FUNCTIONS, RECIPROCITY AND THE OBSTRUCTION TO DIVISORS ON CURVES

MARTIN BRIGHT AND SAMIR SIKSEK

Abstract. Let k be a number field, X a smooth curve over k, and f a non-constant element of the function field $k(X)$. If v is a prime of k then denote the completion of k at v by k_v and let $X_v := X \times k_v$. In this paper we introduce an abelian extension l/k, depending on f in a natural way, which we call the class field of k belonging to f. We give an explicit homomorphism

$$\prod \mathrm{Pic}(X_v) \to \mathrm{Gal}(l/k),$$

such that the image of $\mathrm{Pic}(X)$ in $\prod \mathrm{Pic}(X_v)$ is in the kernel of this map. We explain how this can often obstruct the existence of k-rational divisors of certain degrees.

1. Introduction

Various classical counterexamples to the Hasse principle suggest that functions on a variety can 'conspire' with the reciprocity law for abelian extensions of number fields so as to 'interfere' with the existence of global points. This is clear in Lind's counterexample to the Hasse principle in genus 1 (see [2, page 284] or [26, pp. 316–318]), and again in Swinnerton-Dyer's counterexample to the Hasse principle for cubic surfaces (see [28]). Such examples have long since been interpreted in terms of the Brauer–Manin obstruction, and were the starting point of a great deal of theory (see for example [27]).

In this paper we restrict ourselves to curves, and it is our purpose to make this 'conspiratorial interference' of functions plus reciprocity explicit and transparent. Our motivation is to furnish the basis for attempts at proving that a given curve, suspected of having no rational divisors of a certain degree, does indeed have no rational divisors of that degree. In this light we give detailed guidance for the case of 2-coverings of elliptic curves over the rationals.

Before stating the main theorem of this paper we set some notation. We start by letting k be a perfect field, and X a complete, non-singular and absolutely irreducible curve over k. We denote the function field of X over k by $k(X)$. A closed point $\mathcal{P}$ of X corresponds to a discrete valuation ring $\mathcal{O}_\mathcal{P}$ of $k(X)$ containing k, with maximal ideal $\mathfrak{m}_\mathcal{P}$. The residue field of $\mathcal{P}$ is by definition $k(\mathcal{P}) := \mathcal{O}_\mathcal{P}/\mathfrak{m}_\mathcal{P}$, and is a finite extension of k. The degree of $\mathcal{P}$ is given by $|\mathcal{P}| := [k(\mathcal{P}) : k]$. If $g \in k(X)$ is regular at point $\mathcal{P}$, that is $g \in \mathcal{O}_\mathcal{P}$, then the value of g at $\mathcal{P}$, denoted by $g(\mathcal{P})$, is defined to be the image of g in $k(\mathcal{P})$; it thus makes sense to speak of the

Date: December 17, 2007.

2000 *Mathematics Subject Classification.* Primary 11G30, Secondary 11G25.

Key words and phrases. local-to-global, the Hasse principle, curves, descents.

The second-named author's research is supported by an Engineering and Physical Science Research Council (UK) grant, and by a Marie-Curie International Reintegration Grant.

$\mathrm{Norm}_{k(\mathcal{P})/k}(g(\mathcal{P})) \in k$. We will simplify the notation slightly by writing $\mathrm{Norm}_{\mathcal{P}}$ for $\mathrm{Norm}_{k(\mathcal{P})/k}$.

We denote the set of closed points on X by X^c; this of course is all of X except for the generic point. For $\mathcal{P} \in X^c$ let $\mathrm{ord}_{\mathcal{P}} : k(X)^\times \to \mathbb{Z}$ be the corresponding valuation.

Now we specialize by letting k be a number field. Let $\mathbb{I}_k$ be its idèle group, and $C_k := \mathbb{I}_k/k^\times$ its idèle class group. If k' is a finite extension of k, and n is an integer then let

$$\underset{k'/k}{\mathrm{Norm}}(C_{k'})^n = \{\alpha^n : \alpha \in \underset{k'/k}{\mathrm{Norm}}(C_{k'})\}.$$

Clearly $\mathrm{Norm}_{k'/k}(C_{k'})^0 = \{1\}$.

Suppose $f \in k(X)$ is a non-constant element of the function field of X. We associate to f the following subgroup of C_k:

$$\prod_{\mathcal{P} \in X^c} \underset{\mathcal{P}}{\mathrm{Norm}}(C_{k(\mathcal{P})})^{\mathrm{ord}_{\mathcal{P}}(f)}.$$

We would like this to be an open subgroup of C_k. A little exercise in class field theory shows that this subgroup is open in C_k if and only if the exponents $\mathrm{ord}_{\mathcal{P}}(f)$ do not all share a non-trivial common factor as $\mathcal{P}$ ranges through the support of f. We assume this; the Existence Theorem of class field theory ([16, pages 208–211]) asserts the existence of a unique finite abelian extension l/k (the class field of k belonging to this group), such that

$$\underset{l/k}{\mathrm{Norm}}(C_l) = \prod_{\mathcal{P} \in X^c} \underset{\mathcal{P}}{\mathrm{Norm}}(C_{k(\mathcal{P})})^{\mathrm{ord}_{\mathcal{P}}(f)}. \tag{1}$$

By abuse of language, we call l the class field of k belonging to the function f.

Let $\mathfrak{M}(k)$ be the set of primes of k. For any $v \in \mathfrak{M}(k)$ denote the completion of k at v by k_v and let $X_v := X \times_k k_v$. If v is any prime of k, denote the local Artin map at v for the abelian extension l/k by

$$\theta_v : k_v^\times \to \mathrm{Gal}(l/k).$$

We are finally ready to state our main theorem.

Theorem 1. *Let X be a complete, non-singular and absolutely irreducible curve over the number field k. Let f be a non-constant element of the function field $k(X)$ such that the integers $\mathrm{ord}_{\mathcal{P}}(f)$ do not all share a non-trivial common factor as $\mathcal{P}$ ranges through the support of f. Let l be the class field of k belonging to f (as defined above).*

(a) *Let $v \in \mathfrak{M}(k)$. Then there exists a unique homomorphism*

$$\phi_v : \mathrm{Pic}(X_v) \to \mathrm{Gal}(l/k),$$

which satisfies the following property: if $\mathcal{Q}$ is a closed point of X_v that is neither a pole nor a zero of f then

$$\phi_v\left([\mathcal{Q}]\right) = \theta_v\left(\underset{\mathcal{Q}}{\mathrm{Norm}}(f(\mathcal{Q}))\right),$$

where $[\mathcal{Q}]$ denotes the class of $\mathcal{Q}$ in $\mathrm{Pic}(X)$.

(b) *There exists a finite set B of primes in $\mathfrak{M}(k)$ such that for any $v \notin B$ we have that $\phi_v = 1$.*

(c) *The image of* $\mathrm{Pic}(X)$ *in* $\prod_{v\in B}\mathrm{Pic}(X_v)$ *(under the diagonal map) is contained in the kernel of the homomorphism*

$$\prod_{v\in B}\mathrm{Pic}(X_v)\xrightarrow{\prod_{v\in B}\phi_v}\mathrm{Gal}(l/k). \tag{2}$$

Note that any divisor can be moved in its equivalence class to avoid the poles and zeros of f; thus the map in (a) can be used to compute the image of any divisor class in $\mathrm{Pic}(X_v)$. Moreover, this fact immediately shows that if the homomorphism ϕ_v exists then it must indeed be unique. We shall give an explicit and very simple recipe for the set of primes B appearing in part (b) of the Theorem. Part (c) follows from Artin's reciprocity law, as we shall see.

We now indicate how Theorem 1 can sometimes be used to prove that the curve X does not possess any k-rational divisors of a given degree. Let B be the finite set of primes whose existence is asserted in part (b) of the Theorem. From the computational point-of-view, it seems at first sight that part (c) of the theorem is not useful since the kernel of $\prod\phi_v$ is very large. It is however straightforward to factor the homomorphism $\prod\phi_v$ through a finite group, and so deal only with a finite kernel. Indeed, suppose that n is a positive integer; we obtain an induced homomorphism

$$\prod_{v\in B}\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v)\longrightarrow\mathrm{Gal}(l/k)/(\mathrm{Gal}(l/k))^n \tag{3}$$

such that the image of $\mathrm{Pic}(X)$ in the group on the left-hand side is in the kernel of this map, and it is noteworthy that this kernel is finite, since the set B is finite, and the quotient groups $\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v)$ are finite too. Now an element of $\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v)$ does not have a well-defined degree, but it has a well-defined degree modulo n. If $0\le r<n$, we denote by

$$(\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v))_r$$

the **subset** of elements that have degree r modulo n. This subset contains the images of

$$\mathrm{Pic}^r(X),\ \mathrm{Pic}^{r+n}(X),\ \mathrm{Pic}^{r+2n}(X),\dots$$

in $\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v)$. We immediately obtain the following corollary.

Corollary 1.1. *With notation and assumptions as in Theorem 1, let* n *and* r *be positive integers satisfying* $0\le r<n$. *Let*

$$\prod_{v\in B}(\mathrm{Pic}(X_v)/n\,\mathrm{Pic}(X_v))_r\longrightarrow\mathrm{Gal}(l/k)/\mathrm{Gal}(l/k)^n \tag{4}$$

be the map arising as the restriction of the map in (3). *The subset of elements of the set on the left-hand side sent to* 1 *under this map is finite. If this subset is empty then* $\mathrm{Pic}^r(X),\mathrm{Pic}^{r+n}(X),\mathrm{Pic}^{r+2n}(X),\dots$ *are all empty.*

We will see an application of this corollary at the end. There are of course variants of the corollary involving several functions, and we leave it to the reader to invent his own results with the help of Theorem 1.

The paper is structured as follows: Sections 2–4 are preliminaries necessary for the proof of Theorem 1; Section 5 completes the proof of Theorem 1; in Section 6 we interpret the obstruction of Theorem 1 in terms of torsors under tori, and in

Section 7 we show that it is equivalent to part of the Brauer–Manin obstruction; finally Sections 8 and 9 are concerned with explicit examples.

At the suggestion of the referee we point out some differences between our method and other methods:

- There are two general methods for showing that curves (having points everywhere locally) do not have global points. The first is descent and the second is the Mordell–Weil sieve (see, for example, [1]). Descent usually requires the computation of class groups and unit groups of number fields. The Mordell–Weil sieve is applicable only to curves of genus ≥ 2 and requires computation of the Mordell–Weil group of the Jacobian. This in turn again usually requires the computation of class groups and unit groups. Our method avoids the computationally expensive detour through class groups and unit groups and relies only on local calculations and reciprocity.
- Our method gives information on degree 1 divisors, and not just degree 1 points. In this sense it is more useful than descent and the Mordell–Weil sieve.

In future papers we expect to work out the details of our method for various families of curves of higher genus as well as for 3-coverings of elliptic curves. A particularly promising direction, pioneered in a particular case in [24], is to combine our method with the Mordell–Weil sieve.

We are indebted to Professors J.-L. Colliot-Thélène, A. N. Skorobogatov and the referee for detailed comments and criticisms of an earlier version of this paper. We are also grateful to J. Cremona, S. Donnelly, T. Fisher, N. Bruin and M. Stoll for useful discussions.

2. Preliminaries

In this section we recall a result of the second-named author [23] which will allow us, together with some class-field theory, to construct the homomorphism in part (a) of Theorem 1. Recall that we are denoting, for a curve X, the set of closed points by X^c. The divisor group of X, denoted $\mathrm{Div}(X)$, is the free group on the points of X^c. The subgroup of principal divisors is denoted by $\mathrm{Princ}(X)$, and we let $\mathrm{Pic}(X) := \mathrm{Div}(X)/\mathrm{Princ}(X)$.

Lemma 2.1. *Let X be a complete non-singular absolutely irreducible curve over a perfect field k, and let f be a non-constant element of the function field $k(X)$. Define the subgroup $G_f(k) \subset k^\times$ by*

$$G_f(k) := \prod_{\mathcal{P} \in X^c} \operatorname*{Norm}_{\mathcal{P}}(k(\mathcal{P})^\times)^{\mathrm{ord}_{\mathcal{P}}(f)}. \tag{5}$$

Then f induces a unique homomorphism

$$\hat{f} \ : \ \mathrm{Pic}(X) \to k^\times / G_f(k)$$

satisfying the following property: if $\mathcal{Q} \in X^c$ is neither a pole nor a zero of f then the class $[\mathcal{Q}]$ of $\mathcal{Q}$ in $\mathrm{Pic}(X)$ is mapped, by $\hat{f}$, to the coset represented by $\mathrm{Norm}_{\mathcal{Q}}(f(\mathcal{Q}))$.

Proof. See [23] for the proof. The proof is merely an application of Weil's reciprocity, plus the well-known fact that every divisor can moved in its class to avoid a given finite set (in this case the poles and zeros of f). □

3. A more Powerful 'Moving Lemma'

We have until now made use of the idea that any divisor can be moved in its class to avoid the support of a function f. In this section we prove a more powerful version of this idea: over a non-archimedean local field, any divisor can be moved in its class so that its reduction in the special fibre avoids the support of f, provided X and f satisfy certain 'good reduction' criteria.

Let k_v be a non-archimedean local field; in other words, k_v is a finite extension of $\mathbb{Q}_p$, with p a finite prime. Denote the valuation ring of k_v by $\mathcal{O}_v$, and the group of invertible elements of $\mathcal{O}_v$ by $\mathcal{O}_v^\times$. Let π be a uniformizer for $\mathcal{O}_v$.

Let X be a complete non-singular and absolutely irreducible curve over k_v. Let $\mathcal{X} \subset \mathbb{P}^N_{\mathcal{O}_v}$ be a projective model for X. We identify X with the generic fibre of $\mathcal{X}$; since $\mathcal{X}$ is proper, every point of X extends to a point of $\mathcal{X}$. If $\mathcal{P}$ is a point of X, we denote its image in the special fibre by $\tilde{\mathcal{P}}$.

Now let f be a rational function on X, which of course extends to a rational function on $\mathcal{X}$. We make the following assumptions about the model $\mathcal{X}$:

(1) f does not have a zero or a pole along any component of the special fibre of $\mathcal{X}$. If the special fibre is irreducible, then $v(f)$ is defined and this condition simply requires that $v(f) = 0$.
(2) For each closed point $\tilde{\mathcal{P}}$ lying on a zero or pole of f, the local ring $\mathcal{O}_{\tilde{\mathcal{P}}}$ is regular.

Lemma 3.1. *Let X satisfy the good reduction criteria stated above. Then* $\operatorname{Pic} X$ *is generated by the classes of points $\mathcal{P}$ such that f is regular and non-zero on $\tilde{\mathcal{P}}$.*

Proof. We write $\tilde{\mathcal{P}}_1, \ldots, \tilde{\mathcal{P}}_n$ for the distinct closed points of $\mathcal{X}$ where f is not invertible. Suppose that $\mathcal{P} \in X^c$ and that f is either not regular or zero at $\tilde{P}$. Then $\tilde{\mathcal{P}}$ must equal one of $\tilde{\mathcal{P}}_1, \ldots, \tilde{\mathcal{P}}_n$ and without loss of generality suppose $\tilde{\mathcal{P}} = \tilde{\mathcal{P}}_1$. We construct a function $h \in k_v(\mathcal{X})$ simultaneously satisfying the three conditions

(i) $\operatorname{ord}_{\mathcal{P}}(h) = 1$,
(ii) h is regular and non-zero at $\tilde{\mathcal{P}}_2, \ldots, \tilde{\mathcal{P}}_n$,
(iii) and h is regular and non-zero along all prime divisors passing through $\tilde{\mathcal{P}}$ other than $\mathcal{P}$.

It is seen that $\mathcal{P} - \operatorname{div}(h)$ is linearly equivalent to $\mathcal{P}$ and the intersection of its support with the special fibre avoids all of $\tilde{\mathcal{P}}_1, \ldots, \tilde{\mathcal{P}}_n$.

As we will see, the construction of h is an exercise in applying the Prime Avoidance Theorem, for which see [11, Section 3.2].

Let $\mathcal{O}(1)$ denote the sheaf of hyperplane sections coming from the embedding $\mathcal{X} \subset \mathbb{P}^N_{\mathcal{O}_v}$. This is an ample line bundle on $\mathcal{X}$ [13, Proposition 4.5.10]. By [13, Corollary 4.5.4] (which is one version of the Prime Avoidance Theorem) there exist an integer m and a homogeneous polynomial $g \in \mathcal{O}(m)(\mathcal{X})$ which is non-zero at each of the $\tilde{\mathcal{P}}_i$, such that $U = \mathcal{X}_g$ is an affine subscheme of $\mathcal{X}$ containing all the $\tilde{\mathcal{P}}_i$. From now on we may work in U.

Let $\mathfrak{m}_i$ be the maximal ideal corresponding to $\tilde{\mathcal{P}}_i$, and let $\mathcal{I}$ be the prime ideal corresponding to $\mathcal{P}$. Then $\mathcal{I} \not\subseteq \mathfrak{m}_i$ for $i > 1$. Also $\mathcal{I} \not\subseteq \mathfrak{m}_1^2$: for $\mathcal{O}_{\tilde{\mathcal{P}}}/\mathcal{I}$ is regular, being isomorphic to the ring of integers in $k(\mathcal{P})$; so by [14, Chapter 0, Corollary 17.1.9] $\mathcal{I}$ contains an element of $\mathfrak{m}_1 \setminus \mathfrak{m}_1^2$. It follows from the Prime Avoidance Theorem (which, despite the name, allows up to two of the ideals being avoided to be non-prime) that there exists $h \in \mathcal{I}$ such that $h \notin \mathfrak{m}_i$ for $i > 1$ and $h \notin \mathfrak{m}_1^2$.

Clearly this means that $\mathrm{ord}_{\mathcal{P}}(h) = 1$, and that h is non-zero at each $\tilde{\mathcal{P}}_i$ for $i > 1$. Furthermore, h is non-zero along each prime divisor D passing through $\tilde{\mathcal{P}}$, other than $\mathcal{P}$. For $\mathcal{O}_{\tilde{\mathcal{P}}}$ is regular, hence factorial; so if h were divisible both by a generator t for $\mathcal{I}$ and by a generator t' for the ideal corresponding to D, then h would be divisible by tt' and therefore in $\mathfrak{m}_1^2$. □

4. Extension of Scalars

For now X denotes a non-singular, complete and absolutely irreducible curve over a *number field* k. In preparation for the proof of Theorem 1, where we need to replace k by its completions k_v, we study what happens to the groups $G_f(k)$ (defined in (5)) under extension of scalars. In essence, this comes down to studying the fibres of the projection $X_K \to X$, for field extensions K/k, and this is what we do in this section. We do not claim that results proved in this section are original, but merely that we cannot find a convenient reference for them, and in any case it is useful to collect them all here before embarking on the proof of Theorem 1.

4.1. **Norms on Finite Algebras over Fields.** We need to review (briefly) the definition of a norm and recall a few basic results about it. Our reference here is [12, pages 16–20]. Let L be a finite algebra over a field K. If $\beta \in L$ then β induces a K-linear transformation on L given by $\alpha \mapsto \beta\alpha$. The norm of β, denoted $\mathrm{Norm}_{L/K}(\beta)$, is defined to be the determinant of this linear transformation. It follows that $\beta \mapsto \mathrm{Norm}_{L/K}(\beta)$ is a homomorphism $L^\times \to K^\times$; we denote the image of this map by $\mathrm{Norm}_{L/K}(L^\times)$.

Lemma 4.1. *Suppose K is a field, L is a K-algebra such that $L \cong \prod_{i=1}^n K_i$ where the K_i are also finite K-algebras. For $\beta \in L$ let β_i be the image of β in K_i. Then*

$$\underset{L/K}{\mathrm{Norm}}(\beta) = \prod_{i=1}^{n} \underset{K_i/K}{\mathrm{Norm}}(\beta_i).$$

Proof. See [12, page 20]. □

Lemma 4.2. *Suppose k' is a finite extension of k and K is an extension of k (that is not necessarily finite). Let $L = K \otimes_k k'$. Then L is a finite algebra over K that splits as a product of fields*

$$L \cong K_1 \times K_2 \times \cdots \times K_n$$

where the K_i/K are finite field extensions. If $\beta \in k'$ then let β_i be the image of β in K_i (under the composition $k' \to K \otimes k' \to K_i$). Then

$$\underset{k'/k}{\mathrm{Norm}}(\beta) = \underset{L/K}{\mathrm{Norm}}(\beta) = \prod_{i=1}^{n} \underset{K_i/K}{\mathrm{Norm}}(\beta_i).$$

Proof. See [3, page 54–55]. □

4.2. **The projection $X_K \to X$.** Suppose K/k is a field extension, not necessarily finite, and let $p_K : X_K \to X$ be the projection arising from the fibre product $X_K := X \times_k K$. Suppose $\mathcal{P}$ is a closed point on X. The fibre of p_K over $\mathcal{P}$ is $\mathrm{Spec}(K \otimes_k k(\mathcal{P}))$. Now $k(\mathcal{P})/k$ is finite, and by Lemma 4.2, the algebra $K \otimes_k k(\mathcal{P})$ splits as a product

$$K \otimes_k k(\mathcal{P}) = K_1 \times K_2 \times \cdots \times K_n$$

where the K_i are finite extensions of K. As this algebra does not have nilpotents, the fibre $\mathrm{Spec}(K \otimes_k k(\mathcal{P}))$ does not have multiple points, and so the map p_K is unramified. The points on this fibre are in 1-1 correspondence with the factors K_i. Denote the point corresponding to K_i by $\mathcal{Q}_i$. The residue field of $\mathcal{Q}_i$ is $K(\mathcal{Q}_i) = K_i$, and since the extensions K_i/K are finite, the points $\mathcal{Q}_i \in X_K$ above our closed point $\mathcal{P} \in X$ are all closed.

In what follows it simplifies notation somewhat if we define, for $\mathcal{P} \in X^c$ and K/k an extension

$$G_{\mathcal{P}}(K) := \operatorname*{Norm}_{K \otimes k(\mathcal{P})/K} (K \otimes k(\mathcal{P}))^{\times}. \tag{6}$$

Lemma 4.3. *Suppose K/k is a field extension (not necessarily finite), and let $\mathcal{P}$ be a closed point of X. Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ be the distinct points of X_K lying above $\mathcal{P}$.*

(a) *The points $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ are all closed, and the pull-back of $\mathcal{P}$ by p_k is the divisor $p_K^*(\mathcal{P}) = \sum \mathcal{Q}_i$.*

(b) *The algebra $K \otimes_k k(\mathcal{P})$ splits as a product of fields*

$$K \otimes_k k(\mathcal{P}) = \prod_{i=1}^{n} K(\mathcal{Q}_i).$$

(c) *The norm groups of the residue fields are related by*

$$\operatorname*{Norm}_{k(\mathcal{P})/k}(k(\mathcal{P})^{\times}) \subseteq G_{\mathcal{P}}(K) = \prod_{i=1}^{n} \operatorname*{Norm}_{K(\mathcal{Q}_i)/K}(K(\mathcal{Q}_i)^{\times})$$

(d) *If $g \in k(X)$ is regular at $\mathcal{P}$, then*

$$\operatorname*{Norm}_{k(\mathcal{P})/k}(g(\mathcal{P})) = \prod_{i=1}^{n} \operatorname*{Norm}_{K(\mathcal{Q}_i)/K}(g(\mathcal{Q}_i))$$

where we are identifying the left-hand side (an element of k) as an element of K under the embedding $k \to K$.

Proof. (a) and (b) follow from the preceding discussion, and (c) follows from (b) and Lemmas 4.1 and 4.2. Let us prove (d). Suppose $g \in k(X)$ is regular at $\mathcal{P}$. The 'quantities' $g(\mathcal{Q}_i)$ need a little interpretation, since g is a function on X and the $\mathcal{Q}_i$ are points on X_K. What we are doing is regarding g as a function on X_K by identifying it with $p_K^*(g) = g \circ p_K$. Hence $g(\mathcal{Q}_i)$ is really just $g(p_K(\mathcal{Q}_i)) = g(\mathcal{P})$. The result follows immediately from Lemma 4.2. □

Lemma 4.4. *If f is a non-constant element of $k(X)$ then*

$$G_f(k) \subseteq G_f(K) = \prod_{\mathcal{P} \in X^c} G_{\mathcal{P}}(K)^{\mathrm{ord}_{\mathcal{P}}(f)}.$$

Proof. In Lemma 4.3 we concerned ourselves with a fixed point $\mathcal{P} \in X^c$ and the points on X_K lying above it. Now we have to allow $\mathcal{P}$ to change, and it is convenient to re-express part (c) of Lemma 4.3 as follows:

$$\operatorname*{Norm}_{k(\mathcal{P})/k}(k(\mathcal{P})^{\times}) \subseteq G_{\mathcal{P}}(K) = \prod_{\substack{\mathcal{Q} \in X_K^c \\ \mathcal{Q} \mapsto \mathcal{P}}} \operatorname*{Norm}_{K(\mathcal{Q})/K}(K(\mathcal{Q})^{\times}). \tag{7}$$

To prove the lemma we first recall the definition of $G_f(k)$:

$$G_f(k) := \prod_{\mathcal{P} \in X^c} \operatorname*{Norm}_{k(\mathcal{P})/k} (k(\mathcal{P})^\times)^{\operatorname{ord}_{\mathcal{P}}(f)}.$$

It thus follows from (7) that

$$G_f(k) \subseteq \prod_{\mathcal{P} \in X^c} G_{\mathcal{P}}(K)^{\operatorname{ord}_{\mathcal{P}}(f)}$$

and to complete the proof of the lemma it is enough to show that

$$G_f(K) = \prod_{\mathcal{P} \in X^c} G_{\mathcal{P}}(K)^{\operatorname{ord}_{\mathcal{P}}(f)}. \tag{8}$$

For this we recall the definition of $G_f(K)$:

$$G_f(K) := \prod_{\mathcal{Q} \in X_K^c} \operatorname*{Norm}_{K(\mathcal{Q})/K} (K(\mathcal{Q})^\times)^{\operatorname{ord}_{\mathcal{Q}}(f)}.$$

As in the proof of Lemma 4.3, we need to do some re-interpretation. We (loosely) said in the introduction that our non-constant function $f \in k(X)$ again defines a function on X_K, which we denoted again by f. This function is in fact $p_K^*(f) = f \circ p_K$. The zeros and poles of $p_K^*(f)$ on X_K all lie above zeros and poles of f on X, and are thus all closed points of X_K. Moreover, since $X_K \to X$ is unramified, if $\mathcal{P}$ is a closed point of X, and $\mathcal{Q} \in X_K$ is lying above it then $\operatorname{ord}_{\mathcal{P}}(f) = \operatorname{ord}_{\mathcal{Q}}(p_K^*(f))$. It follows from this and the definition of $G_f(K)$ above that we can write

$$G_f(K) = \prod_{\mathcal{P} \in X^c} \left(\prod_{\substack{\mathcal{Q} \in X_K^c \\ \mathcal{Q} \mapsto \mathcal{P}}} \operatorname*{Norm}_{K(\mathcal{Q})/K} (K(\mathcal{Q})^\times) \right)^{\operatorname{ord}_{\mathcal{P}}(f)}.$$

From this and (7) we obtain the desired equality (8). □

4.3. **A Special Case: $K = k_v$.** We now specialize to the case where $K = k_v$ for some prime $v \in \mathfrak{M}(k)$, and we would like to give an alternative description of $G_{\mathcal{P}}(k_v)$, for $\mathcal{P} \in X^c$.

Lemma 4.5. *If $\mathcal{P} \in X^c$ then*

$$G_{\mathcal{P}}(k_v) = \prod_{\substack{\omega \in \mathfrak{M}(k(\mathcal{P})) \\ \omega | v}} \operatorname*{Norm}_{\omega/v} (k(\mathcal{P})_\omega^\times).$$

Proof. Recall the definition of $G_{\mathcal{P}}(K)$ in (6). We would like to show that

$$G_{\mathcal{P}}(k_v) := \operatorname*{Norm}_{k_v \otimes k(\mathcal{P})/k_v} (k_v \otimes k(\mathcal{P}))^\times = \prod_{\omega | v} \operatorname*{Norm}_{\omega/v} (k(\mathcal{P})_\omega^\times)$$

One knows however that (see [12, page 109])

$$k_v \otimes k(\mathcal{P}) \cong \prod_{\omega | v} k(\mathcal{P})_\omega,$$

and taking norms of the subgroups of invertible elements on both sides completes the proof. □

4.4. **A class-field-theoretic interlude.** Suppose now that f is a non-constant element of $k(X)$, and let l be the class field of k belonging to f as defined in the introduction.

It is traditional to identify $k_v^\times$ as a subgroup of $\mathbb{I}_k$ via the embedding $\alpha_v \mapsto (1, 1, \ldots, 1, \alpha_v, 1, \ldots)$. Hence if G is a subgroup of $\mathbb{I}_k$, and $v \in \mathfrak{M}(k)$ then it makes sense to speak of $k_v^\times \cap G$.

Lemma 4.6. *For any closed point $\mathcal{P}$ of X, and any prime $v \in \mathfrak{M}(k)$*

$$G_{\mathcal{P}}(k_v) = k_v^\times \cap \operatorname*{Norm}_{k(\mathcal{P})/k}(\mathbb{I}_{k(\mathcal{P})}).$$

Proof. From the definition of norms on idèles we know that

$$k_v^\times \cap \operatorname*{Norm}_{k(\mathcal{P})/k}(\mathbb{I}_{k(\mathcal{P})}) = \prod_{\omega|v} \operatorname*{Norm}_{\omega/v} k(\mathcal{P})_\omega^\times.$$

The lemma now follows at once from Lemma 4.5. □

Lemma 4.7. *For any prime $v \in \mathfrak{M}(k)$ and any $\omega \in \mathfrak{M}(l)$ above it, $G_f(k_v) \subseteq \operatorname{Norm}_{\omega/v}(l_\omega^\times)$.*

Proof. Recall that l/k is the unique abelian extension of k such that

$$\operatorname*{Norm}_{l/k}(C_l) = \prod_{\mathcal{P} \in X^c} \operatorname*{Norm}_{k(\mathcal{P})/k}(C_{k(\mathcal{P})})^{\operatorname{ord}_{\mathcal{P}}(f)}.$$

This is an equality of subgroups of $C_k := \mathbb{I}_k/k^\times$, and pulling back this relation from C_k to $\mathbb{I}_k$ we get

$$k^\times \operatorname*{Norm}_{l/k}(\mathbb{I}_l) = k^\times \prod_{\mathcal{P} \in X^c} \operatorname*{Norm}_{k(\mathcal{P})/k}(\mathbb{I}_{k(\mathcal{P})})^{\operatorname{ord}_{\mathcal{P}}(f)}.$$

Now we know from Lemma 4.6 that, for $\mathcal{P} \in X^c$,

$$k_v^\times \cap \operatorname*{Norm}_{k(\mathcal{P})/k}(\mathbb{I}_{k(\mathcal{P})}) = G_{\mathcal{P}}(k_v)$$

and so we deduce that

$$k_v^\times \cap \left(k^\times \operatorname*{Norm}_{l/k}(\mathbb{I}_l) \right) \supseteq \prod_{\mathcal{P} \in X^c} G_{\mathcal{P}}(k_v)^{\operatorname{ord}_{\mathcal{P}}(f)}.$$

From the definition (5), the right-hand side of this containment is $G_f(k_v)$. It is a well-known (and easy) consequence of Artin's reciprocity that

$$\operatorname*{Norm}_{\omega/v}(l_\omega^\times) = k_v^\times \cap \left(k^\times \operatorname*{Norm}_{l/k}(\mathbb{I}_l) \right).$$

Thus $G_f(k_v) \subseteq \operatorname{Norm}_{\omega/v}(l_\omega^\times)$ and this completes the proof. □

5. Proof of Theorem 1

In this section we prove Theorem 1; throughout we maintain the assumptions and notation of Theorem 1.

5.1. **Proof of part (a) of Theorem 1.** By Lemma 2.1 we have a homomorphism

$$\hat{f} \ : \ \mathrm{Pic}(X_v) \to k^\times / G_f(k_v),$$

given by

$$\hat{f}([\mathcal{Q}]) = \operatorname*{Norm}_{\mathcal{Q}}(f(\mathcal{Q}))G_f(k_v),$$

for $\mathcal{Q} \in X_v^c$ that is neither a pole nor a zero of f. By Lemma 4.7 we have $G_f(k_v) \subseteq \mathrm{Norm}_{\omega/v}(l_\omega^\times)$, and so $\hat{f}$ induces a homomorphism $\mathrm{Pic}(X_v) \to k^\times / \mathrm{Norm}_{\omega/v}(l_\omega^\times)$, which we may lazily call $\hat{f}$ also. By local class field theory, the local Artin map $\theta_v : k^\times \to \mathrm{Gal}(l/k)$ contains $\mathrm{Norm}_{\omega/v}(l_\omega^\times)$ in its kernel, and thus $\theta_v \circ \hat{f}$ is a well-defined homomorphism $\mathrm{Pic}(X_v) \to \mathrm{Gal}(l/k)$; this is precisely the desired homomorphism ϕ_v of part (a) of Theorem 1.

5.2. **Proof of part (b) of Theorem 1.** Let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be the distinct closed points of X belonging to the support of f. Let B the set of primes $v \in \mathfrak{M}(k)$ satisfying at least one of these conditions:

- v is archimedean;
- v is ramified in l/k;
- v is a prime of bad reduction for X (in other words the special fibre is singular);
- $\mathrm{ord}_v(f) \neq 0$, where v is here thought of as a place on $k(X)$.

It is clear that the set B is finite.

Suppose now that $v \notin B$. By Lemma 3.1, $\mathrm{Pic}(X_v)$ is generated by classes of closed points $\mathcal{Q}$ such that f is regular and non-zero at $\tilde{\mathcal{Q}}$. Thus that for such $\mathcal{Q}$,

$$\hat{f}([\mathcal{Q}]) = \operatorname*{Norm}_{\mathcal{Q}}(f(\mathcal{Q})) \in \mathcal{O}_v^\times.$$

But v is unramified in l/k. Thus local class field theory tells us that $\mathcal{O}_v^\times$ is contained in the kernel of the local Artin map θ_v (see for example [16, page 221]). Hence $\phi_v := \theta_v \circ \hat{f} = 1$. This completes the proof of part (b) of Theorem 1.

5.3. **Proof of part (c) of Theorem 1.** We would like to prove that the diagonal image of $\mathrm{Pic}(X)$ is contained in the kernel of the map (2). By part (b) we know that $\phi_v = 1$ for all $v \notin B$. Hence, it is sufficient to show that the diagonal image of $\mathrm{Pic}(X)$ is contained in the kernel of the map

$$\prod_{v \in \mathfrak{M}(k)} \mathrm{Pic}(X_v) \xrightarrow{\prod_{v \in \mathfrak{M}(k)} \phi_v} \mathrm{Gal}(l/k).$$

It is enough to show that the class of any $\mathcal{Q} \in X^c$ that is not in the support of f belongs to the kernel of the above map. But for such $\mathcal{Q}$ we see that

$$\prod \phi_v([\mathcal{Q}]) = \prod \theta_v(f(\mathcal{Q})) = 1,$$

by Artin's reciprocity law, since $f(\mathcal{Q}) \in k$. This completes the proof of Theorem 1.

6. Interpretation as Torsors under Tori

In this section we interpret the obstruction of Theorem 1 in terms of torsors under tori; we are grateful to Alexei Skorobogatov for pointing out this interpretation to us. This section is closely related to Section 4.4 of [27]. We write $\bar{X}$ to denote the base extension of X to the algebraic closure $\bar{k}$ of k. Let D denote the subgroup of $\operatorname{Div}\bar{X}$ generated by the points $\mathcal{P}$ such that $\operatorname{ord}_{\mathcal{P}}(f) \neq 0$, and consider the embedding $\mathbb{Z} \to D$ given by sending 1 to (f). This map of Galois modules has a quotient, which we denote by M:

$$0 \to \mathbb{Z} \xrightarrow{(f)} D \to M \to 0. \tag{9}$$

Note that M is torsion-free if and only if the $\operatorname{ord}_{\mathcal{P}}(f)$ are coprime.

We now want to consider the dual of the sequence (9). Recall that, if A is a finitely generated abelian group with a continuous action of $\operatorname{Gal}(\bar{k}/k)$, then there is an algebraic k-group of multiplicative type, which we will denote $G = \mathcal{H}om(A, \mathbb{G}_m)$, such that the points of G over a field $K \subseteq \bar{k}$ are the set $\mathcal{H}om(A, \bar{k}^\times)^{\Gamma_K}$, where Γ_K is the subgroup of $\operatorname{Gal}(\bar{k}/k)$ fixing K. We then have $\hat{G} = \mathcal{H}om(G, \mathbb{G}_m) \cong A$, and this correspondence is a contravariant equivalence of categories.

Let $S = \mathcal{H}om(M, \mathbb{G}_m)$ and $T = \mathcal{H}om(D, \mathbb{G}_m)$. The dual sequence to (9) is

$$0 \to S \to T \xrightarrow{N_f} \mathbb{G}_m \to 0. \tag{10}$$

It is clear that $D = \oplus_{\operatorname{ord}_{\mathcal{P}}(f)\neq 0} \operatorname{Ind}_{k(\mathcal{P})/k} \mathbb{Z}$, and a simple exercise shows that $T = \prod_{\operatorname{ord}_{\mathcal{P}}(f)\neq 0} \mathcal{R}_{k(\mathcal{P})/k}\mathbb{G}_m$, where $\mathcal{R}_{k(\mathcal{P})/k}$ is the Weil restriction functor. Further, one can compute that the map N_f is defined on each factor by $(N_{k(\mathcal{P})/k})^{\operatorname{ord}_{\mathcal{P}} f}$. We deduce that, for any field K containing k, the sequence (10) gives rise to an exact sequence

$$0 \to S(K) \to \prod_{\operatorname{ord}_{\mathcal{P}}(f)\neq 0} (k(\mathcal{P}) \otimes_k K)^\times \xrightarrow{N_f} K^\times \xrightarrow{\partial} H^1(K, S) \tag{11}$$

and so a map $K^\times/G_f(K) \to H^1(K, S)$ which we will use to identify our obstruction with that coming from a certain torsor under S.

The torsor in question is the variety $Y \to X$ given, away from the zeros and poles of f, by the local equation

$$\prod_{\operatorname{ord}_{\mathcal{P}}(f)\neq 0} (N_{k(\mathcal{P})/k} u_{\mathcal{P}})^{\operatorname{ord}_{\mathcal{P}} f} = f \tag{12}$$

where $u_{\mathcal{P}}$ is a variable in $k(\mathcal{P})$; by the general theory of [27, Section 4.4] this extends to a smooth variety over X. The fibre over any K-point of X is a K-torsor under S, and so we get a map $X(K) \to H^1(K, S)$ associating to each point the isomorphism class of its fibre. The obstruction coming from the torsor $Y \to X$ may be stated as follows. Let $(\mathcal{P}_v) \in \prod_v X(k_v)$ be an adelic point of X; then the maps $X(k_v) \to H^1(k_v, S)$ described above give us an element α of $\prod_v H^1(k_v, S)$. A necessary condition for the point $(\mathcal{P}_v)$ to come from a global point is that α lie in the image of $H^1(k, S)$.

For any finite extension L/K we can compose $X(L) \to H^1(L, S)$ with the corestriction $H^1(L, S) \to H^1(K, S)$. This allows us to define a map $\operatorname{Div} X_K \to H^1(K, S)$; and, since X is proper, this map in fact factors through $\operatorname{Pic} X_K$ (see Proposition 12 of [8]).

Theorem 2. *The obstruction of Theorem 1 is the same as that coming from the torsor $Y \to X$.*

The proof of the theorem relies on comparing the sequence coming from Poitou–Tate duality for S with the reciprocity map.

Lemma 6.1. *Let K be any field containing k. The diagram*

$$\begin{array}{ccc} \operatorname{Pic} X_K & \xrightarrow{f} & K^\times/G_f(K) \\ & \searrow & \downarrow \partial \\ & & H^1(K,S) \end{array}$$

commutes, where the diagonal arrow comes from the torsor $Y \to X$.

Proof. It is enough to show this for any point $\mathcal{P} \in X(K)$ outside the support of (f). The map ∂ takes an element $x \in K^\times$ to the class of the fibre $N_f^{-1}(x)$ (see [21, I, 5.4]). So the composition $\partial.f$ takes $\mathcal{P}$ to the class of the fibre $N_f^{-1}(f(\mathcal{P}))$, which by (12) is the same as the fibre of $Y \to X$ over $\mathcal{P}$. □

The following lemma will complete the proof of the theorem.

Lemma 6.2. *There is a diagram*

$$\begin{array}{ccccccc} k^\times/Nl^\times & \longrightarrow & \mathbb{I}_k/N\mathbb{I}_l & \xrightarrow{\theta} & \operatorname{Gal}(l/k) & \longrightarrow & 0 \\ \downarrow \partial & & \downarrow \prod_v \partial & & \downarrow & & \\ H^1(k,S) & \longrightarrow & \prod_v{}' H^1(k_v,S) & \longrightarrow & H^1(k,M)^* & \longrightarrow & 0 \end{array} \tag{13}$$

with exact rows, and which commutes up to sign. The notation $\prod'$ denotes the restricted product with respect to the unramified subgroups of $H^1(k_v,S)$.

Proof. The top row of the diagram is from class field theory, and the bottom row is from Poitou–Tate duality applied to M (see [19, I, 4.20]). We just need to check that they fit together as shown.

We take Ext groups (of $\operatorname{Gal}(\bar{k}/k)$-modules) from the sequence (9) to the second short exact sequence

$$0 \to \bar{k}^\times \to \mathbb{I}_{\bar{k}} \to C_{\bar{k}} \to 0$$

to get the following diagram.

$$\begin{array}{ccccc} \operatorname{Hom}_k(D,\bar{k}^\times) & \longrightarrow & \operatorname{Hom}_k(D,\mathbb{I}_{\bar{k}}) & \longrightarrow & \operatorname{Hom}_k(D,C_{\bar{k}}) \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Hom}_k(\mathbb{Z},\bar{k}^\times) & \longrightarrow & \operatorname{Hom}_k(\mathbb{Z},\mathbb{I}_{\bar{k}}) & \longrightarrow & \operatorname{Hom}_k(\mathbb{Z},C_{\bar{k}}) \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Ext}^1_k(M,\bar{k}^\times) & \longrightarrow & \operatorname{Ext}^1_k(M,\mathbb{I}_{\bar{k}}) & \longrightarrow & \operatorname{Ext}^1_k(M,C_{\bar{k}}) \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Ext}^1_k(D,\bar{k}^\times) & \longrightarrow & \operatorname{Ext}^1_k(D,\mathbb{I}_{\bar{k}}) & \longrightarrow & \operatorname{Ext}^1_k(D,C_{\bar{k}}) \end{array}$$

Using Lemmas 4.12 and 4.13 of Chapter I of [19], we can identify these groups with more familiar ones.

(14)
$$\begin{array}{ccccccc}
\prod_{\mathcal{P}} k(\mathcal{P})^\times & \longrightarrow & \prod_{\mathcal{P}} \mathbb{I}_{k(\mathcal{P})} & \longrightarrow & \prod_{\mathcal{P}} C_{k(\mathcal{P})} & \searrow & \\
\downarrow{\scriptstyle N_f} & & \downarrow{\scriptstyle N_f} & & \downarrow{\scriptstyle N_f} & & H^2(k,D)^* \\
k^\times & \longrightarrow & \mathbb{I}_k & \longrightarrow & C_k & \xrightarrow{\theta} & \downarrow \\
\downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \prod_v \partial} & & \downarrow & & \mathrm{Gal}(k^{\mathrm{ab}}/k) \\
H^1(k,S) & \longrightarrow & \prod_v{}' H^1(k_v,S) & \longrightarrow & \mathrm{Ext}^1(M,C_{\bar{k}}) & \xrightarrow{\sim} & \downarrow \\
\downarrow & & \downarrow & & \downarrow & & H^1(k,M)^* \\
0 & \longrightarrow & 0 & \longrightarrow & 0 & \xrightarrow{\sim} & \downarrow \\
 & & & & & & 0
\end{array}$$

Straight rows and columns are still exact here; the diagonal arrows come from the global duality pairing. The diagram commutes up to sign, and one can check that the maps marked as ∂ are indeed. We have defined l so that $N_{l/k}C_l$ coincides with the image in C_k of the map N_f; class field theory says that the reciprocity map θ induces an isomorphism between $C_k/N_{l/k}C_l$ and $\mathrm{Gal}(l/k)$. Putting all this together, we deduce the lemma. □

7. Relation to the Brauer–Manin obstruction

Using the results of the previous section, it is possible to show that the obstruction described in this article is equivalent to part of the Brauer–Manin obstruction. We will first briefly recall some definitions.

For the definition and properties of the Brauer group $\mathrm{Br}\, X$ of a scheme X, we refer the reader to [15]. For our purposes, it is enough to know that the Brauer group of a smooth, absolutely irreducible curve X over a number field k is a subgroup of the Brauer group of its function field, characterised by the following exact sequence:

$$0 \to \mathrm{Br}\, X \to H^2(k, k(\bar{X})^\times) \to H^2(k, \mathrm{Div}\, \bar{X}). \tag{15}$$

An element $\mathcal{A}$ of the Brauer group can be evaluated at a point $x \in X(K)$, where K is any field containing k, to obtain an element $\mathcal{A}(x)$ of $\mathrm{Br}\, K$. Let $X(\mathbb{A}_k)$ be the set of adelic points of X (which is equal to $\prod_v X(k_v)$ when X is complete, the product being over all places of k). We can define a map from $\mathrm{Br}\, X \times X(\mathbb{A}_k)$ to $\mathbb{Q}/\mathbb{Z}$ as follows:

$$(\mathcal{A}, (x_v)) \mapsto \sum_v \mathrm{inv}_v(\mathcal{A}(x_v)).$$

Manin [17] observed that, if (x_v) comes from a global point of X, then its image under this map must be 0. With this in mind, we define, for any subgroup B of $\mathrm{Br}\, X$,

$$X(\mathbb{A}_k)^B := \{(x_v) \in X(\mathbb{A}_k) \mid \sum_v \mathrm{inv}_v(\mathcal{A}(x_v)) = 0 \text{ for all } \mathcal{A} \in B\}.$$

If $X(\mathbb{A}_k)^B = \emptyset$ for some B, then it follows that $X(k) = \emptyset$ and we say that there is a *Brauer–Manin obstruction* to the existence of rational points on X, coming from B. The concept may be extended in an obvious way to give an obstruction to the existence of rational zero-cycles on X.

Elements of the Brauer group can be constructed using cup products, as follows. The character group of $\mathrm{Gal}(\bar{k}/k)$ can be identified with $H^1(k, \mathbb{Q}/\mathbb{Z})$. There is an isomorphism $\delta : H^1(k, \mathbb{Q}/\mathbb{Z}) \to H^2(k, \mathbb{Z})$ which is the boundary map of cohomology arising from the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Let $f \in k(X)^\times$ be a function on X, and let $\chi \in H^1(k, \mathbb{Q}/\mathbb{Z})$ be a character of the absolute Galois group of k. Then the cup-product pairing

$$H^0(k, k(\bar{X})) \times H^2(k, \mathbb{Z}) \to H^2(k, k(\bar{X}))$$

gives us an element $f \cup \delta\chi \in H^2(k, k(\bar{X}))$. With f and l as before, we will define $\mathcal{A}_\chi := f \cup \delta\chi$, and $\mathrm{Br}_f(X) := \{\mathcal{A}_\chi : \chi \in \mathrm{Gal}(l/k)^*\}$.

Theorem 3. (a) *Let χ be a character of $\mathrm{Gal}(l/k)$, which we identify with its lift to $\mathrm{Gal}(\bar{k}/k)$. Then $\mathcal{A}_\chi$ lies in the Brauer group of X.*

(b) *The obstruction of Theorem 1 is equivalent to the Brauer–Manin obstruction associated to $\mathrm{Br}_f(X)$.*

Proof. To prove (a), we will show that $(f) \cup \delta\chi = 0$ in $H^2(k, \mathrm{Div}\, \bar{X})$. By (15), this will show that $\mathcal{A}_\chi$ lies in $\mathrm{Br}\, X$.

Consider the right-hand column of the diagram (14). This is dual to

$$0 \to H^1(k, M) \to H^2(k, \mathbb{Z}) \xrightarrow{(f)} H^2(k, D)$$

which is part of the long exact sequence in cohomology coming from (9). By reciprocity and the definition of l, the kernel of the map (f) is identified with $H^2(l/k, \mathbb{Z})$. Now note that the map (f) is the same as the cup-product map $x \mapsto (f) \cup x$, because on cochains they are both simply multiplication by (f). Since χ comes from a character on $\mathrm{Gal}(l/k)$, we have $\delta\chi \in H^2(l/k, \mathbb{Z})$ and therefore $(f) \cup \delta\chi = 0$ in $H^2(k, D) \subseteq H^2(k, \mathrm{Div}\, \bar{X})$.

To prove (b), we use the well-known equation characterising the local Artin reciprocity map: for $x \in k_v^\times$ and $\chi \in \mathrm{Gal}(\bar{k_v}/k_v)^*$, we have $\mathrm{inv}_v(x \cup \delta\chi) = \chi(\theta_v(x))$. Now let $(x_v) \in X(\mathbb{A}_k)$ be an adelic point of X. We have

$$\mathrm{inv}_v(\mathcal{A}_\chi(x_v)) = \mathrm{inv}_v(f(x_v) \cup \delta\chi) = \chi(\theta_v(f(x_v)))$$

and therefore

$$\theta(f(x)) = 0 \quad \text{if and only if} \quad \sum_v \mathrm{inv}_v(\mathcal{A}_\chi(x_v)) = 0 \text{ for all } \chi \in \mathrm{Gal}(l/k)^*$$

that is, $\theta(f(x)) = 0$ if and only if $x \in X(\mathbb{A}_k)^{\mathrm{Br}_f(X)}$. The extension to Picard groups is straightforward. □

8. Harmful Functions and Harmless Functions

Recall that X is a smooth curve over the number field k, f is a non-constant element of $k(X)$, and l is the class field of k belonging to the function f. In Theorem 1, we constructed an explicit homomorphism

$$\prod \mathrm{Pic}(X_v) \to \mathrm{Gal}(l/k)$$

such that the image of $\mathrm{Pic}(X)$ in $\prod \mathrm{Pic}(X_v)$ is contained in the kernel of this map. We went on in the introduction to explain how this might obstruct the existence of divisors of certain degrees. Of course all this is useless if $l = k$. We call f harmful if $l \neq k$, and harmless if $l = k$; the motivation for the terminology is that a harmful function might 'harm' the Hasse principle.

Most functions chosen at random turn out to be harmless and so do not obstruct the Hasse principle. In this section we give some examples of harmful functions on curves. Readers are invited to construct harmful functions for their favourite families of curves using the results below as a model.

Proposition 8.1. *Suppose that* $\mathrm{div}(f)$ *is a norm for some non-trivial abelian extension* k'/k. *Then* f *is harmful and* $k' \subseteq l$ *where* l *is the class field belonging to* f.

Proof. Write $\mathrm{div}(f) = \sum n_i \mathcal{P}_i$. It is immediate from the hypotheses that

$$\prod_{\mathcal{P}_i} \mathrm{Norm}(C_{k(\mathcal{P}_i)})^{n_i} \subseteq \mathrm{Norm}_{k'/k}(C_{k'}).$$

But the left-hand side is by definition $\mathrm{Norm}_{l/k}(C_l)$. It is immediate that $k' \subseteq l$. □

Our next two results are concerned with explicit examples of harmful functions for certain families of curves.

Corollary 8.2. *Let* X *be the double cover of the projective line given by an affine equation*

$$X: \quad y^2 = h(x)$$

where $h(x) \in k[x]$ *is a square-free polynomial. Suppose that* $\alpha, \beta \in k$ *are such that* $h(\alpha), h(\beta)$ *are non-zero, non-square and* $\sqrt{h(\alpha)}$ *and* $\sqrt{h(\beta)}$ *generate the same quadratic extension of* k. *Then the function*

$$f = \frac{x-\alpha}{x-\beta}$$

is harmful, and the class field belonging to f *is* $l = k(\sqrt{h(\alpha)})$.

Proof. Let $k' = k(\sqrt{h(\alpha)})$. Let $\mathcal{P}_\alpha, \mathcal{P}_\beta$ be the points

$$\mathcal{P}_\alpha = \{(\alpha, \sqrt{h(\alpha)}), (\alpha, -\sqrt{h(\alpha)})\}$$
$$\mathcal{P}_\beta = \{(\beta, \sqrt{h(\beta)}), (\beta, -\sqrt{h(\beta)})\}$$

Clearly the divisor of f is $\mathcal{P}_\alpha - \mathcal{P}_\beta$. The residue fields of $\mathcal{P}_\alpha$ and $\mathcal{P}_\beta$ are both isomorphic to k'. Thus

$$\mathrm{Norm}(C_l) = \mathrm{Norm}(C_{k'})\,\mathrm{Norm}(C_{k'})^{-1} = \mathrm{Norm}(C_{k'}).$$

Since l and k' are both abelian extensions of k we see that

$$l = k' = k(\sqrt{h(\alpha)}).$$

□

It is easy to formulate and prove a generalization of Corollary 8.2 to cyclic covers of the projective line provided the field k contains the appropriate root of unity.

Corollary 8.3. *Let* X *be the genus* 1 *curve*

$$X: \quad y^2 = ax^4 + bx^3 + cx^2 + dx + e,$$

where the polynomial on the right-hand side is square-free, defined over k, *and* $a \neq 0$. *Let* $\alpha \in k^\times$ *and let*

$$f = y - \left(\frac{b}{2\alpha}x^2 + \alpha x + \frac{d}{2\alpha}\right),$$

and note that

$$ax^4 + bx^3 + cx^2 + dx + e - \left(\frac{b}{2\alpha}x^2 + \alpha x + \frac{d}{2\alpha}\right)^2 = \beta x^4 + \gamma x^2 + \delta$$

for some $\beta, \gamma, \delta \in k$. Suppose that $\beta x^4 + \gamma x^2 + \delta$ is irreducible with $\beta\delta$ and $(\gamma^2 - 4\beta\delta)\beta\delta$ both being non-zero and non-square in k. Then f is harmful and $l = k(\sqrt{\gamma^2 - 4\beta\delta})$.

Proof. Suppose a is a non-square, the proof being similar in the case a is a square. Let $\mathcal{P}_\infty$ be the point that corresponds to the (conjugate) pair of elements of $X(\overline{k})$ at infinity. Clearly $k(\mathcal{P}_\infty) = k(\sqrt{a})$. Let $\mu_1, \ldots, \mu_4$ denote the four roots of $\beta x^4 + \gamma x^2 + \delta$, and let

$$\eta_i = \frac{b}{2\alpha}\mu_i^2 + \alpha\mu_i + \frac{d}{2\alpha}.$$

Write

$$\mathcal{P}_0 = \{(\mu_1, \eta_1), \ldots, (\mu_4, \eta_4)\};$$

clearly $\mathcal{P}_0 \in X$ with residue field isomorphic to $k(\mu_1)$. The divisor of f is $\mathcal{P}_0 - 2\mathcal{P}_\infty$. Thus

$$\mathrm{Norm}(C_l) = \mathrm{Norm}(C_{k(\mu_1)})\,\mathrm{Norm}(C_{k(\sqrt{a})})^{-2}.$$

The conditions of the corollary ensure that the Galois group of $\beta x^4 + \gamma x^2 + \delta$ is D_8 (see [20, page 63]). Clearly, the (degree 4) extension $k(\mu_1)/k$ is not Galois, and hence not abelian. Therefore the maximal abelian subextension of $k(\mu_1)$ is $k' = k(\sqrt{\gamma^2 - 4\beta\delta})$. By the Norm Limitation Theorem ([16, pages 208–211])

$$\mathrm{Norm}(C_{k(\mu_1)}) = \mathrm{Norm}(C_{k'}).$$

Further

$$\mathrm{Norm}(C_{k(\sqrt{a})})^{-2} \subseteq C_k^2 \subseteq \mathrm{Norm}(C_{k'}),$$

since k'/k is a quadratic extension. Hence

$$\mathrm{Norm}(C_l) = \mathrm{Norm}(C_{k'})$$

and this implies that $l = k' = k(\sqrt{\gamma^2 - 4\beta\delta})$. □

9. 2-Coverings of Elliptic Curves

In this section we restrict ourselves to genus 1 curves of the form

$$X : \; y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

where $a, b, c, d, e \in \mathbb{Z}$ and the polynomial on the right-hand side is separable. The curves X are 2-coverings of elliptic curves. We let the ground field be $k = \mathbb{Q}$. We shall always assume that X has degree 1 points everywhere locally, and that we want to prove the non-existence of degree 1 points over $\mathbb{Q}$ if possible. Curves X arise naturally in 2-descent algorithms for elliptic curves. If we have an algorithm for deciding the existence of rational points on curves X, we would have an algorithm for computing Mordell–Weil groups of elliptic curves over the rationals; for more on this see [10, Section 3.6]. The reader may also like to compare what follows with [18], [5], and [22]. In particular, the crude and tentative approach taken in [22] was one of the main inspirations behind the current paper.

We suppose that f is a harmful function arising as in Corollary 8.2. Let l be the class field belonging to f which must be a quadratic field. Hence we can write $l = \mathbb{Q}(\sqrt{D})$ for some square-free integer $D \neq 1$. From Theorem 1 we know of the

existence of a finite set B of primes such that the image of $\mathrm{Pic}(X)$ in $\prod_{p\in B}\mathrm{Pic}(X_p)$ is in the kernel of

$$\prod_{p\in B}\mathrm{Pic}(X_p)\xrightarrow{\prod_{p\in B}\phi_p}\mathrm{Gal}(l/\mathbb{Q}). \tag{16}$$

To put this to use we need to look at how to compute the following:

(a) $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$ for any given prime p.
(b) The local Artin map θ_p.
(c) A suitable set of primes B, such that $\phi_p = 1$ for $p \notin B$.

9.1. **Computing** $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$**.** What we mean is to compute a $\mathbb{Z}/2\mathbb{Z}$-basis for $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$ for a fixed prime p. To simplify the computations that will come later we insist that this basis satisfies the following two conditions:

(i) The elements of this basis are all (classes of) points of degree 1.
(ii) None of these elements are zeros or poles of f.

We show that this is possible and explain how to construct such a basis simultaneously.

First recall our assumption that the curve X has degree 1 points everywhere locally, and so degree 1 points over $\mathbb{Q}_p$. Thus let $P_0 \in X(\mathbb{Q}_p)$. For how to compute such a point see [10, pages 80–82]. In fact the algorithm for finding such a P_0 has steps where one can make infinitely many choices of a certain parameter, and each choice leads to a different point P_0. By making a suitable choice we can ensure that $P_0 \in X(\mathbb{Q}_p)$ is neither a zero nor a pole of f. Next we can construct an explicit parameterization

$$\rho : E(\mathbb{Q}_p) \to X(\mathbb{Q}_p)$$

for some Weierstrass elliptic curve E (the Jacobian of X) defined over $\mathbb{Q}_p$, such that $\rho(O) = P_0$ (for this see [4, pages 35–36]). It follows that $E(\mathbb{Q}_p)$ is isomorphic to $\mathrm{Pic}^0(X_p)$ via the map sending $Q \in E(\mathbb{Q}_p)$ to the class of $\rho(Q) - P_0$. One knows how to compute $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ (see [25]). Let $Q_1, \ldots, Q_r$ be a basis for $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$. We can 'adjust' $Q_1, \ldots, Q_r$, if necessary, by adding suitable elements of $2E(\mathbb{Q}_p)$, so as to make all of the $\rho(Q_i)$ neither zeros nor poles of f. Let $P_i = \rho(Q_i)$ for $i = 1, \ldots, r$. It follows from what has been said so far that the classes of $P_0, \ldots, P_r$ are a basis for $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$ satisfying the conditions (i) and (ii) above.

Perhaps it is helpful to say something about the p-adic precision needed. Basically, we need below to compute the local Artin map for $f(P_i)$. If $\mathrm{ord}_p(f(P_i)) = r_i$ then we need $f(P_i)$ modulo p^{r_i+1} if p is odd and modulo 2^{r_i+3} for $p = 2$. This enables us to decide if the points P_i have been computed to enough p-adic precision, and if not we simply recompute them to a sufficient precision.

9.2. **The local Artin map** θ_p**.** Recall that the class field l is a quadratic extension of $\mathbb{Q}$, and that we wrote $l = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer. We identify $\mathrm{Gal}\,(l/\mathbb{Q})$ with the (multiplicative) group of two elements $\{1, -1\}$. Thus $\theta_p : \mathbb{Q}_p^\times \to \{1, -1\}$ is the map that sends an element $\alpha \in \mathbb{Q}_p$ to 1 if α is a local norm, and -1 if α is not a local norm. Note that if $\alpha \in \mathbb{Q}_p$ then $\theta_p(\alpha)$ is just the Hilbert symbol $(\alpha, D)_p$, and can easily be determined from standard formulae for the Hilbert symbol as in [7, pages 161–162].

9.3. **The Set of 'Bad Primes' B.** We now come to the problem of explicitly constructing the set B with the property that if p is a prime not included in B then $\hat{\phi}_p = 1$. Whilst we can use the recipe given in page 10, it is easier to construct a suitable set B from scratch.

For our curve X above let $h(x) = ax^4 + bx^3 + cx^2 + dx + e$. Suppose $\alpha, \beta \in \mathbb{Q}$ such that $\sqrt{h(\alpha)}$, $\sqrt{h(\beta)}$ generate the same quadratic extension, and let

$$f = \frac{x - \alpha}{x - \beta}. \tag{17}$$

That is f is arising as in Corollary 8.2. From that result the class field belonging to f is $l = \mathbb{Q}(\sqrt{D})$, where D is the square-free part of $h(\alpha)$ (and is the square-free part of $h(\beta)$ as well). Let B be the set containing the ramified primes (i.e. those dividing the discriminant of l), 2 unless it is split, the primes belonging to the denominators of α, β unless they are split, and the primes belonging to the support of $h(\alpha), h(\beta)$ unless they are split. The archimedean prime ∞ is included only if l is complex.

Lemma 9.1. *For all $p \notin B$, we have $\hat{\phi}_p = 1$.*

Proof. We have excluded all split primes from B for the following reason: if p is split then $l_\omega = \mathbb{Q}_p$ (for any prime ω of l above p), and since $\hat{\phi}_p$ is a homomorphism

$$\hat{\phi}_p : \mathrm{Pic}(X_p) \to \mathbb{Q}_p / \mathrm{Norm}(l_\omega^\times)$$

we see that $\hat{\phi}_p = 1$. Similarly, if l is real then $\hat{\phi} = 1$.

Suppose $p \notin B$ and we would like to show that $\hat{\phi}_p = 1$. We may assume that p is non-archimedean, odd and (from the above) inert. Since B contains all the ramified primes, we reduce to the case when p is non-split, and hence $\left(\frac{D}{p}\right) = -1$.

Clearly $2\,\mathrm{Pic}(X_p)$ is in the kernel of $\hat{\phi}_p$, and we know from the discussion above that $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$ has a basis consisting of degree 1 points that are neither zeros nor poles of f. It is sufficient to show that for every $P \in X(\mathbb{Q}_p)$ that is neither a zero nor a pole of f we have $\hat{\phi}_p([P]) = 1$. From the definition of $\hat{\phi}_p$ we see that we must prove, for any such such a point, that $f(P) \in \mathrm{Norm}(l_\omega^\times)$. We claim that $\upsilon_p(f(P)) = 0$. Since p is unramified, local class field theory tells us that $\mathrm{Norm}(\mathcal{O}_\omega^\times) = \mathbb{Z}_p^\times$. It follows from our claim that $f(P) \in \mathbb{Z}_p^\times$.

Thus to complete our proof all that remains is to prove that $\upsilon_p(f(P)) = 0$. Rearranging (17), we see that $x = (\beta f - \alpha)/(f - 1)$. Substituting into the equation for X and clearing the denominators we get

$$g^2 = a'f^4 + b'f^3 + c'f^2 + d'f + e' \tag{18}$$

where $g = y(f-1)$, $a' = h(\beta), e' = h(\alpha)$. Now from the definition of B we know that $\alpha, \beta \in \mathbb{Z}_p$, and so $a', \ldots, e' \in \mathbb{Z}_p$. If $\upsilon_p(f(P)) < 0$ then $\left(\frac{a'}{p}\right) = 1$, and if $\upsilon_p(f(P)) > 0$ then $\left(\frac{e'}{p}\right) = 1$. However it is easy to see that both must be -1 (since they are both equivalent to D modulo squares) and hence $\upsilon_p(f(P)) = 0$. □

9.4. **An Example.** The first *optimal* elliptic curve in Cremona's tables having non-trivial Tate–Shafarevich group is the curve $571A$. This is not the first elliptic curve with non-trivial Tate–Shafarevich group (as observed in [9]), but for us it is a natural example as it is treated elsewhere by more complicated methods (see below). Here the Tate–Shafarevich group has order 4 and so has 3 non-trivial elements of order 2. These elements can be represented as genus 1 double covers

of the projective line. We apply the above to one of these elements of order 2, represented by the curve:

$$X : y^2 = -727x^4 - 104x^3 + 92x^2 + 4x - 4.$$

This curve is treated in [18, page 402], [5] and [22], though we claim that our treatment here is the most elegant to date. Let $h(x) = -727x^4 - 104x^3 + 92x^2 + 4x - 4$. Note that

$$h(0) = -1 \times 2^2, \qquad h\left(\frac{-16}{53}\right) = \frac{-1 \times 2^2}{53^4}.$$

Corollary 8.2 suggests that we let

$$f = \frac{1}{x}\left(x + \frac{16}{53}\right).$$

The corresponding class field is $l = \mathbb{Q}(i)$. We can take the set $B = \{\infty, 2\}$ (the prime 53 is split). The following table summarizes the results of the calculations using the method outlined above:

Primes	Basis for $\mathrm{Pic}(X_p)/2\,\mathrm{Pic}(X_p)$	$f(P)$	$\phi_p(P)$
$p = \infty$	$P_0 = (-0.3018, 0.0003\ldots)$	$-0.00028\ldots$	-1
$p = 2$	$P_0 = (2^{-1}, 2^{-2} + 1 + 2 + \ldots)$	$1 + 2^5 + \ldots$	1
	$P_1 = (2^{-4} + 2^{-1} + \ldots, 2^{-8} + 2^{-6} + \ldots)$	$1 + 2^8 + \ldots$	1

Thus for any divisor class $[D]$ in $\mathrm{Pic}(X_\infty)$ we have that $\phi_\infty([D]) = (-1)^{\deg(D)}$. Also for any divisor class $[D]$ in $\mathrm{Pic}(X_2)$ we have that $\phi_2([D]) = 1$. Hence if $[D]$ is a divisor class in $\mathrm{Pic}(X)$ then

$$\prod_{p \in B} \phi_p([D]) = (-1)^{\deg(D)}.$$

However $\mathrm{Pic}(X)$ is in the kernel of $\prod \phi_p$. It is immediate that X does not have any rational divisors of odd degree. In particular X does not have any rational points of degree 1.

References

[1] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: an experiment*, to appear in Experimental Math.

[2] J. W. S. Cassels, *Survey article: Diophantine equations with special reference to elliptic curves*, Journal of the London Mathematical Society **41** (1966), 193–291.

[3] J. W. S. Cassels, *Global Fields*, pages 42–84 in [6].

[4] J. W. S. Cassels, *Lectures on elliptic curves*, LMS Student texts **24**, Cambridge University Press, 1991.

[5] J. W. S. Cassels, *Second descents for elliptic curves*, J. reine angew. Math. **494** (1998), 101–127.

[6] J. W. S. Cassels, A. Fröhlich (Eds), *Algebraic Number Theory*, Academic Press, 1967.

[7] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer-Verlag, 1978.

[8] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. series 4, vol **10** no 2 (1977), pp. 175–229.

[9] J. E. Cremona, *The Analytic Order of* Ш *for modular elliptic curves*, Journal de théorie des nombres de Bordeaux **5** (1993), no. 1, 179–184.

[10] J. E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, 1997.

[11] D. Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry*, Springer-Verlag, 1994.

[12] A. Fröhlich, M. J. Taylor, *Algebraic number theory*, Cambridge Studies in advanced mathematics **27**, Cambridge University Press, 1991.
[13] A. Grothendieck, *Éléments de géométrie algébrique II. Étude globale élémentaire de quelques classes de morphismes*, Inst. Hautes Études Sci. Publ. Math. **8**, 1961.
[14] A. Grothendieck, *Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. **20**, 1964.
[15] A. Grothendieck, *Le Groupe de Brauer. I, II, III*, pages 46–188 of *Dix Exposés sur la Cohomologie des Schémas*, A. Grothendieck and N. H. Kuipers (eds.), North–Holland, 1968.
[16] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1994.
[17] Yu. I. Manin, *Le Groupe de Brauer-Grothendieck en géométrie diophantienne*, pages 401–411 of *Actes Congrès Int. Math. Nice*, 1970, tome **I**, Gauthier-Villars, 1971.
[18] J. R. Merriman, S. Siksek, N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **LXXVII.4** (1996), 358–404.
[19] J. S. Milne, *Arithmetic Duality Theorems*, Academic Press, 1986.
[20] J. Rotman, *Galois Theory*, Springer-Verlag, 1990.
[21] J.-P. Serre, *Cohomologie Galoisienne*, 5ème éd., Lecture Notes. Math. **5**, Springer-Verlag, 1994.
[22] S. Siksek, *Sieving for rational points on hyperelliptic curves*, Mathematics of Computation **70** (2001), 1661–1674.
[23] S. Siksek, *Descent on Picard groups using functions on curves*, Bulletin of the Australian Mathematical Society **66** (2002), 119–124.
[24] S. Siksek and A. Skorobogatov, *On a Shimura curve that is a counterexample to the Hasse principle*, Bulletin of the London Mathematical Society **35** (2003), 409–414.
[25] S. Siksek and N. P. Smart, *On the complexity of computing the 2-Selmer group of an elliptic curve*, Glasgow Mathematical Journal **39** (1997), 251–257.
[26] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, 1986.
[27] A. N. Skorobogatov, *Torsors and rational points*, Cambridge University Press, 2001.
[28] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56.

Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom
E-mail address: M.Bright@bristol.ac.uk

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: S.Siksek@warwick.ac.uk