_0 x + v_0 y + w_0 z}$$

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

$$\#\frac{J(k_v)}{2J(k_v)} = \begin{cases} \#J[2](k_v) & \text{if } v \neq 2, \\ 8\#J[2](k_v) & \text{if } v = 2. \end{cases} \tag{26}$$

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

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

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

(i) $S'_{\mathcal{T}}$ may be larger than $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$.

(ii) $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$ may fail to be contained in $\alpha(H^1(k, J[2]))$ (both are subgroups of $H^1(k, E^\vee)$).

(iii) If $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J) \subseteq \alpha(H^1(k, J[2]))$, then α induces a map $\mathrm{Sel}^2(J) \to \mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$ (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 $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J) = S_{\mathcal{T}}$, 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 $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J) \subseteq \alpha(H^1(k, J[2]))$ follows if $Ш^1(k, R^\vee) = 0$, and Proposition 8.3 gives an upper bound on $Ш^1(k, R^\vee)$ that is often 0. More precisely, this upper bound is 0 for 1103 of the subgroup classes of $\mathrm{Sp}_6(\mathbb{F}_2)$. Any group in one of the remaining 266 classes has a small orbit in Σ, of size at most 15, so the ideas of Appendix A are probably practical. Furthermore, in all these 266 cases, $J[2]$ is reducible, so there are nontrivial isogenies available for descent computations.

(iii) In order to estimate the kernels and cokernels of $\mathrm{Sel}^2(J) \to \mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$, 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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

$$\begin{tikzcd} 0 \arrow[r] & J[2](k) \arrow[r] \arrow[d, hook] & E^\vee(k) \arrow[r, "q"] \arrow[d, hook] & R^\vee(k) \arrow[d, hook] \\ 0 \arrow[r] & J[2](k_v) \arrow[r] & E^\vee(k_v) \arrow[r, "q"] & R^\vee(k_v). \end{tikzcd}$$

Let κ'_v be the map $\mathcal{K} = \ker\alpha \to \ker\alpha_v$ implicit in (22), which can be identified with

$$\frac{R^\vee(k)}{qE^\vee(k)} \longrightarrow \frac{R^\vee(k_v)}{qE^\vee(k_v)},$$

and hence computed. The map in (22) we are really interested in is the map

$$\kappa_v \colon \mathcal{K} = \ker\alpha \longrightarrow W_v := \frac{\ker\alpha_v}{\ker\alpha_v \cap \operatorname{im}\gamma_v},$$

which factors through κ'_v. We computed $\#J(k_v)/2J(k_v)$ and $\#\operatorname{im} C_v$. Dividing gives the size of $\ker C_v \simeq \gamma_v(\ker C_v) = \ker\alpha_v \cap \operatorname{im}\gamma_v$, so in some cases we may have sufficient information to deduce κ_v and piece together $\kappa = \prod_v \kappa_v$ and its kernel and cokernel. Even if we can determine $\#\operatorname{coker}\kappa$, however, it is only an upper bound on $\#\operatorname{coker}(\mathrm{Sel}^2(J) \to \mathrm{Sel}^\alpha_{\mathrm{fake}}(J))$ (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

$$N_{L[x,y,z]/k[x,y,z]}(u_\theta x + v_\theta y + w_\theta z) \equiv c r_{14}(x, y, z)^2 \pmod{g(x, y, z)}. \tag{27}$$

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 ℓ 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 $\mathcal{S} \subset \Omega_k$ be a finite set of places containing the archimedean places, the places of residue*

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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* $\operatorname{im} C_f \subset \widetilde{L(2, \mathcal{S})}$.

Proof. Let $v \in \Omega_k \setminus \mathcal{S}$. 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 $(u_\theta : v_\theta : w_\theta) \in \widehat{\mathbb{P}}^2(L)$ extends to a point in $\widehat{\mathbb{P}}^2(\mathcal{O}_{L,v})$. Given $Q \in \Delta(k_{v,u}) = \Delta(k_s)$, we can specialize u_θ 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 $L \otimes k_{v,u}$. □

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 $\mathcal{T} \subset \Omega_k$, we compute

$$S'_{\mathcal{T}} := \left\{ \delta \in \widetilde{L(2, \mathcal{S})} : N(\delta) \in ck^{\times 2} \text{ and } \delta_v \in C_{f,v}(X(k_v)) \text{ for all } v \in \mathcal{T} \right\},$$

which contains $\operatorname{Sel}^f_{\text{fake}}(X)$. In particular, if $S'_{\mathcal{T}}$ 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. □

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\mathcal{G}_{\mathbb{Q}}$ acts transitively on the bitangents. We compute $\mathcal{O}_L$ and find that $\operatorname{Disc} \mathcal{O}_L = 2^{42} \cdot 29^6 \cdot 163^6$.

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 36984868, 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 $\mathrm{Sp}_6(\mathbb{F}_2)$ 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

$$\begin{array}{ccccc} 0 & \longrightarrow & J[2](\mathbb{Q}) & \longrightarrow & E^\vee(\mathbb{Q}) & \longrightarrow & R^\vee(\mathbb{Q}) \\ & & \| & & \| & & \| \\ & & 0 & & 0 & & \mathbb{F}_2. \end{array} \tag{28}$$

Step 6. Taking $\mathcal{T} = \emptyset$ (that is, doing no local computations with X) yields the upper bound $S'_\emptyset \simeq (\mathbb{Z}/2\mathbb{Z})^{13}$ on $\mathrm{Sel}^\alpha_{\mathrm{fake}}(J)$. 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 Δ. 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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

$$\begin{array}{ccccc} 0 \longrightarrow & J[2](\mathbb{Q}_2) & \longrightarrow & E^\vee(\mathbb{Q}_2) & \xrightarrow{q} R^\vee(\mathbb{Q}_2) \\ & \| & & \| & \| \\ & 0 & & 0 & \mathbb{F}_2. \end{array} \tag{29}$$

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

$$W_2 \simeq \ker\alpha_2 \simeq \frac{R^\vee(\mathbb{Q}_2)}{qE^\vee(\mathbb{Q}_2)} \simeq \mathbb{Z}/2\mathbb{Z}, \tag{30}$$

in which the last isomorphism follows from (29).

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

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

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

By (28) and Corollary 10.15, $\mathrm{Sel}^2(J)$ 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 $\mathcal{K} \to W_2$ is $R^\vee(\mathbb{Q})/qE^\vee(\mathbb{Q}) \to R^\vee(\mathbb{Q}_2)/qE^\vee(\mathbb{Q}_2)$, which is an isomorphism, so κ is injective; thus $\mathrm{Sel}^2(J) = 0$ by Theorem 10.14.

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

PROPOSITION 12.16. *If X is the curve*

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

in $\mathbb{P}^2_{\mathbb{Q}}$, then $J(\mathbb{Q}) = \langle[(0:1:0) - (0:0:1)]\rangle \simeq \mathbb{Z}/51\mathbb{Z}$ and

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Proof. Since $\mathrm{Sel}^2(J) = 0$, the group $J(\mathbb{Q})$ is finite and of odd order. Reduction modulo 3 injects $J(\mathbb{Q})_{\mathrm{tors}}$ 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 $[(0:1:0)-(0:0:1)]$ is of exact order 51 in $J(\mathbb{Q})$. Thus $J(\mathbb{Q}) \simeq \mathbb{Z}/51\mathbb{Z}$.

Finally, we determine $X(\mathbb{Q})$. The Abel–Jacobi map $X \to J$ 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. □

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 $J(\mathbb{Q})_{\mathrm{tors}}$ 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 $J(\mathbb{Q})_{\mathrm{tors}} = 0$. 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 $\mathrm{rk}\, J(\mathbb{Q}) \geqslant 1$.

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

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 the groups $L(2,\mathcal{S}) \simeq (\mathbb{Z}/2\mathbb{Z})^{17}$ and $\widetilde{L(2,\mathcal{S})} \simeq (\mathbb{Z}/2\mathbb{Z})^{15}$.

Step 5. By computing the Frobenius action at 5 and 7, we find that $G \simeq \mathrm{Sp}_6(\mathbb{F}_2)$. 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 $S'_{\{2\}} \simeq \mathbb{Z}/2\mathbb{Z}$ on $\mathrm{Sel}^{\alpha}_{\mathrm{fake}}(J)$.

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 $\mathrm{Sp}_6(\mathbb{F}_2)$-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 $\#\,\mathrm{im}\, C_2 \leqslant \#J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 8$ (see (26)), but we also find enough points in $X(\mathbb{Q}_2)$ to show that $\#\,\mathrm{im}\, C_2 \geqslant 8$, so $\#\,\mathrm{im}\, C_2 = 8$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

Step 7. We can compute the map

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

explicitly, and we have $\operatorname{im} C_2$; from this we compute that $S'_{\mathcal{T}} = \mathbb{Z}/2\mathbb{Z}$.

Since $R^\vee(\mathbb{Q}) = 0$, Corollary 10.15 implies that $\mathrm{Sel}^2(J) \to \mathrm{Sel}^\alpha_{\mathrm{fake}}(J)$ is injective. Thus

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow \mathrm{Sel}^2(J) \hookrightarrow \mathrm{Sel}^\alpha_{\mathrm{fake}}(J) \subset S'_{\mathcal{T}} = \mathbb{Z}/2\mathbb{Z},$$

so $\operatorname{rk} J(\mathbb{Q}) \leqslant 1$. 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

$$\begin{aligned} X(\mathbb{Q}) = \{&(1:1:0), (-1:0:1), (0:-1:1), (0:1:0),\\ &(1:1:-1), (0:0:1), (1:0:0), (1:4:-3)\}. \end{aligned}$$

Proof. We already proved that $J(\mathbb{Q}) \simeq \mathbb{Z}$. To determine $X(\mathbb{Q})$ we use an explicit version of the method of Chabauty and Coleman over $\mathbb{Q}_3$ (see [21] for a survey).

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 $\operatorname{rk} J(\mathbb{Q}) = 1$ and $\dim J = 3$, there is a 2-dimensional subspace $V \subset H^0(X_{\mathbb{Q}_3}, \Omega^1)$ such that $\int_P^{P'} \omega = 0$ 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 $V = \{\omega : \int_{P_0}^{P_1} \omega = 0\}$. We compute this integral (to some 3-adic precision) for ω 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 linear 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 ω_1 corresponding to $(21\,262 + O(3^{10}))x - y$ and ω_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 ω_1, ω_2 is nonvanishing at Q, so by [40, Proposition 6.3], 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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

$\int_{P_0}^{P} \omega_1 = \int_{P_0}^{P} \omega_2 = 0$; 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 $X_{\mathrm{split}}(13)$ (respectively, $X_{\mathrm{nonsplit}}(13)$) be the modular curve of level 13 over $\mathbb{Q}$ corresponding to the normalizer of a split (respectively, nonsplit) Cartan subgroup of $\mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z})$. These are nonhyperelliptic curves of genus 3, and it turns out [2, 3] that both are isomorphic to the smooth plane quartic curve

$$X\colon x^3y+x^3z-2x^2y^2-x^2yz+xy^3-xy^2z+2xyz^2-xz^3-2y^2z^2+3yz^3=0. \quad (31)$$

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 $J(\mathbb{Q})_{\mathrm{tors}}$ injects into both groups, $J(\mathbb{Q})_{\mathrm{tors}} = 0$. One can verify that the three 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 $\operatorname{rk} J(\mathbb{Q}) \geqslant 3$.

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

Steps 1 and 2. The algebra L is a degree 28 number field with $\operatorname{Disc} \mathcal{O}_L = 2^{42} \cdot 13^{24}$.

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 8158 071 456. 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 the groups $L(2, \mathcal{S}) \simeq (\mathbb{Z}/2\mathbb{Z})^{17}$ and $\widetilde{L(2, \mathcal{S})} \simeq (\mathbb{Z}/2\mathbb{Z})^{15}$.

Step 5. Since L is a field, G acts transitively on the bitangents. There are 18 subgroups of $\mathrm{Sp}_6(\mathbb{F}_2)$ up to conjugacy with that property. The Fieker–Klüners

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

implementation in `Magma` for finding Galois groups yields $\#G = 504$. This determines G uniquely up to conjugacy.

This information allows us to compute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & J[2](\mathbb{Q}) & \longrightarrow & E^\vee(\mathbb{Q}) & \longrightarrow & R^\vee(\mathbb{Q}) \\ & & \| & & \| & & \| \\ & & 0 & & 0 & & \mathbb{F}_2^2. \end{array} \tag{32}$$

Steps 6 and 7. It will turn out that taking $\mathcal{T} = \{2\}$ is enough to obtain the upper bound $S'_{\{2\}} \simeq \mathbb{Z}/2\mathbb{Z}$ on $\mathrm{Sel}^\alpha_{\mathrm{fake}}(J)$. 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 $\mathrm{Sp}_6(\mathbb{F}_2)$. We obtain $\#D_2 = 56$ and

$$\begin{array}{ccccccc} 0 & \longrightarrow & J[2](\mathbb{Q}_2) & \longrightarrow & E^\vee(\mathbb{Q}_2) & \longrightarrow & R^\vee(\mathbb{Q}_2) \\ & & \| & & \| & & \| \\ & & 0 & & 0 & & \mathbb{F}_2^2. \end{array} \tag{33}$$

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

$$S'_\emptyset \longrightarrow \frac{(L \otimes \mathbb{Q}_2)^\times}{(L \otimes \mathbb{Q}_2)^{\times 2}\mathbb{Q}_2^\times}$$

is injective. It follows that $\#S'_{\mathcal{T}} \leqslant \#\operatorname{im} C_2 \leqslant 2^3$. Thus $\#\mathrm{Sel}^\alpha_{\mathrm{fake}}(J) \leqslant 2^3$. By Corollary 10.15 and (32), this implies $\#\mathrm{Sel}^2(J) \leqslant 2^5$, so $\operatorname{rk} J(\mathbb{Q}) \leqslant 5$.

We now present two approaches to improve this to $\operatorname{rk} J(\mathbb{Q}) \leqslant 3$. The first is to use the isomorphism $\operatorname{End} J \simeq \mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ of [3, Proposition 2.4] to obtain that $\operatorname{rk} J(\mathbb{Q})$ is a multiple of 3, which improves the bound to $\operatorname{rk} J(\mathbb{Q}) \leqslant 3$. The second is to follow Section 11.1 to compute that $\#\operatorname{im} C_2 = 2$, which can be used as follows. By the same argument as in the previous paragraph, $\#\operatorname{im} C_2 = 2$ implies $\#\mathrm{Sel}^\alpha_{\mathrm{fake}}(J) \leqslant 2^1$ and $\#\mathrm{Sel}^2(J) \leqslant 2^3$. On the other hand, $3 \leqslant \operatorname{rk} J(\mathbb{Q}) \leqslant \dim_{\mathbb{F}_3} \mathrm{Sel}^2(J)$, so equality holds everywhere in this paragraph. In particular, if $Ш(J)$ is the Shafarevich–Tate group of J, then $Ш(J)[2] = 0$. We have proved the following:

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

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.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\mathrm{Sel}^f_{\mathrm{fake}}(X)$ for a smooth plane quartic X.

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

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

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

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 $p \geqslant 37$. 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 $\mathcal{S} = \{\infty, 2, 5, 1361, 97103\}$. It is straightforward to find $(u_\theta, v_\theta, w_\theta)$ satisfying the hypotheses of Lemma 12.13 for $\mathcal{S}$. We find that $\mathrm{Disc}(\mathcal{O}_L) = 2^{30} \cdot 5^{10} \cdot 1361^6 \cdot 97103^6$ and the Minkowski bound exceeds 10^{22}, so determining $\mathrm{Cl}(\mathcal{O}_{L,\mathcal{S}})$ unconditionally is out of the question. Conditional on the Generalized Riemann hypothesis for L, which we assume from now on, we find that $\mathrm{Cl}(\mathcal{O}_{L,\mathcal{S}}) = \mathbb{Z}/2\mathbb{Z}$ and we also find $\mathcal{O}^\times_{L,\mathcal{S}}/\mathcal{O}^{\times 2}_{L,\mathcal{S}}$. This leads to explicit generators of $L(2, \mathcal{S}) \simeq (\mathbb{Z}/2\mathbb{Z})^{41}$ and $\widetilde{L(2, \mathcal{S})} \simeq (\mathbb{Z}/2\mathbb{Z})^{36}$. We compute $c = -1$. For $\mathcal{T} = \{2, 1361\}$, we find $S'_{\mathcal{T}} = \emptyset$, so $X(\mathbb{Q}) = \emptyset$. □

Appendix A. Determining the ϕ-Selmer group directly

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

The fundamental idea behind a true descent setup is to replace the Galois module $\widehat{J}[\widehat{\phi}]$ whose cohomology we want by a permutation module $(\mathbb{Z}/n\mathbb{Z})^\Delta$ whose cohomology we can compute. The discrepancies between $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$ and $\mathrm{Sel}^\phi(J)$ come from the noninjectivity of $(\mathbb{Z}/n\mathbb{Z})^\Delta \to \widehat{J}[\widehat{\phi}]$. In this section we deal with the noninjectivity by finding another permutation module $(\mathbb{Z}/n\mathbb{Z})^{\Delta'}$ that surjects onto the kernel. This allows us to describe, in terms of efficiently computable objects, a subgroup $H \subset H^1(k, A[\phi])$ that contains $\mathrm{Sel}^\phi(J)$; see Propositions A.12 and A.15. Theorem A.16 summarizes the computational tasks we need to be able to perform in order to compute the Selmer group explicitly via this method.

A.1. Correspondences. A *correspondence* $\Delta \overset{\tau}{\dashrightarrow} \Delta'$ between finite $\mathcal{G}$-sets is a $\mathcal{G}$-homomorphism $\mathbb{Z}^\Delta \to \mathbb{Z}^{\Delta'}$. Given a $\mathcal{G}$-module M and $\Delta \overset{\tau}{\dashrightarrow} \Delta'$, we define

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

homomorphisms $\tau^*\colon M^{\Delta'} \to M^{\Delta}$ and $\tau_*\colon M^{\Delta} \to M^{\Delta'}$ as follows. Restricting the composition pairing

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta'}, M) \times \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, M)$$

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

EXAMPLE A.1. Suppose that X is a nice k-variety. If we apply the previous remark to the étale group scheme M such that $M(k_s)$ is the $\mathcal{G}_k$-module $\mathrm{Div}\, X_s$, then $M^{\Delta}(k) = \mathrm{Div}(X \times \Delta)$, and we obtain $\tau_*\colon \mathrm{Div}(X \times \Delta) \to \mathrm{Div}(X \times \Delta')$. Similarly we obtain $\tau_*\colon k(X \times \Delta)^\times \to k(X \times \Delta')^\times$.

LEMMA A.2. *Let M be a finite $\mathcal{G}$-module, and let n be a positive integer such that $nM = 0$.*

(a) *There exists a finite $\mathcal{G}$-set Δ with a surjection $(\mathbb{Z}/n\mathbb{Z})^{\Delta} \twoheadrightarrow M$.*

(b) *There exists a finite $\mathcal{G}$-set Δ with an injection $M \hookrightarrow \mu_n^{\Delta}$ (here we assume* $\mathrm{char}\, k \nmid n$*).*

Proof. For (a), take $\Delta = M$: the identity $M \to M$ induces $\mathbb{Z}^M \twoheadrightarrow M$, which factors through $(\mathbb{Z}/n\mathbb{Z})^M$ since $nM = 0$. Applying (a) to $M^\vee := \mathrm{Hom}_{\mathbb{Z}}(M, k_s^\times)$ and applying $\mathrm{Hom}_{\mathbb{Z}}(-, k_s^\times)$ yields (b). □

LEMMA A.3. *Let n be a positive integer. Each of the four homomorphisms*

$$\begin{aligned}
&\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'}) \xrightarrow{\tau \mapsto \tau_*} \mathrm{Hom}_{\mathbb{Z}}((\mathbb{Z}/n\mathbb{Z})^{\Delta}, (\mathbb{Z}/n\mathbb{Z})^{\Delta'}),\\
&\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'}) \xrightarrow{\tau \mapsto \tau^*} \mathrm{Hom}_{\mathbb{Z}}((\mathbb{Z}/n\mathbb{Z})^{\Delta'}, (\mathbb{Z}/n\mathbb{Z})^{\Delta}),\\
&\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'}) \xrightarrow{\tau \mapsto \tau_*} \mathrm{Hom}_{\mathbb{Z}}(\mu_n^{\Delta}, \mu_n^{\Delta'}),\\
&\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'}) \xrightarrow{\tau \mapsto \tau^*} \mathrm{Hom}_{\mathbb{Z}}(\mu_n^{\Delta'}, \mu_n^{\Delta})
\end{aligned}$$

is surjective with kernel $n\,\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\Delta}, \mathbb{Z}^{\Delta'})$ (in the last two we assume $\mathrm{char}\, k \nmid n$*).*

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

A.2. Determining the Selmer group. Set $\widetilde{\mathbb{G}_m^\Delta} := \mathbb{G}_m^\Delta$ for a true descent setup, and $\widetilde{\mathbb{G}_m^\Delta} := \mathbb{G}_m^\Delta/\mu_n$ for a fake descent setup.

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

$$(\mathbb{Z}/n\mathbb{Z})^{\Delta'} \longrightarrow E \xrightarrow{\alpha^\vee} \widehat{J}[\widehat{\phi}] \longrightarrow 0 \tag{A.1}$$

and its dual

$$0 \longrightarrow A[\phi] \longrightarrow E^\vee \longrightarrow \mu_n^{\Delta'} \tag{A.2}$$

in which the image of the last map is $R^\vee$.

REMARK A.4. Define Q and q' by the exact sequence

$$0 \longrightarrow R^\vee \longrightarrow \mu_n^{\Delta'} \xrightarrow{q'} Q \longrightarrow 0. \tag{A.3}$$

If $Q(k) = q'\big(\mu_n(L')\big)$ and $Ш^1(k, \mu_n^{\Delta'}) = 0$ (the latter holds if n is prime, by Lemma 8.2), then $Ш^1(k, R^\vee) = 0$, so by Lemma 10.17(b) the first assumption in Corollary 10.16 is satisfied. This gives a simple way of showing that $Ш^1(k, R^\vee)$ vanishes, but the criterion can be weaker than that coming from Section 8.

By Lemma A.3, the composition

$$(\mathbb{Z}/n\mathbb{Z})^{\Delta'} \twoheadrightarrow R \hookrightarrow E \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^{\Delta} \tag{A.4}$$

is τ^* for some correspondence $\Delta \overset{\tau}{\dashrightarrow} \Delta'$. We use τ_* to denote any of several homomorphisms induced by τ; the context will make the meaning clear. In the fake case, $\tau_*\colon \mu_n^\Delta \to \mu_n^{\Delta'}$ kills the diagonal μ_n, because taking duals in (A.4) shows that τ_* factors through $E^\vee = \mu_n^\Delta/\mu_n$. Thus $\tau_*\colon \mathbb{G}_m^\Delta \to \mathbb{G}_m^{\Delta'}$ induces $\tau_*\colon \widetilde{\mathbb{G}_m^\Delta} \to \mathbb{G}_m^{\Delta'}$ in both cases.

Let U be the image of $(\tau_*, n)\colon \mathbb{G}_m^\Delta \to \mathbb{G}_m^{\Delta'} \times \mathbb{G}_m^\Delta$. The last map in (A.2) is induced by $\tau_*\colon \mu_n^\Delta \to \mu_n^{\Delta'}$, so we have a commutative diagram with exact rows and columns

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

$$\begin{tikzcd}
 & & 0 \arrow[d] & \\
 & 0 \arrow[d] & R^\vee \arrow[d] & \\
0 \arrow[r] & A[\phi] \arrow[r] \arrow[d, "\alpha"'] & \widetilde{\mathbb{G}_m^\Delta} \arrow[r, "(\tau_*,n)"] \arrow[d, equal] & U \arrow[r] \arrow[d, "\mathrm{pr}_2"] & 0 \\
0 \arrow[r] & E^\vee \arrow[r] \arrow[d, "q"'] & \widetilde{\mathbb{G}_m^\Delta} \arrow[r, "n"] & \mathbb{G}_m^\Delta \arrow[r] \arrow[d] & 0 \\
 & R^\vee \arrow[d] & & 0 & \\
 & 0 & & &
\end{tikzcd} \tag{A.5}$$

in which $\ker \mathrm{pr}_2$ is identified as $R^\vee$ by the snake lemma. Taking cohomology, we obtain

$$\begin{tikzcd}
 & & R^\vee(k) \arrow[d, hook] & & \\
 & (\widetilde{\mathbb{G}_m^\Delta})(k) \arrow[r, "(\tau_*,n)"] \arrow[d, equal] & U(k) \arrow[r] \arrow[d, "\mathrm{pr}_2"] & H^1(k, A[\phi]) \arrow[r] \arrow[d, "\alpha"'] & H^1(k, \widetilde{\mathbb{G}_m^\Delta}) \arrow[d, equal] \\
E^\vee(k) \arrow[r] & (\widetilde{\mathbb{G}_m^\Delta})(k) \arrow[r, "n"] & L^\times \arrow[r] & H^1(k, E^\vee) \arrow[r] & H^1(k, \widetilde{\mathbb{G}_m^\Delta}).
\end{tikzcd} \tag{A.6}$$

We record the following lemma and corollary for use in Section A.3.

LEMMA A.5. *There exist a finite étale k-scheme Δ'' and a correspondence $\Delta' \overset{\tau'}{\dashrightarrow} \Delta''$ such that*

$$\mu_n^\Delta \xrightarrow{\tau_*} \mu_n^{\Delta'} \xrightarrow{\tau'_*} \mu_n^{\Delta''}$$

is exact. There is another correspondence $\Delta \overset{\tau''}{\dashrightarrow} \Delta''$ such that $\tau' \circ \tau = n\tau''$. Then

$$U = \ker\left(\mathbb{G}_m^{\Delta'} \times \mathbb{G}_m^{\Delta} \longrightarrow \mathbb{G}_m^{\Delta'} \times \mathbb{G}_m^{\Delta''}, \quad (\ell', \ell) \longmapsto \left(\frac{\ell'^n}{\tau_*(\ell)}, \frac{\tau'_*(\ell')}{\tau''_*(\ell)}\right)\right).$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

$$\tau'_*(\zeta') = \frac{\tau'_*(\ell')}{\tau'_*\tau_*(\lambda)} = \frac{\tau'_*(\ell')}{(n\tau'')_*(\lambda)} = \frac{\tau'_*(\ell')}{\tau''_*(\lambda^n)} = \frac{\tau'_*(\ell')}{\tau''_*(\ell)} = 1,$$

which implies that $\zeta' = \tau_*(\zeta)$ for some $\zeta \in \mu_n^{\Delta}$. Then

$$(\ell', \ell) = (\tau_*(\zeta\lambda), (\zeta\lambda)^n) \in U. \qquad \square$$

COROLLARY A.6. *Keeping the notation from Lemma A.5, we have*

$$U(k) = \left\{(\ell', \ell) \in L'^{\times} \times L^{\times} : \tau_*(\ell) = \ell'^n, \tau''_*(\ell) = \tau'_*(\ell')\right\}.$$

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

LEMMA A.7.

(a) *In the true case, $\widetilde{\mathbb{G}_m^{\Delta}}(k)$ is mapped by $\widetilde{\mathbb{G}_m^{\Delta}} \xrightarrow{n} \mathbb{G}_m^{\Delta}$ to $L^{\times n} \subseteq L^{\times}$ and by (τ_*, n) to*

$$\left\{(\tau_*(\ell), \ell^n) : \ell \in L^{\times}\right\} \subseteq U(k). \tag{A.7}$$

(b) *In the fake case, $\widetilde{\mathbb{G}_m^{\Delta}}(k)$ is mapped by $\widetilde{\mathbb{G}_m^{\Delta}} \xrightarrow{n} \mathbb{G}_m^{\Delta}$ to $L^{\times n}k^{\times} \subseteq L^{\times}$ and by (τ_*, n) to*

$$\left\{(\tau_*(\ell)\theta_*(a), \ell^n a) : \ell \in L^{\times}, a \in k^{\times}\right\} \subseteq U(k). \tag{A.8}$$

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

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathbb{G}_m^{\Delta} \times \mathbb{G}_m \xrightarrow{j} \widetilde{\mathbb{G}_m^{\Delta}} \longrightarrow 0$$

with maps induced by $a \mapsto (a, a^{-n})$ and $(\ell, a) \mapsto \ell a^{1/n}$ (the nth root is well-defined modulo μ_n). Taking cohomology shows that j induces a surjection $L^{\times} \times k^{\times} \to \widetilde{\mathbb{G}_m^{\Delta}}(k)$. Following j by $\widetilde{\mathbb{G}_m^{\Delta}} \xrightarrow{n} \mathbb{G}_m^{\Delta}$ yields $(\ell, a) \mapsto \ell^n a$, whose image on k-points is $L^{\times n}k^{\times}$. Following j by $\widetilde{\mathbb{G}_m^{\Delta}} \xrightarrow{(\tau_*, n)} U \subseteq \mathbb{G}_m^{\Delta'} \times \mathbb{G}_m^{\Delta}$ yields $(\ell, a) \mapsto (\tau_*(\ell)\theta_*(a), \ell^n a)$. $\square$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

Define $V := \operatorname{im}\left(\widetilde{\mathbb{G}_m^\Delta}(k) \xrightarrow{(\tau_*,n)} U(k)\right)$, so V is given by (A.7) or (A.8).

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

Proof. In the true case, the composition

$$(\mathbb{Z}/n\mathbb{Z})^{\Delta'} \xrightarrow{\tau^*} (\mathbb{Z}/n\mathbb{Z})^{\Delta} \xrightarrow{\alpha^\vee} \widehat{J}[\widehat{\phi}] \subseteq \operatorname{Pic} X_s$$

is 0 by (A.1), 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:

$$\begin{tikzcd}
\mathbb{Z}^{\Delta'} \arrow[r, "(\tau^*,\theta^*)"] \arrow[d, two heads] & \dfrac{\mathbb{Z}^{\Delta} \times \mathbb{Z}}{\langle (nP, 1) : P \in \Delta\rangle} \arrow[r, "(\beta,-D)"] & \operatorname{Pic} X_s \\
(\mathbb{Z}/n\mathbb{Z})^{\Delta'} \arrow[r, "\tau^*"] & (\mathbb{Z}/n\mathbb{Z})^{\Delta}_{\deg 0} \arrow[r, "\alpha^\vee"] \arrow[u] & \widehat{J}[\widehat{\phi}] \arrow[u, hook]
\end{tikzcd} \tag{A.9}$$

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

$$\left(\sum_P \tau_{P',P} P, \frac{\sum_P \tau_{P',P}}{n}\right),$$

where $\tau_{P',P}$ is the coefficient of P' in $\tau(P) \in \mathbb{Z}^{\Delta'}$. Both paths from $(\mathbb{Z}/n\mathbb{Z})^{\Delta}_{\deg 0}$ to $\operatorname{Pic} X_s$ send $P_1 - P_2$ to the class of $\beta_{P_1} - \beta_{P_2}$. Thus (A.9) commutes. The composition along the bottom row is zero, so the composition along the top row is zero, which is the desired result. □

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

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

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

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

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

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

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

$$\begin{aligned} \tau_*([y, \beta]_D) &= \frac{[y, \tau_*(\beta - \iota_* H)]}{\tau_*(\iota_*(h(y)^{1/n}))} \\ &= \frac{[y, \tau_*(\beta) - \theta_*(nH)]}{\theta_*(h)(y)} \\ &= \frac{[y, \operatorname{div}(r \cdot \theta_*(h))]}{\theta_*(h)(y)} \\ &= r(y). \end{aligned}$$

□

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 $J[n] \twoheadrightarrow A[\phi]$. The third and fourth rows are the same as in (A.5). The two maps from $\mathcal{Z}^0 \times \mathcal{Y}^0$ to U coincide by Lemma A.10. Thus the diagram below commutes:

$$\begin{tikzcd}
0 \arrow[r] \arrow[dd, bend right=60, equal] & A[\phi] \arrow[r] & A \arrow[r, "\phi"] & J \arrow[r] & 0 \\
0 \arrow[r] & \widetilde{J[n]} \arrow[r] \arrow[u] \arrow[d] & \mathcal{Z}^0 \times \mathcal{Y}^0 \arrow[r, "nz+y"] \arrow[u] \arrow[d] & \mathcal{Z}^0 \arrow[r] \arrow[u] \arrow[d, "(r,f)"] \arrow[ddl, bend left=60, "f"] & 0 \\
0 \arrow[r] & A[\phi] \arrow[r] \arrow[d, "\alpha"'] & \widetilde{\mathbb{G}_m^{\Delta}} \arrow[r, "(\tau_*,n)"] \arrow[d, equal] & U \arrow[r] \arrow[d, "\mathrm{pr}_2"] & 0 \\
0 \arrow[r] & E^\vee \arrow[r] & \widetilde{\mathbb{G}_m^{\Delta}} \arrow[r, "n"] & \mathbb{G}_m^{\Delta} \arrow[r] & 0
\end{tikzcd} \tag{A.10}$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{J(k)}{\phi A(k)} \arrow[r, "\gamma"] & H^1(k, A[\phi]) \arrow[dd, equal] & & \\
& \mathcal{Z}^0(X^{\mathrm{good}}) \arrow[u] \arrow[d, "(r,f)"] & & & \\
0 \arrow[r] & \dfrac{U(k)}{V} \arrow[r] \arrow[d, "\mathrm{pr}_2'"] & H^1(k, A[\phi]) \arrow[r] \arrow[d, "\alpha"] & H^1(k, \widetilde{\mathbb{G}_m^{\Delta}}) \arrow[d, equal] \\
0 \arrow[r] & \dfrac{\widetilde{L^\times}}{L^{\times n} k^\times} \arrow[r] & H^1(k, E^\vee) \arrow[r] & H^1(k, \widetilde{\mathbb{G}_m^{\Delta}})
\end{tikzcd} \tag{A.11}$$

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

LEMMA A.11. *We have* $Ш^1(k, \widetilde{\mathbb{G}_m^{\Delta}}) = 0$.

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

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m^{\Delta} \longrightarrow \widetilde{\mathbb{G}_m^{\Delta}} \longrightarrow 0$$

yields an injection $H^1(k, \widetilde{\mathbb{G}_m^{\Delta}}) \hookrightarrow H^2(k, \mu_n)$, which restricts to an injection $Ш^1(k, \widetilde{\mathbb{G}_m^{\Delta}}) \hookrightarrow Ш^2(k, \mu_n)$. But $Ш^2(k, \mu_n) = 0$ 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 (A.11) identifies

$$\big\{h \in H : \rho_v(h) \in (r, f)\big(\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})\big) \text{ for all places } v\big\}$$

with $\mathrm{Sel}^{\phi}(J)$.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$, which in (A.11) for k_v maps to 0 in $H^1(k_v, \widetilde{\mathbb{G}_m^{\Delta}})$. Thus, the image of $\mathrm{Sel}^{\phi}(J) \subseteq H^1(k, A[\phi])$ in $H^1(k, \widetilde{\mathbb{G}_m^{\Delta}})$ lies in $Ш^1(k_v, \widetilde{\mathbb{G}_m^{\Delta}})$, which is 0 by Lemma A.11, so $\mathrm{Sel}^{\phi}(J) \subseteq H$ by (A.11). For $h \in H$, the element $\rho_v(h)$ is in the image of $J(k_v)/\phi A(k_v)$ (or $\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$ as above) if and only if it is in the image of $(r, f)\big(\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})\big)$, by (A.11). □

We now describe the fibers of the map pr_2' in (A.11). This will help us obtain a computable description of $\mathrm{Sel}^{\phi}(J)$: see Proposition A.15 below.

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

$$0 \longrightarrow A[\phi] \longrightarrow E^{\vee} \xrightarrow{\tau_*} \mu_n^{\Delta'} \xrightarrow{q'} Q \longrightarrow 0. \tag{A.12}$$

LEMMA A.13. *Let $\ell \in L^{\times}$ and let ξ be its image in $H^1(k, E^{\vee})$.*

(a) *If ξ lifts to $H^1(k, A[\phi])$, then $\tau_*(\ell)$ is an nth power in L'.*

(b) *Conversely, suppose that $\tau_*(\ell)$ is an nth 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 $\mathcal{G}$-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 ξ is the image of the set $\{(\zeta u, \ell) : \zeta \in Z\}$ under $U(k) \to H^1(k, A[\phi])$.*

  (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 ξ lifts to an element of $H^1(k, A[\phi])$ if and only if $\tau_*(\ell)$ is an nth power in L'.*

Proof. In (A.6), the image of $\mathrm{pr}_2^{-1}(\ell)$ under $U(k) \to H^1(k, A[\phi])$ equals the set $\alpha^{-1}(\xi)$ of lifts of ξ.

(a) If ξ lifts, then there is a pair $(u, \ell) \in U(k)$. By Lemma A.5, $\tau_*(\ell) = u^n$.

(b) (1) First,

$$\left(\frac{\tau_*(\lambda)}{u}\right)^n = \frac{\tau_*(\lambda^n)}{u^n} = \frac{\tau_*(\ell)}{u^n} = 1,$$

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

so $\tau_*(\lambda)/u \in \mu_n^{\Delta'}$. For $\sigma \in \mathcal{G}$,

$$\frac{{}^\sigma w}{w} = \frac{{}^\sigma q'\big(\tau_*(\lambda)/u\big)}{q'\big(\tau_*(\lambda)/u\big)} = q'\Big(\frac{{}^\sigma \tau_*(\lambda)}{\tau_*(\lambda)}\Big) = q'\Big(\tau_*\Big(\frac{{}^\sigma \lambda}{\lambda}\Big)\Big) = 1,$$

since $q' \circ \tau_*$ is trivial and u is $\mathcal{G}$-invariant.

(2) For $\zeta \in \mu_n(L')$, the following are equivalent:

- $(\zeta u, \ell) \in U(k)$;
- there exists $\widetilde{\lambda} \in L_s^\times$ with $\tau_*(\widetilde{\lambda}) = \zeta u$ and $\widetilde{\lambda}^n = \ell$ (by definition of U);
- there exists $\widetilde{\zeta} \in \mu_n(L_s)$ such that $\tau_*(\widetilde{\zeta}) = \zeta u/\tau_*(\lambda)$ (write $\widetilde{\lambda} = \widetilde{\zeta}\lambda$);
- $q'(\zeta u/\tau_*(\lambda))$ is trivial (Equation (A.12) yields $\tau_*(\mu_n(L_s)) = \ker(q')$);
- $q'(\zeta) = q'(\tau_*(\lambda)/u)$;
- $q'(\zeta) = w$ (by definition of w).

(3) By the first sentence of this proof, it suffices to prove the equality $\mathrm{pr}_2^{-1}(\ell) = \{(\zeta u, \ell) : \zeta \in Z\}$. An element of $\mathrm{pr}_2^{-1}(\ell)$ has the form (u', ℓ) for some $u' \in L'$, and $(u')^n = \tau_*(\ell) = u^n$ as in (a), so $u' = \zeta u$ for some $\zeta \in \mu_n(L')$. Now part (2) identifies the possibilities for ζ.

(4) In (A.6), the intersection of $\ker \mathrm{pr}_2$ with the kernel of $U(k) \to H^1(k, A[\phi])$ is $(\tau_*, n)(E^\vee(k)) = \tau_*(E^\vee(k)) \times \{1\}$.

(c) This follows from part (b). □

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 ℓ is a unit at v. The formula in Lemma A.13(b)(1), applied over $\mathbb{F}_v$ to the reductions of ℓ and u modulo v, 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 $Q(k) \to Q(\mathbb{F}_v)$ 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 $\mathcal{S}$ lets us replace H by a finite subgroup $H_{\mathcal{S}}$. This will reduce the determination of $\mathrm{Sel}^\phi(J)$ to a finite computation. Let $H^1(k, A[\phi])_{\mathcal{S}}$ be the group of classes unramified outside $\mathcal{S}$, as in Section 7.1.

PROPOSITION A.15. *Assume Hypothesis 10.1. Let $\mathcal{S}$ 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*

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

ramified. Let $H_{\mathcal{S}}$ be the preimage in $H = U(k)/V$ of $\widetilde{L(n,\mathcal{S})} \subset \widetilde{L^\times/L^{\times n}k^\times}$ under the map pr_2' in (A.11). Then the injection $H \hookrightarrow H^1(k, A[\phi])$ in the third row of (A.11) identifies the subgroup $H_{\mathcal{S}}$ with

$$H^1(k, A[\phi])_{\mathcal{S}} \cap \mathrm{im}(H \to H^1(k, A[\phi])),$$

and identifies

$$\left\{ h \in H_{\mathcal{S}} : \rho_v(h) \in (r, f)\big(\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})\big) \text{ for all } v \in \mathcal{S} \right\} \tag{A.13}$$

with $\mathrm{Sel}^\phi(J)$.

Proof. Let $v \notin \mathcal{S}$ 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

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

is surjective. This shows that for $\xi \in H^1(k, A[\phi])$, ξ is unramified outside $\mathcal{S}$ if and only if $\alpha(\xi)$ is unramified outside $\mathcal{S}$. On the other hand, Proposition 7.2 shows that $H_{\mathcal{S}}$ equals the set of $h \in H$ whose image $\mathrm{pr}_2'(h)$ in $\widetilde{L^\times/L^{\times n}k^\times}$ is unramified outside $\mathcal{S}$. By (A.11), 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. □

We now sketch an algorithm for computing $\mathrm{Sel}^\phi(J)$, using the explicit description given in Proposition A.15. First compute $\widetilde{L(n,\mathcal{S})}$. Lemma A.13 lets us compute its inverse image $H_{\mathcal{S}}$ under the map pr_2' in (A.11). To perform the computations required by Lemma A.13, we need to be able to evaluate $\tau_*\colon L^\times \to L'^\times$ and extract nth roots in L'; the remaining computations use only finite Galois modules like $E^\vee$, $\mu_n^{\Delta'}$, or Q, so they are not difficult.

Similarly, for each $v \in \mathcal{S}$, first compute $\widetilde{L_v^\times/L_v^{\times n}k_v^\times}$, and use Lemma A.13 (over k_v) to obtain a description of H_v. The map $H_{\mathcal{S}} \to H_v$ 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 $\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$, 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 $\mathrm{Sel}^\phi(J)$.

We summarize this discussion as follows.

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

- *Compute in the algebras L and L' and their completions (this includes the ability to take nth roots).*

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

- *Determine a set $\mathcal{S}$ of places of k as in Proposition A.15.*
- *Compute $k(n, \mathcal{S})$ and $L(n, \mathcal{S})$.*
- *Evaluate τ_* on $L^\times$ and $L_v^\times$ for $v \in \mathcal{S}$, and on finite residue fields.*
- *Evaluate f and r on $\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$ for $v \in \mathcal{S}$.*

EXAMPLE A.17. Consider the case of 2-descent on Jacobians of nonhyperelliptic genus 3 curves X, as in Section 12. For generic X, the smallest usable set Δ' 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 $\mathrm{Sel}^\phi(J)$ as described in Section A.2 can be simplified. In particular, in the following proposition, the set $\mathcal{S}$ is potentially smaller than that required in Proposition A.15.

PROPOSITION A.18. *In the situation of Section A.2, let $\mathcal{S}$ be a set of places of k containing the set of places in Proposition 9.2. Assume that the homomorphism $E^\vee(k') \to R^\vee(k')$ is surjective for all field extensions k' of k and that the map $q' \colon \mu_n(L') \to Q(k)$ is surjective. Then*

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

Proof. Since $E^\vee(k) \to R^\vee(k)$ is surjective, the map $H^1(k, A[\phi]) \xrightarrow{\alpha} H^1(k, E^\vee)$ is injective. So the map pr_2' in (A.11) identifies H with a subgroup of $\widetilde{L^\times/L^{\times n}k^\times}$, and similarly identifies H_v with a subgroup of $\widetilde{L_v^\times/L_v^{\times n}k_v^\times}$, for each v. Also $E^\vee(k_{v,u}) \to R^\vee(k_{v,u})$ is surjective for each v, so the proof of Proposition A.15 shows that $H_{\mathcal{S}}$ is the subgroup of elements of H unramified outside $\mathcal{S}$. Since $\mu_n(L') \to Q(k)$ is surjective, Lemma A.13(c) yields

$$H_{\mathcal{S}} \simeq \{[\ell] \in \widetilde{L(n, \mathcal{S})} : \tau_*(\ell) \in L'^{\times n}\}. \tag{A.14}$$

In (A.11), $C_v = \mathrm{pr}_2' \circ (r, f)$, so $(r, f)\big(\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})\big) = \operatorname{im} C_v$. Substituting this and (A.14) into (A.13) completes the proof. □

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

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

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 $E^\vee(k') \to R^\vee(k')$ for all extension fields k' of k, let Γ be the (finite) Galois group over k of the splitting field of $E^\vee$; then the action of $\mathcal{G}_{k'}$ on $E^\vee$ (and therefore also $R^\vee$) factors through a subgroup $\Gamma' \leqslant \Gamma$. The surjectivity of $E^\vee(k') \to R^\vee(k')$ is determined by Γ', so it suffices to check it for each Γ'; in fact, we need only consider one Γ' 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 $Ш^1(k, R^\vee) = 0$ by Remark A.4, and $W_v = 0$ for all v by Lemma 10.5(b), and $\mathcal{K} = 0$ by its second definition (preceding (22)). So by Lemma 10.17(b) and Corollary 10.16, we have $\mathrm{Sel}^\phi(J) \simeq \mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$. The advantage of computing $\mathrm{Sel}^\phi(J)$ using Proposition A.18 instead of computing $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$ using Theorem 10.9(b) is that the former requires local computations at only the places in $\mathcal{S}$ instead of the places in the potentially much larger set $\mathcal{T}$ of Theorem 10.9(b). This improvement is possible because of the additional condition $\tau_*(\ell) \in L'^{\times n}$: in terms of the notation $S_\mathcal{T}$ of Section 10.2, Proposition A.18 says that

$$\mathrm{Sel}^\phi(J) \simeq S_\mathcal{S} \cap \{[\ell] \in \widetilde{L(n, \mathcal{S})} : \tau_*(\ell) \in L'^{\times n}\},$$

which by Lemma A.13(c) equals $S_\mathcal{S} \cap \alpha(H^1(k, A[\phi]))$ under the assumptions made. In other words, enlarging $\mathcal{S}$ to a $\mathcal{T}$ large enough that $S_\mathcal{T} = \mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$ has the effect of intersecting $S_\mathcal{S}$ with $\alpha(H^1(k, A[\phi]))$.

EXAMPLE A.22. We consider 3-descent on an elliptic curve J, as in [**37**]. Let $\Delta = J[3] - \{0\}$, and let β be the graph of the map $\Delta \to \mathrm{Div}^0 J_s$ 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 Δ' be the set of eight lines in $\mathbb{P}^2$ passing through three of the points in Δ, together with the four vertical lines passing through two of them and the origin of J. Let the correspondence τ be given by incidence. A finite computation as in Remark A.20 shows that the maps $\mu_3(L') \to Q(k)$ and $\mu_3(L) \to R^\vee(k)$ are surjective over any field. So Proposition A.18 gives us a way to determine $\mathrm{Sel}^3(J)$, if we can compute $L(3, \mathcal{S})$.

The approach described here and in Section A.2 has advantages and disadvantages compared to computing $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$ 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 $\mathcal{S}$ instead of

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

the places in a potentially much larger set $\mathcal{T}$. 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 the ($\mathcal{S}$-)class and unit groups of L, but also a presentation of L', the map $\tau_*\colon L^\times \to L'^\times$, 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

$$0 \longrightarrow \ker\kappa \longrightarrow \mathrm{Sel}^\phi(J) \xrightarrow{\alpha} \mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J) \cap \alpha\big(H^1(k, A[\phi])\big) \longrightarrow \operatorname{coker}\kappa$$

from Theorem 10.14. Assuming that we have computed the group $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$, we can determine the order of $\mathrm{Sel}^\phi(J)$ if we can

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

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

Lemma A.13 implies the following.

COROLLARY A.23. *If we can evaluate the map τ_* explicitly on $L^\times$ and if we can extract nth roots in L', then we can determine whether any given element in the image of $L^\times$ in $H^1(k, E^\vee)$ lies in $\alpha\big(H^1(k, A[\phi])\big)$.*

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 homomorphism $\kappa\colon \mathcal{K} \to \prod_v W_v$. The group $\mathcal{K} = R^\vee(k)/qE^\vee(k)$ can be found by a finite computation, using the inclusion $R^\vee(k) \hookrightarrow \mu_n(L')$ arising from (A.3) to represent elements of $R^\vee(k)$. 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

$$\ker C_v \overset{\gamma_v}{\hookrightarrow} \ker\alpha_v \simeq R^\vee(k_v)/qE^\vee(k_v)$$

can be described explicitly as follows. Given $[z] \in \ker C_v \subseteq J(k_v)/\phi A(k_v)$, represented by some $z \in \mathcal{Z}^0(X^{\mathrm{good}}_{k_v})$, the image $\gamma_v([z])$ is represented by

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

$\zeta \in R^\vee(k_v) \subset \mu_n(L'_v)$ defined as follows:
In the true case, $f(z) = \ell^n$ for some $\ell \in L_v^\times$; then set $\zeta := r(z)/\tau_*(\ell)$.
In the fake case, $f(z) = \ell^n a$ for some $\ell \in L_v^\times$ and $a \in k_v^\times$; then set $\zeta := r(z)/(\tau_*(\ell)\theta_*(a))$.

(b) *Assume Hypothesis 11.1. If we know $\#\big(J(k_v)/\phi A(k_v)\big)$ and we can compute the functions f and r on $\mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$ and τ_* on $L_v^\times$, then we can compute W_v in the course of the computation of $\operatorname{im} C_v$ 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) *For finite extensions K/k_v of degree d, randomly generate elements $z := \operatorname{tr}_{K/k_v}(x) - dx_0 \in \mathcal{Z}^0(X_{k_v}^{\mathrm{good}})$ as in Remark 11.6, let $\mathcal{J}$ be the subgroup of $J(k_v)/\phi A(k_v)$ they generate so far, and compute the groups*

$$I := C_v(\mathcal{J}) \subseteq \widetilde{L_v^\times/L_v^{\times n}k_v^\times},$$
$$G := \gamma_v(\ker(C_v|_{\mathcal{J}})) \subseteq R^\vee(k_v)/qE^\vee(k_v)$$

until $\#I \cdot \#G = \#\big(J(k_v)/\phi A(k_v)\big)$.

(3) *When equality occurs, $I = \operatorname{im} C_v$ and $W_v \simeq \big(R^\vee(k_v)/qE^\vee(k_v)\big)/G$.*

Proof.

(a) In the true case, $C_v([z]) = 0$ means that $f(z) = \ell^n$ 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 $(\tau_*(\ell), \ell^n) \in V_v$ (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, we divide instead by the element $(\tau_*(\ell)\theta_*(a), \ell^n a) \in V_v$. Lemma A.13(b)(2) applied with $\ell = 1, u = 1, \lambda = 1$, and hence $w = 1$, yields $\zeta \in \ker(q'|_{\mu_n(L')}) = R^\vee(k_v)$ (see (A.3)).

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

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

Once we know W_v as a quotient of $R^\vee(k_v)$ for all v for which W_v might be nonzero, the map $\kappa : \mathcal{K} \to \prod_v W_v$, with $\mathcal{K} = R^\vee(k)/qE^\vee(k)$, is induced by the

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

maps $R^\vee(k) \to R^\vee(k_v)$ 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* $\xi \in \mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J) \cap \alpha(H^1(k, A[\phi]))$, *represented by some explicit* $\ell \in L^\times$, *we can find the image of* ξ *in* $\operatorname{coker} \kappa$.

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

$$\begin{tikzcd} 0 \arrow[r] & R^\vee(k) \arrow[r] \arrow[d] & U(k) \arrow[r, "\mathrm{pr}_2"] \arrow[d] & L^\times \arrow[d] \\ 0 \arrow[r] & \prod_v R^\vee(k_v) \arrow[r] & \prod_v U(k_v) \arrow[r, "\mathrm{pr}_2"] & \prod_v L_v^\times \end{tikzcd} \tag{A.15}$$

(with exact rows from (A.6)), which maps to (23).

Use Lemma A.13 to compute u such that $(u, \ell) \in U(k)$, that is, such that $\tau_*(\ell) = u^n$. For the places v for which $W_v = 0$, set $\zeta_v := 1 \in R^\vee(k_v)$. For the finitely many remaining v, we have $\xi_v = C_v([z_v])$ for some $z_v \in \mathcal{Z}^0(X^{\mathrm{good}}_{k_v})$ found during the local image computation; then $f(z_v) \equiv \ell$ in $\widetilde{L_v^\times / L_v^{\times n} k_v^\times}$. 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, ℓ) in the group $H^1(k_v, A[\phi])/\operatorname{im} \gamma_v$ in the corresponding position of (23). By exactness of the second row of (A.15), we have $\zeta_v \in R^\vee(k_v)$. Then $(\zeta_v) \in \prod R^\vee(k_v)$ maps to an element of $\prod W_v$ in (23), which represents the image of ξ in $\operatorname{coker} \kappa$. □

We conclude that in order to find (the order of) $\mathrm{Sel}^\phi(J)$ from $\mathrm{Sel}^\alpha_{\mathrm{true/fake}}(J)$, 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 τ_* locally at the places with potentially nontrivial W_v. But if we can do all this, then we can also compute $\mathrm{Sel}^\phi(J)$ 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 Universität Bayreuth. We thank them all for their hospitality. We also thank 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. We thank the referee for many helpful comments.

N.B. was partially supported by the Natural Sciences and Engineering Research Council. B.P. was partially supported by the Guggenheim Foundation, by a grant from the Simons Foundation (#340694 to Bjorn Poonen), and by National Science Foundation grants DMS-0301280, DMS-0841321, and DMS-1069236. M.S. was partially supported by the Deutsche Forschungsgemeinschaft.

References

[1] M. F. Atiyah and C. T. C. Wall, 'Cohomology of groups', in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)* (Thompson, Washington, DC, 1967), 94–115.

[2] B. Baran, 'An exceptional isomorphism between modular curves of level 13', *J. Number Theory* **145** (2014), 273–300.

[3] B. Baran, 'An exceptional isomorphism between level 13 modular curves via Torelli's theorem', *Math. Res. Lett.* **21**(5) (2014), 919–936.

[4] M. Bhargava, B. H. Gross and X. Wang, 'Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits', in *Representations of Reductive Groups*, (eds. M. Nevins and P. E. Trapa) Progress in Mathematics, 312 (Springer International Publishing, Boston, 2015), 139–171.

[5] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), 21 (Springer, Berlin, 1990).

[6] N. Bruin and M. Stoll, 'Two-cover descent on hyperelliptic curves', *Math. Comp.* **78**(268) (2009), 2347–2370.

[7] P. Deligne and D. Mumford, 'The irreducibility of the space of curves of given genus', *Publ. Math. Inst. Hautes Études Sci.* (36) (1969), 75–109.

[8] M. Demazure, 'Résultant, discriminant', *Enseign. Math. (2)* **58**(3–4) (2012), 333–373.

[9] J. Dixmier, 'On the projective invariants of quartic plane curves', *Adv. Math.* **64**(3) (1987), 279–304.

[10] Z. Djabri, E. F. Schaefer and N. P. Smart, 'Computing the p-Selmer group of an elliptic curve', *Trans. Amer. Math. Soc.* **352**(12) (2000), 5583–5597.

[11] E. V. Flynn, B. Poonen and E. F. Schaefer, 'Cycles of quadratic polynomials and rational points on a genus-2 curve', *Duke Math. J.* **90**(3) (1997), 435–463.

[12] K. Geißler, 'Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern', PhD Thesis, Technische Universität Berlin, 2003, available at http://www.math.tu-berlin.de/ kant/publications/diss/geissler.pdf.

[13] K. Geissler and J. Klüners, 'Galois group computation for rational polynomials', *J. Symbolic Comput.* **30**(6) (2000), 653–674. Algorithmic methods in Galois theory.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

[14] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, Modern Birkhäuser Classics (Birkhäuser Boston Inc., Boston, MA, 2008), reprint of the 1994 edition.

[15] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, 101 (Cambridge University Press, Cambridge, 2006).

[16] B. H. Gross and J. Harris, 'On some geometric constructions related to theta characteristics', in *Contributions to Automorphic Forms, Geometry, and Number Theory* (Johns Hopkins University Press, Baltimore, MD, 2004), 279–311.

[17] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, 52 (Springer, New York, 1977).

[18] D. R. Kohel, Algorithms for elliptic curves and higher dimensional analogues (Echidna). Available at http://echidna.maths.usyd.edu.au/kohel/alg/index.html.

[19] S. Lang, *Abelian Varieties* (Springer, New York, 1983), reprint of the 1959 original.

[20] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265. Computational algebra and number theory (London, 1993). Magma is available at http://magma.maths.usyd.edu.au/magma/.

[21] W. McCallum and B. Poonen, 'The method of Chabauty and Coleman', in *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et Synthèses, 36 (Société Mathématique de France, Paris, 2012), 99–117.

[22] J. S. Milne, *Arithmetic Duality Theorems*, 2nd edn, (BookSurge, LLC, 2006).

[23] L. J. Mordell, 'On the rational solutions of the indeterminate equations of the third and fourth degrees', *Proc. Cambridge Phil. Soc.* **21** (1922), 179–192.

[24] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5 (Published for the Tata Institute of Fundamental Research, Bombay, 1970).

[25] D. Mumford, 'Theta characteristics of an algebraic curve', *Ann. Sci. Éc. Norm. Supèr. (4)* **4** (1971), 181–192.

[26] David Mumford, *Tata Lectures on Theta. II*, Progress in Mathematics, 43 (Birkhäuser Boston Inc., Boston, MA, 1984), Jacobian theta functions and differential equations; with the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[27] S. Pauli and X.-F. Roblot, 'On the computation of all extensions of a p-adic field of a given degree', *Math. Comp.* **70**(236) (2001), 1641–1659. (electronic).

[28] B. Poonen, 'Bertini theorems over finite fields', *Ann. of Math. (2)* **160**(3) (2004), 1099–1127.

[29] B. Poonen and E. F. Schaefer, 'Explicit descent for Jacobians of cyclic covers of the projective line', *J. Reine Angew. Math.* **488** (1997), 141–188.

[30] B. Poonen, E. F. Schaefer and M. Stoll, 'Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$', *Duke Math. J.* **137**(1) (2007), 103–158.

[31] B. Poonen and M. Stoll, 'The Cassels-Tate pairing on polarized abelian varieties', *Ann. of Math. (2)* **150**(3) (1999), 1109–1149.

[32] G. Salmon, *Lessons Introductory to the Modern Higher Algebra*, 3rd edn, (Hodges, Foster, and Co., Dublin, 1876).

[33] G. Salmon, *A Treatise on the Higher Plane Curves*, 3rd edn, (Hodges, Foster, and Figgis, Dublin, 1879).

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

[35] E. F. Schaefer, 'Class groups and Selmer groups', *J. Number Theory* **56**(1) (1996), 79–114.

[36] E. F. Schaefer, 'Computing a Selmer group of a Jacobian using functions on the curve', *Math. Ann.* **310**(3) (1998), 447–471.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press

[37] E. F. Schaefer and M. Stoll, 'How to do a p-descent on an elliptic curve', *Trans. Amer. Math. Soc.* **356**(3) (2004), 1209–1231, (electronic).
[38] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, 67 (Springer, New York, 1979), translated from the French by Marvin Jay Greenberg.
[39] R. P. Stauduhar, 'The determination of Galois groups', *Math. Comp.* **27** (1973), 981–996.
[40] M. Stoll, 'Independence of rational points on twists of a given curve', *Compos. Math.* **142**(5) (2006), 1201–1214.
[41] J. A. Thorne, 'The arithmetic of simple singularities', PhD Thesis, Harvard University, April, 2012.
[42] A. Weil, 'L'arithmétique sur les courbes algébriques', *Acta Math.* **52**(1) (1929), 281–315.

https://doi.org/10.1017/fms.2016.1 Published online by Cambridge University Press