EFFECTIVITY OF BRAUER–MANIN OBSTRUCTIONS

ANDREW KRESCH AND YURI TSCHINKEL

Abstract. We study Brauer–Manin obstructions to the Hasse principle and to weak approximation, with special regard to effectivity questions.

1. Introduction

Let k be a number field, X be a smooth projective (geometrically irreducible) variety over k, and $X(k)$ its set of k-rational points. An important problem in arithmetic geometry is to find an effective procedure to determine whether $X(k) \neq \emptyset$. A necessary condition is that $X(k_v) \neq \emptyset$ for all completions k_v of k. This condition can be tested effectively and easily, given the defining equations for X. One says that X *satisfies the Hasse principle* when

$$X(k) \neq \emptyset \Leftrightarrow X(k_v) \neq \emptyset \ \forall v. \tag{1.1}$$

When X is a quadric hypersurface (of arbitrary dimension) over the rational numbers, the validity of (1.1) was established in 1921 by Hasse in his doctoral thesis [Has23a]. The statement (1.1) was proposed as a *principle* by Hasse in 1924 [Has24], where it was proved to hold for quadric hypersurfaces over arbitrary number fields. Hasse's main insight was to relate the existence of solutions to equations over a number field to existence of solutions over its completions, i.e., the v-adic numbers, which had been introduced and developed into a theory by his thesis advisor Hensel [Hen08]. In fact, Hensel had studied v-adic solutions to quadratic equations (see [Hen13] Chapter 12), obtaining necessary and sufficient conditions for local solvability. Earlier, Minkowski had defined a complete system of invariants of quadratic forms over the rationals, one at each prime p [Min90]; the Hasse principle for quadratic forms [Has23b] (or in other settings) is often referred to as the Hasse–Minkowski principle.

A related problem in arithmetic geometry is to find k-rational points on X matching local data, i.e., determining whether or not $X(k)$ is dense in the adelic space

$$X(\mathbb{A}_k) = \prod_v X(k_v).$$

(The adelic space is equipped with the product topology.) In this case one says that X *satisfies weak approximation.*

The Hasse principle, and weak approximation, are known to fail for general projective varieties, e.g., cubic curves and cubic surfaces. Counterexamples to the Hasse principle appeared as early as 1880 [Pép80]. (For a discussion, and proofs of the claims that appeared at that time, see [Lem03].) By the early 1940's it was well established that genus 1 curves may fail to satisfy the Hasse principle [Lin40], [Rei42].

Date: December 24, 2007.

2000 *Mathematics Subject Classification.* 14G25 (primary); 14F22 (secondary).

The first author was supported by an Alexander von Humboldt Foundation Research Fellowship. The second author was supported by the NSF.

All known obstructions to the Hasse principle and weak approximation are based on the *Brauer–Manin obstruction* defined by Manin [Man71] or reduce to this after finite étale covers of X [Sko99]. The Brauer–Manin obstruction is based on the Brauer group $\mathrm{Br}(X)$ of X and class field theory for k. It cuts out a subspace $X(\mathbb{A}_k)^{\mathrm{Br}}$ of the adelic space $X(\mathbb{A}_k)$ with the property that $X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}}$. In particular, if $X(\mathbb{A}_k) \neq \emptyset$ and $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$, then $X(k) = \emptyset$ and X fails to satisfy the Hasse principle. If $X(k) \neq \emptyset$ and $X(\mathbb{A}_k)^{\mathrm{Br}} \neq X(\mathbb{A}_k)$ then weak approximation fails for X. In the former case, we speak of a *Brauer–Manin obstruction to the Hasse principle*, and in the latter case, of a *Brauer–Manin obstruction to weak approximation*. We explain this in Section 3.

For geometrically rational surfaces, one expects that the Brauer–Manin obstruction is the only obstruction to the Hasse principle and to weak approximation [CTS80]. However, the explicit computation of this obstruction is a nontrivial task, even in such concrete classical cases as cubic surfaces over $\mathbb{Q}$ [CTKS87].

In this note, we prove (Theorem 3.4) that there is a general procedure for computing this obstruction, provided the geometric Picard group is finitely generated, torsion free, and known explicitly by means of cycle representatives with an explicit Galois action, and the geometric Brauer group is trivial (see Section 2 for the precise requirements). In particular this procedure is applicable to all del Pezzo surfaces.

The procedure is presented in Section 5. It involves several steps, which we now summarize. A splitting field (a finite extension of k over which all the cycle representatives are defined) must be chosen; this is taken to be Galois. The first Galois cohomology group of the geometric Picard group can be identified abstractly with a Brauer group. Generators, which are 1-cocycles for group cohomology, are computed. The next step is to obtain cocycle data for Brauer group elements from these generators, i.e., 2-cocycles of rational functions on X. With this, the computation of the subspace of $X(\mathbb{A}_k)$ cut out by these Brauer group elements is carried out. The description of the Brauer–Manin obstruction for conic bundles over $\mathbb{P}^1$ in [CTS87] (given in the language of universal torsors) can be viewed an effective algorithm in this setting, as can [CTKS87], [KT04] for diagonal cubic surfaces. Results in this direction have also been discussed in [BSD04], [Bri07]. A `Magma` package for degree 4 del Pezzo surfaces is available [Log04].

2. Preliminaries

In this section we introduce notation and give details of the input data required for the algorithm of Section 5. We fix a number field k and a smooth projective geometrically irreducible variety X over k. When K/k is a field extension, we write X_K for the base change of X to K. We write $\mathrm{Gal}(K/k)$ for the Galois group when the extension is normal. The Picard group of X is denoted $\mathrm{Pic}(X)$.

Assumption 2.1. We suppose that we are given explicit equations defining X in $\mathbb{P}^N$, i.e., generators $f_1, \ldots, f_r$, of the ideal $\mathcal{J} = \mathcal{J}(X) \subset k[x_0, \ldots, x_N]$. We assume that $X(\mathbb{A}_k) \neq \emptyset$, that $\mathrm{Pic}(X_{\bar{k}})$ is torsion free, and that the following are specified:

(1) a collection of codimension one geometric cycles $D_1, \ldots, D_m \in Z^1(X_{\bar{k}})$ whose classes generate $\mathrm{Pic}(X_{\bar{k}})$, i.e., there is an exact sequence of abelian groups

$$0 \to R \to \bigoplus_{i=1}^{m} \mathbb{Z} \cdot [D_i] \to \mathrm{Pic}(X_{\bar{k}}) \to 0; \tag{2.1}$$

(2) the subgroup of relations R;
(3) a finite Galois extension K of k, over which the D_i are defined, with known Galois group
$$G := \mathrm{Gal}(K/k);$$
(4) the action of G on $\mathrm{Pic}(X_{\bar{k}})$.

For simplicity, we assume that the cycles in (1) are effective, and the collection of cycles is closed under the Galois action.

We adopt the convention that the Galois action on the splitting field is a left action, written $\alpha \mapsto {}^g\alpha$ ($g \in G$, $\alpha \in K$). Hence there is an induced right action of G on X_K, which we denote by $a_g \colon X_K \to X_K$. For a divisor D on X_K we denote $a_g^* D$ by ${}^gD$. The action of G on $\mathrm{Pic}(X_{\bar{k}})$, mentioned in (4), is the action of pullback by a_g, meaning that $g \in G$ sends the class of D to the class of ${}^gD$.

Example. Let X be a del Pezzo surface of degree $d \le 4$. (Note that Hasse principle and weak approximation hold for $d \ge 5$ [Man74].) It is known that $X_{\bar{k}}$ is isomorphic to a blow-up of $\mathbb{P}^2$ in $9 - d$ points. For $d = 3$, 4, the anticanonical class $-\omega_X$ gives an embedding $X \hookrightarrow \mathbb{P}^d$; this supplies the ideal $\mathcal{J}$. When $d = 2$ we get an embedding $X \hookrightarrow \mathbb{P}(1,1,1,2) \hookrightarrow \mathbb{P}^6$ from $-2\omega_X$, and when $d = 1$ we get a embedding $X \hookrightarrow \mathbb{P}(1,1,2,3) \hookrightarrow \mathbb{P}^{22}$ by $-6\omega_X$.

There is a finite collection of exceptional curves on $X_{\bar{k}}$, with explicit equations. For instance, when $d = 3$, $X \subset \mathbb{P}^3$ is a (smooth) cubic surface, and [Sou17] gives a procedure for the determination of the lines on X.

The classes of the exceptional curves generate $\mathrm{Pic}(X_{\bar{k}})$. The number n_d of these curves is given in the following table:

d	1	2	3	4
n_d	240	56	27	16

We may take $m = n_d$ in the exact sequence (2.1). Furthermore, we know that $\mathrm{Pic}(X_{\bar{k}})$ is isomorphic to $\mathbb{Z}^{10-d}$. Intersection numbers of curves on X are readily computed, and R can be obtained using the fact that the intersection pairing on $\mathrm{Pic}(X_{\bar{k}})$ is nondegenerate. The Galois group $G = \mathrm{Gal}(K/k)$ acts by permutations on the set of exceptional curves, and thus on their classes in $\mathrm{Pic}(X_{\bar{k}})$.

In this paper, we make use of computations of group cohomology, cf. [Bro94]. For G a finite group, any resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module (by finite free $\mathbb{Z}[G]$-modules) defines the cohomology $H^i(G, M)$ of a G-module M, as the ith cohomology of the complex obtained by applying the functor $\mathrm{Hom}(-, M)$. We write $(\mathsf{C}^\bullet(M), \partial)$ for this complex. (This complex depends on the choice of resolution, which we suppress in the notation; the cohomology is an invariant of M.) We write $M^G = H^0(G, M)$ for the submodule of M of G-invariant elements.

3. The Brauer–Manin obstruction

In this section we recall basic facts about the Brauer groups of fields and schemes. The Brauer group $\mathrm{Br}(F)$ of a field F is the group of equivalence classes of central simple algebras over F. The Brauer group $\mathrm{Br}(X)$ of a Noetherian scheme X, defined by Grothendieck [Gro68], is the group of equivalence classes of sheaves of Azumaya algebras on X. It injects naturally into the cohomological Brauer group $\mathrm{Br}'(X)$, defined as the torsion subgroup of $H^2(X, \mathbb{G}_m)$, étale cohomology of the sheaf $\mathbb{G}_m$ of invertible regular functions (multiplicative group scheme). For X projective over a field (or more generally, arbitrary X possessing an ample invertible sheaf), $\mathrm{Br}(X) = \mathrm{Br}'(X)$ by a result of Gabber (see [dJ05]).

By class field theory (see, e.g., [CF67]), the Brauer group of a number field k fits in an exact sequence

$$0 \to \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z} \to 0 \tag{3.1}$$

where the direct sum is over completions v of k. The Brauer groups of the fields k_v are known by local class field theory. More precisely, there is a *local invariant*

$$\mathrm{inv}_v \colon \mathrm{Br}(k_v) \xrightarrow{\sim} \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{when} \quad v \nmid \infty \\ (\frac{1}{2}\mathbb{Z})/\mathbb{Z} & \text{when} \quad k_v = \mathbb{R} \\ 0 & \text{when} \quad k_v = \mathbb{C} \end{cases} \tag{3.2}$$

In (3.1),

$$\mathrm{inv} = \sum_v \mathrm{inv}_v.$$

Define

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \big\{\, (x_v) \in X(\mathbb{A}_k) \,\big|\, \sum_v \mathrm{inv}_v(A(x_v)) = 0 \ \ \forall A \in \mathrm{Br}(X) \,\big\}. \tag{3.3}$$

By (3.1), $X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}}$.

The Leray spectral sequence

$$H^p(\mathrm{Gal}(\bar{k}/k), H^q(X_{\bar{k}}, \mathbb{G}_m)) \Rightarrow H^{p+q}(X, \mathbb{G}_m) \tag{3.4}$$

and the vanishing of $H^3(\mathrm{Gal}(\bar{k}/k), \bar{k}^*)$ (see [AT68, §7.4]) give rise to an exact sequence

$$\begin{aligned} &0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(X_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)} \to \\ &\qquad \mathrm{Br}(k) \to \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}})) \to H^1(\mathrm{Gal}(\bar{k}/k), \mathrm{Pic}(X_{\bar{k}})) \to 0. \end{aligned} \tag{3.5}$$

Our assumptions imply (see Remark 3.2 below)

$$\ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}}))/\mathrm{Br}(k) \cong H^1(\mathrm{Gal}(\bar{k}/k), \mathrm{Pic}(X_{\bar{k}})). \tag{3.6}$$

This kernel $\ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}}))$ is known as the *algebraic part* of the Brauer group. We define

$$X(\mathbb{A}_k)^{\mathrm{Br.alg}} = \big\{\, (x_v) \in X(\mathbb{A}_k) \,\big|\, \sum_v \mathrm{inv}_v(A(x_v)) = 0 \ \ \forall A \in \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}})) \,\big\}. \tag{3.7}$$

Remark 3.1. By virtue of the sequence (3.1) it suffices in (3.3) and (3.7) to consider one representative from each $\mathrm{Br}(k)$-coset in $\mathrm{Br}(X)$.

Remark 3.2. Since $X(\mathbb{A}_k) \neq \emptyset$,

(i) $\mathrm{Br}(k) \hookrightarrow \mathrm{Br}(X)$;
(ii) $\mathrm{Pic}(X) \cong \mathrm{Pic}(X_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)}$.

Indeed, each of the homomorphisms $\mathrm{Br}(k_v) \to \mathrm{Br}(X_{k_v})$ is split because points exist locally, and fact (i) follows from the exact sequence (3.1). This implies the vanishing of the edge homomorphism in (3.5), which in turn implies (ii).

By assumption, the field K is chosen so that

$$\mathrm{Pic}(X_K) \cong \mathrm{Pic}(X_{\bar{k}}). \tag{3.8}$$

The corresponding Leray spectral sequence gives rise to an exact sequence

$$\begin{aligned} 0 \to \ker(\mathrm{Br}(k) \to \mathrm{Br}(K)) \to \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_K)) \xrightarrow{\lambda} H^1(G, \mathrm{Pic}(X_K)) \\ \to H^3(G, K^*). \end{aligned} \tag{3.9}$$

The inflation map

$$H^1(G, \mathrm{Pic}(X_K)) \to H^1(\mathrm{Gal}(\bar{k}/k), \mathrm{Pic}(X_{\bar{k}})), \tag{3.10}$$

is an isomorphism by the Hochschild–Serre spectral sequence of group cohomology (the inflation map is injective, and the cokernel maps into H^1 of a torsion-free module with trivial action of a profinite group, which is trivial).

Summarizing, we have

Proposition 3.3. *The composition of the inflation map* (3.10) *and the isomorphism* (3.6) *is an isomorphism*

$$\ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}}))/\mathrm{Br}(k) \cong H^1(G, \mathrm{Pic}(X_K)). \tag{3.11}$$

In particular, the set $X(\mathbb{A}_k)^{\mathrm{Br.alg}}$ in (3.7) is determined by finitely many coset representatives $A \in \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}}))$, i.e., coset representatives of generators of the finite group (3.11). The conditions involve only the components of $X(\mathbb{A}_k)$ at finitely many places of k. Our main theorem asserts that these conditions are effectively computable. Specifically, we describe an algorithm to compute the conditions, which are finite in number, expressed in terms of points of $X(k_v)$ to finite precision in case v is non-archimedean and connected components of $X(k_v)$ in case v is archimedean.

Theorem 3.4. *If X is as in Assumption 2.1 then $X(\mathbb{A}_k)^{\mathrm{Br.alg}}$ is effectively computable.*

We do not address the time or memory requirements of the algorithm. *A priori* bounds are available for each of the constituent steps of the algorithm, and these may be combined to yield overall bounds for the algorithm, in terms of the input data.

Remark 3.5. In this paper, we focus exclusively on the algebraic part of the Brauer group and on effectively computing $X(\mathbb{A}_k)^{\mathrm{Br.alg}}$. Whenever $\mathrm{Br}(X_{\bar{k}}) = 0$, we have

$$\mathrm{Br}(X)/\mathrm{Br}(k) \cong H^1(G, \mathrm{Pic}(X_K))$$

by (3.6) and (3.10), and by the definition (3.7) we have

$$X(\mathbb{A}_k)^{\mathrm{Br.alg}} = X(\mathbb{A}_k)^{\mathrm{Br}}.$$

The condition $\mathrm{Br}(X_{\bar{k}}) = 0$ holds automatically in either of the following cases:

(i) $X_{\bar{k}}$ is rational (by birational invariance of $\mathrm{Br}(X)$ for smooth projective X over a field of characteristic zero [Gro68, (III.7.4)]), or
(ii) X is Fano (i.e., has ample anticanonical divisor) and $\dim X \leq 3$ [IP99].

Examples of computations of Brauer–Manin obstructions based on *transcendental* (i.e., non-algebraic) elements of the Brauer group are given in [Har96], [Wit04].

Example. Let X be a del Pezzo surface of degree 3 given by an equation of diagonal form

$$ax^3 + by^3 + cz^3 + dt^3 = 0, \tag{3.12}$$

where a, b, c, d are nonzero integers. Then $X(\mathbb{Q}) \neq \emptyset \Leftrightarrow X(k) \neq \emptyset$ where $k = \mathbb{Q}(e^{2\pi i/3})$. A splitting field is

$$K = k(\sqrt[3]{b/a}, \sqrt[3]{c/a}, \sqrt[3]{d/a}).$$

Specifically, all 27 exceptional curves of $X_{\bar{k}}$ are defined over K. The Galois action of $G = (\mathbb{Z}/3\mathbb{Z})^3$ on $\mathrm{Pic}(X_K) = \mathbb{Z}^7$ can be computed. By [CTKS87], the result is:

$$H^1(G, \mathrm{Pic}(X_K)) = \begin{cases} 0 & \text{if one of } ab/cd,\ ac/bd,\ ad/bc \text{ is a cube,} \\ (\mathbb{Z}/3\mathbb{Z})^2 & \text{if exactly 3 of } a/b,\ a/c,\ \ldots,\ c/d \text{ are cubes,} \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases} \tag{3.13}$$

4. Descent for divisors

In this section we explain how to make effective the isomorphism

$$\mathrm{Pic}(X) \cong \mathrm{Pic}(X_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)} \tag{4.1}$$

from Remark 3.2. While this is not a logical requirement for the proof of Theorem 3.4 (in fact it relies on results from Sections 6 and 7), it is important in practical applications. More precisely, given the data of Assumption 2.1, let H be a subgroup of G, with corresponding intermediate field extension $K_0 = K^H$. Then (4.1) applied to X_{K_0} yields divisors on X_{K_0} representing elements of $\mathrm{Pic}(X_{\bar{k}})^H$. In this way, effective implementation of (4.1) sometimes allows K to be replaced by a smaller splitting field, or at least a smaller extension over which a sufficiently interesting submodule of $\mathrm{Pic}(X_{\bar{k}})$ is defined.

We start with an example, and then explain how to carry this out in general.

Example. Let $k = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/3}$, and let X be the diagonal cubic surface (3.12). Recall, we can take $K = k(\sqrt[3]{b/a}, \sqrt[3]{c/a}, \sqrt[3]{d/a})$ and $G = (\mathbb{Z}/3)^3$. Assume the coefficients a, b, c, and d to be generic, so that

$$H^1(G, \mathrm{Pic}(X_{\bar{k}})) = \mathbb{Z}/3\mathbb{Z} \tag{4.2}$$

(see (3.13)). If we consider the subfield

$$K_0 = k(\sqrt[3]{ad/bc})$$

then a computation reveals that the inflation map of Galois cohomology

$$H^1(\mathrm{Gal}(K_0/k), \mathrm{Pic}(X_{K_0})) \to H^1(G, \mathrm{Pic}(X_{\bar{k}})) \tag{4.3}$$

is an isomorphism. Concretely, $\mathrm{Pic}(X_{K_0}) \cong \mathbb{Z}\cdot(-\omega_X) \oplus M$ where M is a rank 2 module with nontrivial action of $\mathrm{Gal}(K_0/K) \cong \mathbb{Z}/3\mathbb{Z}$. The Galois-invariant combinations of exceptional lines on $X_{\bar{k}}$ generate only an index 3 subgroup of M. An additional generator of M is the class of the following divisor

$$D = D' - D'', \quad D' : \begin{cases} x + \zeta^2 \sqrt[3]{b/a}\, y = 0 \\ z + \sqrt[3]{d/c}\, t = 0 \end{cases} \quad D'' : \begin{cases} x + \sqrt[3]{b/a}\, y = 0 \\ z + \zeta^2 \sqrt[3]{d/c}\, t = 0 \end{cases} \tag{4.4}$$

for which we do not, *a priori*, have a representative defined over K_0. Notice that D is defined over

$$K_1 = K_0(\sqrt[3]{b/a}) = k(\sqrt[3]{b/a}, \sqrt[3]{d/c}).$$

We define

$$\mathcal{L}_1 = \mathcal{O}_{X_{K_1}}(D).$$

To make the isomorphism (4.1) effective, we apply the following strategy: We use *descent* to produce a line bundle $\mathcal{L}_0$ defined over K_0 having the desired class in the Picard group. A rational section of $\mathcal{L}_0$ defined over K_0 will produce the required cycle.

The theory of descent is a machinery for patching, i.e., the construction of a global object from local data (see [SGA1, exp. VIII]). In this case, the local data consists of the line bundle $\mathcal{L}_1$ on X_{K_1}, together with isomorphisms of $\mathcal{L}_1$ with its translates under $\mathrm{Gal}(K_1/K_0)$. The isomorphisms which we must supply need to satisfy a compatibility condition called the *cocycle condition*.

For the sake of illustration, we carry this out for the special choice of coefficients

$$a = 5, \qquad b = 9, \qquad c = 10, \qquad d = 12.$$

These coefficients are those of the famous example of Cassels and Guy of a cubic surface which violates the Hasse principle [CG66]. Then

$$K_0 = k(\sqrt[3]{2/3}), \qquad \text{and} \qquad K_1 = K_0(\sqrt[3]{9/5}).$$

Let ρ denote a generator of $\mathrm{Gal}(K_1/K_0) \cong \mathbb{Z}/3\mathbb{Z}$. To apply descent, we need to produce an isomorphism $\varphi\colon \mathcal{L}_1 \to {}^{\rho}\mathcal{L}_1$ satisfying the cocycle condition ${}^{\rho\rho}\varphi \circ {}^{\rho}\varphi \circ \varphi = \mathrm{id}$; then the descent machinery produces a line bundle $\mathcal{L}_0$ on X_{K_0}. This is easy to do because X has a K_0-point, e.g.,

$$p := (3, 1, 0, -\sqrt[3]{12}).$$

If we require φ to act as identity on the fiber of $\mathcal{L}_1$ over p, then φ is uniquely determined (since it is unique up to scale):

$$\varphi = -\frac{1}{2}(1 + \sqrt[3]{15})\frac{z + \sqrt[3]{6/5}\,t}{x + \sqrt[3]{9/5}\,y}. \tag{4.5}$$

Starting with the function 1 (viewed as a rational section of $\mathcal{L}_1$ or any of its Galois translates), the rational section $1 + {}^{\rho\rho}\varphi(1) + {}^{\rho\rho}\varphi \circ {}^{\rho}\varphi(1)$ is compatible with the Galois action, hence descends to a rational section s of $\mathcal{L}_0$. The divisor associated with the rational section s, which must have the same class in the Picard group as D, is

$$C - (L + {}^{\rho}L + {}^{\rho\rho}L)$$

where C is the cubic curve on X_{K_0} defined by the equations

$$\begin{aligned}
2x^2 - 6xy - xz + 3\zeta\sqrt[3]{2/3}\,xt + 3yz - 9\zeta\sqrt[3]{2/3}\,yt + 8z^2 &= 0,\\
4x^2 - 2xz - 6\sqrt[3]{2/3}\,xt - 6\zeta^2 yz + z^2 + 3\sqrt[3]{2/3}\,zt + 9\sqrt[3]{4/9}\,t^2 &= 0,\\
-2xy - 5\zeta xz - \zeta^2\sqrt[3]{2/3}\,xt + 6y^2 - \zeta yz + 3\zeta^2\sqrt[3]{2/3}\,yt - 8\sqrt[3]{2/3}\,zt &= 0,
\end{aligned} \tag{4.6}$$

and where L is the exceptional curve defined by $x + \sqrt[3]{9/5}y = 0$ and $z + \zeta^2\sqrt[3]{6/5}t = 0$. Now $\mathrm{Pic}(X_{K_0})$ is generated by an anticanonical divisor and C together with its translates under $\mathrm{Gal}(K_0/k)$.

We return to the general setting. Let X be as in Assumption 2.1. The machinery of descent associates, to a vector bundle $\widetilde{\mathcal{E}}$ on X_K (or more generally a quasi-coherent sheaf of $\mathcal{O}_{X_K}$-modules) together with a collection of isomorphisms $\varphi_g\colon \widetilde{\mathcal{E}} \to a_g^*\widetilde{\mathcal{E}}$ (for all $g \in G$) satisfying the cocycle condition

$$\varphi_{gh} = ({}^{g}\varphi_h) \circ \varphi_g \tag{4.7}$$

(for all g, $h \in G$) a vector bundle (or quasi-coherent sheaf) $\mathcal{E}$ on X together with an isomorphism $\xi\colon \mathcal{E}_K \to \widetilde{\mathcal{E}}$, which is compatible with the φ_g. Here ${}^g\varphi_h$ denotes $a_g^*\varphi_h$, where a_g is the automorphism of X_K induced by $g \in G$. (The reversed order of the composition on the right-hand side of (4.7) is accounted for by our convention, in which the Galois action induces a *right* action of G on X.) The $\mathcal{E}$ and ξ that are produced by descent are unique up to canonical isomorphism.

Let $D \subset X_K$ be a divisor (given by equations) whose class $[D] \in \mathrm{Pic}(X_{\bar{k}})$ is invariant under $G = \mathrm{Gal}(K/k)$. By Proposition 7.3, if $D' \subset X_K$ is a divisor with $[D'] = [D]$ in $\mathrm{Pic}(X_{\bar{k}})$, then there is an effective procedure to construct a rational function in $K(X)^*$ whose associated divisor is $D - D'$. Multiplication by this function is then an explicit isomorphism $\mathcal{O}_{X_K}(D) \to \mathcal{O}_{X_K}(D')$. For each $g \in G$, let

$$\varphi_g\colon \mathcal{O}_{X_K}(D) \to \mathcal{O}_{X_K}({}^gD)$$

be such an isomorphism.

Each isomorphism φ_g is uniquely determined up to a multiplicative constant. We can characterize whether it is possible to modify each isomorphism by a multiplicative constant, in order to satisfy (4.7). The obstruction to (4.7) is the class in $H^2(G, k^*) = \ker(\mathrm{Br}(k) \to \mathrm{Br}(K))$ of the following K^*-valued 2-cocycle $(\gamma_{g,h})$:

$$\gamma_{g,h} := \varphi_{gh}^{-1} \circ {}^g\varphi_h \circ \varphi_g.$$

As we have seen in the Example, the condition $X(k) \neq \emptyset$ is sufficient for the obstruction to vanish. In general we do not know whether $X(k)$ is empty. But we have, by assumption, $X(k_v) \neq \emptyset$ for all completions k_v of k. So the obstruction vanishes upon base change to any completion of k; hence by the exact sequence (3.1) (the Hasse principle for the Brauer group of a number field) the obstruction indeed vanishes. In other words, $(\gamma_{g,h})$ must be a 2-coboundary. There is an effective algorithm to express $(\gamma_{g,h})$ as the coboundary of a 1-cochain with values in K^* (see the proof of Proposition 6.3). So the φ_g can be modified, using these multiplicative factors, in order to satisfy (4.7). Applying descent, we obtain a line bundle $\mathcal{L}$ on X, such that $\mathcal{L}$ is a representative of $[D] \in \mathrm{Pic}(X_{\bar{k}})$.

It remains to express the line bundle $\mathcal{L}$ (which is determined by means of descent) explicitly as the class of a divisor on X. Given any rational section of $\mathcal{L}$, the associated divisor (of zeros minus poles, with respect to local trivializations of $\mathcal{L}$) will be defined over k and will have class in the Picard group equal to $[D]$. The theory of descent also includes descent for sections: a rational section of $\mathcal{L}$ is determined uniquely by a tuple of rational sections of $\mathcal{O}_{X_K}({}^gD)$, for each g, that are compatible with the φ_g. We obtain such a collection of sections from a single rational section of $\mathcal{O}_{X_K}(D)$, by means of the "trace" operation: we translate the given section by each of the elements of G, apply to each the inverse of the isomorphism φ_g, and form the sum. So it suffices to exhibit a rational section of $\mathcal{O}_{X_K}(D)$ having nontrivial trace. Let $x \in X_K$ be a closed point (not necessarily a K-rational point), not lying in D or in any of its Galois translates, with Galois orbit $O(x)$ and image $y \in X$. The extension from the residue field of y to the coordinate ring of $O(x)$, with G-action on the latter, can be calculated explicitly. An element of the residue field of x with nontrivial trace can be produced and lifted to an element of $H^0(X_K \smallsetminus \bigcup_{g\in G} {}^gD, \mathcal{O}_{X_K}(D))$, also with nontrivial trace.

5. Computing the obstruction

In this section we explain the main steps of the computation of $X(\mathbb{A}_k)^{\mathrm{Br.alg}}$ in terms of the data of Assumption 2.1. The details will be provided in subsequent sections, completing the proof of Theorem 3.4.

We first need some additional notation. Put

$$U = X \smallsetminus \bigcup_{i=1}^{m} D_i.$$

Note that U is defined over k. We have an exact sequence

$$0 \to K^* \to \mathcal{O}(U_K)^* \to R \to 0. \tag{5.1}$$

Step 1. Compute the Galois cohomology group $H^1(G, \mathrm{Pic}(X_K))$, and exhibit (finitely many) explicit 1-cocycle representatives of generators.

For *each* generator (with cocycle representative) we implement the following.

Step 2. Apply the connecting homomorphism of the cohomology exact sequence of (2.1) to the cocycle representative of the generator from Step 1 to obtain a 2-cocycle representative of the corresponding element in $H^2(G, R)$.

Step 3. Extending K if necessary, kill the obstruction in $H^3(G, K^*)$ to lifting the element of $H^2(G, R)$ to an element $B \in H^2(G, \mathcal{O}(U_K)^*)$; carry out the lifting explicitly on the cocycle level.

The element $B \in H^2(G, \mathcal{O}(U_K)^*)$ will be the restriction to U of an element $A \in \mathrm{Br}(X)$. More precisely the Leray spectral sequence

$$\mathsf{E}_2^{p,q} = H^p(G, H^q(U_K, \mathbb{G}_m)) \Rightarrow H^{p+q}(U, \mathbb{G}_m)$$

induces a map

$$H^2(G, \mathcal{O}(U_K)^*) \to \mathrm{Br}(U). \tag{5.2}$$

This map sends the class of a 2-cocycle with values in $\mathcal{O}(U_K)^*$ to the element of $\mathrm{Br}(U)$ represented by the same cocycle, viewed now as a Čech cocycle for the covering $U_K \to U$. Then Proposition 6.1, below, exhibits the required $A \in \mathrm{Br}(X)$. The $\mathrm{Br}(k)$-coset $\widetilde{A}$ of A will be one of finitely many generators of $\ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}}))/\mathrm{Br}(k)$. Define

$$X(\mathbb{A}_k)^A = \{\, (x_v) \in X(\mathbb{A}_k) \mid \sum_v \mathrm{inv}_v(A(x_v)) = 0 \,\}.$$

Then

$$X(\mathbb{A}_k)^{\mathrm{Br.alg}} = \bigcap_A X(\mathbb{A}_k)^A,$$

where A runs over the finite set of representatives.

Step 4. Obtain from the set $\mathcal{D}^1 := \{D_i\}$, new finite collections $\mathcal{D}^2, \ldots, \mathcal{D}^r$ of geometric cycles, such that the corresponding complements $U =: U^1, U^2, \ldots, U^r$ form an open covering of X. Repeat Steps 2 and 3 for each $\mathcal{D}^j$ to obtain $B^j \in H^2(G, \mathcal{O}(U_K^j)^*)$ such that the restriction of A to U^j is equal to B^j, modulo $\mathrm{Br}(k)$.

Step 5. (Calibration) Compute $I^j \in \mathrm{Br}(k)$ such that

$$B^j + I^j = A|_{U^j}$$

in $\mathrm{Br}(U^j)$.

Step 6. Compute the local invariants $\mathrm{inv}_v(A(x_v))$ for all v and all $x_v \in X(k_v)$.

Step 6 generally makes use of the cocycle representatives on more than one open set U^j. Indeed, by evaluating the given cocycle representative for $A|_{U^j}$ at k_v-points in Step 6 we only ever obtain the local invariants of A on compact subsets of $U^j(k_v)$, when v is non-archimedean. So, unless $X(k_v)$ is contained in a single U^j, cocycle representatives for A on more than one open set will be required. The fact that the U^j cover X will allow us to apply an effective arithmetic Nullstellensatz to carry out Step 6 effectively.

6. 2-cocycle representatives

In this section we carry out Steps 1 through 3 outlined above. We obtain 2-cocycle representatives for the classes $B \in H^2(G, \mathcal{O}(U_K)^*)$ from Section 5.

Step 1, the computation of $H^1(G, \mathrm{Pic}(X_K))$, is implemented in standard computer algebra packages, e.g., `Magma`. Indeed, by Assumption 2.1, $\mathrm{Pic}(X_K)$ with its Galois action is known. The output is a presentation of $H^1(G, \mathrm{Pic}(X_K))$ as a finite abelian group, with 1-cocycle representatives of a set of generators.

Steps 2 and 3 produce lifts of a generator to $\mathrm{Br}(X)$, via the map λ of the sequence (3.9). All computations are done on the level of cocycle representatives. The obstructions in $H^3(G, K^*)$ to producing the lift are killed by enlarging K, if necessary.

Let $\widetilde{B} \in H^1(G, \mathrm{Pic}(X_K))$ be one of the generators, with 1-cocycle representative $\tilde{\beta}$. Concretely, $\tilde{\beta}$ is a tuple of elements of $\mathrm{Pic}(X_K)$, satisfying a cocycle condition.

Combining the cohomology exact sequences coming from (2.1) and (5.1) and a portion of the exact sequence (3.9) we obtain a diagram

$$
\begin{array}{ccccccc}
 & & & & \mathrm{Br}(U) & & \\
 & \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_K)) & \nearrow & H^2(G, \mathcal{O}(U_K)^*) \nearrow & & & \\
 & \downarrow \lambda & & \downarrow \mu & & & \\
0 \longrightarrow & H^1(G, \mathrm{Pic}(X_K)) & \xrightarrow{\delta} & H^2(G, R) & \longrightarrow & H^2(G, \bigoplus_{i=1}^m \mathbb{Z} \cdot [D_i]) & \\
 & & \searrow^{\varepsilon} & \downarrow \nu & & & \\
 & & & H^3(G, K^*) & & &
\end{array}
\tag{6.1}
$$

In this diagram, we have used the fact that $\bigoplus_{i=1}^m \mathbb{Z} \cdot [D_i]$ is a permutation module, and hence its first cohomology vanishes. The maps to $\mathrm{Br}(U)$ are the restriction map from $\mathrm{Br}(X)$ and the map from $H^2(G, \mathcal{O}(U_K)^*)$ of (5.2), respectively.

Proposition 6.1. *Let X be as in Assumption 2.1, let $\widetilde{B} \in H^1(G, \mathrm{Pic}(X_K))$.*

(i) *The map ε in (6.1) is the rightmost map in (3.9).*

(ii) *Suppose that $\varepsilon(\widetilde{B}) = 0$. Let $A \in \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_K))$ be a lift of $\widetilde{B}$ by the map λ and $B \in H^2(G, \mathcal{O}(U_K)^*)$ a lift of $\delta(\widetilde{B})$ by the map μ in (6.1). Then the images of A and B in $\mathrm{Br}(U)$ via the maps in (6.1) are equal modulo $\mathrm{Br}(k)$.*

Proposition 6.2. *With notation as above, there is an effective construction of a (not necessarily G-equivariant) splitting $\sigma\colon R \to \mathcal{O}(U_K)^*$ of the sequence (5.1), viewed as a sequence of abelian groups.*

Proposition 6.3. *Let k be a number field, and K/k a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Let κ be a cocycle representative of an element in $H^3(G, K^*)$. There is an effective algorithm to determine whether κ is trivial in $H^3(G, K^*)$. If so, we can effectively produce a lift of κ to a 2-cochain via the coboundary map. Otherwise, we can effectively produce a finite extension L/K, with L Galois over k, such that the inflation of κ to $H^3(\mathrm{Gal}(L/k), L^*)$ is trivial.*

It is straightforward to compute $\delta(\tilde{\beta})$. Now $\varepsilon(\tilde{\beta}) = \nu(\delta(\tilde{\beta}))$, and $\nu(\delta(\tilde{\beta}))$ is computed using the splitting $\sigma\colon R \to \mathcal{O}(U_K)^*$ of Proposition 6.2. Proposition 6.3 supplies an extension L of K killing the class of $\varepsilon(\tilde{\beta})$ in $H^3(G, K^*)$. Replacing K by L, we now invoke Proposition 6.3 to produce a 2-cochain η with values in K^*, such that

$$\varepsilon(\tilde{\beta}) = \partial(\eta)$$

Now put

$$\beta := \frac{\sigma(\delta(\tilde{\beta}))}{\eta}.$$

Then β is a 2-cocycle with values in $\mathcal{O}(U_K)^*$, such that the class of β is a lift via μ of the class $\delta(\widetilde{B})$. We let $B \in H^2(G, \mathcal{O}(U_K)^*)$ denote the class of β.

By the exact sequence (3.9) and Proposition 6.1 (i) the class $\widetilde{B} \in H^1(G, \mathrm{Pic}(X_K))$ lifts via λ to a class

$$A \in \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_K)), \tag{6.2}$$

defined up to an element of $\mathrm{Br}(k)$. By Proposition 6.1 (ii), A can be chosen so that the image of B in $\mathrm{Br}(U)$ is equal to the restriction $A|_U$. Thus, in (6.2), we have a Brauer group element A whose restriction to U is known explicitly, by means of the 2-cocycle β.

Proof of Proposition 6.1. We follow [CTS87]. Let $j\colon U \to X$ be the inclusion, with complement $D = \bigcup_{j=1}^m D_i$. There is an exact sequence of étale sheaves on X

$$0 \to \mathbb{G}_m \to j_*(\mathbb{G}_m|_U) \to \mathcal{Z}^1_D \to 0 \tag{6.3}$$

where on the right is the sheaf of divisors on X with support on D. Evaluating global sections on X_K, we obtain the exact sequence of G-modules, which is the amalgamation of (2.1) and (5.1)

$$0 \to K^* \to \mathcal{O}(U_K)^* \to \bigoplus_{i=1}^m \mathbb{Z} \cdot [D_i] \to \mathrm{Pic}(X_K) \to 0.$$

The sequence (6.3) provides a resolution of the sheaf $\mathbb{G}_m$ on X. Taking $(\mathcal{I}_\bullet, \mathsf{d})$ to be a resolution of $\mathbb{G}_m$ by injective sheaves on X, we know that there exists a morphism of resolutions from the resolution (6.3) to $\mathcal{I}_\bullet$. Applying the equivariant global section functor, we get a morphism of four-term exact sequences

$$\begin{array}{ccccccc}
K^* & \hookrightarrow & \mathcal{O}(U_K)^* & \xrightarrow{\mathrm{div}} & \bigoplus_{i=1}^m \mathbb{Z} \cdot [D_i] & \twoheadrightarrow & \mathrm{Pic}(X_K) \\
\| & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} & & \| \\
K^* & \hookrightarrow & H^0(X_K, \mathcal{I}_0) & \xrightarrow{\mathsf{d}} & \ker(H^0(X_K, \mathcal{I}_1) \to H^0(X_K, \mathcal{I}_2)) & \twoheadrightarrow & \mathrm{Pic}(X_K)
\end{array} \tag{6.4}$$

where the first and last maps are identity maps.

The map ε in the diagram (6.1) is the composition of the connecting homomorphisms in cohomology associated with the short exact sequences (2.1) and (5.1). Spectral sequence machinery shows that the edge map $H^1(G, \mathrm{Pic}(X_K)) \to H^3(G, K^*)$ of the sequence (3.9) is equal to the composition of connecting homomorphisms gotten by breaking the four-term exact sequence of the bottom line of (6.4) into a pair of short exact sequences. Because there is a map between these sequences inducing identity maps on the first and last terms, the morphism ε is equal to the edge map of (3.9). This establishes part (i).

For (ii), let $\widetilde{B} \in H^1(G, \mathrm{Pic}(X_K))$ be given, represented by the 1-cocycle $\tilde{\beta}$. Computing $\delta(\widetilde{B})$ involves lifting $\tilde{\beta}$ to a 1-cochain $\tilde{\gamma}$ with values in $\bigoplus_{i=1}^m \mathbb{Z} \cdot [D_i]$. Now $\partial(\tilde{\gamma})$ is a tuple of divisors rationally equivalent to zero, hence $\partial(\tilde{\gamma}) = \mathrm{div}(\beta)$ for some 2-cochain β with values in $\mathcal{O}(U_K)^*$. Moreover $\partial(\beta)$ is a 3-cocycle representative of $\varepsilon(\widetilde{B})$ which by hypothesis vanishes. So, by adjusting β by a K^*-valued 2-cochain we may arrange that $\partial(\beta) = 0$. Then β is a 2-cocycle representative of a class $B \in H^2(G, \mathcal{O}(U_K)^*)$, such that $\mu(B) = \delta(\widetilde{B})$.

We may identify $\mathrm{Br}(X)$ with the second cohomology of the total complex of the term $\mathsf{E}_0^{p,q} = \mathsf{C}^p(H^0(X_K, \mathcal{I}_q))$ of the Leray spectral sequence. Now $A \in \mathrm{Br}(X)$ is represented by a cocycle of the total complex

$$(\alpha_0, \alpha_1, \alpha_2) \in \mathsf{C}^0(H^0(X_K, \mathcal{I}_2)) \times \mathsf{C}^1(H^0(X_K, \mathcal{I}_1)) \times \mathsf{C}^2(H^0(X_K, \mathcal{I}_0)).$$

Since $A \in \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_K))$, we may suppose that $\alpha_0 = 0$. The condition to be a cocycle is now

$$\mathsf{d}(\alpha_1) = 0, \qquad \partial(\alpha_1) = \mathsf{d}(\alpha_2), \qquad \partial(\alpha_2) = 0.$$

The cocycle representative $(\alpha_0, \alpha_1, \alpha_2)$ may be replaced by an equivalent representative with $\alpha_1 = \varphi(\tilde{\gamma})$. Then $\mathsf{d}(\psi(\beta)) = \varphi(\mathrm{div}(\beta)) = \partial(\varphi(\tilde{\gamma})) = \mathsf{d}(\alpha_2)$. Hence the image of $A - B$ in $\mathrm{Br}(U)$ is represented by a 2-cocycle with values in $\ker(\mathsf{d}) = K^*$. □

Proof of Proposition 6.2. The map to R in (5.1), for which we wish to find a splitting, is the divisor map from rational functions on X, regular and nonvanishing on U, to divisors with support outside U. So it suffices to solve the problem, given effective divisors D and E on a smooth projective variety X over k (all given explicitly by equations), with $[D] = [E]$ in $\mathrm{Pic}(X)$, to produce effectively a rational function in $k(X)^*$ whose divisor is $D - E$. This is the content of Proposition 7.3, given in the next section. □

Proof of Proposition 6.3. By [BSD04] Theorem 3, there is an effective method to test whether $\kappa = 0$ in $H^3(G, K^*)$, and to produce a lift to a 2-cochain if this is the case. The method is to produce, effectively, a finite set of primes S such that $\kappa = 0$ if and only if the given cocycle is the coboundary of a 2-cochain taking values in the S-units of K. (The same argument applies to test for triviality of an i-cocycle, for any i, and to produce an $(i-1)$-cochain in case it is trivial.)

If $\kappa \neq 0$ in $H^3(G, K^*)$, then there exist cyclic extensions ℓ of k such that $L := \ell K$ satisfies $\kappa \in \ker(H^3(G, K^*) \to H^3(\mathrm{Gal}(L/k), L^*))$. For instance, let q be a prime not dividing the discriminant $\mathrm{disc}(K/\mathbb{Q})$ such that $q \equiv 1 \pmod{n}$. Then $[L : k] = (q-1)n$ where $n = [K : k]$. By the Chebotarev density theorem, there exists some prime ideal $\mathfrak{p}$ in k (which we do not need explicitly) which remains inert in the cyclic extension ℓ of k. Then the local degree $n_{\mathfrak{p}}$ of $\mathfrak{p}$ in L must be a multiple of $q - 1$. Therefore the inflation map $H^3(G, K^*) \to H^3(\mathrm{Gal}(L/k), L^*)$ is trivial (cf. [AT68], §7.4). □

Example. For the cubic surface over $k = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/3}$, defined by

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0,$$

we have found that already for the cyclic degree 3 extension $K_0 = k(\sqrt[3]{2/3})$ we have

$$H^1(\mathrm{Gal}(K_0/k), \mathrm{Pic}(X_{K_0})) \cong H^1(G, \mathrm{Pic}(X_{\bar{k}})) = \mathbb{Z}/3\mathbb{Z}.$$

Let τ denote the generator of $\mathrm{Gal}(K_0/k) \cong \mathbb{Z}/3\mathbb{Z}$ which sends $\sqrt[3]{2/3}$ to $\zeta\sqrt[3]{2/3}$. Cohomology $H^i(\mathrm{Gal}(K_0/k), M)$ can be computed by means of the resolution

$$\mathsf{C}^\bullet(M): \qquad 0 \longrightarrow M \xrightarrow{\Delta_\tau} M \xrightarrow{N_\tau} M \xrightarrow{\Delta_\tau} \cdots \tag{6.5}$$

where the maps alternate between $\Delta_\tau := \mathrm{id} - \tau$ and $N_\tau := \mathrm{id} + \tau + \tau^2$. The group $H^1(\mathrm{Gal}(K_0/k), \mathrm{Pic}(X_{K_0}))$ is thus identified with $\ker(N_\tau)/\mathrm{im}(\Delta_\tau)$, and this group (which is cyclic of order 3) is generated by the class of

$$[C] + \omega_X \tag{6.6}$$

where C is the curve in X_{K_0} given in (4.6). This is Step 1.

Choose an anticanonical divisor $H \subset X$ defined, say, by $x = 0$, so that $C - H$ is a divisor in the class (6.6). Now $\{H, C, {}^\tau C, {}^{\tau\tau}C\}$ is a Galois-invariant set of divisors generating $\mathrm{Pic}(X_{K_0})$. For this set of divisors the sequence (2.1) becomes

$$0 \to \mathbb{Z} \to \mathbb{Z} \cdot H \oplus \mathbb{Z} \cdot C \oplus \mathbb{Z} \cdot {}^\tau C \oplus \mathbb{Z} \cdot {}^{\tau\tau}C \to \mathrm{Pic}(X_{K_0}) \to 0. \tag{6.7}$$

The connecting homomorphism induced by the resolution (6.5) on the exact sequence (6.7) sends the 1-cocycle (6.6) to the 2-cocycle

$$C + {}^\tau C + {}^{\tau\tau}C - 3H \tag{6.8}$$

in R. Notice that in this example R is isomorphic to $\mathbb{Z}$ (the left-hand term in (6.7)), and in fact (6.8) is a generator. We have completed Step 2.

We have $U = X \smallsetminus (H \cup C \cup {}^\tau C \cup {}^{\tau\tau}C)$. A splitting $\sigma\colon R \to \mathcal{O}(U_{K_0})^*$, required for Step 3, sends the generator (6.8) to a rational function which vanishes on $C \cup {}^\tau C \cup {}^{\tau\tau}C$ and has a pole of order 3 along H. The obstruction group $H^3(\mathrm{Gal}(K_0/k), K_0^*)$ is identified by (6.5) with $H^1(\mathrm{Gal}(K_0/k), K_0^*)$, which vanishes by Hilbert's Theorem 90. So it is possible to lift the 2-cocycle (6.8) to an element of $\mathcal{O}(U_{K_0})^*$ invariant under τ. To carry this out, we use the explicit equations (4.6) for C to produce directly a function in $\mathcal{O}(U)^*$ of the form f/x^3, where f is a polynomial (with coefficients in k) whose divisor is $C + {}^\tau C + {}^{\tau\tau}C - 3H$. We obtain

$$\begin{aligned} f = (2\zeta - 2)x^3 - 3\zeta x^2 y - 8\zeta x^2 z - 9\zeta^2 xy^2 + 24\zeta xyz + 4\zeta xz^2 + (-6\zeta - 21)y^3 \\ - 12\zeta yz^2 + (-18\zeta - 14)z^3 + (4\zeta - 4)t^3. \end{aligned} \tag{6.9}$$

So we have completed Step 3. The 2-cocycle given by f/x^3 corresponds to a cyclic Azumaya algebra for the extension K_0 of k and the rational function $f/x^3 \in \mathcal{O}(U)^*$. The class $B \in \mathrm{Br}(U)$ of this Azumaya algebra is the restriction of some $A \in \mathrm{Br}(X)$ such that A generates $\mathrm{Br}(X)/\mathrm{Br}(k)$.

7. Effectivity

In this section, we present effectivity results concerning ample line bundles and homogeneous ideals.

Many results in effective algebraic geometry are based on Gröbner bases. There are effective algorithms to compute a Gröbner basis of a homogeneous ideal $\mathcal{I} \subset k[x_0, \ldots, x_N]$, which is given by means of generators. Based on this, there are effective algorithms (implemented in computer algebra packages for several classes of fields k including number fields) to:

- test whether a given polynomial is in $\mathcal{I}$,

- compute the saturation of $\mathcal{I}$,
- compute the primary decomposition of an ideal $\mathcal{I}$.

(See, e.g., [CLO97], [KR00].)

Lemma 7.1. *Let $X \subset \mathbb{P}^N$ be a projective variety, given by means of equations. Denote by $\mathcal{O}_X(1)$ the restriction of $\mathcal{O}_{\mathbb{P}^N}(1)$ to X. Let $\mathcal{L}$ be an arbitrary line bundle on X, presented (as a coherent sheaf on X) by means of homogeneous generators and relations. Then there is, effectively, a positive integer d_0 such that for all $d \geq d_0$ the line bundle $\mathcal{L} \otimes \mathcal{O}_X(d)$ is ample and generated by global sections.*

Proof. Choose finitely many sections $s_i \in H^0(X, \mathcal{O}_X(1))$ such that X is covered by the open subsets X_{s_i} where each section is nonvanishing. From the presentation of $\mathcal{L}$ we have generators $t_{i,j} \in H^0(X_{s_i}, \mathcal{L})$. These give rise to a covering of the affine scheme X_{s_i} by open affines $X_{t_{i,j}}$.

There is, effectively, a positive integer d_0 such that for all $d \geq d_0$, one has that $t_{i,j} \otimes s_i^d$ is the restriction to X_{s_i} of a section $u_{i,j} \in H^0(X, \mathcal{L} \otimes \mathcal{O}_X(d))$ for each i and j. This is achieved following the proof of [EGAI, 9.3.1(ii)]. The open subsets $X_{u_{i,j}} = X_{t_{i,j}}$ cover X, hence $\mathcal{L} \otimes \mathcal{O}_X(d)$ is generated by global sections, and by [EGAII, 4.5.2(a′)], $\mathcal{L} \otimes \mathcal{O}_X(d)$ is ample. □

Remark 7.2. By an effective Matsusaka theorem [Siu93] there is, for given $d \geq d_0$, an effective bound r_0 such that $(\mathcal{L} \otimes \mathcal{O}_X(d))^{\otimes r}$ is very ample for all $r \geq r_0$.

Proposition 7.3. *Given effective divisors D and E (by means of equations) on a smooth projective variety X (also defined by given equations) over k, such that $[D] = [E]$ in $\mathrm{Pic}(X)$, there is an effective algorithm to produce a rational function $h \in k(X)^*$ such that $\mathrm{div}(h) = D - E$.*

Proof. Let H denote a hyperplane section of $X \subset \mathbb{P}^N$. By effective Serre vanishing [BEL91, Prop. 1] we have

$$H^0(\mathbb{P}^N, \mathcal{O}_{\mathbb{P}^N}(d)) \to H^0(X, dH) \tag{7.1}$$

surjective for d greater than some effective lower bound. Combining this with the lower bound from Lemma 7.1 applied to $\mathcal{L} = \mathcal{O}_X(-D)$, we obtain d such that (7.1) is surjective and such that we can produce a homogeneous polynomial f of degree d, not identically zero on X, and vanishing on D. So, f vanishes on a cycle $D + D'$ for some cycle D' that can be determined effectively.

Now $E + D'$ is linearly equivalent to dH. By surjectivity of (7.1), there exists a homogeneous polynomial g of degree d, not identically zero on X, contained in the ideal of the sum of divisors $E + D'$. The ideals can be computed effectively, so we can find g, and then defining h to be f/g we have $\mathrm{div}(h) = D - E$. □

Remark 7.4. Since the linear system $|dH - D|$ that arises in the proof of Proposition 6.2 is base point free, the divisor D' in the proof can be chosen to avoid any given finite set of points of X.

Remark 7.5. The elements f/g constructed in the proof of Proposition 6.2 do indeed lie in $\mathcal{O}(U_K)^*$. However, f and g individually vanish on the residual divisor D' that appears in the proof. For the purposes of effective computations, we would really require alternative representations of this rational function, such that at any point of U there is some representative that is amenable to evaluation. A way of avoiding this extra complication is to carry out the following steps:

(i) Fix a choice of hyperplane section H of X (in its given projective embedding), which we assume to be defined by a linear polynomial h having coefficients in k and included among the cycles D_i.
(ii) Enlarge the collection of cycles D_i by adding, for each generator of R, the corresponding residual cycle D' from the proof of Proposition 6.2 along with its Galois translates.
(iii) For each additional cycle D' (or Galois translate thereof), add a new generator $D + D' - dH$ (or Galois translate thereof) to R.
(iv) For each additional generator to R, extend the definition of the splitting σ by sending $D + D' - dH$ to f/h^d and each Galois translate of $D + D' - dH$ to the corresponding Galois translate of f/h^d.

Having done this, U will be the complement of the zero locus of some homogeneous polynomial, and all the rational functions in the image of σ will be of the form f/g where f and g are homogeneous polynomials nonvanishing on U.

8. Multiple representatives and calibration

It is necessary to produce several representatives of a given $\widetilde{A} \in \mathrm{Br}(X)/\mathrm{Br}(k)$ (Step 4) and to calibrate these classes, i.e., to compute the difference in $\mathrm{Br}(k)$ between two given representatives in $\mathrm{Br}(X)$ of the $\mathrm{Br}(k)$-coset $\widetilde{A}$ (Step 5).

We now describe how to carry out Step 4. For each divisor D_i, Lemma 7.1 applied to $\mathcal{O}_X(-D_i)$ yields d such that $|dH - D_i|$ is base point free. We may therefore choose a member of this linear system which avoids any finite collection of points. So we can obtain divisors D'_i, such that D_i is in the $\mathbb{Z}$-linear span of D'_i and a hyperplane class, and such that no irreducible component of any D_i is contained in any of the D'_j. We then take $\mathcal{D}^2$ to be the collection of D'_i together with a hyperplane class, the latter also chosen not to contain any irreducible component of any of the D_i.

Now we repeat Steps 2 and 3, and also carry out steps (i)–(iv) of Remark 7.5 (which adds extra divisors to $\mathcal{D}^2$), so that every rational function that has been constructed from the divisors D'_i has the property that its numerator and denominator are both nonvanishing on U^2. In carrying this out, we use Remark 7.4 to ensure that U^2 contains the generic points of all the irreducible components of the divisors in $\mathcal{D}^1$.

For $m = 2, \ldots, \dim X$ we recursively construct $\mathcal{D}^{m+1}$ and repeat Steps 2 and 3 and steps (i)–(iv) of Remark 7.5 for the divisors in $\mathcal{D}^{m+1}$, making use of Remark 7.4 to ensure that U^{m+1} contains all the generic points of $\bigcap_{i=1}^{m}(X \smallsetminus U^i)$. It follows inductively that

$$\dim\Big(\bigcap_{i=1}^{m}(X \smallsetminus U^i)\Big) = \dim X - m.$$

At the end of the construction X is covered by the open sets $U^1, \ldots, U^{\dim X+1}$.

Now we treat Step 5. Let $\mathcal{D} = \{D_i\}$ and $\mathcal{D}' = \{D'_i\}$ be a pair of sets of divisors, with $\mathcal{D} = \mathcal{D}^1$ and $\mathcal{D}' = \mathcal{D}^j$ for some $j > 1$. Let $U = X \smallsetminus \bigcup D_i$ and $U' = X \smallsetminus \bigcup D'_i$. Let $\widetilde{B}$ be an element of $H^1(G, \mathrm{Pic}(X_K))$, with cocycle representative $\tilde{\beta}$ (constructed in Step 1). Consider the 2-cocycles β and β' resulting from Steps 2 and 3 applied to $\mathcal{D}$ and $\mathcal{D}'$, respectively. These are 2-cocycles with values in $\mathcal{O}(U_K)^*$ and $\mathcal{O}(U'_K)^*$, respectively.

The exact sequence (2.1) can be enlarged to an exact sequence

$$0 \to S \to \bigoplus_i \mathbb{Z}\cdot[D_i] \oplus \bigoplus_i \mathbb{Z}\cdot[D'_i] \to \mathrm{Pic}(X_{\bar{k}}) \to 0 \tag{8.1}$$

where S contains R as a direct summand. There is also a sequence analogous to (5.1),

$$0 \to K^* \to \mathcal{O}(U_K \cap U'_K)^* \to S \to 0, \tag{8.2}$$

and the splitting σ of Proposition 6.2 can be extended to a splitting

$$\pi\colon S \to \mathcal{O}(U_K \cap U'_K)^*.$$

Looking at Step 2, carried out using the collection of divisors $\mathcal{D}$ and again using the collection of divisors $\mathcal{D}'$, we have the same 1-cocycle $\tilde{\beta}$ with values in $\mathrm{Pic}(X_{\bar{k}})$ mapped to the same element of $H^2(G,S)$ represented by two different 2-cocycles with values in S. So, these 2-cocycles differ by a 2-coboundary. We apply π (note that π is compatible with the splitting used in Step 3 for the collection of divisors $\mathcal{D}'$ only up to multiplicative constants), to obtain

$$\beta = \iota'\, \beta'\, \partial(\pi(\theta))$$

for some 1-cochain θ with values in S and some 2-cochain ι' with values in K^*. This ι' is a 2-cocycle, and its associated class $I' \in \mathrm{Br}(k)$ satisfies

$$B' + I' = A.$$

Example. In the case of the diagonal cubic surface

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0,$$

we found that with $K_0 = k(\sqrt[3]{2/3})$, we have $\mathrm{Pic}(X_{K_0})$ generated by the class of the hyperplane H (given by $x = 0$) and the Galois orbit of the class of the cubic curve C which we determined in (4.6) starting from a choice of $p \in X(K_0)$. Additional choices of K_0-points $p', \ldots$, lead to further divisors having the same class in the Picard group as C. For instance, the point

$$p' := (3\zeta, 1, 0, -\sqrt[3]{12})$$

gives rise to the curve C' defined by

$$\begin{gathered}
2x^2 - 6\zeta xy - xz + 3\zeta^2 \sqrt[3]{2/3}\, xt + 3\zeta yz - 9\sqrt[3]{2/3}\, yt + 8z^2 = 0, \\
4x^2 - 2xz - 6\zeta \sqrt[3]{2/3}\, xt - 6yz + z^2 + 3\zeta \sqrt[3]{2/3}\, zt + 9\zeta^2 \sqrt[3]{4/9}\, t^2 = 0, \\
-2xy - 5xz - \zeta^2 \sqrt[3]{2/3}\, xt + 6\zeta y^2 - \zeta yz + 3\sqrt[3]{2/3}\, yt - 8\sqrt[3]{2/3}\, zt = 0.
\end{gathered}$$

Applying Steps 2 and 3 to C' we obtain

$$\begin{aligned}
f' = (2\zeta + 4)x^3 - 3\zeta x^2y - 8x^2z - 9xy^2 + 24\zeta xyz + 4xz^2 + (21\zeta + 15)y^3 \\
- 12\zeta yz^2 + (14\zeta - 4)z^3 + (4\zeta + 8)t^3
\end{aligned} \tag{8.3}$$

such that $\mathrm{div}(f'/x^3) = C' + {}^{\tau}C' + {}^{\tau\tau}C' - 3H$.

The sequence (8.1) is

$$0 \to \mathbb{Z} \oplus \mathbb{Z}^3 \to \mathbb{Z} \oplus \mathbb{Z}^3 \oplus \mathbb{Z}^3 \to \mathrm{Pic}(X_{K_0}) \to 0$$

where in the middle the generators are H and the Galois translates of C and C'. The first generator of the rank 4 module S on the left is the previously identified cycle $C + {}^{\tau}C + {}^{\tau\tau}C - 3H$, and the additional generators are

$$C' - C, \qquad {}^{\tau}C' - {}^{\tau}C, \qquad {}^{\tau\tau}C' - {}^{\tau\tau}C.$$

We need to construct a splitting $\pi\colon \mathbb{Z}\oplus\mathbb{Z}^3 \to \mathcal{O}(U_K \cap U'_K)^*$. We already have the image f/x^3 for the first generator, with f as in (6.9). Images of the other generators are readily constructed. We send $C' - C$ to g/f, where

$$\begin{aligned}g &= (8\zeta+16)x^3 + (-4\zeta-8)x^2y - 2x^2z + (-2\zeta+2)\sqrt[3]{2/3}\,x^2t + (2\zeta+4)xyz\\ &\quad + (6\zeta-6)\sqrt[3]{2/3}\,xyt + (-5\zeta+6)xz^2 + (\zeta-1)\sqrt[3]{2/3}\,xzt + (-6\zeta-3)\sqrt[3]{4/9}\,xt^2\\ &\quad + (12\zeta+24)y^3 + (-6\zeta+6)y^2z + (-\zeta-2)yz^2 + (-3\zeta+3)\sqrt[3]{2/3}\,yzt\\ &\quad + (18\zeta+9)\sqrt[3]{4/9}\,yt^2 + (16\zeta+24)z^3 + (-8\zeta+8)\sqrt[3]{2/3}\,z^2t + (16\zeta+32)t^3\end{aligned}$$

and the remaining generators to the Galois conjugates of g/f.

The 2-cocycles $C + {}^{\tau}C + {}^{\tau\tau}C - 3H$ used to construct f and $C' + {}^{\tau}C' + {}^{\tau\tau}C' - 3H$ used to construct f' differ by a 2-coboundary,

$$C + {}^{\tau}C + {}^{\tau\tau}C - C' - {}^{\tau}C' - {}^{\tau\tau}C' = N_\tau(C - C').$$

We have

$$\pi(C - C') = \frac{f}{g}.$$

Consequently

$$\frac{f}{x^3} = \vartheta\frac{f'}{x^3}N_\tau\Big(\frac{f}{g}\Big)$$

for some constant ϑ. By an explicit computation, we find

$$\vartheta = \frac{\zeta}{4}.$$

Repeating everything with the point

$$p'' := (3, \zeta, 0, -\sqrt[3]{12})$$

yields a curve C'' with explicit equations and a function

$$\begin{aligned}f'' = (-4\zeta-2)x^3 &- 3\zeta x^2y - 8x^2z - 9\zeta xy^2 + (-24\zeta-24)xyz + 4\zeta xz^2\\ &+ (-15\zeta+6)y^3 - 12yz^2 + (4\zeta+18)z^3 + (-8\zeta-4)t^3\end{aligned} \tag{8.4}$$

such that $\operatorname{div}(f''/x^3) = C'' + {}^{\tau}C'' + {}^{\tau\tau}C'' - 3H$. Continuing, we obtain a rational function whose norm times $(-15\zeta^2/2)f''/x^3$ is equal to f/x^3.

Therefore the rational functions

$$\frac{f}{x^3}, \qquad \frac{\zeta}{4}\frac{f'}{x^3}, \qquad \frac{-15\zeta^2}{2}\frac{f''}{x^3} \tag{8.5}$$

have the property that their corresponding Azumaya algebras (for the cyclic extension K_0 of k) all define (restrictions of) the same element of $\operatorname{Br}(X)$. Each Azumaya algebra is defined over an open subset of X. We would like to have X covered by such open sets. Indeed, the divisors on X defined by f, f', and f'' have trivial intersection. All we do now is replace H by other hyperplane sections $H' : y = 0$, etc. So, in (8.5) we replace x by the other coordinate functions, and obtain a larger collection of Azumaya algebras which all represent the same element of $\operatorname{Br}(X)$ and whose domains of definition cover X.

9. Local invariants

The classical Nullstellensatz theorem asserts that if polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_N]$ define the empty scheme in affine space $\mathbb{A}^N_k$ then there exist polynomials g_i satisfying $\sum_i f_i g_i = 1$. An effective arithmetic Nullstellensatz theorem [KPS01] applies to a number field k with ring of integers $\mathfrak{o}_k$. Then, assuming $f_i \in \mathfrak{o}_k[x_1, \ldots, x_N]$ for all i, there exist $g_i \in \mathfrak{o}_k[x_1, \ldots, x_N]$ satisfying

$$\sum_i f_i g_i = \varpi \tag{9.1}$$

for some $\varpi \in \mathfrak{o}_k$. The theorem asserts that such g_i can be found, satisfying bounds on their degrees and on the heights of their coefficients. The bounds are effective and depend on the degrees and the heights of the coefficients of the f_i.

The given Brauer group element A is unramified at all but a finite set of places of k. Consider a fixed integral model $\mathcal{X}$ of X over $\mathfrak{o}_k$. Recall, a place v of k is said to be of good reduction when the integral model is smooth over the residue field $\mathbf{k}_v$. At all but finitely many of these places, the polynomials appearing in the cocycles reduce to nonzerodivisors of $\mathcal{O}(\mathcal{X}_{\mathbf{k}_v \otimes_k K})$. Then by purity [Gro68, (III.6.1)], the Brauer group elements are unramified at all v-adic points of X.

Consequently, it is only necessary to carry out the local analysis, i.e., the computation of local invariants (3.2) of $X(k_v)$-points, at those v which are places of bad reduction, places where the rational functions appearing in the cocycles fail to extend, and real places of k.

We first treat a non-archimedean place v. Choose a valuation $v_1 \mid v$ of K and an embedding $K \to K_{v_1}$. The Galois group of $\mathrm{Gal}(K_{v_1}/K)$ is the subgroup G_1 of elements of G which stabilize v_1. The embedding $K^{G_1} \to K_{v_1}$ then factors through k_v. Replacing k by K^{G_1} we are thereby reduced to the case that v extends uniquely to a valuation v_1 of K, and $\mathrm{Gal}(K_{v_1}/k_v) = G$. We then have G-equivariant inclusions

$$\mathcal{O}(U_K) \to \mathcal{O}(U_{K_{v_1}})$$

for any variety U over k.

We fix an element $A \in \mathrm{Br}(X)$, an open covering $\{U^j\}$ of X, and 2-cocycle representatives $\{\beta^j\}$ with values in $\mathcal{O}(U^j_K)^*$, as constructed in Steps 1 through 5 (so that β^j is a representative of the restriction of A to U^j for each j). We may suppose each β^j is a tuple $(f^j_t/g^j_t)_{t\in T}$ for some finite index set T, indexing a basis of $\mathsf{C}^2(M)$. We may require that f^j_t and g^j_t should be polynomials with coefficients in the ring of integers $\mathfrak{o}_K$. These are constructed algorithmically, so it is possible to give an effective bound on the valuation of the coefficients.

Lemma 9.1. *Let k be a number field, K a finite Galois extension of k with Galois group G, and let v be a non-archimedean valuation of k admitting a unique extension to a valuation v_1 on K. Fix a resolution $\mathsf{C}^\bullet(K^*_{v_1})$ for computing group cohomology of the G-module $K^*_{v_1}$, and let us write elements of $\mathsf{C}^2(K^*_{v_1})$ as tuples (α_t) indexed by $t \in T$ for some finite index set T. Then there is, effectively in terms of the given data, a number N such that every 2-cocycle (α_t) with $\min_t v_1(\alpha_t - 1) > N$ is a 2-coboundary.*

Proof. By restriction of scalars, there is a smooth affine scheme Z over k_v such that 2-cocycles (α_t) with values in $K^*_{v_1}$ map bijectively to $Z(k_v)$, where the map is k_v-linear and explicit. Let $z_1 \in Z$ correspond to the 2-cocycle (1). There is, furthermore, a smooth affine scheme Y over k_v and a similar bijection with 1-cochains, and a smooth surjective map of k_v-schemes $\varrho\colon Y \to Z$ such that 2-coboundaries correspond to points of $\varrho(Y(k_v))$.

Fix coordinates for Y and Z. Equations for Y, Z, and ϱ can be written down explicitly. By the Inverse Function Theorem, there is an explicit v-adic neighborhood W of z_1 in $Z(k_v)$ and an analytic splitting (not needed explicitly) of $\varrho\colon Y(k_v) \to Z(k_v)$ on W. Hence for every k_v-point of W the corresponding 2-cocycle (α_t) is a 2-coboundary.

The restriction of scalars map, sending a $K^*_{v_1}$-valued cocycle (α_t) to a point $z \in Z(k_v)$, is given coordinatewise by k_v-linear expressions. Since v_1 is Galois-invariant, each coordinate of z has v-adic valuation bounded from below by $\min_t(v_1(\alpha_t))$ plus an explicit constant. So there is an effective bound N such that $\min_t(v_1(\alpha_t - 1)) > N$ implies $z \in W$, so that (α_t) must be a 2-coboundary. □

Corollary 9.2. *Keep the notation of Lemma 9.1. Fix an integer P, and let (α_t) and (α'_t) be 2-cocycles with values in $K^*_{v_1}$ with $|v_1(\alpha_t)| \le P$ and $|v_1(\alpha'_t)| \le P$ for all t. Then there is an effective bound Q, depending on the fields k_v and K_{v_1} and P but not on the given 2-cocycles, such that if $v_1(\alpha_t - \alpha'_t) \ge Q$ for all t then (α_t) and (α'_t) define the same element of $\mathrm{Br}(k_v)$.*

The proof of the next result contains an algorithmic description of the computation of local invariant in $\mathbb{Q}/\mathbb{Z}$ of the element in $\mathrm{Br}(k_v)$, given as a 2-cocycle (α_t).

Proposition 9.3. *With notation as in Lemma 9.1, let an integer P be given, and let (α_t) be a 2-cocycle with values in $K^*_{v_1}$ such that $|v_1(\alpha_t)| \le P$ for all t. Then there is an effective computation, taking as input the collection of α_t each specified to an effectively determined degree of precision, of the local invariant of the element of $\mathrm{Br}(k_v)$ corresponding to this 2-cocycle.*

Remark 9.4. Formally speaking, Proposition 9.3 implies Lemma 9.1. We have included Lemma 9.1 because it admits a direct proof independent of the detailed algorithmic treatment of the proof of Proposition 9.3. Lemma 9.1 is significant because it can be used to simplify the computation in practice. Indeed the bound N arising in the proof of the lemma can be quite reasonable, while the algorithmic description tends to lead to a much worse bound. See the example at the end of this section, where such bounds are obtained, compared, and used to help complete the local analysis.

Proof of Proposition 9.3. It is possible to obtain an explicit map between the given resolution $\mathsf{C}^\bullet$ and the standard resolution $\mathsf{C}^\bullet_G$ with

$$\mathsf{C}^2_G(M) = \bigoplus_{(g,h)\in G\times G} M.$$

Thus we are reduced to the case of given cocycle data $(\alpha_{g,h})$ satisfying the standard cocycle condition

$$\alpha_{g,h}\alpha_{gh,j} = \alpha_{g,hj}{}^g\alpha_{h,j}$$

for all g, h, $j \in G$. There is no loss of generality in assuming that for all $g \in G$ that $\alpha_{e,g} = \alpha_{g,e} = 1$, where e denotes the identity element of G. Then the identification via crossed products

$$H^2(\mathrm{Gal}(\bar{k}_v), \bar{k}^*_v) = \mathrm{Br}(k_v)$$

associates to $(\alpha_{g,h})$ the element of the Brauer group corresponding to the central simple algebra

$$\mathcal{A} = \bigoplus_{g \in G} K_{v_1} \cdot e_g$$

where e_g are generators, subject to the relations

$$e_g e_h = \alpha_{g,h} e_{gh}$$
$$e_g c = {}^g c e_g$$

for g, $h \in G$ and $c \in K_{v_1}$ (see, e.g., [Dra83]).

Now we recall the local invariant isomorphism $\mathrm{Br}(k_v) = \mathbb{Q}/\mathbb{Z}$. There exists, up to isomorphism, a unique unramified extension ℓ_v/k_v of each degree d; such ℓ_v is cyclic Galois over k_v. Taking d such that the class of $\mathcal{A}$ in $\mathrm{Br}(k_v)$ is d-torsion (e.g., we can take $d = |G|$), there must exist an isomorphism

$$\chi\colon \mathcal{A} \otimes_{k_v} \ell_v \to M_{|G|}(\ell_v) \tag{9.2}$$

of the extension of $\mathcal{A}$ to the degree d unramified field extension ℓ_v with the $|G|$-by-$|G|$ matrix algebra over ℓ_v. The extension ℓ_v can be obtained explicitly (e.g., from a cyclotomic extension).

We let $n = |G|$, and write $\mathcal{A}_{k'}$ for $\mathcal{A} \otimes_{k_v} k'$ where k'/k_v is any field extension. The first step toward the construction of an isomorphism (9.2) is to find an ℓ_v-point on the Brauer–Severi variety associated with $\mathcal{A}$. The Brauer–Severi variety of $\mathcal{A}$ has the property that k'-points correspond bijectively with n-dimensional left ideals of $\mathcal{A}_{k'}$, for any extension k'/k_v. This description supplies explicit equations for the Brauer–Severi variety as a subvariety of the Grassmannian variety $Gr(n, n^2)$ over k_v (see, e.g., [Art82]), and hence there are *a priori* bounds on the v-adic height of an ℓ_v-valued solution. We let $\mathcal{A}_1 \subset \mathcal{A}_{\ell_v}$ denote the corresponding left ideal.

There are $1 = x_1, x_2, \ldots, x_n \in \mathcal{A}_{\ell_v}$ such that if we set $\mathcal{A}_i = \mathcal{A}_1 x_i$ then the spaces $\mathcal{A}_1, \ldots, \mathcal{A}_n$ span $\mathcal{A}_{\ell_v}$. The $\mathcal{A}_i$ can be found effectively, and their entries can be effectively bounded. More precisely, if we vary over a choice of possible x_i (e.g., a fixed k_v-basis of $\mathcal{A}$), then for each choice we get a map $(\mathcal{A}_1)^n \to \mathcal{A}$, given by $(y_i) \mapsto \sum_i y_i x_i$. Such a map is represented by a matrix; now we consider the determinant of the matrix. The tuple of determinants over all choices of x_i is nonvanishing, so appealing to an effective Nullstellensatz we have an *a priori* bound on the minimum of the determinants.

Under the isomorphism of vector spaces

$$\mathcal{A}_{\ell_v} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$$

the vector $1 \in \mathcal{A}_{\ell_v}$ maps to some $(e_{1,1}, \ldots, e_{n,n}) \in \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$. Now we define χ to map $e_{i,i}$ to the matrix with a single entry 1 in the ith row and ith column, and all other entries 0. The prescription $e_{i,j} \in e_{i,i}\mathcal{A}_{\ell_v} \cap \mathcal{A}_{\ell_v} e_{j,j}$, defines the $e_{i,j}$ uniquely up to scale, and we can thereby choose $e_{i,i+1}$ for each i. Then the relations $e_{i,j} e_{i',j'} = \delta_{j,i'} e_{i,j'}$ determine all the $e_{i,j}$ and complete the definition of the algebra isomorphism χ.

The action of $g \in G$ on ℓ_v induces the algebra automorphism $\varphi_g\colon M_n(\ell_v) \to M_n(\ell_v)$ defined by

$$\varphi_g(m) = {}^g(\chi({}^{g^{-1}}(\chi^{-1}(m))))$$

Write

$$\varphi_g(m) = p_g^{-1} m p_g.$$

This is effective Skolem–Noether: for any vector w, the matrix q with vector $\varphi(e_{i,1})w$ in column i (where $e_{i,1}$ denotes the matrix with 1 in row i column 1 and 0 elsewhere) for each i satisfies $\varphi(m)q = qm$ for all $m \in M_n(\ell_v)$, and for some choice of w the determinant of q must have valuation less than some bound that can be made explicit. Then take $p_g = q^{-1}$.

Now we follow [Ser68, §X.5]: if we define $\beta_{g,h}$ by

$$\beta_{g,h}^{-1} = p_g{}^g p_h p_{gh}^{-1} \tag{9.3}$$

then $(\beta_{g,h})$ is a 2-cocycle with values in ℓ_v^* for the extension ℓ_v/k_v such that its class in $\mathrm{Br}(k_v)$ is equal to $\mathcal{A}$. (As remarked in *ibid.*, the construction applied to an algebra defined by a 2-cocycle for the extension ℓ_v representing $B \in H^2(\mathrm{Gal}(\bar{k}_v/k_v), \bar{k}_v^*) = \mathrm{Br}(k_v)$ naturally gives rise to a 2-cocycle for the class $-B$; this explains the power -1 in the definition of $\beta_{g,h}$.) Now $v(\beta_{g,h})$ is a 2-cocycle with values in $\mathbb{Z}$. Using the long exact sequence of cohomology of the sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and acyclicity of $\mathbb{Q}$ we obtain a 1-cocycle with values in $\mathbb{Q}/\mathbb{Z}$, that is, a group homomorphism

$$\mathrm{Gal}(\ell_v/k_v) \to \mathbb{Q}/\mathbb{Z}.$$

The local invariant of the algebra $\mathcal{A}$ (associated with the given 2-cocycle with values in $K_{v_1}^*$) is the image in $\mathbb{Q}/\mathbb{Z}$ of the unique element of $\mathrm{Gal}(\ell_v/k_v)$ which induces the Frobenius automorphism on residue fields (cf. [Ser68, §XIII.3]). □

We write k_v-points of X as tuples

$$\mathbf{x} = (x_0, \ldots, x_N)$$

with $x_{i_0} = 1$ for some i_0 and $x_i \in \mathfrak{o}_v$ (the ring of integers of k_v) for all i. It suffices to consider one chart at a time (i.e., choice of i_0). Henceforth we work with points in a single chart.

Set $h^j := \prod_t f_t^j g_t^j$. The h^j are nonvanishing on U^j, which cover X. So we can apply effective Nullstellensatz (9.1) to the h^j to deduce that there are homogeneous polynomials H^j with coefficients in $\mathfrak{o}_v$ and an equation

$$\sum_j h^j H^j = A x_{i_0}^r$$

for some $A \in \mathfrak{o}_v$ and r. The valuations of A and of the coefficients of the H^j are effectively bounded, as are the degrees of the H^j. It follows that for each $\mathbf{x} \in X(k_v)$ there exists j such that the cocycle (β_t^j) can be evaluated at $\mathbf{x}$, with $\max(v(f_t^j(\mathbf{x})), v(g_t^j(\mathbf{x}))) \leq P$ for some effective bound P that is independent of $\mathbf{x}$.

Proposition 9.5. *Fix the data of Assumption 2.1 and consider $A \in \mathrm{Br}(X)$ with representing cocycles (β_t^j) from Steps 1 through 5. There is an effective bound Q' such that if $\mathbf{x}$ and $\mathbf{x}'$ are points of (a fixed chart of) $X(k_v)$ satisfying $v(x_i - x_i') > Q'$ for all i, then $\mathrm{inv}_v(A(\mathbf{x})) = \mathrm{inv}_v(A(\mathbf{x}'))$.*

Proof. There is an effective bound P such that for some j we have

$$\max(v(f_t^j(\mathbf{x})), v(g_t^j(\mathbf{x}))) \leq P$$

for all t. Hence, for large enough Q', we also have $\max(v(f_t^j(\mathbf{x}')), v(g_t^j(\mathbf{x}'))) \leq P$ for this value of j and all t. The result now follows by Corollary 9.2. □

We can now give an effective procedure to compute the local invariants of the k_v-points of X. As before, we focus on a single chart of X. Then, with Q' as in Proposition 9.5, we enumerate the classes of points of $X(k_v)$, where points $\mathbf{x}$, $\mathbf{x}'$ are considered to lie in the same class if we have $v(x_i - x_i') > Q'$. For each class, we choose a representative point and compute it to a precision which is

(i) enough to identify the j such that $\max(v(f_t^j(\mathbf{x})), v(g_t^j(\mathbf{x}))) \le P$ for all t,
(ii) enough to carry out the algorithm of Proposition 9.3.

Then we evaluate $(\beta_t^j(\mathbf{x}))$ and apply the algorithm of Proposition 9.3. The output is the local invariant of all points $\mathbf{x}' \in X(k_v)$ lying in the same class (in the sense we have just introduced) as $\mathbf{x}$.

We now treat the case of a real place v of k. Then $X(k_v)$ is a real algebraic manifold, and the local invariant of the Brauer group element A is constant on connected components. So we are reduced to determining whether none, some, or all of the connected components of $X(k_v)$ have points where a cocycle representative of A has values in the image of an algebraic coboundary map. For real algebraic varieties there are effective procedures for computing the number of connected components and the image of an algebraic map (cf. [HRR91]). So the ramification pattern of any Brauer group element (or finite collection of Brauer group elements) can be determined effectively.

Example. We carry out the local analysis in the Cassels–Guy example

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0 \tag{9.4}$$

to deduce that this cubic surface X violates the Hasse principle. The original proof of this fact from [CG66] is based on ideal class group computations. The work of Colliot-Thélène, Kanevsky, and Sansuc [CTKS87] treated diagonal cubic surface using the Brauer–Manin obstruction; however they used more complicated (non-cyclic) Azumaya algebras.

The base field is $k = \mathbb{Q}(\zeta)$ with $\zeta = e^{2\pi i/3}$. We have produced an element $A \in \mathrm{Br}(X)$ which generates $\mathrm{Br}(X)/\mathrm{Br}(k) \cong \mathbb{Z}/3\mathbb{Z}$. On various open subsets, A is represented by cyclic Azumaya algebras, for the field extension $k(\sqrt[3]{2/3})$, of the function field elements

$$g_1 := \frac{f}{x^3}, \qquad g_2 := 2\zeta\frac{f'}{x^3}, \qquad g_3 := -60\zeta^2\frac{f''}{x^3}$$

where f, f', and f'' are the polynomials of (6.9), (8.3), and (8.4).

We proceed with the evaluation of the functions g_i at v-adic points of X. The equation (9.4) has good reduction outside of the primes 2, $\sqrt{-3}$, and 5. Since the functions g_i reduce to nontrivial rational functions on the reduction at any place v outside these primes, it follows that A is unramified at any point of $X(k_v)$.

Consider first $v = 2$. We proceed to evaluate the functions g_i at 2-adic points of X and compute the local invariants of the resulting 2-cocycles. Every point of $X(k_2)$ with 2-adic integer coefficients must have x and y not divisible by 2, so we are free to consider $x = 1$ throughout the analysis. It suffices to consider y, z, and t mod 8, as we see in the following computations. For all y, z, and t satisfying (9.4) mod 8, there is always some i such that g_i is of the form $2^n(1+2a)$ with $a \in \mathfrak{o}_2$ and $0 \le n \le 2$. Any number of this form is a norm, since 2 is the norm of $2 + \sqrt[3]{12} + \sqrt[3]{18}$ and for any $a \in \mathfrak{o}_2$ the number $1 + 2a$ is a cube in k_2. So the corresponding 2-cocycle is always trivial, and the local invariant at all 2-adic points of X is 0.

Now consider the place $v = \sqrt{-3}$. Again, we may suppose $x = 1$. We observe that at all points of $X(k_v)$ the value of g_1 is $\sqrt{-3}$ times a unit $u \in \mathfrak{o}_v^*$. To determine the required precision, we make some remarks concerning norms for the extension $k_v(\sqrt[3]{2/3})/k_v$. We have that $\sqrt{-3}$ is a norm,

$$\sqrt{-3} = N\big(-1 - 2\zeta + (1-\zeta)\sqrt[3]{2/3}\big),$$

and that any $u \in \mathfrak{o}_v^*$ congruent to 1 mod 9 is a cube in k_v. Consequently it suffices to evaluate $(1/\sqrt{-3})g_1$ modulo 9, and for this it suffices to consider y, z, and t modulo $9\sqrt{-3}$. It results that $(1/\sqrt{-3})g_1$, modulo 9, always equals one of the following:

$$\zeta, \quad 4\zeta, \quad 7\zeta, \quad 3+\zeta, \quad 3+4\zeta, \quad 3+7\zeta. \tag{9.5}$$

The equation from the previous paragraph expressing 2 as a norm is valid in k_v, and we also have

$$N\big(1 + (-1-2\zeta)\sqrt[3]{2/3}\big) = 3 + 4\zeta.$$

Consequently, all numbers in (9.5) are of the form ζ times a norm. By the algorithm of Proposition 9.3, the local invariant of the cyclic division algebra defined by ζ is computed to be 2/3. So the local invariant at all v-adic points of X is 2/3.

We remark that the application of Proposition 9.3 in the previous paragraph to compute a v-adic local invariant requires solving for the isomorphism (9.2) to certain precision in order to ensure that the subsequent steps of the algorithm lead to a meaningful evaluation. The observed loss of significance in computing $\beta_{g,h}$ (9.3) from χ is on the order of 3^{10}, meaning that according to the algorithmic description of the computation we would require y, z, and t to such a high precision (the *a priori* bounds are of course much worse). This is in contrast to the analysis from Lemma 9.1, which implies that values modulo $9\sqrt{-3}$ suffice.

Finally, the field k_5 contains $\sqrt[3]{2/3}$, so the 5-adic analysis is trivial. At any adelic point of X, the sum of local invariants is 2/3. In conclusion, the surface X defined by (9.4) violates the Hasse principle.

References

[Art82] M. Artin, "Brauer-Severi varieties" in *Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981)*, Lecture Notes in Math. **917**, Springer-Verlag, Berlin, 1982, 194–210.

[AT68] E. Artin and J. Tate, *Class field theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[BEL91] A. Bertram, L. Ein, and R. Lazarsfeld *Vanishing theorems, a theorem of Severi, and the equations defining projective varieties*, J. Amer. Math. Soc. **4** (1991), no. 3, 587–602.

[Bri07] M. Bright, *Efficient evaluation of the Brauer-Manin obstruction*, Math. Proc. Cambridge Philos. Soc. **142** (2007), no. 1, 13–23.

[Bro94] K. S. Brown, *Cohomology of groups*, Springer-Verlag, New York, 1994.

[BSD04] M. Bright and P. Swinnerton-Dyer, *Computing the Brauer-Manin obstructions*, Math. Proc. Cambridge Philos. Soc. **137** (2004), no. 1, 1–16.

[CF67] J. W. S. Cassels and A. Fröhlich, eds., *Algebraic number theory*, London, Academic Press, 1967.

[CG66] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120.

[CLO97] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, second ed., Springer-Verlag, New York, 1997.

[CTKS87] J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc, "Arithmétique des surfaces cubiques diagonales" in *Diophantine approximation and transcendence theory (Bonn, 1985)*, Lecture Notes in Math. **1290**, Springer-Verlag, Berlin, 1987, 1–108.

[CTS80] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles" in *Journées de Géometrie Algébrique d'Angers, July 1979*, Sijthoff & Noordhoff, Alphen aan den Rijn, 1980, 223–237.

[CTS87] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles, II*, Duke Math. J. **54** (1987), no. 2, 375–492.

[dJ05] A. J. de Jong, *A result of Gabber*, 2005, preprint.

[Dra83] P. K. Draxl, *Skew fields*, Cambridge University Press, Cambridge, 1983.

[EGAI] A. Grothendieck, *Éléments de géométrie algébrique, I*, Inst. Hautes Études Sci. Publ. Math. **4** (1960).

[EGAII] A. Grothendieck, *Éléments de géométrie algébrique, II*, Inst. Hautes Études Sci. Publ. Math. **8** (1961).

[Gro68] A. Grothendieck, "Le groupe de Brauer, I–III" in *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam, 1968, 46–188.

[SGA1] A. Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Math. **224**, Springer-Verlag, Berlin, 1971,

[Har96] D. Harari, "Obstructions de Brauer–Manin transcendantes" in *Number theory (Paris, 1993–1994)*, London Math. Soc. Lecture Note Ser. **235**, Cambridge Univ. Press, Cambridge, 1996, 75–87.

[Has23a] H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148.

[Has23b] H. Hasse, *Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 205–224.

[Has24] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 113–130.

[Hen08] K. Hensel, *Theorie der algebraischen Zahlen*, B. G. Teubner, Leipzig, 1908.

[Hen13] K. Hensel, *Zahlentheorie*, G. J. Göschen'sche Verlagshandlung, Berlin, 1913.

[HRR91] J. Heintz, T. Recio, and M.-F. Roy, "Algorithms in real algebraic geometry and applications to computational geometry" in *Discrete and computational geometry (New Brunswick, NJ, 1989/1990)*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **6**, Amer. Math. Soc., Providence, RI, 1991, 137–163.

[IP99] V. A. Iskovskikh and Y. G. Prokhorov, *Fano varieties*, Algebraic geometry, V, Encyclopaedia Math. Sci. **47**, Springer-Verlag, Berlin, 1999, 1–247.

[KPS01] T. Krick, L. M. Pardo, and M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), no. 3, 521–598.

[KR00] M. Kreuzer and L. Robbiano, *Computational commutative algebra, 1*, Springer-Verlag, Berlin, 2000.

[KT04] A. Kresch and Y. Tschinkel, *On the arithmetic of del Pezzo surfaces of degree 2*, Proc. London Math. Soc. (3) **89** (2004), no. 3, 545–569.

[Lem03] F. Lemmermeyer, *A note on Pépin's counterexamples to the Hasse principle for curves of genus 1*, Abh. Math. Sem. Univ. Hamburg **69** (1999), 335–345.

[Lin40] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, 1940, Thesis, University of Uppsala.

[Log04] A. Logan, `Brauer`, 2004, Magma package for determining the Brauer–Manin obstruction of a del Pezzo surface of degree 4.

[Man71] Y. I. Manin, "Le groupe de Brauer-Grothendieck en géométrie diophantienne" in *Actes du Congrès International des Mathématiciens (Nice, 1970)*, Tome 1, Gauthier-Villars, Paris, 1971, 401–411.

[Man74] Y. I. Manin, *Cubic forms: algebra, geometry, arithmetic*, North-Holland Publishing Co., Amsterdam, 1974.

[Min90] H. Minkowski, *Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten ineinander rational transformiert werden können*, J. Reine Angew. Math. **106** (1890), 5–26.

[Pép80] T. Pépin, *Nouveaux théorèmes sur l'équation indéterminée* $ax^4 + by^4 = z^2$, C. R. Acad. Sci Paris **91** (1880), no. 2, 100–101.

[Rei42] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18.

[Ser68] J.-P. Serre, *Corps locaux*, second ed., Hermann, Paris, 1968.

[Siu93] Y. T. Siu, *An effective Matsusaka big theorem*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 5, 1387–1405.

[Sko99] A. N. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), no. 2, 399–424.

[Sou17] C. P. Sousley, *Invariants and covariants of the Cremona cubic surface*, Amer. J. Math. **39** (1917), 135–146.

[Wit04] O. Wittenberg, "Transcendental Brauer-Manin obstruction on a pencil of elliptic curves" in *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, Progr. Math. **226**, Birkhäuser Boston, Boston, MA, 2004, 259–267.

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland

E-mail address: `andrew.kresch@math.unizh.ch`

Mathematisches Institut, Georg-August-Universität Göttingen, Bunsenstrasse 3-5, D-37073 Göttingen, Germany

Current address: Courant Institute, 251 Mercer Street, New York, NY 10012, USA

E-mail address: `tschinkel@cims.nyu.edu`