RATIONAL POINTS ON ELLIPTIC FIBRATIONS COURSE NOTES

YONATAN HARPAZ

Contents

1. Introduction

A fundamental question in arithmetic geometry is to understand when a given variety X, say smooth and projective, defined over a number field k (e.g., the field $k = \mathbb{Q}$ of rational numbers), has a rational points (that is, a point defined over k). In more explicit terms, if we consider for example the case where $X \subseteq \mathbb{P}^n_k$ is given by collection of homogeneous polynomial equations $f_1(x_0, ..., x_n) = \cdots = f_m(x_0, ..., x_n) = 0$, then our question becomes whether this set of equations has a solution with all the variables $x_0, ..., x_n$ taking values in k.

A standard approach to this problem is to start by considering the easier question of existence of points defined over every completion k_v of k. Given a place v on k (that is, a suitable equivalence class of absolute values defined on k), the field k_v obtained by completing k with respect to the corresponding absolute value. The absolute value may be archimedean, in which case we have $k_v = \mathbb{C}$ or $k_v = \mathbb{R}$, or nonarchimedean, in which case k_v is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers for some prime p. When $k_v = \mathbb{C}$ it is in particular algebraically close, and the question of determining whether or not k_v-points exists becomes purely algebraic (and easy in practice). If $k_v = \mathbb{R}$ then we can can determine whether or not X as a k_v-point "analytically", by performing a kind of a (finite time) Newton Raphson algorithm. This procedure can be done also in the nonarchimedean case. In particular, we can determine in a finite time (and also easily in practice) whether X has points over k_v. In fact, even though k always has infinitely many places,

one can determine in finitely many steps whether or not X has k_v-points for all completions k_v. When this happens, we say that X has points **every locally**. We note that when X is smooth and projective the product space $\prod_v X(k_v)$ is also known as the space of **adelic points**, and is denote by $X(\mathbb{A}_k)$.

Of course, if $X(k_v) = \varnothing$ for at least one place v then we know that $X(k) \neq \varnothing$. The question of existence of rational points can then be essentially reduced to the following: supposing that X has points everywhere locally, does it have a rational point? types of varieties for which the answer to this question is positive are said to satisfy the **local–global principle**, or the **Hasse principle**. The latter name comes from the famous Hasse-Minkowski theorem, which asserts that if $X \subseteq \mathbb{P}^n_k$ is determined by a single quadratic equation then X has rational points as soon as it has points everywhere locally.

It is known that the Hasse principle does not hold in general: there are smooth projective varieties X over k which have points everywhere locally but do not have rational points. One the simplest examples of such a variety is Selmer's cubic curve

$$3X^3 + 4y^3 + 5z^3 = 0,$$

and many other examples are known. In 1970 Manin [17] found a way to explain all the violations of the Hasse principle known at his time via what is now known as the **Brauer-Manin obstruction**. Manin's construction uses the Brauer group $\mathrm{Br}(X)$ of X. This group can be defined in terms of equivalences classes of Azumaya algebras over X, but when X is smooth and projective (which will be our case throughout this minicourse) it is also naturally isomorphic to the étale cohomology group $H^2(X, \mathbb{G}_m)$. Given an adelic point $(x_v) \in X(\mathbb{A}_k) = \prod_v X(k_v)$ and an element $\beta \in \mathrm{Br}(X)$, we can restrict β along $x_v : \mathrm{spec}(k_v) \longrightarrow X$ for each place v to obtain a Brauer element $x_v^*\beta \in \mathrm{Br}(k_v)$. Local class field theory then tells us that there are canonical isomorphisms $\mathrm{inv}_v : \mathrm{Br}(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z}$ which fit in a short exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\Sigma \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0\ . \tag{1.1}$$

We may then consider the pairing

$$\begin{aligned} X(\mathbb{A}_k) \times \mathrm{Br}(k) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ ((x_v), \beta) &\longmapsto \textstyle\sum_v \mathrm{inv}_v\, x_v^*\beta. \end{aligned} \tag{1.2}$$

We note that the sum above is well-defined because for a given $\beta \in \mathrm{Br}(X)$ there exists a finite set of places S such that $x_v^*\beta = 0$ for every $v \notin S$ and every $x_v \in X(k_v)$. In particular, by the exactness of (1.1) we get that if (x_v) is the image of a rational point $x \in X(k)$ under the diagonal embedding $X(k) \longrightarrow X(\mathbb{A}_k)$ then $\sum_v \mathrm{inv}_v\, x_v^*\beta \in \mathbb{Q}/\mathbb{Z}$ must vanish for every $\beta \in \mathrm{Br}(X)$, and hence that (x_v) belongs in that case to the left kernel of the pairing (1.2). This left kernel is known as the **Brauer set** of X, and is denote by $X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k)$. When $X(\mathbb{A}_k) \neq \varnothing$ but $X(\mathbb{A}_k)^{\mathrm{Br}} = \varnothing$ we say that there is a **Brauer–Manin obstruction to the Hasse principle** on X.

The question of existence of rational points can then be essentially reduced to the following:

Question 1.1. *For which geometric types of varieties the Brauer–Manin obstruction is the only obstruction to the Hasse principle?*

The term "geometric types" appearing in Question 1.1 is somewhat vague. It can be given however the following precise meaning. First, it can be shown that the

answer to Question 1.1 is a k**-birational invariant** of smooth, projective integral varieties. In other words, if X and Y are two such varieties and X is k-birational to Y (that is, X and Y have isomorphic function fields) then the answer to Question 1.1 is positive for X if and only if it is positive for Y. We may hence consider this property as a property of an integral k-birational equivalence class (that is as a property of finitely presented fields over k). We may then understand "geometric type" as referring to an integral $\overline{k}$-birational class, where $\overline{k}$ is an algebraic closure of k. It is hence natural to phrase Question 1.1 in the following more precise formalism:

Question 1.2. *Which integral $\overline{k}$-birational equivalence classes $\mathcal{M}$ have the property that the Brauer–Manin obstruction is the only obstruction to the Hasse principle for every k-birational equivalence class contained in $\mathcal{M}$?*

The simplest kind of a $\overline{k}$-birational equivalence class for which we can consider Question (1.2) is the class of (geometrically) rational varieties, that is, varieties which are birational over $\overline{k}$ to projective space $\mathbb{P}^n$. In this case the answer is conjecturally positive:

Conjecture 1.3 (Colliot-Thélène–Sansuc)**.** *If X is a smooth, proper, integral variety which is $\overline{k}$-birational to $\mathbb{P}^n$ then $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \varnothing \Rightarrow X(k) \neq \varnothing$.*

Conjecture 1.3 is known, for example, in the following cases:

Examples 1.4.

(1) If X is actually $\overline{k}$-isomorphic to $\mathbb{P}^n$ (such varieties are known as **Brauer-Severi** varieties).
(2) If $X \subseteq \mathbb{P}^{n+1}$ is a smooth quadric. This is the Hasse–Minkowski theorem.
(3) If X is a k-birational to a torsor under an algebraic k-torus T (Voskresenskii [31]). Furthermore, such a variety is k-birational to T itself as soon as it has a rational point. In particular, in the latter case rational points are Zariski dense.

Remark 1.5. The list above is by no means exhaustive. It is meant to give a preliminary idea of varieties for which a positive answer to Conjecture 1.3 is classically known without digressing to much from our main topic. We will see more known cases in §3 below. In a similar vein, the statement of Conjecture 1.3 was actually conjectured by Colliot-Thélène to hold for more general birational equivalence classes, namely, for all **rationally connected varieties**. For curves and surfaces, however, which will be our main concern in this minicourse, the property of being rationally connected coincides with being rational (over $\overline{k}$).

We note that the interest in answering such a question is two-fold. On the one hand, we wish to have a better conceptual understanding of the geometric, algebraic and arithmetic properties of X which control the existence of rational points. On the other hand, when the Brauer group $\mathrm{Br}(X)$ is finite, the question of whether or not $\mathrm{Br}(\mathbb{A}_k)^{\mathrm{Br}}$ is empty is in principle finitely determinable. In particular, if we know that for a certain geometric type of varieties the Brauer-Manin obstruction is the only obstruction to the Hasse principle, and we know that the Brauer group is finite for varieties of this class, then we have an explicit and straightforward receipt to determine the existence of a rational point on any given instance X of this family. This can yield applications, for example, in cases where X is a variety

whose rational points parameterize some interesting mathematical structures. For example, if K/k is a finite extension and we have an element $a \in k^*$ then we can ask if a is a norm from K. This can be encoded by the existence of a rational point on certain quasi-projective algebraic variety V, which is a torsor under an algebraic torus T (whose rational points correspond to elements of norm 1 in K). The existence of rational points on any smooth compactification of V is controlled by the Brauer–Manin obstruction by Example (3) above. In addition, the Brauer group of such a compactification is finite. The determination of whether X has rational points (in which case V has rational points as well) the becomes a finite procedure involving points of norm a in the completions of K at finitely many places and a certain explicitly computable finite Brauer group.

It is now known that the Brauer–Manin obstruction does not account for all violations of the Hasse principle: there exists smooth projective varieties X for which $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \varnothing$ but $X(k) = \varnothing$. Most of these examples are based on the fact that X has a non-abelian fundamental group, in which case one can often still explain the violation of the Hasse principle by construction a certain intermediate set

$$X(k) \subseteq X(\mathbb{A}_k)^{\text{ét,Br}} \subseteq X(\mathbb{A}_k)^{\mathrm{Br}},$$

defined by considering the Brauer sets of all finite étale covers of X (see [24]). When $\subseteq X(\mathbb{A}_k)^{\text{ét,Br}} = \varnothing$ one says that there is an **étale Brauer–Manin** obstruction to the existence of rational points. In 2001 Poonen [20] constructed the first known example of a smooth projective variety X for which $X(\mathbb{A}_k)^{\text{ét,Br}} \neq \varnothing$ but $X(k) = \varnothing$. Since then several other examples have been constructed (see [13], [9]).

2. Curves

Let us now discuss Question 1.1 in the case where X is a (smooth, projective, geometrically integral) **curve**. In this case the fundamental geometric invariant of X is its **genus** g. If X is defined over the complex numbers then the space of complex points $X(\mathbb{C})$ is homeomorphic to a "donut" with g handles. In particular, if $g = 0$ then $X(\mathbb{C})$ is a sphere and if $g = 1$ then $X(\mathbb{C})$ is a torus.

The genus, which is essentially a geometric invariant, also dramatically effects the behavior of rational points on X when X is defined over a number field k:

Theorem 2.1. *Let X be a smooth projective curve of genus g defined over k. If $g = 0$ then X has a rational point as soon as it has a point everywhere locally. In addition, in the latter case X is k-isomorphic to $\mathbb{P}^1_k$ and has infinitely many rational points. If $g = 1$ then X may violate the Hasse principle and may have finitely or infinitely many rational points. If $g \geq 2$ then X may violate the Hasse principle and $X(k)$ is always finite.*

It is not known whether the Brauer–Manin obstruction is the only obstruction to the Hasse principle on curves, though many authors conjecture this to be the case, or that at least, the étale Brauer–Manin obstruction is sufficient (see, e.g., [27]). When $g = 1$ this is related to another conjecture, which has become standard: the finiteness of the Tate-Shafarevich group of elliptic curves. Let us describe this case in more details. Recall that:

Definition 2.2. An **elliptic curve** over k is smooth, projective geometrically integral curve E/k of genus 1, equipped with a base point $e \in E(k)$.

Given an elliptic curve (E, e), there is a canonically defined multiplication operation $E \times E \longrightarrow E$ which endows E with the structure of **commutative algebraic group** with $e : \mathrm{spec}(k) \longrightarrow E$ as the unit. In fact, every smooth projective connected algebraic group of dimension 1 is an elliptic curve. Now suppose that X is a smooth projective curve of genus 1. Then X is does not necessarily carry a rational point, and hence cannot in general be given the structure of an elliptic curve. However, there is always a canonically associated elliptic curve $J(X)$, known as the **Jacobian** of X, which acts on X in free and transitive manner.

To construct $J(X)$ let hence take X to be any smooth projective geometrically integral curve (of arbitrary genus). We first define the **Picard scheme** of X. Given a field K containing k let us denote by X_K the base change of X from k to K. Then for each K/k we may consider the Picard group $\mathrm{Pic}(X_K)$ of X_K defined as the quotient of the group of zero-cycles on X defined over K, modulu those divisors which are the zeros of rational functions defined over K. Here by a zero-cycle defined over K we mean a formal combination of points $z := \sum_i a_i x_i$ where $a_i \in \mathbb{Z}$ and the x_i's are defined over some Galois extension L/K such that z is $\mathrm{Gal}(L/K)$-invariant as a linear combination. One can then prove that the étale sheafification of the functor $K \mapsto \mathrm{Pic}(X_K)$ is represented by a group scheme $\mathcal{P}\mathrm{ic}(X)$ defined over k. The degree map $\sum_i a_i x_i \mapsto \sum_i a_i \in \mathbb{Z}$ then descends to a homomorphism $\mathcal{P}\mathrm{ic}(X) \longrightarrow \mathbb{Z}$ whose kernel $\mathcal{P}\mathrm{ic}^0(X)$ is a connected algebraic group. This algebraic group is in fact an elliptic curve $J(X) = \mathcal{P}\mathrm{ic}^0(X)$, which we call the Jacobian of X. Each point x on X can be considered as a zero-cycle of degree 1 (defined over the same field as x). This determined a map $X \longrightarrow \mathcal{P}\mathrm{ic}(X)$ whose image is contained in the component $\mathcal{P}\mathrm{ic}^1(X)$ of divisor classes of degree 1.

In general $\mathcal{P}\mathrm{ic}^0(X)$ is a an abelian variety (that is, a commutative connected projective algebraic group) of dimension g. We now specialize again to the case where X has genus 1. In this case $\mathcal{P}\mathrm{ic}^0(X)$ is an elliptic curve, and one can show that the map $X \longrightarrow \mathcal{P}\mathrm{ic}(X)$ yields an **isomorphism** of k-varieties $X \cong \mathcal{P}\mathrm{ic}^1(X)$. We then have an associated action of $J(X) = \mathcal{P}\mathrm{ic}^0(X)$ on $X = \mathcal{P}\mathrm{ic}^1(X)$ simply by addition of zero-cycles, and this action is free and transitive. In other words, X is a **torsor** under $J(X)$. Such a torsor is trivial (equivalent as a torsor under $J(X)$ to $J(X)$ itself) if and only if it has a rational point. In particular, if we let $\overline{k}$ denote the algebraic closure of k then $X_{\overline{k}}$ is trivial as a torsor under $J(X)_{\overline{k}}$. The isomorphism types over k of such torsors can then be classified by the Galois cohomology group $H^1(k, J(X))$, where we consider $J(X)$ as a Galois module by taking the group of $\overline{k}$-points $J(X)(\overline{k})$. We may then consider the class $[X] \in H^1(k, J(X))$ which classifies X as a torsor under $J(X)$. The discussion so far then leads to the following important conclusion concerning the question of rational points on X:

$(*)$ The curve X has a rational points if and only if $[X] = 0 \in H^1(k, J(X))$.

The conclusion $(*)$ is quite striking: it means that there is a purely algebraic criteria for X to have a rational point. On the other hand, the group $H^1(k, J(X))$ is generally infinite, and we usually cannot compute it entirely. We now recall that in the setting of determining the existence of rational points, we may as well assume that local points exists at every place v of k. In this case, the torsor X becomes trivial when scalars are extended to any completion k_v, which means that $[X] \in H^1(k, J(X))$ is a class whose image in $H^1(k_v, J(X))$ is zero for any place v. The subgroup of such elements plays a very important role in the arithmetic of elliptic curves:

Definition 2.3. Let E be an elliptic curve. The **Tate-Shafarevich** group of E is defined to be the kernel:

$$Ш(E) \coloneqq \mathrm{Ker}[H^1(k,E) \longrightarrow \prod_v H^1(k_v,E)].$$

In particular, if X is a curve of genus 1 which has points everywhere locally then the class $[X] \in H^1(k,J(X))$ lies in $Ш(J(X))$. The following is one of the most important conjectures in the arithmetic of elliptic curves:

Conjecture 2.4. *The Tate-Shafarevich group* $Ш(E)$ *is finite for any elliptic curve* E*.*

Assuming conjecture 2.4, we may envision the following finite procedure to determine if a curve X of genus 1 has rational points. We first determine if it has points everywhere locally. If not, it does not have a rational point. If X has points everywhere locally, then we compute the finite group $Ш(J(X))$ and compute the element $[X] \in Ш(J(X))$ in this finite group. If $[X] = 0$ then X has rational points, and otherwise $X(k) = \varnothing$.

Let us explain how the above approach is related to the Brauer–Manin obstruction. By a theorem of Grothendieck we have that $\mathrm{Br}(X_{\overline{k}}) = 0$, that is, the Brauer group of X vanishes when passing to the algebraic closure of k. In addition, since we assume that X has points everywhere locally the map $\mathrm{Br}(k) \longrightarrow \mathrm{Br}(X)$ is injective. The **Hochschild–Serre spectral sequence** then yields a natural isomorphism

$$\mathrm{Br}(X)/\mathrm{Br}(k) \longrightarrow H^1(k,\mathcal{P}\mathrm{ic}(X)).$$

Let us set $E \coloneqq J(X)$. The group $H^1(k,\mathcal{P}\mathrm{ic}(X))$ sits in an exact sequence

$$\mathbb{Z} = H^0(k,\mathbb{Z}) \longrightarrow H^1(k,E) \longrightarrow H^1(k,\mathcal{P}\mathrm{ic}(X)) \longrightarrow H^1(k,\mathbb{Z}) = 0,$$

where the first map sends the generator of $\mathbb{Z}$ to the class $[X] \in H^1(k,E)$. In particular, we may identify $H^1(k,\mathcal{P}\mathrm{ic}(X))$ with the quotient of $H^1(k,E)$ by the subgroup generated by the class $[X] \in H^1(k,E)$. Let us write $\rho : Ш(E) \longrightarrow \mathrm{Br}(X)/\mathrm{Br}(k)$ for the composed map

$$Ш(E) \longrightarrow H^1(k,E) \longrightarrow H^1(k,\mathcal{P}\mathrm{ic}(X)) \cong \mathrm{Br}(X)/\mathrm{Br}(k),$$

so that the kernel of ρ is spanned by $[X] \in Ш(E)$. We will denote by $Б(X) \subseteq \mathrm{Br}(X)$ the preimage in $\mathrm{Br}(X)$ of $\rho(Ш(E)) \subseteq \mathrm{Br}(X)/\mathrm{Br}(k)$. We note that $Б(X)$ can equivalently by described as the subgroup of $\mathrm{Br}(X)$ consisting of those elements whose image in $\mathrm{Br}(X_{k_v})$ comes from $\mathrm{Br}(k_v)$ for every place v. Such Brauer elements are also called **locally constant elements**.

Now let $(x_v) \in X(\mathbb{A}_k)$ be an adelic point and let $\alpha \in Ш(E)$ be a class. Let $\beta \in Б(X)$ be a locally constant Brauer element whose image in $\mathrm{Br}(X)/\mathrm{Br}(k)$ is $\rho(\alpha)$. Then the pullback $x_v^*\beta \in \mathrm{Br}(k_v)$ does not depend on x_v: indeed, the image of α in $H^1(k_v,E)$ is zero, and hence the image of β in $\mathrm{Br}(X_{k_v})$ comes from some $\beta_v \in \mathrm{Br}(k_v)$, which means that $x_v^*\beta = \beta_v$ regardless of x_v. On the other hand, the sum $\mathrm{inv}_v\, x_v^*\beta$ does not depend on which β we chose, as long as its image in $\mathrm{Br}(X)/\mathrm{Br}(k)$ is $\rho(\alpha)$. Indeed, any two such β's differ by an element $\gamma \in \mathrm{Br}(k)$, and $\sum_v \mathrm{inv}_v\, \gamma = 0$. We may thus conclude that $\sum_v \mathrm{inv}_v\, x_v^*\beta$ depends only on X and α. In fact, it depends only on the isomorphism type of X as a torsor under E, and hence only on the class $[X] \in Ш(E)$.

Proposition 2.5. *The association* $([X],\alpha) \mapsto \sum_v \mathrm{inv}_v\, x_v^*\beta$ *determines a bilinear alternating pairing*

$$Ш(E) \times Ш(E) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

This pairing is known as the ***Cassels-Tate*** *pairing.*

Remark 2.6. The pairing of Proposition 2.5 was defined by Cassels in [3] (and later extended to general abelian varieties by Tate) in a different way without using the Brauer pairing. The identification of this pairing with the above formula was proven by Milne [19].

Theorem 2.7 (Cassels [3])**.** *An element in* $Ш(E)$ *is in the kernel of the Cassels-Tate pairing if and only if it is infinitely divisible in* $Ш(E)$*. In particular, if* $Ш(E)$ *is finite then the Cassels-Tate pairing is non-degenerate.*

We may summarize the situation as follows:

Corollary 2.8. *Let* X *be a curve of genus* 1 *which has points everywhere locally. Then the following conditions are equivalent:*

(1) X *contains an adelic point* $(x_v) \in X(\mathbb{A}_k)$ *which is orthogonal to* $Б(X)$ *with respect to* (1.2)*.*
(2) The class $[X] \in Ш(E)$ *is in the kernel of Cassels-Tate pairing.*
(3) The class $[X] \in Ш(E)$ *is infinitely divisible in* $Ш(E)$*.*

In addition, if $Ш(E)$ *is finite then the above conditions are also equivalent to the condition* $[X] = 0$*, that is, to the condition that* X *has rational points.*

The last part of Corollary 2.8 explains the importance of Conjecture 2.4 to the question of rational points on X: indeed, under Conjecture 2.4 a curve X of genus 1 has a rational point if and only if it has points everywhere locally and no Brauer–Manin obstruction. Furthermore, in this case only the subgroup $Б(X) \subseteq \mathrm{Br}(X)$, which is finitely generated over $\mathrm{Br}(k)$, needs to be taken into account. In particular, under Conjecture 2.4 the question of whether a curve of genus 1 has a rational point is finitely determinable.

Remark 2.9. The importance of Conjecture 2.4 goes beyond the question of rational points on genus 1 curves: it lies in the core of arithmetic duality theory for elliptic curves over number fields, and more generally, arithmetic duality for abelian varieties. It can be considered as a **standard conjecture**.

Let us finish this section by saying a few words about the case where X is a smooth projective of genus $g \geq 2$. In this case one can still define the Jacobien $J(X) = \mathcal{P}\mathrm{ic}^0(X)$ in the same manner, only that it will generally not be an elliptic curve, but rather an abelian variety, i.e., a commutative connected projective group of dimension g. Then X will certainly not be a torsor under $A := J(X)$, but $\mathcal{P}\mathrm{ic}^1(X)$ will still be, and so we may consider the class $[\mathcal{P}\mathrm{ic}^1(X)] \in H^1(k, A)$. If X has points everywhere locally then $[\mathcal{P}\mathrm{ic}^1(X)]$ will become trivial in $H^1(k_v, A)$ and so will belong to the group $Ш(A) \subseteq H^1(k, A)$ which we define in exactly the same manner as

$$Ш(A) := \mathrm{Ker}[H^1(k, A) \longrightarrow \prod_v H^1(k_v, A)].$$

A generalization of Conjecture 2.4 states that $Ш(A)$ is finite for any abelian variety over k. However, unlike the case of genus 1 curves, even if $[\mathcal{P}\mathrm{ic}^1(X)]$ vanishes in

$Ш(A)$, it does not follow in general that X has a rational point. As mentioned above, it is still believed by many authors that the Brauer–Manin obstruction is the only obstruction to the Hasse principle on X. Support for this conjecture is given by the following theorem of Scharaschkin:

Theorem 2.10 ([23])**.** *Let X be a curve of genus $g \geq 2$ such that $Ш(J(X))$ and $J(X)(k)$ are finite. Then X has rational points if and only if its Brauer set $X(\mathbb{A}_k)^{\mathrm{Br}}$ is non-empty.*

Remark 2.11. Unlike the case of Corollary 2.8, in the situation of Theorem 2.10 one does not expect to have a natural subgroup of $\mathrm{Br}(X)$ which is finitely generated over $\mathrm{Br}(k)$ and which is sufficient for determining the existence of rational points.

3. Conic bundle surfaces

3.1. **Preliminaries.** Let us now turn out attention to the case of surfaces. Let X be a smooth projective geometrically integral surface. What can we say about question 1.1 for X? As in the case of curves we may first classify surfaces according to their geometric invariants. In this case, instead of using the genus we will use **Kodaira dimension**. Given a smooth, projective geometrically integral variety X of dimension n, we denote by $\omega_X = \bigwedge^n \Omega_X$ the line bundle of differential n-forms on X, and we set $p_m = \dim H^0(X_{\overline{k}}, \omega_X^{\otimes m})$.

Definition 3.1. We define the **Kodaira dimension** $\kappa(X)$ to be $-\infty$ if $p_m = 0$ for $m >> 0$, and otherwise to be the smallest integer $k \geq 0$ such that p_m/m^k is bounded (as a function of m).

Remark 3.2. In the situation of Definition 3.1, if $\kappa(X) = -\infty$ then p_m must in fact vanish as soon as $m > 0$ (since we can tensor m sections of ω_X to obtain a section of $\omega_X^{\otimes m}$.

Remark 3.3. The Kodaira dimension $\kappa(X)$ is always smaller or equal to the dimension of X.

Remark 3.4. If X is a smooth projective curve of genus g then $\kappa(X) = -\infty$ if $g = 0$, $\kappa(X) = 0$ if $g = 1$ and $\kappa(X) = 1$ if $g \geq 2$.

For simplicity let us focus our attention on **simply connected surfaces**, that is geometrically integral surfaces which admit no finite unramified étale coverings. Classifying simply connected surfaces by their Kodaira dimension yields the following geometric classes of surfaces:

(1) Simply connected surfaces of Kodaira dimension $-\infty$ are exactly the **rational surfaces**, that is, the surfaces birationally equivalent over $\overline{k}$ to $\mathbb{P}^2$.
(2) Simply connected surfaces of Kodaira dimension 0 are known as **K3 surfaces**. They can equivalently be characterized as those simply connected surfaces for which ω_X is a trivial line bundle.
(3) Surfaces of Kodaira dimension 1 are all elliptic: they admit a dominant map (generally defined over $\overline{k}$) to $\mathbb{P}^1$ whose fibers are curves of genus 1. These are exactly the elliptic surfaces which are not rational and not K3 surfaces.
(4) Surfaces of Kodaira dimension 2 are knows as surfaces of **general type**. In some sense this class contains "most surfaces".

Rational surfaces can be considered as the surface analogue of curves of genus 0. Unlike curves of genus 0, rational surfaces may violate the Hasse principle. Nonetheless, as a particular case of Conjecture 1.3, we expect the Brauer–Manin obstruction to be the only one for the Hasse principle on rational surfaces.

In addition to the examples given in 1.4, a class of surfaces for which the Hasse principle and Brauer–Manin obstruction have been greatly studied is that of **conic bundles**. Recall that a conic bundle surface is a smooth projective geometrically integral surface X equipped with a surjective map $\pi : X \longrightarrow \mathbb{P}^1_k$ whose generic fiber a conic over the function field $k(\mathbb{P}^1_k)$. Such surfaces are always rational. If we consider $\mathbb{A}^1_k = \mathbb{P}^1_k \smallsetminus \{\infty\} \subseteq \mathbb{P}^1_k$ and we let t be a coordinate on $\mathbb{A}^1_k$ (so that $k[\mathbb{A}^1_k] = k[t]$ and $k(\mathbb{P}^1_k) = k(t)$), then the generic fiber of π is given by a conic

$$f(t)x^2 + g(t)y^2 + h(t)z^2 = 0 \tag{3.1}$$

over $k(t)$. Here we used the fact that over a field any quadratic form can be diagonalized. Clearing denominators we may assume that each of f, g, h lies in $k[t]$ (as apposed to $k(t)$) and that there is no polynomial $q \in k[t]$ of positive degree which simultaneously divides f, g and h. In addition, we can even assume that f, g, h are coprime in pairs: if $q \in k[t]$ of positive degree divides f, g (but not h) then we can divide (3.1) by q and make a coordinate change $z \mapsto \frac{z}{q}$ which multiplies h by q. In particular, we may assume that the polynomial $\Delta(t) = f(t)g(t)h(t)$ is separable. For every $t \in k$ such that $\Delta(t) \neq 0$ the fiber X_t of $\pi : X \longrightarrow \mathbb{P}^1_k$ over t is a smooth conic. Using a suitable coordinate change on t we can also make sure that the degrees of f, g, h all have the same parity. In this case the fiber X_∞ over $\infty \in \mathbb{P}^1_k$ is smooth as well. On the other hand, if K/k is a finite extension of k and $\tau \in K$ is such that $\Delta(\tau) = 0$ then the fiber X_τ is singular: for example, if $f(\tau) = 0$ then X_τ is given inside $\mathbb{P}^2_K$ by the equation

$$g(\tau)y^2 + h(\tau)z^2 = 0$$

which is a union of two smooth genus 0 curves defined over the quadratic extension $K(\sqrt{-h(\tau)/g(\tau)})$ and intersecting at a unique point $(x : y : z) = (1 : 0 : 0)$. Let $r = \deg(\Delta) = \deg(f) + \deg(g) + \deg(h)$ be the number of singular fibers (over $\overline{k}$). Conjecture 1.3 is known for X for small values of r:

(1) If $r \leq 3$ then X satisfies the Hasse principle and is k-rational as soon as it has a rational point.
(2) If $r = 4$ then X may violate the Hasse principle but the Brauer–Manin obstruction is the only obstruction to the Hasse principle. We can distinguish two possible cases. When $(\deg(f), \deg(g), \deg(h)) = (0, 0, 4)$ the surface X is also known as a **Châtelet surface**, and the result was proven by Colliot-Thélène, Sansuc and Swinnerton-Dyer in [7]. When $(\deg(f), \deg(g), \deg(h)) = (0, 2, 2)$ the surface X is a del Pezzo surface of degree 4 in which case the result was proven by Colliot-Thélène in [5], using a lot of the machinery developed in [7].
(3) If $r = 5$ then X is k-isomorphic to a smooth cubic surface which contains a rational line, and so $X(k) \neq \varnothing$.
(4) If $r = 6$ and we are in the case $(\deg(f), \deg(f), \deg(h)) = (0, 0, 6)$ with h a product of a degree 2 and a degree 4 polynomial then the Brauer–Manin is the only obstruction to the Hasse principle. This was proven by Swinnerton-Dyer in [29], see also [25, Theorem 7.4.1].

3.2. **The fibration method.** We now discuss a general method for proving that the Brauer–Manin obstruction is the only one for the Hasse principle on conic bundle surfaces, which is however conditional on a certain number theoretical conjecture – **Schinzel's hypothesis** (H) – which is a vast generalization of the twin prime conjecture. In its classical version it takes the following form:

Conjecture 3.5 (Hypothesis (H))**.** *Let $q_1, ..., q_m \in \mathbb{Z}[t]$ be pairwise coprime irreducible polynomials with integer coefficients. Suppose that for every prime p there exists a $t \in \mathbb{Z}$ such that $\prod_i q_i(t)$ is coprime to p. Then there exists infinitely many positive $t \in \mathbb{Z}$ such that $q_i(t)$ is prime for each $i = 1, ..., m$.*

Remark 3.6. When $m = 1$ Hypothesis (H) is equivalent to Dirichlet's theorem on primes in arithmetic progressions. This is the only known case of Hypothesis (H).

It was later realized by Serre that Hypothesis (H) is equivalent to the following, apparently much more general statement:

Conjecture 3.7 (Hypothesis (H_1))**.** *Let k be a number field and $q_1, ..., q_m \in k[t]$ be pairwise coprime irreducible polynomials. Let S a finite set of places of k containing all the archimedian places and large enough so that for every $v \notin S$ there exists a $t_v \in \mathcal{O}_v$ such that $\prod_i q_i(t_v)$ is a v-unit. Suppose given $t_v \in k_v$ for every finite $v \in S$. Then there exist S-integral elements $t \in k$ such that*

(1) t is arbitrarily close to t_v in the v-adic topology for each finite $v \in S$;
(2) for every real $v \in S$ the element t is positive and arbitrarily large in k_v;
(3) for every $i = 1, ..., m$ the element $q_i(t)$ is a unit outside S except at a single place $u_i \notin S$, in which $\mathrm{val}_{u_i}(q_i(t)) = 1$.

Remark 3.8. Given irreducible polynomials $q_1, ..., q_m$, there is always a large enough finite set of places S for which Hypothesis (H_1) is applicable.

Remark 3.9. In the situation of Hypothesis (H_1), if $q_1, ..., q_m$ are irreducible pairwise coprime polynomials and S is a finite set of places for which Hypothesis (H_1) applies, then the hypothesis also applies to any finite set of places S' containing S. Thus, by possibly enlarging S we may always assume that the $q_1, ..., q_m$ have S-integral coefficients and an S-unital leading coefficient and that the discriminant of $\prod_i q_i$ is an S-unit. This means that for every $v \notin S$ the reduction of $\prod_i q_i$ mod v is well-defined and is a separable polynomial of the same degree as $\prod_i q_i$. In particular, we may always assume that the places $u_1, ..., u_l$ are pairwise distinct.

Remark 3.10. When $m = 1$ Hypothesis (H_1) can be proven using the $m = 1$ case of Hypothesis (H), which is Dirichlet's theorem on primes in arithmetic progressions (see Remark 3.6). This is the only known case of Hypothesis (H_1).

Theorem 3.11. *Assume Schinzel's hypothesis* (H_1)*. Then the Brauer–Manin obstruction is the only obstruction for the Hasse principle on any conic bundle surface.*

Theorem 3.11 is proven using an approach which is known as the **fibration method**. To describe the argument, we will need to introduce some terminology. Let $q_1, ..., q_m$ be the irreducible factors of Δ, so that $\Delta = \prod_l q_l$. For each $l \in \{1, ..., m\}$, let us denote by $M_l \in \mathbb{A}^1_k$ the closed point corresponding to the ideal $(q_l) \subseteq k[t]$, and by $k_l := k[t]/q_i$ its residue field. Then the fiber X_{M_l} is singular and breaks as a union of two rational curves defined over a quadratic extension L_l/k_l and meeting at a point. Let $\tau_l \in k_l$ be a root of q_l and let $\gamma_l \in k_l$ be such that

$L_l = k_l(\gamma_l)$. We note that if, for example, $q_l | f$ then $\gamma_l = -h(\tau_l)/g(\tau_l)$ as above, and similarly if q_l divides g or h. For $l \in \{1, ..., m\}$ we will denote by

$$A_l := \mathrm{cores}_{k_l(t)/k(t)}(t - \tau_l, \gamma_l) \in \mathrm{Br}(k(t))$$

the corresponding Brauer element. Here $(t - \tau_l, \gamma_l) \in \mathrm{Br}(k_l(t))$ is the Brauer class of the quaternion algebra over $k_l(t)$ defined by $i^2 = t - \tau_l, j^2 = \gamma_l, ji = -ij$, and $\mathrm{cores}_{k_l(t)/k(t)}$ is the **corestriction** operation $\mathrm{Br}(k_l(t)) \longrightarrow \mathrm{Br}(k(t))$. We will denote by $\mathcal{B} \subseteq \mathrm{Br}(k(X))$ the subgroup generated by the inverse images $\pi^* A_l$ for $l \in \{1, ..., m\}$. We note that $\mathcal{B}$ is a finite subgroup.

The idea of the fibration method is that X is fibered over $\mathbb{P}^1_k$ into conics, and so the smooth fibers of $\mathbb{P}^1_k$ satisfy the Hasse principle by the Hasse–Minkowski theorem. We may then attempt to prove the existence of rational points on X by finding a $t \in k$ such that the fiber X_t has points everywhere locally. In particular, Theorem 3.11 will be a consequence of the following more precise statement:

Proposition 3.12. *Suppose that X contains an adelic point which is orthogonal to $\mathcal{B} \cap \mathrm{Br}(X) \subseteq \mathrm{Br}(k(X))$. Then there exists a $t \in k$ such that X_t has an adelic point, and hence also a rational point.*

Proof. Step 1. Let $(x_v) \in X(\mathbb{A}_k)$ be an adelic point which is orthogonal to $\mathcal{B} \cap \mathrm{Br}(X)$. Since $\mathcal{B} \cap \mathrm{Br}(X)$ is finite, we can always find a finite set of places S such that $\mathrm{inv}_v\, x_v^* \beta = 0$ for every $v \notin S$ and every $\beta \in \mathcal{B} \cap \mathrm{Br}(X)$. In light of Remark 3.8 we can also make sure that S is large enough so that Hypothesis (H_1) is applicable to S and the polynomials $q_1, ..., q_m$. We also make sure that S is large enough so that the properties described in Remark 3.9 hold.

For each $v \in S$ we now choose a small neighborhood $\mathcal{V}_v \subseteq \mathbb{P}^1(k_v)$ in the v-topology such that $X_t(k_v) \neq \varnothing$ for every $t \in \mathcal{V}_v$. By possibly replacing x_v with another point in $\pi^{-1}(\mathcal{V})$ which is sufficiently close to x_v we may assume that x_v does not lie on any of the singular fibers of π, nor on the fiber over ∞. Let $t_v = \pi(x_v)$ be the coordinate of $\pi(x_v)$. By possibly shrinking $\mathcal{V}_v$ we may then also assume that $\mathcal{V}_v$ does not contain ∞, that the fiber X_t is smooth for every $t \in \mathcal{V}_v$ and that $\mathrm{inv}_v\, A_l(t) = \mathrm{inv}_v\, A_l(t_v)$ for every $t \in \mathcal{V}_v$. Finally, by using weak approximation on $\mathbb{P}^1_k$ (which is the number field generalization of the Chinese remainder theorem) we can find a $t_0 \in k$ such that $t_0 \in \mathcal{V}_{v_\infty}$ for every real $v_\infty \in S$ and such that $t_0 \neq t_v$ for every nonarchimedean $v \in S$. By performing a coordinate change on $\mathbb{P}^1_k$ which sends t_0 to ∞ we may assume without loss of generality that the neighborhoods $\mathcal{V}_{v_\infty}$ contain a segment of the form $[a_{v_\infty}, \infty)$ for some $a_{v_\infty} < t_{v_\infty}$.

Step 2. The second step in the argument is an application of Harari's lemma, which is known as the "formal lemma". Let $U \subseteq X$ be the complement of the singular fibers and the fiber over $\infty \in \mathbb{P}^1_k$. Then the subgroup $\mathcal{B} \subseteq \mathrm{Br}(k(X))$ is contained in the subgroup $\mathrm{Br}(U) \subseteq \mathrm{Br}(k(X))$. Given the data we have of S and $x_v \in U(k_v)$ for $v \in S$ such that

$$\sum_{v \in S} \mathrm{inv}_v\, x_v^* \beta = 0$$

for every $\beta \in \mathcal{B} \cap \mathrm{Br}(X)$, the formal lemma provides us with a larger finite subset S' and new local points $x_v \in U(k_v)$ for $v \in S' \setminus S$ such that

$$\sum_{v \in S'} \mathrm{inv}_v\, x_v^* \beta = 0 \tag{3.2}$$

for every $\beta \in \mathcal{B}$. Setting $t_v = \pi(x_v)$ for $v \in S'$ we then get by the definition of $\mathcal{B}$ that

$$\sum_{v \in S'} A_l(t_v) = 0 \tag{3.3}$$

for every $l \in \{1, ..., m\}$. Like we did for $v \in S$, we now choose neighborhoods $t_v \in \mathcal{V}_v \subseteq \mathbb{P}^1(k_v)$ for every $v \in S' \setminus S$ such that for every $t \in \mathcal{V}_v$ we have that X_t is smooth, has k_v-points, and $\mathrm{inv}_v A_l(t) = \mathrm{inv}_v A_l(t_v)$.

Step 3. Applying Hypothesis (H_1) we can find a $t_0 \in k$ such that $t_0 \in \mathcal{V}_v$ for every non-archimedean $v \in S$, $t_0 > a_{v_\infty}$ for every real $v \in S'$, and such that for every $l \in \{1, ..., m\}$, the element $q_l(t_0)$ is a unit outside S' except at a single place u_l for which $\mathrm{val}_{u_l}(q_l(t_0)) = 1$. By Remark 3.9 we may also assume that the u_l's are pairwise distinct. We now claim that X_{t_0} has points everywhere locally.

Indeed, for $v \in S'$ we have that $X_{t_0}(k_v) \neq$ since $t_0 \in \mathcal{V}_v$. We also note that if v is a place which does not belong to S' and is not one of the u_l's then $f(t_0), g(t_0)$ and $h(t_0)$ are all units at v and hence the conic X_{t_0} has a k_v-point. It is left to consider the case $v = u_l$ for some $l \in \{1, ..., m\}$. To fix ideas let us suppose that $q_l | f$, so that $\mathrm{val}_{u_l} f(t_0) = 1$ and $g(t_0), h(t_0)$ are units at u_l. In this case the conic (3.1) has a k_{u_l}-point if and only if $-\frac{h(t_0)}{g(t_0)}$ is a square mod u_l. Recall that we fixed a root $\tau_l \in k_l$ of q_l. By our choice of S (see Remark 3.9) the polynomial q_l has S'-integral coefficients and an S'-unital leading coefficient. It then follows that $\tau_l \in k_l$ is $S'(k_l)$-integral and $q_l(t_0) = c\,\mathrm{Norm}_{k_l/k}(t_0 - \tau_l)$ for some S'-unit c. Since $\mathrm{val}_{u_l}(q_l(t_0)) = 1$ there must exist a place $\widetilde{u}_l$ of k_l, of degree 1 over u_l, such that $\mathrm{val}_{\widetilde{u}_l}(t_0 - \tau_l) = 1$, and so mod $\widetilde{u}_l$ we have $\bar{t}_0 = \overline{\tau}_l \in \mathbb{F}_{\widetilde{u}_l} \cong \mathbb{F}_{u_l}$. It then follows that

$$-\frac{h(\bar{t}_0)}{g(\bar{t}_0)} = -\frac{h(\overline{\tau}_l)}{g(\overline{\tau}_l)} = \overline{\gamma}_l,$$

and so X_{t_0} has a k_{u_l}-point if and only if γ_l is a square mod $\widetilde{u}_l$. On the other hand, since $\mathrm{val}_{\widetilde{u}_l}(t_0 - \tau_l) = 1$ we get from the behavior of quaternion algebras over p-adic fields that γ_l is a square mod $\widetilde{u}_l$ if and only if $\mathrm{inv}_{\widetilde{u}_l}(t_0 - \tau_l, \gamma_l) = 0 \in \mathrm{Br}(k_{\widetilde{u}_l})$. Since $t_0 - \tau_l$ and γ_l are units at every place $w \neq \widetilde{u}_l$ of k_l which lies over u_l it follows that

$$\mathrm{inv}_{u_l} A_l(t_0) = \sum_{w | u_l} \mathrm{inv}_w(t_0 - \tau_l, \gamma_l) = \mathrm{inv}_{\widetilde{u}_l}(t_0 - \tau_l, \gamma_l).$$

To finish the proof it will hence suffice to verify that $\mathrm{inv}_{u_l} A_l(t_0) = 0$. We now note that by the exactness of (1.1) we have that

$$\sum_v \mathrm{inv}_v A_l(t_0) = 0 \tag{3.4}$$

and that $\mathrm{inv}_v A_l(t_0) = 0$ for any $v \notin S' \cup \{u_l\}$ since both $t_0 - \tau_l$ and γ_l are units outside the places of k_l lying over $S' \cup \{u_l\}$. In addition, for every place $v \in S'$ we have that $\mathrm{inv}_v A_l(t_0) = \mathrm{inv}_v A_l(t_v)$ since $t_0 \in \mathcal{V}_v$. It then follows from 3.3 that

$$\sum_{v \in S'} \mathrm{inv}_v A_l(t_0) = \sum_{v \in S'} \mathrm{inv}_v A_l(t_v) = 0. \tag{3.5}$$

Combining (3.4) and (3.5) we may conclude that $\mathrm{inv}_{u_l} A_l(t_0) = 0$ and hence $X_{t_0}(u_l) \neq \varnothing$, as desired. □

Theorem 3.11 gives a very attractive result but at the price of assuming a very difficult open conjecture. In their landmark paper [2], Browning, Matthiesen and Skorobogtov used recent substantial advancements in additive combinatorics to

unconditionally prove Theorem 3.11 in the the case where $k = \mathbb{Q}$ and the singular fibers of π all lie over rational points:

Theorem 3.13 (Browning–Matthiesen–Skorobogtov)**.** *Let $\pi : X \longrightarrow \mathbb{P}^1_k$ be a conic bundle surface over $\mathbb{Q}$ whose singular fibers are all defined over $\mathbb{Q}$. Then the Brauer–Manin obstruction is the only one for the Hasse principle on X.*

A slightly different approach to Theorem 3.13 was later suggested in [15], applying a similar type of additive combinatorics results. To explain the latter approach, we recall the following **homogeneous** variant of Hypothesis (H_1):

Conjecture 3.14 (Hypothesis (HH_1))**.** *Let k be a number field and $q_1, ..., q_m \in k[\lambda, \mu]$ be irreducible homogeneous polynomials. Let S be a finite set of places of k containing all the archimedian places and large enough so that for every $v \notin S$ there exist $\lambda_v, \mu_v \in \mathcal{O}_v$ such that $\prod_i q_i(\lambda_v, \mu_v)$ is a v-unit. Suppose given $\lambda_v, \mu_v \in k_v$ for every $v \in S$ such that $(\lambda_v, \mu_v) \neq (0, 0)$ when v is archimedean. Then there exist S-integral elements $\lambda_0, \mu_0 \in k$ such that*

(1) (λ_0, μ_0) is arbitrarily close to $(\lambda_v, \mu_v) \in k_v \times k_v$ in the v-adic topology for each finite $v \in S$;
(2) $(\lambda_0 : \mu_0)$ is arbitrarily close to $(\lambda_v : \mu_v) \in \mathbb{P}^1(k_v)$ in the v-adic topology for each archimedean $v \in S$;
(3) for every real $v \in S$ the element $\lambda_v\lambda_0 + \mu_v\mu_0$ is positive in k_v;
(4) for every $i = 1, ..., m$ the element $q_i(\lambda_0, \mu_0)$ is a unit outside S except at a single place $u_i \notin S$, in which $\mathrm{val}_{u_i}(q_i(\lambda_0, \mu_0)) = 1$.

Remarks 3.15.

(1) Remarks 3.8 and 3.9 apply just as well for Hypothesis (HH_1).
(2) Given a polynomial $q(t)$ in one variable we can always consider it as a homogeneous polynomial in two variables λ, μ by setting $q(\lambda, \mu) = \mu^{\deg(q)} q(\lambda/\mu)$. One can the show that Hypothesis (H_1) for a given set of irreducible polynomials $q_1, ..., q_l$ implies Hypothesis (HH_1) for their respective homogenizations.

Given irreducible coprime homogeneous polynomials $q_1, ...q_m$ let us denote by $r = \sum_l \deg(q_l)$. When $r = 1$ Hypothesis (H_1) can be proven by elementary methods and when $r = 2$ Hypothesis (H_1) can be proven using Dirichlet's theorem on primes in arithmetic progressions. When $r = 3$, $m = 1$ and $k = \mathbb{Q}$ Hypothesis (H_1) can be deduced from the work of Heath-Brown and Moroz on primes represented by binary cubic form, see [16]. However, the main breakthrough towards Hypothesis (HH_1) was obtained by the seminal work of Green, Tao and Ziegler (see [15] for a more detailed discussion), which gives Hypothesis (HH_1) over $\mathbb{Q}$ for a collection of **linear forms**:

Theorem 3.16 (Green–Tao–Ziegler)**.** *Hypothesis (HH_1) holds if $k = \mathbb{Q}$ and $\deg(q_i) = 1$ for every $i \in \{1, ..., m\}$.*

In order to deduce Theorem 3.13 from Theorem 3.16 one needs to perform the fibration argument described in the proof of Proposition 3.12 using Hypothesis (HH_1) instead of Hypothesis (H_1). The precise details are described in [15].

4. Elliptic surfaces

The results described in the previous section on conic bundle surfaces give important support to Conjecture 1.3. They provide, however, no information regarding Question 1.1 for surfaces which are not rational: indeed, all conic bundle surfaces are rational. Remaining in the realm of simply-connected surfaces, it is natural to wonder what one should expect with respect to Question 1.1 for the next type of surfaces in the classification described in §3.1: namely, the class of **K3 surfaces**. Very little is known about this question: we do not know of any example of a K3 surface which is a counter-example to the Hasse principle not explained by the Brauer–Manin obstruction, and the only cases where we can prove that the Brauer–Manin obstruction is the only one are conditional on open conjectures. These latter results are however precious: they yield the only clues concerning Question 1.1 for K3 surfaces, indicating that the answer might be yes. For this reason some authors have actually conjectured this to be the case.

These positive conditional results are all based on a method, originally invented by Swinnerton-Dyer [28] and later generalized and extended by Swinnerton-Dyer–Skorobogatov–Colliot-Thélène [8], Wittenberg [32], and Swinnerton-Dyer–Bender [1]. A variant of this method applicable to Kummer surfaces was constructed by Swinnerton-Dyer and Skorobogatov in [26], and later extended by Harpaz–Skorobogatov [14] and Harpaz [12]. We will discuss this variant in §5.

We will refer to this method as the **descent–fibration** method. Roughly speaking, we would like to generalize the argument of Proposition 3.12 from conic bundles, which are fibrations into curves of genus 0, to **elliptic bundles**, or fibrations $\pi : X \longrightarrow \mathbb{P}^1_k$ into curves of genus 1. We will refer to such bundles as **elliptic surfaces** (though we emphasize that we are not assuming that π admits a section defined over the base field). In trying to generalize the proof of Proposition 3.12 we immediately encounter a difficulty: the fibration method described in the proof of Proposition 3.12 gave us the possibility to find a rational point $t \in \mathbb{P}^1_k(k)$ such that the fiber X_t is smooth and has points everywhere locally. When the fibers were conics this was enough: a conic with points everywhere locally has a rational points. For genus 1 curves this is no longer the case. In order to continue further we will need use the theory of genus 1 curves described §2. In particular, the generic fiber X_η is a genus 1 curve over the function field $k(\eta) = k(t)$, and we may consider its Jacobien $E_\eta := J(X_\eta)$, which is an elliptic curve over $k(t)$. The curve E_η can then be extended to a smooth projective surface $E \longrightarrow \mathbb{P}^1_k$, which is fibered over $\mathbb{P}^1_k$ with generic fiber E_η. In this case it will also be true that for every $t \in \mathbb{P}^1_k(k)$ such that X_t is smooth the elliptic curve E_t will be canonically isomorphic to the Jacobian of X_t. In particular, if $t \in \mathbb{P}^1_k(k)$ is such that X_t has points everywhere locally then the class $[X_t] \in H^1(k, E_t)$ belongs to $Ш(E_t)$. We might then hope to find a t such that X_t is everywhere locally solvable and the Tate-Shafarevich group $Ш(E_t)$, or at least some subgroup of it which contains α_t, is trivial. In this case we could deduce that $[X_t] = 0$ and hence that the fiber X_t has a rational point. The descent–fibration method allows us to do exactly that, at the price of assuming two major conjectures:

(1) Schinzel's hypothesis (H_1), as in §3.2.
(2) The Tate-Shafarevich conjecture stating that $Ш(E)$ is finite for any elliptic curve E (or at least, for the elliptic curves which appear in the pencil $E \longrightarrow \mathbb{P}^1_k$).

Remark 4.1. In the Kummer surface variant of the method described in §5 Schinzel's hypothesis is not needed (in fact, it is needed in the only known case of Dirichlet's theorem).

Remark 4.2. In light of the discussion in §3.2 it is natural to wonder if one can replace Hypothesis (H_1) in the descent–fibration method by Hypothesis (HH_1), and thus remove the conditional dependence when $k = \mathbb{Q}$ and all singular fibers of π are defined over $\mathbb{Q}$. The answer is in fact positive: this is topic of current work in progress, which we may discuss if time permits.

In addition to providing a window to the arithmetic of K3 surfaces (as well as some types of elliptic surfaces of Kodaira dimension 1), the descent–fibration method can also be used to obtain (conditional) results on certain rational surfaces which are not covered by the results described in §3.2. Consider for example the simplest types of rational surfaces, the **del Pezzo surfaces**. These are by definition the surfaces X whose anti-canonical class $-K_X \in \mathrm{Pic}(X)$ is ample. The **degree** of del Pezzo surface is defined to be the self intersection number $d = (-K_X)\cdot(-K_X)$, and can take any value between 1 and 9. Over $\overline{k}$ a del Pezzo surface is either isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ (in which case its degree is 8) or is obtained by blowing up $\mathbb{P}^2_k$ at $9-d$ sufficiently general points. When $d \geq 7$ every such surface is birational over k to either a quadric or $\mathbb{P}^2$. Del Pezzo surfaces of degree 6 all satisfy the Hasse principle [4]. Del Pezzo surfaces of degree 5 always contain a rational point (Enrique, Swinnerton-Dyer). Unlike these cases, when $d \leq 4$ the Hasse principle can fail, and in some sense, these are the simplest types of counter-examples to the Hasse principle in the realm of surfaces. It is hence quite desirable from the point of view of Conjecture 1.3 to prove that the Brauer–Manin obstruction is the only obstruction to the Hasse principle on such del Pezzo surfaces. Despite a lot of effort that has gone to this question it remains open in general. The only cases one can successfully attack are those del Pezzo surfaces which admit a suitable type of a conic bundle structure, either when $d = 4$ by the work of Colliot-Thélène [5] or when the conic bundles are of the form of Theorem 3.13 (see [2] for some examples).

Generically, a del Pezzo surface of degree ≤ 6 is not k-birational to a conic bundle. By contrast, every del Pezzo surface is always k-birational to an elliptic surface. This is because a general member of the linear system associated to the anti-canonical class $-K_X$ is a curve of genus 1 by the adjunction formula. Since $-K_X$ is always defined over the base field one obtains that a del Pezzo surface of degree d is equipped with a canonical $\mathbb{P}^d_k$-family of curves of genus 1, such that a generic penceil in this family has exactly d base points. Choosing a generic pencil and blowing up the base points yields a k-birational equivalence to an elliptic surfaces. The case of del Pezzo surfaces of degree 4 was the original case handled by Swinnerton-Dyer in [28], where the method was first invented. The case considered in loc. cit. was that of del Pezzo surfaces of degree 4 defined inside $\mathbb{P}^4_k$ by the intersection of two **diagonal quadrics**. This leads to the type of elliptic fibrations for which the method was first developed in [28], and which we will describe in detail in §4.2. The method was later extended to cover more general del Pezzo surfaces in [1] (see also [6]), and eventually to cover all sufficiently general del Pezzo surfaces in the work of Wittenberg [32] (still conditional on the two conjectures above). To give an idea of the type of results one can obtain we give the following sample result from [32]. In what follows, for a del Pezzo surface of degree 4 given by the

intersection of two (not necessarily diagonal) quadrics $q_1(x_1,...,x_5) = q_2(x_1,...,x_5) = 0$ we denote by $f(t,s) = \det(tq_1 + sq_2)$ the associated characteristic polynomial.

Theorem 4.3 (Wittenberg)**.** *Assume Schinzel's hypothesis* (H_1) *and that the Tate–Shafarevich group of elliptic curves is finite. Let X be a del Pezzo surface of degree 4 with characteristic polynomial f. If the Galois group of f acts 3-transitively on its roots then the Hasse principle holds for X.*

Using an instance of the fibration method one can bootstrap Theorem 4.4 to obtain the following higher dimensional analogue:

Theorem 4.4 (Wittenberg)**.** *Assume Schinzel's hypothesis* (H_1) *and that the Tate–Shafarevich group of elliptic curves is finite. Then any smooth intersection of two quadrtics in $\mathbb{P}^n_k$ for $n \geq 5$ satisfies the Hasse principle.*

4.1. **Selmer groups and 2-coverings.** The method as we shall describe in §4.2 is designed to handle elliptic surfaces of a certain type. In order to explain this we will need to recall some notions regarding the notion of a **2-covering** of an elliptic curve. Until otherwise stated we may take the base field k to be arbitrary.

Definition 4.5. Let E be an elliptic curve. A **2-covering** of E is a smooth projective genus 1 curve X equipped with a finite étale map $X \longrightarrow E$ such that the induced map $J(X) \longrightarrow J(E) = E$ is surjective with kernel $J(X)[2]$.

Remark 4.6. In the situation of Definition 4.5 the map $J(X) \longrightarrow E$ induces an isomorphism $J(X)/J(X)[2] \cong E$. On the other hand, the multiplication by 2 map $J(X) \longrightarrow J(X)$ determines an isomorphism $J(X)/J(X)[2] \cong J(X)$. We hence see that any 2-covering of E is equipped with a canonical isomorphism of its Jacobian with E. Under this isomorphism the map $J(X) \longrightarrow E$ induced by p identifies with the multiplication by 2 map $E \xrightarrow{2} E$.

Warning 4.7. The terminology 2-covering might cause confusion: if $p : X \longrightarrow E$ is a 2-covering in the sense of Definition 4.5 then p is a finite étale map of degree 4, and not 2.

Consider the exact sequence of algebraic groups

$$0 \longrightarrow E[2] \longrightarrow E \xrightarrow{2} E \longrightarrow 0 \tag{4.1}$$

where $2 : E \longrightarrow E$ is the multiplication by 2 map and $E[2] \subseteq E$ is the subgroup of 2-torsion elements (which is a commutative algebraic group of dimension 0, so essentially a finite Galois module). The short exact sequence (4.1) induces a long exact sequence in Galois cohomology

$$\cdots \longrightarrow H^0(k,E) \longrightarrow H^1(k,E[2]) \longrightarrow H^1(k,E) \xrightarrow{2} H^1(k,E) \longrightarrow \cdots, \tag{4.2}$$

and so every 2-torsion element in $H^1(k,E)$ comes from an element of $H^1(k,E[2])$. Now suppose that $p : X \longrightarrow E$ is a 2-covering. Then $J(X) \cong E$ by remark 4.6 and hence X is a torsor under E classified by an element $[X] \in H^2(k,E)$. The induced map $p_* : H^1(k,E) \longrightarrow H^1(k,E)$ must then send $[X]$ to $[E] = 0$, and by Remark 4.6 this map is simply given by multiplication by 2. It then follows that $[X]$ is a 2-torsion element of $H^1(k,E)$, and hence comes from an element in $H^1(k,E[2])$ by the long exact sequence 4.2. Furthermore, the inverse image $Z_p := p^{-1}(e) \subseteq X$ is a 0-dimensional scheme which is becomes a torsor under $E[2]$ with respect to the action

restricted from the action of E. The class $[Z_p] \in H^1(k, E[2])$ which classifies this torsor is then sent to the class $[X]$ under the map $H^1(k, E[2]) \longrightarrow H^1(k, E)$. In other words, it's not just that $[X] \in H^1(k, E)$ is in principal liftable to $H^1(k, E[2])$, the 2-covering map $p : X \longrightarrow E$ determines a distinguished such lift. Furthermore, it can be shown that the association $p \mapsto [Z_p]$ determines a bijection between isomorphism types of 2-coverings of E (where an isomorphism of 2-coverings is an isomorphism of the underlying curves which commutes with the map to E) and cohomology classes $\alpha \in H^1(k, E[2])$.

Let us now focus on the case where the 2-torsion points of E are all defined over the base field k. An elliptic curve E of this form can always be given an affine equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \tag{4.3}$$

where $e_1, e_2, e_3 \in k$ are such that $(e_2 - e_1)(e_3 - e_2)(e_1 - e_3) \neq 0$. More precisely, E is a smooth projective model for the affine curve (4.3), and contains, in addition to the solutions (x, y) of (4.3), one addition point "at infinity" $e \in E$, which we take to be the base point. The 2-torsion points are then given by 2 together with the rational points $P_1 := (0, e_1), P_2 := (0, e_2), P_3 := (0, e_3)$ for which the y-coordinate vanishes. The group $E[2]$ can then be generated by any distinct two out of P_1, P_2, P_3, but in order to avoid breaking the symmetry we may think of $E[2]$ as generated by the three points P_1, P_2, P_3 under the relations $2P_1 = 2P_2 = 2P_3 = 0$ and $P_1 + P_2 + P_3 = 0$. Identifying $H^1(k, \mathbb{Z}/2) \cong H^1(k, \mu_2)$ with the group $k^*/(k^*)^2$ of non-zero elements mod squares we may use the above presentation of $E[2]$ to identify $H^1(k, E[2])$ with the group of triples of classes $([a_1], [a_2], [a_3])$ with $a_i \in k^*$ such that $a_1 a_2 a_3 \in (k^*)^2$ (here we use $[\bullet]$ to denote the class mod squares of an element in k^*). Given an $\alpha = ([a_1], [a_2], [a_3]) \in H^1(k, E[2])$, its image in $H^1(k, E)$ determines a curve X^α of genus 1 whose Jacobian is E. The curve X^α can be described via the explicit affine equations

$$a_1 u_1^2 = x - e_1 \qquad a_2 u_2^2 = x - e_2 \qquad a_3 u_3^2 = x - e_3. \tag{4.4}$$

in the variables u_1, u_2, u_3, x. More precisely, X^α is a smooth projective model for the affine curve (4.4). An explicit such projective model can be written by introducing a new variable u_4 and eliminating x to obtain three homogeneous quadratic equations

$$\begin{array}{rcrcrcl} & & a_2 u_2^2 & - & a_3 u_3^2 & = & (e_3 - e_2) u_4^2 \\ -a_1 u_1^2 & + & & & a_3 u_3^2 & = & (e_1 - e_3) u_4^2 \\ a_1 u_1^2 & - & a_2 u_2^2 & & & = & (e_2 - e_1) u_4^2 \end{array} \tag{4.5}$$

any two of which are linearly independent (but not all three). Considering u_1, u_2, u_3, u_4 as homogeneous coordinates on $\mathbb{P}^3_k$ we now obtain an embedding of X^α in $\mathbb{P}^3_k$ as the intersection of two diagonal quadrics. Conversely, suppose that $X \subseteq \mathbb{P}^3_k$ is a curve given by the smooth intersection of two diagonal quadrics

$$\sum_{i=1}^{4} b_i u_i^2 = \sum_{i=1}^{4} c_i u_i^2 = 0. \tag{4.6}$$

Define $\Delta_{i,j} = c_i b_j - b_i c_j$. Our assumption that X is smooth implies that $\Delta_{i,j} \neq 0$. We also note that the $\Delta_{i,j}$'s always satisfy the identity

$$\Delta_{1,2}\Delta_{4,3} + \Delta_{2,3}\Delta_{4,1} + \Delta_{3,1}\Delta_{4,2} = 0. \tag{4.7}$$

Eliminating each of the variables u_1, u_2, u_3 in turn we obtain three linearly depend quadratic equations

$$\begin{array}{rcrcrcl} & & \Delta_{1,2}u_2^2 & - & \Delta_{3,1}u_3^2 & = & \Delta_{4,1}u_4^2 \\ -\Delta_{1,2}u_1^2 & + & & & \Delta_{2,3}u_3^2 & = & \Delta_{4,2}u_4^2 \\ \Delta_{3,1}u_1^2 & - & \Delta_{2,3}u_2^2 & & & = & \Delta_{4,3}u_4^2 \end{array} \tag{4.8}$$

each two of which are linearly independent. We now observe that the system (4.8) identifies with (4.5) if we set $a_i = -\Delta_{i,j}\Delta_{i,k}$ for every cyclic permutation (i,j,k) of $(1,2,3)$ and let e_1, e_2, e_3 be such that

$$e_2 - e_1 = \Delta_{1,2}\Delta_{4,3} \qquad e_3 - e_2 = \Delta_{2,3}\Delta_{4,1} \qquad e_1 - e_3 = \Delta_{3,1}\Delta_{4,2},$$

which is always possible in light of the identity (4.7). It follows that the Jacobian of X is given by the curve E of (4.3). We can summarize the discussion as follows: genus 1 curves of exponent 2 whose Jacobians have rational 2-torsion points are exactly the curves which can be written as smooth intersections of two diagonal quadrics in $\mathbb{P}^3$.

Let us now reinstate the assumption that k is a number field.

Definition 4.8. We define the **Selmer group** $\mathrm{Sel}(E)$ to be the subgroup of $H^1(k, E[2])$ consisting of those elements whose image in $H^1(k, E)$ belongs to $Ш(E)$.

The long exact sequence in Galois cohomology associated to (4.1) then induces a short exact sequence of the form

$$0 \longrightarrow E(k)/2E(k) \longrightarrow \mathrm{Sel}(E) \longrightarrow Ш(E)[2] \longrightarrow 0.$$

By the discussion above we see that $\mathrm{Sel}(E)$ classifies the isomorphism types of 2-coverings $p : X \longrightarrow E$ of E whose underlying curve X has points everywhere locally. The map $\mathrm{Sel}(E) \longrightarrow Ш(E)[2]$ then sends the isomorphism type of such a 2-covering to the underlying isomorphism type of X as a torsor under E.

The explicit construction above can be used to compute the Selmer group $\mathrm{Sel}(E)$ when E has all its 2-torsion points defined over k. In particular, given a triple $\alpha = ([a_1], [a_2], [a_3])$ and a place v of k, it is usually straightforward using valuation considerations and Hensel's lemma to check if the curve X^α given by the system of equations 4.5 has a k_v-point. Multiplying a_1, a_2, a_3 by squares we may assume, for example, that $0 \leq \mathrm{val}_v(a_i) \leq 1$, so that either all three a_i's are v-units or one of them is a v-unit and two of them have valuation 1. We note two cases which are particularly simple:

(1) If v is a place such that $e_j - e_i$ is a v-unit for every $i \neq j$ then E as good reduction at v. In this case the system of (4.5) has a k_v-point if and only if a_1, a_2, a_3 are all v-units. Indeed, we can assume that all the u_i's are v-integral and that at least one of them is a v-unit. Now if for example $\mathrm{val}_v(a_1) = \mathrm{val}_v(a_2) = 1$ then the first equation implies that u_4 must vanish mod v, and hence the last two equations imply that u_3 must vanish mod v. Then $\mathrm{val}_v(u_4^2) \geq 2$ and $\mathrm{val}_v(u_3^2) \geq 2$, so that

the last two equations imply that u_1 and u_2 must also vanish mod v. $a_3u_3^2$ must be equal to both $(e_2-e_3)u_4^2$ and $(e_1-e_3)u_4^2$ mod v and $(e_2-e_1)u_4^2$ must be vanish mod v - a contradiction.

(2) If v is a place such that $\mathrm{val}_v(e_1-e_2)=1$ and e_3-e_2, e_1-e_3 are v-units then (4.5) has a k_v-point if and only if either a_1,a_2,a_3 are all v-units and a_3 is a square mod v, or $\mathrm{val}_v(a_1)=\mathrm{val}_v(a_2)=1$ and $a_3(e_3-e_2)$ is a square mod v.

Let S be a finite set of places such that e_i-e_j is a unit outside S for every $i\neq j$. We then see by (1) above the Selmer group $\mathrm{Sel}(E)\subseteq H^1(k,E[2])$ is contained in the subgroup $H^1(\mathcal{O}_S,E[2])$, where $\mathcal{O}_S$ is the ring of S-integers. If furthermore $\mathrm{Pic}(\mathcal{O}_S)=0$ (equivalently, S contains a set of generators for the class group) then every element in $H^1(\mathcal{O}_S,E[2])$ can be represented by a triple of classes $([a_1],[a_2],[a_3])$ such that each a_i is an S-unit.

Remark 4.9. Since we assumed that the 2-torsion points of E are defined over k we map consider the images $\partial P_1,\partial P_2,\partial P_3\in\mathrm{Sel}(E)$ of P_1,P_2,P_3 via the map $\partial: E(k)\longrightarrow \mathrm{Sel}(E)$. These correspond to the triples

(4.9)

$$((e_1-e_2)(e_1-e_3),e_1-e_2,e_1-e_3)\quad (e_2-e_1,(e_2-e_1)(e_2-e_3),e_2-e_3)\quad (e_3-e_1,e_3-e_2,(e_3-e_1)(e_3-e_2)),$$

respectively.

In the course of the descent-fibration method described in the next section we will need to make use of another piece of structure. Recall that the 2-torsion of an elliptic curve are endowed with a canonical pairing

$$\langle\bullet,\bullet\rangle: E[2]\times E[2]\longrightarrow \mu_2,$$

known as the **Weil pairing**. This pairing is alternating and non-degenerate. In fact, since $E[2]\cong\mathbb{Z}/2\times\mathbb{Z}/2$ there is exactly one such pairing, which is the one such that

$$\langle P_1,P_2\rangle=\begin{cases}1 & P_1=P_2\\ -1 & P_1\neq P_2\end{cases}.$$

The Weil pairing induces a cup product pairing

$$\cup: H^1(k,E[2])\times H^1(k,E[2])\longrightarrow H^2(k,\mu_2), \tag{4.10}$$

which is known as the **Tate pairing**. The Tate pairing is also alternating, and has the following important property, which is part of local Tate duality for elliptic curves:

Proposition 4.10. *For every place v of k, the image $\partial(E(k_v))\subseteq H^1(k_v,E[2])$ is a maximal isotropic subspace of $H^1(k_v,E[2])$ with respect to the Tate pairing (of the base change to k_v). In particular, the Tate pairing of every two classes in* $\mathrm{Sel}(E)$ ***vanishes***.

Remark 4.11. In the case where the 2-torsion of E is defined over k and we represent classes in $H^1(k,E[2])$ by triples $([a_1],[a_2],[a_3])$ such that $a_1a_2a_3\in(k^*)^2$ then the Tate pairing of $\alpha=([a_1],[a_2],[a_3])$ and $\beta=([b_1],[b_2],[b_3])$ is given by either of the equivalent formulas

$$\alpha\cup\beta=[a_1]\cup[b_1]+[a_2]\cup[b_2]+[a_3]\cup[b_3]=$$
$$[a_1]\cup[b_2]+[a_2]\cup[b_1]=[a_1]\cup[b_3]+[a_3]\cup[b_1]=[a_2]\cup[b_3]+[a_3]\cup[b_2].$$

We finish this section by discussing another way in which genus 1 curves of exponent 2 can appear. Suppose that X is a curve of genus 1 and exponent 2. Recall that the **index** of X is the smallest degree of a Galois invariant divisor. The index is always divisible by the exponent, which is the smallest degree of a Galois invariant divisor class. In addition, by the explicit equations (4.6) it follows that any genus 1 curve of exponent 2 has index at most 4, and is hence either 2 or 4. When the index is 2 there is another type of explicit presentation one can use, and that we will employ in §5. This is obtained as follows. Suppose that D is a divisor on X of degree 2. Then D determines a linear system on X of dimension 2, which in turn determines a map $p : X \longrightarrow \mathbb{P}^1_k$ of degree 2. Such a map must be ramified at 4 points by the Euler formula. We may assume without loss of generality that $\infty \in \mathbb{P}^1_k$ is not one of the ramification points. Let $g(t)$ be a polynomial of degree 4 whose vanishing locus is the ramification locus of p. Then X admits an affine equation of the form

$$y^2 = g(t). \tag{4.11}$$

We can also obtain an explicit compactification by considering that homogenization $g(t,s)$ of g, and considering the curve in weighted projective space $\mathbb{P}^2(2,1,1)$ given by an equation of the form

$$y^2 = g(t,s),$$

where y has weight 2 and t,s have weight 1. We note that the Jacobian of the curve (4.11) is the elliptic curve

$$y^2 = f(t)$$

where f is the **resolvent cubic** of g. s

Remark 4.12. Using the Hasse principal on conics one can show that any curve of genus 1 and exponent 2 which has points everywhere locally is automatically of index 2. In particular, if we are only interested in curves of this type then we lose no generality in considering only curves of type (4.11). In the sections below we will be interested however not in individual genus 1 curves, but rather in pencils of such curves, i.e., in elliptic surfaces. The generic fiber of such a pencil is a genus 1 curve over the function field $k(t)$. In this case it is not true that every exponent 2 curve has index 2, even if the corresponding surface has points everywhere locally.

4.2. **The descent–fibration method.** In this section we will review the descent–fibration method as developed by Colliot-Thélène, Skorobogatov and Swinnerton-Dyer in [8]. The proof that we will give below is however different from the one given in [8], and is based on the approach of Wittenberg [32] (see also [33]). We will apply the method in order to study rational points on the following type of fibred surfaces:

Definition 4.13. A **diagonal biquadric surface** is a smooth, porjective, geometrically integral surface X, equipped with a surjective map $X \longrightarrow \mathbb{P}^1_k$ whose generic fiber X_η is a genus 1 curve given by a smooth intersection of two diagonal quadrics in $\mathbb{P}^3_{k(\eta)}$.

Examples 4.14.

(1) Let $X \subseteq \mathbb{P}^4$ be the smooth intersection of two diagonal quadrics

$$\sum_{i=1}^{5} a_i u_i^2 = \sum_{i=1}^{5} b_i u_i^2 = 0$$

with $a_i, b_i \in k$. Then X is a del Pezzo surface of degree 4. If we now cut X by the hyperplane $u_5 = tu_4$ then we get the curve in $\mathbb{P}^3$ given by

$$\sum_{i=1}^{3} a_i u_i^2 + (a_4 + t^2 a_5)u_4^2 = \sum_{i=1}^{3} b_i u_i^2 + (b_4 + t^2 b_5)u_4^2 = 0.$$

The family of hyperplace sections of the form $u_5 = tu_4$ has four base points which are the intersection of X with $u_4 = u_5 = 0$. Blowing up these four base point we now get a diagonal biquadric surface $\widetilde{X} \longrightarrow \mathbb{P}^1_k$. This was the original example to which Swinnerton-Dyer applied his method in [28].

(2) Let $X \subseteq \mathbb{P}^1 \times \mathbb{P}^3$ be the projective surface given by the smooth intersection of two equations of the form

$$\sum_{i=1}^{4} a_i(t,s)u_i^2 = \sum_{i=1}^{4} b_i(t,s)u_i^2 = 0 \tag{4.12}$$

where $a_i(t,s), b_i(t,s)$ are linear forms in t, s and $u_1, ..., u_4$ are projective coordinates on $\mathbb{P}^3$. Then X is a diagonal biquadric surface which is a particular case of a **K3 surface**.

(3) Let $X \subseteq \mathbb{P}^4$ be a surface given by a single diagonal quartic equation

$$\sum_{i=1}^{4} a_i x_i^4 = 0.$$

If $\prod_i a_i$ is a square in k then X admits a pencil of curves of genus 1 of the form (4.12). However, it is a rather special case of such a diagonal biquadric surface: the singular fibers of its Jacobian are not of type I_2, as happens in the generic case of (4.12), but of type I_4. The method as we elaborate below will not, strictly speaking, apply to this case, though a suitable variant of it will, see Swinnerton–Dyer [30].

Let us now fix a diagonal biquadric surface $X \longrightarrow \mathbb{P}^1_k$. As explained in §4.1, the generic fiber X_η is a 2-covering of its Jacobian E_η, and all the 2-torsion points of E_η are defined over $k(t)$. We may then write E_η by an equation of the form

$$y^2 = (x - f_1(t))(x - f_2(t))(x - f_3(t)), \tag{4.13}$$

with $f_1, f_2, f_3 \in k(t)$, and the isomorphism type of X_η as a 2-covering is classified by an element $\alpha \in H^1(k(t), E_\eta[2])$, which we shall henceforth consider as **fixed**. Applying a suitable variable change to (4.13) we may assume that f_1, f_2, f_3 belong to $k[t]$, and we denote

$$\Delta := (f_2 - f_1)(f_3 - f_2)(f_1 - f_3) \in k[t].$$

Let $\pi : E \longrightarrow \mathbb{P}^1_k$ be a smooth projective model for E_η. We will make the following assumption on f_1, f_2, f_3, Δ in order to have control on the bad fibers of π:

Assumption 4.15.

(1) There is no polynomial of positive degree which simultaneously divides f_1, f_2, f_3.
(2) The polynomials $f_2 - f_1, f_3 - f_2$ and $f_1 - f_3$ all have the same even degree d, and the polynomial Δ is separable.

Assumption 4.15 assures that $E \longrightarrow \mathbb{P}^1_k$ has a smooth fiber over $\infty \in \mathbb{P}^1_k$ and that the bad fibers of E are all of type I_2, that is, they are unions of two smooth curves of genus 0 which meet at two distinct points.

Let $U \subseteq \mathbb{A}^1$ be the complement of the singular locus $\Delta = 0$. As explained in §4.1, every $\beta \in H^1(k(t), E_\eta[2])$ determines a 2-covering of E_η, which can then be extended to diagonal biquadric surface $X^\beta \longrightarrow \mathbb{P}^1_k$ (uniquely up to k-birational equivalence).

Claim 4.16. *If $\beta \in H^1(k(t), E_\eta[2])$ is contained in $H^1(U, E[2]) \subseteq H^1(k(t), E_\eta[2])$ then X^β can be chosen so that its fibers over U are smooth genus 1 curves. On the other hand, if this is not the case then X^β must have at least one double fiber outside U.*

In light of Claim 4.16 we will allow ourselves to assume that our fixed element $\alpha \in H^1(k(t), E_\eta[2])$, which classifies the diagonal biquadric surface X we started from, lies in $H^1(U, E[2])$. We note that we may encode elements of $H^1(U, E[2])$ by triples $([p_1], [p_2], [p_3])$ where $p_i \in k[t]$ are non-zero square-free polynomials which do not vanish over U, $p_1p_2p_3$ is a square in $k[U]^*$ and $[\bullet]$ denotes the class in $k[U]^*/(k[U]^*)^2$. Let

$$\mathcal{G} \subseteq H^1(U, E[2]) \subseteq k[U]^*/(k[U]^*)^2 \times k[U]^*/(k[U]^*)^2 \times k[U]^*/(k[U)]^*)^2$$

be the subgroup consisting of the classes of those triples $([p_1], [p_2], [p_3])$ with $p_1p_2p_3$ a square for which p_i divides $(f_i - f_j)(f_i - f_k)$ for every cyclic permutation (i, j, k) of $(1, 2, 3)$. We will denote by $\mathcal{G}^{\text{even}} \subseteq \mathcal{G}$ the subgroup of elements which can be represented by triples $([p_1], [p_2], [p_3])$ for which furthermore $\deg(p_i)$ is even for $i = 1, 2, 3$.

Claim 4.17. *Let $\beta \in H^1(U, E[2])$ be an element. If $\beta \in \mathcal{G}$ then X^β can be chosen so that its fibers over each point in $\mathbb{A}^1_k \smallsetminus U$ have two geometric components, each a smooth conic, which intersect at two points. Otherwise X^β must have at least one double fiber over $\mathbb{A}^1_k \smallsetminus U$. In addition, if $\deg(p_i)$ is even for $i = 1, 2, 3$ then X^β can be chosen to have a smooth fiber at ∞. Otherwise, X^β has a double fiber at ∞.*

In light of Claim 4.17 we will allow ourselves to assume that $\alpha \in \mathcal{G}^{\text{even}}$.

Remark 4.18. The group $\mathcal{G}^{\text{even}}$ always contains the elements represented by the following three triples

(4.14)

$$((f_1-f_2)(f_1-f_3), f_1-f_2, f_1-f_3) \quad (f_2-f_1, (f_2-f_1)(f_2-f_3), f_2-f_3) \quad (f_3-f_1, f_3-f_2, (f_3-f_1)(f_3-f_2)).$$

These are the images of the non-trivial 2-torsion sections in $H^0(U, E)$ under the boundary map $H^0(U, E) \longrightarrow H^1(U, E[2])$. If $\beta \in \mathcal{G}^{\text{even}}$ is in this image then the associated 2-covering surface $X^\beta \longrightarrow \mathbb{P}^1$ is k-birational over $\mathbb{P}^1$ to E itself. We will hence generally assume that our fixed class α is **not** of the form (4.14).

We will denote by $q_1, ..., q_m$ the irreducible divisors of Δ in $k[t]$. For every $l \in \{1, ..., m\}$ we will denote by M_l the closed point of $\mathbb{A}^1_k$ corresponding to the prime ideal (q_l) of $k[t]$, by $k_l := k(M_l) = k[t]/q_l$ its residue field, and by $\tau_l \in k_l$ the coordinate of M_l (i.e., the image of t in $k[t]/q_l$).

Construction 4.19. Let $\beta \in \mathcal{G}$ be an element. Given $l \in \{1, ...m\}$ we will denote by L_l^β/k_l the (at most) quadratic extension over which the components of the singular fiber X_{M_l} are defined, and we let $\chi_l^\beta \in H^1(k_l, \mathbb{Z}/2) = k_l^*/(k_l^*)^2$ be the quadratic character corresponding to the extension L_l^β/k_l.

If $\beta \in \mathcal{G}^{\text{even}}$ is represented by a triple $([p_1],[p_2],[p_3])$, then, over U, we may write $X^\beta \times_{\mathbb{P}^1} U$ as the intersection of either two of the three linearly dependent quadrics:

$$\begin{array}{rcrcrcl} & & p_2(t)u_2^2 & - & p_3(t)u_3^2 & = & (f_3(t)-f_2(t))u_4^2 \\ -p_1(t)u_1^2 & + & & & p_3(t)u_3^2 & = & (f_1(t)-f_3(t))u_4^2 \\ p_1(t)u_1^2 & - & p_2(t)u_2^2 & & & = & (f_2(t)-f_1(t))u_4^2 \end{array} \tag{4.15}$$

Now if q_l is such that $q_l | f_1 - f_2$ then q_l either divides non of p_1, p_2, p_3, or it divides p_1 and p_2 but not p_3. In the first case we can use the last two equations in order to see that the fiber at q_l consists of two conics defined over the field $k_l(\sqrt{\gamma_l})$ where $\gamma_l = \frac{p_1(\tau_l)}{p_2(\tau_l)}$, which is equal to $p_3(\tau_l)$ mod squares. In the second case q_l divides exactly once all the coefficients of the last quadric, and so we can divide it by q_l. We can then use the second and (divided) third equations in order to see that the fiber aver q_l consists of two conics defined over the field $k_l(\sqrt{\gamma_l})$ with $\gamma_l = \frac{p_3(\tau_l)}{f_3(\tau_l)-f_1(\tau_l)}$. We may hence conclude that for every $l \in \{1,...,m\}$ and and cyclic permutation $\sigma = (i,j,k)$ of $(1,2,3)$ such that $q_l | f_j - f_k$ we have the formula

$$\chi_l^\beta = \begin{cases} [p_i(\tau_l)] & q_l | p_j, p_k \\ [p_i(\tau_l)(f_i(\tau_l) - f_j(\tau_l))] & \text{otherwise} \end{cases} \tag{4.16}$$

Remark 4.20. If $\beta, \beta' \in \mathcal{G}^{\text{even}}$ are such that $\beta - \beta'$ is one of the triples (4.14) then $\chi_l^\beta = \chi_l^{\beta'}$ for every $l \in \{1,...,m\}$. This can either be seen by inspecting the formula (4.16), or by arguing that the association $\beta \mapsto \chi_l^\beta$ is linear in β, and for a triple of the form (4.14) the associated fibred surface admits a section and hence its bad fibers all have a component defined over the base field.

Definition 4.21. Let $\beta \in \mathcal{G}$ be an element and let $X^\beta \longrightarrow \mathbb{P}^1_k$ be the corresponding diagonal biquadric surface with reduced fibers over $\mathbb{A}^1_k$. We will then denote by

$$A_l^\beta := \text{cores}_{k_l/k}(t - \tau_l, \chi_l^\beta) \in \text{Br}(k(t)).$$

We will denote by $\mathcal{B}_\beta \subseteq \text{Br}(X^\beta)$ the intersection of $\text{Br}(X^\beta)$ with the subgroup of $\text{Br}(k(X^\beta))$ generated by $\pi_\alpha^* A_l^\beta$ for $l = 1,...,m$.

Recall that we have fixed a class $\alpha \in \mathcal{G}^{\text{even}}$ which corresponds to the diagonal biquadric surface $X = X^\alpha$ we are interested in.

Definition 4.22. Let $\mathcal{G}_\alpha \subseteq \mathcal{G}$ denote the subgroup consisting of those $\beta \in \mathcal{G}$ which have the following property: for every $l \in \{1,...,m\}$ the element $\chi_l^\beta \in H^1(k_l, \mathbb{Z}/2)$ belongs to the subgroup generated by χ_l^α. We then let $\mathcal{G}_\alpha^{\text{even}}$ be the intersection $\mathcal{G}_\alpha^{\text{even}} := \mathcal{G}_\alpha \cap \mathcal{G}^{\text{even}}$.

Assumption 4.23 (Condition (D))**.** *The subgroup $\mathcal{G}_\alpha^{\text{even}} \subseteq \mathcal{G}^{\text{even}}$ is generated by α and the triples* (4.14)*.*

Given a $t \in \mathbb{P}^1_k(k)$ such that the fiber E_t is smooth we will denote by $\alpha_t \in H^1(k, E_t[2])$ the specialization of α. We may now formulate the main result of [8]:

Theorem 4.24 (Colliot-Thélène–Skorobogatov–Swinnerton-Dyer)**.** *Assume Hypothesis* (H_1) *and that the Tate-Shafarevich group of the smooth fibers of $\pi : E \longrightarrow$*

$\mathbb{P}^1$ *is finite. Let* $\alpha \in \mathcal{G}^{\mathrm{even}}$ *be a class which satisfies Condition (D) (Assumption 4.23). If the surface* X^α *contains an adelic point which is orthogonal to* $\mathcal{B}_\alpha$ *then there exists a* $t \in U(k)$ *such that* $\alpha_t \in \mathrm{Sel}(E_t)$ *and* $Ш(E_t)[2] = 0$. *In particular, the class* $[X^\alpha_t] \in Ш(E_t)[2]$ *vanishes and the fiber* X^α_t *contains a rational point.*

Example 4.25. Consider a degree 4 del Pezzo surface $X \subseteq \mathbb{P}^3_k$ given by the smooth intersection of two diagonal quadrics

$$\sum_{i=1}^{5} a_i u_i^2 = \sum_{i=1}^{5} b_i u_i^2 = 0$$

with $a_i, b_i \in k$. Let $d_{i,j} = a_i b_j - a_j b_j$. If none of $-d_{i,1}d_{i,5}$ is a square then the group $\mathcal{B}_\alpha \cap \mathrm{Br}(X)$ is just the image of $\mathrm{Br}(k)$. If in addition the classes of $-d_{2,3}d_{2,4}, -d_{3,2}d_{3,4}$ and $\prod_{i\neq 5} d_{i,5}$ are linearly independent in $k^*/(k^*)^2$ then Condition (D) holds. In particular, Theorem 4.24 applies in this case to show that under Hypothesis (H_1) and the Tate-Shafarevich conjecture for elliptic curves, the Hasse principle holds for X.

The strategy is based on the following fundamental idea:

Proposition 4.26. *Under the assumptions of Theorem 4.24, suppose that there exists a* $t \in U(k)$ *such that* $\mathrm{Sel}(E_t)$ *is generated by* α_t *and the image* $\partial(E_t[2]) \subseteq \mathrm{Sel}(E_t)$ *of the 2-torsion subgroup. Then* $Ш(E_t)[2] = 0$.

Proof. If $\mathrm{Sel}(E_t)$ is generated by α_t and $\partial(E_t[2]) \subseteq \mathrm{Sel}(E_t)$ then $Ш(E_t)[2]$ is generated by the image $[X^\alpha_t]$ of α_t, and is hence either trivial or cyclic of order 2. By assumption $Ш(E)$ is finite and is hence a direct sum of cyclic subgroups. Since its 2-torsion part is cyclic it follows that the 2-primary part of $Ш(E_t)$ is cyclic. Now since $Ш(E_t)$ is finite Theorem 2.7 tells us that the Cassels-Tate pairing is non-degenerate, and is hence also non-degenerate when restricted to the 2-primary part. On the other hand, it is also alternating. But a non-trivial cyclic subgroup cannot carry a non-degenerate alternating pairing. We conclude that the 2-primary part of $Ш(E_t)$ vanishes and in particular $Ш(E_t)[2] = 0$. □

In light of Proposition 4.26, to achieve Theorem 4.24 it will suffice to prove the following:

Proposition 4.27. *Under the assumptions of Theorem 4.24, there exists a* $t \in U(k)$ *such that* $\mathrm{Sel}(E_t)$ *is generated by* α_t *and the image* $\partial(E_t[2]) \subseteq \mathrm{Sel}(E_t)$ *of the 2-torsion subgroup.*

The remainder of this section is devoted to the proof of Proposition 4.27. Let S_0 be a finite set of places containing all the archimedean places, all the places above 2 and all the places of bad reduction for E or X^α. In addition, we will assume that S_0 is large enough so that all the polynomials $q_1, ..., q_m$ have S_0-integral coefficients and an S_0-unital leading coefficient, that the resultant of each pair q_i, q_j is an S_0-unit and that S_0 contains a set of generators for the class group of k. We will also assume that S_0 contains all the places of bad reduction of all the bad fibers of X^α (and so, in particular, all the places where at least one of the L^α_l's is ramified). Finally, we will assume as well that S_0 is large enough so that U admits an S_0-integral model $\mathcal{U}$ and $\pi : E \longrightarrow \mathbb{A}^1_k$ admits an S-integral model $\mathcal{E} \longrightarrow \mathbb{A}^1_{\mathcal{O}_S}$.

Definition 4.28. Let S be a finite set of places containing S_0. We will say that $t_0 \in U(k)$ is **S-admissible** if t_0 is S-integral and for every $l \in \{1, ..., m\}$ the element

$q_l(t_0)$ is a unit outside S except in a unique place $u_l^0 \notin S$ in which $\mathrm{val}_{u_l^0}(t_0) = 1$. We will then denote by $S(t_0) := S \cup \{u_1^0, ..., u_m^0\}$.

Remark 4.29. In the situation of Definition 4.28, our assumption on S_0 insures that for $v \notin S_0$ the polynomials $q_l, q_{l'}$ for $l \neq l'$ cannot have a common root mod v. In particular, the u_l's are necessarily pairwise distinct.

Definition 4.30. Let S be a finite set of places containing S_0. By a **suitable S-collection** of local points of X^α we will mean a point

$$(x_v)_{v\in S} \in \prod_{v\in S} X^\alpha(k_v)$$

in the product of the $X^\alpha(k_v)$, such that:

(1) for every $v \in S$ we have $\pi(k_v) \in U(k_v)$;
(2) for every $l \in \{1, ..., m\}$ we have $\sum_{v\in S} \mathrm{inv}_v A_l^\alpha(\pi(x_v)) = 0$.

Definition 4.31. Given a place v of k, we will denote by $\mathcal{G}_v \subseteq H^1(U_{k_v}, E[2])$ the subgroup consisting of the those triples $([p_1], [p_2], [p_3]) \in \left[k_v[U]^*/(k_v[U]^*)^2\right]^3$ with $p_1p_2p_3 \in (k_v[U]^*)^2$ for which p_i divides $(f_i - f_j)(f_i - f_k)$ in $k_v[t]$ for every cyclic permutation (i, j, k) of $(1, 2, 3)$. We note that the group $\mathcal{G}_v$ is contained in the finite group $H^1(U_{k_v}, E[2])$ and is hence finite.

Construction 4.32. Let S be a finite set of places containing S_0 and $x_S = (x_v)_{v\in S}$ a suitable S-collection of local points. Set $t_v = \pi(x_v)$ for $v \in S$. Then we may always find v-adic neighborhoods $t_v \in \mathcal{V}_v \subseteq k_v$ such that for every $t \in \mathcal{V}_v$ and every β in the finite group $\mathcal{G}_v$ the following holds:

(1) the fiber X_t^β is smooth and $X_t^\beta(k_v) \neq \emptyset$ if and only if $X_{t_v}^\beta(k_v) \neq \emptyset$.
(2) for every $l \in \{1, ..., m\}$ we have $\mathrm{inv}_v A_l^\beta(t) = \mathrm{inv}_v A_l^\beta(t_v)$.

In addition, as in the proof of Proposition 3.12, we can perform a variable change on $\mathbb{P}^1_k$ which insures that for every real $v_\infty \in S$ the neighborhood $\mathcal{V}_{v_\infty}$ contains a semi-infinite segment of the form (a_{v_∞}, ∞).

Definition 4.33. Let S be a finite set of places containing S_0, $x_S := (x_v)_{v\in S}$ a suitable S-collection of local points with $t_v = \pi(x_v) \in U(k_v)$ and $t \in U(k)$ a point. We will say that t **approximates** x_S if there exists neighborhoods $\mathcal{V}_v \subseteq k_v$ of the form described in Construction 4.32 such that $t \in \mathcal{V}_v$ for every $v \in S$.

Lemma 4.34. *Let S be a finite set of places containing S_0 and let $t_0 \in U(k)$ is an S-admissible point with associated places $\{u_1^0, ..., u_l^0\}$. Then for every $\beta \in \mathcal{G}$ and every $l \in \{1, ..., m\}$ we have that X_t^β has a $k_{u_l^0}$-point if and only if $\mathrm{inv}_{u_l^0} A_l^\beta(t_0) = 0$.*

Proof. We argue as in the proof of Proposition 3.12. We first note that X_t^β has a reduced special fiber at u_l^0 and the reduction of X_t^β mod u_l^0 is the same as the reduction of $X_{M_l}^\beta$ mod $\widetilde{u}_l^0$, where $\widetilde{u}_l^0$ is the unique place of k_l such that the reduction of t_l mod $\widetilde{u}_l^0$ coincides with the reduction of t_0 mod u_l^0 (such a place exists since $q_l(t_0)$ vanishes mod u_l^0 and $q_l(t_0)$ has no multiple roots mod u_l^0). In addition, the extension L_l^β/k_l is the minimal one which splits the fiber $X_{M_i}^\beta$ and each geometrically irreducible component of $X_{M_l}^\beta$ is a smooth conic with good reduction at u_l^0 (since $u_l^0 \notin S_0$) which hence a smooth $\mathbb{F}_{\widetilde{u}_l^0}$-point. It then follows

by Hensel's lemma that $X^{\beta}_{t_0}$ has a $k_{u_i^0}$-point if and only if the place $\widetilde{u}_l^0$ splits in L_l^{β}, which is equivalent $\mathrm{inv}_{\widetilde{u}_l^0}(t-\tau_l, \chi_l^{\beta}) = 0$. Since $t_0 - \tau_l$ and γ_l are units at every place $w \neq \widetilde{u}_l^0$ of k_l which lies over u_l^0 this in turn equivalent to the statement that $\mathrm{inv}_{u_l^0} A_l^{\beta}(t_0) = 0$. □

Lemma 4.35. *Let S be a finite set of places containing S_0, $x_S = (x_v)_{v\in S}$ a suitable S-collection of local points on X^{α} and t_0 an S-admissible point which approximates x_S. Then the fiber $X^{\alpha}_{t_0}$ has points everywhere locally.*

Proof. For $v \in S$ the fiber $X^{\alpha}_{t_0}$ has a k_v-point since t approximates x_S and $X^{\alpha}_{t_v}$ has a k_v point x_v. For $v \notin S \cup \{u_1^0, ..., u_m^0\}$ we have that X_t^{α} is a smooth projective curve of genus 1 with good reduction at v and hence has a k_v-point by the Hasse-Weil estimates. Finally, for $v = u_l^0$ with $l \in \{1, ..., m\}$ Lemma 4.34 tells us that we just need to check that $\mathrm{inv}_{u_l^0} A_l^{\alpha}(t_0) = 0$. But this follows from quadratic reciprocity which gives

$$\mathrm{inv}_{u_l^0} A_l^{\alpha}(t_0) = \sum_{v\in S} A_l^{\alpha}(t_0) = \sum_{v\in S} A_l^{\alpha}(t_v) = 0,$$

since t_0 approximates x_S. □

Proposition 4.36. *Let S be a finite set of places which contains S_0 and $t \in U(k)$ an S-admissible point. Then the specialization map*

$$\mathrm{ev}_{t_0} : H^1(\mathcal{U}_S, \mathcal{E}[2]) \longrightarrow H^1(\mathcal{O}_{S(t_0)}, E_{t_0}[2]) \tag{4.17}$$

is an isomorphism.

Definition 4.37. Let S be a finite set of places which contains S_0 and $t \in U(k)$ an S-admissible point. We will denote by $\mathrm{Sel}_{t_0}(\mathcal{E}) \subseteq H^1(\mathcal{U}_S, \mathcal{E}[2])$ the inverse image of $\mathrm{Sel}(E_{t_0}) \subseteq H^1(\mathcal{O}_{S(t_0)}, E_{t_0}[2])$ via the isomorphism (4.17).

Definition 4.38. Let S be a finite set of places containing S_0. We will denote by $\mathcal{G}_S \subseteq H^1(\mathcal{U}_S, \mathcal{E}[2])$ the intersection of $H^1(\mathcal{U}_S, \mathcal{E})$ and $\mathcal{G}$, that is, the subgroup consisting of those triples $([p_1], [p_2], [p_3]) \in [\mathcal{O}_S[\mathcal{U}]^*/(\mathcal{O}_S[\mathcal{U}]^*)^2]^3$ such that $p_i | f_j - f_k$ (in $k[t]$) for every cyclic permutation (i, j, k) of $(1, 2, 3)$. We will denote by $\mathcal{G}_S^{\mathrm{even}} := \mathcal{G}_S \cap \mathcal{G}^{\mathrm{even}} \subseteq \mathcal{G}_S$. We note that the groups $\mathcal{G}_S$ and $\mathcal{G}_S^{\mathrm{even}}$ are contained in the finite group $H^1(\mathcal{U}_S, \mathcal{E}[2])$, and are hence finite (as opposed to the groups $\mathcal{G}$ and $\mathcal{G}^{\mathrm{even}}$ above, which are infinite).

Lemma 4.39. *Let S be a finite set of places which contains S_0 and $t \in U(k)$ an S-admissible point. Then the subgroup $\mathrm{Sel}_{t_0} \subseteq H^1(\mathcal{U}_S, \mathcal{E}[2])$ is contained in the subgroup $\mathcal{G}_S \subseteq H^1(\mathcal{U}_S, \mathcal{E}[2])$.*

Proposition 4.40. *Assume Schinzel's Hypothesis* (H_1)*. Suppose that X^{α} contains an adelic point which is orthogonal to $\mathcal{B}_{\alpha} \subseteq \mathrm{Br}(X^{\alpha})$ (see Definition 4.21). Then there exists a finite set of places S containing S_0, a suitable S-collection of local points x_S and an S-admissible point $t_0 \in U(k)$ such that t_0 approximates x_S (and so the fiber $X^{\alpha}_{t_0}$ contains local points at every place of k by Lemma 4.35). In addition, we may choose t_0 in such a way that $\mathrm{Sel}_{t_0}(\mathcal{E}) \cap \mathcal{G}_{\alpha} \subseteq \mathcal{G}_S^{\mathrm{even}}$.*

Proof. By Harari's formal lemma there exists a finite set of places S_1 containing S_0 and a suitable S_1-collection of local points $x_{S_1} := (x_v)_{v\in S_0'}$ with $t_v = \pi(x_v) \in U(k_v)$ such that

$$\sum_{v\in S_1} \mathrm{inv}_v A_l^{\alpha}(t_v) = 0 \tag{4.18}$$

for every $l \in \{1,...,m\}$. Let w be a place not in S_1 which splits completely in L_l^α for every $l = 1,...,m$. Let $t_w \in k_w$ be an element such that $\mathrm{val}_w(t_w) = -1$. In this case we have in particular that $\Delta(t_w) \neq \emptyset$, i.e., the fibers E_{t_w} and $X_{t_w}^\alpha$ are smooth and so $X_{t_w}^\alpha(k_w) \neq \emptyset$. In addition, since w splits completely in L_l^α we have that $A_l^\alpha(t_w) = 0$ for every $l \in \{1,...,m\}$. Setting $S = S_1 \cup \{w\}$ and choosing a point $x_w \in X_{t_w}^\alpha(k_w)$ we may now extend our collection of local points to range over S. The resulting S-collection $x_S = (x_v)_{v\in S}$ is again suitable by construction. Applying Hypothesis (H_1) we may deduce the existence of an S-admissible point $t_0 \in U(k)$ which approximates x_S in the sense of Definition 4.33. The fiber $X_{t_0}^\alpha$ then has points everywhere locally by Lemma 4.35. In particular, α_{t_0} belongs to $\mathrm{Sel}_{t_0}(\mathcal{E})$. By requiring sufficient approximation at w we may also assume that the fiber E_{t_0} has good reduction at w.

Let us now show that $\mathrm{Set}_{t_0}(\mathcal{E}) \cap \mathcal{G}_\alpha$ belongs to $\mathcal{G}_\alpha^{\mathrm{even}}$. Suppose that $\gamma = ([p_1^\gamma],[p_2^\gamma],[p_3^\gamma]) \in \mathcal{G}_S$ belongs both to $\mathrm{Sel}_{t_0}(\mathcal{E})$ and $\mathcal{G}_\alpha$. Since the E_{t_0} has good reduction at w we must have that $\mathrm{val}_w\, p_i^\gamma(t_0)$ is even for $i = 1,2,3$. Since S_1 contains a set of generators for the class group we may find an element $a \in k$ such that $\mathrm{val}_w(a) = 1$ and a is a unit outside $S = S_1 \cup \{w\}$. We may then write p_i^γ up to squares as a product $ca^{\varepsilon^i}\prod_l q_l^{\varepsilon_l^i}$ with $\varepsilon^i, \varepsilon_l^i \in \{0,1\}$ and $c \in \mathcal{O}_{S_1}^*$. By our choice of t_w we have that $\mathrm{val}_w\, q_l(t_w) = -\deg(q_l)$ and so the condition that $\mathrm{val}_w\, p_i^\gamma(t_0)$ is even then implies that $\varepsilon^i + \sum_l \varepsilon_l^i$ is even. On the other hand, the condition that γ belongs to $\mathcal{G}_\alpha$ says that for every $l \in \{1,...,m\}$ the class $\chi_l^\gamma \in H^1(k_l, \mathbb{Z}/2)$ is in the subgroup generated by the class χ_l^α. In particular, this means that the quadratic character χ_l^γ is unramified outside S_0, and in particular over w. Since $f_i(\tau_l) - f_j(\tau_l)$ is a unit outside S_0 we may deduce from the explicit formula (4.16) that $\mathrm{val}_w\, p_i^\gamma(\tau_l)$ is even. Since $q_{l'}(\tau_l)$ is an S_0-unit this implies that ε^i must be even, and hence that $\deg(p_i^\gamma) = \sum_l \varepsilon_l^i$ is even, as desired. □

Let now S, x_S and t_0 be as in the conclusion of Proposition 4.40, and set $S(t_0) = S \cup \{u_1^0,...,u_l^0\}$ for the places associated to t_0 as an S-admissible point. In particular, we have $\alpha \in \mathrm{Sel}_{t_0}(\mathcal{E})$. Let $\beta \in \mathrm{Sel}_{t_0}(\mathcal{E})$ be another element. Let $w \notin S$ be a place of k and suppose there exists a $l_w \in \{1,...,m\}$ such that $q_{l_w} | f_j - f_k$ for some $\sigma = (i,j,k)$ and such that w splits completely in $L_{l_w}^\alpha$ but does not split completely in $L_{l_w}^\beta$. In particular, since w splits in k_{l_w} there exists a $t_w \in U(k_v)$ such that $\mathrm{val}_w\, q_{l_w}(t_w) = 1$ and we have

$$\mathrm{inv}_w\, A_{l_w}^\alpha(t_w) = 0 \qquad \mathrm{inv}_w\, A_{i_w}^\beta(t_w) \neq 0.$$

By Lemma 4.34 we have that $X_{t_w}^\alpha$ has a k_w-point $x_{k_w} \in X_{t_w}^\alpha(k_w)$, while $X_{t_w}^\beta(k_w) = \emptyset$. Let $S_w := S \cup \{w\}$ and let $x_{S_w} = (x_v)_{v\in S_w}$ be the suitable S_w-collection of local points obtained by adding x_w to x_S. Let t_1 be an S_w-admissible point which approximates x_{S_w} (such a point exists under Schinzel's hypothesis) and set $S(t_1) = S \cup \{u_1^1,...,u_l^1\}$. Our goal is to understand the relation between $\mathrm{Sel}_{t_0}(\mathcal{E})$ and $\mathrm{Sel}_{t_1}(\mathcal{E})$. More precisely, our goal is to prove the following:

Proposition 4.41. *We have an inclusion* $\mathrm{Sel}_{t_1}(\mathcal{E}) \subseteq \mathrm{Sel}_{t_0}(\mathcal{E})$ *of subgroups of* $H^1(\mathcal{U}_S, \mathcal{E})$. *In addition,* $\mathrm{Sel}_{t_1}(\mathcal{E})$ *contains* α *but not* β.

The proof of Proposition 4.41 will require the following lemma:

Lemma 4.42. *Let* $\gamma \in \mathcal{G}_S$ *be an element. Then the following holds:*

(1) *for every place* $v \notin \{u^0_1, ..., u^0_m, u^1_1, ..., u^1_m, w\}$ *we have that* $X^\gamma_{t_0}(k_v) \neq \varnothing$ *if and only if* $X^\gamma_{t_1}(k_v) \neq \varnothing$;
(2) *for every* $l \in \{1, ..., m\} \smallsetminus \{l_w\}$ *we have that* $X^\gamma_{t_0}(k_{u^0_l}) \neq \varnothing$ *if and only if* $X^\gamma_{t_1}(k_{u^1_l}) \neq \varnothing$;
(3) *the equality* $\mathrm{inv}_{u^0_{l_w}} A^\gamma_{l_w,\sigma}(t_0) = \mathrm{inv}_{u^1_{l_w}} A^\gamma_{l_w,\sigma}(t_1) + \mathrm{inv}_w A^\gamma_{l_w,\sigma}(t_1)$ *holds.*

In particular, if $\gamma \in \mathcal{G}_S \cap \mathrm{Sel}_{t_1}(\mathcal{E}) \subseteq \mathcal{G}_{S_w}$ *then* $\gamma \in \mathrm{Sel}_{t_0}(\mathcal{E})$.

Proof. If v is a place of S then

$$X^\gamma_{t_0}(k_v) \neq \varnothing \quad \Leftrightarrow \quad X^\gamma_{t_v}(k_v) \neq \varnothing \quad \Leftrightarrow \quad X^\gamma_{t_1}(k_v) \neq \varnothing$$

since both t_0 and t_1 approximate x_S. If v does not belong to $S(t_0) \cup S(t_1)$ then $X^\gamma_{t_0}$ and $X^\gamma_{t_1}$ are both smooth projective curve of genus 1 with good reduction at v, and so admit k_v-points. This proves (1).

To prove (2), suppose that $l \in \{1, ..., m\} \smallsetminus \{l_w\}$. We then have by Lemma 4.34 and quadratic reciprocity that

$$X^\gamma_{t_0}(k_{u^0_l}) \neq \varnothing \quad \Leftrightarrow \quad \mathrm{inv}_{u^0_l} A^\gamma_l(t_0) = 0 \quad \Leftrightarrow \quad \sum_{v \in S} \mathrm{inv}_v A^\gamma_l(t_0) = 0 \quad \Leftrightarrow$$

$$\sum_{v \in S} \mathrm{inv}_v A^\gamma_l(t_1) = 0 \quad \Leftrightarrow \quad \mathrm{inv}_{u^1_l} A^\gamma_l(t_1) = 0 \quad \Leftrightarrow \quad X^\gamma_{t_1}(k_{u^1_l}) \neq \varnothing,$$

as desired. Finally, to prove (3) we note that the same quadratic reciprocity argument gives

$$\mathrm{inv}_{u^0_{l_w}} A^\gamma_{l_w}(t_0) =$$

$$\sum_{v \in S} \mathrm{inv}_v A^\gamma_{l_w}(t_0) = \sum_{v \in S} \mathrm{inv}_v A^\gamma_{l_w}(t_1) =$$

$$\mathrm{inv}_{u^1_{l_w}} A^\gamma_{l_w}(t_1) + \mathrm{inv}_w A^\gamma_{l_w}(t_1) = 0,$$

and so the proof is complete. □

Proof of Proposition 4.41. Let $\gamma \in \mathrm{Sel}_{t_1}(\mathcal{E}) \subseteq \mathcal{G}_{S_w}$ be an element. We wish to show that γ belongs to $\mathrm{Sel}_{t_0}(\mathcal{E})$. We first claim that γ lies in $\mathcal{G}_S \subseteq \mathcal{G}_{S_w}$. Consider the **Tate pairing** (4.10)

$$b_{\beta,\gamma} := \mathrm{ev}_{t_1}(\beta) \cup \mathrm{ev}_{t_1}(\gamma) \in H^2(k, \mu_2) \subseteq \mathrm{Br}(k).$$

By Lemma 4.42 and Proposition 4.10 we have that $\mathrm{inv}_v b_{\beta,\gamma} = 0$ for every $v \neq u^1_{l_w}, w$ and hence by quadratic reciprocity we have that

$$\mathrm{inv}_{u^1_{l_w}} b_{\beta,\gamma} + \mathrm{inv}_w b_{\beta,\gamma} = 0.$$

Let us make the above expression more explicit. Suppose that β is represented by a triple $(p^\beta_1, p^\beta_2, p^\beta_3)$ and γ is represented by a triple $(p^\gamma_1, p^\gamma_2, p^\gamma_3)$. Let (i, j, k) be the unique cyclic permutation of $(1, 2, 3)$ such that $q_{l_w} | f_k - f_j$. We note that since $\beta \in \mathcal{G}_S$ we have that $p^\beta_i(t_1)$ is a unit at $u^1_{l_w}$ and w and since $\gamma \in \mathrm{Sel}_{t_1}(\mathcal{E})$ we have that $p^\gamma_i(t_1)$ is also a unit at $u^1_{l_w}$ and w. By possibly adding to β one of the triples (4.14) (see Remark 4.20) we may also assume that $p^\beta_j(t_1), p^\beta_k(t_1)$ are units at $u^1_{l_w}$ and w. Then for $v \in \{u^1_{l_w}, w\}$ we have

$$\mathrm{inv}_v b_{\beta,\gamma} = \left\langle p^\beta_i(t_1), p^\gamma_j(t_1) \right\rangle_v + \left\langle p^\beta_j(t_1), p^\gamma_i(t_1) \right\rangle_v = \mathrm{val}_v(p^\gamma_j(t_1)) \, \mathrm{inv}_v A^\beta_{l_w}(t_1) \in \mathbb{Z}/2$$

On the other hand, we have $\mathrm{inv}_w A^{\beta}_{l_w}(t_1) = 1$ by our choice of β and by Lemma 4.42(3) we have that

$$\mathrm{inv}_{u^1_{l_w}} A^{\beta}_{l_w}(t_1) + \mathrm{inv}_w A^{\beta}_{l_w}(t_1) = \mathrm{inv}_{u^0_{l_w}} A^{\beta}_{l_w}(t_0) = 0,$$

and so $\mathrm{inv}_{u^1_{l_w}} A^{\beta}_{l_w}(t_1) = 1$. Combining all the above we may now conclude that

$$0 = \mathrm{inv}_{u^1_{l_w}} b_{\beta,\gamma} + \mathrm{inv}_w b_{\beta,\gamma} = \mathrm{val}_{u^1_{l_w}}(p^{\gamma}_j(t_1)) + \mathrm{val}_w(p^{\gamma}_j(t_1)) \in \mathbb{Z}/2. \tag{4.19}$$

We now observe that if we write $p^{\gamma}_j = c\prod_l q_l^{\varepsilon_l}$ with $\varepsilon_l \in \{0,1\}$ for $c \in \mathcal{O}^{\star}_{S_w}$ then (4.19) implies that $\mathrm{val}_w(c)$ must be even. Since S_0 contains a set of generators for the class group we get that c is equivalent up to squares to an element in $\mathcal{O}_S$. It then follows that γ lies in $\mathcal{G}_S \subseteq \mathcal{G}_{S_w}$, as desired. By Lemma 4.42 we may conclude that $\gamma \in \mathrm{Sel}_{t_0}(\mathcal{E})$.

We have thus shown that $\mathrm{Sel}_{t_1}(\mathcal{E}) \subseteq \mathrm{Sel}_{t_0}(\mathcal{E})$. To show that $\mathrm{Sel}_{t_1}(\mathcal{E})$ contains α we note that by Lemma 4.42 we have that $X^{\alpha}_{t_1}(k_v) \neq \varnothing$ for every $v \neq u^1_{l_w}, w$, and that $\mathrm{inv}_w A^{\alpha}_{l_w}(t_1) = 0$ by the choice of w. The equality $\mathrm{inv}_{u^1_{l_w}} A^{\alpha}_{l_w}(t_1) = 0$ then follows from Lemma 4.42(3), and so $\alpha \in \mathrm{Sel}_{t_1}(\mathcal{E})$. On the other hand, by our choice of w we have that $\mathrm{inv}_w A^{\beta}_{l_w}(t_1) \neq 0$ and so $\beta \notin \mathrm{Sel}_{t_1}(\mathcal{E})$. □

Corollary 4.43. *Suppose that $\alpha \in \mathcal{G}^{\mathrm{even}}$ satisfies Condition (D). Then there exists a finite set of places S, a suitable collection of local points x_S and an S-admissible point $t \in U(k)$ such that $\mathrm{Sel}(E_t)$ is generated by α_t and the images $\partial E_t[2] \subseteq \mathrm{Sel}(E_t)$ of the 2-torsion points. In particular, α_t is in the kernel of the map $\mathrm{Sel}(E_t) \longrightarrow Ш^1(k, E_t)$ and $X^{\alpha}_t(k) \neq \varnothing$.*

Proof. By Proposition 4.40 and Lemma 4.35 we may find a finite set of places S, a suitable S-collection of local points x_S and an S-admissible point $t \in U(k)$ such that $\alpha \in \mathrm{Sel}_{t_0}(\mathcal{E})$ and $\mathrm{Sel}_{t_0}(\mathcal{E}) \cap \mathcal{G}_{\alpha} \subseteq \mathcal{G}^{\mathrm{even}}_S$. If $\mathrm{Sel}(E_{t_0})$ is generated by $\mathrm{ev}_{t_0}(\alpha)$ and the image $\partial E_{t_0}[2] \subseteq \mathrm{Sel}(E_{t_0})$ then we can take $t = t_0$ and finish the proof. Otherwise, there must exist a $\beta = ([p^{\beta}]_1, [p^{\beta}_2], [p^{\beta}_3]) \in \mathrm{Sel}_{t_0}(\mathcal{E})$ which does not belong to the subgroup of $\mathrm{Sel}_{t_0}(\mathcal{E})$ generated by α and the classes of the triples (4.14). Since α satisfies Condition (D) and $\mathrm{Sel}_{t_0}(\mathcal{E}) \cap \mathcal{G}_{\alpha} \subseteq \mathcal{G}^{\mathrm{even}}_S$ we must conclude that $\beta \notin \mathcal{G}_{\alpha}$. There must then exists an $l_0 \in \{1, ..., m\}$ such that $\chi^{\beta}_{l_0} \in H^1(k_l, \mathbb{Z}/2)$ does not belong to the subgroup generated by $\chi^{\alpha}_{l_0}$. By Chebotarev's density theorem there must exist a place $w \notin S$ such that w splits completely in $L^{\alpha}_{l_0}$ but does not split completely in $L^{\beta}_{l_0}$. In particular, there exists a $t_w \in \mathcal{O}_w$ such that $\mathrm{val}_w\, q_{l_0}(t_w) = 1$ and $\mathrm{inv}_w A^{\alpha}_{l_0}(t_w) = 0$ but $\mathrm{inv}_w A^{\beta}_{l_0}(t_w) \neq 0$. By Lemma 4.34 we have that $X^{\alpha}_{t_w}$ has a k_w-point $x_{k_w} \in X^{\alpha}_{t_w}(k_w)$. Let $S_w := S \cup \{w\}$ and let $x_{S_w} = (x_v)_{v \in S_w}$ be the S_w-collection of local points obtained by adding x_w to x_S. Applying Hypothesis (H_1) there exists an S_w-admissible point t_1 which approximates x_{S_w}. Proposition 4.41 then tells us that $\mathrm{Sel}_{t_1}(\mathcal{E}) \subseteq \mathrm{Sel}_{t_0}(\mathcal{E})$ and that $\alpha \in \mathrm{Sel}_{t_1}(\mathcal{E})$ but $\beta \notin \mathrm{Sel}_{t_1}(\mathcal{E})$. In particular, the Selmer group of $\mathrm{Sel}_{t_1}(\mathcal{E})$ is strictly smaller. Iterating this procedure we may find a finite set S', a suitable S'-collection of local points $x_{S'}$ and an S'-admissible point t such that $\mathrm{Sel}(E_{t_0})$ is generated by $\mathrm{ev}_{t_0}(\alpha)$ and the image $\partial E_{t_0}[2] \subseteq \mathrm{Sel}(E_{t_0})$, as desired. It then follows from Proposition 4.26 that $Ш(E_t)[2] = 0$ and so $[X^{\alpha}_t] = 0 \in Ш(E_t)$, so that X^{α}_t has a rational point. □

5. Kummer surfaces

5.1. **Preliminaries.** Recall that an **abelian surface** A over a field k is a commutative projective algebraic group of dimension 2 over k. If k is embedded in $\mathbb{C}$ then the space of complex points $A(\mathbb{C})$ is homeomorphic to torus $(S^1)^4$. Examples of abelian surfaces include products of two elliptic curves and the Jacobians of curves of genus 1.

Given a an abelian surface A, a **2-covering** of A is a torsor Y under A equipped with a finite étale map $p : Y \longrightarrow A$ which covers the multiplication by 2 map $A \xrightarrow{2} A$. More precisely, we ask that the diagram

$$\begin{array}{ccc} A \times Y & \xrightarrow{(2,p)} & A \times A \\ \downarrow & & \downarrow{\scriptstyle m} \\ Y & \xrightarrow{p} & A \end{array}$$

commutes, where $m : A \times A \longrightarrow A$ is the group structure of A. Given Y, the data of such a map $p : Y \longrightarrow A$ is equivalent to the data of a lift of the class $[Y] \in H^1(k, A)$ to a class $\alpha \in H^1(k, A[2])$. The antipodal involution $\iota_A = [-1] : A \longrightarrow A$ then induces an involution $\iota_Y : Y \longrightarrow Y$, and one defines the **Kummer surface** $X = \mathrm{Kum}(Y)$ associated to Y as the minimal desingularisation of Y/ι_Y. We note that this desingularisation simply consists of blowing up the fixed locus of ι_Y. The resulting exceptional divisor $D \subseteq X$ then forms, geometrically, a disjoint union of 16 rational curves, each of self intersection -2. The surface $\mathrm{Kum}(Y)$ is an example of a **K3 surface**.

It is well-known that the Kummer surface X does not determine A and Y up to isomorphism (see, e.g., [22]). Over the algebraic closure $\overline{k}$, a theorem of Nikulin states that one can reconstruct A from X together with the additional data of the exceptional divisor $D \subseteq X$. Over k, the data of D only determines A and Y up to a **quadratic twist**. More precisely, for a quadratic extension F/k we may consider the quadratic twists A^F and Y^F with respect to the $\mathbb{Z}/2$-actions given by ι_A and ι_Y. We may then consider Y^F as a torsor under A^F determined by the same class $\alpha \in H^1(k, A^F[2]) = H^1(k, A[2])$, and for every such F/k we have a canonical isomorphism $\mathrm{Kum}(Y^F) \cong \mathrm{Kum}(Y)$. We note that the collection of quadratic twists A^F can be organized into a fibration $\mathscr{A} := (A \times \mathbb{G}_m)/\mu_2 \longrightarrow \mathbb{G}_m/\mu_2 \cong \mathbb{G}_m$, where the generator of μ_2 acts diagonally by $(\iota_A, -1)$. In particular, for a point $t \in k^* = \mathbb{G}_m(k)$, the fiber $\mathscr{A}_t$ is naturally isomorphic to the quadratic twist $A^{k(\sqrt{t})}$. Similarly, we may organize the quadratic twists of Y into a pencil $\mathscr{Y} \longrightarrow \mathbb{G}_m$ with $\mathscr{Y}_t \cong Y^{F(\sqrt{t})}$. We may then consider the **entire family** $\mathscr{A}_t$ as the family of abelian surfaces associated to (X, D), and similarly the family $\mathscr{Y}_t$ as the family of 2-coverings associated to (X, D).

Conjecture 5.1. *Let X be a Kummer surface over k with associated exceptional divisor $D \subseteq X$. If the Brauer-Manin obstruction to the Hasse principle is the only one for all 2-coverings $\mathscr{Y}_t$ associated to (X, D), then the same holds for X.*

Remark 5.2. In Conjecture 5.1 one may freely replace the Brauer-Manin obstruction by the analogous obstruction formed only by the 2-primary part of the Brauer group. This is because for 2-coverings of abelian varieties as well as for Kummer

surfaces the latter obstruction is equivalent to the full Brauer-Manin obstruction, see [11, Theorem 1.2 and Theorem 1.7].

The statement that the Brauer–Manin obstruction is the only one for **all** 2-coverings of A is equivalent to the statement that the 2-primary part of $Ш(A)$ is finite. In particular, Conjecture 5.1 combined with the Tate-Shafarevich conjecture for abelian surfaces together imply that the Brauer-Manin obstruction controls the existence of rational points on Kummer surfaces. We may therefore consider any instance of Conjecture 5.1 as giving support for this latter statement, or more generally, support for the conjecture that the Brauer-Manin obstruction controls the existence of rational points on K3 surfaces.

In their paper [26], Swinnerton-Dyer and Skorobogatov suggested a variant of the argument described in §4.2 which is capable of proving instances of Conjecture 5.1. The strategy they suggested is as follows. Let Y be a 2-covering of A with associated class $\alpha \in H^1(k, A[2])$. To find a rational point on $X = \mathrm{Kum}(Y)$, it is enough to find a rational point on a quadratic twist Y^F for some F/k. At the first step of the proof, using a fibration argument, one produces a quadratic extension F such that Y^F is everywhere locally soluble. Equivalently, $\alpha \in H^1(k, A^F[2])$ is in the **2-Selmer group** of A^F. At the second step one modifies F so that the 2-Selmer group of A^F is spanned by α and the image of $A^F[2](k)$ under the Kummer map. This implies that $Ш(A^F)[2]$ is spanned by the class $[Y^F]$, and hence $\dim_{\mathbb{F}_2} Ш(A^F)[2] \le 1$. Let us remark that in all existing applications of the method, as well as in the current paper, one assumed that A (and hence all its quadratic twists) is equipped with a principal polarization which is induced by a symmetric line bundle. In that case it is known (see [21]) that the **Cassels–Tate pairing** on $Ш(A^F)$ is alternating. If one assumes in addition that the 2-primary part of $Ш(A^F)$ is finite then the 2-part of the Cassels-Tate pairing is non-degenerate and hence the dimension of $Ш(A^F)[2]$ over $\mathbb{F}_2$ is even. The above bound on $\dim_{\mathbb{F}_2} Ш(A^F)[2]$ now implies that $Ш(A^F)[2]$ is trivial and $[Y^F] = 0$, i.e., Y^F has a rational point. Alternatively, instead of assuming that the 2-primary part of $Ш(A^F)$ is finite, it is enough to assume that $[Y^F]$ itself is not a non-trivial divisible element of $Ш(A^F)$ (as is effectively assumed in Conjecture 5.1). Indeed, the latter is generally weaker but implies the former when $Ш(A^F)[2]$ is generated by $[Y^F]$.

The above strategy was implemented in [26] for the case where A is a product of two elliptic curves whose 2-torsion points are defined over k, under certain technical conditions. We will describe their results, together with a full proof, in the next section. Since then the method was implemented in several additional cases (each time under suitable conditions on the Kummer surface in question). Let us give a sample of two results. The first result also concerns Kummer surfaces attached to products of elliptic curves. In particular, given two irreducible polynomials g_1, g_2 of degree 4, the equation

$$y^2 = g_i(x)$$

determines a curve D_i of genus 1 which is a 2-covering of its Jacobien E_i (see §4.1). The kummer surface associated to the 2-covering $D_1 \times D_2$ of $E_1 \times E_2$ is then given by the affine equation

$$y^2 = g_1(x)g_2(z).$$

Theorem 5.3 ([13]). *Let $g_1(x)$ and $g_2(x)$ be irreducible polynomials of degree 4 over a number field k, each with the Galois group S_4. Let w_1 and w_2 be distinct*

primes of k not dividing 6 such that for all $i,j \in \{1,2\}$ the coefficients of $g_i(x)$ are integral at w_j and $\mathrm{val}_{w_j}(\Delta(g_i)) = \delta_{ij}$. Let E_i be the Jacobian of the curve D_i given by $y^2 = g_i(x)$, where $i = 1,2$. For $i = 1,2$ assume the finiteness of the 2-primary torsion subgroup of the Shafarevich–Tate group for each quadratic twist of E_i whose 2-Selmer group has rank 1. If the Kummer surface with the affine equation

$$z^2 = g_1(x)g_2(y) \tag{5.1}$$

is everywhere locally soluble, then it has a Zariski dense set of k-points.

To describe the next sample result, let $f(x) = \prod_{i=0}^{5}(x-a_i) \in k[x]$ be a polynomial of degree 6 which splits completely over k and such that $d := \prod_{i<j}(a_j - a_i) = \sqrt{\mathrm{disc}(f)} \neq 0$, and let C be the hyperelliptic curve given by $y^2 = f(x)$. Let $b_0, ..., b_5 \in k^*$ be elements such that $\prod_i b_i$ is a square and consider the surface $X \subseteq \mathbb{P}^5$ given by the smooth complete intersection

$$\sum_i \frac{b_i x_i^2}{f'(a_i)} = \sum_i \frac{a_i b_i x_i^2}{f'(a_i)} = \sum_i \frac{a_i^2 b_i x_i^2}{f'(a_i)} = 0. \tag{5.2}$$

The surface X is a Kummer surface whose associated family of abelian surfaces $\mathscr{A}_t$ is the family of quadratic twists of the Jacobian $A = \mathrm{Jac}(C)$. Here, it is useful to think of the coordinates $x_0, ..., x_5$ in (5.3) as indexed by the roots $a_0, ...a_5$ of f. Indeed, if we denote by $W := \{a_0, ..., a_5\}$ the set of roots of f then we may identify $A[2]$ with the submodule of $\mu_2^W/(-1,-1,...,-1)$ spanned by those vectors $(\varepsilon_0, ..., \varepsilon_5) \in \mu_2^W$ such that $\prod_i \varepsilon_i = 1$. In this formulation the action of $(\varepsilon_0, ..., \varepsilon_5) \in A[2]$ on X (induced by the action on the corresponding 2-covering of A) is given by $x_i \mapsto \varepsilon_i x_i$. As $\prod_i b_i$ is a square the classes $[b_i] \in H^1(k, \mu_2)$ determine a class $([b_0], ..., [b_5]) \in H^1(k, A[2])$, and the family of 2-coverings of $\mathscr{A}_t$ associated to X is exactly the family of 2-coverings determined by this class.

Theorem 5.4 ([12])**.** *Assume that the classes of $\frac{b_1}{b_0}, ..., \frac{b_4}{b_0}$ are linearly independent in $k^*/(k^*)^2$ and that there exist finite odd places $w_1, ..., w_5$ such that for every $i = 1, ..., 5$ we have:*

(1) The elements $\{a_0, ..., a_5\}$ are w_i-integral and $\mathrm{val}_{w_i}(a_i - a_0) = \mathrm{val}_{w_i} d = 1$.

(2) The elements $\frac{b_1}{b_0}, ..., \frac{b_4}{b_0}$ are all units at w_i but are not all squares at w_i.

Then Conjecture 5.1 holds for the Kummer surface X given by (5.3). In particular, if the 2-primary Tate-Shafarevich conjecture holds for every quadratic twist of A then the (2-primary part of the) Brauer-Manin obstruction is the only obstruction to the Hasse principle on X (see Remark 5.2).

5.2. **Products of elliptic curves with rational 2-torsion.** In this section we will describe the results of [26] in more detail. The technical details of the argument are slightly different from those of [26], but the strategy is the same.

Let k be a number field. For $i = 1,2$ let $E^{(i)}$ be an elliptic curve given by

$$E^{(i)} : y^2 = x(x - a_i)(x - b_i)$$

with $a_i \neq b_i \in k^*$. Using the 2-torsion points $(a_i, 0)$ and $(b_i, 0)$ as basis we identify $H^1(k, E^{(i)}[2]) \cong k^*/(k^*)^2 \times k^*/(k^*)^2$ in such a way that for a point $(x,y) \neq (a_i,0), (b_i,0)$ on E_i, the element of $k^*/(k^*)^2 \times k^*/(k^*)^2$ corresponding to (x,y) by the Kummer sequence is the pair $([x-a_i], [x-b_i])$, and for the points $(a_i, 0)$ and $(b_i, 0)$ the corresponding pairs are $([a_i(a_i - b_i)], [a_i - b_i])$ and $([b_i - a_i], [b_i(b_i - a_i)])$ respectively.

Remark 5.5. Unlike the situation in §4.2 where we worked with triples to avoid choosing a basis for the 2-torsion group, here it will be convenient to break the symmetry and use a particular basis. This break of symmetry is due to Condition (Z) that we will introduce below.

Given a $c \in k^*$ we will denote by

$$E_c^{(i)} : y^2 = x(x - ca_i)(x - cb_i)$$

the quadratic twist of $E^{(i)}$ by the class $[c] \in k^*/(k^*)^2$. Using the 2-torsion points $(ca_i, 0)$ and $(cb_i, 0)$ to identify $H^1(k, E_c^{(i)}[2]) \cong k^*/(k^*)^2 \times k^*/(k^*)^2$ as above.

For $i = 1, 2$ let us fix an element $\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}) \in k^*/(k^*)^2 \times k^*/(k^*)^2$. Then $\alpha^{(i)}$ determines a 2-covering $D^{(i)}$ of $E^{(i)}$, which can be written as a curve of the form

$$y^2 = g_i(x)$$

for a suitable quartic polynomial g_i (whose resolvant cubic is $x(x - a_i)(x - b_i)$). In this case the surface $D^{(1)} \times D^{(2)}$ is a 2-covering of the abelian surface $A := E^{(1)} \times E^{(1)}$. The associated Kummer surface $\mathrm{Kum}(D^{(1)} \times D^{(2)})$ is then a smooth and proper model for the affine surface

$$y^2 = g_1(x)g_2(z).$$

Given $c \in k^*$ we will denote by

$$D_c^{(i)} : y^2 = cg_i(x)$$

the corresponding quadratic twist. Then we may consider $D_c^{(i)}$ as the 2-covering of $E_c^{(i)}$ associated to the same element $\alpha^{(i)} \in k^*/(k^*)^2 \times k^*/(k^*)^2$.

We will denote by $\mathcal{M} \subseteq k^*/(k^*)^2$ the subgroup generated by $\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_1^{(2)}, \alpha_2^{(2)}$. Let S be a finite set of places containing the archimedean places, the places above 2, all the places of bad reduction for either $D^{(1)}$ or $D^{(2)}$ and a set of generators for the class group of k. As in [26], consider the following conditions:

Condition 5.6 (Condition (E))**.** *There exist $c_v \in k_v^*$ for $v \in S$ such that the following holds:*

(1) $D_{c_v}^{(1)}$ and $D_{c_v}^{(2)}$ are soluble in k_v for all $v \in S$;
(2) for each $i = 1, 2$ and for each $\beta \in (\mathcal{M} \times \mathcal{M}) \setminus \{(1, 1), \alpha^{(i)}\}$ there exists a $v \in S$ such that the 2-covering of $E_{c_w}^{(i)}$ determined by β is not soluble in k_v.

Condition 5.7 (Condition (Z))**.** *There exist places $w_1^{(1)}, w_2^{(1)}, w_1^{(2)}, w_2^{(2)} \notin S$ such that*

(1) $a_1, b_1, a_1 - b_1$ are units at $w_1^{(2)}, w_2^{(2)}$ and $a_2, b_2, a_2 - b_2$ are units at $w_1^{(1)}, w_2^{(1)}$.
(2) The elements $b_1 - a_1$ and $b_2 - a_2$, as well as the components of $\alpha^{(1)}, \alpha^{(2)}$, are all units at $w_j^{(i)}$ for $i, j = 1, 2$.
(3) $\mathrm{val}_{w_1^{(i)}}(a_i) = \mathrm{val}_{w_2^{(i)}}(b_i) = 1$ and $\mathrm{val}_{w_1^{(i)}}(b_i) = \mathrm{val}_{w_2^{(i)}}(a_i) = 0$ for $i = 1, 2$.

Remark 5.8. The places $w_j^{(i)}, w_j^{(i)}$ are in particular places of bad (multiplicative) reduction for E_i and hence belong to S by definition.

We can now formulate the main result of [26]:

Theorem 5.9 ([26, Theorem 1])**.** *Assume Condition (E) and Condition (Z) hold, and that the Tate-Shafarevich group of every quadratic twist of $E^{(1)}$ and $E^{(2)}$ is*

finite. If the Kummer surface

$$y^2 = g_1(x)g_2(z) \tag{5.3}$$

is everywhere locally soluble, then it is soluble in k.

The first step, which can be considered as an instance of the fibration method, is the following:

Proposition 5.10 ([26, Lemma 8])**.** *Assume Condition (E) and that (5.3) is everywhere locally soluble. Then there exists a $c \in k^*$ which is a unit at the places $w_j^{(i)}$ for $i,j = 1,2$ and such that for $i = 1,2$ the 2-covering of $E_c^{(i)}$ determined by an element $\beta \in \mathcal{M}\times\mathcal{M}$ is everywhere locally soluble if and only if β is trivial or $\beta = \alpha^{(i)}$. Furthermore, we may choose c such that there exists a place $u \notin S$ at which c is a uniformizer.*

Recall (see §4.1) that the Selmer group $\mathrm{Sel}_2(E^{(i)}) \subseteq k^*/(k^*)^2 \times k^*/(k^*)^2$ is the subgroup consisting of those pairs such that the corresponding 2-covering of $E^{(i)}$ is everywhere locally soluble. We then understand the conclusion of Proposition 5.10 as saying that the element $\alpha^{(i)}$ belongs to $\mathrm{Sel}_2(E^{(i)})$, and is in fact the only element which belongs to the intersection of $\mathrm{Sel}_2(E^{(i)})$ and $\mathcal{M} \times \mathcal{M}$.

Now suppose that c is as in Proposition 5.10. If $\beta = (\beta_1, \beta_2)$ is now a pair which does not belong to $\mathcal{M} \times \mathcal{M}$ then there exists a $j \in \{1,2\}$ such that β_j does not belong to $\mathcal{M}$. By Chebotarev's theorem one may then find a place v such that $\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_1^{(2)}, \alpha_2^{(2)}$ are all squares at v and such that β_j is not a square at v. If $c' \in k^*$ is now any element which is sufficiently close to 1 over S and a uniformizer at v then $E_{cc'}^{(1)}, E_{cc'}^{(2)}$ will still satisfy the conclusion of Proposition 5.10, and in addition the element β will not belong to either $\mathrm{Sel}_2(E_{cc'}^{(1)})$ or $\mathrm{Sel}_2(E_{cc'}^{(2)})$. Elaborating on this argument one quickly proves the following strengthening of Proposition 5.10, which is a variant of Lemma 9 of [26], where we replace the notion of being in the **restricted Selmer group** by that of not belonging to some finite subgroup of the form $\mathcal{M}' \times \mathcal{M}'$

Proposition 5.11 (cf. [26, Lemma 9(i)])**.** *Let $\mathcal{M}' \subseteq k^*/(k^*)^2$ be any finite subgroup containing $\mathcal{M}$. Assume Condition (E) and that (5.3) is everywhere locally soluble. Then there exists a $c \in k^*$ which is a unit at the places $w_j^{(i)}$ for $i,j \in \{1,2\}$ and such that for $i = 1,2$ the 2-covering of $E_c^{(i)}$ determined by a $\beta \in \mathcal{M}' \times \mathcal{M}'$ is everywhere locally soluble if and only if β is trivial or $\beta = \alpha^{(i)}$. Furthermore, we may choose c such that there exists a place $u \notin S$ at which c is a uniformizer.*

In particular, let us consider the finite subgroup $\mathcal{M}' \subseteq k^*/(k^*)^2$ spanned by the elements $\alpha_1^{(i)}, \alpha_2^{(i)}, [a_i(a_i - b_i)], [b_i(b_i - a_i)]$ for $i = 1,2$ as well as the elements $[-1], [(a_1 - b_1)(a_2 - b_2)]$. Applying Proposition 5.11 and replacing $E^{(i)}$ by $E_c^{(i)}$ we may assume that the conclusion of Proposition 5.11 actually held to begin with, namely, that:

(*) for $i = 1,2$ the 2-covering of $E^{(i)}$ determined by an element $\beta \in \mathcal{M}' \times \mathcal{M}'$ is everywhere locally soluble if and only if β is trivial or $\beta = \alpha^{(i)}$. In addition, there exists a place $u \in S \smallsetminus \{w_j^{(i)}\}$ such that each of $a_i, b_i, a_i - b_i$ is a uniformizer at u for $i = 1,2$.

The core step in the proof of Theorem 5.9 is the following:

Proposition 5.12. *Assume that (*) and Condition (Z) hold. Then there exists a $c \in k^*$ such that for $i = 1, 2$ the Selmer group $\mathrm{Sel}_2(E_c^{(i)})$ is generated by $\alpha^{(i)}$ and the image of the 2-torsion.*

The conclusion of Proposition 5.12 implies, in particular, that the 2-torsion part $Ш(E_c^{(i)})[2]$ of the Tate-Shafarevich group is generated by the image of $\alpha^{(i)}$. Under the assumptions of Theorem 5.9 the group $Ш(E_c^{(i)})$ is finite. In this case the alternating Cassels-Tate pairing is non-degenerate (Theorem 2.7), implying, in particular, that the 2-rank of $Ш(E_c^{(i)})[2]$ is even. This means that the image of $\alpha^{(i)}$ in $Ш(E_c^{(i)})$ must vanish, i.e., $E_c^{(i)}$ has a rational point for $i = 1, 2$, yielding a rational point on 5.3.

We now start working towards a proof of Proposition 4.27. To explain the argument let us fix an elliptic curve

$$E : y^2 = x(x-a)(x-b)$$

and an element $c \in k^*$. As above we will identify $H^1(k, E[2]) \cong H^1(k, E_c[2]) \cong k^*/(k^*)^2 \times k^*/(k^*)^2$. Similarly, for a place v of k we identify $H^1(k_v, E[2]) \cong H^1(k_v, E_c[2]) \cong k_v^*/(k_v^*)^2 \times k_v^*/(k_v^*)^2$

Given a place v of k let us denote by $W_v, W_{v,c} \subseteq k_v^*/(k_v^*)^2 \times k_v^*/(k_v^*)^2$ the images of $E(k_v)/2E(k_v)$ and $E_c(k_v)/2E_c(k_v)$ respectively under the relevant boundary maps.In particular, we may identify the Selmer group $\mathrm{Sel}_2(E) \subseteq k^*/(k^*)^2 \times k^*/(k^*)^2$ (resp. $\mathrm{Sel}_2(E_c)$) with the subgroup consisting of those pairs whose local image in $k_v^*/(k_v^*)^2 \times k_v^*/(k_v^*)^2$ belongs to W_v (resp. $W_{v,c}$). We will denote by $U_v = W_v \cap W_{v,c}$ the intersection of the Selmer conditions and by $Q_v = W_v/U_v$ and $Q_{v,c} = W_{v,c}/U_v$ the corresponding quotients. Given a finite subset T of places of k, we will denote by $V_T \subseteq \oplus_{v \in T} Q_v$ the image of $\mathrm{Sel}_2(E)$ and by $V_{T,c} \subseteq \oplus_{v \in T} Q_{v,c}$ the image of $\mathrm{Sel}_2(E_c)$.

Example 5.13.

(1) If v is a place of good reduction for E and c is such that $\mathrm{val}_v(c) = 1$ then $U_v = \{0\}$.
(2) If v is such that $\mathrm{val}_v(a) = 1$ and $\mathrm{val}_v(b) = \mathrm{val}_v(b-a) = 0$ and $c \in k^*$ is such that c is a non-square unit at v then $\dim_2 U_v = 1$.

We now give a general lemma for predicting the change of the 2-Selmer group after quadratic twist, which is based on and is a mild refinement of the results of [18, §3].

Lemma 5.14 (Mazur-Rubin)**.** *Let E be as above and let $c \in k^*$ be an element. Let T be a finite set of finite odd places of k such that $W_v = W_{v,c}$ for every $v \notin T$. Then*

$$\dim_2(\mathrm{Sel}(E_c)) - \dim_2(\mathrm{Sel}(E)) = \dim_2(V_{T,c}) - \dim_2(V_T)$$

and

$$\dim_2(V_{T,c}) + \dim_2(V_T) \leq 2|T| - \sum_v \dim_2(U_v).$$

Proof. Let $\mathrm{S}_T \subseteq k^*/(k^*)^2 \times k^*/(k^*)^2$ denote the subgroup of those elements whose local image at v lies in U_v for every v. Since $U_v = W_v = W_{v,c}$ for every $v \notin T$ we see that S_T appears in two short exact sequences

$$0 \longrightarrow \mathrm{S}_T \longrightarrow \mathrm{Sel}_2(A) \longrightarrow V_T \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{S}_T \longrightarrow \mathrm{Sel}_2(E_c) \longrightarrow V_{T,c} \longrightarrow 0$$

We may hence conclude that

$$\dim_2(\mathrm{Sel}(E_c)) - \dim_2(\mathrm{Sel}(E)) = \dim_2(V_{T,c}) - \dim_2(V_T).$$

Now for each place v of k, the Weil pairing induces the alternating Tate pairing on $H^1(k, E[2]) \cong H^1(k, E_c[2]) \cong k_v^*/(k_v^*)^2 \times k_v^*/(k_v^*)^2$ which admits both W_v and $W_{v,c}$ as maximal isotropic subspaces. Let

$$U_v^\perp \subseteq k_v^*/(k_v^*)^2 \times k_v^*/(k_v^*)^2$$

be the orthogonal subspace of U_v with respect to the Tate pairing. Since U_v is contained in W_v it is isotropic, and so $U_v \subseteq U_v^\perp$. Furthermore, since the Tate pairing is non-degenerate we see that U_v is also the orthogonal subspace of $U_v^\perp$ and so the induced pairing

$$[U_v^\perp/U_v] \times [U_v^\perp/U_v] \longrightarrow \mathbb{Z}/2 \tag{5.4}$$

is non-degenerate. Since both W_v and W_v^c are isotropic we get that $Q_v, Q_{v,c} \subseteq U_v^\perp/U_v$ and so we have an induced pairing

$$Q_v \times Q_{v,c} \longrightarrow \mathbb{Z}/2 \tag{5.5}$$

The fact that both W_v and W_v^c are **maximal** isotropic implies that 5.5 is non-degenerate. By summing over the places of T we obtain a non-degenerate alternating form

$$\sum_{v\in T} Q_v \times \sum_{v\in T} Q_{v,c} \longrightarrow \mathbb{Z}/2 \tag{5.6}$$

Finally, by quadratic reciprocity and the fact that $W_v = W_{v,c}$ for $v \notin T$ we get that the subspaces $V_T \subseteq \sum_v Q_v$ and $V_{T,c} \subseteq \sum_v Q_{v,c}$ are orthogonal to each other with respect to 5.6 (although not necessarily maximally orthogonal). Since every $v \in T$ is odd we know that for such v

$$\dim_2 Q_v = \dim_2 Q_{v,c} = 2 - \dim_2 U_v$$

and so we obtain the bound

$$\dim_2(V_T) + \dim_2(V_{T,c}) \leq 2|T| - \sum_{v\in T} \dim_2(U_v).$$

□

Using the Mazur-Rubin lemma we may now give a relatively short proof of Proposition 5.12. More precisely, we will prove the following statement, from which Proposition 5.12 can easily be deduced by induction and switching the roles of $E^{(1)}$ and $E^{(2)}$:

Proposition 5.15. *Assume that (*) and Condition (Z) hold. If* $\dim_2 \mathrm{Sel}_2(E^{(1)}) > 3$ *then there exists a* $c \in k^*$ *such that* $\dim_2 \mathrm{Sel}_2(E_c^{(1)}) < \dim_2 \mathrm{Sel}_2(E^{(1)})$ *and* $\dim_2 \mathrm{Sel}_2(E_c^{(2)}) = \dim_2 \mathrm{Sel}_2(E^{(2)})$. *Furthermore, c can be chosen so that Condition (*) and Condition (Z) hold for* $E_c^{(1)}$ *and* $E_c^{(2)}$.

Proof. By assumption there exists an element $\beta \in \mathrm{Sel}_2(E^{(1)})$ which does not belong to the subgroup generated by $\alpha^{(1)}$ and the image of the 2-torsion. By possibly adding to β an element in the image of the 2-torsion we may assume that β is unramified at $w_1^{(1)}, w_2^{(1)}$. Since β is in the Selmer group but is not $(1,1)$ or $\alpha^{(1)}$ it cannot belong to $\mathcal{M}' \times \mathcal{M}'$ by (*). There must therefore exists a $j \in \{1,2\}$ such that the component β_j does not belong to $\mathcal{M}'$. To fix ideas, let us assume that

β_1 does not belong to $\mathcal{M}'$. By Condition (*) there exists a place $u \in S$ at which $a_i, b_i, a_i - b_i$ are all uniformizers for both $i = 1$ and $i = 2$. This implies, in particular, that $[a_i - b_i] \notin \mathcal{M}'$ for $i = 1, 2$. We note that since $[a_1 - b_1][a_2 - b_2] \in \mathcal{M}'$ by definition it follows that $\beta_1[a_1 - b_1][a_2 - b_2] \notin \mathcal{M}'$. By Chebotarev's theorem there now exists a place $v_0 \notin S$ such that all the elements of $\mathcal{M}'$ are squares at v_0 and such that $\beta_1, a_1 - b_i$ and $a_2 - b_2$ are not squares at v_0. Note that since $[-1] \in \mathcal{M}'$ we have that -1 is a square at v_0 and hence $b_1 - a_1$ and $b_2 - a_2$ are also non-squares at v_0.

Since S contains a set of generators for the class group we may find a quadratic extension K/k which is purely ramified at $w_2^{(1)}$ and unramified outside S. Let $\mathfrak{m}$ be the modulus which is a product of 8 and all the places in S except $w_j^{(2)}$ and let $k_{\mathfrak{m}}$ be the ray class field of $\mathfrak{m}$. Since K is purely ramified at $w_j^{(2)}$ but unramified outside S it is linearly disjoint from $k_{\mathfrak{m}}$. We may hence deduce the existence of a place $v_1 \notin S \cup \{v_0\}$ such that

(1) The Frobenius element $\mathrm{Frob}_{v_1}(k_{\mathfrak{m}})$ of v_1 in $\mathrm{Gal}(k_{\mathfrak{m}}/k)$ is equal to the inverse of the Frobenius element $\mathrm{Frob}_{v_0}(k_{\mathfrak{m}})$.
(2) The product $\mathrm{Frob}_{v_0}(K) \cdot \mathrm{Frob}_{v_1}(K) \in \mathrm{Gal}(K/k)$ is non-trivial.

By property (1) above we see that the divisor $v_0 + v_1$ pairs trivially with the kernel of $H^1(k, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(k_{\mathfrak{m}}, \mathbb{Q}/\mathbb{Z})$ and so there exists a $c \in k^*$ which is equal to 1 mod $\mathfrak{m}$ and such that $\mathrm{div}(c) = v_0 + v_1$. In particular, we see that c is a square at each $v \in S \setminus \{w_2^{(1)}\}$. By quadratic reciprocity and (2) above it follows that c is **not** a square in $w_2^{(1)}$. We now claim that the element c satisfies the required conditions. First since c is a unit at $w_j^{(i)}$ for $i, j = 1, 2$ it is clear that Condition (Z) still holds. For Condition (*), since c is a unit over S and all the element of $\mathcal{M}'$ are unramified outside S it is clear that any $\beta \in \mathcal{M}' \times \mathcal{M}'$ which did not belong to $\mathrm{Sel}_2(E^{(i)})$ will not belong to $\mathrm{Sel}_2(E_c^{(i)})$ either. On the other hand, since $\alpha^{(1)}$ and $\alpha^{(2)}$ belong to $\mathcal{M}'$ they are squares at v_0 by construction. Furthermore, since $\alpha^{(1)}, \alpha^{(2)}$ are units outside S and are units at $w_2^{(1)}$ it follows that the splitting field of $\alpha^{(1)}, \alpha^{(2)}$ is contained in $k_{\mathfrak{m}}$, and so (1) above implies that $\alpha^{(1)}, \alpha^{(2)}$ are squares at v_1 as well. We may now conclude that (*) holds for $E^{(1)}$ and $E^{(2)}$.

Let us now prove that $\dim_2 \mathrm{Sel}_2(E_c^{(2)}) = \dim_2 \mathrm{Sel}_2(E^{(2)})$. Since c is 1 mod $\mathfrak{m}$ and $\mathfrak{m}$ is divisible by all places of bad reduction for $E^{(2)}$ we see that the only places where the Selmer conditions of $E^{(2)}$ and $E_c^{(2)}$ differ are v_0 and v_1. By Example 5.13(1) we have $U_{v_0} = U_{v_1} = \{0\}$. Applying Lemma 5.14 with $T = \{v_0, v_1\}$ we get that

$$\dim_2(\mathrm{Sel}(E_c^{(2)})) - \dim_2(\mathrm{Sel}(E^{(2)})) = \dim_2(V_{T,c}) - \dim_2(V_T)$$

with

$$\dim_2(V_{T,c}) + \dim_2(V_T) \leq 4.$$

To show that $\dim_2(\mathrm{Sel}(E_c^{(2)})) = \dim_2(\mathrm{Sel}(E^{(2)}))$ it will hence suffice to show that $\dim_2(V_{T,c}), \dim_2(V_T) \geq 2$, which we can verify by checking that the image of the 2-torsion has dimension 2 in both V_T and $V_{T,c}$. For $V_{T,c}$ this is clear by simply looking at the valuation at v_0 (or v_1). In the case of V_T this follows from the fact that the pairs $([b_i - a_i], [b_i(b_i - a_i)]), ([a_i(a_i - b_i)], [a_i - b_i])$ reduce mod v to the standard basis of $(\mathbb{F}_{v_0}^*/(\mathbb{F}_{v_0}^*)^2) \times (\mathbb{F}_{v_0}^*/(\mathbb{F}_{v_0}^*)^2)$ by our choice of v_0.

Finally, let us prove that $\dim_2 \mathrm{Sel}_2(E_c^{(1)}) < \dim_2 \mathrm{Sel}_2(E^{(1)})$. This time the places where the Selmer conditions of $E^{(1)}$ and $E_c^{(1)}$ differ are v_0, v_1 and $w_2^{(1)}$. By Example 5.13 we have $U_{v_0} = U_{v_1} = \{0\}$ and $\dim_2 U_{w_2^{(1)}} = 1$. Applying Lemma 5.14 with $T = \{v_0, v_1, w_2^{(1)}\}$ we have

$$\dim_2(\mathrm{Sel}(E_c^{(1)})) - \dim_2(\mathrm{Sel}(E^{(1)})) = \dim_2(V_{T,c}) - \dim_2(V_T)$$

with

$$\dim_2(V_{T,c}) + \dim_2(V_T) \leq 5$$

and by the same argument as above we see that the image of the 2-torsion is of dimension 2 in both $V_{T,c}, V_T$. To finish the proof it will suffice to show that the image of β in V_T is not spanned by the image of the 2-torsion. By our choice of v_0 the component β_1 of β reduces to a non-square mod v_0, and in addition we know that β is unramified at $w_2^{(1)}$. A direct examination now verifies that out of the pairs $([b_i - a_i], [b_i(b_i - a_i)])$, $([a_i(a_i - b_i)], [a_i - b_i])$ and $([-a_i], [-b_i])$ corresponding to the 2-torsion points, there is no pair which is both unramified at $w_2^{(1)}$ and whose first component is a non-square at v_0. □

References

[1] Bender A. O., Swinnerton-Dyer P., Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbb{P}^4$, *Proceedings of the London Mathematical Society*, 83.2, 2001, p. 299–329.

[2] Browning T. D., Matthiesen L., Skorobogatov A. N., Rational points on pencils of conics and quadrics with many degenerate fibres, *Annals of Mathematics*, 2014, p. 381–402.

[3] Cassels J. W. S., Arithmetic on Curves of Genus 1 (IV), *Journal für die reine und angewandte Mathematik*, 211, 1962, p. 95–112.

[4] Colliot-Thélène J.-L., Surfaces de Del Pezzo de degré 6, CR Acad. Sci. Paris Sér. AB 275, 1972, p. A109–A111.

[5] Colliot-Thélène J.-L., Surfaces rationnelles fibrées en coniques de degré 4, Séminaire de théorie des nombres, Paris 1989–91.

[6] Colliot-Thélène J.-L., Hasse principle for pencils of curves of genus one whose Jacobians have a rational 2-division point.

[7] Colliot-Thélene J.-L., Sansuc J.-J., Swinnerton-Dyer P., Intersections of two quadrics and Châtelet surfaces, *Journal für die reine und angewandte Mathematik 373*, 1987.

[8] Colliot-Thélene J-L., Skorobogatov A. N., Swinnerton-Dyer P., Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, *Inventiones mathematicae*, 134.3, 1998, p. 579–650.

[9] Colliot-Thélène J.-L., Pál A., Skorobogatov A. N., Pathologies of the Brauer—Manin obstruction, *Mathematische Zeitschrift*, 282.3-4, 2016, p. 799–817.

[10] Creutz B., No transcendental Brauer-Manin obstruction on abelian varieties, preprint arXiv:1711.01541, 2017.

[11] Creutz B., Viray B., Degree and the Brauer-Manin obstruction, preprint arXiv:1703.02187, 2017.

[12] Harpaz Y., Second descent and rational points on Kummer varieties, *Proceedings of the London Mathematical Society*, 118.3, 2019, p. 606–648.

[13] Harpaz Y., Skorobogatov A.N., Singular curves and the étale Brauer–Manin obstruction for surfaces, *Annales Scientifiques de l'École Normale Supérieure*, 47, 2014, p. 765–778.

[14] Harpaz Y., Skorobogatov A. N., The Hasse principle for generalized kummer varieties.

[15] Harpaz Y. Skorobogatov A. N., Wittenberg O., The Hardy–Littlewood conjecture and rational points, *Compositio Mathematica*, 150.12, 2014, p. 2095–2111.

[16] Heath-Brown D. R., Moroz B. Z., On the representation of primes by cubic polynomials in two variables, *Proceedings of the London Mathematical Society*, 88.3, 2004, p. 289—312

[17] Manin Y. I., Le groupe de Brauer-Grothendieck en géométrie diophantienne, *Actes du Congrès International Des Mathématiciens*, Tome 1, 1970, p. 401–411.

[18] Mazur B., Rubin K., Ranks of twists of elliptic curves and Hilbert's tenth problem, *Inventiones Mathematicae*, 181.3, 2010, p. 541–575.
[19] Milne J. S, Comparison of the Brauer group with the Tate-Shafarevich group, *J. Fac. Science, Univ. Tokyo*, Sec. IA 28, 1981, p. 735–743.
[20] Poonen B., Insufficiency of the Brauer-Manin obstruction applied to étale covers, Annals of Mathematics, 171.3, 2010, p. 2157–2169.
[21] Poonen B., Stoll M., Cassels–Tate pairing on polarized abelian varieties. *Annals of Mathematics*, 150, 1999, p. 1109–1149.
[22] Roulleau X., Sarti A., Construction of Nikulin configurations on some Kummer surfaces and applications, preprint arXiv:1711.05968, 2017.
[23] Scharaschkin V, The Brauer-Manin obstruction for curves, to appear (1998).
[24] Skorobogatov A. N., Beyond the Manin obstruction, *Inventiones Mathematicae*, 135.2, 1999, p. 399–424.
[25] Skorobogatov A. N., *Torsors and rational points*, Vol. 144, Cambridge University Press, 2001.
[26] Skorobogatov A. N, Swinnerton-Dyer P, 2-descent on elliptic curves and rational points on certain Kummer surfaces, *Advances in Mathematics*, 198.2, 2005, p. 448–483.
[27] Stoll M., Finite descent obstructions and rational points on curves, *Algebra & Number Theory*, 1.4, 2007, p. 349–391.
[28] Swinnerton-Dyer P. Rational points on certain intersections of two quadrics, *Abelian varieties*, ed. W. Barth, K. Hulek and H. Lange, de Gruyter, Berlin, 1995, p. 273–292.
[29] Swinnerton-Dyer P., Rational points on some pencils of conics with 6 singular fibres, *Annales de la Faculté des sciences de Toulouse: Mathématiques*, Vol. 8, No. 2, 1999.
[30] Swinnerton-Dyer P., Arithmetic of diagonal quartic surfaces, II, *Proceedings of the London Mathematical Society*, 80.3, 2000, p. 513–544.
[31] Voskresenskiĭ V. E., Birational properties of linear algebraic groups, *Mathematics of the USSR-Izvestiya*, 4.1, 1970.
[32] Wittenberg O., *Intersections de deux quadriques et pinceaux de courbes de genre 1*, Springer, 2007.
[33] Wittenberg O., Rational points of surfaces fibered into curves of genus 1, Lausanne, Nov. 2012, available at: https://www.math.u-psud.fr/~wittenberg/transparents/lausanneexp.pdf.