THE BRAUER-MANIN OBSTRUCTION ON DEL PEZZO SURFACES OF DEGREE 2

PATRICK CORN

Abstract. This paper explores the computation of the Brauer-Manin obstruction on Del Pezzo surfaces of degree 2, with examples coming from the class of "semi-diagonal" Del Pezzo surfaces of degree 2. It is conjectured that the failure of the Hasse principle for a broad class of varieties, including Del Pezzo surfaces, can always be explained by a nontrivial Brauer-Manin obstruction. We provide computational evidence in support of this conjecture for semi-diagonal Del Pezzo surfaces of degree 2. In addition, we determine the complete list of the possibilities for the finite abelian group $H^1(k, \operatorname{Pic} \overline{X})$, where X is a Del Pezzo surface of any degree, thus completing a computation which had been previously carried out in various special cases only.

1. Introduction

If X is a variety over a number field k, the simplest question one can ask about the rational points on X is whether $X(k)$ is empty. This is a difficult question in general, but it is relatively easy to check whether $X(k_v)$ is empty, for all places v of k. So the difficult part of the question of rational points is detecting whether or not the Hasse principle holds for a class of varieties containing X.

When the Hasse principle does not hold for a class of varieties, its failure can often be explained by the Brauer-Manin obstruction. This obstruction is the subject of much recent research; while it has been established that the Brauer-Manin obstruction explains the failure of the Hasse principle completely for certain classes of varieties (cf. [19] for a summary), and it is conjectured that this is also the case for a much broader class of varieties, the gap between what is conjectured and what can be proved is quite wide.

In this context, Del Pezzo surfaces and their arithmetic have been explored quite extensively in recent years. These surfaces are important examples of rational surfaces, and their geometry is rather well-understood. To each Del Pezzo surface is associated a positive integer $d \leq 9$, called the degree. It is known that if a Del Pezzo surface is a counterexample to the Hasse principle, then $2 \leq d \leq 4$; and counterexamples to the Hasse principle are known for all of these values of d. As the degree decreases, the surface tends to become more difficult to understand. When $d = 2$, X is the surface in weighted projective space $\mathbb{P}(2, 1, 1, 1)$ given by the equation

$$w^2 = F(x, y, z),$$

where F is a homogeneous polynomial of degree 4. So X is a double cover of $\mathbb{P}^2$ ramified over the (smooth) quartic curve $F = 0$. The lifts of the 28 bitangents to this quartic curve come in pairs, forming 56 exceptional curves on $\overline{X}$.

A systematic exploration of the Brauer-Manin obstruction on Del Pezzo surfaces of degree 4 and 3 was carried out by Swinnerton-Dyer in [20] and [21]. Calculations in [6], extended

Date: July 18, 2006.

in the author's Ph.D. thesis [8], gave strong computational evidence that the "standard conjecture"–namely, that any failure of the Hasse principle could be explained by a Brauer-Manin obstruction–was true for diagonal cubic surfaces (which are Del Pezzo surfaces of degree 3); see also [22] for further theoretical steps in this direction.

In this paper, we explore the Brauer-Manin obstruction on Del Pezzo surfaces of degree 2. In the paper [12], the authors studied *diagonal* Del Pezzo surfaces of degree 2. The advantage of studying this special class of surfaces was that the exceptional curves could be written down quite explicitly, and the same was true of the Galois group of the field extension over which all the exceptional curves were defined. Here, we study general Del Pezzo surfaces of degree 2, and in particular we study elements of $H^1(k, \operatorname{Pic} \overline{X})$ of order 2, and show how to obtain nonconstant elements of the Brauer group coming from certain such elements. This can be seen as a generalization of the method of [12], with the advantage that we are able to study the Brauer-Manin obstruction on a much broader class of surfaces, including the "semi-diagonal" surfaces we introduce in Section 7.

The Brauer-Manin obstruction arises from elements of $\operatorname{Br} X$ not coming from $\operatorname{Br} k$. There is an isomorphism

$$\frac{\operatorname{Br} X}{\operatorname{Br} k} \to H^1(k, \operatorname{Pic} \overline{X})$$

coming from the Hochschild-Serre spectral sequence. The explicit computation of the Brauer-Manin obstruction splits naturally into two parts: first, understanding the right side of the above isomorphism; and second, attempting to use the inverse of the above isomorphism to obtain explicit elements of $\operatorname{Br} X$ whose invariants we can compute.

Our first result is an enumeration of the possibilities for the finite abelian group $H^1(k, \operatorname{Pic} \overline{X})$, where X is a Del Pezzo surface of any degree. For $5 \le d \le 9$, this group is trivial, and the computation was carried out for $d = 3, 4$ in [20]. Other authors have carried out this computation in special cases as well. Using the methods of [20] and the computer algebra system MAGMA, we obtain:

Theorem 4.1. *Let X/k be a Del Pezzo surface of degree d. Then $H^1(k, \operatorname{Pic} \overline{X})$ is isomorphic to one of the following groups:*

$5 \le d \le 9$: $\{1\}$

$d = 4$: $\{1\}, \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2$

$d = 3$: any of the above groups, or $\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2$

$d = 2$: any of the above groups, or $(\mathbb{Z}/2\mathbb{Z})^s$ $(3 \le s \le 6)$,
$\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(0 \le t \le 2)$, $(\mathbb{Z}/4\mathbb{Z})^2$

$d = 1$: any of the above groups, or $(\mathbb{Z}/2\mathbb{Z})^7, (\mathbb{Z}/2\mathbb{Z})^8, (\mathbb{Z}/3\mathbb{Z})^s (s = 3, 4)$,
$\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^s$ $(s = 3, 4)$, $(\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(t = 1, 2)$, $\mathbb{Z}/5\mathbb{Z}, (\mathbb{Z}/5\mathbb{Z})^2$,
$\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/6\mathbb{Z})^2$

This theorem is interesting on its own, but we will be particularly interested in part of the proof in the case $d = 2$. Using it, we analyze elements of order 2 in $(\operatorname{Br} X)/(\operatorname{Br} k)$, and separate them into two types. While elements of the second type remain quite mysterious to us (we do not know of any explicit examples of such elements, although they must exist), we will be able to say quite a bit about elements of the first type.

Our first result about elements of the first type describes a correspondence between them and certain Galois-stable configurations of bitangents to the associated quartic curve called *Steiner complexes*. It is the analogue of the results of Swinnerton-Dyer in [20] relating nonconstant elements of $\operatorname{Br} X$, X a cubic surface, to Galois-stable subsets of the 27 lines on $\overline{X}$.

Theorem 6.10. *Let X be a Del Pezzo surface of degree 2 over a field k, isomorphic to a double cover of $\mathbb{P}^2$ ramified over a quartic curve C. There is a one-to-one correspondence between nonzero 2-torsion elements of $H^1(k, \operatorname{Pic} \overline{X})$ of the first type and Steiner complexes on $\overline{C}$ defined over k which have the property that the action of G_k on the 24 exceptional curves over the complex satisfies four nontriviality conditions C_2, C_{12}, C_{32}, C_{160} (which are given explicitly in the proof).*

Next, we define S_C to be the set of 2×2 symmetric matrices whose entries are homogeneous quadratic polynomials in x, y, z and whose determinant is equal to a nonzero constant multiple of F. We view two matrices in S_C as equivalent if one is obtained from the other by pre- and post-multiplying by a constant matrix.

There is a one-to-one correspondence between Steiner complexes and nonzero 2-torsion elements of the Jacobian of C, and another correspondence relating such elements to elements of $S_C/\equiv$. Putting these together, we obtain the following results, which give a completely explicit description of cyclic Azumaya algebras corresponding to elements of the first type:

Proposition 6.8. *If c is an element of the first type, there is an extension N_c of k, with $[N_c : k] \leq 2$, such that c is in the kernel of the restriction map $H^1(k, \operatorname{Pic} \overline{X}) \to H^1(N_c, \operatorname{Pic} \overline{X})$. The field N_c is the field of definition of the difference between two skew exceptional curves in $\operatorname{Pic} \overline{X}$.*

Theorem 6.12. *Suppose X is a Del Pezzo surface of degree 2 over a number field k given by a double cover of $\mathbb{P}^2$ ramified above a (nonsingular) quartic curve C over k. Suppose also that $X(\mathbb{A}_k) \neq \emptyset$. If ω is a G_k-invariant element of $S_C/\equiv$, then it corresponds to an element c of $H^1(k, \overline{P})[2]$ (which may or may not be zero). Then:*

(1) *If $[N_c : k] = 2$, ω lifts to an element of the form*

$$B = \begin{pmatrix} B_1 & B_2 \\ B_2 & b(\alpha B_1) \end{pmatrix} \in S_C$$

where B_1 is a homogeneous quadratic polynomial in x, y, z with coefficients in N_c, B_2 is a homogeneous quadratic polynomial in x, y, z with coefficients in k, $b \in k$, and α is the nontrivial element of $\operatorname{Gal}(N_c/k)$.

(2) *If $N_c = k$, ω lifts to an element of the form*

$$B = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix} \in S_C$$

with the B_i homogeneous quadratic polynomials defined over k.

In both cases, we may choose the B_i so that the equation of X can be written as $-w^2 = \det B$.

The proof of the theorem is constructive: given a G_k-invariant element $\omega \in S_C/\equiv$, it describes how to construct the lift B given in the theorem.

Theorem 6.16. *Let X be a Del Pezzo surface of degree 2 isomorphic to a double cover of $\mathbb{P}^2_k$ ramified over a quartic curve C. Suppose there is a nonzero element $c \in H^1(k, \operatorname{Pic} \overline{X})[2]$*

of the first type, and let ω be the corresponding element of $S_C/\equiv$. Let $B = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix}$ be the matrix produced by Theorem 6.12. Then $[N_c : k] = 2$ and c maps to the class of the quaternion Azumaya algebra

$$(N_c/k, (B_2 - w)/x^2) \in \operatorname{Br} X.$$

Next, we use the above theorems to discuss the computation of the Brauer-Manin obstruction for *semi-diagonal* Del Pezzo surfaces of degree 2; that is, surfaces where the quartic polynomial F is a polynomial in x^2, y^2, z^2. In Proposition 7.1, we construct a cyclic quaternion algebra $\mathcal{A}$ in terms of the coefficients A, B, C, D, E, G of the polynomial F, and we show that, at least generically, it represents the only nontrivial equivalence class in $(\operatorname{Br} X)/(\operatorname{Br} k)$:

Proposition 7.2. *Let A, B, C, D, E, G be indeterminates, and let G_{sd} be the Galois group of the 56 lines on the surface X_{sd} given by the equation (9), considered over the field $\mathbb{Q}(A, B, C, D, E, G)$. Let H_{sd} be the image of G_{sd} under the natural map $G_{sd} \to W(E_7)$. Then $H^1(H_{sd}, \mathbb{Z}^8) = \mathbb{Z}/2$. So $(\operatorname{Br} X_{sd})/(\operatorname{Br} k)$ is generated by the cyclic quaternion algebra $\mathcal{A}$ of Proposition 7.1.*

After a discussion of the implementation in MAGMA of the computation of the Brauer-Manin obstruction for the cyclic Azumaya algebras obtained from the above theorems, we give some examples of this computation, as well as some computational evidence that the standard conjecture is true for diagonal Del Pezzo surfaces of degree 2:

Theorem 9.1. *Let X be a Del Pezzo surface of degree 2 over $\mathbb{Q}$ given by the equation*

$$w^2 = Ax^4 + By^4 + Cz^4$$

with $|A|, |B|, |C| \leq 50$. Then if X fails to satisfy the Hasse principle, X has a nontrivial Brauer-Manin obstruction.

2. Preliminaries

2.1. **Del Pezzo surfaces.** A Del Pezzo surface is a (smooth) Fano variety of dimension 2. Here we recall the basic properties of Del Pezzo surfaces. (Throughout this paper, G_k will denote the absolute Galois group $\operatorname{Gal}(\overline{k}/k)$.)

Proposition 2.1. *Let X be a Del Pezzo surface over a field k. Let d be the self-intersection $(\omega_X^{-1}, \omega_X^{-1})$ of the anticanonical divisor. Let $\overline{X} = X \times_k \overline{k}$.*

(a) $1 \leq d \leq 9$.

(b) $\operatorname{Pic} \overline{X}$ is a free abelian group of rank $10 - d$.

(c) If $X' \to X$ is a birational morphism and X' is a Del Pezzo surface, then X is a Del Pezzo surface.

(d) Either $\overline{X}$ is isomorphic to the blowup of $\mathbb{P}^2$ at $r = 9 - d$ points $\{x_1, \ldots, x_r\}$ in general position, or $d = 8$ and $\overline{X} = \mathbb{P}^1 \times \mathbb{P}^1$. Conversely, any surface X satisfying the above condition is a Del Pezzo surface. (For a definition of "general position," see Definition 2.2 below.)

(e) For $\overline{X}$ isomorphic to the blowup of $\mathbb{P}^2$ at $r = 9 - d$ points $\{x_1, \ldots, x_r\}$ in general position, let C be an exceptional curve on $\overline{X}$; that is, C is a curve on $\overline{X}$ such that $(C, C) = -1$ and $C \cong \mathbb{P}^1_{\overline{k}}$. Then the image of C under the blowing-down map to $\mathbb{P}^2$ is either:

(1) *one of the x_i*

(2) *a line passing through two of the* x_i
(3) *a conic passing through five of the* x_i
(4) *a cubic passing through seven of the* x_i *such that one* x_i *is a double point*
(5) *a quartic passing through eight of the* x_i *such that three* x_i *are double points*
(6) *a quintic passing through eight of the* x_i *such that six* x_i *are double points*
(7) *a sextic passing through eight of the* x_i *such that seven* x_i *are double points and one is a triple point*

Conversely, each object in the preceding list gives rise to exactly one exceptional curve C.

(f) The anticanonical map $X \to \mathbb{P}^d$ *is a closed immersion for* $d \geq 3$, *so* X *can be realized as a degree-d surface in* $\mathbb{P}^d$ *for* $d \geq 3$. *For* $d = 2$ *the anticanonical map has degree* 2.

(g) Let X *be a Del Pezzo surface of degree* d. *A* G_k*-stable set of* n *pairwise skew exceptional curves on* $\overline{X}$ *can be blown down over* k*; that is, there is a birational morphism* $f: X \to Y$ *exhibiting* X *as the blowup of* Y *at a set of* n G_k*-stable points in general position. (By (c),* Y *is a Del Pezzo surface of degree* $d + n$*).*

Proof of proposition: Parts (a)-(g) are Theorem 24.3(i), Lemma 24.3.1, Corollary 24.5.2(i), Theorem 24.4, Theorem 26.2, Theorem 24.5 (and Remark 24.5.1), and a special case of Theorem 21.5 of [14], respectively. ■

Definition 2.2. A set of points $x_1, \ldots, x_r$ in $\mathbb{P}^2$ are in *general position* if no three of the points lie on a line, no six lie on a conic, and no eight lie on a singular cubic with a singularity at an x_i.

Remark 2.3. Part (e) shows that there are only finitely many exceptional curves on $\overline{X}$, and in fact, for each value of r, the number c_r of exceptional curves is easily computable from the description in part (e):

r	0	1	2	3	4	5	6	7	8
c_r	0	1	3	6	10	16	27	56	240

Remark 2.4. The finite set of exceptional curves is G_k-stable, because G_k preserves intersections.

2.2. **The Brauer-Manin obstruction.** Here we briefly recall the notation we will use in describing the Brauer-Manin obstruction. If we let $X(\mathbb{A}_k)$ be the set of adelic points of X, where X is a proper k-variety, then the natural map $X(\mathbb{A}_k) \to \prod_v X(k_v)$, where the product runs over all places v of k, is a bijection. (Cf. [19], pp. 98-99.)

For X a k-variety, k a global field, and $\mathcal{A} \in \operatorname{Br} X$, define

$$X(\mathbb{A}_k)^{\mathcal{A}} = \{(x_v) \in X(\mathbb{A}_k) \colon \sum_v \operatorname{inv}_v \mathcal{A}(x_v) = 0\}$$

and define

$$X(\mathbb{A}_k)^{\operatorname{Br}} = \bigcap_{\mathcal{A} \in \operatorname{Br} X} X(\mathbb{A}_k)^{\mathcal{A}}.$$

Class field theory shows that

$$X(k) \subseteq X(\mathbb{A}_k)^{\operatorname{Br}},$$

and we say that X has a Brauer-Manin obstruction to rational points if $X(\mathbb{A}_k)^{\operatorname{Br}} = \emptyset$. We will assume throughout that the varieties X we study satisfy $X(\mathbb{A}_k) \neq \emptyset$, as we are only interested in counterexamples to the Hasse principle. The standard conjecture about the

Brauer-Manin obstruction is that, at least for sufficiently nice varieties, it should explain every counterexample to the Hasse principle (cf. [4]):

Conjecture 2.5. (Colliot-Thélène) The Brauer-Manin obstruction to rational points is the only one for rationally connected smooth projective geometrically integral varieties over number fields; that is, for such varieties, $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset \Rightarrow X(k) \neq \emptyset$.

3. The cohomological invariant

3.1. **Definitions and previously known results.** Del Pezzo surfaces of degree ≥ 5 satisfy the Hasse principle, and in fact a Del Pezzo surface of degree $1, 5$, or 7 must automatically have a k-point. (See [5] for a summary, and [19], Corollary 3.1.5 for $d = 5$.) This leaves $d = 2, 3, 4$ as interesting cases. There are well-known counterexamples to the Hasse principle for each of these remaining degrees (see [12], [3], and [1] for examples with $d = 2, 3, 4$, respectively). Also, Adam Logan has created a MAGMA program for computing the Brauer-Manin obstruction in complete generality in the case $d = 4$. Cf. [13].

The first step in computing the Brauer-Manin obstruction is understanding the cokernel of the natural map $\operatorname{Br} k \to \operatorname{Br} X$. Elements in the image of this map are called *constant* algebras. Class field theory implies that $X(\mathbb{A}_k)^{\mathrm{Br}}$ equals the intersection of the sets $X(\mathbb{A}_k)^{\mathcal{A}}$ as $\mathcal{A}$ runs over representatives of the cokernel $(\operatorname{Br} X)/(\operatorname{Br} k)$ (the map $\operatorname{Br} k \to \operatorname{Br} X$ is injective whenever X has points everywhere locally, which we are already assuming).

From Proposition 2.1(d), we see that Del Pezzo surfaces are *rational*; that is, $\overline{X}$ is birational to $\mathbb{P}^2_{\overline{k}}$. So the Brauer group has no transcendental part, and the Hochschild-Serre spectral sequence gives an isomorphism

$$\frac{\operatorname{Br} X}{\operatorname{Br} k} \to H^1(k, \operatorname{Pic} \overline{X}) \tag{1}$$

When X is a Del Pezzo surface, we will see that $H^1(k, \operatorname{Pic} \overline{X})$ turns out to be finite and quite small. This is extremely useful for computation of the Brauer-Manin obstruction. Here is a summary of what was previously known about this group for Del Pezzo surfaces X of degree d:

- For $5 \leq d \leq 9$, $H^1(k, \operatorname{Pic} \overline{X})$ is trivial ([14]).
- For $d = 4$, $H^1(k, \operatorname{Pic} \overline{X}) \cong 1, \mathbb{Z}/2$, or $(\mathbb{Z}/2)^2$ ([20]).
- For $d = 3$, $H^1(k, \operatorname{Pic} \overline{X}) \cong 1, \mathbb{Z}/2, (\mathbb{Z}/2)^2, \mathbb{Z}/3$, or $(\mathbb{Z}/3)^2$ ([20]).
- If $X/\mathbb{Q}$ is a *diagonal* Del Pezzo surface of degree 2 (defined in [12]), then $H^1(k, \operatorname{Pic} \overline{X}) \cong 1, \mathbb{Z}/2, (\mathbb{Z}/2)^2, (\mathbb{Z}/2)^3, \mathbb{Z}/4$, or $\mathbb{Z}/4 \oplus \mathbb{Z}/2$.
- For all values of d, Urabe gave a list of the possibilities for $H^1(k, \operatorname{Pic} \overline{X})$ when $\operatorname{Pic} \overline{X}$ can be generated by elements of $\operatorname{Pic} X_F$, F a cyclic extension of k ([23]).

The first main theorem of this paper, Theorem 4.1, completes this classification by determining the possibilities for $H^1(k, \operatorname{Pic} \overline{X})$ when X is a Del Pezzo surface of degree 2 or 1. Most of the main ideas are due to Swinnerton-Dyer, outlined in his paper [20], in which he solved the problem for $d = 3, 4$. These ideas also give some insight into the connection between the geometry of $\overline{X}$ and the presence of nontrivial elements of $H^1(k, \operatorname{Pic} \overline{X})$. It will be convenient to review Swinnerton-Dyer's results for $d = 3$ to illustrate this connection in a more well-known setting, before we move on to the more computationally difficult cases covered in the proof of Theorem 4.1.

First, we describe $\overline{P} := \operatorname{Pic} \overline{X}$ for Del Pezzo surfaces X. When $\overline{X}$ is isomorphic to the blow-up of $\mathbb{P}^2$ at r points, $\operatorname{Pic} \overline{X}$ is freely generated by the class μ of a line in $\mathbb{P}^2$ together with the classes $e_1, \ldots, e_r$ of the exceptional curves lying over the blown-up points $x_1, \ldots, x_r$ $(r = 9 - d)$. The canonical class, with respect to this basis, equals $(-3, 1, \ldots, 1)$. This will be the standard basis we will use in our calculations.

To compute $H^1(k, \overline{P})$, we begin by reducing to the cohomology of a finite group. If M/k is a Galois extension such that $\overline{P}^{G_M} = \overline{P}$, then the inflation map $H^1(\operatorname{Gal}(M/k), \overline{P}) \to H^1(k, \overline{P})$ is an isomorphism. In practice, we choose M to be the field of definition of the exceptional curves on $\overline{X}$, since the classes of these curves generate $\overline{P}$.

Now, since the set of exceptional curves on a Del Pezzo surface is G_k-invariant, we have a natural map $G_k \to A$, where A is the automorphism group of the exceptional curves preserving intersections (since the intersection pairing is preserved by the action of G_k as well). By the definition of the field M in the above paragraph, the kernel of this map is exactly G_M, so we get an induced injection $\operatorname{Gal}(M/k) \hookrightarrow A$.

The group A can be obtained from the theory of lattices and root systems. For a thorough exposition, see [14], Ch. 4, especially Theorem 23.9. When $d \leq 3$, i.e. $r \geq 6$, it is well-known that $A \cong W(E_r)$, the Weyl group of the lattice E_r.

At any rate, $W(E_r)$ is a finite group with a fixed action on $\mathbb{Z}^{r+1} = \operatorname{Pic} \overline{X}$, and to determine the possible groups which appear as $(\operatorname{Br} X)/(\operatorname{Br} k)$, we need only determine the possibilities for $H^1(H, \mathbb{Z}^{r+1})$, where H is any subgroup of $W(E_r)$. However, $W(E_r)$ is too large for us to solve the problem simply by listing its subgroups and computing the cohomology of each of them (at least when $d = 1$). This is where Swinnerton-Dyer's method enters the picture. Here we give several elementary lemmas about group cohomology that will be helpful to us later.

Lemma 3.1. *Let G be a finite (or profinite) group, and A a (continuous) G-module. Then there is an isomorphism*

$$\frac{(A/mA)^G}{A^G/mA^G} \to H^1(G, A)[m]$$

defined by

$$(\textit{class of } x \in A) \mapsto (\sigma \mapsto \frac{1}{m}(\sigma x - x))$$

Proof of lemma: Consider the exact sequence

$$0 \to A \xrightarrow{m} A \to A/mA \to 0$$

of G-modules. This gives the long exact sequence of cohomology which begins

$$0 \to A^G \xrightarrow{m} A^G \to (A/mA)^G \xrightarrow{\partial} H^1(G, A) \xrightarrow{m} H^1(G, A)$$

and the lemma follows. (The description of the isomorphism is simply the definition of the boundary map ∂.) $\square$

Lemma 3.2. *Let H be any subgroup of G, for G and A as above. For integers d and n with $d|n$, we have a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^H/nA^H & \longrightarrow & (A/nA)^H & \longrightarrow & H^1(H,A)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \cdot n/d} & & \\ 0 & \longrightarrow & A^H/dA^H & \longrightarrow & (A/dA)^H & \longrightarrow & H^1(H,A)[d] & \longrightarrow & 0 \end{array}$$

where the unlabeled vertical arrows are the natural maps given by reduction mod d.

Proof of lemma: This follows directly from the proof of Lemma 3.1. □

Remark 3.3. Let H be a subgroup of G, for G and A as above. If H' is a conjugate of H, there is a natural isomorphism $H^1(H,A) \to H^1(H',A)$. We will use this fact quite often in what follows.

Remark 3.4. Similarly, if an element $x \in A/mA$ maps to $c_x \in H^1(G,A)[m]$, then $c_{gx} = gc_x$ for any $g \in G$, so c_x will be a coboundary if and only if c_{gx} is. If we are looking for elements $x \in A/mA$ which map to nontrivial cocycles, we need only consider one element from each G-orbit of A/mA.

Lemma 3.5. *If G is a finite group, A is a G-module, p is a prime number, and G_p is a Sylow p-subgroup of G, then the restriction map*

$$H^1(G,A)_p \to H^1(G_p,A)$$

is injective, where $H^1(G,A)_p$ is the unique Sylow p-subgroup of the finite abelian group $H^1(G,A)$.

Proof of lemma: The composition

$$\mathrm{cores} \circ \mathrm{res}\colon H^1(G,A) \to H^1(G_p,A) \to H^1(G,A)$$

is multiplication by $[G : G_p]$ ([15], p. 54), which is prime to p, so passing to $H^1(G,A)_p$ gives an isomorphism. The first map, restriction, must therefore be injective. □

Remark 3.6. We will apply Lemmas 3.1, 3.2, and 3.5, and Remarks 3.3 and 3.4 with $A = \operatorname{Pic} \overline{X}$ and $G = G_k$ or some quotient of G_k (e.g. $\mathrm{Gal}(M/k)$ for M as defined above). For notational convenience, let $P = \overline{P}^{G_k}$; then Lemma 3.1 gives an explicit isomorphism

$$\frac{(\overline{P}/m\overline{P})^{G_k}}{P/mP} \to H^1(k,\overline{P})[m]$$

3.2. **The case $d = 3$.** Since the group $W(E_6)$ in which G_k embeds is of order $51840 = 2^7{\cdot}3^4{\cdot}5$ (cf. [14], p. 139), the only possible prime orders of elements of $H^1(k,\overline{P})$ are $2, 3$, and 5, by Lemma 3.5. It is not hard to show that 5 cannot occur (see [14], Theorem 29.3). On the other hand, elements of order 2 or 3 can occur, and next we show that these elements correspond to certain G_k-invariant configurations of exceptional curves on $\overline{X}$.

For $d = 3$, the set $\mathcal{E}$ of exceptional curves on $\overline{X}$ has cardinality 27; with respect to the basis $\mu, e_1, \ldots, e_6$, we obtain the following list of their classes by using the description in Proposition 2.1(e):

- 6 classes e_i, $1 \le i \le 6$
- 15 classes $f_{ij} = \mu - e_i - e_j$, $1 \le i < j \le 6$
- 6 classes $g_i = 2\mu - (e_1 + \ldots + e_6) + e_i$, $1 \le i \le 6$

Denote the curves corresponding to these classes by E_i, F_{ij}, G_i, respectively.

Using Lemma 3.1, we let $m = 2$ or 3, and look for elements $x \in \overline{P}/m\overline{P}$ whose mod-m stabilizer $S_{x,m}$ in $W(E_6)$ is strictly larger than the stabilizer S_y of any lift y of x to $\overline{P}$. This is precisely what is needed for there to be a nontrivial element on the left side of the isomorphism in Lemma 3.1 (where G will be contained in $S_{x,m}$ but not S_y).

For $m = 2$, a simple computation shows that any nonzero element $x \in \overline{P}/2\overline{P}$ is in the same $W(E_6)$-orbit as $e_1, \pi + e_1, e_1 + e_2$, or $\pi + e_1 + e_2$, where $\pi = 3\mu - \sum_{i=1}^{6} e_i$. Adding π does not change the cocycle $c_x \in H^1(k, \overline{P})$, since $\pi \in P$. So we need only consider e_1 and $e_1 + e_2$.

It is immediate from the description of the classes of exceptional curves in $\mathcal{E}$ that these classes are distinct in $\overline{P}/2\overline{P}$, so $e_1 \in (\overline{P}/2\overline{P})^H \Rightarrow e_1 \in \overline{P}^H$. So c_{e_1} can never be a nontrivial cocycle.

On the other hand, let $x_2 = e_1 + e_2$. Using MAGMA, one can show that $\overline{P}^{S_{x_2,2}} = \mathbb{Z}\pi$, so $S_{x_2,2}$ is strictly larger than the stabilizer of any element congruent to x_2 mod $2\overline{P}$. But $S_{x_2,2}$ must fix the set

$$T_1 = \{Y \in \mathcal{E} \colon (y, x_2) \equiv 1 (\mathrm{mod}\ 2)\} = \{E_1, E_2, G_1, G_2\} \cup \{F_{1j}, F_{2j} \colon 3 \le j \le 6\}.$$

Definition 3.7. If X is a Del Pezzo surface of degree 3, a *double-six* is a set of twelve exceptional curves $\{L_1, \ldots, L_6\} \cup \{M_1, \ldots, M_6\}$ on $\overline{X}$ such that

(1) the L_i are pairwise skew
(2) the M_i are pairwise skew
(3) $(L_i, M_j) = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } i \neq j \end{cases}$

The sets $\{L_1, \ldots, L_6\}$ and $\{M_1, \ldots, M_6\}$ are called *(skew) sixes*, and we will call the six disjoint sets $\{L_i, M_i\}$ *opposite pairs.*

Note that the set $T_1 = \{E_1, G_1, F_{23}, F_{24}, F_{25}, F_{26}\} \cup \{E_2, G_2, F_{13}, F_{14}, F_{15}, F_{16}\}$ is a double-six.

Lemma 3.8. *Let X be a Del Pezzo surface of degree* 3. *There is a one-to-one correspondence between nonzero elements of $H^1(k, \mathrm{Pic}\,\overline{X})[2]$ and G_k-stable double-sixes on $\overline{X}$ with the following three properties:*

(1) *neither of the two skew sixes is itself G_k-stable*
(2) *no opposite pair is G_k-stable*
(3) *no set of three opposite pairs is G_k-stable*

Proof of lemma: Consider a nonzero element c of order 2 in $H^1(k, \overline{P})$. As we have seen, we can assume without loss of generality that $c = c_{x_2}$, or in other words that G_k embeds via the natural map into the subgroup $S_{x_2,2}$ of $W(E_6)$ which fixes x_2 mod $2\overline{P}$. This gives rise to a double-six T_1 which is G_k-invariant, as above. Now we already know that the orbit of the ordered pair (e_1, e_2) under $S_{x_2,2}$ consists of pairs of skew exceptional curves in T_1 whose sum is congruent to $e_1 + e_2 \bmod 2\overline{P}$. The only possible sums satisfying this requirement are

$$e_1 + e_2,\ g_1 + g_2,\ f_{1j} + f_{2j}\,(3 \leq j \leq 6).$$

So the orbit of (e_1, e_2) under $S_{x_2,2}$ has at most 12 elements, consisting of (e_1, e_2), (g_1, g_2), (f_{2j}, f_{1j}) $(3 \leq j \leq 6)$, and the other six pairs resulting from switching coordinates. But since $W(E_6)$ acts transitively on ordered pairs of skew lines, all 12 of these elements lie in the orbit.

For each of the six given ordered pairs (x, y) above, the difference $x - y$ is the same in $\overline{P}$. It follows from this that the orbit of $e_1 - e_2$ under the action of $S_{x_2,2}$ consists of only two elements, $e_1 - e_2$ and its negative; moreover, the stabilizer of $e_1 - e_2$ is an index-2 subgroup which equals the stabilizer of (either of) the sixes.

Because we began with a nontrivial element of $H^1(k, \overline{P})[2]$, the image of G_k in $S_{x_2,2}$ cannot be contained in this index-2 subgroup; otherwise there would be an element, namely $e_1 - e_2$, in the class of $x_2 \bmod 2\overline{P}$ which was G_k-stable. So G_k does not stabilize either of the sixes. Moreover, the sum of the classes of an opposite pair is congruent to the difference of those classes mod $2\overline{P}$, which is equal to $\pm(e_1 - e_2)$, so again, since we began with a nontrivial element of $H^1(k, \overline{P})[2]$, this sum cannot be fixed by G_k.

Finally, the sum of three opposite pairs is congruent to the difference of those three opposite pairs mod $2\overline{P}$, which is equal to

$$\pm(e_1 - e_2) \pm (e_1 - e_2) \pm (e_1 - e_2),$$

(the $\pm$ are independent of each other), which is congruent to $e_1 - e_2 \bmod 2\overline{P}$, and again it follows that this sum cannot be fixed by G_k.

For the converse, assume that there is a G_k-stable double-six with the requisite properties. Then it is clear that the difference between the two classes of an opposite pair gives rise to an element of $H^1(k, \operatorname{Pic}\overline{X})[2]$; it is harder, however, to show that this element is nonzero. Here we will need to use MAGMA.

The stabilizer of a double-six in $W(E_6)$ has index 36, because each skew six determines a unique double-six and $W(E_6)$ acts transitively on skew sixes (cf. [11], Proposition V.4.10), and there are

$$\frac{27 \cdot 16 \cdot 10 \cdot 6 \cdot 2 \cdot 1}{6!} = 72$$

skew sixes, hence 36 double-sixes.

We call this stabilizer H_{1440} (it is a conjugate of the group $S_{x_2,2}$), and use the MAGMA command `SubgroupLattice` to produce the full list of conjugacy classes of subgroups of H_{1440}, together with poset relations determined by inclusion (i.e. $C_1 \leq C_2$ if and only if there is a subgroup in class C_1 contained in a subgroup in class C_2). There are 194 classes of subgroups of H_{1440}.

Then, we compute $H^1(H, \overline{P})$ for representative subgroups H of each class, and search for classes C such that $H^1(H, \overline{P}) = 0$ for a representative H of C, and there is no class $C' > C$ such that $H^1(H', \overline{P}) = 0$ for a representative H' of C'. We find that there are three classes of subgroups with this property, so that any subgroup of H_{1440} with trivial H^1 is contained in a subgroup in one of these three classes. Then we compute the vectors in $\overline{P}$ which are fixed by these classes, and discover that the classes are the classes of

(1) the stabilizer of one of the sixes in the fixed double-six
(2) the stabilizer of an opposite pair

(3) the stabilizer of a set of three opposite pairs

This completes the proof. (The MAGMA code used to make this computation, as well as the output of the computation, can be found in Algorithm A.1.1 of [8].) □

Remark 3.9. In [20], Swinnerton-Dyer asserts that condition (1) alone is sufficient for a double-six to give rise to a nontrivial element of $H^1(k, \operatorname{Pic} \overline{X})[2]$, but this is false: certainly, if the image of $G_k \hookrightarrow W(E_6)$ equals the stabilizer of a set $\{E_1, E_2\}$ of two skew exceptional curves, then the double-six T_1 constructed above is fixed by G_k, and condition (1) is satisfied, but in fact it is easy to see that $H^1(k, \operatorname{Pic} \overline{X}) = 0$, because we may blow down $\{E_1, E_2\}$ over k (by Proposition 2.1(g)) to get a Del Pezzo surface Y of degree 5, for which it is known that $H^1(k, \operatorname{Pic} \overline{Y}) = 0$; and now Theorem 23.3 of [14] implies that $H^1(k, \operatorname{Pic} \overline{X}) = 0$ as well.

A similar analysis works for $m = 3$. There is a different configuration of lines corresponding to these elements.

Definition 3.10. A *nine* on a Del Pezzo surface X of degree 3 is a set consisting of three skew curves together with the six curves intersecting exactly two of those three. A *triple-nine* on a Del Pezzo surface X of degree 3 is a partition of the 27 exceptional curves on X into three nines.

Lemma 3.11. *Let X be a Del Pezzo surface of degree* 3*. There is a one-to-one correspondence between nontrivial elements of $H^1(k, \operatorname{Pic} \overline{X})[3]$ and triple-nines on $\overline{X}$ satisfying the condition that each nine is G_k-stable, but no set of three skew lines in any nine is itself G_k-stable.*

Proof of lemma: There are more elements in $(\mathbb{Z}/3\mathbb{Z})^7$ than in $(\mathbb{Z}/2\mathbb{Z})^7$, but the process is the same: we split $(\mathbb{Z}/3\mathbb{Z})^7$ into $W(E_6)$-orbits, and consider only one representative from each orbit (we will see below that this process can be streamlined).

There are 20 orbits under the action of $W(E_6)$; here we give a representative for each, and its size.

(1) $0, 1$
(2) $\pi, 1$
(3) $2\pi, 1$
(4) $\mu, 72$
(5) $\pi + \mu, 72$
(6) $2\pi + \mu, 72$
(7) $e_1, 27$
(8) $\pi + e_1, 27$
(9) $2\pi + e_1, 27$
(10) $2e_1, 27$
(11) $\pi + 2e_1, 27$
(12) $2\pi + 2e_1, 27$
(13) $\mu - 2e_1, 216$
(14) $\pi + \mu - 2e_1, 216$
(15) $2\pi + \mu - 2e_1, 216$
(16) $2\mu - e_1, 216$
(17) $\pi + 2\mu - e_1, 216$

(18) $2\pi + 2\mu - e_1, 216$
(19) $f_{12} - e_2, 270$
(20) $e_1 + e_2 + e_3, 240$

If two elements are related by adding multiples of π or multiplying by 2, then the stabilizer of one element equals the stabilizer of the other, so we are reduced to considering stabilizers of representatives of orbits $\#1, 4, 7, 13, 19$, and 20.

Since 0 does not give rise to a nontrivial element of $H^1(k, \overline{P})[3]$, we are reduced to considering the five elements μ, e_1, $\mu - 2e_1$, $f_{12} - e_2$, and $e_1 + e_2 + e_3$. (Again, the computations done in this argument are all essentially done "by hand" in [20].) We will now show that only the last of these five elements can give a nontrivial element of order 3, by showing that the other four elements satisfy the implication $x \in (\overline{P}/3\overline{P})^H \Rightarrow x \in \overline{P}^H$, for $H \subseteq W(E_6)$.

Before we begin, it will be helpful to introduce the following notation: if we are considering an element $\beta \in (\overline{P}/3\overline{P})^H$, then $\mathcal{E}_r(\beta)$ will denote the set of exceptional curves whose intersection with (a lift of) β is congruent to r mod 3. The set $\mathcal{E}_r(\beta)$ must be fixed by H.

Suppose $\mu \in (\overline{P}/3\overline{P})^H$. Then $\mathcal{E}_0(\mu) = \{E_1, \dots, E_6\}$, so $e_1 + \cdots + e_6 \in \overline{P}^H$. Thus $3\mu = e_1 + \cdots + e_6 - \pi \in \overline{P}^H$, so $\mu \in \overline{P}^H$.

Suppose $e_1 \in (\overline{P}/3\overline{P})^H$. From the description of the classes of the 27 exceptional curves, we see that none of them are congruent to e_1 mod 3, so we must have $e_1 \in \overline{P}^H$.

Suppose $\mu - 2e_1 \in (\overline{P}/3\overline{P})^H$. Then

$$\mathcal{E}_2(\mu - 2e_1) = \{E_1, G_1, F_{12}, F_{13}, \dots, F_{16}\}.$$

Since E_1 and G_1 are the only curves which intersect five of the other curves in $\mathcal{E}_2(\mu - 2e_1)$, the set $\{E_1, G_1\}$ is fixed by H; so $e_1 + g_1 \in \overline{P}^H$, whence $\mu - 2e_1 = \pi - (e_1 + g_1) \in \overline{P}^H$.

Suppose $f_{12} - e_2 \in (\overline{P}/3\overline{P})^H$. Then

$$\mathcal{E}_1(f_{12} - e_2) = \{F_{12}, G_2, E_1, F_{34}, F_{35}, F_{36}, F_{45}, F_{46}, F_{56}\}.$$

Since F_{12} is the only curve which intersects eight of the curves in the above set, we must have $f_{12} \in \overline{P}^H$. Similarly, looking at $\mathcal{E}_2(f_{12} - e_2)$, we find that $e_2 \in \overline{P}^H$. So the difference is in $\overline{P}^H$ as well.

The only element left to consider is $e_1 + e_2 + e_3$. If this lies in $(\overline{P}/3\overline{P})^{G_k}$, then the sets $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2$ form a triple-nine with each nine G_k-stable, and if $e_1 + e_2 + e_3 \in \overline{P}^{G_k}$, the corresponding element of $H^1(k, \overline{P})[3]$ is trivial; so if we assume that $e_1 + e_2 + e_3$ gives rise to a nontrivial element of $H^1(k, \overline{P})[3]$, the set $\{E_1, E_2, E_3\}$ cannot be G_k-stable. Moreover, let $x = e_1 + e_2 + e_3$; then it is not hard to check that the sum of any three skew lines in any nine is congruent mod $3\overline{P}$ to one of the following possibilities:

$$x, \pi - x, -\pi - x, -\pi + x, -x, \pi + x.$$

Since none of these elements can be G_k-stable by the nontriviality assumption on x, no set of three skew lines in a nine can be G_k-stable.

For the converse, we must again examine subgroups of $W(E_6)$ in MAGMA. To determine the index of the simultaneous stabilizer of the three nines in a given triple-nine, we reason as follows: a nine is determined by a skew triple, of which there are $\frac{27 \cdot 16 \cdot 10}{3!} = 720$. We could have chosen any of 6 skew triples in a given nine, so there are actually 120 nines. Any nine gives rise to exactly one triple-nine, so there are 40 triple-nines. So the stabilizer of a triple-nine has index 40, but it permutes the three nines inside the triple-nine in any of 3! ways, so the simultaneous stabilizer of the three nines has index 240, and hence order 216.

This is a subgroup H_{216} with the property that any subgroup $H \subset W(E_6)$ such that $H^1(H, \overline{P})[3] \neq 0$ must be contained in a conjugate of H_{216}, so again we employ the `SubgroupLattice` command in MAGMA to enumerate its subgroups (there are 162 conjugacy classes of subgroups). Searching again for the classes of subgroups which are maximal with respect to the property $H^1(H, \overline{P}) = 0$, we find three classes, and searching for fixed elements of $\overline{P}$, we find that each class is the class of a stabilizer of three skew lines in a nine. Since any subgroup with trivial H^1 is contained in one of these, the condition that the subgroup not fix three skew lines in a nine is sufficient to ensure that the element of $H^1(H, \overline{P})[3]$ corresponding to the sum of three skew lines in a nine is nontrivial. (Again, see Algorithm A.1.3 of [8] for the MAGMA code.) □

Remark 3.12. This lemma appears in [20] as stated, but to prove the "if" direction, Swinnerton-Dyer simply asserts that a triple-nine with the given properties must give rise to an element of order 3 in $H^1(k, \overline{P})$. As in the order-2 case, the nontriviality of this element is certainly not clear without looking explicitly at the subgroups of the stabilizer of a triple-nine, as we did above using MAGMA.

Swinnerton-Dyer carries out the rest of the analysis for $d = 3$ by using Lemmas 3.8 and 3.11 to rule out the existence of elements of order 4, 6, or 9, and to restrict the number of elements of order 2 or 3 that can occur. For details, see [20]. The analogous computations for $d = 2$ and $d = 1$ will require significant computer assistance; but this approach is still more fruitful than the naive approach of enumerating the subgroups of $W(E_r)$ and computing the cohomology of each, because analogues of Lemmas 3.8 and 3.11 will be very helpful when we attempt to say more about the actual computation of the Brauer-Manin obstruction in later sections.

4. The main classification theorem

For the cases $d = 2$ and $d = 1$, we will try to preserve the flavor of the clever manipulations with the sets $\mathcal{E}_r$ employed in the proofs of the last section, but we will have to rely more heavily on MAGMA to carry out the various orbit and stabilizer computations that arise.

Theorem 4.1. *Let X/k be a Del Pezzo surface of degree d. Then $H^1(k, \operatorname{Pic} \overline{X})$ is isomorphic to one of the following groups:*

$5 \leq d \leq 9$: $\{1\}$

$d = 4$: $\{1\}, \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2$

$d = 3$: *any of the above groups, or* $\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2$

$d = 2$: *any of the above groups, or* $(\mathbb{Z}/2\mathbb{Z})^s$ $(3 \leq s \leq 6)$,
$\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(0 \leq t \leq 2)$, $(\mathbb{Z}/4\mathbb{Z})^2$

$d = 1$: *any of the above groups, or* $(\mathbb{Z}/2\mathbb{Z})^7, (\mathbb{Z}/2\mathbb{Z})^8, (\mathbb{Z}/3\mathbb{Z})^s (s = 3, 4)$,
$\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^s$ $(s = 3, 4)$, $(\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(t = 1, 2)$, $\mathbb{Z}/5\mathbb{Z}, (\mathbb{Z}/5\mathbb{Z})^2$,
$\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/6\mathbb{Z})^2$

Proof of theorem: All but $d = 2$ and $d = 1$ have been done already. First we tackle $d = 2$. Before we begin, let us fix our notation for the 56 exceptional curves on $\overline{X}$. With respect to the standard basis $\{\mu, e_1, \ldots, e_7\}$, we have the following list of their classes, again using Proposition 2.1(e):

- 7 classes e_i, $1 \leq i \leq 7$
- 21 classes $f_{jk} = \mu - e_i - e_j$, $1 \leq j < k \leq 7$
- 21 classes $g_{jk} = \pi - f_{jk}$, $1 \leq j < k \leq 7$
- 7 classes $h_i = \pi - e_i$, $1 \leq i \leq 7$

As before, the curves corresponding to these classes are denoted E_i, F_{jk}, G_{jk}, H_i, respectively.

Step 1: $H^1(H, \overline{P})[5] = H^1(H, \overline{P})[7] = 0$ for all $H \subseteq W(E_7)$.

This follows from Shapiro's lemma, just as it did for $m = 3$. See [14], Theorem 29.3.

Step 2: A description of the $x \in \overline{P}/2\overline{P}$ that can give rise to nontrivial elements of $H^1(H, \overline{P})[2]$.

As with $d = 3$, we can reduce to the study of the elements $x_\ell = \sum_{i=1}^{\ell} x_i$, for $1 \leq \ell \leq 7$. And an easy computation shows that x_1, x_5 are conjugate mod 2, as well as $x_2, \pi + x_4, x_6$ and x_3, x_7. (For example, e_1 is conjugate to g_{67}, which is congruent to x_5 mod $2\overline{P}$. And $e_1 + e_2 + e_3$ is conjugate to $e_1 + e_2 + g_{12}$, which is congruent to x_7. The other facts are proved similarly.)

Since, as before, no exceptional curve is congruent mod $2\overline{P}$ to x_1, it cannot give rise to a nontrivial element of $H^1(H, \overline{P})[2]$. But x_2 and x_3 both can, and they are not in the same $W(E_7)$-orbit mod $2\overline{P}$, or even mod $\mathbb{Z}\pi + 2\overline{P}$. We will explore this situation in more detail later in this paper; for now, we will simply note that this is different from the case $d = 3$, when there was only one orbit of elements mod $\mathbb{Z}\pi + 2\overline{P}$ that gave rise to nontrivial elements of $H^1(H, \overline{P})[2]$.

Step 3: A description of the $x \in \overline{P}/3\overline{P}$ that can give rise to nontrivial elements of $H^1(H, \overline{P})[3]$.

This is not necessary for computing $H^1(H, \overline{P})[3]$ in general, because the possible 3-torsion groups that arise are the same as the possible 3-torsion groups for $d = 3$; this is because the Sylow 3-subgroups of $W(E_7)$ are Sylow 3-subgroups of some copy of $W(E_6)$ contained in $W(E_7)$, because the index $[W(E_7)\colon W(E_6)] = 56$ is not divisible by 3. However, this description will still be useful for our examination of elements of order 6. Again, we make a list of orbits of $(\mathbb{Z}/3\mathbb{Z})^8$ under the action of $W(E_7)$. This time, there are 18, which split up into six groups of 3:

(1) Orbits of 0, π, 2π: 1 element each
(2) Orbits of e_1, $\pi + e_1$, $2\pi + e_1$: 56 elements each
(3) Orbits of $e_1 - e_2$, $\pi + e_1 - e_2$, $2\pi + e_1 - e_2$: 126 elements each
(4) Orbits of $e_1 - e_2 + e_3$, $\pi + e_1 - e_2 + e_3$, $2\pi + e_1 - e_2 + e_3$: 576 elements each
(5) Orbits of $e_1 + e_2 + e_3$, $\pi + e_1 + e_2 + e_3$, $2\pi + e_1 + e_2 + e_3$: 672 elements each
(6) Orbits of $e_1 + e_2$, $\pi + e_1 + e_2$, $2\pi + e_1 + e_2$: 756 elements each

Once again, we rule out elements from all but the fifth set of orbits by showing that, for the elements x in the above list of orbit representatives, the implication $x \in (\overline{P}/3\overline{P})^H \Rightarrow x \in \overline{P}^H$ holds for any subgroup $H \subseteq W(E_7)$. It suffices to prove this for $x = 0, e_1, e_1 - e_2, e_1 - e_2 + e_3$, and $e_1 + e_2$.

This is immediate for 0 and e_1 (no exceptional curve is congruent mod $3\overline{P}$ to e_1, except e_1 itself). Suppose now that $e_1 - e_2$ is fixed mod $3\overline{P}$ by $H \subseteq W(E_7)$. The set $\mathcal{E}_1(e_1 - e_2)$ of exceptional curves whose intersection with $e_1 - e_2$ is 1 mod 3 equals

$$\{E_2, H_1, F_{1j}, G_{2j} \colon 3 \le j \le 7\}.$$

Summing the classes of these curves in $\overline{P}$ gives $6\pi - 6(e_1 - e_2)$, which is fixed by H, so $e_1 - e_2$ is fixed by H.

Now suppose $e_1 - e_2 + e_3$ is fixed mod $3\overline{P}$ by H. Summing the classes of the 21 elements in $\mathcal{E}_0(e_1 - e_2 + e_3)$ gives $9\pi + 3(e_1 - e_2 + e_3)$, which is fixed by H, so $e_1 - e_2 + e_3$ is fixed by H.

Now suppose $e_1 + e_2$ is fixed mod $3\overline{P}$ by H. Summing the classes of the 18 elements in $\mathcal{E}_0(e_1 + e_2)$ gives $6\pi + 4(e_1 + e_2)$, which is fixed by H, so $e_1 + e_2$ is fixed by H.

So there is only one orbit of elements mod $\mathbb{Z}\pi + 3\overline{P}$ that can possibly give rise to a nontrivial element of $H^1(k, \overline{P})[3]$, that of $e_1 + e_2 + e_3$.

Step 4: $H^1(H, \overline{P})$ has no elements of order 6, for all $H \subseteq W(E_7)$.

Any element of order 6 must come from a nontrivial element of $\frac{(\overline{P}/6\overline{P})^H}{\overline{P}^H/6\overline{P}^H}$. Furthermore, by Remark 3.2, reducing a representative mod 3 multiplies the corresponding cocycle by 2, so the reduction must be a nontrivial element of $\frac{(\overline{P}/3\overline{P})^H}{\overline{P}^H/3\overline{P}^H}$.

So instead of breaking $(\mathbb{Z}/6\mathbb{Z})^8$ into $W(E_7)$-orbits (there are 237), we may simply look at elements of $(\mathbb{Z}/6\mathbb{Z})^8$ which give $(0, 1, 1, 1, 0, 0, 0, 0) \in (\mathbb{Z}/3\mathbb{Z})^8$ when reduced mod 3; there are 2^8 such elements, but only 14 distinct $W(E_7)$-orbits containing these. So, for representatives x of each of these 14 orbits, we are reduced to the following computation: Given $x \in (\mathbb{Z}/6\mathbb{Z})^8$, compute the stabilizer $S_{x,6}$ of x in $W(E_7)$. Then compute the submodule M_x of $\mathbb{Z}^8$ consisting of vectors fixed by $S_{x,6}$. If $M_x/6M_x \subseteq (\mathbb{Z}/6\mathbb{Z})^8$ contains x or $3x$, then it follows that x has order 1 or 3 in

$$\frac{(\overline{P}/6\overline{P})^{S_{x,6}}}{\overline{P}^{S_{x,6}}/6\overline{P}^{S_{x,6}}} \cong H^1(S_{x,6}, \mathbb{Z}^8)[6]$$

and so for any subgroup $H \subseteq S_{x,6}$, it must also be the case that x induces an element of order strictly less than 6 in $H^1(H, \mathbb{Z}^8)[6]$, since the restriction map $H^1(S_{x,6}, \mathbb{Z}^8)[6] \to H^1(H, \mathbb{Z}^8)[6]$ cannot send an element of order less than 6 to an element of order 6.

Now we list the results of the computation for these 14 orbits. The left vectors are all in $(\mathbb{Z}/6\mathbb{Z})^8$. The vectors on the right are lifts of x or $3x$ in $\mathbb{Z}^8$.

$$
\begin{aligned}
&x = (0,4,4,4,0,0,0,0)\colon 3x \text{ lifts to } 0 \in M_x\\
&x = (3,1,1,1,3,3,3,3)\colon 3x \text{ lifts to } 3\pi \in M_x\\
&x = (3,1,4,4,3,3,3,3)\colon x \text{ lifts to } (9,-5,-2,-2,-3,-3,-3,-3) \in M_x\\
&x = (0,1,1,4,0,0,0,0)\colon x \text{ lifts to } (0,1,1,-2,0,0,0,0) \in M_x\\
&x = (0,1,1,1,0,0,0,0)\colon x \text{ lifts to } (0,1,1,1,0,0,0,0) \in M_x\\
&x = (3,1,1,1,0,0,0,3)\colon x \text{ lifts to } (3,-1,-1,-1,0,0,0,-3) \in M_x\\
&x = (3,1,1,1,0,0,0,0)\colon 3x \text{ lifts to } (9,-3,-3,-3,0,0,0,0) \in M_x\\
&x = (0,1,1,1,3,0,0,0)\colon x \text{ lifts to } (0,1,1,1,-3,0,0,0) \in M_x\\
&x = (0,1,4,4,3,3,3,3)\colon x \text{ lifts to } (0,1,4,4,-3,-3,-3,-3) \in M_x\\
&x = (0,1,4,4,0,0,0,0)\colon x \text{ lifts to } (0,1,4,4,0,0,0,0) \in M_x\\
&x = (0,1,1,1,3,3,0,0)\colon 3x \text{ lifts to } (-6,3,3,3,3,3,0,0) \in M_x\\
&x = (0,1,4,4,3,0,0,0)\colon x \text{ lifts to } (0,1,-2,-2,3,0,0,0) \in M_x\\
&x = (0,1,1,4,3,3,0,0)\colon x \text{ lifts to } (-6,1,1,4,3,3,0,0) \in M_x\\
&x = (0,1,1,4,3,0,0,0)\colon x \text{ lifts to } (0,1,1,-2,3,0,0,0) \in M_x
\end{aligned}
$$

This completes the proof that there are no elements of order 6.

Step 5: Determination of the 2-primary part of $H^1(H,\overline{P})$ in general.

This is the last step for $d = 2$, since the previous steps imply that $H^1(H,\overline{P})$ is either a 2-group or a 3-group, and we know that the only possible 3-groups are $\mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z})^2$.

First, we know that $H^1(H,\overline{P})[2]$ is a quotient A/B, where A is a subgroup of $(\overline{P}/2\overline{P})$, which is itself isomorphic to $(\mathbb{Z}/2\mathbb{Z})^8$; and B always contains the nontrivial element $\pi \in \overline{P}^H/2\overline{P}^H$. Also, A is a proper subgroup, because the only element that fixes $\overline{P}$ mod 2 is the identity element (proof: no exceptional curve is congruent mod $2\overline{P}$ to any other, so any such element must fix every exceptional curve, hence equals the identity.) Since this implies that the $\mathbb{F}_2$-rank of $H^1(H,\overline{P})[2]$ is at most 6, the only possible 2-torsion groups that can occur are $(\mathbb{Z}/2\mathbb{Z})^i$, $0 \le i \le 6$. All of these are already contained in the list given in the statement of the theorem.

Finally, we examine elements of order 4. The technique is similar to that of Step 4: without loss of generality, we can assume that our element of order 4 must either be congruent mod 2 to $(0,1,1,0,0,0,0,0)$ or $(0,1,1,1,0,0,0,0)$, and there are of course 2^8 elements of each type. There are exactly 17 distinct $W(E_7)$-orbits containing these (9 of the first type, 8 of the second type). For a representative x of each orbit, we check, as in Step 4, whether or not x or $2x$ lifts to an element in M_x (notation as in Step 4).

$$x=(0,1,3,0,0,0,0,0)\colon x \text{ lifts to } (0,1,-1,0,0,0,0,0)\in M_x$$
$$x=(2,1,3,2,2,2,2,2)\colon x \text{ lifts to } (-6,1,3,2,2,2,2,2)\in M_x$$
$$x=(0,1,1,0,0,0,0,0)\colon x \text{ lifts to } (0,1,1,0,0,0,0,0)\in M_x$$
$$x=(0,3,3,0,0,0,0,0)\colon x \text{ lifts to } (0,3,3,0,0,0,0,0)\in M_x$$
$$x=(0,1,1,2,2,2,0,0)\colon x \text{ lifts to } (0,1,1,-2,-2,-2,4,4)\in M_x$$
$$x=(0,1,1,2,0,0,0,0)\colon x \text{ lifts to } (0,1,1,-2,0,0,0,0)\in M_x$$
$$x=(0,1,1,2,2,0,0,0)\colon M_x=\mathbb{Z}\pi$$
$$x=(0,1,3,2,2,0,0,0)\colon 2x \text{ lifts to } (0,2,-2,0,0,0,0,0)\in M_x$$
$$x=(0,1,3,2,0,0,0,0)\colon x \text{ lifts to } (0,1,-1,2,0,0,0,0)\in M_x$$

$$x=(0,1,1,3,0,0,0,0)\colon x \text{ lifts to } (0,1,1,-1,0,0,0,0)\in M_x$$
$$x=(0,1,3,3,0,0,0,0)\colon x \text{ lifts to } (0,1,-1,-1,0,0,0,0)\in M_x$$
$$x=(2,1,1,1,0,0,0,0)\colon x \text{ lifts to } (-2,1,1,1,0,0,0,0)\in M_x$$
$$x=(2,3,3,3,0,0,0,0)\colon x \text{ lifts to } (2,-1,-1,-1,0,0,0)\in M_x$$
$$x=(0,1,1,1,0,0,0,0)\colon x \text{ lifts to } (0,1,1,1,0,0,0,0)\in M_x$$
$$x=(0,3,3,3,0,0,0,0)\colon x \text{ lifts to } (0,3,3,3,0,0,0,0)\in M_x$$
$$x=(0,1,1,1,2,0,0,0)\colon x \text{ lifts to } (0,1,1,1,-2,0,0,0)\in M_x$$
$$x=(0,3,3,3,2,0,0,0)\colon x \text{ lifts to } (0,-1,-1,-1,2,0,0,0)\in M_x$$

So any element of order 4 must come from the orbit of $(0,1,1,2,2,0,0,0)$ in $(\mathbb{Z}/4\mathbb{Z})^8$. In other words, if $H^1(H,\overline{P})$ contains an element of order 4, then H is contained in a conjugate of H_4, where H_4 is the stabilizer of $(0,1,1,2,2,0,0,0)\in(\mathbb{Z}/4\mathbb{Z})^8$. MAGMA gives $|H_4|=1152$. This group is small enough that MAGMA can actually carry out the computation of its subgroups' cohomology directly.

Since two conjugate subgroups have isomorphic cohomology groups, we need only find the conjugacy classes of subgroups of H_4 (or its Sylow 2-subgroup). The `Subgroups` command in MAGMA cannot be used on matrix groups; but we avoid this problem by constructing a permutation representation of H_4 via its action on the 56 exceptional curves. We find that there are 1371 different conjugacy classes of subgroups of H_4, and computing the cohomology of each is straightforward using the `CohomologyModule` package in MAGMA. The entire list is:

$$(\mathbb{Z}/2\mathbb{Z})^i(0\le i\le 3), \mathbb{Z}/4\mathbb{Z}\oplus(\mathbb{Z}/2\mathbb{Z})^j(0\le j\le 2), (\mathbb{Z}/4\mathbb{Z})^2.$$

The last four groups in this list are therefore the only groups which can occur with an element of order 4. So our list is complete. (Note that this implies that there can be no elements of order 8.)

Remark 4.2. A similar approach to that used on elements of order 4 allows us to show that the subgroups $(\mathbb{Z}/2\mathbb{Z})^s$, $3\le s\le 6$, all actually occur as cohomology groups $H^1(H,\mathbb{Z}^8)$ for some subgroup $H\subseteq W(E_7)$. If we let K be the intersection of the mod-2 stabilizers of e_1+e_2

and $e_1 + e_3$, MAGMA shows that $|K| = 1440$, with 194 conjugacy classes of subgroups, and running through their cohomology groups gives $\{1\}$ and $(\mathbb{Z}/2\mathbb{Z})^i$, $2 \le i \le 6$.

We now go on to the proof of the theorem in the most general case, $d = 1$. Again, we divide the proof into several steps. (From now on, H will denote a subgroup of $W(E_8)$.)

Step 1: $H^1(H, \overline{P})[7] = 0$; determination of the 5-primary part of $H^1(H, \overline{P})$.

The vanishing of the 7-torsion is part of Theorem 29.3 of [14]. On the other hand, the Sylow 5-subgroups of $W(E_8)$ have order 25; the full list of cohomology groups for the eight subgroups of such a group is $(\mathbb{Z}/5\mathbb{Z})^i$, $0 \le i \le 2$.

Step 2: A description of the $x \in \overline{P}/2\overline{P}$ that can give rise to nontrivial elements of $H^1(H, \overline{P})[2]$.

Again, we reduce to $x_\ell = \sum_{i=1}^{\ell} e_i$. We see quickly that x_1, x_5, $\pi + x_2$, and $\pi + x_6$ are all conjugate mod 2, while x_3, x_7, $\pi + x_4$, $\pi + x_8$ are also all conjugate mod 2. So there are two orbits mod $\mathbb{Z}\pi + 2\overline{P}$ which give rise to a nontrivial element of $H^1(H, \overline{P})[2]$.

Step 3: A description of the $x \in \overline{P}/3\overline{P}$ that can give rise to nontrivial elements of $H^1(H, \overline{P})[3]$.

$(\mathbb{Z}/3\mathbb{Z})^9$ breaks up into 15 orbits under $W(E_8)$, which decompose into 5 sets of 3 orbits each:

- orbits of 0, π, 2π: 1 element each
- orbits of e_1, $\pi + e_1$, $2\pi + e_1$: 240 elements each
- orbits of $e_1 + e_2 + e_3 + e_4$, $\pi + e_1 + e_2 + e_3 + e_4$, $2\pi + e_1 + e_2 + e_3 + e_4$: 1920 elements each
- orbits of $e_1 + e_2 - e_3$, $\pi + e_1 + e_2 - e_3$, $2\pi + e_1 + e_2 - e_3$: 2160 elements each
- orbits of $e_1 + e_2$, $\pi + e_1 + e_2$, $2\pi + e_1 + e_2$: 2240 elements each

Again, we check for nontriviality in each case. The first case clearly gives rise to a trivial element of $H^1(H, \overline{P})[3]$, as does the second one (again, there are no exceptional curves other than e_1 whose class is congruent to e_1 mod $3\overline{P}$). The mod-3 stabilizer of $e_1 + e_2 - e_3$ actually fixes $e_1 + e_2 - e_3$ outright, so this cannot give rise to a nontrivial element of $H^1(H, \overline{P})[3]$.

So this leaves two cases, both of which can give nontrivial elements: if $x \in \overline{P}$ gives rise to a nontrivial element of $H^1(k, \overline{P})[3]$, then x is congruent mod $\mathbb{Z}\pi + 3\overline{P}$ to $x_2 = e_1 + e_2$ or $x_4 = e_1 + e_2 + e_3 + e_4$.

Step 4: The proof that there are no elements of order 10, 12, or 15, and the determination of $H^1(H, \overline{P})[6]$.

Suppose that $H^1(H, \overline{P})[2] \ne 0$. By Step 2, we may assume without loss of generality that H is a subgroup of the stabilizer of e_1 or $e_1 + e_2 + e_3$ mod $2\overline{P}$. This in turn implies that the Sylow 5-subgroup H_5 of H injects into the Sylow 5-subgroup of one of these two stabilizers. However, a quick computation with MAGMA shows that the Sylow 5-subgroups of these two stabilizers have order 5 and trivial H^1. So any subgroup of either of these Sylow 5-subgroups has trivial H^1 (since there are only two subgroups, the whole group and the trivial group). Therefore $H^1(H, \overline{P})[5] = 1$ by Lemma 3.5. This implies that there are no elements of order 10.

Suppose that $H^1(H, \overline{P})[3] \ne 0$. By Step 3, we may assume without loss of generality that H lies in the stabilizer of $e_1 + e_2$ or $e_1 + e_2 + e_3 + e_4$ mod $3\overline{P}$. And again, the Sylow

5-subgroup H_5 of H injects into the Sylow 5-subgroup of one of these two stabilizers. As in the previous paragraph, a computation with MAGMA shows that the Sylow 5-subgroups of these two stabilizers have order 5 and trivial H^1. This implies that $H^1(H, \overline{P})[5] = 1$ by Lemma 3.5, so there are no elements of order 15.

Finally, suppose that $H^1(H, \overline{P})$ contains an element of order 6. We may assume without loss of generality that it comes from an element $x \in \overline{P}/6\overline{P}$ which is congruent mod $3\overline{P}$ to either $(0, 1, 1, 0, 0, 0, 0, 0, 0)$ or $(0, 1, 1, 1, 1, 0, 0, 0, 0)$. There are 12 conjugacy classes of elements of the first type, and 10 of elements of the second type. For a representative x of each orbit, we check whether some small multiple of x lifts to an element in M_x, the submodule of $\mathbb{Z}^9$ consisting of vectors fixed by the mod-6 stabilizer $S_{x,6}$ of x.

$x = (0, 4, 4, 0, 0, 0, 0, 0, 0)$: $3x$ lifts to $0 \in M_x$

$x = (3, 1, 1, 3, 3, 3, 3, 3, 3)$: $3x$ lifts to $3\pi \in M_x$

$x = (0, 1, 4, 0, 0, 0, 0, 0, 0)$: x lifts to $(0, 1, -2, 0, 0, 0, 0, 0, 0) \in M_x$

$x = (3, 4, 1, 3, 3, 3, 3, 3, 3)$: x lifts to $(9, -2, -5, -3, -3, -3, -3, -3, -3) \in M_x$

$x = (0, 1, 1, 3, 0, 0, 0, 0, 0)$: x lifts to $(0, 1, 1, -3, 0, 0, 0, 0, 0) \in M_x$

$x = (3, 4, 4, 0, 3, 3, 3, 3, 3)$: x lifts to $(9, -2, -2, -6, -3, -3, -3, -3, -3) \in M_x$

$x = (0, 4, 4, 3, 3, 0, 0, 0, 0)$: $M_x = \mathbb{Z}\pi$

$x = (3, 1, 1, 0, 0, 3, 3, 3, 3)$: $M_x = \mathbb{Z}\pi$

$x = (3, 4, 4, 3, 3, 0, 0, 0, 0)$: x lifts to $(3, 4, 4, -3, -3, 0, 0, 0, 0) \in M_x$

$x = (0, 1, 1, 0, 0, 3, 3, 3, 3)$: x lifts to $(12, 1, 1, -6, -6, -3, -3, -3, -3) \in M_x$

$x = (0, 1, 4, 3, 3, 0, 0, 0, 0)$: $2x$ lifts to $(0, 2, -4, 0, 0, 0, 0, 0, 0) \in M_x$

$x = (3, 4, 1, 0, 0, 3, 3, 3, 3)$: $2x$ lifts to $(0, 2, -4, 0, 0, 0, 0, 0, 0) \in M_x$

$x = (0, 4, 4, 4, 4, 0, 0, 0, 0)$: $3x$ lifts to $0 \in M_x$

$x = (3, 1, 1, 1, 1, 3, 3, 3, 3)$: $3x$ lifts to $3\pi \in M_x$

$x = (0, 1, 1, 1, 4, 0, 0, 0, 0)$: x lifts to $(0, 1, 1, 1, -2, 0, 0, 0, 0) \in M_x$

$x = (3, 4, 4, 4, 1, 3, 3, 3, 3)$: x lifts to $(9, -2, -2, -2, -13, -3, -3, -3) \in M_x$

$x = (0, 1, 1, 4, 4, 0, 0, 0, 0)$: x lifts to $(0, 1, 1, -2, -2, 0, 0, 0, 0) \in M_x$

$x = (3, 4, 4, 1, 1, 3, 3, 3, 3)$: x lifts to $(9, -2, -2, -5, -5, -3, -3, -3, -3) \in M_x$

$x = (0, 1, 1, 1, 1, 3, 3, 0, 0)$: $3x$ lifts to $(-6, 3, 3, 3, 3, 3, 3, 0, 0) \in M_x$

$x = (3, 4, 4, 4, 4, 0, 0, 3, 3)$: $3x$ lifts to $(3, 0, 0, 0, 0, 0, 0, -3, -3) \in M_x$

$x = (0, 1, 1, 1, 4, 3, 0, 0, 0)$: x lifts to $(0, 1, 1, 1, -2, -3, 0, 0, 0) \in M_x$

$x = (3, 4, 4, 4, 1, 0, 3, 3, 3)$: x lifts to $(9, -2, -2, -2, -5, -6, -3, -3, -3) \in M_x$

Notice that the orbits come in pairs with representatives x and $3\pi + x$. So the only orbit mod $\mathbb{Z}\pi + 6\overline{P}$ of an element in $\overline{P}$ that gives rise to an element in $H^1(H, \overline{P})$ of order 6 is the orbit of $x = (0, 4, 4, 3, 3, 0, 0, 0, 0)$. The mod-6 stabilizer $S_{x,6}$ of this element has order 8640. This has 1924 conjugacy classes of subgroups, and we can compute the cohomology of each of them quickly in MAGMA. The resulting list is:

$$1, (\mathbb{Z}/2\mathbb{Z}), (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z}), (\mathbb{Z}/3\mathbb{Z})^2, (\mathbb{Z}/6\mathbb{Z}), (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}), (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}), (\mathbb{Z}/6\mathbb{Z})^2$$

So the last four groups are the only possibilities for an $H^1(H, \overline{P})$ with an element of order 6. (Note that this implies that there are no elements of order 12.)

Step 5: Determination of the 3-primary part of $H^1(H, \overline{P})$ in general.

By Step 3, any H such that $H^1(H, \overline{P})[3] \neq 0$ is contained in a subgroup conjugate to either the mod-3 stabilizer of $(0, 1, 1, 0, 0, 0, 0, 0, 0)$ or the mod-3 stabilizer of $(0, 1, 1, 1, 1, 0, 0, 0, 0)$. The Sylow 3-subgroups of these two groups have orders 243 and 81, respectively, so it suffices to compute the cohomology of the subgroups of these. We find that the only possibilities are $(\mathbb{Z}/3\mathbb{Z})^s$, $0 \leq s \leq 4$. (Note that this implies that there are never any elements of order 9.)

Step 6: Determination of the 2-primary part of $H^1(H, \overline{P})$ in general.

This is the last step, because we have enumerated all the possibilities for $H^1(H, \overline{P})$ when it is not a 2-group. Unfortunately, the Sylow 2-subgroups arising from Step 2 are not quite small enough for MAGMA to easily list all their subgroups, as we did for the Sylow 3-subgroups (there are two Sylow 2-subgroups to consider, of orders 2^{11} and 2^{14}, respectively). So we will proceed as we did for $d = 2$; to reduce the size of H and its Sylow subgroups, we suppose first that there is an element of order 4 in $H^1(H, \overline{P})$.

We may assume that this element reduces mod 2 to $(0, 1, 0, 0, 0, 0, 0, 0, 0)$ or $(0, 1, 1, 1, 0, 0, 0, 0, 0)$. There are 512 elements of each type, and these split into 8 and 6 orbits, respectively. As usual, we investigate representatives of each orbit:

$$x = (0, 1, 0, 0, 0, 0, 0, 0, 0)\colon x \text{ lifts to } (0, 1, 0, 0, 0, 0, 0, 0, 0) \in M_x$$
$$x = (2, 3, 2, 2, 2, 2, 2, 2, 2)\colon x \text{ lifts to } (6, -1, -2, -2, -2, -2, -2, -2, -2) \in M_x$$
$$x = (0, 1, 2, 2, 2, 2, 2, 0, 0)\colon x \text{ lifts to } (0, 1, -2, -2, -2, -2, -2, 4, 4) \in M_x$$
$$x = (2, 3, 0, 0, 0, 0, 0, 2, 2)\colon x \text{ lifts to } (6, -1, -4, -4, -4, -4, -4, 2, 2) \in M_x$$
$$x = (0, 3, 2, 2, 2, 0, 0, 0, 0)\colon M_x = \mathbb{Z}\pi$$
$$x = (2, 1, 0, 0, 0, 2, 2, 2, 2)\colon M_x = \mathbb{Z}\pi$$
$$x = (0, 3, 2, 2, 2, 2, 0, 0, 0)\colon 2x \text{ lifts to } (0, 2, 0, 0, 0, 0, 0, 0, 0) \in M_x$$
$$x = (2, 1, 0, 0, 0, 0, 2, 2, 2)\colon 2x \text{ lifts to } (6, 0, -2, -2, -2, -2, -2, -2, -2) \in M_x$$

$$x = (0, 1, 3, 1, 0, 0, 0, 0, 0)\colon x \text{ lifts to } (0, 1, -1, 1, 0, 0, 0, 0, 0) \in M_x$$
$$x = (2, 3, 1, 3, 0, 0, 0, 0, 0)\colon x \text{ lifts to } (6, -1, -3, -1, -2, -2, -2, -2, -2) \in M_x$$
$$x = (0, 1, 1, 1, 2, 2, 0, 0, 0)\colon M_x = \mathbb{Z}\pi$$
$$x = (2, 3, 3, 3, 0, 0, 2, 2, 2)\colon M_x = \mathbb{Z}\pi$$
$$x = (0, 1, 1, 1, 2, 2, 2, 0, 0)\colon x \text{ lifts to } (0, 1, 1, 1, -2, -2, -2, 4, 4) \in M_x$$
$$x = (2, 3, 3, 3, 0, 0, 0, 2, 2)\colon x \text{ lifts to } (6, -1, -1, -1, -4, -4, -4, 2, 2) \in M_x$$

So if there is an element of order 4 in $H^1(H, \overline{P})$, H must be contained in a group conjugate to either the mod-4 stabilizer of $(0, 3, 2, 2, 2, 0, 0, 0, 0)$ or $(0, 1, 1, 1, 2, 2, 0, 0, 0)$. These groups have orders 80640 and 46080, which is still rather large; however, in fact it is easier for MAGMA to compute their subgroups than it is to compute those of their Sylow 2-subgroups. The first group has 1291 conjugacy classes of subgroups, while the second has 12395. Running through the cohomology groups of their subgroups yields the following list:

$$(\mathbb{Z}/2\mathbb{Z})^i (0 \le i \le 4), \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^j (0 \le j \le 4), (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^k (0 \le k \le 2).$$

So these are the only possibilities containing an element of order 4.

Finally, for the elementary 2-groups, we note that the maximum $\mathbb{F}_2$-rank of an elementary 2-group that can appear is $9 - 1 = 8$, because $H^1(H, \overline{P})[2]$ is a quotient of an elementary 2-group of rank at most 9 by an elementary 2-group of rank at least 1. (It is not hard to see that this maximum is attained when $H = Z(W(E_8))$.) This completes the proof. ■

Remark 4.3. It is proved in [20] that a Del Pezzo surface of degree 3 with $H^1(k, \operatorname{Pic} \overline{X})[2] \neq 0$ satisfies the Hasse principle. Analogously, we might suspect that a Del Pezzo surface X of degree 2 with $H^1(k, \operatorname{Pic} \overline{X})[3] \neq 0$ satisfies the Hasse principle. If we tried to prove this, we would begin by supposing that $X(\mathbb{A}_k) \neq 0$. Then, the assumption on the 3-torsion implies that we can assume that G_k fixes $e_1 + e_2 + e_3$ mod 3, by Step 3 of the case $d = 2$ of the above proof, and then G_k must fix the set

$$\begin{aligned}\mathcal{E}_2(e_1 + e_2 + e_3) = &\{E_1, F_{23}, G_{14}, G_{15}, G_{16}, G_{17}\} \cup \{E_2, F_{13}, G_{24}, G_{25}, G_{26}, G_{27}\} \\ &\cup \{E_3, F_{12}, G_{34}, G_{35}, G_{36}, G_{37}\},\end{aligned}$$

so that each of the three sets of six skew exceptional curves in $\mathcal{E}_2(e_1 + e_2 + e_3)$ is defined over some cubic extension. Let L be the cubic extension over which the first set of skew exceptional curves is defined. Note that there is a birational morphism from X_L to a Del Pezzo surface Y of degree 8 over L, by blowing down the six skew lines. Since X_L has local points everywhere, so does Y, and hence $Y(L) \neq \emptyset$ because the Hasse principle holds for Y. Thus $X(L) \neq \emptyset$, by the Lang-Nishimura theorem ([17]). But it is not clear whether this implies that $X(k) \neq \emptyset$. (The analogous statement for cubic surfaces–that if a cubic surface has a point over a quadratic extension of k, it has a k-point–is well-known.)

In fact, there is a Del Pezzo surface X over $\mathbb{Q}$ of degree 2 which has points everywhere locally and points on a cubic extension of $\mathbb{Q}$, but no $\mathbb{Q}$-rational points. The surface X is given by the equation $w^2 = 34(x^4 + y^4 + z^4)$. See Example 9.4. However, this surface has no 3-torsion in $H^1(k, \operatorname{Pic} \overline{X})$, which in this case is isomorphic to $(\mathbb{Z}/2)^3$.

Question 4.4. Is there a Del Pezzo surface of degree 2 over a number field k with $X(\mathbb{A}_k) \neq \emptyset$, $X(L) \neq \emptyset$ for some extension L/k of degree 3, $X(k) = \emptyset$, and $H^1(k, \operatorname{Pic} \overline{X})[3] \neq 0$?

Question 4.5. Is there a Del Pezzo surface of degree 2 with a nontrivial Brauer-Manin obstruction coming from an element of order 3 in $(\operatorname{Br} X)/(\operatorname{Br} k)$?

What we have shown is that a negative answer to Question 4.4 would imply a negative answer to Question 4.5.

5. Geometry of Del Pezzo surfaces of degree 2

Let X be a smooth Del Pezzo surface of degree 2 over an algebraically closed field of characteristic $\neq 2$. From Proposition 2.1(f), we know that the anticanonical map $X \to \mathbb{P}^2$ has degree 2. It is a fact (see [9], p. 67 or [14], p. 142) that it gives a double cover of $\mathbb{P}^2$ ramified precisely above a nonsingular quartic, which gives rise to the following equation for X:

$$w^2 = F(x, y, z) \tag{2}$$

where F is a homogeneous polynomial of degree 4. This equation should be understood as representing a surface in weighted projective space $\mathbb{P}(2,1,1,1)$.

The smooth plane quartic C cut out by F has 28 bitangents (lines in $\mathbb{P}^2$ whose intersection with the quartic is 2 times a divisor of degree 2). The 56 exceptional curves on X are precisely the preimages of these bitangents under the anticanonical map; they come in pairs Y_1, Y_2 such that the class of the divisor $Y_1 + Y_2$ is the anticanonical class π. Thus, the geometry of X is intimately related to the geometry of C, which we now review. Our primary reference is [10], Chapter 6.

Let K_C be a canonical divisor of C. The intersection of a bitangent with C is linearly equivalent to C, but this intersection divisor equals $2(P+Q)$, where P and Q are the points of intersection. Thus each bitangent gives rise to a divisor class $\theta = P+Q$ in $\operatorname{Pic} C$ satisfying $2\theta = K_C$. Elements of $\operatorname{Pic} C$ satisfying this equation are called *theta characteristics*. These have been studied extensively in the literature. In fact, the usual proof that C has 28 bitangents uses various properties of theta characteristics, as in [10], Theorem 6.1.1. It will suffice for our purposes to note that different bitangents give rise to different theta characteristics: if $P+Q$ and $P'+Q'$ are linearly equivalent, then $P+Q+P'+Q'$ is a canonical divisor, which must be cut out by a line; and the only way that the four points P, Q, P', Q' can be collinear is if their respective bitangents coincide.

Proposition 5.1. *Given a set of four bitangents to C cut out by lines L_i, $i = 1,2,3,4$, the following conditions are equivalent:*

1. *There is a conic whose intersection with C is exactly the eight points where the bitangents intersect C (with multiplicities)*
2. *The sum of the four theta characteristics corresponding to the four bitangents, as above, equals twice the canonical class*
3. *If $\theta_1, \theta_2, \theta_3, \theta_4$ are the four theta characteristics corresponding to the bitangents, numbered in any order, then $\theta_1 - \theta_2 = \theta_3 - \theta_4$*
4. *C is the zero set of the quartic polynomial*

$$R^2 - L_1 L_2 L_3 L_4$$

for some quadratic polynomial R

Proof: (1) $\Rightarrow$ (2) is immediate, because the intersection divisor of a conic is linearly equivalent to $2K_C$. To see (2) $\Rightarrow$ (4), let R be a quadratic polynomial cutting out a conic whose intersection divisor with C equals the sum of the four divisors corresponding to the four bitangents. Then the rational function $R^2/L_1L_2L_3L_4$ has zero divisor, so it is a constant. Since we are over an algebraically closed field, we can assume that the constant is 1 by absorbing constants into R (but when we begin to work over number fields in the next section, we will have to worry much more about constants). Because its degree is 4, the polynomial $R^2 - L_1L_2L_3L_4$ must cut out C precisely.

(4) $\Rightarrow$ (1) is immediate. And to see (2) $\Leftrightarrow$ (3), simply notice that the equations $\theta_1 + \theta_2 + \theta_3 + \theta_4 = 2K_C$ and $\theta_1 - \theta_2 - \theta_3 + \theta_4 = 0$ in $\operatorname{Pic} C$ are equivalent, by subtracting or adding the identity $2\theta_2 + 2\theta_3 = 2K_C$. $\square$

A set of four bitangents satisfying the equivalent conditions of the lemma is called a *syzygetic tetrad* on C.

Proposition 5.2. *Given a syzygetic tetrad and a choice of an exceptional curve D_1 lying over one of the bitangents in the tetrad, we can choose exceptional curves D_2, D_3, D_4 lying over each of the other three bitangents, such that $D_1 - D_2 = D_3 - D_4$ in $\operatorname{Pic}^0(X)$. Conversely, given D_i satisfying this equation, the corresponding bitangents form a syzygetic tetrad if they are distinct.*

Proof: Choose D_2 and D_3 so that they do not intersect D_1, and D_4 so that it does. This is always possible: if D_i and D_i' are the two exceptional curves lying over a bitangent, then $(D_1, D_i + D_i') = (D_1, \pi) = 1$, so one of the intersections is 0 and the other is 1.

We can make this explicit: Suppose the syzygetic tetrad is given by lines cut out by L_1, L_2, L_3, L_4. If R is the conic given by Proposition 5.1, then the two exceptional curves lying over the bitangent $L_i = 0$ are given by the equations $w = \pm R, L_i = 0$. Without loss of generality, assume that D_1 is given by $w = R, L_1 = 0$. Then our choice of D_2 is given by $w = -R, L_2 = 0$. D_3 is given by $w = -R, L_3 = 0$, and D_4 is given by $w = R, L_4 = 0$.

Now, the divisor of the rational function

$$\frac{(w-R)L_1L_4}{(w+R)L_2L_3}$$

is

$$\begin{aligned}(D_1 + D_2' + D_3' + D_4) + (D_1 + D_1') + (D_4 + D_4')\\ - (D_1' + D_2 + D_3 + D_4') - (D_2 + D_2') - (D_3 + D_3') = 2(D_1 + D_4 - D_2 - D_3)\end{aligned}$$

so that the class of this element is 0 in $\operatorname{Pic} X$. But $\operatorname{Pic} X$ is torsion-free, so the class $D_1 + D_4 - D_2 - D_3$ must be 0 in $\operatorname{Pic} X$.

For the converse, view C as embedded in X via $w = 0$ and assume $D_1 - D_2 = D_3 - D_4$ in $\operatorname{Pic} X$. Note that $D_i \cap C = D_i' \cap C$, so

$$2(D_i \cap C) = (D_i + D_i') \cap C = L_i \cap C = 2B_i,$$

where the B_i are the degree-2 divisors corresponding to the L_i. This holds in $\operatorname{Div} C$, so we can halve both sides to get $D_i \cap C = B_i$. The natural map $\operatorname{Pic} X \to \operatorname{Pic} C$ sends the class of D_i to the class of $D_i \cap C$, so since the class of $D_1 - D_2 - D_3 + D_4$ is 0 in $\operatorname{Pic}(X)$, the class of its image, which is $B_1 - B_2 - B_3 + B_4$, is 0 in $\operatorname{Pic}(C)$. This is precisely condition (3) of Proposition 5.1. □

Let T_C be the set of 28 bitangents to C. Define a map $d\colon T_C \times T_C \to \operatorname{Pic}^0(C)[2]$ by $d(L, L') = \theta_L - \theta_{L'}$, where the θ's are the theta characteristics corresponding to the L's. Then $d^{-1}(0)$ is just the diagonal of $T_C \times T_C$, because different bitangents give rise to different theta characteristics.

Since d is symmetric, it induces a map

$$d' \colon \left\{ \begin{matrix} \text{unordered pairs of} \\ \text{distinct elements of } T_C \end{matrix} \right\} \to \operatorname{Pic}^0(C)[2] \setminus \{0\}.$$

Following [10], we define a *Steiner complex* to be the union of pairs in $(d')^{-1}(c)$, for some fixed $c \in \operatorname{Pic}^0(C)[2] \setminus \{0\}$. Suppose two pairs are in the same Steiner complex; this is equivalent to the fact that the four bitangents in the two pairs form a syzygetic tetrad, by condition (3) of Proposition 5.1.

Note also that $\mathrm{Pic}^0(C)[2]$ is isomorphic to $(\mathbb{Z}/2)^6$ as an abelian group ([11], B.5). So the map d' sends a set of cardinality 378 to a set of cardinality 63. Consider a pair in the domain of d'. Without loss of generality, we may assume that the pair lies under the exceptional curves with classes e_1 and e_2. Proposition 5.2 implies that the Steiner complex containing this pair consists of the pairs of bitangents lying under exceptional curves whose classes d_1 and d_2 satisfy $e_1 - e_2 = d_1 - d_2$.

It is not hard to list the possibilities for the d_i; in fact, we have already given this list above. Either the pair d_1, d_2 equals e_1, e_2, h_2, h_1, or f_{2j}, f_{1j} or g_{1j}, g_{2j} for $3 \leq j \leq 7$. There are precisely six pairs of bitangents lying under these twelve pairs of exceptional curves. So d' is six-to-one—this also implies that it is surjective. So we have proved

Proposition 5.3. *There are* 63 *Steiner complexes of pairs of bitangents, each containing* 6 *pairs, which correspond bijectively to elements of* $\mathrm{Pic}^0(C)[2] \setminus \{0\}$ *via the map* d'.

6. Quaternion algebras in $\mathrm{Br}\, X$ and elements of the first type

6.1. **Cyclic algebras.** We have not yet related our results about $H^1(k, \overline{P})$ to the construction of nonconstant elements of $\mathrm{Br}\, X$. Here we recall the definition of cyclic algebras and give a simple criterion for a cyclic $k(X)$-algebra to come from a nonconstant element of $\mathrm{Br}\, X$.

Definition 6.1. Let L/K be a cyclic extension of fields of degree n, with Galois group generated by σ. Given $c \in K^*$, we define the central simple K-algebra $(L/K, c)$ as follows: take the L-vector space with basis $\{1, x, \ldots, x^{n-1}\}$, with multiplication given by the rules

$$x^n = c$$
$$x\ell = (\sigma\ell)x$$

for all $\ell \in L$. (Though the notation does not indicate it, $(L/K, c)$ depends also on the choice of generator σ.)

Remark 6.2. Let X be a K-variety, L/K a finite cyclic extension, and $f \in k(X)$. Then the cyclic algebra $(k(X_L)/k(X), f)$ is often written as $(L/K, f)$; this makes sense because the Galois groups of the respective extensions are isomorphic.

Remark 6.3. The natural map $\mathrm{Br}\, X \to \mathrm{Br}\, k(X)$ is injective when X is a regular integral quasi-compact scheme (cf. [16], III.2.22), so we can view elements of $\mathrm{Br}\, X$ as elements of $\mathrm{Br}\, k(X)$ which "specialize nicely."

Proposition 6.4. *Let X be a smooth geometrically integral K-variety, L/K a finite cyclic extension, and $f \in k(X)$. Then the class of the algebra $(L/K, f)$ in* $\mathrm{Br}\, k(X)$ *comes from an element of* $\mathrm{Br}\, X$ *if and only if $(f) = N_{L/K}(D)$ for some divisor $D \in \mathrm{Div}\, X_L$. Furthermore, if $X(\mathbb{A}_K) \neq \emptyset$, the class of this algebra comes from* $\mathrm{Br}\, K$ *if and only if we can take D to be a principal divisor.*

For the proof, we refer the reader to [8], Proposition 2.2.3 or [2], Proposition 4.17. (The author knows of no published proof of this "standard" result.)

6.2. **Determinantal representations,** $\mathrm{Pic}^0(\overline{C})$**, and** $H^1(k, \mathrm{Pic}\, \overline{X})$**.** In this section, we will study degree-2 Del Pezzo surfaces X over a number field k whose equations are written in the form

$$w^2 = A_2^2 - A_1 A_3, \tag{3}$$

where the A_i are quadratic homogeneous polynomials in x, y, z, such that the right side of (3) is actually defined over k. As we have seen above (condition (4) of Proposition 5.1), any Del Pezzo surface of degree 2 over k can be written in the form (3), if we allow the A_i to have coefficients in $\overline{k}$. For our purposes, however, we want the A_i to be defined over a field extension which is as close to k as possible.

Note that (3) can be written as $-w^2 = \det A$, where A is the symmetric matrix

$$\begin{pmatrix} A_1 & A_2 \\ A_2 & A_3 \end{pmatrix}$$

So the following result about such a "determinantal representation" will be the key to our investigation:

Proposition 6.5. *Let C be a nonsingular quartic curve in $\mathbb{P}^2_k$, and let S_C be the set of symmetric 2×2 matrices with entries which are homogeneous quadratic polynomials in x, y, z (whose coefficients are in $\overline{k}$), such that $\overline{C}$ is the zero set of $\det A$. For $M, M' \in S_C$, say that $M \equiv M'$ if there exist $E, E' \in GL_2(\overline{k})$ such that $M' = EME'$. Then there is a G_k-equivariant bijection between* $\operatorname{Pic}^0(\overline{C})[2] \setminus \{0\}$ *and the set $S_C/\equiv$.*

Proof of proposition: Everything but the statement about the G_k-action is taken from Theorem 6.2.2 in [10]. The central idea is due to Coble, and comes from a more general correspondence, which we outline here. Let $K = K_{\overline{C}}$. For any nonzero $\alpha \in \operatorname{Pic}^0(\overline{C})$, there is a map

$$f\colon |K+\alpha| \times |K-\alpha| \to |2K|$$

defined by $f(D, D') = D + D'$. Note that $\ell(K+\alpha) = \ell(K-\alpha) = 2$ by Riemann-Roch. So $|K+\alpha|$ and $|K-\alpha|$ have the natural structure of a $\mathbb{P}^1$. Then the corresponding map on global sections, which is bilinear by construction, is given by

$$\begin{array}{rcl} g\colon H^0(\overline{C}, \mathcal{L}(K+\alpha)) \times H^0(\overline{C}, \mathcal{L}(K-\alpha)) & \to & H^0(\overline{C}, \mathcal{L}(2K)) \\ ((\lambda,\mu),(\lambda',\mu')) & \mapsto & \lambda\lambda' M_{11} + \lambda\mu' M_{12} + \lambda'\mu M_{21} + \lambda'\mu' M_{22} \end{array}$$

for certain sections M_{ij}, by bilinearity. The M_{ij} can be viewed uniquely as homogeneous quadratic polynomials in x, y, z. Let M be the 2×2 matrix of the M_{ij}. It is not hard to show (see [10], Theorem 6.2.1) that this gives a bijection between $\operatorname{Pic}^0(\overline{C}) \setminus \{0\}$ and $R_C/\equiv$, where R_C is defined exactly the same as S_C, except that we do not require the matrices to be symmetric.

Now note that if we consider $\alpha \in \operatorname{Pic}^0(\overline{C})[2]$, the linear systems $|K+\alpha|$ and $|K-\alpha|$ are the same, so if we restrict our attention to symmetric maps f and g, we get a correspondence between 2-torsion elements α and symmetric matrices M, with the same equivalence relation.

It should be clear from the explanation of this construction that it respects the action of G_k on both sides. ■

Now we return to an examination of elements of order 2 in $H^1(k, \operatorname{Pic}\overline{X})$. From the work we did in previous sections, any element in

$$H^1(k, \operatorname{Pic}\overline{X})[2] \cong \frac{(\overline{P}/2\overline{P})^{G_k}}{P/2P}$$

comes from an element of $\overline{P}$ in the same $W(E_7)$-orbit as $x_2 = e_1 + e_2$ or $x_3 = e_1 + e_2 + e_3$.

Definition 6.6. Elements of $H^1(k, \overline{P})[2]$ coming from an element in the orbit of x_2 will be called *(2-torsion) elements of the first type*; elements coming from an element in the orbit of x_3 will be called *elements of the second type.* (Of course, a 2-torsion element can be both of the first type and of the second type.)

Remark 6.7. Elements of the second type are more difficult to understand than elements of the first type. The mod-2 stabilizer of x_3 inside $W(E_7)$ has index 72 and is isomorphic to S_8, which has no useful index-2 subgroups. For our purposes, a useful index-2 subgroup H would be one with the property that $\overline{P}^H$ contains a lift of x_3; Proposition 6.4 implies that this is a necessary condition for there to be a cyclic quaternion algebra corresponding to the element of the second type. Unfortunately, it can be checked that $\overline{P}^{A_8} = \mathbb{Z}\pi$. On the other hand, the situation is better for elements of the first type; the mod-2 stabilizer of x_2 inside $W(E_7)$ has index 63 and an useful index-2 subgroup, as we will see. We will also see that the reappearance of the number 63 is not a coincidence.

Proposition 6.8. *If c is an element of the first type, there is an extension N_c of k, with $[N_c : k] \leq 2$, such that c is in the kernel of the restriction map $H^1(k, \operatorname{Pic} \overline{X}) \to H^1(N_c, \operatorname{Pic} \overline{X})$. The field N_c is the field of definition of the difference between two skew exceptional curves in $\operatorname{Pic} \overline{X}$.*

Proof of proposition: Suppose c is an element of the first type. Without loss of generality, we can assume that c corresponds to the class of $x_2 = e_1 + e_2 \in (\overline{P}/2\overline{P})^{G_k}$, or, in other words, the action of G_k on the exceptional curves gives a map $G_k \to H_{63} \subset W(E_7)$, where H_{63} is the subgroup of index 63 stabilizing $e_1 + e_2$ mod 2. We have already seen that $\sigma(e_1 - e_2) = \pm(e_1 - e_2)$ for any $\sigma \in H_{63}$, so H_{63} has a subgroup H_{126} of index 2, namely the stabilizer of $e_1 - e_2 \in \overline{P}$. (It can be checked that $\overline{P}^{H_{63}} = \mathbb{Z}\pi$.) Now if the image of G_k lies inside the subgroup H_{126}, then $c = 0$, because if $e_1 - e_2 \in P$, then x_2 gives rise to the zero element in $\frac{(\overline{P}/2\overline{P})^{G_k}}{P/2P}$. So the fixed field N_c of $G_k \cap H_{126}$ is quadratic if $c \neq 0$, and in any case it is the field of definition of the difference $e_1 - e_2$, so restriction to N_c kills c. ■

Remark 6.9. From now on, when we refer to N_c, we will refer to the N_c constructed in the proof of the proposition. Obviously, if $N_c = k$, then $c = 0$. But the converse is not necessarily true, as we will see.

6.3. **Elements of the first type and Steiner complexes.** The following theorem is, as promised, an analogue of Lemmas 3.8 and 3.11. Like those lemmas, it relates a (particular type of) nonconstant element of the Brauer group to a certain G_k-invariant configuration of exceptional curves on $\overline{X}$.

Theorem 6.10. *Let X be a Del Pezzo surface of degree 2 over a field k, isomorphic to a double cover of $\mathbb{P}^2$ ramified over a quartic curve C. There is a one-to-one correspondence between nonzero 2-torsion elements of $H^1(k, \operatorname{Pic} \overline{X})$ of the first type and Steiner complexes on $\overline{C}$ defined over k which have the property that the action of G_k on the 24 exceptional curves over the complex satisfies four nontriviality conditions C_2, C_{12}, C_{32}, C_{160} (which are given explicitly in the proof).*

Proof of theorem: Let c be an element of order 2 in $H^1(k, \operatorname{Pic} \overline{X})$. We may assume that c comes from the element $x_2 = e_1 + e_2$ in $(\overline{P}/2\overline{P})^{G_k}$. In this case, there are 24 exceptional curves whose divisor classes have odd intersection with $e_1 - e_2$. If $E = E_1$ and $F = E_2$, then these 24 curves are $E_1, E_2, H_1, H_2, F_{ij}, G_{ij}$, where $1 \le i \le 2$ and $3 \le j \le 7$. (As usual, $W(E_7)$ acts transitively on pairs of skew exceptional curves, so indeed we do not lose any generality by supposing c comes from x_2 and not one of its $W(E_7)$-conjugates.)

These exceptional curves lie over 12 bitangents, which form a Steiner complex. Because G_k preserves intersections, this Steiner complex is fixed by G_k. Conversely, it is easy to see that the construction is completely reversible–a Steiner complex defined over k gives rise to an element of $H^1(k, \overline{P})[2]$. However, we require MAGMA to see what conditions we need to impose on this Steiner complex to make the corresponding element nonzero.

Given a Steiner complex on $\overline{C}$, define an *opposite pair* on $\overline{X}$ to be a pair of skew exceptional curves lying over one of the six pairs of bitangents that comprise the Steiner complex. So there are two opposite pairs lying over each pair of bitangents. For example, if we consider the Steiner complex T consisting of the bitangents lying under

$$E_1, E_2, F_{13}, F_{23}, F_{14}, F_{24}, \ldots, F_{17}, F_{27}, \tag{4}$$

then the opposite pairs lying over $\{E_1, E_2\}$ are $\{e_1, e_2\}$ and $\{h_1, h_2\}$, and the opposite pairs lying over $\{F_{1j}, F_{2j}\}$ are $\{f_{1j}, f_{2j}\}$ and $\{g_{1j}, g_{2j}\}$.

Now, we claim that a Steiner complex defined over k gives rise to a nontrivial element of $H^1(k, \overline{P})[2]$ if and only if all four of the following conditions hold:

- C_2**:** the class of the difference $a - b$ is not G_k-invariant, for any opposite pair $\{a, b\}$
- C_{12}**:** the class of the sum $a + b$ is not G_k-invariant, for any opposite pair $\{a, b\}$
- C_{32}**:** (assuming the Steiner complex defined over k is T, and H_T is the stabilizer inside $W(E_7)$ of the set T) the element $(0, 1, 1, -2, 0, 0, 0, 0) \in \operatorname{Pic} \overline{X}$ is not G_k-invariant; nor are any of its H_T-conjugates
- C_{160}**:** there is no way to pick three opposite pairs (a_i, b_i), each lying over different pairs of bitangents, so that the class of $\sum_{i=1}^{3}(a_i + b_i)$ is G_k-invariant

As we have seen, the map $G_k \to W(E_7)$ has image lying inside a certain index-63 subgroup H_{63} in $W(E_7)$. Each condition C_i says that the image cannot lie inside the stabilizer in H_{63} of some divisor class in $\overline{P}$; the number i equals the index of this stabilizer in H_{63}. (If the Steiner complex is T, then $H_{63} = H_T$.)

First we show that the conditions C_i are necessary. First of all, without loss of generality we can take the Steiner complex T of (4); the corresponding element of $H^1(k, \operatorname{Pic} \overline{X})[2]$ is nontrivial if and only if nothing congruent to $e_1 - e_2$ mod $2\overline{P}$ is fixed by G_k. So suppose this element is nontrivial, and we will show that the conditions C_i hold.

First, the difference between any opposite pair is $\pm(e_1 - e_2)$, which is congruent to $e_1 - e_2$ mod $2\overline{P}$, so it cannot be G_k-invariant; this is C_2.

The sum $a + b$ of an opposite pair is $(a - b) + 2b = \pm(e_1 - e_2) + 2b$, which is congruent to $e_1 - e_2$ mod $2\overline{P}$, so it cannot be G_k-invariant; this is C_{12}.

C_{32} is a strange condition, in that there seems to be no convenient "coordinate-free" way to state it in terms of the exceptional curves alone. Nevertheless, an easy MAGMA computation shows that the element $(0, 1, 1, -2, 0, 0, 0, 0)$ has the property that every element in its H_T-orbit is congruent mod $2\overline{P}$ to $e_1 - e_2$. So since none of these elements can be G_k-invariant, we get C_{32}.

Suppose $\sum_{i=1}^{3}(a_i+b_i)$ is G_k-invariant, for a similar choice of three opposite pairs. This is

$$\sum_{i=1}^{3}(a_i-b_i)+2\sum_{i=1}^{3}b_i=\pm(e_1-e_2)\pm(e_1-e_2)\pm(e_1-e_2)+2\sum_{i=1}^{3}b_i$$

(the $\pm$ are independent), so this is congruent to e_1-e_2 mod $2\overline{P}$, so it cannot be G_k-invariant; this is C_{160}.

The proof that these conditions are sufficient is the content of Algorithm A.4.3 of [8], which we outline here. Just as in the proof of Lemmas 3.8 and 3.11, we examine subgroups of H_{63} and find that there are four maximal conjugacy classes of subgroups with respect to the condition $H^1(H,\overline{P})=0$ for subgroups H in the class; these classes are the classes of the stabilizers of the elements indicated in the statements of the conditions C_i. ■

Remark 6.11. Continuing Remark 6.9, we note that condition C_2 is precisely the statement that $[N_c:k]=2$. But condition C_2 is not sufficient to show that $c\neq 0$.

6.4. **Combining our results; the main theorems.** So far, we have described three correspondences:

$$\begin{Bmatrix}\text{elements of } H^1(k,\overline{P})[2]\setminus\{0\}\\ \text{of the first type}\end{Bmatrix} \overset{6.10}{\longleftrightarrow} \begin{Bmatrix}G_k\text{-invariant Steiner complexes}\\ \text{with nontriviality assumptions}\end{Bmatrix}$$
$$\{\text{Steiner complexes}\} \overset{5.3}{\longleftrightarrow} \mathrm{Pic}^0(\overline{C})[2]\setminus\{0\}$$
$$\mathrm{Pic}^0(\overline{C})[2]\setminus\{0\} \overset{6.5}{\longleftrightarrow} S_C/\equiv$$

Recall that if we are given a G_k-invariant Steiner complex, the map given in the first correspondence will send it to an element of $H^1(k,\overline{P})[2]$, but that element will be trivial unless the action of G_k on the set of exceptional curves lying over the complex satisfies the conditions C_i.

Since the latter two correspondences are G_k-equivariant, it follows that a nontrivial element of $H^1(k,\overline{P})[2]$ of the first type gives rise to a G_k-invariant element of $S_C/\equiv$. The natural question to ask is: can we lift this G_k-invariant element of $S_C/\equiv$ to a G_k-invariant element of S_C; and if not, can we lift it to an element of S_C defined over a relatively small extension of k? The following theorem answers this question.

Theorem 6.12. *Suppose X is a Del Pezzo surface of degree 2 over a number field k given by a double cover of $\mathbb{P}^2$ ramified above a (nonsingular) quartic curve C over k. Suppose also that $X(\mathbb{A}_k)\neq\emptyset$. If ω is a G_k-invariant element of $S_C/\equiv$, then it corresponds to an element c of $H^1(k,\overline{P})[2]$ (which may or may not be zero). Then:*

(1) *If $[N_c:k]=2$, ω lifts to an element of the form*

$$B=\begin{pmatrix}B_1 & B_2\\ B_2 & b(\alpha B_1)\end{pmatrix}\in S_C$$

where B_1 is a homogeneous quadratic polynomial in x,y,z with coefficients in N_c, B_2 is a homogeneous quadratic polynomial in x,y,z with coefficients in k, $b\in k$, and α is the nontrivial element of $\mathrm{Gal}(N_c/k)$.

(2) *If $N_c = k$, ω lifts to an element of the form*

$$B = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix} \in S_C$$

with the B_i homogeneous quadratic polynomials defined over k.

In both cases, we may choose the B_i so that the equation of X can be written as $-w^2 = \det B$.

Proof of theorem: For any two matrices A, A' (in $GL_2(\overline{k})$ or in S_C), we will say that $A \sim A'$ if and only if $A = A'a$ for some $a \in \overline{k}^*$. It will be useful to prove the following elementary lemma.

Lemma 6.13. *Let C be a nonsingular quartic curve in $\mathbb{P}^2_k$, and $M = \begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix} \in S_C$.*

(a) The set $\{M_1, M_2, M_3\}$ is linearly independent over $\overline{k}$.
(b) If DMD' is symmetric, for constant invertible matrices D, D', we have $D' \sim D^T$.
(c) If $DMD^T \sim EME^T$, for invertible matrices D, E, then $D \sim E$.

Proof of lemma: For (a), suppose first that M_1 is a $\overline{k}$-linear combination of M_2 and M_3. Then there is a point $P \in C(\overline{k})$ such that $M_2(P) = M_3(P) = 0$ by Bézout's Theorem. Then $M_1(P) = 0$ as well. But this implies that P is a singular point of C, which is a contradiction. The same argument works if we start with M_2 or M_3 being a linear combination of the other two polynomials.

For (b), we are given that $DMD' = D'^T M^T D^T = D'^T M D^T$. So both (b) and (c) reduce to the following claim: If $FMG \sim M$, where F, G are constant invertible matrices, then $F \sim I \sim G$, where I is the identity matrix.

The claim follows from a simple computation, and part (a):

$$\begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix} \sim \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} =$$

$$\begin{pmatrix} aeM_1 + (ag + be)M_2 + bgM_3 & afM_1 + (bf + ah)M_2 + bhM_3 \\ ceM_1 + (cg + de)M_2 + dgM_3 & cfM_1 + (ch + df)M_2 + dhM_3 \end{pmatrix},$$

and now part (a) implies that we can equate coefficients of the M_i, so that $ag + be = bg = af = bh = ce = dg = cf = ch + df = 0$ and $ae = bf + ah = cg + de = dh \neq 0$. Hence a, d, e, h are nonzero; so $b = c = f = g = 0$; so $ae = ah = de = dh$, which implies that $a = d$ and $e = h$. $\square$

The main tool we will use in the rest of the proof of Theorem 6.12 will be nonabelian group cohomology. Pick a lift $M \in S_C$ of ω, normalized so that the equation of X can be written $-w^2 = \det M$. (So $\det M$ has coefficients in k.) Then Lemma 6.13(b) implies that we can write

$$\sigma M = \frac{c_\sigma}{\det D_\sigma} D_\sigma M D_\sigma^T \tag{5}$$

for all $\sigma \in G_k$, where $D_\sigma \in GL_2(\overline{k})$ and $c_\sigma \in \overline{k}$.

Now Lemma 6.13(c) implies that, given M, D_σ is well-defined up to a constant times the identity. Notice also that, taking the determinant of both sides and using the fact that det $\sigma M = \det M$, we must have $c_\sigma = \pm 1$, and the sign is independent of our choice of D_σ. It is also clear that $c_{\sigma\tau} = c_\sigma c_\tau$.

Let N be the fixed field of the subgroup $\{\sigma \in G_k : c_\sigma = 1\}$. Then N is quadratic or equal to k. For now, suppose that N is quadratic, equal to $k(\sqrt{n})$. We will deal with the degenerate case $N = k$ later.

The key observation is that the map $G_k \to PGL_2(\overline{k})$ defined by $\sigma \mapsto D_\sigma$ satisfies the cocycle condition $D_{\sigma\tau} = (\sigma D_\tau)D_\sigma$. (This follows from part (c) of Lemma 6.13.) Here is the outline of the rest of the proof:

Step 1: We define quadratic extensions L and N and find a matrix $M' \equiv M$ such that $\sigma M' = M'$ for all $\sigma \in G_{LN}$. Using inflation-restriction, we show that we have a similar equation to (5) for M', with all matrices defined over LN. Also, $\det M' = \det M$.

Step 2: We use the assumption $X(\mathbb{A}_k) \neq \emptyset$ to show that we can actually find an $M'' \equiv M$ such that $\sigma M'' = M''$ for all $\sigma \in G_N$. Also, $\det M'' = \det M$. We also argue that this is true even when $N = k$, so that the second statement of the theorem is proved (modulo the equality $N = N_c$).

Step 3: We find a matrix defined over N having the form of the matrix in the statement of the theorem which is equivalent to M'' and has the same determinant as M''.

Step 4: We show that $N = N_c$.

It is well-known (see for instance [18], X.5) that elements of the nonabelian cohomology group $H^1(G_k, PGL_2(\overline{k}))$ correspond to isomorphism classes of quaternion algebras over k. So let $Q = H(d, \ell)$ be the quaternion algebra corresponding to our cocycle, where $H(d, \ell)$ is the 4-dimensional central simple algebra over k generated by elements i and j satisfying $i^2 = d$, $j^2 = \ell$, $ij = -ji$. (See [15], p. 111 for more details.) Let $L = k(\sqrt{\ell})$. Then L splits Q, so our cocycle becomes a coboundary when restricted to G_L; that is, there is some matrix $U \in GL_2(\overline{k})$ such that D_τ and $(\tau U)U^{-1}$ differ by a constant for all $\tau \in G_L$. Of course, D_τ was only defined up to a constant multiple anyway, so we can take $D_\tau = (\tau U)U^{-1}$ for all $\tau \in G_L$.

Thus, for $\tau \in G_L$,

$$\begin{aligned} \tau M &= \frac{c_\tau(\det U)}{\tau(\det U)}(\tau U)U^{-1}M(U^{-1})^T(\tau U)^T \\ \tau((\det U)U^{-1}M(U^{-1})^T) &= c_\tau(\det U)U^{-1}M(U^{-1})^T. \end{aligned}$$

Let $M' = (\det U)U^{-1}M(U^{-1})^T$; then $\det M' = \det M$, and $\tau M' = c_\tau M'$. Therefore M' is defined over the fixed field of $\{\tau \in G_L : c_\tau = 1\}$, which is LN. Note also that if we define, for any $\sigma \in G_k$, $E_\sigma = (\sigma U^{-1})D_\sigma U$, then

$$\sigma M' = \frac{c_\sigma}{\det E_\sigma} E_\sigma M' E_\sigma^T,$$

and $\sigma \mapsto E_\sigma$ is still a cocycle $G_k \to PGL_2(\overline{k})$, which is cohomologous to the original cocycle and trivial on G_L. In fact, the same computation shows that even though the definition of D_σ depends on the choice of representative M for ω, the class of $(\sigma \mapsto D_\sigma) \in H^1(k, PGL_2(\overline{k}))$ and the value of c_σ are both independent of this choice.

Lemma 6.14. *For $\beta \in \mathrm{Gal}(LN/k)$, there are unique elements $c_\beta \in \{\pm 1\}$ and $E_\beta \in PGL_2(L)$ such that, for any representative $\tilde{E_\beta}$ of E_β in $GL_2(L)$,*

$$\beta M' = \frac{c_\beta}{\det \tilde{E_\beta}} \tilde{E_\beta} M' \tilde{E_\beta}^T$$

Also, $c_\beta = 1$ if and only if β fixes N, and $E_\beta = 1$ if and only if β fixes L.

Proof of lemma: This is a standard inflation-restriction argument, but it is worth emphasizing the result: once it is proved, we can forget completely about $\overline{k}$ and restrict our attention to LN.

In what follows, we will routinely abuse notation and drop the $\tilde{}$ everywhere; whenever an equation involving matrices contains an element of a PGL_2, it is understood that we are to choose a representative of that element in GL_2, and that it does not matter which representative we choose.

As noted above, the class of the cocycle $\sigma \mapsto E_\sigma$ in $H^1(G_k, PGL_2(\overline{k}))$ restricts to zero in $H^1(G_L, PGL_2(\overline{k}))$; so the inflation-restriction exact sequence implies that it is the inflation of a cocycle in $H^1(\mathrm{Gal}(L/k), PGL_2(\overline{k})^{G_L})$.

Now it is easy to see that $PGL_2(\overline{k})^{G_L} = PGL_2(L)$: from the short exact sequence

$$1 \to \overline{k}^* \to GL_2(\overline{k}) \to PGL_2(\overline{k}) \to 1$$

we get an exact sequence of cohomology

$$H^0(G_L, GL_2(\overline{k})) \to H^0(G_L, PGL_2(\overline{k})) \to H^1(G_L, \overline{k}^*).$$

The first term is just $GL_2(L)$, and the third term is zero by Hilbert's Theorem 90. So the left map is surjective.

So for $\sigma \in G_k$, E_σ can be chosen to be in $PGL_2(L)$, and to take one of two values, depending only on whether or not $\sigma \in G_L$ (by definition, if $\sigma \in G_L$, then $E_\sigma = 1$). By definition, c_σ is 1 if and only if $\sigma \in G_N$. These facts imply the lemma. □

It is clear that the quaternion algebra Q is also the quaternion algebra corresponding to the cocycle $(\delta \mapsto E_\delta)\colon \mathrm{Gal}(LN/N) \cong \mathrm{Gal}(L/k) \to PGL_2(L)$. Now we move on to step 2, showing that N actually splits Q; this is where we will use the assumption about local points on X.

So let α be the nontrivial element of $\mathrm{Gal}(LN/L)$, and let δ be the nontrivial element of $\mathrm{Gal}(LN/N)$. From the lemma, we have

$$\begin{aligned} \delta M' &= \frac{1}{\det E_\delta} E_\delta M' E_\delta^T \\ \alpha M' &= -M' \end{aligned}$$

for some $E_\delta \in PGL_2(L)$.

We claim that the cocycle determined by $\delta \mapsto E_\delta$ is cohomologous to $\delta \mapsto \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$. This is just a consequence of the correspondence between Q and E_δ, which we will now give in detail (see [18], X.5).

The correspondence proceeds as follows: Conjugation by E_δ, as an isomorphism of $M_2(L)$, is equal to $(\delta\varphi)(\varphi^{-1})$ where $\varphi : Q \otimes_k L \to M_2(L)$ is an isomorphism. Further, different isomorphisms give rise to cohomologous E_δ's.

Now let φ be the isomorphism sending

$$\begin{aligned} i &\mapsto \begin{pmatrix} \sqrt{\ell} & 0 \\ 0 & -\sqrt{\ell} \end{pmatrix} \\ j &\mapsto \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} \end{aligned}$$

Then it is easy to check that $(\delta\varphi)(\varphi^{-1})$ is conjugation by $\begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$, which proves the claim.

So write

$$E_\delta = (\delta Z) \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} Z^{-1}$$

for some $Z \in PGL_2(L)$. Pick a representative for Z in $GL_2(L)$ (for clarity, abuse notation and call it Z). Write $M'' = (\det Z) Z^{-1} M' (Z^{-1})^T$. Then $\det M'' = \det M'$ and

$$\begin{aligned} \delta M'' &= (\det \delta Z)(\delta Z^{-1})(\delta M')(\delta Z^{-1})^T \\ &= \frac{\det \delta Z}{\det E_\delta} (\delta Z^{-1}) E_\delta M' E_\delta^T (\delta Z)^T \\ &= \frac{\det \delta Z}{\det E_\delta} \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} Z^{-1} M' (Z^{-1})^T \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} \\ &= \frac{\det \delta Z}{(\det Z)(\det E_\delta)} \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} M'' \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} \\ &= \frac{-1}{d} \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} M'' \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Since α fixes L, we continue to have

$$\alpha M'' = -M''.$$

Finally, consider $M''' = \sqrt{n\ell} M''$. The effect of replacing M'' with M''' in the above two equations is that it eliminates the negative signs (though note that it changes the determinant, which the previous two substitutions did not).

So write $M''' = \begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix}$. Then $\alpha M''' = M'''$, so the M_i are defined over L, and

$$\delta \begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix} = \begin{pmatrix} M_3/d & M_2 \\ M_2 & dM_1 \end{pmatrix}.$$

Then we can write the equation for X as

$$M_2^2 - dM_1(\delta M_1) = M_2^2 - M_1 M_3 = -\det M''' = -n\ell(\det M) = n\ell w^2.$$

By assumption, this has local solutions everywhere. Dividing both sides by w^2, remembering that M_2 is defined over k, and plugging in the local solutions, we obtain local solutions to the equation

$$x^2 - d(y^2 - \ell z^2) = n\ell.$$

Dividing by ℓ and writing $x' = x/\ell$ and $y' = y/\ell$, we obtain local solutions to the equation

$$\ell(x')^2 + dz^2 - d\ell(y')^2 = n. \tag{6}$$

Hence this equation is solvable over k by the Hasse Principle. Let (x_0, y_0, z_0) be a solution. Then $(z_0 i + x_0 j + y_0 ij)^2 = n$ in Q, which shows that N embeds into Q, which is equivalent to N splitting Q ([15], IV.3.7).

Notice that if $N = k$, we can repeat the above arguments with $n = 1$ (omitting the equations involving α), and we obtain local solutions to (6):

$$1 - dz^2 - \ell(x')^2 + d\ell(y')^2 = 0$$

This equation has a solution (x_0, y_0, z_0) by the Hasse principle, which implies that the element $1 + z_0 i + x_0 j + y_0 ij$ has reduced norm 0. This implies that $Q \cong M_2(k)$ ([15], IV.5.1(b)). So then the cocycle $\sigma \mapsto D_\sigma$ was actually a coboundary, which means that we can find a matrix $M' \equiv M$ defined over k with the same determinant as M. (In other words, we could have taken $L = k$ when we were constructing M' in Step 1.) This is the second statement of the conclusion of the theorem, with N in place of N_c.

This completes Step 2.

Step 2 implies that we could have taken $L = N$ in Step 1. If we do this, we obtain a matrix $B' \equiv M$ defined over N with the same determinant as M. And Lemma 6.14 implies that there is a matrix $E_\alpha \in PGL_2(N)$ such that

$$\alpha B' = \frac{-1}{\det E_\alpha} E_\alpha B' E_\alpha^T,$$

where α is the nontrivial element of $\mathrm{Gal}(N/k)$. Then, again by the explicit description of the correspondence between cocycles and quaternion algebras, the cocycle determined by $\alpha \mapsto E_\alpha$ is cohomologous to $\alpha \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$, where b is an element of k chosen so that $H(n, b) \cong H(d, \ell)$. So we find a B'' defined over N with the same determinant as B', such that

$$\alpha B'' = \frac{1}{b} \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} B'' \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

Writing $B'' = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix}$ and expanding $w^2 = -\det B''$ gives exactly the first statement of the conclusion of the theorem, with N in place of N_c. This completes Step 3.

Lemma 6.15. *$N = N_c$.*

Proof of lemma: Without loss of generality, suppose that N_c is the field of definition of $e_1 - e_2 \in \overline{P}$. We would like to show that $c_\sigma = 1$ if and only if $\sigma(e_1 - e_2) = e_1 - e_2$. Let ℓ_1, ℓ_2 be the bitangents over which e_1 and e_2 lie, respectively, and let $\sigma\ell_i = m_i$ for $i = 1, 2$. By Proposition 5.1, there is a homogeneous quadratic polynomial Q such that

$$\begin{pmatrix} \ell_1\ell_2 & Q \\ Q & m_1 m_2 \end{pmatrix}$$

is in S_C. We now claim that it is a representative of ω. This follows naturally from an inspection of the details of the correspondences defined in Proposition 6.5 and Proposition 5.3: Let θ_1, θ_2 be the theta characteristics corresponding to ℓ_1, ℓ_2. Then the element $\epsilon \in \mathrm{Pic}^0(\overline{C})[2]$ corresponding to c is just $\theta_1 - \theta_2$. Similarly let θ_3, θ_4 be the theta characteristics corresponding to m_1, m_2, so that $\theta_1 - \theta_2 = \theta_3 - \theta_4$. Then $\theta_1 + \theta_2, \theta_3 + \theta_4 \in |K + \epsilon|$. So we can take the sections M_{11} and M_{22} of Proposition 6.5 to be the sections cutting out the divisors $2\theta_1 + 2\theta_2$ and $2\theta_3 + 2\theta_4$. Of course, these are just the divisors cut out by $\ell_1\ell_2$ and $m_1 m_2$, so the claim follows.

Since ω is G_k-invariant, we obtain the following formula, where $n_i = \sigma m_i$:

$$\begin{pmatrix} m_1 m_2 & \sigma Q \\ \sigma Q & n_1 n_2 \end{pmatrix} = \frac{c_\sigma}{\det D_\sigma} D_\sigma \begin{pmatrix} \ell_1\ell_2 & Q \\ Q & m_1 m_2 \end{pmatrix} D_\sigma^T \tag{7}$$

for some matrix D_σ. Note that the element c_σ in this formula is equal to the c_σ we defined in the proof of Theorem 6.12, because we have seen that c_σ is independent of the choice of representative mod $\equiv$.

We may as well choose D_σ over $\overline{k}$ so that its determinant is 1. Having done this, let $D_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and consider the upper left entry of the product in (7). It equals

$$c_\sigma(a^2\ell_1\ell_2 + 2abQ + b^2 m_1 m_2).$$

If this is supposed to equal m_1m_2, we must have $a = 0$ and $c_\sigma b^2 = 1$, by Lemma 6.13(a). Looking at the upper right entry of the product (7) gives

$$\sigma Q = c_\sigma(ac\ell_1\ell_2 + (ad + bc)Q + bdm_1m_2) = -c_\sigma Q + c_\sigma bdm_1m_2.$$

Without loss of generality, the exceptional curve representing e_1 is cut out by $\{\ell_1 = 0, w = Q\}$, and the exceptional curve representing e_2 is cut out by $\{\ell_2 = 0, w = -Q\}$. Then the class of $\sigma(e_1 - e_2)$ is represented by

$$\begin{Bmatrix} m_1 = 0 \\ w = \sigma Q \end{Bmatrix} - \begin{Bmatrix} m_2 = 0 \\ w = -\sigma Q \end{Bmatrix} = \begin{Bmatrix} m_1 = 0 \\ w = -c_\sigma Q \end{Bmatrix} - \begin{Bmatrix} m_2 = 0 \\ w = c_\sigma Q \end{Bmatrix}$$

Suppose $c_\sigma = 1$. Then the divisor of the function

$$\frac{(w+Q)m_1\ell_2}{(w-Q)m_2\ell_1}$$

is

$$2\begin{Bmatrix} m_1 = 0 \\ w = -Q \end{Bmatrix} - 2\begin{Bmatrix} m_2 = 0 \\ w = Q \end{Bmatrix} - 2\begin{Bmatrix} \ell_1 = 0 \\ w = Q \end{Bmatrix} + 2\begin{Bmatrix} \ell_2 = 0 \\ w = -Q \end{Bmatrix}$$

(see the proof of Proposition 5.2), so

$$2\sigma(e_1 - e_2) - 2(e_1 - e_2) = 0$$

in $\operatorname{Pic}\overline{X}$, so $\sigma(e_1 - e_2) = e_1 - e_2$ in $\operatorname{Pic}\overline{X}$. If $c_\sigma = -1$, a similar argument with the divisor of $\frac{(w+Q)m_1\ell_1}{(w-Q)m_2\ell_2}$ shows that $\sigma(e_1 - e_2) = -(e_1 - e_2)$ in $\operatorname{Pic}\overline{X}$. This proves the lemma (in case (2) of the theorem, $c_\sigma = 1$ for all $\sigma \in G_k$, so that $e_1 - e_2$ is defined over G_k). □ ■

Here is the point of the previous theorem:

Theorem 6.16. *Let X be a Del Pezzo surface of degree 2 isomorphic to a double cover of $\mathbb{P}^2_k$ ramified over a quartic curve C. Suppose there is a nonzero element $c \in H^1(k, \operatorname{Pic}\overline{X})[2]$ of the first type, and let ω be the corresponding element of $S_C/\equiv$. Let $B = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix}$ be the matrix produced by Theorem 6.12. Then $[N_c : k] = 2$ and c maps to the class of the quaternion Azumaya algebra*

$$(N_c/k, (B_2 - w)/x^2) \in \operatorname{Br} X.$$

Proof: First, we know $[N_c : k] = 2$ because of Remark 6.9. Then, using Theorem 6.12, we can write the equation for X as

$$B_2^2 - w^2 = bB_1(\alpha B_1) \tag{8}$$

where α is the nontrivial element of $\mathrm{Gal}(N_c/k)$. Now consider the divisor of $\frac{B_2-w}{x^2}$ in $\mathrm{Div}\,\overline{X}$. It decomposes as

$$\left(\begin{Bmatrix} w = B_2 \\ B_1 = 0 \end{Bmatrix} - (x)\right) + \left(\begin{Bmatrix} w = B_2 \\ \alpha B_1 = 0 \end{Bmatrix} - (x)\right),$$

so by Proposition 6.4, the algebra $(N_c/k, (B_2 - w)/x^2)$ comes from $\mathrm{Br}\,X$. To show that it corresponds to c, we need to know about the class of the divisor $D(B) := \{w = B_2, B_1 = 0\}$ in $\overline{P}$. What we want will follow from a general lemma:

Lemma 6.17. *Suppose $D(B)$ and $D(B')$ are defined as above, where*

$$-w^2 = \det B = \det B',$$

and further suppose that $B \equiv B'$. Then $D(B)$ and $D(B')$ are linearly equivalent.

Proof of lemma: Fix B, and suppose that $B' = (\det A')^{-1}A'B(A')^T$. Then we consider the map $GL_2(\overline{k}) \to \mathrm{Div}\,\overline{X}$ given by $A \mapsto D((\det A)^{-1}ABA^T)$, or equivalently we consider the corresponding divisor $\mathcal{D}$ on $X \times GL_2(\overline{k}) \subset X \times \mathbb{A}^4$. Then B and B' are pullbacks of this divisor via the natural maps $i = (\mathrm{id}, \{I\})$ and $j = (\mathrm{id}, \{A'\})\colon \overline{X} \to \overline{X} \times GL_2(\overline{k})$.

Now consider the natural map $p^* : \mathrm{Pic}\,\overline{X} \to \mathrm{Pic}(\overline{X} \times GL_2(\overline{k}))$ coming from the projection $\overline{X} \times GL_2(\overline{k}) \to \overline{X}$. It factors as

$$\mathrm{Pic}\,\overline{X} \to \mathrm{Pic}(\overline{X} \times \mathbb{A}^4) \to \mathrm{Pic}(\overline{X} \times GL_2(\overline{k})).$$

The first map is an isomorphism ([11], II.6.6) and the second map is surjective ([11], II.6.5(a)). So p^* is surjective, but notice that we have $i^* \circ p^* = j^* \circ p^* =$ the identity map on $\mathrm{Pic}\,\overline{X}$. This implies that p^* is an isomorphism. Then $i^* = j^*$, so $B = i^*\mathcal{D} = j^*\mathcal{D} = B'$ in $\mathrm{Pic}\,\overline{X}$. □

As we saw in the proof of Lemma 6.8, the matrix B is equivalent to a matrix

$$M = \begin{pmatrix} \ell_1\ell_2 & Q \\ Q & m_1m_2 \end{pmatrix}$$

where ℓ_1 and ℓ_2 are bitangents lying under an opposite pair. The divisor $D(M)$ is just

$$\begin{Bmatrix} w = Q \\ \ell_1 = 0 \end{Bmatrix} + \begin{Bmatrix} w = Q \\ \ell_2 = 0 \end{Bmatrix} = \{\ell_1 = 0\} - \begin{Bmatrix} w = -Q \\ \ell_1 = 0 \end{Bmatrix} + \begin{Bmatrix} w = Q \\ \ell_2 = 0 \end{Bmatrix}$$

but the class of this in $\mathrm{Pic}\,\overline{X}$ is $\pi - (a - b)$, where a, b is an opposite pair lying over ℓ_1, ℓ_2.

So, since the divisor class of (x) is π, we have that

$$((B_2 - w)/x^2) = N_{N_c/k}(D(B) - (x)) = N_{N_c/\mathbb{Q}}(E),$$

where the divisor class of E is $-(a-b)$, but standard Tate cohomology arguments (as in [8], Proposition 2.2.5) show that this algebra maps to the class of c if and only if the divisor class of E is $\frac{1}{2}(\alpha(a-b) - (a-b)) = -(a-b)$, because c comes from the class of $a - b \in (\overline{P}/2\overline{P})^{G_k}$. So we are done. ■

7. Semi-diagonal Del Pezzo surfaces of degree 2

Consider the surface X defined by the following equation:

$$w^2 = Ax^4 + By^4 + Cz^4 + 2Dx^2y^2 + 2Ex^2z^2 + 2Gy^2z^2, \tag{9}$$

where $A, B, C, D, E, G \in k$. We will use the results of the previous section to give a formula for a 2-torsion element of $(\operatorname{Br} X)/(\operatorname{Br} k)$. For lack of a better word, we will call surfaces given by this equation *semi-diagonal* Del Pezzo surfaces of degree 2.

First, assume that $C \neq 0$. Let $A' = A - E^2/C$, $B' = B - G^2/C$, $D' = D - EG/C$, $E' = E/C$, $G' = G/C$. Then we can rewrite our equation as

$$w^2 = A'x^4 + B'y^4 + 2D'x^2y^2 + C(z^2 + E'x^2 + G'y^2)^2,$$

and now let us also assume that $A' \neq 0$ and neither $(D'^2 - A'B')$ nor $(D'^2 - A'B')/C$ is a square in k. Let $m' = D'^2 - A'B'$. We can then rewrite the equation for X as $-w^2 = \det M$, where

$$M = \begin{pmatrix} x^2 + (\frac{D'+\sqrt{m'}}{A'})y^2 & \sqrt{C}(z^2 + E'x^2 + G'y^2) \\ \sqrt{C}(z^2 + E'x^2 + G'y^2) & -A'(x^2 + (\frac{D'-\sqrt{m'}}{A'})y^2) \end{pmatrix}.$$

Since M is defined already over the biquadratic extension $k(\sqrt{C}, \sqrt{m'})$, we can restrict our attention to this extension by inflation-restriction, as above. With the above assumptions, it is clear that the fixed field of $\{\tau \in \operatorname{Gal}(k(\sqrt{C}, \sqrt{m'})/k) : c_\tau = 1\}$, which we denoted by N in the above arguments, is $k(\sqrt{Cm'})$, and that if σ is the nontrivial element of the Galois group fixing $\sqrt{Cm'}$, then

$$\sigma M = \frac{-1}{A'} \begin{pmatrix} 0 & 1 \\ A' & 0 \end{pmatrix} M \begin{pmatrix} 0 & A' \\ 1 & 0 \end{pmatrix}.$$

Now, if $X(\mathbb{A}_k) \neq \emptyset$, we can use the equation $-w^2 = \det M$ and plug in local points everywhere to obtain that A' is the quotient of a norm from $k_v(\sqrt{C})$ and a norm from $k_v(\sqrt{m'})$, for all places v. This clearly implies that A' is a norm from $k_v(\sqrt{C}, \sqrt{m'})$ to $k_v(\sqrt{Cm'})$. Then by the Hasse Norm Theorem, A' is a norm from $k(\sqrt{C}, \sqrt{m'})$ to N.

Writing $A' = \operatorname{Norm}_\sigma(\gamma)$, with $\gamma = n_1 + n_2\sqrt{C}$, $n_1, n_2 \in N$, we find that

$$\begin{pmatrix} 0 & 1 \\ A' & 0 \end{pmatrix} \sim (\sigma U)U^{-1}, \quad U^{-1} = \begin{pmatrix} 1 & \gamma/A' \\ \gamma & 0 \end{pmatrix},$$

and writing $M' = (\det U)U^{-1}M(U^{-1})^T$ gives $\sigma M' = M'$, $\det M' = \det M$, and

$$M' = \frac{A'}{A' - \gamma^2} \begin{pmatrix} M_1 + \frac{2\gamma}{A'}M_2 + \frac{\gamma^2}{(A')^2}M_3 & \gamma M_1 + \frac{A'+\gamma^2}{A'}M_2 + \frac{\gamma}{A'}M_3 \\ \gamma M_1 + \frac{A'+\gamma^2}{A'}M_2 + \frac{\gamma}{A'}M_3 & \gamma^2 M_1 + 2\gamma M_2 + M_3 \end{pmatrix},$$

where the M_i are the entries of M as written above.

The last step is changing M' to an equivalent matrix also defined over N with the same determinant, such that the off-diagonal entries are defined over k. We can do this completely explicitly:

Proposition 7.1. *With notation as above, if M_1', M_2', M_3' are the entries of M', then either there exists $g \in k$ such that $gM_1' + M_2'$ is defined over k, or M_1' is already defined over k. In the first case, $\mathcal{A} = (N/k, (w - gM_1' - M_2')/x^2)$ is an Azumaya algebra representing the nontrivial order-2 element of $\operatorname{Br} X/\operatorname{Br} k$ corresponding to M', and in the second case, this element can be represented by $(N/k, ((M_1' - M_3')/2 - w)/x^2)$.*

Proof: By assumption, $n_2 \neq 0$. There are several cases:
Case 1: $n_1 = 0, n_2 \in k$. In this case, M_1' is defined over k.
Case 2: $n_1 \neq 0, n_1 \in k, n_2 \in k$. In this case, we can take $g = -A'/n_1$.

Case 3: $n_1 \notin k, n_2 \in k$. In this case, n_1 must be in $k^*\sqrt{m'C}$, and M_1' is defined over k.

Case 4: $n_2 \notin k$. Take $g = \frac{n_1\bar{n}_2 - \bar{n}_1 n_2}{n_2 - \bar{n}_2}$, where the bar denotes conjugation in N.

As for the statement about the Azumaya algebra, in the first case we are given a g such that $gM_1' + M_2'$ is defined over k, where $\overline{X}$ has the equation

$$w^2 = M_2'^2 - M_1'M_3' = (gM_1' + M_2')^2 - M_1'(g^2M_1' + 2gM_2' + M_3').$$

So the desired conclusion follows from Theorem 6.16.

If M_1' is defined over k, then we are in Case 1 or 3 above, in which case a computation shows that M_3' is also defined over k. Now, since $\overline{X}$ has the equation

$$w^2 = M_2'^2 - M_1'M_3' = \left(\frac{M_1' - M_3'}{2}\right)^2 - \left(\frac{M_1' + M_3'}{2} + M_2'\right)\left(\frac{M_1' + M_3'}{2} - M_2'\right),$$

the desired conclusion follows again from Theorem 6.16. ■

We can use these results to compute $X(\mathbb{A}_\mathbb{Q})^\mathcal{A}$ for a semi-diagonal Del Pezzo surface X of degree 2, where $\mathcal{A}$ is the cyclic Azumaya algebra given by Proposition 7.1. This may not be the same as $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$, if $\mathcal{A}$ does not generate $\operatorname{Br} X$. However, we expect that "generically" $\mathcal{A}$ will generate $\operatorname{Br} X$. More concretely:

Proposition 7.2. *Let A, B, C, D, E, G be indeterminates, and let G_{sd} be the Galois group of the 56 lines on the surface X_{sd} given by the equation (9), considered over the field $\mathbb{Q}(A, B, C, D, E, G)$. Let H_{sd} be the image of G_{sd} under the natural map $G_{sd} \to W(E_7)$. Then $H^1(H_{sd}, \mathbb{Z}^8) = \mathbb{Z}/2$. So $(\operatorname{Br} X_{sd})/(\operatorname{Br} k)$ is generated by the cyclic quaternion algebra $\mathcal{A}$ of Proposition 7.1.*

Proof of proposition: The Galois group G_d of the 56 exceptional curves on a generic diagonal degree-2 Del Pezzo surface, that is, a semi-diagonal Del Pezzo surface of degree 2 with $D = E = G = 0$, is a subgroup of G_{sd}. By [12], Propositions 3 and 6, $|G_d| = 128$ and $H^1(H_d, \mathbb{Z}^8) \cong \mathbb{Z}/2$, where H_d is the image of $G_d \to W(E_7)$.

The element $\mathcal{A}$ constructed by Proposition 7.1 corresponds to a Steiner complex on the generic semi-diagonal surface which is fixed by the action of G_{sd}; this Steiner complex consists of the four lines cut out by the linear factors of $A'x^4 + B'y^4 + 2D'x^2y^2$ (where A', B', D' are defined as in the beginning of this section), and the other two analogous sets of four lines obtained by permuting the roles of the variables x, y, z in the algebraic manipulations we did at the beginning of this section. Furthermore, we will see later in the chapter (Example 9.3) that this element gives rise to a nontrivial Brauer-Manin obstruction when we specialize the values of the coefficients as follows: $A = -126, B = -91, C = 78, D = E = G = 0$. It is proved in [12] that the Galois group of the lines in this example is equal to G_d. The upshot is that the restriction map $H^1(H_{sd}, \mathbb{Z}^8) \to H^1(H_d, \mathbb{Z}^8) \cong \mathbb{Z}/2$ must send the cocycle corresponding to $\mathcal{A}$ to the nontrivial element of $\mathbb{Z}/2$. We must now only show that $H^1(H_{sd}, \mathbb{Z}^8)$ cannot be any larger than $\mathbb{Z}/2$. From Theorem 4.1, we know that it must be a 2-group, so the only possibilities are that it contains a copy of $\mathbb{Z}/4$ or that it contains a copy of $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

First of all, suppose that $H^1(H_{sd}, \mathbb{Z}^8)$ has an element of order 4. Then H_{sd} is contained in a group H_4 of order 1152 (Step 5 of the proof of Theorem 4.1). Then H_d is contained in this group as well. But since $1152 = 128 \cdot 9$, H_d would then be a Sylow 2-subgroup of H_4, and therefore $H^1(H_4, \mathbb{Z}^8)_2 \cong \mathbb{Z}/4$ injects into $H^1(H_d, \mathbb{Z}^8) \cong \mathbb{Z}/2$, by Lemma 3.5. This is impossible, so there is no element of order 4 in $H^1(H_{sd}, \mathbb{Z}^8)$.

Now we must also show that there are not two separate copies of $\mathbb{Z}/2$ inside $H^1(H_{sd}, \mathbb{Z}^8)$. Notice that any order-2 element in $H^1(H_{sd}, \mathbb{Z}^8)$ must be an element of the first type: if there were an element of the second type, then H_{sd}, and hence H_d, would be contained inside both the subgroup H_{63} of index 63 that we have already encountered and a subgroup $K \cong S_8$ of index 72 that stabilizes a conjugate of $x_7 \in \overline{P}/2\overline{P}$. Then, as before, H_d would be a Sylow 2-subgroup of K, which would imply that the restriction map $\mathbb{Z}/2 = H^1(K, \mathbb{Z}^8)_2 = H^1(K, \mathbb{Z}^8) \to H^1(H_d, \mathbb{Z}^8)$ would be injective. This factors through the restriction map $H^1(H_{sd}, \mathbb{Z}^8)_2 = H^1(H_{sd}, \mathbb{Z}^8) \to H^1(H_d, \mathbb{Z}^8)$, which must also be injective because H_d would also have to be a Sylow 2-subgroup of H_{sd}. But we have already seen that $H^1(H_d, \mathbb{Z}^8) \cong \mathbb{Z}/2$, generated by an element of the first type, so both restriction maps would have to be isomorphisms and we would have $H^1(H_{sd}, \mathbb{Z}^8) \cong \mathbb{Z}/2$, in which case it would already be generated by the nontrivial element of the first type constructed in Proposition 7.1.

Now suppose there are two distinct elements of the first type inside $H^1(H_{sd}, \mathbb{Z}^8)$. Then H_{sd}, and hence H_d, will be contained in the intersection of two conjugates of the subgroup H_{63} defined above. A MAGMA computation shows that, up to conjugation, there are exactly two such groups, one of order 1440 and the other of order 1536. Neither group contains a subgroup H of order 128 satisfying the conditions $H^1(H, \mathbb{Z}^8) \cong \mathbb{Z}/2$ and rank $(\mathbb{Z}^8)^H = 1$, which is a contradiction since H_d satisfies these conditions. ■

Remark 7.3. If X is a semi-diagonal Del Pezzo surface of degree 2, then the most obvious exceptional curves on X are the 24 curves lying over the 12 bitangents in the Steiner complex described above (the complex corresponding to the element $\mathcal{A}$ we construct in Proposition 7.1). Proposition 7.2 shows that these are the only exceptional curves we will need to find, unless our semi-diagonal surface is non-generic.

8. Computing invariants

Here we collect various observations and results that aid us in the implementation of the computation of the Brauer-Manin obstruction for Del Pezzo surfaces of degree 2 over $\mathbb{Q}$. Our first observation is that cyclic algebras are very nice in general for the purposes of invariant computations. In fact, the discussion in sections XIV.1 and XIV.2 of [18] implies that if $L = k(\sqrt[n]{c})$ and P_v is a point in $X(k_v)$ for some place v of k, then

$$\operatorname{inv}_v(L/k, f)(P_v) = [c, f(P_v)]_v,$$

where $[a, b]_v \in \mathbb{Z}/n$ is the local norm residue symbol written additively, in the sense that

$$\theta^{[a,b]_v} = (a, b)_v$$

where $(a, b)_v \in \mu_n$ is the standard norm residue symbol, and θ is the nth root of unity equal to $\sigma(\sqrt[n]{c})/\sqrt[n]{c}$, where σ is the generator of $\operatorname{Gal}(L/k)$ chosen in the construction of $(L/k, f)$. Of course, there will only be one choice in the case we are interested in here, where L is a quadratic extension of k. Note that we can assume that $f(P_v)$ is defined and nonzero by multiplying f by a suitable element $N_{L/k}(g) \in k(X)$, which will not change the class of the algebra $(L/k, f)$ in $\operatorname{Br} X$. This follows from the criteria in Proposition 6.4.

The next result is a "shortcut" that rules out an obstruction in many cases with a minimum of computational effort.

Proposition 8.1. *Suppose X is a Del Pezzo surface of degree 2 over k with $X(\mathbb{A}_k) \neq \emptyset$, and suppose $H^1(k, \operatorname{Pic} \overline{X})$ contains an order-2 element of the first type, so that by Theorem 6.12, X is given by the equation (8):*

$$B_2^2 - w^2 = bB_1(\alpha B_1)$$

where B_2 is defined over k, $b \in k$, and B_1 is defined over N_c with α the nontrivial element of $\operatorname{Gal}(N_c/k)$. Then, if $b \notin N_{N_c/k}N_c^*$, we must have $X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} \neq \emptyset$, so that $\mathcal{A}$ cannot give a nontrivial Brauer-Manin obstruction for X.

Proof of proposition: Suppose b is not a norm from N_c. Then, by the Hasse Norm Theorem, there is some place v of k (which is either ramified or inert in N_c) such that b is not a norm from $(N_c)_w$ to k_v, where w is the unique place of N_c lying over v. Let $N_c = k(\sqrt{n})$, and extend α to an element of $\operatorname{Gal}((N_c)_w/k_v)$.

Now take $P_v \in X(k_v)$. Let P'_v be the image of P_v under the involution $w \mapsto -w$ on $X(k_v)$. Then

$$\operatorname{inv}_v \mathcal{A}(P_v) + \operatorname{inv}_v \mathcal{A}(P'_v) = [n, (B_2 - w)(P_v)]_v + [n, (B_2 - w)(P'_v)]_v$$

Here we have chosen projective coordinates for P_v, defined up to scaling; we can disregard the denominator x^2 because it is automatically a square (if the x-coordinate of P_v happens to be 0, then for purposes of evaluation we can change the denominator of the function defining $\mathcal{A}$ to the square of a different coordinate, without changing $\mathcal{A}$). Note that the above expression really does make sense, because multiplying the coordinates x, y, z for P_v by λ and multiplying w by λ^2 scales $(B_2 - w)(P_v)$ by λ^2, which leaves the norm residue symbol unchanged.

Now we have

$$\begin{aligned}[n, (B_2 - w)(P_v)]_v + [n, (B_2 - w)(P'_v)]_v &= [n, (B_2 - w)(P_v)]_v + [n, (B_2 + w)(P_v)]_v \\ &= [n, (B_2^2 - w^2)(P_v)]_v \\ &= [n, bB_1(P_v)(\alpha B_1)(P_v)]_v \\ &= [n, b]_v\end{aligned}$$

so if b is not a norm, then $\operatorname{inv}_v \mathcal{A}(P_v) + \operatorname{inv}_v \mathcal{A}(P'_v) = 1$ in $\mathbb{Z}/2$, so either P_v or P'_v is in $X(\mathbb{A}_k)^{\mathcal{A}}$. ■

So we will not be able to find an obstruction using only $\mathcal{A}$ if b is not a norm from N_c. However, if b is a norm, we will actually have to calculate the obstruction over $\mathbb{Q}$ by approximating all the points in $X(\mathbb{Q}_p)$ closely enough to ensure sufficient accuracy in evaluating the function $(B_2 - w)/x^2$ at those points. We will sometimes use the following remark as well:

Remark 8.2. If b is a norm, then for all places v and points $P_v \in X(k_v)$,

$$\operatorname{inv}_v \left(N_c/k, \frac{B_2 - w}{x^2} \right)(P_v) = \operatorname{inv}_v \left(N_c/k, \frac{B_2 + w}{x^2} \right)(P_v)$$

because the sum of these invariants equals

$$\operatorname{inv}_v \left(N_c/k, \frac{B_2^2 - w^2}{x^4} \right)(P_v) = \operatorname{inv}_v \left(N_c/k, \frac{bB_1(\alpha B_1)}{x^4} \right)(P_v) = 0$$

since $(bB_1(\alpha B_1)/x^4)(P_v)$ is always a norm. So we can use either of these two expressions to evaluate the invariant.

Remark 8.3. Suppose v is a place of k that does not split in N_c. When we compute the invariants $\operatorname{inv}_v \mathcal{A}(P_v)$ using Remark 8.2, it is important to note that B_2-w and B_2+w cannot simultaneously vanish on $X(k_v)$, for the following reason: if they did, we would have $B_2(P_v) = w(P_v) = 0$ for some $P_v \in X(k_v)$, and then that would imply that $bB_1(P_v)(\alpha B_1(P_v)) = 0$. Since b is clearly nonzero, one of the other factors is zero, but then they both are, because α extends to an automorphism of $N_c \otimes_k k_v$, which is the completion of N_c at the unique place above v. But if w, B_2, B_1, and αB_1 all vanish on P_v, taking partial derivatives of (8) shows that P_v is a singular point of X_{k_v}, which cannot happen.

When we compute invariants, we will need the following standard result that tells us at which places we must compute the local invariants. Class field theory implies that for all but finitely many places v of k, the local invariant will be trivial; here we give an explicit criterion that makes this result effective for computational purposes.

Proposition 8.4. *Let X be a smooth geometrically integral variety over a number field k. Let f be an element of $k(X)^*$ and let $\mathcal{A} = (L/k, f)$ be a cyclic algebra in $\operatorname{Br} X$ (as in Proposition 6.4). Let v be a nonarchimedean place of k, and suppose that v does not ramify in L and that X has smooth reduction at v. Then $\operatorname{inv}_v \mathcal{A}(P_v)$ is independent of the choice of $P_v \in X(k_v)$.*

Proof of proposition: Let K be the decomposition field of v with respect to the extension L/k. Then

$$\operatorname{inv}_v(L/k, f)(P_v) = \operatorname{inv}_w(L/K, f)(P_v),$$

where w is a place of K above v. So we must only prove the proposition in the case when v is inert. Let w be the unique place of L over v in this case.

In this case, we have $(f) = N_{L/k}(D)$ for some $D \in \operatorname{Div} X_L$, by Proposition 6.4. Consider P_v as a point in $X(\mathfrak{o}_v)$ (by scaling coordinates). On the smooth model $\mathcal{X}$ for X over $\operatorname{Spec} \mathfrak{o}_v$, consider the divisor $\mathcal{D}$ equal to the sum of the closures of the prime divisors in D (with multiplicities). Then the divisor of the function $f \in k(\mathcal{X}) = k(X)$ on $\mathcal{X}$ is of the form

$$N_{\mathfrak{o}_w/\mathfrak{o}_v} \mathcal{D} + mX_v,$$

where m is some integer and X_v is the special fiber of $\mathcal{X}$. Let π be a uniformizer for $\mathfrak{o}_v$; then the divisor of $g = f/\pi^m$ is $N_{\mathfrak{o}_w/\mathfrak{o}_v}\mathcal{D}$. But $\mathcal{D}$ is locally principal, and we can replace g by $g/N_{L/k}(h)$ for some h in $k(X_L)^*$ without changing the value of the invariant, so we can assume P_v is not in the support of $\mathcal{D}$. In that case, $g(P_v) \in \mathfrak{o}_v^*$. But then $\operatorname{inv}_v(L/k, g)(P_v) = 0$, so that $\operatorname{inv}_v \mathcal{A}(P_v) = \operatorname{inv}_v(L/k, \pi^m)(P_v)$, which is independent of P_v. ■

Remark 8.5. Naturally, $\operatorname{inv}_v \mathcal{A}(P_v)$ depends on the choice of f, which is defined only up to a constant multiple if we are only concerned with the class of $\mathcal{A} \in (\operatorname{Br} X)/(\operatorname{Br} k)$. If we choose f so that it is a quotient of two polynomials, neither of whose coefficients in $\mathfrak{o}_v$ have a common multiple of π, then the proof of Proposition 8.4 shows that $\operatorname{inv}_v \mathcal{A}(P_v) = 0$.

For $k = \mathbb{Q}$, $d = 2$, there are three different cases: $p = \infty$, p odd, and $p = 2$. For each p, we describe the MAGMA program we used to compute the invariant $\operatorname{inv}_v \mathcal{A}(P_p)$ for all $P \in X(\mathbb{Q}_p)$, for semi-diagonal Del Pezzo surfaces of degree 2. Note that we first multiply both sides by the square of whatever denominators occur in B_2, and then absorb this square into w^2, so that we can assume that the polynomial B_2 has coefficients in $\mathbb{Z}$.

The case $p = \infty$: First of all, if $n > 0$, then $\mathrm{inv}_v \mathcal{A}(P_v) = 0$ for all $P_v \in X(\mathbb{R})$ (p splits in N_c). And if $n < 0$, we have $\mathrm{inv}_v \mathcal{A}(P_v) = 0$ if $(B_2 - w)(P_v) > 0$ and 1 if $(B_2 - w)(P_v) < 0$. If $(B_2 - w)(P_v) = 0$, we use the same statement for $(B_2 + w)(P_v)$ instead.

Assume from now on that $n < 0$ and b is a norm (otherwise there is nothing to compute). Then b is positive, and in fact the right side of the defining equation (8) is always nonnegative. Then $|B_2(P)| \geq |w(P)|$ for all $P \in X(\mathbb{R})$. Then the sign of $(B_2 \pm w)(P)$, if it is nonzero, equals the sign of $B_2(P)$ (note $B_2(P) \neq 0$ because there are no singular points on $X(\mathbb{R})$). Note that for semi-diagonal Del Pezzo surfaces of degree 2 over $\mathbb{Q}$ and the algebra $\mathcal{A}$ constructed in Proposition 7.1, we have $B_2 = a_0x^2 + b_0y^2 + c_0z^2$ for some $a_0, b_0, c_0 \in \mathbb{Q}$. B_1 is also a linear polynomial in x^2, y^2, z^2.

The equation of a semi-diagonal Del Pezzo surface of degree 2 is of the form $w^2 = F(x^2, y^2, z^2)$ for some quadratic polynomial F. So, letting $x' = x^2, y' = y^2, z' = z^2$, we must find the sign of $B_2 = a_0x' + b_0y' + c_0z'$ for all points $(x', y', z') \in \mathbb{R}^3_{\geq 0}$ such that $F(x', y', z') \geq 0$.

Proposition 8.6. *With notation as above,*

$$\{sign(a_0x' + b_0y' + c_0z') : (x', y', z') \in \mathbb{R}^3_{\geq 0}, F(x', y', z') \geq 0\} =$$
$$\{sign(a_0x' + b_0y' + c_0z') : (x', y', z') \in \mathbb{R}^3_{\geq 0}, x'y'z' = 0, F(x', y', z') = 0\},$$

unless the latter set is empty, in which case the former set equals $\{sign(F(P))\}$, where P is the center of the conic section $F(x', y', 1) = 0$ in $\mathbb{A}^2_{\mathbb{R}}$ (which, in this case, is an ellipse contained in the first quadrant of the $x'y'$-plane).

Proof of proposition: Call the first set in the statement of the theorem S. Consider the set $\mathcal{P}$ cut out by $F(x', y', 1) \geq 0$ in $\mathbb{A}^2_{\mathbb{R}}$. The line $a_0x' + b_0y' + c_0 = 0$ cannot intersect $\mathcal{P}$, because we have

$$(a_0x' + b_0y' + c_0)^2 - F(x', y', 1)^2 = bF_1(x', y', 1)(\alpha F_1(x', y', 1))$$

for all points (x', y', z') in $\mathcal{P}$, where $F_1(x^2, y^2, z^2) = B_1(x, y, z)$. But the right side of the above equation is nonnegative, as we have seen already, and so if $a_0x' + b_0y' + c_0 = 0$ for $(x', y') \in \mathcal{P}$, we must have $F(x', y', 1) = 0$, but then $(x', y', 1)$ gives a singular point on the conic cut out by F (just as in Remark 8.3), which is not allowed.

So the sign of $a_0x' + b_0y' + c_0$ remains constant inside the connected components of $\mathcal{P}$ in $\mathbb{A}^2_{\mathbb{R}}$. We are interested in those connected components that intersect the first quadrant of the affine plane. Let

$$F = A(x')^2 + B(y')^2 + C(z')^2 + 2Dx'y' + 2Ex'z' + 2Gy'z'.$$

Suppose $D^2 - AB < 0$. Then $F(x', y', 0) = 0$ has no real solutions, and $F(x', y', 1)$ cuts out an ellipse (or a point) in $\mathbb{A}^2_{\mathbb{R}}$; the region $F(x', y', 1) > 0$ must be the interior of the ellipse since the line $a_0x' + b_0y' + c_0 = 0$ cannot intersect it. So $|S| = 1$, and so it suffices to compute the sign of $a_0x' + b_0y' + c_0$ for the points on the boundary of the ellipse intersecting the x- or y- axes. If there are no such points, then it suffices to compute $\mathrm{sign}(P)$ for P the center of the ellipse.

If $D^2 - AB = 0$, then we can write $F(x^2, y^2, 0) = ((y_0x)^2 - (x_0y)^2)^2$ for some x_0, y_0, and then X will have a singular point at $(x_0 : y_0 : 0)$, which is not allowed.

Now suppose $D^2 - AB > 0$. Then $F(x', y', 1)$ cuts out a hyperbola, and $\mathcal{P}$ will have two connected components in $\mathbb{A}^2_{\mathbb{R}}$, on each of which the sign of $a_0x' + b_0y' + c_0$ will be constant. Again, if a component intersects the x- or y-axes, it suffices to compute the sign of $a_0x' + b_0y' + c_0$ for the intersection points on the boundary of the component. So the only case left to consider is when a component intersects the first quadrant without intersecting the x- or y-axes, so that it is bounded by one of the branches of the hyperbola contained entirely inside the first quadrant.

But in this case, there will be "points at infinity" contained in the interior of this component, and the sign of $a_0x' + b_0y' + c_0z'$ at these points will equal the sign of $a_0x' + b_0y' + c_0z'$ for any point in the component. To see this, suppose $(x_0 : y_0 : 0)$ is a point at infinity in the interior; this means that $(\lambda x_0, \lambda y_0)$ is in the component for λ sufficiently large (because $F(x_0, y_0, \frac{1}{\lambda})$ is positive for λ sufficiently large). But the sign of $a_0x_0 + b_0y_0$ equals the sign of $a_0(\lambda x_0) + b_0(\lambda y_0) + c_0$ for λ sufficiently large (x_0 and y_0 are not both zero, and the same is true for a_0 and b_0 in this case, because $a_0x' + b_0y' + c_0z'$ cannot vanish anywhere on the component). ■

It is very easy to compute the invariant at ∞ using this proposition, as we only have to compute the sign of $a_0x' + b_0y' + c_0z'$ at a finite, easily computable set of points.

The case p odd: We start by assuming that p does not split in N_c (otherwise the invariant is automatically zero, as we have seen). We also assume that b is indeed a norm from $N_c/\mathbb{Q}$ (so that Proposition 8.1 does not apply). We extend X to a $\mathbb{Z}_p$-scheme (using its defining equation, whose coefficients are integers), and we have $X(\mathbb{Q}_p) = X(\mathbb{Z}_p)$ (by scaling coordinates). For $P \in X(\mathbb{Z}_p)$, we consider the integer $v_p(\nabla(P))$, which we define to be the minimum of the valuations

$$v_p(2w(P)), v_p(f_x(P)), v_p(f_y(P)), v_p(f_z(P))$$

where $f(x, y, z) = F(x^2, y^2, z^2)$ is the right side of the equation (9).

Proposition 8.7. *If p is an odd prime and $v_p(\nabla(P)) < m$, then either $B_2(P) - w(P)$ or $B_2(P) + w(P)$ is nonzero mod p^m, so we only need to know P mod p^m in order to compute the invariant* $\text{inv}_p(N_c/\mathbb{Q}, (B_2 - w)/x^2)$.

Proof of proposition: If $B_2(P) - w(P) \equiv B_2(P) + w(P) \equiv 0 \bmod p^m$, then $B_2(P) \equiv w(P) \equiv 0 \bmod p^m$. We can absorb the constant $b = b_1(\alpha b_1)$ into the product $B_1(\alpha B_1)$; having done this, we obtain the equation $v_p(B_1(P)(\alpha B_1(P))) \geq 2m$. But α preserves valuations, so that both factors have valuation at least m. But now, as in Remark 8.3, this implies that $v_p(\nabla) \geq m$.

As for the invariant, the norm residue symbol $[n, p^d u]_p$, where $u \in \mathbb{Z}_p^*$, depends only on the value of $u \in \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. So we only need to know $p^d u$ mod p^{d+1}; if $d < m$ it suffices to know $p^d u$ mod p^m. ■

So our program runs as follows: starting at $m = 1$, we find solutions to equation (9) mod p^m. Then for each solution, we compute $d = v_p(\nabla)$, and if $d < m$, we can compute the relevant norm residue symbol $[n, (B_2 \pm w)(P_p)]_p$, *if* the solution lifts to a point $P_p \in X(\mathbb{Z}_p)$. To check whether it does, we simply look at the set of all solutions mod p^{m+2d} which reduce mod p^m to our solution. By Hensel's lemma, there is a point $P_p \in X(\mathbb{Z}_p)$ which reduces to our solution mod p^m if and only if this set is nonempty.

If $d = m$, we must lift our solution to solutions mod p^{m+1} and go through the same computations we did for m above. The process eventually terminates, because there are no singular points in $X(\mathbb{Z}_p)$. (Note, for instance, that the process terminates after $m = 1$ if and only if the equation $w^2 = f(x, y, z)$ reduces mod p to a nonsingular surface.)

The case $p = 2$: The computation is the same, except for one minor issue: Proposition 8.7 is not quite true for $p = 2$. However, it is true that $v_p(\nabla(P)) < m - 1$ implies that $B_2(P) - w(P)$ or $B_2(P) + w(P)$ is nonzero mod p^m, because if they are both zero, then $v_2(2B_2(P))$ and $v_2(2w(P))$ are $\geq m$.

9. Evidence for the standard conjecture; examples

Theorem 9.1. *Let X be a Del Pezzo surface of degree 2 over $\mathbb{Q}$ given by the equation*

$$w^2 = Ax^4 + By^4 + Cz^4 \tag{10}$$

with $|A|, |B|, |C| \leq 50$. Then if X fails to satisfy the Hasse principle, X has a nontrivial Brauer-Manin obstruction.

Remark 9.2. We actually show that in every case but one where the Hasse principle fails, there is an obstruction coming from a single order-2 element of the first type. (In the exceptional case, the obstruction comes from two elements of the first type: see Example 9.4.) While we expect the conclusion of the theorem to remain valid for all values of A, B, C, it will not in general be true that all obstructions come from elements of the first type, or even elements of order 2; see [12], Example 8, for a diagonal Del Pezzo surface X with an obstruction coming only from an element of order 4 in $(\operatorname{Br} X)/(\operatorname{Br} k)$.

There is nothing particularly noteworthy about the number 50 in the above theorem; it might be worthwhile to extend these computations to more diagonal surfaces, if only to observe more exceptionally behaving examples (for instance, examples with an order-4 element in $H^1(k, \overline{P})$).

Proof of theorem: This is proved entirely by running MAGMA programs implementing the algorithms we have developed in the previous sections (as well as basic programs designed to compute points of small height on diagonal Del Pezzo surfaces of degree 2). Here is the outline of the computations we carried out using MAGMA.

First, we compiled a list of all tuples (A, B, C), $A \leq B \leq C$, in the given range such that the surface X defined by equation (10) had points everywhere locally and no integer-valued points with height up to 500. For our purposes, the height of a solution (w, x, y, z) with relatively prime integral coordinates is defined to be the maximum of the absolute values of x, y, z. We found 159 such tuples. Using the description of the generic order-2 algebra we described above, as well as the outline of the actual computation of the Brauer-Manin obstruction for this algebra described in the previous section, we separated these into two groups: there were 139 tuples such that the order-2 algebra constructed above gave a nontrivial Brauer-Manin obstruction, and 20 tuples where it did not.

There was some redundancy in the tuples in the first list, as different tuples can give rise to isomorphic surfaces (for instance, if one tuple is obtained from the other by multiplying all the coefficients by a perfect square, or multiplying one coefficient by a perfect fourth power). After eliminating this redundancy, we were left with 96 surfaces with a nontrivial Brauer-Manin obstruction.

As for the second list, we increased the height of the points we searched for, finding points on all of the surfaces but one: $A = B = C = 34$. Here $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q}) \cong (\mathbb{Z}/2)^3$.

In [12], Example 7, the authors give a rather delicate construction of a generating set of elements of $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q})$, which they use to show that there is a nontrivial Brauer-Manin obstruction on X. In Example 9.4 below, we show that we can give representatives of the nontrivial elements of $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q})$ using determinantal equations (i.e.: these elements are all of the first type), and use these to exhibit the Brauer-Manin obstruction on X. So there are a total of 97 counterexamples to the Hasse principle defined by the equation (10) with $|A|, |B|, |C| \leq 50$, and we have found a nontrivial Brauer-Manin obstruction on each. For a complete list of these surfaces, see the Appendix. ■

Example 9.3. Consider the surface X defined by the equation

$$w^2 = 16(-126x^4 - 91y^4 + 78z^4)$$

We find that $N_c = \mathbb{Q}(\sqrt{-3})$, and $B_2 = -21x^2 + 39z^2$. (We multiplied by 16 so that B_2 would have integral coefficients.) The relevant determinantal equation is

$$16(-126x^4 - 91y^4 + 78z^4) = \\ (-21x^2 + 39z^2)^2 - 2457(x^2 - \frac{4}{9}\sqrt{-3}y^2 - \frac{1}{3}z^2)(x^2 + \frac{4}{9}\sqrt{-3}y^2 - \frac{1}{3}z^2)$$

Note that $2457 = N_{N_c/\mathbb{Q}}(45 + 12\sqrt{-3})$.

Clearly $B_2(P)$ is positive for any $P \in X(\mathbb{R})$, so the invariant at ∞ is 0. The only bad primes (i.e. primes for which the invariant is not always 0) are those that ramify in N_c or are primes of bad reduction for X, by Proposition 8.4 and Remark 8.5. In this case, the bad primes are $p = 2, 3, 7, 13$. Then, for any $P_v \in X(\mathbb{Q}_v)$ $(v = 2, 3, 7, 13)$, we compute

$$\begin{aligned} \operatorname{inv}_2(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_2) &= 1 \\ \operatorname{inv}_3(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_3) &= 0 \\ \operatorname{inv}_7(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_7) &= 0 \\ \operatorname{inv}_{13}(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_{13}) &= 0 \end{aligned}$$

(the invariants are written additively, as elements of $\mathbb{Z}/2$). So the sum of the invariants is 1, which means that this algebra gives a Brauer-Manin obstruction to rational points.

While the coefficients A, B, C of this example are too large to fit into the list in the Appendix, the Brauer-Manin obstruction is computed in exactly the same way, using the "generic" order-2 element constructed in section 7, for every surface in that list except for one: $(A, B, C) = 34$.

Example 9.4. Consider the surface $X/\mathbb{Q}$ given by the equation

$$w^2 = 34(x^4 + y^4 + z^4) \tag{11}$$

It is not hard to show that this surface has points everywhere locally, and it is also not hard to see that the generic order-2 element of $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q})$ does not give a Brauer-Manin obstruction. In fact, it is possible to show that $X(\mathbb{A}_\mathbb{Q})^\mathcal{A} \neq \emptyset$ for all $\mathcal{A} \in \operatorname{Br} X$. Nevertheless, it is true that $X(\mathbb{A}_\mathbb{Q})^{\operatorname{Br}} = \emptyset$, which we will verify by showing that $X(\mathbb{A}_\mathbb{Q})^{\mathcal{A}_1} \cap X(\mathbb{A}_\mathbb{Q})^{\mathcal{A}_2} = \emptyset$ for two elements $\mathcal{A}_1, \mathcal{A}_2 \in \operatorname{Br} X$. The situation is thus rather more complex than it is in the generic case; compare also with [7], Lemma 3.4, which shows that if X is a Del Pezzo surface of degree 3 or 4 over a number field k with a nontrivial Brauer-Manin obstruction, then $X(\mathbb{A}_k)^\mathcal{A} = \emptyset$ for some $\mathcal{A} \in \operatorname{Br} X$.

For the interested reader, we write down representatives of the seven nontrivial elements of $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q})$. We obtained these by examining the list of exceptional curves in [12], writing down seven Steiner complexes fixed by $G_{\mathbb{Q}}$, and then applying the correspondences described above to produce determinantal equations for X. Note that these representatives involved choices of solutions to certain norm equations; different choices lead to algebras which differ from the given ones by a constant algebra.

- $(\mathbb{Q}(\sqrt{-34})/\mathbb{Q}, (-3x^2 - 5y^2 - w)/x^2)$; this is the "generic element" given by our construction
- $\left(\mathbb{Q}(\sqrt{17})/\mathbb{Q}, \left(\frac{35}{2}z^2 + \frac{33}{2}(x-y)^2 - w\right)/x^2\right)$, and the other two algebras obtained by cyclically permuting the variables x, y, z
- $(\mathbb{Q}(\sqrt{-17})/\mathbb{Q}, (-4x^2 + 6xy + 4y^2 - w)/x^2)$, and the other two algebras obtained by cyclically permuting the variables x, y, z

We leave as an exercise the verification that these seven algebras give distinct representatives of $(\operatorname{Br} X)/(\operatorname{Br} \mathbb{Q})$; probably, the easiest way to show this is to obtain them in the same way we did, by starting with seven distinct Steiner complexes. The local invariant computations which show that $X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} \neq \emptyset$ for every $\mathcal{A}$ are also straightforward.

Now, let

$$\begin{aligned} \mathcal{A}_1 &= \left(\mathbb{Q}(\sqrt{17})/\mathbb{Q}, \left(\tfrac{35}{2}z^2 + \tfrac{33}{2}(x-y)^2 - w\right)/x^2\right) \\ \mathcal{A}_2 &= \left(\mathbb{Q}(\sqrt{17})/\mathbb{Q}, \left(\tfrac{35}{2}y^2 + \tfrac{33}{2}(z-x)^2 - w\right)/x^2\right) \end{aligned}$$

Because 17 is positive, the local invariants at ∞ are trivial. The bad primes in this case are 2 and 17. Because 17 is a square in $\mathbb{Q}_2$, the local invariants at 2 are automatically trivial as well.

As for the invariant at 17, let $P = (w, x, y, z)$ be a solution to the equation (11); scale the coordinates so that they lie in $\mathbb{Z}_{17}$, with not all of x, y, z divisible by 17. Then w is divisible by 17 and exactly one of x, y, z is divisible by 17. It can also be verified that if we let $f_1 = \frac{35}{2}z^2 + \frac{33}{2}(x-y)^2$, then $f_1(P)$ is never divisible by 17. So the invariant $\mathcal{A}_1(P)$ is trivial if and only if $f_1(P)$ is a square mod 17, which happens if and only if $z^2 - (x-y)^2$ is a square mod 17.

So certainly if z is divisible by 17, then $\operatorname{inv}_{17} \mathcal{A}_1(P)$ is trivial. Now suppose y is divisible by 17. Plugging into (11), we get that $x^4 + z^4$ is divisible by 17. We can scale so that $x \equiv 1 \bmod 17$, so that $z \equiv \pm 2$ or $\pm 8 \bmod 17$. Then $z^2 - x^2 \equiv 3$ or $12 \bmod 17$; neither of these is a square, so $\operatorname{inv}_{17} \mathcal{A}_1(P)$ is nontrivial. This is also the case if x is divisible by 17.

In summary, suppose we have a point $(P_v) \in X(\mathbb{A}_{\mathbb{Q}})$, and choose coordinates for P_{17} scaled, as above, so that $x(P_{17}), y(P_{17}), z(P_{17}) \in \mathbb{Z}_{17}$ are not all divisible by 17. Then

$$\begin{aligned} (P_v) \in X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}_1} &\Leftrightarrow \ z(P_{17}) \text{ is divisible by } 17 \\ (P_v) \in X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}_2} &\Leftrightarrow \ y(P_{17}) \text{ is divisible by } 17 \end{aligned}$$

but no point (P_v) can satisfy both these conditions, as exactly one of $x(P_{17}), y(P_{17}), z(P_{17})$ is divisible by 17.

Finally, we also show that X has a point in the cyclic cubic extension $L = K(\alpha)$, where α is a root of the polynomial $p(x) = x^3 - 3x + 1$. If we let $\gamma = 7\alpha^2 + 2\alpha - 2$, and γ_2, γ_3 be its conjugates in L, then we have the equation

$$(2754)^2 = 34(\gamma^4 + \gamma_2^4 + \gamma_3^4).$$

Example 9.5. We conclude with an example of an obstruction on a semi-diagonal surface. Consider the surface X defined by the equation

$$w^2 = 16(-2x^4 - y^4 + 2z^4 - 4x^2y^2 - 4x^2z^2 - 4y^2z^2)$$

We find that $N_c = \mathbb{Q}(\sqrt{2})$ and $B_2 = -6x^2 - y^2$. (We multiplied by 16 to clear the denominators of B_2, as before.) The relevant determinantal equation is

$$16(-2x^4 - y^4 + 2z^4 - 4x^2y^2 - 4x^2z^2 - 4y^2z^2) =$$
$$(-6x^2 - y^2)^2 - 68\left(x^2 + \frac{19 - 6\sqrt{2}}{34}y^2 + \frac{8 + 10\sqrt{2}}{17}z^2\right)\left(x^2 + \frac{19 + 6\sqrt{2}}{34}y^2 + \frac{8 - 10\sqrt{2}}{17}z^2\right)$$

Note that $68 = N_{N_c/\mathbb{Q}}(10 + 4\sqrt{2})$.

Because N_c is real, the invariant at ∞ is automatically 0. Here the only bad primes are 2 and 3, and we get

$$\begin{aligned} \mathrm{inv}_2(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_2) &= 1 \\ \mathrm{inv}_3(N_c/\mathbb{Q}, (B_2 - w)/x^2)(P_3) &= 0 \end{aligned}$$

So the invariants again sum to $1 \in \mathbb{Z}/2$, and there is a Brauer-Manin obstruction.

Appendix A. Diagonal surfaces with small coefficients

In this appendix, we list the 97 diagonal Del Pezzo surfaces of degree 2 over $\mathbb{Q}$ with coefficients of absolute value ≤ 50 and a nontrivial Brauer-Manin obstruction. These are exactly the surfaces in this range with points everywhere locally but no rational points.

-50	-49	18	-50	-46	23	-50	-36	2	-50	-36	3	-50	-36	27
-50	-34	17	-50	-27	12	-50	-27	18	-50	-23	46	-50	-18	8
-50	-14	7	-50	-14	28	-50	-12	18	-50	-9	6	-50	-9	12
-50	-7	14	-50	-4	2	-50	-4	18	-50	-3	18	-50	-1	18
-50	2	8	-50	8	18	-50	18	24	-49	-36	8	-49	-36	18
-49	-25	5	-49	-25	45	-49	-24	42	-49	-18	6	-49	-18	12
-49	-14	2	-49	-14	8	-49	-14	28	-49	-4	18	-49	-3	21
-49	2	28	-49	6	12	-49	14	18	-49	18	28	-45	-4	30
-44	-22	50	-42	-14	24	-42	-6	21	-39	-13	12	-38	-19	2
-38	-19	50	-36	-34	17	-36	-18	50	-36	-17	34	-36	-15	10
-36	-9	50	-36	-2	50	-36	17	34	-34	-34	8	-34	-17	2
-34	-4	17	-34	-2	17	-33	-18	44	-33	6	44	-33	24	44
-30	-6	5	-30	-6	20	-27	-2	12	-25	-20	5	-25	-5	45
-24	14	42	-23	-2	46	-21	-14	12	-21	6	42	-20	-9	5
-18	-9	50	-18	-8	50	-18	-1	6	-18	-1	12	-18	12	50
-18	14	21	-18	24	50	-17	-4	34	-17	-2	34	-14	-1	28
-12	-8	27	-12	-6	50	-9	-4	2	-9	-4	50	-9	22	44
-8	-8	18	-8	-2	50	-8	18	50	-8	34	34	-7	-2	14
-6	-3	2	-6	-3	50	-4	-2	50	-4	-1	18	-4	17	34
-1	6	12	34	34	34									

Acknowledgements

I thank my advisor Bjorn Poonen, who introduced me to this subject and helped me greatly along the way. I thank Andrew Kresch for several helpful comments, especially the observation reproduced in the last paragraph of Example 9.4.

References

[1] B.J. Birch and H.P.F. Swinnerton-Dyer. The Hasse problem for rational surfaces. In *Collection of problems dedicated to Helmut Hasse on his seventy-fifth birthday*, pages 164–174. Walter de Gruyter, Berlin-New York, 1975.

[2] Martin Bright. *Computations on diagonal quartic surfaces*. PhD thesis, Cambridge University, 2002.

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

[4] Jean-Louis Colliot-Thélène. Points rationelles sur les fibrations. In K. Böröczky, J. Kollár, and T. Szamuely, editors, *Higher dimensional varieties and rational points: proceedings of the 2001 Budapest conference*. Springer-Verlag, 2003.

[5] Jean-Louis Colliot-Thélène. Points rationnels sur les variétés non de type général. Cours IHP, lecture notes, `http://www.math.u-psud.fr/~colliot/liste-prepub.html`, 2003.

[6] Jean-Louis Colliot-Thélène, Dimitri Kanevsky, and Jean-Jacques Sansuc. Arithmétique des surfaces cubiques diagonales. In *Diophantine Approximation and Transcendence Theory: Seminar, Bonn 1985*, pages 1–108. Springer-Verlag, Berlin, 1987. Lecture notes in mathematics, 1290.

[7] Jean-Louis Colliot-Thélène and Bjorn Poonen. Algebraic families of nonzero elements of Shafarevich-Tate groups. *J. Amer. Math. Soc.*, 13(1):83–99, 2000.

[8] Patrick Corn. *Del Pezzo surfaces and the Brauer-Manin obstruction*. PhD thesis, University of California, Berkeley, 2005.

[9] Michel Demazure. Surfaces de Del Pezzo - V - modèles anticanoniques. In M. Demazure, H. Pinkham, and B. Teissier, editors, *Séminaire sur les singularités des surfaces, Palaiseau, France 1976-1977*, pages 61–69. Springer-Verlag, Berlin-Heidelberg-New York, 1980. Lecture Notes in Mathematics, 777.

[10] Igor Dolgachev. Topics in classical algebraic geometry, part I. `http://www.math.lsa.umich.edu/~idolga/topics1.pdf`, 2004.

[11] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[12] Andrew Kresch and Yuri Tschinkel. On the arithmetic of del Pezzo surfaces of degree 2. *Proc. London Math. Soc.*, 89(3):545–569, 2004.

[13] Adam Logan. MAGMA algorithm for computing the Brauer-Manin obstruction on a Del Pezzo surface of degree 4. `http://www.liv.ac.uk/~adaml/math/index.html`, 2004.

[14] Yuri I. Manin. *Cubic Forms*. North-Holland, Amsterdam, 1974. Translated from the Russian by M. Hazewinkel.

[15] James Milne. Class field theory. Online lecture notes, `http://www.jmilne.org/math/CourseNotes/math776.pdf`, 1997.

[16] James Milne. Lectures on étale cohomology. Online lecture notes, `http://www.jmilne.org/math/CourseNotes/math732.pdf`, 1998.

[17] Hajime Nishimura. Some remarks on rational points. *Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math.*, 29:189–192, 1955.

[18] Jean-Pierre Serre. *Local fields*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[19] Alexei Skorobogatov. *Torsors and rational points*. Cambridge University Press, Cambridge, 2001. Cambridge tracts in mathematics, 144.

[20] Peter Swinnerton-Dyer. The Brauer group of cubic surfaces. *Math. Proc. Cambridge Philos. Soc.*, 113(3):449–460, 1993.

[21] Peter Swinnerton-Dyer. Brauer-Manin obstructions on some Del Pezzo surfaces. *Math. Proc. Cambridge Philos. Soc.*, 125(2):193–198, 1999.

[22] Sir Peter Swinnerton-Dyer. The solubility of diagonal cubic surfaces. *Ann. Sci. E.N.S.*, 34:891–912, 2001.

[23] Tohsuke Urabe. Calculation of Manin's invariant for Del Pezzo surfaces. *Math. Comp.*, 65(213):247–258, S15–S23, 1996.

Department of Mathematics, University of Georgia, Athens, GA 30602-7403, USA
E-mail address: `corn@math.uga.edu`
URL: `http://www.math.uga.edu/~corn`