SECOND DESCENT AND RATIONAL POINTS ON KUMMER VARIETIES

YONATAN HARPAZ

ABSTRACT. A powerful method, pioneered by Swinnerton-Dyer, allows one to study rational points on pencils of curves of genus 1 by combining the fibration method with a sophisticated form of descent. A variant of this method, first used by Skorobogatov and Swinnerton-Dyer in 2005, can be applied to the study of rational points on Kummer varieties. In this paper we extend the method to include an additional step of second descent. Assuming finiteness of the relevant Tate-Shafarevich groups, we use the extended method to show that the Brauer-Manin obstruction is the only obstruction to the Hasse principle on Kummer varieties associated to abelian varieties with all rational 2-torsion, under relatively mild additional hypotheses.

CONTENTS

1. INTRODUCTION

Let k be a number field. A fundamental problem in Diophantine geometry is to determine for which geometric classes of smooth, proper and simply connected varieties over k the Brauer-Manin obstruction is the only obstruction to the existence of a rational point. A geometric class which is expected to exhibit an extremely favorable behavior with respect to this question is the class of **rationally connected varieties**. Such varieties are always simply connected, and a conjecture of Colliot-Thélène ([CT01]) predicts that the set of rational points on a smooth, proper and rationally connected variety X over k is dense in the Brauer set of X. While this conjecture is still largely open, it has been established in a wide range of special cases. On the other extreme lie simply-connected varieties of **general type**. For this class Lang's conjecture asserts that rational points are not Zariski dense, and their existence is not expected to be controlled at all by the Brauer-Manin obstruction (see [SW95] and [Sm14] for two kinds of conditional counter-examples).

An intermediate class whose arithmetic is still quite mysterious is the class of simply connected Calabi-Yau varieties. In dimension 2, these varieties are also known as **K3 surfacecs**. A conjecture far less documented than the two conjectures above predicts that the Brauer-Manin obstruction is the only obstruction to the existence of rational points on K3 surfaces (see [Sk09, p. 77] and [SZ08, p. 484]). The only evidence towards this conjecture is conditional, and relies on a method invented by Swinnerton-Dyer in [SD95]. In the realm of K3 surfaces there are two cases in which this method has been applied. The first case is when the K3 surface in question admits a fibration into curves of genus 1 (see [CTSSD98],[SD00],[CT01],[Wi07]). In this case Swinnerton-Dyer's method depends on two big conjectures: the finiteness of Tate-Shafarevich groups of elliptic curves, and Schinzel's hypothesis. The second case is that of **Kummer surfaces** ([SSD05],[HS15]). In this case the method does not require Schinzel's hypothesis (using, in effect, the only known case of the hypothesis, which is covered by Dirichlet's theorem), but only the Tate-Shafarevich conjecture.

Recall that a Kummer surface over k is a K3 surface which is associated to a **2-covering** Y of an abelian surface A, by which we mean a torsor under A equipped with a map of torsors $p : Y \longrightarrow A$ which covers the multiplication-by-2 map $A \longrightarrow A$ (and so, in particular, p is finite tale of degree 16). Given Y, the data of such a map p 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** $X = \mathrm{Kum}(Y)$ 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.

It is well-known that the Kummer surface X does not determine A and Y up to isomorphism (see, e.g., [RS17]). 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).

When applying Swinnerton-Dyer's method to a Kummer surface X, one typically assumes the finiteness of the 2-primary part of the Tate-Shafarevich groups for all the associated abelian surfaces $\mathscr{A}_t$. Interestingly enough, the finiteness of the 2-primary part of $Ш(\mathscr{A}_t)$ is actually equivalent to the statement that the Brauer-Manin obstruction to the Hasse principle is the only one for any 2-covering of $\mathscr{A}_t$ (the implication of the latter by the former is classical, see [Ma71, Thorme 6], and the inverse implication follows from [Cr17, Theorem 1]). In fact, to make the method work it is actually sufficient to assume that the Brauer-Manin obstruction is the only one for all the $\mathscr{Y}_t$ (as apposed to all the 2-coverings of all the $\mathscr{A}_t$). Equivalently, one just needs to assume that the class $[\mathscr{Y}_t] \in H^1(k, \mathscr{A}_t)$ is not a non-trivial divisible element of $Ш(\mathscr{A}_t)$ for any t. We may consequently consider a successful application of Swinnerton-Dyer's method to a given Kummer surface as establishing, **unconditionally**, an instance of the following conjecture:

Conjecture 1.1. *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 1.2. In Conjecture 1.1 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 [CV17, Theorem 1.2 and Theorem 1.7].

Conjecture 1.1 combined with the Tate-Shafarevich conjecture together imply that the Brauer-Manin obstruction controls the existence of rational points on Kummer surfaces. We may therefore consider any instance of Conjecture 1.1 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.

Let us now recall the strategy behind Swinnerton-Dyer's method. 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 $\dim_{\mathbb{F}_2} Ш(A^F)[2] \leq 1$. 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 (see §3.4 for further details). In that case it is known (see [PS99]) 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 1.1). Indeed, the latter is generally weaker but implies the former when $Ш(A^F)[2]$ is generated by $[Y^F]$.

The process of controlling the 2-Selmer group of A^F while modifying F can be considered as a type of **2-descent procedure** done "in families". In his paper [SD00], Swinnerton-Dyer remarks that in some situations one may also take into account considerations of **second descent**. This idea is exploited in [SD00] to show a default of weak approximation on a particular family of quartic surfaces, but is not included systematically as an argument for the **existence** of rational points. As a main novelty of this paper, we introduce a form of Swinnerton-Dyer's method which includes a built-in step of "second 2-descent in families". This involves a somewhat delicate analysis of the way the Cassels-Tate pairing changes under quadratic twists. It is this step that allows us to obtain Theorem 1.3 below under reasonably simple assumptions, which resemble the type of assumptions used in [SSD05], and does not require an analogue of [SSD05]'s Condition (E). Beyond this particular application, our motivation for introducing second descent into Swinnerton-Dyer's method is part of a long term goal to obtain a unified method which can be applied to an as general as possible Kummer surface. In principle, we expect the method as described in this paper and the method as appearing in [HS15] to admit a common generalization, which would be applicable, say, to certain cases where the Galois module $A[2]$ is **semi-simple**, specializing to the cases of [HS15] when the action is simple and to the cases of [SSD05] and the current paper when the action is trivial.

With this motivation in mind, our main goal in this paper is to prove Conjecture 1.1 for a certain class of Kummer surfaces. 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

$$\sum_i \frac{b_i x_i^2}{f'(a_i)} = \sum_i \frac{a_i b_i x_i^2}{f'(a_i)} = \sum_i \frac{a_i^2 b_i x_i^2}{f'(a_i)} = 0. \tag{1}$$

By [Sk10, Theorem 3.1] 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 (1) 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 $\prod_i \varepsilon_i = 1$ (see, e.g.,[Mu84, Lemma 2.4]). 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 $x_i \mapsto \varepsilon_i x_i$ (see [Sk10, Proof of Theorem 3.1]). 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. Our main result is then the following:

Theorem 1.3. *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 1.1 holds for the Kummer surface X given by (1). 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 1.2).

The first known case of Conjecture 1.1 was established in [SSD05]. In that paper, Skorobogatov and Swinnerton-Dyer consider K3 surfaces which are smooth and proper models of the affine surface

$$y^2 = g_0(x)g_1(z) \tag{2}$$

where g_0, g_1 are separable polynomials of degree 4. These are in fact Kummer surfaces whose associated family of 2-coverings $\mathscr{Y}_t$ is the family of quadratic twists of the surface $D_0 \times D_1$, where D_i is the genus 1 curve given by

$$D_i : y^2 = g_i(x).$$

The associated family of abelian surfaces $\mathscr{A}_t$ is the family of quadratic twists of $E_0 \times E_1$, where E_i is the Jacobian of D_i given by $E_i : y^2 = f_i(x)$, where f_i is the cubic resolvant of g_i. Three types of conditions are required in [SSD05]:

(1) The curves E_0, E_1 have all their 2-torsion defined over k, i.e., f_0 and f_1 split completely in k. Equivalently, the discriminants of g_0 and g_1 are squares and their splitting fields are at most biquadratic.
(2) Condition (Z). This condition asserts the existence, for each $i = 0, 1$, of multiplicative places v_i, w_i for E_i satisfying suitable conditions, and at which, in particular, E_{1-i} has good reduction and the classes α_0, α_1 are non-ramified. It is known to imply that the 2-primary part of the Brauer group of X is algebraic.
(3) Condition (E). This condition, which we shall not describe here, is to some extent analogous to Condition (D) in applications of the method to pencils of genus 1 curves. It is known to imply, in particular, that there is no algebraic Brauer-Manin obstruction to the existence of rational points on X.

Given a Kummer surface X of the form (2) satisfying the above conditions, the main result of [SSD05] asserts that Conjecture 1.1 holds for X. Even more, under conditions (1)-(3) above there is no 2-primary Brauer-Manin obstruction on X. It then follows (see Remark 1.2), and this is how the main theorem of [SSD05] is actually stated, that under the Tate-Shafarevich conjecture for all the quadratic twists of E_0, E_1, the **Hasse principle** holds for X.

The second case of conjecture 1.1 established in the literature appears in [HS15], where the authors consider also **Kummer varieties**, i.e., varieties obtained by applying the Kummer construction to abelian varieties of arbitrary dimension. When restricted to surfaces, the results of [HS15] cover two cases:

(1) The case where X is of the form (2) where now g_0, g_1 are polynomials whose Galois group is S_4. The only other assumption, which is analogous to Condition (Z) above, is that there exist odd places w_0, w_1 such that g_0 and g_1 are w_i-integral and such that $\mathrm{val}_{w_i}(\mathrm{disc}(g_j)) = \delta_{i,j}$ for $i, j = 0, 1$.
(2) The case where $X = \mathrm{Kum}(Y)$ and Y is a 2-covering of the Jacobian A of a hyperelliptic curve $y^2 = f(x)$, with f is an irreducible polynomial of degree 5. In this case X can be realized as an explicit complete intersection of three quadrics in $\mathbb{P}^5$. It is then required that there exists an odd place w such that f is w-integral and $\mathrm{val}_w(\mathrm{disc}(f)) = 1$, and such that the class $\alpha \in H^1(k, A[2])$

associated to Y is unramified at w.

Remark 1.4. While the main theorem of [HS15] can be considered as establishing Conjecture 1.1 for the Kummer surfaces of type (1) and (2), what it actually states is that under the 2-primary Tate-Shafarevich conjecture (for the relevant abelian varieties) the Kummer surfaces of type (1) and (2) satisfy the Hasse principle. The gap between these two claims can be explained by a recent paper of Skorobogatov and Zarhin [SZ16], which shows, in particular, that there is no 2-primary Brauer-Manin obstruction for Kummer surfaces of type (1) and (2) (see also Remark 1.2).

2. Main results

While our main motivation in this paper comes from Kummer surfaces, it is often natural to work in the more general context of **Kummer varieties**. These are the higher dimensional analogues of Kummer surfaces which are obtained by applying the same construction to a 2-covering Y of an abelian variety A of dimension $g \geq 2$. A detailed discussion of such varieties occupies the majority of §3.3. For now, we will focus on formulating the main theorem of this paper in the setting of Kummer varieties and show how Theorem 1.3 is implied by it. We begin with some terminology which will be used throughout this paper.

Let k be a number field and let A be a principally polarized abelian variety of dimension g over k. Assume that $A[2](k) \cong (\mathbb{Z}/2)^{2g}$, i.e., that A has all of its 2-torsion points defined over k. Let $\mathcal{A}$ be the Nron model for A. We will denote by C_v the component group of the geometric special fiber of $\mathcal{A}$ at v. Generalizing the ideas of [SSD05], we will need to equip A with a collection of "special places". We suggest the following terminology:

Definition 2.1. Let A be an abelian variety over k whose 2-torsion points are all rational. A **2-structure** on A is a set $M \subseteq \Omega_k$ consisting of $2g$ odd places of **bad semi-abelian reduction** and such that the natural map

$$A[2] \longrightarrow \oplus_{w \in M} C_w/2C_w \tag{3}$$

is an **isomorphism**.

Remark 2.2. If M is a 2-structure for A then for each $w \in M$ the composed map $C_w[2] \longrightarrow C_w \longrightarrow C_w/2C_w$ is surjective, implying that the 2-primary part of C_w is all 2-torsion, i.e., isomorphic to $(\mathbb{Z}/2)^{r_w}$ for some r_w. Since A has all its 2-torsion defined over k this r_w must be equal to the toric rank of the (semi-abelian) reduction at w, which we assume to be at least 1. The map (3) being an isomorphism then implies that each $r_w = 1$. In particular, the reduction at each $w \in M$ is semi-abelian of toric rank 1 and the 2-primary part of C_w is cyclic of order 2.

To formulate our main result we will also need the following extension of the notion of a 2-structure:

Definition 2.3. Let A be an abelian variety over k whose 2-torsion points are all rational. An **extended 2-structure** on A is a set $M \subseteq \Omega_k$ consisting of $2g+1$ odd places of bad semi-abelian reduction such that for every $w \in M$ the set $M \smallsetminus \{w\}$ is a 2-structure.

Example 2.4. Let E be an elliptic curve given by $y^2 = (x-c_1)(x-c_2)(x-c_3)$. If w_1, w_2, w_3 are three places such that $\mathrm{val}_{w_i}(c_j - c_k) = 1$ for any permutation i, j, k

of $1, 2, 3$, and such that $\mathrm{val}_{w_i}(c_i - c_j) = 0$ for any two $i \neq j$, then $\{w_1, w_2, w_3\}$ constitutes an extended 2-structure for E.

Remark 2.5. If $M \subseteq \Omega_k$ is an extended 2-structure for A then $C_w/2C_w \cong \mathbb{Z}/2$ for every $w \in M$ (see Remark 2.2). Furthermore, the natural map

$$A[2] \longrightarrow \oplus_{w \in M} C_w/2C_w \tag{4}$$

is injective and its image consists of those vectors $(c_w)_{w\in M} \in \prod_{w\in M} C_w/2C_w$ for which $c_w \neq 0$ at an even number of $w \in M$.

Remark 2.6. If A carries an extended 2-structure M then A is necessarily **simple** (over k). Indeed, if $A = A_1 \times A_2$ then for every place w we have $C_w = C_{w,1} \times C_{w,2}$, where $C_{w,1}, C_{w,2}$ are the corresponding geometric component groups for A_1, A_2 respectively. Since the 2-primary part of C_w for $w \in M$ is cyclic of order 2 (Remark 2.2) we see that the 2-primary part of $C_{w,i}$ must be cyclic of order 2 for one $i \in \{1, 2\}$ and trivial for the other. We may then divide M into two disjoint subsets $M = M_1 \cup M_2$ such that for $w \in M_i$ we have $C_{w,j}/2C_{w,j} \cong (\mathbb{Z}/2)^{\delta_{i,j}}$. By definition $M \smallsetminus \{w\}$ is a 2-structure for every $w \in M$. It then follows that $|M_i \smallsetminus \{w\}| \geq 2\dim(A_i)$ for every $i = 1, 2$ and every $w \in M_i$ and so $|M| = |M_0| + |M_1| \geq 2\dim(A_0) + 1 + 2\dim(A_1) + 1 = 2g + 2$, a contradiction.

Definition 2.7 ((cf. [HS15, Definition 3.4]))**.** Let M be a semi-simple Galois module and let R be the endomorphism algebra of M (in which case R naturally acts on $H^1(k, M)$). We will say that $\alpha \in H^1(k, M)$ is **non-degenerate** if the R-submodule generated by α in $H^1(k, M)$ is free.

Definition 2.7 will be applied to the Galois module $M = A[2]$, which in our case is a trivial Galois module isomorphic to $(\mathbb{Z}/2)^n$, and so R is the $n \times n$ matrix ring over $\mathbb{Z}/2$. In particular, if $\alpha = (\alpha_1, ..., \alpha_n) \in H^1(k, (\mathbb{Z}/2)^n) \cong H^1(k, \mathbb{Z}/2)^n$ is an element then α is non-degenerate if and only if the classes $\alpha_1, ..., \alpha_n \in H^1(k, \mathbb{Z}/2)$ are linearly independent.

We are now ready to state our main result.

Theorem 2.8. *Let k be a number field and let $A_1, ..., A_n$ be principally polarized abelian varieties over k such that each A_i has all its 2-torsion defined over k. For each i, let $M_i \subseteq \Omega_k$ be an extended 2-structure on A_i such that A_j has good reduction over M_i whenever $j \neq i$. Let $A = \prod_i A_i$ and let $\alpha \in H^1(k, A[2])$ be a non-degenerate element which is unramified over $M = \cup_i M_i$ but has non-zero image in $H^1(k_w, A[2])$ for each $w \in M$. Let $X_\alpha = \mathrm{Kum}(Y_\alpha)$ where Y_α is the 2-covering of A determined by α. Then Conjecture 1.1 holds for X_α. In particular (see Remark 1.2), under the 2-primary Tate-Shafarevich conjecture the 2-primary Brauer-Manin obstruction is the only one for the Hasse principle on X_α.*

Remark 2.9. The proof of Theorem 2.8 actually yields a slightly stronger result: under the Tate-Shafarevich conjecture the 2-primary **algebraic** Brauer-Manin obstruction is the only one for the Hasse principle on X (see Remark 4.9). In fact, one can isolate an explicit finite subgroup $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)$ (see Definition 4.3) whose associated obstruction is, in this case, the only one for the Hasse principle.

Remark 2.10. When A is a product of two elliptic curves with rational 2-torsion points one obtains the same type of Kummer surfaces as the ones studied in [SSD05]. However, the conditions required in Theorem 2.8 are not directly comparable to those of [SSD05]. On the one hand, Theorem 2.8 does not require any analogue of Condition (E). On the other hand, Theorem 2.8 requires each elliptic curve to come equipped with an extended 2-structure (consisting, therefore, of three special places for each curve, see Example 2.4), while the main theorem of [SSD05] only requires each elliptic curve to have a 2-structure (consisting, therefore, of two special places for each curve). Modifying the argument slightly, one can actually make the proof of Theorem 2.8 work with only a 2-structure for each A_i, at the expense of assuming some variant of Condition (E). In the case of a product of elliptic curves, this variant is slightly weaker than the Condition (E) which appears in [SSD05]. This can be attributed to the existence of a phase of second descent, which does not appear in [SSD05].

We finish this section by showing how Theorem 1.3 can be deduced from Theorem 2.8. Let $f(x) = \prod_{i=0}^{5}(x - a_i) \in k[x]$ be a polynomial of degree 6 which splits completely in k and such that $d := \prod_{i<j}(a_j - a_i) = \sqrt{\mathrm{disc}(f)} \neq 0$. Let C be the hyperelliptic curve given by $y^2 = f(x)$ and let A be the Jacobian of C. 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 $\prod_i \varepsilon_i = 1$ (see [Mu84, Lemma 2.4]). Consequently, if we denote by $\mathcal{G} := k^*/(k^*)^2 = H^1(k, \mu_2)$ then we may identify

$$H^1(k, A[2]) \cong \left\{(\beta_0, ..., \beta_5) \in \mathcal{G}^W \,\middle|\, \prod \beta_i = 1\right\}/\mathcal{G}.$$

In particular, we may represent elements of $H^1(k, \mu_2)$ by vectors of the form $\overline{b} = (b_0, ..., b_5) \in (k^*)^W$, satisfying the condition that $\prod_i b_i \in (k^*)^2$, and defined up to squares and up to multiplication by a constant $b \in k^*$. We note that the corresponding element $\beta = [\overline{b}] \in H^1(k, A[2])$ is non-degenerate (in the sense of Definition 2.7) if and only if the classes $[b_1/b_0], ..., [b_4/b_0]$ are linearly independent in $k^*/(k^*)^2$.

of Theorem 1.3 assuming Theorem 2.8. Let Y be the 2-covering of A determined by the class $\beta = [\overline{b}] \in H^1(k, A[2])$. Then the Kummer surface $X = \mathrm{Kum}(Y)$ is isomorphic to the smooth complete intersection (1) by [Sk10, Theorem 3.1]. Assumption (2) of Theorem 1.3 effectively states that β is unramified over $M = \{w_1, ..., w_5\}$ but is non-trivial at each $H^1(k_{w_i}, A[2])$. To show that the assumptions of Theorem 2.8 hold it will hence suffice to show that M forms an extended 2-structure for A. Now for each i the polynomial f is w_i-integral and the place w_i satisfies $\mathrm{val}_{w_i}(a_i - a_0) = 1$ and $\mathrm{val}_{w_i}(a_j - a_{j'}) = 0$ whenever $j \neq j'$ and $\{j, j'\} \neq \{0, i\}$. Since f is w_i-integral it determines a w_i-integral model $\mathcal{C}$ for C, and a local analysis shows that the reduction of $\mathcal{C}$ mod w_i is a curve of geometric genus 1 and a unique singular point P, which is also a rational singular point of the model $\mathcal{C}$. Blowing up at P one obtains a regular model for C at w_i whose special fiber has two components (of genus 1 and 0 respectively) which intersect at two points. Using [BLR90, Theorem 9.6.1] we may compute that the group of components C_{w_i} of a Néron model for A is isomorphic to $\mathbb{Z}/2$. Now for each $i = 1, ..., 4$ let $P_i \in A$ be the point corresponding to the formal sum $(a_i, 0) - (a_5, 0)$ of points of C. Then for $i, j = 1, ..., 4$ we have that the image of P_i in C_{w_j} is nontrivial if and only if $i = j$. On the other hand, all the four points $P_1, ..., P_4$ map to the non-zero component of

w_5. It then follows that the map

$$A[2] \longrightarrow \prod_{i=1}^{5} C_{w_i} = \prod_{i=1}^{5} C_{w_i}/2C_{w_i}$$

is injective and its image consists of exactly those vectors $(c_1, ..., c_5) \in \prod_{i=1}^{5} C_{w_i}$ in which an even number of the entries are non-trivial. We may hence conclude that the composed map $A[2] \longrightarrow \prod_{i=1}^{5} C_{w_i} \longrightarrow \prod_{i=1,...,5; i \neq i_0} C_{w_i}$ is an isomorphism for any $i_0 \in \{1, ..., 5\}$, and so M constitutes an extended 2-structure, as desired. □

3. Preliminaries

In this section we establish some preliminary machinery that will be used in §4 to prove Theorem 2.8. We begin in §3.1 by recalling the **Weil pairing** and establishing some useful lemmas in the case where all the 2-torsion points of A are defined over k. In §3.2 we simply recall a definition of the Cassels-Tate pairing via evaluation of Brauer elements. In §3.3 we give a short introduction to Kummer varieties and consider cases where the Brauer elements appearing in §3.2 descend to the corresponding Kummer varieties. Finally, in §3.6 we recall the approach of Mazur and Rubin to the analysis of the change of Selmer groups in families of quadratic twists. While mostly relying on ideas from [MR10], this section is essentially self-contained, and we give detailed proofs of all the results we need. We then complement the discussion of Selmer groups in families of quadratic twist by considering the change of the **Cassels-Tate pairing** under quadratic twist, using the results of §3.3.

3.1. The Weil pairing.

Let A be an abelian variety over a number field k and let $\hat{A}$ be its dual abelian variety. Recall that for $n \geq 1$ we have the **Weil pairing**

$$\langle , \rangle^n : A[n] \times \hat{A}[n] \longrightarrow \mu_n,$$

which is a perfect pairing of finite Galois modules. For positive integers m, k and $n = mk$ the Weil pairings associated to m and n are compatible in the following sense: if $P \in A[n]$ and $Q \in \hat{A}[m]$ then $\langle kP, Q\rangle^m = \langle P, Q\rangle^n \in \mu_m \subseteq \mu_n$. If A is equipped with a principal polarization, i.e., a self dual isomorphism $\lambda : A \xrightarrow{\cong} \hat{A}$, then we obtain an induced isomorphism $A[n] \cong \hat{A}[n]$ and an induced self-pairing

$$\langle , \rangle^n_\lambda : A[n] \times A[n] \longrightarrow \mu_n \tag{5}$$

which is known to be **alternating**. We will be mostly interested in the case $n = 2$, where we will denote the corresponding Weil pairing simply by $\langle , \rangle_\lambda$. We note that the principal polarization λ induces a principal polarization $A^F \xrightarrow{\cong} \hat{A}^F$ after quadratic twist by any quadratic extension F/k. To keep the notation simple we will use the same letter λ to denote all these principal polarizations. Similarly, we will denote by $\langle , \rangle^n_\lambda$ all the associated Weil pairings.

From now until the end of this section we shall **fix the assumption** that A has all of its 2-torsion points defined over k. Let M be a 2-structure on A (see Definition 2.1). For each $w \in M$ let $Q_w \in A[2]$ be such that the image of Q_w in $C_{w'}/2C_{w'}$ for $w' \in M$ is non-trivial if and only if $w = w'$. It then follows from Definition 2.1 that $\{Q_w\}_{w \in M}$ forms a basis for $A[2]$. We will denote by $\{P_w\}$ the dual basis of $\{Q_w\}$ with respect to the Weil pairing. We note that by construction $\langle P_w, Q\rangle_\lambda = -1$ for a given point $Q \in A[2]$ if and only if the image of Q in $C_w/2C_w$

is non-trivial.

Remark 3.1. The 2-torsion modules $A[2]$ and $A^F[2]$ are **canonically** isomorphic for any F/k. We will consequently often abuse notation and denote by $A[2]$ the 2-torsion module of any given quadratic twist of A. Since the Weil pairing (5) depends only on the base change of A to $\overline{k}$ we see that the Weil pairings induced on $A[2] \cong A^F[2]$ by all quadratic twists of λ are the same.

Remark 3.2. While our notation for the group structure on $A[2]$ is additive, i.e., we write $P + Q$ for the sum of two points $P, Q \in A[2]$, our notation for the group structure on $\mu_2 = \{-1, 1\}$ is **multiplicative**. For example, the linearity of the Weil pairing $\langle , \rangle_\lambda$ in its left entry will be written as $\langle P + Q, R\rangle_\lambda = \langle P, R\rangle_\lambda \langle Q, R\rangle_\lambda$. Similarly, the group operation of $H^1(k, A[2])$ will be written additively, while that of $H^1(k, \mu_2)$ multiplicatively.

In what follows it will be useful to consider the bilinear pairing

$$\langle , \rangle_\lambda : H^1(k, A[2]) \times A[2] \longrightarrow H^1(k, \mu_2) \tag{6}$$

induced by the Weil pairing, and which by abuse of notation we shall denote by the same name.

Definition 3.3. We will denote by $\delta : A(k) \longrightarrow H^1(k, A[2])$ the boundary map induced by the Kummer sequence of A. Similarly, for a quadratic extension F/k we will denote by $\delta_F : A^F(k) \longrightarrow H^1(k, A[2])$ the boundary map associated to the Kummer sequence of A^F, where we have implicitly identified $A^F[2]$ with $A[2]$ (see Remark 3.1).

Remark 3.4. The bilinear map $(P, Q) \mapsto \langle \delta(P), Q\rangle_\lambda \in H^1(k, \mu_2)$ is **not** symmetric in general. While this fact will not be used in this paper we note more precisely that

$$\langle \delta(P), Q\rangle_\lambda \langle \delta(Q), P\rangle_\lambda = [\langle P, Q\rangle_\lambda],$$

where $[\langle P, Q\rangle_\lambda]$ denotes the image of $\langle P, Q\rangle_\lambda \in \mu_2$ under the composed map $\mu_2 \longrightarrow k^* \longrightarrow k^*/(k^*)^2 \cong H^1(k, \mu_2)$.

For the purpose of the arguments in §4 we will need to establish some preliminary lemmas. The first one concerns the behavior of the bilinear map $(P, Q) \mapsto \langle \delta(P), Q\rangle_\lambda$ under quadratic twists.

Lemma 3.5. *Let A be a principally polarized abelian variety with all 2-torsion points defined over k and let $P, Q \in A[2]$ be two 2-torsion points. Let $F = k(\sqrt{a})$ be a quadratic extension. Then*

$$\langle \delta_F(P), Q\rangle_\lambda \langle \delta(P), Q\rangle_\lambda^{-1} = \begin{cases} 1 & \langle P, Q\rangle_\lambda = 1 \\ [a] & \langle P, Q\rangle_\lambda = -1 \end{cases}$$

where $[a] \in k^*/(k^*)^2 \cong H^1(k, \mu_2)$ denotes the class of a mod squares.

Proof. Let $Z_P \subseteq A$ be the finite subscheme determined by the condition $2x = P$. Then Z_P carries a natural structure of an $A[2]$-torsor whose classifying element in $H^1(k, A[2])$ is given by $\delta(P)$. Given a point $x \in Z_P(\overline{k})$ we can represent $\delta(P)$ by the 1-cocycle $\sigma \mapsto \sigma(x) - x$, and consequently represent $\langle \delta(P), Q\rangle_\lambda$ by the 1-cocycle $\sigma \mapsto \langle \sigma(x) - x, Q\rangle_\lambda \in \mu_2$. Let Γ_k be the absolute Galois group of k and let $\chi : \Gamma_k \longrightarrow \mu_2$ be the quadratic character associated with F/k. In light of Remark 3.1

we see that the class $\langle \delta_F(P), Q\rangle_\lambda$ can be represented by the 1-cocycle

$$\sigma \mapsto \langle \chi(\sigma)\sigma(x) - x, Q\rangle_\lambda \in \mu_2.$$

We may hence compute that

$$\langle \chi(\sigma)\sigma(x) - x, Q\rangle_\lambda \langle \sigma(x) - x, Q\rangle_\lambda^{-1} = \langle (\chi(\sigma) - 1)\sigma(x), Q\rangle_\lambda = \begin{cases} 1 & \chi(\sigma) = 1 \\ \langle P, Q\rangle_\lambda & \chi(\sigma) = -1 \end{cases}$$

This means that when $\langle P, Q\rangle_\lambda = 1$ the class $\langle \delta_F(P), Q\rangle_\lambda \langle \delta(P), Q\rangle_\lambda^{-1}$ vanishes, and when $\langle P, Q\rangle_\lambda = -1$ the class $\langle \delta_F(P), Q\rangle_\lambda \langle \delta(P), Q\rangle_\lambda^{-1}$ coincides with $[a]$, as desired. □

For a place $w \in \Omega_k$ we will denote by k_w^{un}/k_w the maximal unramified extension of k_w and by $\Gamma_{k_w^{\mathrm{un}}}$ the absolute Galois group of k_w^{un}. The following lemma concerns the Galois action on certain 4-torsion points which are defined over extensions ramified at w. The proof makes use of the Weil pairing.

Lemma 3.6. *Let $w \in M$ be a place in the 2-structure M of A and let $P \in A[2]$ be a point whose image in $C_w/2C_w$ is non-trivial. Let $x \in A(\overline{k})$ be a point such that $2x = P$ and let L_P/k_w^{un} be the minimal Galois extension of k_w^{un} such that x is defined over L_P. Then $\mathrm{Gal}(L_P/k_w^{\mathrm{un}}) \cong \mathbb{Z}/2$ and if $\sigma \in \mathrm{Gal}(L_P/k_w^{\mathrm{un}})$ is the non-trivial element then $\sigma(x) = x + P_w$.*

Proof. Since P is divisible by 2 in $A(L_P)$ the class $\delta(P)$ maps to 0 in $H^1(L_P, A[2])$. The restriction of $\delta(P)$ to k_w^{un} then determines a homomorphism $\Gamma_{k_w^{\mathrm{un}}} \longrightarrow A[2]$ which descends to an injective homomorphism $\mathrm{Gal}(L_P/k_w^{\mathrm{un}}) \longrightarrow A[2]$. In particular, L_P is a finite abelian 2-elementary extension of k_w^{un}. Since w is odd L_P/k_w^{un} is tamely ramified and hence cyclic, which means that $\mathrm{Gal}(L_P/k_w^{\mathrm{un}})$ is either $\mathbb{Z}/2$ or trivial. Since the image of P in $C_w/2C_w$ is non-trivial x cannot be defined over k_w^{un} and we may hence conclude that $\mathrm{Gal}(L_P/k_w^{\mathrm{un}}) \cong \mathbb{Z}/2$. Let $\sigma \in \mathrm{Gal}(L_P/k_w^{\mathrm{un}})$ be the non-trivial element.

Let $Q \in A[2]$ be any 2-torsion point whose image in $C_w/2C_w$ is trivial. It then follows from Hensel's lemma that there exists a $y \in A(k_w^{\mathrm{un}})$ such that $2y = Q$. Consider the Weil pairing

$$\langle , \rangle_\lambda^4 : A[4] \times A[4] \longrightarrow \mu_4$$

on 4-torsion. Then by the compatibility property of the Weil pairings we have

$$\langle \sigma(x) - x, Q\rangle_\lambda = \langle \sigma(x) - x, y\rangle_\lambda^4 = \langle \sigma(x), y\rangle_\lambda^4 \left[\langle x, y\rangle_\lambda^4\right]^{-1} = 1$$

where the last equality holds since $\sigma(y) = y$, the Weil pairing is Galois invariant, and μ_4 is fixed by σ. It follows that the 2-torsion point $\sigma(x) - x$ is orthogonal to every 2-torsion point whose w-reduction lies on the identity component. The only two 2-torsion points which have this orthogonality property are 0 and P_w by construction. The former option is not possible since x is not defined over k_w^{un} and hence we may conclude that $\sigma(x) - x = P_w$, as desired. □

We now explore two corollaries of Lemma 3.6.

Corollary 3.7. *Let $w \in M$ be a place in the 2-structure M of A, let L/k be a non-trivial quadratic extension which is ramified at w and let w' be the unique place of L lying above w. Let $A_L = A \otimes_k L$ be the base change of A to L and let $C_{w'}$ be the group of components of geometric fiber of the Nron model of A_L at w'. Then the*

2-primary part of $C_{w'}$ is cyclic of order 4 and the induced action of $\mathrm{Gal}(L/k)$ *on* $C_{w'}/4C_{w'} \cong \mathbb{Z}/4$ *is trivial.*

Proof. Since the reduction of A at w is semi-abelian the reduction of A_L at w' is semi-abelian as well by Grothendieck's semi-stable reduction theorem. By [HN10, Theorem 5.7] the natural map of component groups $C_w \longrightarrow C_{w'}$ is injective and $C_{w'}/C_w$ has order 2. Since all the 2-torsion points of A are defined over k the group $C_{w'}$ cannot have 2-torsion elements which do not come from C_w, and hence the 2-primary part of $C_{w'}$ must be cyclic of order 4.

Let $L' = L \cdot k_w^{\mathrm{un}}$ be the compositum of L and the maximal unramified extension k_w^{un}. Since L is purely ramified the map $\mathrm{Gal}(L'/k) \longrightarrow \mathrm{Gal}(L/k)$ is surjective and restricts to an isomorphism $\mathrm{Gal}(L'/k_w^{\mathrm{un}}) \xrightarrow{\cong} \mathrm{Gal}(L/k) \cong \mathbb{Z}/2$. Furthermore, this isomorphism is compatible with the actions of both sides on $C_{w'}$. To finish the proof it will hence suffice to show that $\mathrm{Gal}(L'/k_w^{\mathrm{un}})$ acts trivially on $C_{w'}/4C_{w'}$. To see this, let $\sigma \in \mathrm{Gal}(L'/k_w^{\mathrm{un}})$ be a generator and let $C \in C_{w'}$ be a component of order exactly 4. Then $C(\overline{\mathbb{F}}_{w'})$ must contain a point $\overline{x} \in C(\overline{\mathbb{F}}_{w'})$ of order exactly 4. Using Hensel's lemma we may lift $\overline{x}$ to a point $x \in A(L')$ of order exactly 4. It then follows that $P := 2x$ is a 2-torsion point whose reduction lies on a component of order exactly 2. By Lemma 3.6 we then have that $\sigma(x) = x + P_w$, and since the reduction of P_w lies on the identity component of $C_w \subseteq C_{w'}$ by construction (note $\langle P_w, P_w\rangle_\lambda = 1$) it follows that $\sigma(C) = C$. Since C is a component of order exactly 4 the image of C in $C_{w'}/4C_{w'}$ is a generator and hence the action of $\mathrm{Gal}(L'/k_w^{\mathrm{un}})$ on $C_{w'}/4C_{w'}$ is trivial, as desired. □

Corollary 3.8. *Let $P, Q \in A[2]$ be two points. Then $\alpha := \langle \delta(P), Q\rangle_\lambda$ is ramified at w if and only if the images of both P and Q in $C_w/2C_w$ are non-trivial.*

Proof. If P reduces to the identity of $C_w/2C_w$ then the entire class $\delta(P) \in H^1(k, A[2])$ is unramified. We may hence assume that P reduces to the non-trivial element of $C_w/2C_w$. Let $x \in A(\overline{k})$ be a point such that $2x = P$ and let L_P/k_w^{un} be the minimal Galois extension of k_w^{un} such that x is defined over L_P. By Lemma 3.6 we know that $G := \mathrm{Gal}(L_P/k_w^{\mathrm{un}})$ is isomorphic to $\mathbb{Z}/2$ and that if $\sigma \in G$ denotes the non-trivial element then $\sigma(x) - x = P_w$. Since $\delta(P)$ vanishes when restricted to L_P the same holds for α and by the inflation-restriction exact sequence the element $\alpha|_{k_w^{\mathrm{un}}}$ comes from an element $\overline{\alpha} \in H^1(L_P/k_w^{\mathrm{un}}, \mu_2) = H^1(G, \mu_2)$, which in turn can be written as a homomorphism $\overline{\alpha} : G \longrightarrow \mu_2$. Furthermore, as in the proof of Lemma 3.6 the value $\overline{\alpha}(\sigma)$ is given by the explicit formula

$$\overline{\alpha}(\sigma) = \langle \sigma(x) - x, Q\rangle_\lambda = \langle P_w, Q\rangle .$$

By the definition of P_w we now get that $\alpha|_{k_w^{\mathrm{un}}}$ is trivial if and only if Q reduces to the identity of $C_w/2C_w$, as desired. □

3.2. **The Cassels-Tate pairing.** Let A be an abelian variety over a number field k with dual abelian variety $\hat{A}$. Recall the **Cassels-Tate pairing**

$$\langle \alpha, \beta\rangle^{\mathrm{CT}} : Ш(A) \times Ш(\hat{A}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

whose kernel on either side is the corresponding group of divisible elements (which is conjectured to be trivial by Tate-Shafarevich).

There are many equivalent ways of defining the Cassels-Tate pairing. In this paper it will be useful to have an explicit description of it via evaluation of Brauer element. We will hence recall the following definition, which is essentially the "homogeneous space definition" appearing in [PS99]. Let $\alpha \in Ш(A), \beta \in Ш(\hat{A})$ be elements, we may describe the Cassels-Tate pairing $\langle \alpha, \beta \rangle^{\mathrm{CT}}$ as follows. Let Y_α be the torsor under A classified by α. Since α belongs to $Ш(A)$ we have that $Y_\alpha(\mathbb{A}_k) \neq \varnothing$. The Galois module $\mathrm{Pic}^0(\overline{Y}_\alpha)$ is canonically isomorphic to $\hat{A}(\overline{k})$. Let $\mathrm{Br}_1(Y_\alpha) = \mathrm{Ker}[\mathrm{Br}(Y_\alpha) \longrightarrow \mathrm{Br}(\overline{Y}_\alpha)]$ be the algebraic Brauer group of Y_α. The Hochschild-Serre spectral sequence yields an isomorphism

$$\mathrm{Br}_1(Y_\alpha)/\mathrm{Br}(k) \xrightarrow{\cong} H^1(k, \mathrm{Pic}(\overline{Y}_\alpha)).$$

Let

$$B_\alpha : H^1(k, \hat{A}) \xrightarrow{\cong} H^1(k, \mathrm{Pic}^0(\overline{Y}_\alpha)) \longrightarrow H^1(k, \mathrm{Pic}(\overline{Y}_\alpha)) \cong \mathrm{Br}_1(Y_\alpha)/\mathrm{Br}(k)$$

denote the composed map.

Definition 3.9. Let $B \in \mathrm{Br}(Y_\alpha)$ be an element whose class in $\mathrm{Br}(Y_\alpha)/\mathrm{Br}(k)$ is $B_\alpha(\beta)$ and let $(x_v) \in Y_\alpha(\mathbb{A}_k)$ be an adelic point. Then the Cassels-Tate pairing of α and β is given by

$$\langle \alpha, \beta \rangle^{\mathrm{CT}} := \sum_{v \in \Omega_k} B(x_v) \in \mathbb{Q}/\mathbb{Z}$$

Given a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$ we obtain an isomorphism $Ш(A) \cong Ш(\hat{A})$ and hence a self-pairing

$$\langle , \rangle^{\mathrm{CT}}_\lambda : Ш(A) \times Ш(A) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

Remark 3.10. The pairing $\langle , \rangle^{\mathrm{CT}}_\lambda$ is not alternating in general. However, as is shown in [PR11], it is the case that $\langle , \rangle^{\mathrm{CT}}_\lambda$ is alternating when λ is induced by a symmetric line bundle on A. The obstruction to realizing λ via a symmetric line bundle is an element $c_\lambda \in H^1(k, A[2])$, which vanishes, for example, when the Galois action on $A[2]$ is trivial, see [HS15, Lemma 5.1]. In particular, in all the cases considered in this paper the Cassels-Tate pairing associated to a principal polarization will be alternating.

3.3. **Kummer varieties.**

In this section we will review some basic notions and constructions concerning Kummer varieties. Let A be an abelian variety over k (not necessarily principally polarized) of dimension $g \geq 2$. Let $\alpha \in H^1(k, A[2])$ be a class and let Y_α be the associated 2-covering of A. Then Y_α is equipped with a natural action of $A[2]$ and the base change of Y_α to the algebraic closure of k is $A[2]$-equivariantly isomorphic to the base change of A. More precisely, the class α determines a distinguished Galois invariant subset of $A[2]$-equivariant isomorphisms $\Psi_\alpha \subseteq \mathrm{Iso}_{A[2]}(\overline{Y}_\alpha, \overline{A})$ which is a torsor under $A[2]$ with class α (where $A[2]$ acts on $\mathrm{Iso}_{A[2]}(\overline{Y}_\alpha, \overline{A})$ via post-composition). Using any one of the isomorphisms $\psi \in \Psi_\alpha$ we may transport the antipodal involution $[-1] : \overline{A} \longrightarrow \overline{A}$ to an involution $\iota_\psi : \overline{Y}_\alpha \longrightarrow \overline{Y}_\alpha$. Since $[-1]$ commutes with translations by $A[2]$ it follows that ι_ψ is independent of ψ, and is consequently Galois invariant. By classical Galois descent we may realize this Galois invariant automorphism uniquely as an automorphism $\iota_{Y_\alpha} : Y_\alpha \longrightarrow Y_\alpha$ defined over k.

Let $Z_\alpha \subseteq Y_\alpha$ denote the fixed locus of ι_{Y_α} (considered as a 0-dimensional subscheme). We note that the points of $Z_\alpha(\overline{k})$ are mapped to $A[2]$ by any of the isomorphisms $\psi \in \Psi_\alpha$, and the Galois invariant collection of isomorphisms $\{\psi|_{\overline{Z}_\alpha} | \psi \in \Psi_\alpha\}$

exhibits Z_α as a torsor under $A[2]$ with class α. The quotient $(Y_\alpha)/\iota_{Y_\alpha}$ has Z_α as its singular locus and this singularity can be resolved by a single blow-up. Alternatively, one can first consider the blow-up $\widetilde{Y}_\alpha$ of Y_α at Z_α, and then take the quotient of $\widetilde{Y}_\alpha$ by the induced involution $\iota_{\widetilde{Y}_\alpha}$. A local calculation then shows that $\widetilde{Y}_\alpha/\iota_{\widetilde{Y}_\alpha}$ is **smooth**.

Definition 3.11. The **Kummer variety** associated to Y_α is the variety

$$\mathrm{Kum}(Y_\alpha) = \widetilde{Y}_\alpha/\iota_{\widetilde{Y}_\alpha}$$

Let now $X_\alpha = \mathrm{Kum}(Y_\alpha)$ be the Kummer variety of Y_α. We will denote by $D_\alpha \subseteq \widetilde{Y}_\alpha$ the exceptional divisor. Since the action of $\iota_{\widetilde{Y}_\alpha}$ on D_α is trivial we will abuse notation and denote the image of D_α in X_α by the same name. Let us denote by $U_\alpha = \widetilde{Y}_\alpha \smallsetminus D_\alpha$ and $W_\alpha = X_\alpha \smallsetminus D_\alpha$, so that the quotient map $\widetilde{Y}_\alpha \longrightarrow X_\alpha$ restricts to an étale covering $p_\alpha : U_\alpha \longrightarrow W_\alpha$ of degree 2. Let $\iota_{U_\alpha} : U_\alpha \longrightarrow U_\alpha$ denote the restriction of ι_{Y_α}. We note that we may also identify U_α with the complement of the 0-dimensional scheme Z_α in Y_α. Since the codimension of Z_α in Y_α is at least 2 we may identify $H^1(\overline{U}_\alpha, \mathbb{Q}/\mathbb{Z}(1))$ with $H^1(\overline{Y}_\alpha, \mathbb{Q}/\mathbb{Z}(1)) \cong \hat{A}(\overline{k})_{\mathrm{tor}}$ and $H^1(\overline{U}_\alpha, \mathbb{Q}/\mathbb{Z}(1))^{\iota_{U_\alpha}}$ with $\hat{A}(\overline{k})^{[-1]}_{\mathrm{tor}} = \hat{A}[2]$. Applying the Hochshild-Serre spectral sequence and using the vanishing of $H^2(\langle \iota_{U_\alpha} \rangle, H^0(\overline{U}_\alpha, \mathbb{Q}/\mathbb{Z}(1))) = H^2(\langle \iota_{U_\alpha} \rangle, \mathbb{Q}/\mathbb{Z})$ we now obtain a short exact sequence of Galois modules

$$0 \longrightarrow \mu_2 \xrightarrow{\iota} H^1(\overline{W}_\alpha, \mathbb{Q}/\mathbb{Z}(1)) \xrightarrow{p_\alpha^*} \hat{A}[2] \longrightarrow 0 \tag{7}$$

where the image of ι is spanned the element $[p_\alpha] \in H^1(\overline{W}_\alpha, \mu_2) \subseteq H^1(\overline{W}_\alpha, \mathbb{Q}/\mathbb{Z}(1))$ which classifies the tale covering $p_\alpha : U_\alpha \longrightarrow W_\alpha$.

Our next goal is to describe the Galois module $H^1(\overline{W}_\alpha, \mathbb{Q}/\mathbb{Z}(1))$ in more explicit terms. For this it will be convenient to use the following terminology. Let us say that a map of schemes $L : \overline{Z}_\alpha \longrightarrow \mu_2$ is **affine-linear** if there exists a $Q \in \hat{A}[2]$ such that for every geometric point $x \in Z_\alpha(\overline{k})$ and every $P \in A[2]$ we have $L(Px) = \langle P, Q \rangle \cdot L(x)$ (here the notation Px denotes the action of $A[2]$ on its torsor Z_α). We will refer to Q as the **homogeneous part** of L. We note that Q (when exists) is uniquely determined by L. We will denote by $\mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$ the abelian group of affine-linear maps (under pointwise multiplication). The action of Γ_k on $\overline{Z}_\alpha$ induces an action on $\mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$ by pre-composition and we will consequently consider $\mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$ as a Galois module. The map

$$h_\alpha : \mathrm{Aff}(\overline{Z}_\alpha, \mu_2) \longrightarrow \hat{A}[2]$$

which assigns to each affine-linear map its homogeneous part is then a homomorphism of Galois modules. The following lemma is a variant of [SZ16, Proposition 2.3] and is essentially reformulated to make the Galois action more apparent. Here we consider $\mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$ as a Galois submodule of $H^0(\overline{Z}_\alpha, \mathbb{Q}/\mathbb{Z})$, by identifying elements of the latter with set theoretic functions $Z_\alpha(\overline{k}) \longrightarrow \mathbb{Q}/\mathbb{Z}$ and using the embedding $\mu_2 \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

Lemma 3.12 ((cf. [SZ16, Proposition 2.3]))**.** *The residue map $H^1(\overline{W}_\alpha, \mathbb{Q}/\mathbb{Z}(1)) \longrightarrow H^0(\overline{D}_\alpha, \mathbb{Q}/\mathbb{Z})$ is injective and its image coincides with $\mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$. Furthermore, the resulting composed map $H^1(\overline{W}_\alpha, \mathbb{Q}/\mathbb{Z}(1)) \longrightarrow \mathrm{Aff}(\overline{Z}_\alpha, \mu_2) \xrightarrow{h_\alpha} \hat{A}[2]$ coincides with the map p_α^* appearing in (7).*

Proof. For the purpose of this lemma we may as well extend our scalars to the algebraic closure. We may hence assume without loss of generality that $\alpha = 0$ (i.e., that $X = \mathrm{Kum}(A)$) and that the Galois action on $A[2]$ is trivial. We will consequently write A instead of Y, $A[2]$ instead of Z_α, W instead of W_α and U instead of U_α. Let $Q \in \hat{A}[2]$ be a non-zero element and let $f_Q : B \longrightarrow A$ be the degree 2 isogeny of abelian varities classified by $Q \in \hat{A}[2] \cong H^1(\overline{A}, \mu_2)$ (in particular, the kernel of the dual isogeny $\hat{f}_Q : \hat{A} \longrightarrow \hat{B}$ is spanned by Q). Given another point $P \in A[2]$ we will denote by $f_{Q,P} : B \longrightarrow A$ the map given by $f_{Q,P}(x) = f_Q(x) + P$.

Let $\widetilde{A}$ denote the blow-up of A at the subscheme $A[2]$ and let $\widetilde{B}$ be the variety obtained from B by blowing up the pre-image $M = f_Q^{-1}(A[2])$ of $A[2]$. For each $P \in A[2]$ the map $f_{Q,P}$ is a degree 2 tale covering sending M to $A[2]$ and hence induces an tale covering

$$\widetilde{f}_{Q,P} : \widetilde{B} \longrightarrow \widetilde{A}.$$

Consider the automorphisms $\iota_{\widetilde{B}} : \widetilde{B} \longrightarrow \widetilde{B}$ and $\iota_{\widetilde{A}} : \widetilde{A} \longrightarrow \widetilde{A}$ induced by the respective antipodal involutions. Since $f_{P,Q}$ commutes with the antipodal involutions the same holds for $\widetilde{f}_{Q,P}$. We then obtain an induced (ramified) degree 2 map between smooth varieties

$$g_{Q,P} : \widetilde{B}/\iota_{\widetilde{B}} \longrightarrow \widetilde{A}/\iota_{\widetilde{A}} = \mathrm{Kum}(A).$$

Note that $g_{Q,P}$ is unramified over the complement $W \subseteq \mathrm{Kum}(A)$ of the image of the exceptional divisor in $\widetilde{A}$: indeed, any geometric point $x \in W(\overline{k})$ has two points lying above it in $\widetilde{A}$, and hence four points lying above it in $\widetilde{B}$, which must give two distinct points in $\widetilde{B}/\iota_{\widetilde{B}}$. The pullback of $g_{Q,P}$ to W hence determines an tale map of degree 2

$$g'_{Q,P} : V \longrightarrow W$$

which is classified by an element $[g'_{Q,P}] \in H^1(W, \mu_2) \subseteq H^1(W, \mathbb{Q}/\mathbb{Z}(1))$. Now consider the commutative diagram

$$\begin{tikzcd} B \setminus M \arrow[r] \arrow[d, "f'_{Q,P}"'] & V \arrow[d, "g'_{Q,P}"] \\ U \arrow[r, "p"] & W \end{tikzcd} \tag{8}$$

where the map $f'_{Q,P}$ is obtained by restricting the domain and codomain of $f_{Q,P} : B \longrightarrow A$ and the horizontal maps are quotients by the respective antipodal involutions. Then all the maps in the square (8) are tale of degree 2 and by inspecting the fibers over W we see that the induced map $B \setminus M \longrightarrow V \times_W U$ is an isomorphism. It follows that $p^*[g'_{Q,P}] = [f'_{Q,P}] \in H^1(U, \mu_2)$. On the other hand, the inclusion $U \subseteq A$ as the complement of $A[2]$ induces an isomorphism $H^1(U, \mu_2) \cong H^1(A, \mu_2) \cong \hat{A}[2]$ which identifies the image of $[f'_{Q,P}]$ in $H^1(U, \mu_2)$ with $Q \in \hat{A}[2]$. Finally, a direct examination verifies that $g_{Q,P} : \widetilde{B}/\iota_{\widetilde{B}} \longrightarrow \widetilde{A}/\iota_{\widetilde{A}}$ is ramified at the exceptional divisor $D_x \subseteq X \setminus W$ corresponding to $x \in A[2]$ if and only if x is not in the image of $f_{Q,P}|_{B[2]} : B[2] \longrightarrow A[2]$. By the compatibility of the Weil pairing with duality of isogenies we see that the image of $f_{Q,P}|_{B[2]}$ consists of exactly those $x \in A[2]$ such that the Weil pairing $\langle x + P, Q\rangle$ is trivial. It then follows that the residue $\mathrm{res}_D([g'_{Q,P}]) \in H^0(\overline{A}[2], \mathbb{Q}/\mathbb{Z})$ can be identified with the affine-linear function $L_{Q,P}(x) = \langle x + P, Q\rangle = \langle x, Q\rangle \langle P, Q\rangle$.

We note that by varying P we obtain in this way for each non-zero $Q \in A[2]$ at least two different elements of $H^1(W,\mu_2)$ whose image in $H^1(U,\mu_2) \cong \hat{A}[2]$ is Q. By the short exact sequence (7) we have thus covered **all** elements of $H^1(W,\mathbb{Q}/\mathbb{Z}(1))$ whose image in $\hat{A}[2]$ is non-trivial. On the other hand, the only non-trivial element of the kernel $H^1(W,\mathbb{Q}/\mathbb{Z}(1)) \longrightarrow \hat{A}[2]$ is the one classifying the tale covering $p : U \longrightarrow W$, which is ramified at all the components D_x, and whose residue hence corresponds to the constant function $A[2] \longrightarrow \mathbb{Q}/\mathbb{Z}$ with value $1/2$. Finally, the trivial element has trivial residue, which corresponds to the constant function $A[2] \longrightarrow \mathbb{Q}/\mathbb{Z}$ with value 0. This concludes the enumeration of all element of $H^1(W,\mathbb{Q}/\mathbb{Z}(1))$, and so the proof is complete. □

Lemma 3.12 tells us that the residue map induces an isomorphism of Galois modules $H^1(\overline{W}_\alpha,\mathbb{Q}/\mathbb{Z}(1)) \cong \mathrm{Aff}(\overline{Z}_\alpha,\mu_2)$. We may hence rewrite the short exact sequence (7) as

$$0 \longrightarrow \mu_2 \xrightarrow{\iota} \mathrm{Aff}(\overline{Z}_\alpha,\mu_2) \xrightarrow{h_\alpha} \hat{A}[2] \longrightarrow 0\ , \tag{9}$$

where $\iota : \mu_2 \hookrightarrow \mathrm{Aff}(\overline{Z}_\alpha,\mu_2)$ is the inclusion of constant affine-linear functions. We note that since $\overline{U}_\alpha \cong \overline{Y}_\alpha \smallsetminus \overline{Z}_\alpha \cong \overline{A} \smallsetminus A[2]$ has no non-constant invertible functions the same holds for $\overline{W}_\alpha$ and so we have a canonical isomorphism of Galois modules $H^1(\overline{W}_\alpha,\mathbb{Q}/\mathbb{Z}(1)) \cong \mathrm{Pic}(\overline{W}_\alpha)_{\mathrm{tor}}$. We note that the injectivity of the residue map $H^1(\overline{W}_\alpha,\mathbb{Q}/\mathbb{Z}(1)) \longrightarrow H^0(\overline{D}_\alpha,\mathbb{Q}/\mathbb{Z})$ implies, in particular, that $H^1(\overline{X}_\alpha,\mathbb{Q}/\mathbb{Z}(1)) = 0$ and hence that $\mathrm{Pic}(\overline{X}_\alpha)$ is **torsion free**.

Remark 3.13. Consider the pullback map $\mathrm{Pic}(\overline{X}_\alpha) \longrightarrow \mathrm{Pic}(\overline{W}_\alpha)$ on geometric Picard groups. The inverse image $\Pi \subseteq \mathrm{Pic}(\overline{X}_\alpha)$ of the torsion subgroup $\mathrm{Pic}(\overline{W}_\alpha)_{\mathrm{tor}} \subseteq \mathrm{Pic}(\overline{W}_\alpha)$ is called the **Kummer lattice** in [SZ16]. Given an affine-linear map $L : \overline{Z}_\alpha \longrightarrow \mu_2$, we may realize the corresponding element of $\mathrm{Pic}(\overline{W}_\alpha)_{\mathrm{tor}}$ as a degree 2 covering of $\overline{W}_\alpha$. This covering extends to a degree 2 covering of $\overline{X}_\alpha$ which is ramified along D_x if and only if $L(x) = -1$. It then follows that there exists a class $E_L \in \mathrm{Pic}(\overline{X}_\alpha)$ such that

$$2E_L = \sum_{x \in Z_\alpha(\overline{k}) | L(x) = -1} [D_x]$$

and the image of E_L in $\mathrm{Pic}(\overline{W}_\alpha)_{\mathrm{tor}}$ is L. In particular, the Kummer lattice is generated over Π_0 by the classes E_L. This description of the Kummer lattice was established by Nikulin ([Ni75]) in the case of Kummer surfaces and extended to general Kummer varieties by Skorobogatov and Zarhin in [SZ16].

From now until the rest of this section we **fix the assumption** that the Galois action on $A[2]$ is **trivial**. Recall from §3.2 that we have a homomorphism

$$B_\alpha : H^1(k,\hat{A}) \longrightarrow \mathrm{Br}(Y_\alpha)/\mathrm{Br}(k)$$

which can be used to define the Cassels-Tate pairing between the image of α in $H^1(k,A)$ and a class $\beta \in H^1(k,\hat{A})$. It will be useful to consider similar types of Brauer elements on W_α. Using the map $H^1(k,\mathrm{Pic}(\overline{W}_\alpha)) \longrightarrow \mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ furnished by the Hochschild-Serre spectral sequence, the map

$$\mathrm{Aff}(\overline{Z}_\alpha,\mu_2) \cong \mathrm{Pic}(\overline{W}_\alpha)_{\mathrm{tor}} \longrightarrow \mathrm{Pic}(\overline{W}_\alpha)$$

determines a map

$$C_\alpha : H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2)) \longrightarrow \mathrm{Br}(W_\alpha)/\mathrm{Br}(k) \tag{10}$$

which fits into a commutative square

$$\begin{tikzcd}
H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2)) \arrow[r, "(h_\alpha)_*"] \arrow[d, "C_\alpha"] & H^1(k, \hat{A}[2]) \arrow[d, "B_\alpha"] \\
\mathrm{Br}(W_\alpha)/\mathrm{Br}(k) \arrow[r] & \mathrm{Br}(Y_\alpha)/\mathrm{Br}(k)
\end{tikzcd}$$

where the bottom horizontal map is induced by the composition of $p_\alpha^* : \mathrm{Br}(W_\alpha) \longrightarrow \mathrm{Br}(U_\alpha)$ and the isomorphism $\mathrm{Br}(U_\alpha) \cong \mathrm{Br}(Y_\alpha)$ induced by the inclusion $U_\alpha \subseteq Y_\alpha$ (since its complement has codimenional at least 2). It will be useful to recall the following general construction:

Construction 3.14. Let G be a group acting on an abelian group M and let $f : \Gamma_k \longrightarrow G$ be a homomorphism, through which we can consider M as a Galois module. Let k_f/k be the fixed field of $\ker(f) \subseteq \Gamma_k$. We will refer to k_f as the **splitting field** of f. Given an element $x \in H^1(k, M)$ we may consider the torsor Z_x under M classified by x, and the Galois action on $Z_x(\overline{k})$ is via the semi-direct product $M \rtimes G$. The kernel of the resulting homomorphism $\Gamma_k \longrightarrow M \rtimes G$ is a normal subgroup $\Gamma_x \subseteq \Gamma_k$ and we will refer to the corresponding normal extension k_x/k as the **splitting field** of x. We then obtain an induced injective homomorphism $\overline{x} : \mathrm{Gal}(k_x/k) \longrightarrow M \rtimes G$. We note that the field k_x contains the field k_f and the restriction of $\overline{x}$ to $\mathrm{Gal}(k_x/k_f)$ lands in M. Finally, the homomorphism $f : \Gamma_k \longrightarrow G$ descends to an injective homomorphism $\overline{f} : \mathrm{Gal}(k_f/k) \longrightarrow G$, and we obtain a commutative diagram with exact rows and injective vertical maps

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(k_x/k_f) \arrow[r] \arrow[d, hook, "\overline{x}|_{k_f}"] & \mathrm{Gal}(k_x/k) \arrow[r] \arrow[d, hook, "\overline{x}"] & \mathrm{Gal}(k_f/k) \arrow[r] \arrow[d, hook, "\overline{f}"] & 1 \\
1 \arrow[r] & M \arrow[r] & M \rtimes G \arrow[r] & G \arrow[r] & 1
\end{tikzcd} \tag{11}$$

Now let $\beta \in H^1(k, \hat{A}[2])$ be an element and suppose that $\theta \in H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ is such that $(h_\alpha)_*(\theta) = \beta \in H^1(k, \hat{A}[2])$. Applying Construction 3.14 with $G = A[2], M = \mathrm{Aff}(\overline{Z}_\alpha, \mu_2)$ and $\alpha : \Gamma_k \longrightarrow A[2]$ the homomorphism determined by the class $\alpha \in H^1(k, A[2])$ we obtain a commutative diagram with exact rows and injective vertical maps

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(k_\theta/k_\alpha) \arrow[r] \arrow[d, hook, "\overline{\theta}|_{k_\alpha}"] & \mathrm{Gal}(k_\theta/k) \arrow[r] \arrow[d, hook, "\overline{\theta}"] & \mathrm{Gal}(k_\alpha/k) \arrow[r] \arrow[d, hook, "\overline{\alpha}"] & 1 \\
1 \arrow[r] & \mathrm{Aff}(\overline{Z}_\alpha, \mu_2) \arrow[r] & \mathrm{Aff}(\overline{Z}_\alpha, \mu_2) \rtimes A[2] \arrow[r] & A[2] \arrow[r] & 1
\end{tikzcd} \tag{12}$$

where k_α and k_θ are the splitting fields of α and θ respectively. Let k_β be the splitting field of β and let $k_{\alpha,\beta}$ be the compositum of k_α and k_β. Applying Construction 3.14 again with $G = A[2]$ and $M = \hat{A}[2]$ (with trivial $A[2]$-action) we obtain a commutative diagram with exact rows and injective vertical maps

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(k_{\alpha,\beta}/k_{\alpha}) \arrow[r] \arrow[d, hook, "\overline{\beta}|_{k_{\alpha}}"] & \mathrm{Gal}(k_{\alpha,\beta}/k) \arrow[r] \arrow[d, hook, "\overline{\beta}\times\overline{\alpha}"] & \mathrm{Gal}(k_{\alpha}/k) \arrow[r] \arrow[d, hook, "\overline{\alpha}"] & 1 \\
1 \arrow[r] & \hat{A}[2] \arrow[r] & \hat{A}[2] \times A[2] \arrow[r] & A[2] \arrow[r] & 1
\end{tikzcd} \tag{13}$$

By the naturality of Construction 3.14 and since $(h_{\alpha})_*(\theta) = \beta$ the left vertical maps in 13 and 14 fit together in a commutative diagram with exact rows and injective vertical maps of the form:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(k_{\theta}/k_{\alpha,\beta}) \arrow[r] \arrow[d, hook] & \mathrm{Gal}(k_{\theta}/k_{\alpha}) \arrow[r] \arrow[d, hook, "\overline{\theta}|_{k_{\alpha}}"] & \mathrm{Gal}(k_{\alpha,\beta}/k_{\alpha}) \arrow[r] \arrow[d, hook, "\overline{\beta}|_{k_{\alpha}}"] & 1 \\
1 \arrow[r] & \mu_2 \arrow[r] & \mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2) \arrow[r] & \hat{A}[2] \arrow[r] & 1
\end{tikzcd} \tag{14}$$

In particular, the extension $k_{\theta}/k_{\alpha,\beta}$ is either trivial or quadratic. The following proposition plays a key role in the analysis of the behavior of the Cassels-Tate pairing under quadratic twists (see Proposition 3.29):

Proposition 3.15.

(1) An element $\beta \in H^1(k, \hat{A}[2])$ can be lifted to an element $\theta \in H^1(k, \mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2))$ if and only if $\alpha \cup \beta = 1 \in H^2(k, \mu_2)$. Furthermore, if S is a set of places which contains a set of generators for the class group of k and α, β are unramified outside S then θ can be chosen so that the splitting field k_{θ} is unramified outside S.

(2) The image of the residue $\mathrm{res}_{D_{\alpha}}(C_{\alpha}(\theta)) \in H^1(D_{\alpha}, \mathbb{Q}/\mathbb{Z})$ in $H^1(D_{\alpha} \otimes_k k_{\alpha,\beta}, \mathbb{Q}/\mathbb{Z})$ is constant and comes from the element $u_{\theta} \in H^1(k_{\alpha,\beta}, \mathbb{Z}/2)$ which classifies the (at most) quadratic extension $k_{\theta}/k_{\alpha,\beta}$.

Proof. We begin by proving (1). Consider the exact sequence

$$H^1(k, \mu_2) \longrightarrow H^1(k, \mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2)) \xrightarrow{(h_{\alpha})_*} H^1(k, \hat{A}[2]) \xrightarrow{\partial} H^2(k, \mu_2) \tag{15}$$

associated to the short exact sequence (9). We note that by choosing a base point $x_0 \in Z_{\alpha}(\overline{k})$ we may identify $Z_{\alpha}(\overline{k}) \cong A[2]$ and consequently identify each affine-linear map $L : Z_{\alpha}(\overline{k}) \longrightarrow \mu_2$ with an affine-linear map $A[2] \longrightarrow \mu_2$ of the form $P \mapsto \varepsilon \cdot \langle P, Q \rangle$ for some $Q \in \hat{A}[2]$ and $\varepsilon \in \mu_2$. The association $L \mapsto (\varepsilon, Q)$ then identifies the underlying abelian group of $\mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2)$ with the abelian group $\mu_2 \oplus \hat{A}[2]$ and identifies the corresponding Galois action as $\sigma(\varepsilon, Q) = (\varepsilon \cdot \langle \overline{\alpha}(\sigma), Q \rangle, Q)$. Now let $\beta' : \Gamma \longrightarrow \mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2) \cong \mu_2 \times A[2]$ be the 1-cochain $\beta'(\sigma) = (1, \beta(\sigma))$, where $\beta : \Gamma_k \longrightarrow \hat{A}[2]$ is the homomorphism determined by the class β. Then

$$\beta'(\sigma) + \sigma\beta'(\tau) - \beta'(\sigma\tau) = (\langle \alpha(\sigma), \beta(\tau) \rangle, 0)$$

and so

$$\partial\beta = \alpha \cup \beta \in H^2(k, \mu_2).$$

It then follows that β lifts to $H^1(k, \mathrm{Aff}(\overline{Z}_{\alpha}, \mu_2))$ if and only if $\alpha \cup \beta$ vanishes.

Now let S be a set of places which contains a set of generators for the class group of k and such that α, β are unramified outside S. By (14) we have that k_{θ} is an at most quadratic extension of $k_{\alpha,\beta}$ which is classified by an element $u_{\theta} \in$

$H^1(k_{\alpha,\beta},\mathbb{Z}/2)$. Furthermore, if we replace θ by $\theta' = \theta \cdot \iota_*\varphi$ for some $\varphi \in H^1(k,\mu_2)$ then we get $u_{\theta'} = u_\theta + \varphi|_{k_{\alpha,\beta}}$: this follows from the formula

$$\overline{\theta}'|_{k_\alpha} = \overline{\theta}|_{k_\alpha} \cdot (\iota \circ \overline{\varphi}|_{k_\alpha}) : \mathrm{Gal}(k_\theta/k_\alpha) \longrightarrow \mathrm{Aff}(\overline{Z}_\alpha,\mu_2)$$

relating the homomorphisms associated to the classes $\theta|_{k_\alpha} \in H^1(k_\alpha,\mathrm{Aff}(\overline{Z}_\alpha,\mu_2))$, $\theta'|_{k_\alpha} \in H^1(k_\alpha,\mathrm{Aff}(\overline{Z}_\alpha,\mu_2))$ and $\varphi|_{k_\alpha} \in H^1(k_\alpha,\mu_2)$. Now for every $v \notin S$, since k_θ is Galois over k we have that the ramification index of $k_\theta/k_{\alpha,\beta}$ is the same for all places u of $k_{\alpha,\beta}$ which lie above v. Let T denote the set of places v of k such that $k_\theta/k_{\alpha,\beta}$ is ramified at all places u of $k_{\alpha,\beta}$ which lie above v. Since S contains a set of generators for the class group we can find an $a \in k^*$ such that for every $v \notin S$ we have that $\mathrm{val}_v(a)$ is odd if and only if $v \in T$. If we now set $\theta' = \theta \cdot \iota_*([a])$ then we get that k_θ is unramified outside S, as desired.

Let us now prove (2). Let $C \in \mathrm{Br}(W_\alpha)$ be a Brauer element whose image in $\mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ is $C_\alpha(\theta)$, and let $r_\theta = \mathrm{res}_{D_\alpha}(C) \in H^1(D_\alpha,\mathbb{Q}/\mathbb{Z})$. Since $C_\alpha(\theta)$ is a 2-torsion element it follows that $2C$ is a constant class and hence r_θ is a 2-torsion element. We may hence (uniquely) consider r_θ as an element of $H^1(D_\alpha,\mathbb{Z}/2)$. Let $r'_\theta = (r_\theta)|_{D_\alpha \otimes_k k_{\alpha,\beta}} \in H^1(D_\alpha \otimes_k k_{\alpha,\beta},\mathbb{Z}/2)$ denote the restriction of r_θ. Since θ vanishes in $H^1(k_\theta,\mathrm{Aff}(\overline{Z}_\alpha,\mu_2))$ it follows that the image of C in $\mathrm{Br}(W_\alpha \otimes_k k_\theta)$ is constant and hence r'_θ vanishes in $H^1(D_\alpha \otimes_k k_\theta,\mathbb{Z}/2)$. It then follows that r'_θ is either trivial or is the pullback of u_θ. To show that r'_θ can only be trivial if u_θ is trivial we use the fact that both r'_θ and u_θ depend on the choice of θ in the same way. More precisely, if we replace θ by $\theta' = \theta \cdot \iota_*\varphi$ for some $\varphi \in H^1(k,\mu_2)$ then θ' still maps to $\beta \in H^1(k,\hat{A}[2])$, and both $r'_{\theta'} - r'_\theta$ and $u_{\theta'} - u_\theta$ will equal the corresponding image of φ. For u_θ this was shown above. As for r'_θ, this follows from the fact that the Brauer element $C_\alpha(\iota_*\varphi)$ can be identified with the image of the cup product $\varphi \cup [p_\alpha] \in H^2(W_\alpha,\mu_2)$, and hence the residue of $C_\alpha(\iota_*\varphi)$ along D_α is the image of φ. It will now suffice to show that $r'_\theta = u_\theta$ for just a single θ which lifts β. As such we may choose θ so that both u_θ and r'_θ are non-zero, in which case they must coincide by the above considerations (i.e., since r'_θ vanishes in $H^1(D_\alpha \otimes_k k_\theta,\mathbb{Z}/2)$). □

We finish this section with some analysis of the way the Brauer element $C_\alpha(\theta)$ pairs with local points in certain circumstances. We begin with some remarks concerning integral models for the open subvariety W.

Let v be a finite odd place of k and let A be an abelian variety over k_v such that the Galois module $A[2]$ is unramified (in the cases of interest in this paper, the Galois action on $A[2]$ will in fact be trivial). Let $\mathcal{A} \longrightarrow \mathrm{spec}(\mathcal{O}_v)$ be a Nron model for A and let $\mathcal{A}[2] \subseteq \mathcal{A}$ be the scheme theoretic fixed locus of the antipodal involution $\iota_{\mathcal{A}} : \mathcal{A} \longrightarrow \mathcal{A}$, so that the special fiber $\mathcal{A}[2]_{\mathbb{F}_q}$ is just the 2-torsion subscheme of $\mathcal{A}_{\mathbb{F}_q}$. Let $\mathcal{U} = \mathcal{A} \smallsetminus \mathcal{A}[2]$ be the complement of $\mathcal{A}[2]$ in $\mathcal{A}$, so that $\mathcal{U}$ is a v-integral model for U and inherits a free involution $\iota_{\mathcal{U}} : \mathcal{U} \longrightarrow \mathcal{U}$ which extends the free involution of $\iota_U : U \longrightarrow U$. Since $\mathcal{A}$ is quasi-projective (see [BLR90]) so is $\mathcal{U}$ and so we may realize the quotient of $\mathcal{U}$ by $\iota_{\mathcal{U}}$ as a scheme $\mathcal{W} := \mathcal{U}/\iota_{\mathcal{U}}$. Furthermore, since we assume that v is odd the corresponding action of $\mathbb{Z}/2$ is tame and hence $\mathcal{W}$ is also a **universal** geometric quotient (see [CEPT96]). This means, in particular, that the generic fiber of $\mathcal{W}$ is isomorphic to W and that its special fiber is the quotient of $\mathcal{U}_{\mathbb{F}_q} = \mathcal{A}_{\mathbb{F}_q} \smallsetminus \mathcal{A}_{\mathbb{F}_q}[2]$ by the associated antipodal involution.

Now let $\alpha \in H^1(k_v, A[2])$ be an unramified element. Then we may naturally consider α as an element of $H^1(\mathcal{O}_v, \mathcal{A}[2])$ and consequently twist $\mathcal{A}$ by α. This results in a regular $\mathcal{O}_v$-model $\mathcal{Y}_\alpha$ for Y_α, whose special fiber $(\mathcal{Y}_\alpha)_{\mathbb{F}_v}$ is a torsor under the special fiber $\mathcal{A}_{\mathbb{F}_v}$ of $\mathcal{A}$ associated to the reduction $\overline{\alpha} \in H^1(\mathbb{F}_v, \mathcal{A}[2]_{\mathbb{F}_v})$. In particular, $\mathcal{Y}_\alpha$ inherits an involution $\iota_{\mathcal{Y}_\alpha} : \mathcal{Y}_\alpha \longrightarrow \mathcal{Y}_\alpha$ which extends the involution $\iota_{Y_\alpha} : Y_\alpha \longrightarrow Y_\alpha$. Repeating the construction of the previous paragraph with $\mathcal{Y}_\alpha$ instead of $\mathcal{A}$ and $\iota_{\mathcal{Y}_\alpha}$ instead of the antipodal involution we obtain natural v-integral models $\mathcal{U}_\alpha$ and $\mathcal{W}_\alpha$ for U_α and W_α respectively, together with an tale quotient map $\mathcal{U}_\alpha \longrightarrow \mathcal{W}_\alpha$.

Lemma 3.16. *Let w be a finite odd place of k, let A be an abelian variety over k_w with semi-abelian reduction of toric rank* 1 *and such that the Galois module $A[2]$ is unramified. Let $\alpha \in H^1(k_w, A[2])$ be an unramified and non-zero element and let $x \in W_\alpha(k_w)$ be a point. Then there exists a (possibly trivial) unramified quadratic extension F/k_w such that x lifts to a point $y \in U^F_\alpha$ which extends to an integral point $y \in \mathcal{U}^F_\alpha(\mathcal{O}_w)$. In particular, x extends to an integral point $x \in \mathcal{W}_\alpha(\mathcal{O}_w)$.*

Proof. Let F/k_w be the (at most) quadratic extension splitting the fiber $(\widetilde{Y}_\alpha)_x$ of the degree 2 map $\widetilde{Y}_\alpha \longrightarrow X$ over the point x (note that x belongs to $W_\alpha(k_w)$ by assumption and hence does not lie on the ramified locus). We first claim that that F/k_w is unramified. Assume by way of contradiction that F/k_w is ramified, and let w_F be a valuation extending w. Since the image of α in $H^1(k_w, A[2])$ is unramified there exists an unramified finite extension K/k_w and an isomorphism $\varphi_K : (Y_\alpha)_K \cong A_K$ such that $\varphi_K \circ \iota_{Y_\alpha} = \iota_A \circ \varphi$. Let L be the compositum of F and K. Our assumption that F/k_w is ramified means that L is quadratic ramified extension of K. Let $\sigma \in \mathrm{Gal}(L/K)$ be the non-trivial element.

Let $\mathcal{A}_K$ be a Nron model for A_K and let $\mathcal{A}_L$ be a Nron model for A_L. Let w_K and w_L be valuations extending w, and let C_{w_K} and C_{w_L} denote the groups of components of the geometric special fibers of $\mathcal{A}_K$ and $\mathcal{A}_L$ respectively. Since L/K is purely ramified it induces an isomorphism of residue fields $\mathbb{F}_{w_K} \cong \mathbb{F}_{w_L}$. Since A, and hence also A_K, has semi-abelian reduction of toric rank 1, we have an isomorphism $C_{w_K}/2C_{w_K} \cong \mathbb{Z}/2$. Arguing as in Corollary 3.7 we see that the group $C_{w_L}/4C_{w_L}$ is cyclic of order 4 and the induced action of $\mathrm{Gal}(L/K)$ on $C_{w_L}/4C_{w_L}$ is trivial.

By construction there exists a point $y \in \widetilde{Y}_\alpha(F)$ which maps to x and such that $\sigma(y) = \iota_{Y_\alpha}(y)$. Let $y' \in Y_\alpha(F)$ be the image of y and let $y'' \in A(L)$ be the image of y' under the induced isomorphism $\varphi_L : (Y_\alpha)_L \xrightarrow{\cong} A_L$. In particular, we have $\sigma(y'') = \iota_A(y'') = -y''$. Since the action of $\mathrm{Gal}(L/K)$ on $C_{w_L}/4C_{w_L}$ is trivial we may conclude that y'' reduces to a component of $C_{w_L}/4C_{w_L}$ of order 2, and hence to a component in the image of the open inclusion $(\mathcal{A}_K)_{\mathbb{F}_{w_K}} \hookrightarrow (\mathcal{A}_L)_{w_L}$. This implies that y'' and $\sigma(y'')$ have the same reduction in the special fiber of $\mathcal{A}_L$, and so this reduction must be a 2-torsion point. It then follows that the reduction of y' mod w determines an $\mathbb{F}_w$-point of the fixed point subscheme $Z_{\overline{\alpha}} \subseteq (\mathcal{Y}^F_\alpha)_{\mathbb{F}_w}$ under the induced involution. But this is now a contradiction to our assumption that $\overline{\alpha}$ is non-zero (since in this case $Z_{\overline{\alpha}}$ has no points defined over $\mathbb{F}_w$) and so we may conclude that F/k_w must be unramified.

Now let $y \in \mathcal{Y}^F_\alpha(\mathcal{O}_w)$ be a v-integral point extending the points $y \in Y^F_\alpha(k_w)$ that lifts x (such a point exists since $\mathcal{Y}^F_\alpha$ is proper). To finish the proof it will suffice to show that y lies in $\mathcal{U}^F_\alpha(\mathcal{O}_w)$, i.e., has trivial intersection with $Z_{\overline{\alpha}} \subseteq (\mathcal{Y}^F_\alpha)_{\mathbb{F}_w}$, but this is simply because the intersection of y with $(\mathcal{Y}^F_\alpha)_{\mathbb{F}_w}$ is a point defined over $\mathbb{F}_w$, while $Z_{\overline{\alpha}}$ has no points defined over $\mathbb{F}_w$ when $\overline{\alpha} \neq 0$. □

Corollary 3.17. *Let w be a finite odd place of k and let A be an abelian variety over k_w with semi-abelian reduction of toric rank 1 and such that the Galois action on $A[2]$ is trivial. Let $\alpha \in H^1(k_w, A[2])$ be an unramified element. Let $R \subseteq W_\alpha(k_w)$ be the subset consisting of those points $x \in W_\alpha(k_w)$ which lift to $U^F_\alpha(k_w)$ for some* ***unramified*** *quadratic extension F/k_w. Finally, let $\theta \in H^1(k_w, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ be an unramified element whose image under the composite map*

$$H^1(k_w, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2)) \longrightarrow H^1(k_w, \hat{A}[2]) \longrightarrow H^1(k_w, \hat{A})$$

is trivial and let $C \in \mathrm{Br}(W_\alpha)[2]$ a 2-torsion Brauer element whose image in $\mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ is $C_\alpha(\theta)$. Then $R \neq \varnothing$ and the evaluation map $\mathrm{ev}_C : R \longrightarrow \mathbb{Z}/2$ restricted to R is constant.

Proof. We separate the proof into two cases, according to whether or not α is trivial. First assume that α is non-trivial. In this case Lemma 3.16 implies that every point in $W_\alpha(k_w)$ extends to an integral point $\mathscr{x} : \mathrm{spec}(\mathcal{O}_w) \longrightarrow \mathcal{W}_\alpha$. Let $\mathscr{x}_0 : \mathrm{spec}(\mathbb{F}_w) \longrightarrow (\mathcal{W}_\alpha)_{\mathbb{F}_w}$ be the restriction to the residue point. Then the pairing of x with C can then be computed as

$$\mathrm{ev}_C(x) = \mathrm{res}_{\mathbb{F}_w}(x^*C) = \mathscr{x}_0^* \,\mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C) \in H^1(\mathbb{F}_w, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$$

where the second equality is by the compatibility of residues with base change (see discussion on page 25 of [BBL16]) and the last isomorphism is given by evaluation on the Frobenius element. Since θ is unramified it follows that C becomes constant after base changing to k_w^{un} and hence the residue of C along $(\mathcal{W}_\alpha)_{\mathbb{F}_w}$ vanishes in $(\mathcal{W}_\alpha)_{\mathbb{F}_w} \otimes_{\mathbb{F}_w} \overline{\mathbb{F}}_w$. It then follows that the residue $\mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C)$ is constant on each irreducible component of $(\mathcal{W}_\alpha)_{\mathbb{F}_w}$. To show that it is actually constant consider the pulled back element $p_\alpha^*C \in \mathrm{Br}(U_\alpha)$. Then the image of p_α^*C in $\mathrm{Br}(U_\alpha)/\mathrm{Br}(k)$ coincides with the restriction of $B((h_\alpha)_*\theta) \in \mathrm{Br}(Y_\alpha)/\mathrm{Br}(k)$ which vanishes thanks to our assumption that the image of θ in $H^1(k_w, \hat{A})$ vanishes. We may hence conclude that p_α^*C is constant. Let $(p_\alpha)_{\mathbb{F}_w} : (\mathcal{U}_\alpha)_{\mathbb{F}_w} \longrightarrow (\mathcal{W}_\alpha)_{\mathbb{F}_w}$ be the restriction of $p_\alpha : \mathcal{U}_\alpha \longrightarrow \mathcal{W}_\alpha$ to the special fibers. Using again the compatibility of residues and base change we now get that $(p_\alpha)^*_{\mathbb{F}_w} \mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C) = \mathrm{res}_{(\mathcal{U}_\alpha)_{\mathbb{F}_w}}(p_\alpha^*C)$ is constant, i.e., comes from a class in $H^1(\mathbb{F}_w, \mathbb{Q}/\mathbb{Z})$. Now since A has semi-abelian reduction of toric rank 1 and $A[2]$ is unramified we have that $\mathcal{A}_{\mathbb{F}_w}$ has two geometric components, which are thus preserved by the antipodal involution. It then follows that the tale covering $(p_\alpha)_{\mathbb{F}_w}$ is geometrically non-trivial on each irreducible component of $(\mathcal{W}_\alpha)_{\mathbb{F}_w}$. Finally, since $\mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C)$ is constant on each irreducible component and $(p_\alpha)^*_{\mathbb{F}_w} \mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C)$ is globally constant we may conclude that $\mathrm{res}_{(\mathcal{W}_\alpha)_{\mathbb{F}_w}}(C)$ is actually constant, as desired.

Now assume that $\alpha = 0$. In this case we simply write W instead of W_α and U instead of U_α. Let $D_0 \subseteq D$ be the component corresponding to $0 \in A[2]$. Since $D_0 \cong \mathbb{P}^{g-1}$ the residue $\mathrm{res}_{D_0}(C) \in H^1(D_0, \mathbb{Q}/\mathbb{Z})$ is constant and comes from some class $\varphi \in H^1(k, \mathbb{Q}/\mathbb{Z})$. We may then write C as a sum $C' + [p] \cup \varphi$ where $C' \in \mathrm{Br}(W)$ is such that $\mathrm{res}_{D_0}(C') = 0$. In this case C' extends to $W \cup D_0$ and so we can write $C' = C'' + C_0$ where $C_0 \in \mathrm{Br}(k) \subseteq \mathrm{Br}(W)$ is a constant class and C'' vanishes when restricted to $\mathrm{Br}(D_0)$. It will hence suffice to show that $[p] \cup \varphi$ and C'' both pair trivially with $R \subseteq W(k_w)$. For $[p] \cup \varphi$ this is clear $\mathrm{ev}_{[p]\cup\varphi}(x) = [x^*p] \cup \varphi = 0$ since the classes $[x^*p]$ and φ are both unramified by assumption (for $[x^*p]$ this is because $x \in R$, and for φ

this is because θ is unramified). It is hence left to show that C'' pairs trivially with R. Let F/k_w be an unramified quadratic extension such that x lifts to $y \in U^F(k_w)$. Then the pairing of x with C'' is equal to the pairing of y with $(p^F)^*C''$, and so it will suffice to show that $(p^F)^*C'' = 0 \in \mathrm{Br}(U^F)$. Now by construction the image of $(p^F)^*C''$ in $\mathrm{Br}(U^F)/\mathrm{Br}(k)$ coincides with $B(h_*(\theta + \iota_*\varphi)) = B(h_*(\theta))$, where $h_* : H^1(k_w, \mathrm{Aff}(A[2], \mu_2)) \longrightarrow H^1(k_w, \hat{A}[2])$ is the induced map. Since the image of $h_*(\theta)$ in $H^1(k, \hat{A})$ vanishes by assumption it follows that $(p^F)^*C''$ is a constant Brauer element. On the other hand, since C'' extends by 0 to $W \cup D_0$ we get that $(p^F)^*C''$ extends by 0 to $U^F \cup \{D_0\} \subseteq \widetilde{A}^F$. It then follows that $(p^F)^*C'' = 0$, as desired. □

3.4. **The Tate pairing and its quadratic refinement.** Let A be an abelian variety over a field k equipped with a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$. Then the Weil pairing $\langle , \rangle_\lambda : A[2] \times A[2] \longrightarrow \mu_2$ induces a symmetric cup product pairing

$$\cup_\lambda : H^1(k, A[2]) \times H^1(k, A[2]) \longrightarrow H^2(k, \mu_2)$$

which is known as the **Tate pairing**. In [PR12], Poonen and Rains construct a natural **quadratic refinement** of $\cup_\lambda$. In this section we will review this construction, which plays a role in the analysis of the change of Selmer groups under quadratic twists. In particular, to make the argument work we will need to know that this quadratic refinement is invariant under quadratic twists, a statement whose proof is the main goal of this section. We wish to thank the anonymous referee for pointing out this gap in the argument after reading a previous version of this paper.

Before we review Poonen and Rains' construction let us consider the preliminary question of quadratic refinements of the **Weil pairing**. Note that since we are considering the 2-torsion module the Weil pairing (which is usually skew-symmetric) is also symmetric, and so the question of quadratic refinements is meaningful. Recall that there is a natural isomorphism of Galois modules $\mathrm{NS}(\overline{A}) \cong \mathrm{Sym}(\overline{A}, \hat{\overline{A}})$ between the Nron Severi group of $\overline{A}$ and the group of symmetric isogenies $\overline{A} \longrightarrow \hat{\overline{A}}$. In particular, the principal polarization $\lambda : A \longrightarrow \hat{A}$ determines a Galois invariant element (which we will call by the same name) $\lambda \in \mathrm{NS}(\overline{A})^{\Gamma_k}$. As the antipodal involution $\iota_A : A \longrightarrow A$ fixes $\mathrm{NS}(\overline{A})$ while acting as $[-1]$ on $\mathrm{Pic}(\overline{A})_0 \cong \hat{A}(\overline{k}) \overset{\lambda}{\cong} A(\overline{k})$ we obtain a short exact sequence of Galois modules

$$0 \longrightarrow A[2] \longrightarrow \mathrm{Pic}(\overline{A})^{\iota_A} \xrightarrow{\pi} \mathrm{NS}(\overline{A}) \longrightarrow 0 \tag{16}$$

where the middle term is the subgroup of $\mathrm{Pic}(\overline{A})$ fixed by the induced action of the antipodal involution. We note that this latter group classifies **symmetric line bundles** on $\overline{A}$, i.e., line bundles $\mathcal{L}$ such that $\iota_A^*\mathcal{L} \cong \mathcal{L}$. Now if $\mathcal{L}$ is a symmetric line bundle on $\overline{A}$ such that $\pi(\mathcal{L}) = \lambda$ then, over $\overline{k}$, we may write $\lambda : \overline{A} \longrightarrow \hat{\overline{A}}$ using the formula $\lambda(x) = [\tau_x^*\mathcal{L} \otimes \mathcal{L}^{-1}]$ (where τ_x denotes translation by x), in which case one says that λ is the polarization **induced** from $\mathcal{L}$. However, it is in general not possible to choose a preimage $\mathcal{L} \in \pi^{-1}(\lambda)$ which is Galois invariant (and thus realizable as a line bundle on A defined over k). The obstruction to the existence of such a Galois invariant symmetric line bundle is the class

$$c_\lambda := \partial\lambda \in H^1(k, A[2]) \tag{17}$$

where $\partial : H^0(k, \mathrm{NS}(\overline{A})) \longrightarrow H^1(k, A[2])$ is the boundary map associated to (16). We think of c_λ as the element classifying the $A[2]$-torsor $\pi^{-1}(\lambda)$ of symmetric line bundles on $\overline{A}$ which map to $\lambda \in \mathrm{NS}(\overline{A})$. It will consequently be useful to note that this torsor can be identified combinatorially as the torsor of **quadratic refinements** of the Weil pairing $\langle , \rangle_\lambda$. More precisely, given a symmetric line bundle $\mathcal{L}$ on $\overline{A}$ such that $\pi(\mathcal{L}) = \lambda$ we may define a quadratic refinement of $\langle , \rangle_\lambda$ as follows (see [Po03]): since $\mathcal{L}$ is symmetric there exists an isomorphism $\sigma : \mathcal{L} \xrightarrow{\cong} \iota_A^*\mathcal{L}$, and we may choose σ uniquely such that the induced map $(\mathcal{L})_0 \longrightarrow (\iota_A^*\mathcal{L})_0 = (\mathcal{L})_0$ is the identity. It then follows that the composition $\mathcal{L} \xrightarrow{\sigma} \iota_A^*\mathcal{L} \xrightarrow{\iota_A^*\sigma} \mathcal{L}$ is an automorphism of $\mathcal{L}$ which is the identity on $(\mathcal{L})_0$ and is hence itself the identity. In particular, for every 2-torsion point $P \in A[2]$ the induced map $(\mathcal{L})_P \longrightarrow (\iota_A^*\mathcal{L})_P = (\mathcal{L})_P$ has order 2 and is consequently given by multiplication by an element $q_{\mathcal{L}}(P) \in \mu_2$. One may then show (see [Po03, Proposition 13.1]) that the association $P \mapsto q_{\mathcal{L}}(P)$ satisfies the equality

$$q_{\mathcal{L}}(P+Q) \cdot q_{\mathcal{L}}(P) \cdot q_{\mathcal{L}}(Q) = \langle P, Q \rangle_\lambda . \tag{18}$$

Functions $q_L : A[2] \longrightarrow \mu_2$ satisfying (18) are also known as **quadratic refinements** of $\langle P, Q \rangle_\lambda$ (in particular, they are not homomorphism of groups, but rather quadratic maps). We note that the collection $\mathrm{Quad}(\lambda)$ of all such quadratic refinements is naturally a torsor under $\mathrm{Hom}(A[2], \mu_2) \cong A[2]$ (where $\mathrm{Hom}(A[2], \mu_2)$ acts by levelwise multiplication). Furthermore, since $\langle , \rangle_\lambda$ is Galois invariant we obtain a natural Galois action on $\mathrm{Quad}(A[2])$ (induced by the Galois action on $A[2]$), which is compatible with this torsor structure. Finally, one can show that the association $\mathcal{L} \mapsto q_{\mathcal{L}}$ determines a map (and hence an isomorphism) of $A[2]$-torsors $\pi^{-1}(\lambda) \longrightarrow \mathrm{Quad}(\lambda)$. In particular, the $A[2]$-torsor $\mathrm{Quad}(\lambda)$ is also classified by the element $c_\lambda \in H^1(k, A[2])$, and so $c_\lambda = 0$ if and only if $\langle , \rangle_\lambda$ admits a Galois invariant quadratic replacement.

Now since the line bundles in the $A[2]$-torsor $\pi^{-1}(\lambda)$ are all equal up to 2-torsion element of $\mathrm{Pic}(\overline{A})$, the square $\mathcal{K} = \mathcal{L} \otimes \mathcal{L}$ is independent of the choice of $\mathcal{L} \in \pi^{-1}(\lambda)$, and is hence a line bundle defined over k. This line bundle can also be identified with the pullback $(\mathrm{Id}, \lambda)^*\mathcal{P}$, where $\mathcal{P}$ is the Poincar line bundle on $A \times \hat{A}$. The isomorphism $\sigma : \mathcal{L} \xrightarrow{\cong} \iota_A^*\mathcal{L}$ then induces an isomorphism $\rho : \mathcal{K} \xrightarrow{\cong} \iota_A\mathcal{K}$, and for every $P \in A[2]$ the induced map $\rho_P : \mathcal{K}_P \longrightarrow (\iota_A^*\mathcal{K})_P$ is given by multiplication by $q_\lambda(P)^2 = 1$, i.e., by the identity. We may summarize the situation as follows:

(1) Geometrically, every principal polarization λ is induced by a line bundle $\mathcal{L}$. This line bundle is however not unique: for every field extension K/k, the choice of such a line bundle over K is equivalent to the choice of a Γ_K-invariant quadratic enhancement of $\langle , \rangle_\lambda$.

(2) The square of any line bundle inducing λ is isomorphic to $\mathcal{K} = (\mathrm{Id}, \lambda)^*\mathcal{P}$, which is always defined over k. In addition, there exists a (unique) isomorphism $\rho : \mathcal{K} \longrightarrow \iota_A^*\mathcal{K}$ with the property that $\rho_P : \mathcal{K}_P \longrightarrow (\iota_A^*\mathcal{K})_P$ is the identity for every $P \in A[2]$.

We now proceed to Poonen and Rains' construction of the quadratic enhancement of the Tate pairing. Let $\mathcal{K} = (\mathrm{Id}, \lambda)^*\mathcal{P}$ be as above. If L is a field containing k and $x \in A(L)$ is a point defined over L, then by construction the line bundle $\tau_x^*\mathcal{K} \otimes \mathcal{K}^{-1}$ on $A \otimes_k L$ has degree 0 and its class in $\hat{A}(L)$ coincides with $2\lambda(x)$. In particular, if P is a 2-torsion point then $\mathcal{K} \cong \tau_P^*\mathcal{K}$. We may then consider the (non-abelian) group $\mathcal{H}_{\mathcal{K}}(L)$ whose elements are pairs (P,ϕ) where $P \in A[2](L)$ is a 2-torsion point defined over L and $\phi : \mathcal{K}_L \longrightarrow \tau_P^*\mathcal{K}_L$ is an isomorphism over K. Composition is defined by $(P,\phi)(Q,\psi) = (P+Q,(\tau_Q^*\phi)\circ\psi)$. Mumford ([Mu91]) has shown that the functor $L \mapsto \mathcal{H}_{\mathcal{K}}(L)$ is represented by a **group scheme** $\mathcal{H}_{\mathcal{K}}$ defined over k, which sits in a short exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{H}_{\mathcal{K}} \longrightarrow A[2] \longrightarrow 1 \tag{19}$$

in which the two maps in the middle are given by $t \mapsto (0, m_t)$ and $(P,\phi) \mapsto P$ respectively, where $m_t : \mathcal{K} \longrightarrow \mathcal{K}$ is the multiplication by t automorphism. Following [PR12] we will refer to $\mathcal{H}_{\mathcal{K}}$ as the **Heisenberg group scheme** of $\mathcal{K}$.

Proposition 3.18 ([PR12, Corollary 4.7])**.** *The connecting homomorphism*

$$q_\lambda : H^1(k, A[2]) \longrightarrow H^2(k, \mathbb{G}_m) \tag{20}$$

induced by 19 is a quadratic map whose associated bilinear pairing is $(x,y) \mapsto x \cup_\lambda y$.

Remark 3.19. Since q_λ is quadratic and $H^1(k, A[2])$ is a 2-torsion group we see that $q_\lambda(x) \in H^2(k,\mathbb{G}_m)$ is a 4-torsion element for every $x \in H^1(k, A[2])$. One may then show (see [PR12]) that

$$2q_\lambda(x) = x \cup_\lambda x = x \cup_\lambda c_\lambda \in H^2(k,\mu_2) \subseteq H^2(k,\mathbb{G}_m)$$

for every $x \in H^1(k, A[2])$, where c_λ is the element defined above (see (17)), which vanishes if and only if the Weil pairing $\langle , \rangle_\lambda$ admits a Galois invariant quadratic enhancement. In this latter case (which occurs, for example, when that Galois action on $A[2]$ is trivial), the quadratic map q_λ takes values in $H^2(k,\mu_2)$.

Our goal for the rest of this section is to show that the quadratic map (20) is invariant under quadratic twists. Let $U \subseteq A$ be the complement of $A[2]$ and $p : U \longrightarrow W = U/\mu_2$ the quotient by the free action of ±1 (see §3.3). Since the action of $A[2]$ on A by translations preserves U and commutes with multiplication by ±1 it descends to an action of $A[2]$ on W (which for $P \in A[2]$ we will also denote by $\tau_P : W \longrightarrow W$). The idea is then to show that the line bundle $\mathcal{K}|_U$ which is used to define q_λ descends to a line bundle $\overline{\mathcal{K}}$ on W (defined over k) which is invariant under the action of $A[2]$. This would mean that one can define the Heisenberg group, and consequently the map (20), by using W instead of A, and hence manifestly in a way that is invariant under quadratic twists.

Lemma 3.20. *There exists a line bundle $\overline{\mathcal{K}}$ on W such that $p^*\overline{\mathcal{K}} \cong \mathcal{K}|_U$ and such that $\tau_P^*\overline{\mathcal{K}} \cong \overline{\mathcal{K}}$ for every $P \in A[2]$.*

Proof. Let $\rho : \mathcal{K} \xrightarrow{\cong} \iota_A^*\mathcal{K}$ be the isomorphism of (2), which is characterized by the property that $\rho_P : \mathcal{K}_P \longrightarrow (\iota_A^*\mathcal{K})_P$ is the identity for every $P \in A[2]$. In particular, the composition $\rho \circ \iota_A^*\rho : \mathcal{K} \longrightarrow \mathcal{K}$ is an automorphism of $\mathcal{K}$ which is the identity on the fiber at 0, and hence must itself be the identity. This means that $\rho|_U : \mathcal{K}|_U \longrightarrow \mathcal{K}|_U$ is a **descent datum** for $\mathcal{K}|_U$ with respect to $p : U \longrightarrow W$, and hence by tale descent for line bundles the pair $(\mathcal{K}|_U, \rho|_U)$ determines a line bundle $\mathcal{K}_\rho$ on W such that $p^*\mathcal{K}_\rho \cong \mathcal{K}|_U$. We now claim that for every $P \in A[2]$ the line bundle $\tau_P^*\mathcal{K}_\rho$ is isomorphic to $\mathcal{K}_\rho$. By tale descent the line bundle $\tau_P^*\mathcal{K}_\rho$ is classified by the descent data $(\tau_P^*\mathcal{K}|_U, \tau_P^*\rho|_U)$. Applying the uniqueness part of tale descent it will suffice to prove that this descent data is equivalent to $(\mathcal{K}|_U, \rho|_U)$, i.e., that there exists an isomorphism $\phi : \mathcal{K}|_U \longrightarrow \tau_P^*\mathcal{K}|_U$ such that the square

$$\begin{tikzcd} \mathcal{K}|_U \arrow[r, "\phi"] \arrow[d, "\rho|_U"'] & \tau_P^*\mathcal{K}|_U \arrow[d, "\tau_P^*\rho|_U"] \\ \iota_U^*\mathcal{K}|_U \arrow[r, "\iota_U^*\phi"'] & \iota_U^*\tau_P^*\mathcal{K}|_U \end{tikzcd} \tag{21}$$

commutes. Now by the construction of $\mathcal{K}$ we know that there is some isomorphism $\phi : \mathcal{K} \longrightarrow \tau_P^*\mathcal{K}$ defined over all of A. It will hence suffice to show that the square of line bundles over A

$$\begin{tikzcd} \mathcal{K} \arrow[r, "\phi"] \arrow[d, "\rho"'] & \tau_P^*\mathcal{K} \arrow[d, "\tau_P^*\rho"] \\ \iota_A^*\mathcal{K} \arrow[r, "\iota_A^*\phi"'] & \iota_A^*\tau_P^*\mathcal{K} \end{tikzcd} \tag{22}$$

commutes. Since A has no non-constant invertible functions the square (22) commutes if and only if the corresponding square of fibers at 0 commutes. Unwinding the definitions we may identify the latter square with

$$\begin{tikzcd} \mathcal{K}_0 \arrow[r, "\phi_0"] \arrow[d, "\rho_0"'] & \mathcal{K}_{\mathcal{P}} \arrow[d, "\rho_P"] \\ \mathcal{K}_0 \arrow[r, "\phi_0"'] & \mathcal{K}_{\mathcal{P}} \end{tikzcd} \tag{23}$$

which indeed commutes since both ρ_0 and ρ_P are the identity maps by the main property of $\mathcal{K}$ (see (2)). □

Corollary 3.21. *The quadratic map* (20) *is invariant under quadratic twists.*

Proof. Let $\overline{\mathcal{K}}$ be a line bundle on W satisfying the conclusion of Lemma 3.20 and let us fix an isomorphism $p^*\overline{\mathcal{K}} \cong \mathcal{K}|_U$. Since neither W nor U have non-constant invertible functions we obtain an induced isomorphism $\mathrm{Aut}(\overline{\mathcal{K}}) \cong \mathrm{Aut}(\mathcal{K}|_U) \cong \mathrm{Aut}(\mathcal{K})$. We may then conclude that for every field L containing k the L-points of the Heisenberg group are in canonical bijection with the group of pairs (P, ϕ) where $P \in A[2](L)$ and $\phi : \overline{\mathcal{K}} \xrightarrow{\cong} \tau_P^*\overline{\mathcal{K}}$ is an isomorphism. By transport of structure the latter groups also assemble the form a group scheme $\mathcal{H}_{\overline{\mathcal{K}}}$ over k, which is equipped with a canonical isomorphism $\mathcal{H}_{\overline{\mathcal{K}}} \cong \mathcal{H}_{\mathcal{K}}$.

Now suppose that we replace A by a quadratic twist A^F. Then we have a canonical isomorphism $A^F[2] \cong A[2]$ and the complement of $A^F[2]$ in A is the twist U^F of U and carries a canonical map $p^F : U^F \longrightarrow X$ (which can be identified with the twist of the tale covering p by the class of F). The induced action of $A^F[2]$ on W then coincides with the action of $A[2]$ via the isomorphism $A^F[2] \cong A[2]$. Let $\mathcal{P}^F$ be the Poincar line bundle on $A^F \times \hat{A}^F$ and let $\mathcal{K}^F := (\mathrm{Id}, \lambda^F)^*\mathcal{P}$ be the pulled back line bundle on A^F. We now claim that $p^F\overline{\mathcal{K}}$ is isomorphic to $\mathcal{K}^F|_U$. Since the map $\mathrm{Pic}(U^F) \longrightarrow \mathrm{Pic}(U^F \otimes_k F)$ is injective it will suffice to show that $p^F\overline{\mathcal{K}}$ becomes isomorphic to $\mathcal{K}^F|_U$ over F. Now by the construction there exists a canonical isomorphism of abelian varieties $T : U \otimes_k F \xrightarrow{\cong} U^F \otimes_k F$ which is compatible with the corresponding principal polarizations and compatible with the projections $p : U \longrightarrow W$ and $p^F : U^F \longrightarrow W$. Since the Poincar line bundle is preserved under base change it follows that the isomorphism T identifies the line bundle $\mathcal{K}^F|_U$ with the line bundle $\mathcal{K}|_U$. On the other hand, T also identifies $(p^F)^*\overline{\mathcal{K}}$ with $\mathcal{K}|_U$. It then follows that $(p^F)^*\overline{\mathcal{K}}$ is isomorphic to $\mathcal{K}^F|_U$ over F and hence over k. We hence obtain canonical isomorphisms of Heisenberg groups

$$\mathcal{H}_{\mathcal{K}} \cong \mathcal{H}_{\overline{\mathcal{K}}} \cong \mathcal{H}_{\mathcal{K}'}$$

which are compatible with the canonical isomorphism $A^F[2] \cong A[2]$. It then follows that the quadratic refinement (20) of the Tate pairing is invariant under quadratic twists, as desired. □

3.5. **Finite quadratic modules.** Let M be a finite abelian group. By a **quadratic form** on M we will mean a function $q : M \longrightarrow \mathbb{Q}/\mathbb{Z}$ such that

(1) The function $B_q : M \times M \longrightarrow \mathbb{Q}/\mathbb{Z}$ given by $B_q(x, y) = q(x + y) - q(x) - q(y)$ is additive in each variable separately;
(2) $q(av) = a^2 v$ for every $a \in \mathbb{Z}$.

A **finite quadratic module** is a finite abelian group M together with a quadratic form $q : M \longrightarrow \mathbb{Q}/\mathbb{Z}$ such that the associated pairing $B_q : M \times M \longrightarrow \mathbb{Q}/\mathbb{Z}$ is perfect, i.e., induces an isomorphism $M \longrightarrow \hat{M} = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$. If (M, q) is a finite quadratic module then we say that a subgroup $L \subseteq M$ is **isotropic** if q vanishes on L, in which case L is contained in its orthogonal complement $L^\perp = \{m \in M | B_q(m, l) = 0, \forall l \in L\}$. A **Lagrangian** of (M, q) is an isotropic subgroup $L \subseteq M$ such that the inclusion $L \subseteq L^\perp$ is an equality.

Remark 3.22. If L is a Lagrangian of a finite quadratic module (M, q) then the associated bilinear form $B_q(-, -)$ induces a perfect pairing between L and M/L. It then follows that $|L| = |M/L|$ and $|M| = |L||M/L| = |L|^2$. In particular, if M admits a Lagrangian then the size of M is a perfect square and the size of every Lagrangian is a square root of $|M|$.

Our goal in this section is to prove the statement below, which restricts the possible ways in which Lagrangian subgroups of a given finite quadratic module can intersect. The following proposition can be considered as a (mild) generalization of [KMR11, Proposition 2.4] to the setting of finite quadratic modules (using a very similar proof). While we could in principle have made due only with the statements of [KMR11] (as was done in a previous version of this paper), this would have come at a cost of some unnecessary restrictions of generality in the usage of the Mazur-Rubin lemma (see §3.6), and make some of the arguments less transparent. Motivated by some of the remarks made by the referee after reading a previous version of the paper, and with an eye towards future generalizations, we have opted to offer a self-contained proof of the precise result we needed:

Proposition 3.23. *Let (M, q) be a finite quadratic module and let $L_0, L_1, L_2 \subseteq M$ be three Lagrangian subgroups. For $i, j = 0, 1, 2$ let us denote $L_{i,j} = L_i/(L_i \cap L_j)$. Then $|L_{0,1}| \cdot |L_{1,2}| \cdot |L_{2,0}|$ is a perfect square.*

Proof. To facilitate sign conventions we will consider L_0, L_1, L_2 as indexed by $\mathbb{Z}/3$. Consider the chain complex

$$C_\bullet = \left[\bigoplus_{i\in\mathbb{Z}/3} L_i \cap L_{i,i+1} \longrightarrow \bigoplus_i L_i \longrightarrow M \right],$$

located in degrees $1 \longrightarrow 0 \longrightarrow -1$. Here the first map sends $x \in L_i \cap L_{i+1}$ to the sum of the image of x in the L_i component and the image of $-x$ in the L_{i+1} component, and the second map is simply induced by the inclusions $L_i \subseteq M$. Since $|M|$ is a square by Remark 3.22 it will suffice to show that

$$\frac{|L_{0,1}||L_{1,2}||L_{2,0}|}{|M|} = \frac{|C_0|}{|C_{-1}||C_1|} = \frac{|H_0(C_\bullet)|}{|H_{-1}(C_\bullet)||H_1(C_\bullet)|}$$

is a rational square.

We now observe that the diagonal inclusion $L_0 \cap L_1 \cap L_2 \hookrightarrow \oplus_{i\in\mathbb{Z}/3} L_i \cap L_{i,i+1}$ induces an isomorphism $L_0 \cap L_1 \cap L_2 \xrightarrow{\cong} H_1(C_\bullet)$ and the natural projection $M \longrightarrow M/(L_1 + L_2 + L_3)$ induces an isomorphism $H_{-1}(C_\bullet) \xrightarrow{\cong} M/(L_1 + L_2 + L_3)$. In particular, the perfect pairing B_q then induces a perfect pairing between $H_1(C_\bullet)$ and $H_{-1}(C_\bullet)$, and so $|H_1(C_\bullet)| = |H_{-1}(C_\bullet)|$. To finish the proof it will hence suffice to show that the order of $H_0(C_\bullet)$ is a square.

To prove this we will construct a perfect alternating self-pairing on $H_0(C_\bullet)$. Explicitly, we may represent elements of $H_0(C_\bullet)$ by 0-cycles, which in the case of $C_\bullet$ are triples $(x_0, x_1, x_2) \in L_0 \oplus L_1 \oplus L_2$ such that $x_0 + x_1 + x_2 = 0 \in M$. We then define a self-pairing on the level of 0-cycles by $B_\varphi((x_0, x_1, x_2), (x'_0, x'_1, x'_2)) = B_q(x_0, x'_1)$. This bilinear form is alternating already on the level of 0-cycles:

$$B_\varphi((x_0,x_1,x_2),(x_0,x_1,x_2)) = B_q(x_0,x_1) = q(x_0+x_1) - q(x_0) - q(x_1) = q(-x_2) - q(x_0) - q(x_1) = 0,$$

since L_0, L_1, L_2 are all isotropic. In particular, we have $B_\varphi((x_0, x_1, x_2), (x'_0, x'_1, x'_2)) = B_q(x_0, x'_1) = -B_q(x'_0, x_1)$. It then follows that this pairing vanishes for every (x'_0, x'_1, x'_2) as soon as $x_0 = 0$ or $x_1 = 0$ or $x_0 = -x_1$ (since L_1 is isotropic with respect to B_q). The kernel of this pairing then contains the image of the differential $\partial : C_1 \longrightarrow C_0$ and hence descends to an alternating self-pairing on $H_0(C_\bullet)$.

To show that this pairing is perfect suppose that (x_0, x_1, x_2) is orthogonal to all 0-cycles (x'_0, x'_1, x'_2). It then follows that x_0 is B_q-orthogonal to all $x'_1 \in L_1 \cap (L_0 + L_2)$, which means that x_0 belongs to $(L_1 \cap (L_0 + L_2))^\perp = L_1 + (L_2 \cap L_0)$. By adding to (x_0, x_1, x_2) a 0-boundary of the form $(y, 0, -y) = \partial y$ for $y \in L_2 \cap L_0 \subseteq C_1$ we may assume that x_0 belongs to L_1. Since $x_2 = -x_0 - x_1$ it then follows that x_2 belongs to L_1 as well. We then obtain that (x_0, x_1, x_2) is the boundary of the element $(x_0, -x_2, 0) \in (L_0 \cap L_1) \oplus (L_1 \cap L_2) \oplus (L_2 \cap L_0)$ and so (x_0, x_1, x_2) vanishes in $H_0(C_\bullet)$. □

3.6. **Quadratic twists and the Mazur-Rubin lemma.** Let A be an abelian variety over k equipped with a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$. Let $\alpha \in H^1(k, A[2])$ be an element and let Y_α be the associated 2-covering of A. Then Y_α carries an adelic point if and only the image $[Y_\alpha] \in H^1(k, A)$ of α lies in Ш(A). Recall that the **Selmer** group $\mathrm{Sel}_2(A) \subseteq H^1(k, A[2])$ is defined as the preimage of Ш$(A) \subseteq H^1(k, A)$ under the natural map $H^1(k, A[2]) \longrightarrow H^1(k, A)$. We then have a short exact sequence

$$0 \longrightarrow A(k)/2A(k) \longrightarrow \mathrm{Sel}_2(A) \longrightarrow Ш(A)[2] \longrightarrow 0.$$

Given a quadratic extension F/k we may canonically identify $H^1(k, A[2])$ with $H^1(k, A^F[2])$, and consequently consider the Selmer groups $\mathrm{Sel}_2(A^F)$ for all F/k as subgroup of the same group $H^1(k, A[2])$. In order to use Swinnerton-Dyer's method in the proof of the main theorem, we will need to know how the Selmer group changes when one makes sufficiently simple quadratic twists. For this purpose we will use an approach developed by Mazur and Rubin for analyzing the behavior of Selmer groups in families of quadratic twists (see [MR10, §3]).

For a place v of k and a (possibly trivial) quadratic extension F/k, let $W_v^F \subseteq H^1(k_v, A[2])$ be the kernel of the map $H^1(k_v, A[2]) = H^1(k_v, A^F[2]) \longrightarrow H^1(k_v, A^F)$. The Selmer group $\mathrm{Sel}_2(A^F) \subseteq H^1(k, A[2])$ is then determined by the condition that $\mathrm{loc}_v(x) \in W_v^F$ for every place $v \in \Omega_k$. When F is the trivial quadratic extension we will denote W_v^F simply by W_v. The intersection $U_v = W_v \cap W_v^F$ is then a measure of the difference between the Selmer conditions before and after a quadratic twist by F. It will also be useful to encode this information via the corresponding quotients $\overline{W}_v = W_v/U_v$ and $\overline{W}_v^F = W_v^F/U_v$. Given a finite set of places $T \subseteq \Omega_k$ we will write $\overline{W}_T^F := \oplus_{v\in T}\overline{W}_v^F$ and denote by $V_T^F \subseteq \overline{W}_T^F$ the image of $\mathrm{Sel}_2(A^F)$. As above, when F is the trivial extension we will simply drop the supscript F from the notation, yielding $\overline{W}_T$ and V_T.

For each place v of k we have the local Tate pairing (see §3.4):

$$\cup_v : H^1(k_v, A[2]) \times H^1(k_v, A[2]) \longrightarrow H^2(k_v, \mu_2) \overset{\mathrm{inv}}{\cong} \mathbb{Z}/2. \tag{24}$$

as well as its quadratic refinement

$$q_{k_v} : H^1(k_v, A[2]) \longrightarrow H^2(k_v, \mathbb{G}_m) \overset{\mathrm{inv}}{\cong} \mathbb{Q}/\mathbb{Z}. \tag{25}$$

defined as in (20). Local arithmetic duality for abelian varieties asserts that the pairing (24) is non-degenerate and admits $W_v \subseteq H^1(k_v, A[2])$ as a maximal isotropic subspace. Furthermore, by [PR12, Proposition 4.9] the quadratic enhancement q_{k_v} vanishes on W_v, and so W_v is in fact a Lagrangian subgroup (see §3.5). In particular, $\dim_2 W_v = \frac{1}{2}\dim_2 H^1(k_v, A[2])$.

We note that the pairing $\cup_v$ is defined only in terms of the Galois module $A[2]$, and hence in the presence of a quadratic extension F/k the canonical isomorphism $A[2] \cong A^F[2]$ identifies the Tate pairings (24) associated to A and A^F respectively. By Corollary 3.21 this isomorphism also identifies the quadratic enhancements (25) associated to A and A^F respectively.

Lemma 3.24. *Let v be a place of good reduction for A and let F be a quadratic extension which is ramified at v. Then $U_v = 0$.*

Proof. See [HS15, Lemma 4.3]. □

Lemma 3.25. *Let w be a place of semi-abelian reduction for A whose geometric component group is cyclic of order 2 mod 4. Let F be a quadratic extension in which w is inert (and in particular unramified). Then $\dim_2 \overline{W}_w = \overline{W}_w^F = 1$. Furthermore, the intersection $W_w \cap W_w^F$ contains exactly the elements of W_w (or W_w^F) which are unramified.*

Proof. Since F is unramified at w the components groups C_w and C_w^F of A and A^F respectively are naturally isomorphic. To compute $W_w \cap W_w^F$ we use Lemma 4.1

of [HS15] which asserts that

$$W_w \cap W_w^F = \delta(\mathrm{N}(A(F_w)))$$

where $F_w = F \otimes_k k_w$ and $\mathrm{N} : A(F_w) \longrightarrow A(k_w)$ is the norm map. Combining [Ma72, Proposition 4.2, Proposition 4.3], and using the fact that A is isomorphic to its dual by the principal polarization λ, we may deduce that

$$A(k_w)/\mathrm{N}(A(F_w)) \cong H^1(\mathrm{Gal}(F/k_v), C_w) \cong \mathbb{Z}/2.$$

On the other hand, since $2A(k_w) \subseteq \mathrm{N}(A(F_w))$ the boundary map $\delta : A(k_w) \longrightarrow H^1(k_v, A[2])$ induces an isomorphism

$$A(k_w)/\mathrm{N}(A(F_w)) \cong \delta(A(k_w))/\delta(\mathrm{N}(A(F_w))) \cong W_w/(W_w \cap W_w^F)$$

and so the latter group is isomorphic to $\mathbb{Z}/2$, as desired. Finally, let us note that since F/k_w is unramified the base change A_F also has a semi-abelian reduction at w with component group $C_w^F \cong C_w$. In particular $C_w^F/2C_w^F \cong \mathbb{Z}/2$ has trivial Galois action and so every point in $\mathrm{N}(A(F_w))$ reduces to a component in $2C_w$. Since $A(k_w)/\mathrm{N}(A(F_w)) \cong \mathbb{Z}/2$ it follows that this condition is sufficient as well, i.e., the points of $A(k_w)$ which are norm from $A(F_w)$ are exactly those whose image in $C_w/2C_w$ is trivial. On the other hand, by Hensel's lemma these are also exactly the points which are divisible by 2 in $A(k_w^{\mathrm{un}})$, and hence exactly the points $x \in A(k_w)$ such that $\delta(x)$ is unramified. □

Remark 3.26. Suppose that the abelian variety A admits a 2-structure $M \subseteq \Omega_k$ in the sense of Definition 2.1, and let $\{Q_w\}_{w \in M}$ be the basis of $A[2]$ described in §3.1. Then any place w which belongs to M will satisfy the conditions of Lemma 3.25. Combining Lemma 3.25 and Corollary 3.8 we may conclude that the Selmer condition subspace $W_w \subseteq H^1(k_w, A[2])$ is generated over $W_w \cap H^1(\mathcal{O}_w, A[2])$ by the element $\delta(Q_w)$. This implies that every element of $\mathrm{Sel}_2(A)$ can be written uniquely as a sum of an element unramified over M and an element in the image of $A[2]$.

Now let T be such that $W_v = W_v^F$ for every $v \notin T$. Then the kernel of the surjective map $\mathrm{Sel}_2(A) \longrightarrow V_T$ can be identified with the kernel of the surjective map $\mathrm{Sel}_2(A^F) \longrightarrow V_T^F$, and hence

$$\dim_2(\mathrm{Sel}(A^F)) - \dim_2(\mathrm{Sel}(A)) = \dim_2(V_T^F) - \dim_2(V_T).$$

The following lemma, which is based on the ideas of Mazur and Rubin for analyzing the behavior of Selmer groups in families of quadratic twists (see [MR10, §3]), is our key tool for controlling the difference $\dim_2(\mathrm{Sel}(A^F)) - \dim_2(\mathrm{Sel}(A))$ after quadratic twists.

Lemma 3.27 ((Mazur-Rubin))**.** *Let A be a principally polarized abelian variety. Let F/k be a quadratic extension and let T be a finite set of odd places of k such that $W_v = W_v^F$ for every $v \notin T$. Let $r = \dim_2 \overline{W}_T = \dim_2 \overline{W}_T^F$. Then*

$$\dim_2 V_T + \dim_2 V_T^F \leq r$$

and the gap $r - \dim_2 V_T - \dim_2 V_T^F$ is even.

Proof. Let

$$W_v \times W_v^F \longrightarrow \mathbb{Z}/2 \tag{26}$$

be the restriction of the local Tate pairing 24. Since W_v and W_v^F are both maximal isotropic with respect to 24 it follows that the left and right kernels of 26 can both be identified with $W_v \cap W_v^F$, and so 26 descends to a non-degenerate pairing

$$\overline{W}_v \times \overline{W}_v^F \longrightarrow \mathbb{Z}/2 \tag{27}$$

By summing over the places of T we obtain a non-degenerate pairing

$$\overline{W}_T \times \overline{W}_T^F \longrightarrow \mathbb{Z}/2 \tag{28}$$

between two vector spaces of dimension r. Finally, by quadratic reciprocity and the fact that $W_v = W_v^F$ for $v \notin T$ we get that the subspaces $V_T \subseteq \overline{W}_T$ and $V_T^F \subseteq \overline{W}_T^F$ are orthogonal to each other with respect to (28) and so V_T is contained in the orthogonal complement of V_T^F, and vice versa. This yields the desired bound

$$\dim_2(V_T) + \dim_2(V_T^F) \leq r.$$

Let us now show that that the gap between $\dim_2(V_T) + \dim_2(V_T^F)$ and r is even (cf. [HW16, Theorem 2.3]). Since $\dim_2 \overline{W}_v = 0$ for $v \notin T$ we see that for the purpose of this lemma we may as well replace T with any bigger finite subset of places. In particular, we may assume that $W_v = H^1(\mathcal{O}_v, A[2])$ for $v \notin T$ and by global duality theory we may also insure that the group $H^1(\mathcal{O}_T, A[2])$ embeds in $\sum_{v\in T} H^1(k_v, A[2])$ as a maximal isotropic subgroup with respect to the sum of local cup products $\cup_T = \sum_{v\in T} \cup_v$. Now let

$$q_T : \sum_{v\in T} H^1(k_v, A[2]) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

be the quadratic map obtained by summing the local quadratic refinements q_{k_v} (25). We then have $q_T(x+y) - q_T(x) - q_T(y) = x \cup_T y$ and q_T is invariant under quadratic twists by Corollary 3.21. By [PR12, Proposition 4.9, Theorem 4.13] the quadratic form q_T vanishes on the isotropic subgroups $H^1(\mathcal{O}_T, A[2])$, $\oplus_v W_v$ and $\oplus_v W_v^F$. In particular, the pair $(\oplus_{v\in T} H^1(k_v, A[2]), q_T)$ is a **finite quadratic module** (see §3.5) which admits $L_0 := H^1(\mathcal{O}_T, A[2])$, $L_1 := \oplus_v W_v$ and $L_2 := \oplus_v W_v^F$ as Lagrangians. Now let $V_T' \subseteq \sum_{v\in T} W_v$ and $(V_T^F)' \subseteq \sum_{v\in T} W_T^F$ be the images of $\mathrm{Sel}_2(A)$ and $\mathrm{Sel}_2(A^F)$ respectively. Then the kernel of $V_T' \longrightarrow V_T$ and the kernel of $(V_T^F)' \longrightarrow V_T^F$ are both isomorphic to the image of $\mathrm{Sel}_2(A) \cap \mathrm{Sel}_2(A^F)$ in $\sum_{v\in T}\left[W_v \cap W_v^F\right]$ and so

$$\dim_2 V_T - \dim_2 V_T^F = \dim_2 V_T' - \dim_2 (V_T^F)'.$$

In particular, $\dim_2 V_T + \dim_2 V_T^F$ has the same parity as $\dim_2 V_T' + \dim_2 (V_T^F)'$. On the other hand, since $W_v = W_v^F = H^1(\mathcal{O}_v, A[2])$ for $v \notin T$ we have $V_T' = L_1 \cap L_0$ and $(V_T^F)' = L_2 \cap L_0$. Applying Proposition 3.23 to L_0, L_1, L_2 (and using the fact that all Lagrangians have the same size) we may conclude that the quantity

$$\dim_2 V_T' + \dim_2 (V_T^F)' = \dim_2(L_1 \cap L_0) + \dim_2(L_2 \cap L_0)$$

has the same parity as

$$r = \dim_2(\overline{W}_T) = \dim_2(L_1/(L_1 \cap L_2)).$$

It then follows that $\dim_2 V_T + \dim_2(V_T^F)$ has the same parity as r, as desired. □

The above lemma of Mazur and Rubin will be used to understand the change in Selmer groups under quadratic twists. This step in Swinnerton-Dyer's method can be roughly described as performing "2-descent in families". As explained in §1, our current application of this method includes a new step of "second 2-descent in families". To this end we will need to know not only how the Selmer group changes in quadratic twists, but also how the Cassels-Tate pairing changes in quadratic twists.

From this point on we **fix the assumption** that the Galois action on $A[2]$ is trivial. By pre-composing the Cassels-Tate pairing with the natural map $\mathrm{Sel}_2(A) \longrightarrow Ш(A)[2]$ we obtain an induced (generally degenerate) pairing

$$\langle,\rangle_A^{\mathrm{CT}} : \mathrm{Sel}_2(A) \times \mathrm{Sel}_2(A) \longrightarrow \mathbb{Z}/2.$$

We note that if $\alpha,\beta \in \mathrm{Sel}_2(A)$ are elements which also belong to $\mathrm{Sel}_2(A^F)$ then the Cassels-Tate pairings $\langle\alpha,\beta\rangle_A^{\mathrm{CT}}$ and $\langle\alpha,\beta\rangle_{A^F}^{\mathrm{CT}}$ are generally different. The following proposition gives some information on the difference between $\langle\alpha,\beta\rangle_A^{\mathrm{CT}}$ and $\langle\alpha,\beta\rangle_{A^F}^{\mathrm{CT}}$. To phrase the result we will need to establish some terminology.

Recall that the Cassels-Tate pairing is defined using a certain homomorphism

$$B_\alpha : H^1(k,\hat{A}[2]) \longrightarrow \mathrm{Br}(Y_\alpha)/\mathrm{Br}(k)$$

as described in §3.2. For every quadratic extension F/k let

$$B_\alpha^F : H^1(k,\hat{A}[2]) \longrightarrow \mathrm{Br}(Y_\alpha^F)/\mathrm{Br}(k)$$

be the analogous map, constructed using the canonical isomorphism $\hat{A}[2] \cong \hat{A}^F[2]$.

Let us now resume the notation of §3.3. In particular, we have the involution $\iota_{Y_\alpha} : Y_\alpha \longrightarrow Y_\alpha$ whose fixed locus is the 0-dimensional scheme $Z_\alpha \subseteq Y_\alpha$. The variety $\widetilde{Y}_\alpha$ is the blow-up of Y_α at Z_α and the Kummer variety X_α is defined as the quotient $\widetilde{Y}_\alpha/\iota_{Y_\alpha}$. Recall that we have denoted by $D_\alpha \subseteq X_\alpha$ the image of the exceptional divisor of $\widetilde{Y}_\alpha$ and by $W_\alpha = X_\alpha \smallsetminus D_\alpha \subseteq X_\alpha$ its complement. The degree 2 map $\widetilde{Y} \longrightarrow X_\alpha$ is then ramified exactly along $D_\alpha \subseteq X_\alpha$ and restricts to an tale covering $p_\alpha : U_\alpha \longrightarrow W_\alpha$, where $U_\alpha \subseteq Y_\alpha$ is the complement of Z_α. In particular, we may find an open subset $X_\alpha^0 \subseteq X_\alpha$ and a regular function f on X_α^0 such that $\mathrm{div}(f) = D_\alpha \cap X_\alpha^0 =: D_\alpha^0$ and such that the map $\widetilde{Y}_\alpha \times_{X_\alpha} X_\alpha^0 \longrightarrow X_\alpha^0$ admits an affine equation of the form $x^2 = f$ inside $X_\alpha^0 \times \mathbb{A}_k^1$, where x is a coordinate on $\mathbb{A}_k^1$. Reducing X_α^0 if necessary we may also assume that the differential df is nowhere vanishing on D_α^0.

In §3.3 we considered a map of the form

$$C_\alpha : H^1(k,\mathrm{Aff}(\overline{Z}_\alpha,\mu_2)) \longrightarrow \mathrm{Br}(W_\alpha)/\mathrm{Br}(k),$$

see (10) and the discussion following it. In particular, if $\theta \in H^1(k,\mathrm{Aff}(\overline{Z}_\alpha,\mu_2))$ is an element such that $(h_\alpha)_*(\theta) = \beta$, then $p_\alpha^* C_\alpha(\theta) = B_\alpha(\beta)|_{U_\alpha} \in \mathrm{Br}(U_\alpha)/\mathrm{Br}(k)$. In fact $(p_\alpha^F)^* C_\alpha(\theta) = B_\alpha^F(\beta)|_{U_\alpha^F}$ for every F/k.

Let us now fix a finite set S of places containing all the archimedean places, all the places above 2 and all the places of bad reduction for A. By possibly enlarging S we may find $\mathcal{O}_S$-smooth models $\mathcal{X}_\alpha, \mathcal{X}_\alpha^0$ and $\mathcal{D}_\alpha$ for X_α, X_α^0 and D_α respectively and an S-integral regular function $\mathfrak{f} \in \mathcal{O}_S[\mathcal{X}_\alpha^0]$ extending f such that $\mathcal{D}_\alpha^0 := \mathrm{div}(\mathfrak{f})$ is an integral model for D_α^0 and such that $d\mathfrak{f}$ does not vanish on $\mathcal{D}_\alpha^0$. We then also obtain an $\mathcal{O}_S$-smooth model $\mathcal{W}_\alpha := \mathcal{X}_\alpha \smallsetminus \mathcal{D}_\alpha$ for W_α. For a $v \notin S$ we will denote by $(\mathcal{X}_\alpha)_v, (\mathcal{X}_\alpha^0)_v, (\mathcal{D}_\alpha^0)_v$ and $(\mathcal{D}_\alpha)_v$ the respective base changes from $\mathrm{spec}(\mathcal{O}_S)$ to $\mathrm{spec}(\mathcal{O}_v)$. Finally, by possibly enlarging S we may assume that the class $[p_\alpha] \in H^1(W_\alpha,\mathbb{Z}/2)$ comes from $H^1(\mathcal{W}_\alpha,\mathbb{Z}/2)$ and that for every $v \notin S$ the corresponding evaluation map $\mathcal{W}_\alpha(\mathcal{O}_v) \longrightarrow H^1(\mathcal{O}_v, \mathbb{Z}/2) \cong \mathbb{Z}/2$ sending $x \in \mathcal{W}_\alpha(\mathcal{O}_v)$ to $[x^*p_\alpha] \in H^1(\mathcal{O}, \mathbb{Z}/2)$ is surjective.

Remark 3.28. Let $v \notin S$ be a place. Given a uniformizer $\pi \in \mathcal{O}_v$ and an $\mathbb{F}_v$-point $\overline{x} \in \mathcal{D}^0_\alpha(\mathbb{F}_v) \subseteq \mathcal{X}^0_\alpha(\mathbb{F}_v)$, since $df(x) \neq 0$ we may use Hensel's lemma to find a point $x \in \mathcal{X}^0_\alpha(\mathcal{O}_v)$ which reduces to $\overline{x}$ and such that $f(x) = \pi \mod (\pi^2)$. In particular, in this case $x : \mathrm{spec}(\mathcal{O}_n) \hookrightarrow \mathcal{X}^0_\alpha$ intersects $\mathcal{D}^0_\alpha \subseteq \mathcal{X}^0_\alpha$ transversely and the tale covering $x^*p_\alpha : \widetilde{Y}_\alpha \times_{X_\alpha} \mathrm{spec}(k_v) \longrightarrow \mathrm{spec}(k_v)$ is classified by $[\pi] \in H^1(k_v, \mu_2)$.

Proposition 3.29. *Let $\alpha, \beta \in \mathrm{Sel}_2(A)$ be two elements unramified outside $S \smallsetminus M$ and let $\theta \in H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ be an element such that $(h_\alpha)_*(\theta) = \beta$, and such that the splitting field k_θ is unramified outside $S \smallsetminus M$. Assume in addition that $C_\alpha(\theta)$ can be represented by a Brauer element $C \in \mathrm{Br}(W_\alpha)$ which extends to the S-integral model $\mathcal{W}_\alpha$. Let $a \in k^*$ be an element which is a unit over S and a square over $S \smallsetminus M$, and such that for each place v with $\mathrm{val}_v(a)$ odd, the Frobenius element $\mathrm{Frob}_v(k_{\alpha,\beta})$ is trivial. Set $F = k(\sqrt{a})$. Then α and β belong to $\mathrm{Sel}_2(A^F)$ and*

$$\langle \alpha, \beta \rangle^{\mathrm{CT}}_{A^F} - \langle \alpha, \beta \rangle^{\mathrm{CT}}_{A} = \prod_{\mathrm{val}_v(a) = 1 \bmod 2} \mathrm{Frob}_v(k_\theta / k_{\alpha,\beta}) \in \mathrm{Gal}(k_\theta / k_{\alpha,\beta}) \subseteq \mathbb{Z}/2$$

Proof. Let us first show that α and β belong to the Selmer group $\mathrm{Sel}_2(A^F)$ after quadratic twist. For a place $v \in S \smallsetminus M$ we have that a is a square at v and hence the Selmer conditions of A and A^F are the same at v. For $w \in M$ the fact that α, β satisfy the Selmer condition of A at w and are furthermore unramified at w implies by Lemma 3.25 that α, β satisfy the Selmer condition of A^F at w. Finally, for $v \notin S$, if $\mathrm{val}_v(a)$ is even then A^F has good reduction at v and so the Selmer condition of A^F at v is the same as that of A. On the other hand, if $\mathrm{val}_v(a)$ is odd then by assumption the Frobenius element $\mathrm{Frob}_v(k_{\alpha,\beta})$ is trivial which means that α, β restrict to 0 in $H^1(k_v, A[2])$, and hence in particular satisfy the Selmer condition of A^F at v. We may hence conclude that $\alpha, \beta \in \mathrm{Sel}_2(A^F)$.

Now since α belongs to both $\mathrm{Sel}_2(A)$ and $\mathrm{Sel}_2(A^F)$ we may find two adelic points $(x_v), (x^F_v) \in \prod_v W_\alpha(k_v) \subseteq X_\alpha(\mathbb{A}_k)$ such that (x_v) lifts to $\prod_v U_\alpha(k_v) \subseteq Y_\alpha(\mathbb{A}_k)$ and (x^F_v) lifts to $\prod_v U^F_\alpha(k_v) \subseteq Y^F_\alpha(\mathbb{A}_k)$. Furthermore, by the properties of S and using Remark 3.28 we may insure the following:

(1) For every place v such that a is a square at v (e.g., every $v \in S \smallsetminus M$) we have $x^F_v = x_v$.
(2) For every v such that $\mathrm{val}_v(a)$ is odd the Zariski closure $\mathcal{x}^F_v \in (\mathcal{X}_\alpha)_v$ of x^F_v intersects $(\mathcal{D}_\alpha)_v \subseteq (\mathcal{X}_\alpha)_v$ transversely at a single closed point of degree 1 (see Remark 3.28).
(3) For every $v \notin S$ we have $x_v \in \mathcal{W}_\alpha(\mathcal{O}_v)$.
(4) For every $v \notin S$ such that $\mathrm{val}_v(a)$ is even we have $x^F_v \in \mathcal{W}_\alpha(\mathcal{O}_v)$.

Let $S(a)$ denote the set of places v such that $\mathrm{val}_v(a)$ is odd. Since $p^*_\alpha C_\alpha(\theta) = B_\alpha(\beta)|_{U_\alpha}$ and $(p^F_\alpha)^* C_\alpha(\theta) = B^F_\alpha(\beta)|_{U^F_\alpha}$ and by our assumptions on C we have

$$\langle \alpha, \beta \rangle^{\mathrm{CT}}_{A} = \sum_v \mathrm{inv}_v\, C(x_v) = \sum_{v \in S} \mathrm{inv}_v\, C(x_v)$$

and

$$\langle \alpha, \beta \rangle^{\mathrm{CT}}_{A^F} = \sum_v \mathrm{inv}_v\, C(x^F_v) = \sum_{v \in S \cup S(a)} \mathrm{inv}_v\, C(x^F_v).$$

Now for $v \in S \smallsetminus M$ we have $x_v = x_v^F$ and so $C(x_v) = C(x_v^F)$. Furthermore, by Corollary 3.17 we have that C evaluates to the same value on x_w and x_w^F for every $w \in M$. We may hence conclude that

$$\langle \alpha, \beta \rangle_{A^F}^{\mathrm{CT}} - \langle \alpha, \beta \rangle_{A}^{\mathrm{CT}} = \sum_{v \in S(a)} \mathrm{inv}_v \, C(x_v^F).$$

Now let $v \in S(a)$ be a place. Since C extends to the S-integral model $\mathcal{W}_\alpha$ it has non-trivial residues only along $\mathcal{D}_\alpha$. Since x_v^F intersects $\mathcal{D}_\alpha$ transversely at a single closed point of degree 1 we see that the residue of $x^*C \in \mathrm{Br}(\mathrm{spec}(k_v))$ along $\mathrm{spec}(\mathbb{F}_v)$ coincides with the restriction of $\mathrm{res}_{\mathcal{D}_\alpha}(C) \in H^1(\mathcal{D}_\alpha, \mathbb{Q}/\mathbb{Z})$ to the intersection point $x_v^F \cap \mathcal{D}_\alpha$. Now since the images of α and β in $H^1(k_v, A[2])$ vanish it follows that the extension $k_{\alpha,\beta}/k$ splits completely over k_v for every $v \in S(a)$. To prove the theorem we may hence extend our scalars to $k_{\alpha,\beta}$. Proposition 3.15(2) now tells us that the residue $\mathrm{res}_{\mathcal{D}_\alpha}(C) \in H^1(\mathcal{D}_\alpha, \mathbb{Q}/\mathbb{Z})$ becomes constant when restricted to $D_\alpha \otimes_k k_{\alpha,\beta}$ and its value there is given by the quadratic extension $k_\theta/k_{\alpha,\beta}$. The restriction of $\mathrm{res}_{\mathcal{D}_\alpha}(C) \in H^1(\mathcal{D}_\alpha, \mathbb{Q}/\mathbb{Z})$ to the intersection point $x_v^F \cap \mathcal{D}_\alpha$ is then trivial if and only if the Frobenius element $\mathrm{Frob}_v(k_\theta)$ is trivial, and so the desired result follows. □

4. Rational points on Kummer varieties

Our goal in this section is to carry out the proof of Theorem 2.8. We will do so in three steps, which are described in sections §4.1, §4.2 and §4.3, respectively. Each of these steps will be formalized as a proposition (see Propositions 4.8, 4.10 and 4.12 respectively) and the proof of Theorem 2.8, which appears in §4.4, essentially consists of assembling these three propositions into one argument.

In the course of all three steps it will be convenient to know that the abelian varieties and associated 2-coverings under consideration satisfy the following technical condition:

Definition 4.1. Let A be an abelian variety such that the Galois action on $A[2]$ is trivial, let M be a 2-structure for A (Definition 2.1) and let $\alpha \in H^1(k, A[2])$ be an element. We will say that (A, α) is **admissible** if for every pair of functions $f : M \longrightarrow \{0,1\}$ and $h : M \times M \longrightarrow \{0,1\}$ such that

$$\prod_{w \in M} \langle \alpha, P_w \rangle_\lambda^{f(w)} \prod_{(w,u) \in M \times M} \langle \delta(P_w), P_u \rangle_\lambda^{h(w,u)} = 1 \in H^1(k, \mu_2)$$

we also have

$$\prod_{(w,u) \in M \times M} \langle P_w, P_u \rangle_\lambda^{h(w,u)} = 1 \in \mu_2.$$

The following lemma will be used to insure that the condition of Definition 4.1 can be assumed to hold whenever necessary.

Lemma 4.2. *Let A, M and α be as in Definition 4.1. Let S be a finite set of places containing all the archimedean places, all the places above 2, all the places of bad reduction for A and all the places where α is ramified. Let $F = k(\sqrt{a})$ be a quadratic extension which is unramified over S but that is ramified in at least one place outside S. Then (A^F, α) is admissible.*

Proof. Assume that (A^F, α) is not admissible and let $(f, h) \in (\mathbb{Z}/2)^M \times (\mathbb{Z}/2)^{M \times M}$ be such that

$$\prod_{w \in M} \langle \alpha, P_w \rangle_\lambda^{f(w)} \prod_{(w,u) \in M \times M} \langle \delta_F(P_w), P_u \rangle_\lambda^{h(w,u)} = 1 \in H^1(k, \mu_2)$$

but

$$\prod_{(w,u) \in M \times M} \langle P_w, P_u \rangle_\lambda^{h(w,u)} = -1.$$

According to Lemma 3.5 and Remark 3.1 we then have

$$\prod_{w \in M} \langle \alpha, P_w \rangle_\lambda^{f(w)} \prod_{(w,u) \in M \times M} \langle \delta(P_w), P_u \rangle_\lambda^{h(w,u)} = [a] \in H^1(k, \mu_2)$$

Since $k(\sqrt{a})$ is ramified outside S and A has good reduction outside S we obtain a contradiction. It follows that (A^F, α) is admissible. □

4.1. **Quadratic twists with points everywhere locally.** Let A be an abelian variety over k such that the Galois action on $A[2]$ is trivial and let $\alpha \in H^1(k, A[2])$ be an element. Let $X_\alpha = \mathrm{Kum}(Y_\alpha)$ be the Kummer variety associated to Y_α and let $W_\alpha \subseteq X_\alpha$ be as in §3.3. Suppose that $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$. In this section we will consider the problem of finding a quadratic extension F/k such that $Y_\alpha^F(\mathbb{A}_k) \neq \emptyset$, i.e., such that $\alpha \in \mathrm{Sel}_2(A^F)$. Furthermore, to set some prerequisite conditions for the following steps we will wish to guarantee that Y_α^F contains an adelic point which is furthermore orthogonal to certain Brauer elements. Recall that for every quadratic extension F/k we have a homomorphism

$$B_\alpha^F : H^1(k, \hat{A}[2]) \longrightarrow \mathrm{Br}(Y_\alpha^F)/\mathrm{Br}(k)$$

which can be used to define the Cassels-Tate pairing on A^F of α against any other element. Recall also that in §3.3 we considered a similar type of map

$$C_\alpha : H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2)) \longrightarrow \mathrm{Br}(W_\alpha)/\mathrm{Br}(k),$$

see (10) and the discussion following it.

Definition 4.3. We will denote by $\mathcal{C}(W_\alpha) \subseteq \mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ the image of C_α. Similarly, we will denote by $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)/\mathrm{Br}(k)$ the subgroup consisting of those elements whose image in $\mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ lies in $\mathcal{C}(W_\alpha)$.

Proposition 4.4. *Let $\mathcal{B} \subseteq H^1(k, A[2])$ be a finite subgroup which is orthogonal to α with respect to $\cup_\lambda$. If X_α contains an adelic point which is orthogonal to $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)/\mathrm{Br}(k)$ then there exists a quadratic extension F/k such that (A^F, α) is admissible and Y^F contains an adelic point which is orthogonal to $B_\alpha^F(\mathcal{B}) \subseteq \mathrm{Br}(Y_\alpha^F)/\mathrm{Br}(k)$. Furthermore, if M is a 2-structure for A such that α is unramified over M but the image of α in $H^1(k_w, A[2])$ is non-zero for every $w \in M$ then we may choose F to be unramified over M.*

Proof. Let $\mathscr{Y} = (\widetilde{Y}_\alpha \times \mathbb{G}_m)_{/\mu_2}$ where μ_2 acts on $\widetilde{Y}_\alpha$ by ι_{Y_α} and on $\mathbb{G}_m$ by multiplication by -1. Projection on the second factor induces a map $\mathscr{Y} \longrightarrow \mathbb{G}_m/\mu_2 \cong \mathbb{G}_m$ and for $t \in \mathbb{G}_m(k) = k^*$ we may naturally identify the fiber $\mathscr{Y}_t$ with the quadratic twist $\widetilde{Y}_\alpha^{k(\sqrt{t})}$ (which is birational to Y_α^F). As in [SSD05, §5] one can show that $\mathscr{Y} \longrightarrow \mathbb{G}_m$ can be compactified into a fibration $\mathscr{X} \longrightarrow \mathbb{P}^1$ whose fibers over $0, \infty \in \mathbb{P}^1$ are geometrically split (in the sense that they contain a geometric component of multiplicity 1). Furthermore, as explained in [SSD05, §5], the projection

$\mathscr{Y} \longrightarrow \widetilde{Y}_\alpha/\iota_{Y_\alpha} = X_\alpha$ extends to a map $\pi : \mathscr{X} \longrightarrow X_\alpha$ which is birational over X_α to the projection $X_\alpha \times_k \mathbb{P}^1 \longrightarrow X_\alpha$. It then follows that the pullback map $\pi^* : \mathrm{Br}(X_\alpha) \longrightarrow \mathrm{Br}(\mathscr{X})$ is an isomorphism.

By Proposition 3.15 we may find a finite subgroup $\mathcal{C} \subseteq H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ such that $(h_\alpha)_*(\mathcal{C}) = \mathcal{B}$. Since $X_\alpha(\mathbb{A}_k)^{\mathcal{C}(X_\alpha)} \neq \varnothing$, Harari's "formal lemma" implies the existence of an adelic point $(x_v) \in X_\alpha(\mathbb{A}_k)$ which lies in W_α and is orthogonal both to $\mathcal{C}(X_\alpha)$ and to $C_\alpha(\theta)$ for every $\theta \in \mathcal{C}$. For every $v \in S$ let us fix a quadratic extension $F_v = k_v(\sqrt{t_v})/k_v$ such that x_v lifts to a local point $y_v \in \widetilde{Y}_\alpha^{F_v}(k_v)$. In the presence of a 2-structure M satisfying the conditions of the proposition we may rely on Lemma 3.16 to insure that F_w/k_w is unramified for every $w \in M$. The collection (t_v, y_v) now determines an adelic point $(x'_v) \in \mathscr{X}(\mathbb{A}_k)$ which maps to $(x_v) \in X_\alpha(\mathbb{A}_k)$. Since the pullback map $\pi^* : \mathrm{Br}(X_\alpha) \longrightarrow \mathrm{Br}(\mathscr{X})$ is an isomorphism we may deduce that (x'_v) is orthogonal to the pullbacks of the classes in $\mathcal{C}(X_\alpha)$ and the classes $C_\alpha(\theta)$ for $\theta \in \mathcal{C}$. We note that the classes corresponding to $\mathcal{C}(X_\alpha)$ contain, in particular, all the vertical classes with respect to the fibration $\mathscr{X} \longrightarrow \mathbb{P}^1$ (these are the classes of $\mathcal{C}(X_\alpha)$ whose corresponding elements in $H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ are in the kernel of $(h_\alpha)_*$). Let us now choose a place $v_{\mathrm{ad}} \notin S$ such that α maps to 0 in $H^1(k_{v_{\mathrm{ad}}}, A[2])$. Let $t_{v_{\mathrm{ad}}} \in \mathcal{O}_v$ be a uniformizer and $F_{v_{\mathrm{ad}}} = k_{v_{\mathrm{ad}}}(\sqrt{t_{\mathrm{ad}}})$. Then $\widetilde{Y}_\alpha^{F_{v_{\mathrm{ad}}}} \cong \widetilde{A}^{F_{v_{\mathrm{ad}}}}$ and so we may choose a point $x_{v_{\mathrm{ad}}} \in X_\alpha(k_{v_{\mathrm{ad}}})$ which lifts to a point $y_{v_{\mathrm{ad}}} \in \widetilde{Y}_\alpha^{F_{v_{\mathrm{ad}}}}(k_v)$.

By [HW15, Theorem 9.17] there now exists a $t \in k^* \subseteq \mathbb{P}^1(k)$ and an adelic point $(x'_v) \in \mathscr{Y}_t(\mathbb{A}_k) = \widetilde{Y}_\alpha^{k(\sqrt{t})}(\mathbb{A}_k)$ with the following properties:

(1) t is arbitrarily close to t_v for every $v \in S \cup \{v_{\mathrm{ad}}\}$.
(2) x'_v is arbitrarily close to x_v for every $v \in S \cup \{v_{\mathrm{ad}}\}$.
(3) (x'_v) is orthogonal to $\pi^* C_\alpha(\theta)|_{\widetilde{Y}_\alpha^{k(\sqrt{t})}} = B_\alpha^{k(\sqrt{t})}((h_\alpha)_*(\theta)) \in \mathrm{Br}(\widetilde{Y}_\alpha^{k(\sqrt{t})})$ for $\theta \in \mathcal{C}$.

The quadratic extension $F = k(\sqrt{t})$ now has all the required properties (where the admissibility of (A^F, α) follows from Lemma 4.2 applied with respect to the place v_{ad}). □

Let us now specialize to the case where A carries a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$. We will furthermore **fix the assumption** that A admits a 2-structure M such that α is unramified over M but has a non-trivial image in $H^1(k_w, A[2])$ for $w \in M$.

Remark 4.5. As explained in §3.4, the obstruction $c_\lambda \in H^1(k, A[2])$ to realizing λ as induced by a symmetric line bundle on A vanishes when the Galois action on $A[2]$ is trivial (since we can clearly find a Galois invariant quadratic enhancement to the Weil pairing in that case). We may hence assume without loss of generality that λ is induced by a symmetric line bundle.

We would like to describe a particular finite subgroup $\mathcal{B} \subseteq H^1(k, A[2]) \cong H^1(k, \hat{A}[2])$ to which we will apply Proposition 4.4. Let $B_0 \subseteq A[2] \otimes A[2]$ denote the kernel of the Weil pairing map $A[2] \otimes A[2] \longrightarrow \mu_2$. The bilinear map $(P, Q) \mapsto \langle \delta(P), Q \rangle_\lambda$ (see §3.1) then induces a homomorphism $T : B_0 \longrightarrow H^1(k, \mu_2)$. We will denote by L_λ the minimal field extension such that $T(\beta)$ vanishes when restricted to L_λ for every $\beta \in B_0$. We will further denote by $L_{\lambda,\alpha} = L_\lambda k_\alpha$ the compositum of L_λ with the splitting field k_α of α (see Construction 3.14). Finally, we will denote by $L_{M,\alpha} \subseteq L_{\lambda,\alpha}$ the maximal subextension of $L_{\lambda,\alpha}$ which is unramified over M.

Remark 4.6. The field $L_{M,\alpha}$ is invariant under replacing A by a quadratic twist A^F.

We are now ready to describe the finite subgroup $\mathcal{B} \subseteq H^1(k, A[2])$ we wish to apply Proposition 4.4 to. For this it will be convenient to employ the following terminology: given a field extension K/k, we will say that an element $\beta \in H^1(k, A[2])$ is **K-restricted** if $\beta|_K = 0 \in H^1(K, A[2])$. We will denote by $\mathrm{Sel}_2^K(A) \subseteq \mathrm{Sel}_2(A)$ the subgroup consisting of K-restricted elements.

Definition 4.7. We will denote by $\mathcal{B}_\alpha \subseteq H^1(k, A[2])$ the finite subgroup consisting of those elements $\beta \in H^1(k, A[2])$ which are both $L_{M,\alpha}$-restricted and satisfy $\alpha \cup_\lambda \beta = 1 \in H^2(k, \mu_2)$.

The following proposition summarizes the main outcome of this section.

Proposition 4.8. *If $X_\alpha(\mathbb{A}_k)^{\mathcal{C}(X_\alpha)} \neq \varnothing$ then there exists a quadratic extension F/k such that (A^F, α) is admissible, α belongs to $\mathrm{Sel}_2(A^F)$, and α is orthogonal to $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ with respect to the Cassels-Tate pairing. Furthermore, if α is unramified over M but the image of α in $H^1(k_w, A[2])$ is non-zero for every $w \in M$ then we may choose F to be unramified over M.*

Proof. Apply Proposition 4.4 with the subgroup $\mathcal{B}_\alpha \subseteq H^1(k, A[2])$ of Definition 4.7, and use the fact that any element $\beta \in \mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ satisfies $\alpha \cup_\lambda \beta = 1 \in H^2(k, \mu_2)$ by local duality. □

Remark 4.9. The group $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)/\mathrm{Br}(k)$ belongs in fact to $\mathrm{Br}_1(X_\alpha)/\mathrm{Br}(k)$, where $\mathrm{Br}_1(X_\alpha)$ is the kernel of the map $\mathrm{Br}(X_\alpha) \longrightarrow \mathrm{Br}(\overline{X}_\alpha)$. Furthermore, since $\mathcal{C}(X_\alpha)$ is a finite 2-torsion group we can find a finite subgroup $\mathcal{C}' \subseteq \mathrm{Br}_1(X)\{2\}$ in the 2-primary part of $\mathrm{Br}_1(X)$ that maps surjectively onto $\mathcal{C}(X_\alpha)$. We hence see that in Proposition 4.8 we only need to assume the triviality of the 2-primary algebraic Brauer-Manin obstruction.

4.2. **First descent.** In this section we resume all the notation of §4.1, and we keep the assumption that the Galois action on $A[2]$ is trivial, that A carries a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$ (automatically induced by a symmetric line bundle, see Remark 4.5), and that the Kummer surface $X_\alpha = \mathrm{Kum}(Y_\alpha)$ contains an adelic point which is orthogonal to the subgroup $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)/\mathrm{Br}(k)$ of Definition 4.3. We will also, as above, assume that A admits a 2-structure M such that α is unramified over M but has a non-trivial image in $H^1(k_w, A[2])$ for each $w \in M$. In light of Proposition 4.8 we may, by possibly replacing A by a quadratic twist, assume that the following two conditions hold as well:

(A1) (A, α) is admissible.

(A2) α belongs to $\mathrm{Sel}_2(A)$ and is orthogonal to $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$ with respect to the Cassels-Tate pairing.

Our goal in this subsection is to find a quadratic extension F/k such that Conditions (A1) and (A2) still hold for A^F and such that in addition $\mathrm{Sel}_2(A^F)$ is generated by $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ and the image of $A[2]$. We will do so by showing that if this is not the case then there is always a quadratic twist making the Selmer rank smaller.

Proposition 4.10. *Let A an abelian variety as above with a 2-structure M and let $\alpha \in \mathrm{Sel}_2(A)$ be an element which is unramified over M and orthogonal to $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$*

with respect to the Cassels-Tate pairing. Assume that Conditions (A1) and (A2) hold for (A, α). If $\mathrm{Sel}_2(A)$ is not generated by $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$ and $\delta(A[2])$ then there exists a field extension $F = k(\sqrt{a})$ with a a unit over M and such that:

(1) Conditions (A1) and (A2) hold for (A^F, α).
(2) $\dim_2 \mathrm{Sel}_2(A^F) < \dim_2 \mathrm{Sel}_2(A)$.

Proof. Let S be a finite set of places containing all the archimedean places, all the places above 2 and all the places of bad reduction for A or X_α, and such that $S \smallsetminus M$ contains a set of generators for the class group of k. Since the Selmer condition subgroups $W_v \subseteq H^1(k_v, A[2])$ are isotropic with respect to $\cup_v$ it follows that for every $\beta \in \mathrm{Sel}_2(A)$ we have $\alpha \cup_\lambda \beta = 1 \in H^2(k, \mu_2)$. By Proposition 3.15 we may choose a finite subgroup $\mathcal{C}_\alpha \subseteq H^1(k, \mathrm{Aff}(\overline{Z}_\alpha, \mu_2))$ such that $(h_\alpha)_*$ maps $\mathcal{C}_\alpha$ surjectively onto $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$, and such that for every $\theta \in \mathcal{C}_\alpha$ the splitting field k_θ is unramified outside $S \smallsetminus M$. Furthermore, by possibly enlarging S we may assume that we have an $\mathcal{O}_S$-smooth S-integral model $\mathcal{W}_\alpha$ for W_α and such that for every $\theta \in \mathcal{C}_\alpha$ the element $C_\alpha(\theta) \in \mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ can be represented by a Brauer element on W_α which extends to $\mathcal{W}_\alpha$.

Our method for constructing the desired element $a \in k^*$ consists of two parts. In the first part we find two places $v_0, v_1 \notin S$ whose associated Frobenius elements in Γ_k satisfy suitable constraints. These constraints imply in particular that there exists an element $a \in k^*$ such that $\mathrm{div}(a) = v_0 + v_1$. In the second part of the proof we show that the quadratic extension $F = k(\sqrt{a})$ has the desired properties.

By Remark 3.26 every element of $\mathrm{Sel}_2(A)$ can be written uniquely as a sum of an element unramified over M and an element in the image of $A[2]$. In particular, the Selmer group $\mathrm{Sel}_2(A)$ is generated by $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$ and $\delta(A[2])$ if and only if $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$ contains all elements which are unramified over M. Let us hence assume that there exists a $\beta \in \mathrm{Sel}_2(A)$ which is unramified over M and does not belong to $\mathrm{Sel}_2^{L_{M,\alpha}}(A)$.

Let $V = A[2] \oplus A[2] \oplus (A[2] \otimes A[2])$ and consider the homomorphism

$$\Phi : V \longrightarrow H^1(k, \mu_2)$$

given by the formula $\Phi(P_0, P_1, \sum_i P_i \otimes Q_i) = \langle \alpha, P_0 \rangle_\lambda \cdot \langle \beta, P_1 \rangle_\lambda \cdot \prod_i \langle \delta(P_i), Q_i \rangle_\lambda$. Let $R \subseteq V$ be the kernel of Φ and let k_ϕ/k be the minimal Galois extension such that all the elements in the image of Φ vanish when restricted to k_ϕ. Then k_ϕ/k is a 2-elementary extension and we have a natural isomorphism $\mathrm{Gal}(k_\phi/k) \cong \mathrm{Hom}(V/R, \mu_2)$.

Let $B_0 \subseteq A[2] \otimes A[2]$ be the kernel of the Weil pairing $A[2] \otimes A[2] \longrightarrow \mu_2$ and let $b \in A[2] \otimes A[2]$ be an element which is not in B_0, so that $A[2] \otimes A[2]$ is generated over B_0 by b. Let $V_\alpha \subseteq V$ be the image of the left most $A[2]$ factor. The admissibility of (A, α) is then equivalent to the following inclusion of subgroups of V:

$$R \cap (V_\alpha + A[2] \otimes A[2]) \subseteq V_\alpha + B_0,$$

which in turn is equivalent to the statement

$$b \notin R + V_\alpha + B_0.$$

On the other hand, the fact that β is not $L_{M,\alpha}$-restricted means that there exists a $w_\beta \in M$ such that $\Phi(0, P_{w_\beta}, 0)$ does not belong to the subgroup of $H^1(k, \mu_2)$

spanned by $\Phi(V_\alpha)$ and $\Phi(0,0,B_0)$, a statement that is equivalent to

$$P_{w_\beta} \notin R + V_\alpha + B_0.$$

We may hence conclude that there exists a homomorphism $h : V \longrightarrow \mu_2$ which vanishes on $R + V_\alpha + B_0$ but does not vanish on P_{w_β} and does not vanish on b. Now since h vanishes on R it determines a well-defined homomorphism $h' : V/R \longrightarrow \mu_2$ which we may consider as an element of $\mathrm{Gal}(k_\phi/k)$. By Chabotarev's theorem we may choose a place $v_0 \notin S$ such that $\mathrm{Frob}_{v_0}(k_\phi) = h'$. By construction we now have that $\langle \alpha, P\rangle_\lambda$ is a square in k_{v_0} for every $P \in A[2]$, that $\left\langle \beta, P_{w_\beta}\right\rangle_\lambda$ is not a square in k_{v_0}, and that $\langle \delta(P), Q\rangle_\lambda$ is a square in k_{v_0} if and only if $\langle P, Q\rangle_\lambda = 1$. We shall now proceed to choose v_1.

Let is fix a finite large Galois extension L/k which is unramified outside $S \smallsetminus M$ and which contains $L_{M,\alpha}$ and all the splitting fields k_θ above. Let $\mathfrak{m}$ be the modulus which is a product of 8 and all the places in S except w_β, let $k_{\mathfrak{m}}$ be the ray class field of $\mathfrak{m}$, and let us set $L' = k_{\mathfrak{m}} L$. Since $S \smallsetminus M$ contains a set of generators for the class group we may find a quadratic extension K_{w_β}/k which is purely ramified at w_β and is unramified outside S. Since L' is unramified at w_β while K_{w_β} is purely ramified at w_β it follows that K_{w_β} is linearly disjoint from L'. We may hence deduce the existence of a place $v_1 \notin S \cup \{v_0\}$ such that

(1) $\mathrm{Frob}_{v_1}(L') = \mathrm{Frob}_{v_0}(L')^{-1}$.
(2) $\mathrm{Frob}_{v_0}(K_{w_\beta}) \cdot \mathrm{Frob}_{v_1}(K_{w_\beta})$ is the non-trivial element of $\mathrm{Gal}(K_{w_\beta}/k) \cong \mathbb{Z}/2$.

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 an $a \in k^*$ which is equal to 1 mod $\mathfrak{m}$ and such that $\mathrm{div}(a) = v_0 + v_1$. In particular, we see that a is a square at each $v \in S \setminus \{w_\beta\}$. By Artin reciprocity for the quadratic extension K_{w_b}/k together with Property (2) above we get that a is **not** a square at w_β. We now claim that $F = k(\sqrt{a})$ will give the desired quadratic twist.

Let $T = \{w_\beta, v_0, v_1\}$. Then $W_v^F = W_v$ for every $v \notin T$. By Lemmas 3.24 and 3.25 we see that $\dim_2(\overline{W}_{w_\beta}) = 1$ and $\dim_2(\overline{W}_{v_0}) = \dim_2(\overline{W}_{v_1}) = 2g$. Using Lemma 3.27 we may conclude that

$$\dim_2 \mathrm{Sel}_2\left(A^F\right) - \dim_2 \mathrm{Sel}_2\left(A\right) = \dim_2 V_T^F - \dim_2 V_T$$

with

$$\dim_2 V_T^F + \dim_2 V_T \le \dim_2 \overline{W}_{v_0} + \dim_2 \overline{W}_{v_1} + \dim_2 \overline{W}_{w_\beta} = 4g+1.$$

To show that the 2-rank of the Selmer group decreased we hence need to show that $\dim_2 V_T \ge 2g+1$.

Since $\langle \delta(P_{w_0}), P_{w_1}\rangle_\lambda$ is a square in k_{v_0} if and only if $\langle P_{w_0}, P_{w_1}\rangle_\lambda = 1$ we deduce that the local images of $\{\delta(P_w)\}_{w\in M}$ at v_0 are linearly independent and hence span a 2^{2g}-dimensional subspace of $W_{v_0} = \overline{W}_{v_0}$, which is consequently all of W_{v_0}. It will hence suffice to show that the image of β in V_T is not contained in the subgroup generated by the local images of $\{\delta(P_w)\}_{w\in M}$. Let $Q' \in A[2]$ be such that the local image of $\delta(Q')$ and β at v_0 coincides. By construction $\left\langle \beta, P_{w_\beta}\right\rangle_\lambda$ is not a square in k_{v_0} and so $\left\langle \delta(Q'), P_{w_\beta}\right\rangle_\lambda$ is not a square at v_0. This means that $\left\langle Q', P_{w_\beta}\right\rangle_\lambda = -1$ and so by Corollary 3.8 we know that $\left\langle \delta(Q'), Q_{w_\beta}\right\rangle_\lambda$ is ramified at w_β. Since $\left\langle \beta, Q_{w_\beta}\right\rangle_\lambda$ is unramified at w_β it follows that $\delta(Q')$ and β have different local images at w_β. We hence deduce that the image of β in V_T cannot be spanned by images of $\{\delta(P_w)\}_{w\in M}$ and so $\dim(V_T)\geq 2g+1$. This implies that

$$\dim_2 \mathrm{Sel}_2(A^F) < \dim_2 \mathrm{Sel}_2(A).$$

We now claim that $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F) = \mathrm{Sel}_2^{L_{M,\alpha}}(A)$. Let $\beta' \in H^1(k, A[2])$ be an $L_{M,\alpha}$-restricted element. Then β' is unramified over M and in particular at w_β. By Lemma 3.25 this means that β' satisfies the Selmer condition of A at w_β if and only if β' satisfies the Selmer condition of A^F at w_β. By our choice of v_0 and v_1 we see that $L_{M,\alpha}$ splits completely at v_0 and v_1 and so the local images of β' are trivial at v_0 and v_1. This implies that for $L_{M,\alpha}$-restricted elements the local Selmer conditions for A and A^F are identical at every place and so $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F) = \mathrm{Sel}_2^{L_{M,\alpha}}(A)$.

Finally, applying Proposition 3.29 to α and any $L_{M,\alpha}$-restricted element β', and using the fact that $\mathrm{Frob}_{v_1}(k_\theta) = \mathrm{Frob}_{v_0}(k_\theta)^{-1}$ we may now conclude that α belongs to $\mathrm{Sel}_2(A^F)$ and is furthermore orthogonal to $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ with respect to the Cassels-Tate pairing associated to A^F. By Lemma 4.2 (A^F,α) is admissible and so Conditions (A1) and (A2) hold for (A^F,α), as desired.

□

4.3. **Second descent.** In this section we resume all the notation of §4.1 and §4.2, and we keep the assumption that the Galois action on $A[2]$ is trivial, that A carries a principal polarization $\lambda : A \xrightarrow{\cong} \hat{A}$, and that the Kummer surface $X_\alpha = \mathrm{Kum}(Y_\alpha)$ contains an adelic point which is orthogonal to the subgroup $\mathcal{C}(X_\alpha) \subseteq \mathrm{Br}(X_\alpha)/\mathrm{Br}(k)$ of Definition 4.3. Until now we have only used the fact that A admits a 2-structure $M \subseteq \Omega_k$. For the purpose of the second descent phase we will need to utilize the stronger assumption that appears in Theorem 2.8, namely, that A can be written as a product $A = \prod_i A_i$ such that each A_i has an **extended** 2-structure $M_i \subseteq \Omega_k$, and such that A_j has good reduction over M_i for $j \neq i$. Applying Proposition 4.10 repeatedly using $M = \cup_i M_i$ we may find a quadratic extension F/k, unramified over M, and such that

(B1) Each (A^F,α) is admissible.

(B2) α belongs to $\mathrm{Sel}_2(A^F)$ and is orthogonal to $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ with respect to the Cassels-Tate pairing.

(B3) $\mathrm{Sel}_2(A^F)$ is generated by $\mathrm{Sel}_2^{L_{M,\alpha}}(A^F)$ and $\delta(A^F[2])$.

Let $\mathrm{Sel}_2^\circ(A) \subseteq \mathrm{Sel}_2(A)$ denote the subgroup consisting of those elements which are orthogonal to every element in $\mathrm{Sel}_2(A)$ with respect to the Cassels-Tate pairing. We note that Conditions (B1) (B2) and (B3) imply in particular

(B4) α belongs to $\mathrm{Sel}_2^\circ(A)$.

Replacing A with A^F and using the canonical isomorphism $\mathrm{Kum}(Y_\alpha) \cong \mathrm{Kum}(Y_\alpha^F)$ we may assume without loss of generality that Conditions (B1) and (B4) already hold for A. We now observe that we have a natural direct sum decomposition $\mathrm{Sel}_2(A) \cong \oplus_i \mathrm{Sel}_2(A_i)$ and so we can write $\alpha = \alpha_1 + \ldots + \alpha_n$ with $\alpha_i \in \mathrm{Sel}_2(A_i) \subseteq \mathrm{Sel}_2(A)$. Condition (B4) now implies that $\alpha_i \in \mathrm{Sel}_2^\circ(A)$ for every $i = 1,\ldots,n$. Our goal in this subsection is to show that under these conditions one can find a quadratic extension F/k such that $\mathrm{Sel}_2^\circ(A_i^F)$ is generated by α_i and the image of $A_i[2]$. Equivalently, we will show that $\mathrm{Sel}^\circ(A^F)$ is generated by $\alpha_1,\ldots,\alpha_n$ and the image of $A[2]$.

We begin with the following proposition, whose goal is to produce quadratic twists which induce a prescribed change to the Cassels-Tate pairing in suitable circumstances. We note that while the Weil pairing takes values in μ_2 (which we write multiplicatively), the Cassels-Tate pairing takes values in $\mathbb{Z}/2$ (which we write additively). For the purpose of the arguments in this section, it will be convenient to use the fact that the Galois modules μ_2 and $\mathbb{Z}/2$ are isomorphic. Although this isomorphism is unique, it does involves a change between additive and multiplicative notation, and so it seems appropriate to take it into account explicitly. We will hence use the notation

$$(-1)^{(-)} : \mathbb{Z}/2 \longrightarrow \mu_2$$

for the isomorphism in one direction and the notation

$$\log_{(-1)}(-) : \mu_2 \longrightarrow \mathbb{Z}/2$$

for the isomorphism in the other direction. Given a subgroup $B \subseteq H^1(k, A[2])$ and an element $\sigma \in \Gamma_k$, we will denote by $\rho_\sigma : B \longrightarrow A[2]$ the homomorphism sending β to $\beta(\sigma) \in A[2]$, where by abuse of notation we simply identify β with the corresponding homomorphism

$$\beta : \Gamma_k \longrightarrow A[2].$$

Given $\sigma, \tau \in \Gamma_k$ we will denote by $\rho_\sigma \wedge \rho_\tau : B \times B \longrightarrow \mathbb{Z}/2$ the antisymmetric form

$$(\rho_\sigma \wedge \rho_\tau)(\beta, \beta') = \log_{(-1)} \langle \rho_\sigma(\beta), \rho_\tau(\beta') \rangle_\lambda + \log_{(-1)} \langle \rho_\sigma(\beta'), \rho_\tau(\beta) \rangle_\lambda .$$

Proposition 4.11. *Let $B \subseteq \mathrm{Sel}_2(A)$ be a subgroup containing only elements which are unramified over M. For any two elements $\sigma, \tau \in \Gamma_k$ there exists a field extension $F = k(\sqrt{a})$, unramified over M, and such that*

(1) $\mathrm{Sel}_2(A^F)$ contains B and $\dim_2 \mathrm{Sel}_2(A^F) = \dim_2 \mathrm{Sel}_2(A)$.
(2) For every $\beta, \beta' \in B$ we have $\langle \beta, \beta' \rangle^{\mathrm{CT}}_{A^F} = \langle \beta, \beta' \rangle^{\mathrm{CT}}_A + (\rho_\sigma \wedge \rho_\tau)(\beta, \beta')$.

Proof. Let S be a finite set of places which contains all the archimedean places, all the places above 2, all the places of bad reduction for A or X_α, and such that $S \smallsetminus M$ contains a set of generators for the class group. In particular, every $\beta \in B$ is unramified outside $S \smallsetminus M$. Now for any two $\beta, \beta' \in B \subseteq \mathrm{Sel}_2(A)$ we have $\beta \cup_\lambda \beta' = 1 \in H^2(k, \mu_2)$, and so by Proposition 3.15 we may choose an element $\theta \in H^1(k, \mathrm{Aff}(\overline{Z}_\beta, \mu_2))$ such that $(h_\beta)_*(\theta) = \beta'$ and such that the splitting field $k_\theta / k_{\beta,\beta'}$ is unramified outside $S \smallsetminus M$. By possibly enlarging S we may assume that we have an $\mathcal{O}_S$-smooth S-integral model $\mathcal{W}_\alpha$ for W_α and that for every θ as above the element $C_\beta(\theta) \in \mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ can be represented by a Brauer element on W_α which extends to $\mathcal{W}_\alpha$. We may consequently fix a finite large Galois extension L/k which is unramified outside $S \smallsetminus M$ and which contains all the splitting fields k_θ.

For each $w, w' \in M$ let $K_{w,w'}$ be the quadratic extension classified by the element $\langle \delta(Q_w), Q_{w'} \rangle \in H^1(k, \mu_2)$. By Corollary 3.8 we have that $K_{w,w}$ is ramified at w while $K_{w,w'}$ is unramified over M for $w \neq w'$. Since L is unramified over M it follows that the compositum of the $K_{w,w}$'s is linearly independent from the compositum of L's with the $K_{w,w'}$'s for $w \neq w'$. Let m be the modulus which is a product of 8 and all the places in S, and let k_m be the ray class field of m. We note that k_m contains all the $K_{w,w'}$ for $w, w' \in M$. Let $\varepsilon = \sigma\tau\sigma^{-1}\tau^{-1} \in \Gamma_k$ be the commutator of σ and τ and let $\varepsilon_L \in \mathrm{Gal}(L/k)$ be its corresponding image.

Since the image of ε is trivial in any the Galois group of any abelian extension of k it follows from Chabotarev's density theorem that there exists places $v_0, v_1 \in \Omega_k$ such that

(1) $\mathrm{Frob}_{v_0}(L) = \varepsilon_L$.
(2) $\mathrm{Frob}_{v_1}(L) = 1$.
(3) v_0 is inert $K_{w,w}$ for every $w \in M$ and splits in $K_{w,w'}$ for every $w \neq w'$.
(4) $\mathrm{Frob}_{v_1}(k_m) = \mathrm{Frob}_{v_0}(k_m)^{-1}$.

It follows from (4) that the divisor v_0+v_1 pairs trivially with the kernel of $H^1(k,\mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(k_m,\mathbb{Q}/\mathbb{Z})$ and so there exists an $a \in k^*$ which reduces to 1 mod m and such that $\mathrm{div}(a) = v_0 + v_1$. In particular, a is a square at each $v \in S$. We now claim that $F = k(\sqrt{a})$ will give the desired quadratic twist.

We begin by Claim (1) above. Since a is a square at each $v \in S$ it follows the Selmer condition for A and A^F is the same for every $v \in S$. Since the image of ε is trivial in any the Galois group of any abelian extension of k we have by construction that v_0 and v_1 split in k_β for every $\beta \in B$. It then follows that for $v \in \{v_0, v_1\}$ we have $\mathrm{loc}_v\,\beta = 0 \in H^1(k_v, A[2])$ for every $\beta \in B$. In particular, every $\beta \in B$ satisfies the Selmer condition of A^F for every $v \in S \cup \{v_0, v_1\}$ and is unramified outside $S \cup \{v_0, v_1\}$, implying that $B \subseteq \mathrm{Sel}_2(A^F)$.

To see that $\dim_2 \mathrm{Sel}_2(A^F) = \dim_2 \mathrm{Sel}_2(A)$ we use Lemma 3.27 with $T = \{v_0, v_1\}$. Indeed, $W^F_v = W_v$ for every $v \notin T$ and by Lemma 3.24 we see that $\dim_2(\overline{W}_{v_0}) = \dim_2(\overline{W}_{v_1}) = 2g$. We then have by Lemma 3.27 that

$$\dim_2 \mathrm{Sel}_2\left(A^F\right) - \dim_2 \mathrm{Sel}_2\left(A\right) = \dim_2 V^F_T - \dim_2 V_T$$

with

$$\dim_2 V^F_T + \dim_2 V_T \leq 4g.$$

Now since $\langle \delta(P), Q\rangle_\lambda$ is unramified outside S (and in particular at v_0, v_1) for every $P, Q \in A[2]$, Lemma 3.5 implies that $\langle \delta_F(P), Q\rangle_\lambda$ is ramified at v_0 if and only if $\langle P, Q\rangle_\lambda = -1$. The non-degeneracy of the Weil pairing now implies that the image of $\delta(A[2])$ in V^F_T spans a $2g$-dimensional subspace. On the other hand, by Property (3) above $\langle \delta(Q_w), Q_{w'}\rangle_\lambda$ is a square at v_0 if and only if $w = w'$, and so the image of $\delta(A[2])$ in V_T is $2g$-dimensional as well. It then follows that $\dim_2 V_T = \dim_2 V^F_T = 2g$ and so $\dim_2 \mathrm{Sel}_2\left(A^F\right) = \dim_2 \mathrm{Sel}_2\left(A\right)$.

We now prove Claim (2). Fix $\beta, \beta' \in B$ and let $\theta \in H^1(k, \mathrm{Aff}(\overline{Z}_\beta, \mu_2))$ be the element chosen above such that $(h_\beta)_*(\theta) = \beta'$. Let $\varepsilon_\theta \in \mathrm{Gal}(k_\theta/k)$ be the image of $\varepsilon_L \in \mathrm{Gal}(L/k)$. By Proposition 3.29 we have

$$\langle \beta, \beta'\rangle^{\mathrm{CT}}_{A^F} - \langle \beta, \beta'\rangle^{\mathrm{CT}}_{A} = \mathrm{Frob}_{v_0}(k_\theta/k_{\beta,\beta'}) \cdot \mathrm{Frob}_{v_1}(k_\theta/k_{\beta,\beta'}) = \varepsilon_\theta \in \mathrm{Gal}(k_\theta/k_{\beta,\beta'}) \subseteq \mathbb{Z}/2.$$

Recall from §3.3 the commutative diagram (12) for the class β, which is given by

(29)
$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(k_\theta/k_\beta) \arrow[r] \arrow[d, hook, "\overline{\theta}|_{k_\beta}"] & \mathrm{Gal}(k_\theta/k) \arrow[r] \arrow[d, hook, "\overline{\theta}"] & \mathrm{Gal}(k_\beta/k) \arrow[r] \arrow[d, hook, "\overline{\beta}"] & 1 \\
1 \arrow[r] & \mathrm{Aff}(\overline{Z}_\beta, \mu_2) \arrow[r] & \mathrm{Aff}(\overline{Z}_\beta, \mu_2) \rtimes A[2] \arrow[r] & A[2] \arrow[r] & 1
\end{tikzcd}$$

with exact rows and injective vertical maps. Let us write $\overline{\theta}(\sigma) = (x, \overline{\beta}(\sigma)) \in \mathrm{Aff}(\overline{Z}_\beta, \mu_2) \rtimes A[2]$ and $\overline{\theta}(\tau) = (y, \overline{\beta}(\tau)) \in \mathrm{Aff}(\overline{Z}_\beta, \mu_2) \rtimes A[2]$ for suitable $x, y \in \mathrm{Aff}(\overline{Z}_\beta, \mu_2)$. We may then compute that

$$[\overline{\theta}(\sigma), \overline{\theta}(\tau)] = (xy^{\overline{\beta}(\sigma)} x^{\overline{\beta}(\tau)} y, 0).$$

Now $x \in \mathrm{Aff}(\overline{Z}_\beta,\mu_2)$ is an affine-linear map whose homogeneous part is $\overline{\beta'}(\sigma) \in A[2]$ and so $x{\cdot}x^{\overline{\beta}(\tau)}$ is the constant affine-linear map with value $\left\langle \overline{\beta'}(\sigma), \overline{\beta}(\tau)\right\rangle_\lambda$. Similarly, $y \cdot y^{\overline{\beta}(\sigma)}$ is the constant affine-linear map with value $\left\langle \overline{\beta'}(\tau), \overline{\beta}(\sigma)\right\rangle_\lambda$. It then follows that the image $\varepsilon_\theta \in \mathrm{Gal}(k_\theta/k)$ of ε is trivial if and only if $(\rho_\sigma \wedge \rho_\tau)(\beta,\beta') = 0$, and so the desired result follows. □

We are now ready to prove the main result of this section, showing that if $\mathrm{Sel}^\circ_2(A)$ is not generated by $\alpha_1,...,\alpha_n$ and the image of $A[2]$ then there exists a field extension $F = k(\sqrt{a})$ such that $\mathrm{Sel}^\circ_2(A^F)$ is strictly smaller then $\mathrm{Sel}^\circ_2(A)$.

Proposition 4.12. *Let $A_1,...,A_n$ be abelian varieties as above such that each A_i is equipped with an extended 2-structure M_i over which A_j has good reduction for $j \neq i$. Let $A = \prod_i A_i$ and let $\alpha \in \mathrm{Sel}_2(A)$ be a non-degenerate element (see Definition 2.7) which is unramified over $M = \cup_i M_i$ and write $\alpha = \sum_i \alpha_i$ with $\alpha_i \in \mathrm{Sel}_2(A_i)$. Assume that Conditions (B1) and (B4) are satisfied. If $\mathrm{Sel}^\circ_2(A)$ is not generated by $\alpha_1,...,\alpha_n$ and the image of $A[2]$ then there exists a field extension $F = k(\sqrt{a})$ with a is a unit over M and such that*

(1) Conditions (B1) and (B4) hold for (A^F,α).
(2) $\dim_2 \mathrm{Sel}^\circ_2(A^F) < \dim_2 \mathrm{Sel}^\circ_2(A)$.

Proof. Let $U \subseteq \mathrm{Sel}_2(A)$ denote the subgroup consisting of those elements which are unramified over M. By Remark 3.26 we have that $\mathrm{Sel}_2(A)$ decomposes as a direct sum $\mathrm{Sel}_2(2) = U \oplus \delta(A[2])$. Let S be a finite set of places which contains all the archimedean places, all the places above 2, all the places of bad reduction for A or X_α, as well as a set of generators for the class group. In particular, every $\beta \in U$ is unramified outside $S \smallsetminus M$. Now for any two $\beta,\beta' \in U$ we have $\beta \cup_\lambda \beta' = 1 \in H^2(k,\mu_2)$, and so by Proposition 3.15 we may choose an element $\theta \in H^1(k,\mathrm{Aff}(\overline{Z}_\beta,\mu_2))$ such that $(h_\beta)_*(\theta) = \beta'$ and such that the splitting field $k_\theta/k_{\beta,\beta'}$ is unramified outside $S \smallsetminus M$. By possibly enlarging S we may assume that we have an $\mathcal{O}_S$-smooth S-integral model $\mathcal{W}_\alpha$ for W_α and that for every θ as above the element $C_\beta(\theta) \in \mathrm{Br}(W_\alpha)/\mathrm{Br}(k)$ can be represented by a Brauer element on W_α which extends to $\mathcal{W}_\alpha$.

Our general strategy for proving Proposition 4.12 is the following. We first find a suitable $a \in k^*$ which is a unit over S and such that after a quadratic twist by $F = k(\sqrt{a})$ the dimension of the Selmer group $\mathrm{Sel}_2(A^F)$ **increases** by 1 and contains in particular a new element γ which certain favorable properties. We then use Proposition 4.11 in order to find a second quadratic twist which suitably modifies the Cassels-Tate pairing between γ and the elements from $\mathrm{Sel}_2(A)$. This last part is done in a way that effectively decreases the number of elements in the Selmer group which are in the kernel of the Cassels-Tate pairing.

Let $U^\circ = U \cap \mathrm{Sel}^\circ_2$. Since Sel°_2 contains $\delta(A[2])$ we obtain a direct sum decomposition $\mathrm{Sel}^\circ_2(A) = U^\circ \oplus \delta(A[2])$. Similarly, for every $i = 1,...,n$ we have a direct sum decomposition $\mathrm{Sel}_2(A_i) = U_i \oplus \delta(A_i[2])$ and $\mathrm{Sel}^\circ_2(A_i) = U^\circ_i \oplus \delta(A_i[2])$, where $U_i = U \cap \mathrm{Sel}_2(A_i)$ and $U^\circ_i = U^\circ \cap \mathrm{Sel}_2(A_i)$. Let $\beta \in U^\circ$ be an element which does not belong to the subgroup of U° spanned by $\alpha_1,...,\alpha_n$ and let us write $\beta = \sum_i \beta_i$ with $\beta_i \in \mathrm{Sel}_2(A_i)$. It then follows that $\beta_i \in U^\circ_i$. Since β is not spanned by the α_i's there exists an i such that $\beta_i \notin 0,\alpha_i$.

Let us now write $M_i = \{w_0,...,w_{2g_i}\}$ where $g_i = \dim A_i$. By the definition of an extended 2-structure we may choose, for every $j = 0,...,2g_i - 1$, a 2-torsion point

$Q_j \in A_i[2]$ such that the image of Q_j in $C_{w_{j'}}/2C_{w_{j'}}$ is non-trivial if and only if $|j' - j| \leq 1$. Similarly, let Q_{2g_i} be such that the image of Q_{2g_i} in $C_{w_{j'}}/2C_{w_{j'}}$ is non-trivial if and only if $j' \in \{2g_i, 0\}$. We note that by construction $\sum_{j=0}^{2g_i} Q_j = 0$.

We now claim that there exists a $j \in \{0, ..., 2g_i\}$ such that $\langle \beta_i, Q_j \rangle_\lambda$ is non-trivial and different from $\langle \alpha_i, Q_j \rangle_\lambda$. Indeed, assume otherwise and let $J \subseteq \{0, ..., 2g_i\}$ be the subset of those indices for which $\langle \beta_i, Q_j \rangle_\lambda = \langle \alpha_i, Q_j \rangle_\lambda$ (so that $\langle \beta_i, Q_j \rangle_\lambda = 0$ for $j \notin J$). Then

$$\prod_{j \in J} \langle \alpha_i, Q_j \rangle_\lambda = \prod_{j=0}^{2g_i} \langle \beta_i, Q_j \rangle_\lambda = \left\langle \beta_i, \sum_{j=0}^{2g_i} Q_i \right\rangle_\lambda = 1 \in H^1(k, \mu_2).$$

Since $\beta_i \neq 1, \alpha_i$ and the Q_j's span $A_i[2]$ we have that $\emptyset \subsetneq J \subsetneq \{0, ..., 2g_i\}$, and so we obtain a non-trivial relation between the elements $\langle \alpha_i, Q_j \rangle_\lambda$, contradicting our assumption that $\alpha \in H^1(k, A[2])$ is non-degenerate (Definition 2.7). We may hence conclude that $\langle \beta_i, Q_j \rangle \neq 1, \langle \alpha_i, Q_j \rangle$ for some $j = 0, ..., 2g_i$. To fix ideas let us assume that we have this for $j = 2g_i$. We shall now remove w_{2g_i} from M_i and work with the resulting 2-structure $M'_i = M_i \setminus \{w_{2g_i}\} = \{w_0, ..., w_{2g_i - 1}\}$. Let $\{P_w\}_{w \in M'}$ and $\{Q_w\}_{w \in M'_i}$ be the corresponding dual bases of $A_i[2]$. By comparing images in $\oplus_{w \in M'_i} C_w/2C_w$ we see that the 2-torsion point $Q_{w_0} \in A_i[2]$ coincides with the point Q_{2g_i} we had before. In particular, we have that $\langle \beta_i, Q_{w_0} \rangle \neq 0, \langle \alpha_i, Q_{w_0} \rangle$.

Let us now complete M'_i into a 2-structure for A by choosing, for every $i' \neq i$, a 2-structure $M'_{i'} \subseteq M_{i'}$, and setting $M' = M'_1 \cup ... \cup M'_n$. We now note that since $A_i[2]$ is orthogonal to $A_{i'}[2]$ with respect to the Weil pairing when $i \neq i'$ it follows that $\langle \beta, Q_{w_0} \rangle = \langle \beta_i, Q_{w_0} \rangle$ and $\langle \alpha, Q_{w_0} \rangle = \langle \alpha_i, Q_{w_0} \rangle$. We have thus found a point $Q_{w_0} \in M'$ such that $\langle \beta, Q_{w_0} \rangle \neq 1, \langle \alpha, Q_{w_0} \rangle$. We may now forget about the factorization of A into a product of the A_i's, and reconsider it as a single abelian variety.

For each $w, w' \in M'$ let $K_{w,w'}$ be the quadratic extension corresponding to the element $\langle \delta(Q_w), Q_{w'} \rangle \in H^1(k, \mu_2)$. By Corollary 3.8 we have that $K_{w,w}$ is ramified at w while $K_{w,w'}$ is unramified over M' when $w \neq w'$. Let us now fix a finite large Galois extension L/k which is unramified outside $S \setminus M'$ and which contains all the splitting fields $k_{\beta'}$ for $\beta' \in U$, all the splitting fields k_θ, and all the fields $K_{w,w'}$ for $w \neq w'$. Let m be the modulus which is a product of 8 and all the places in $S \setminus \{w_0\}$, and let k_m be the ray class field of m. We note that since L is unramified over M' it is linearly independent from the compositum of all the $K_{w,w}$'s. Similarly, the compositum $L' := k_m L$, which is unramified over w_0, is linearly independent of K_{w_0,w_0}. By Chabotarev's density theorem that there exists places $v_0, v_1 \in \Omega_k$ such that

(1) v_0 splits in L.
(2) v_0 is inert $K_{w,w}$ for every $w \in M'$.
(3) v_1 splits in K_{w_0,w_0}.
(4) $\mathrm{Frob}_{v_1}(L') = \mathrm{Frob}_{v_0}(L')^{-1}$.

It then follows that the divisor $v_0 + v_1$ pairs trivially with the kernel of $H^1(k, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(k_m, \mathbb{Q}/\mathbb{Z})$ and so there exists an $a \in k^*$ which reduces to 1 mod m and such that $\mathrm{div}(a) = v_0 + v_1$. In particular, a is a square at each $v \in S \setminus \{w_0\}$. Artin reciprocity for the field K_{w_0,w_0} and conditions (2) and (3) above imply that a is not a square at w_0. We note that conditions (1)+(4) imply that v_1 splits completely in $k_{\beta'}$ for every $\beta' \in U$, in all the k_θ's, and in $K_{w,w'}$ for $w \neq w'$. On the other hand, conditions (2)+(4) imply that v_1 is inert in $K_{w,w}$ for every $w \neq w_0$. Applying Proposition 3.29

we now get that $U \subseteq \mathrm{Sel}_2(A^F)$ and that the Cassels-Tate pairing between every two elements $\beta, \beta' \in U$ is the same in A^F and A.

Let $T = \{w_0, v_0, v_1\}$. We then have that $W_v^F = W_v$ for every $v \notin T$ and by Lemmas 3.24 and 3.25 we see that $\dim_2(\overline{W}_{v_0}) = \dim_2(\overline{W}_{v_1}) = 2g$ and $\dim_2(\overline{W}_{w_0}) = 1$. By Lemma 3.27 we have that

$$\dim_2 \mathrm{Sel}_2\left(A^F\right) - \dim_2 \mathrm{Sel}_2\left(A\right) = \dim_2 V_T^F - \dim_2 V_T$$

with

$$\dim_2 V_T^F + \dim_2 V_T \leq \dim_2(\overline{W}_{v_0}) + \dim_2(\overline{W}_{v_1}) + \dim_2(\overline{W}_{w_0}) = 4g + 1$$

and $4g + 1 - \dim_2 V_T^F - \dim_2 V_T \geq 0$ is even. Arguing as in the proof of Proposition 4.11 we see that the image of $\delta(A[2])$ in V_T^F spans a $2g$-dimensional subspace by Lemma 3.5. By Properties (1)+(2) above we have that $\langle \delta(Q_w), Q_{w'} \rangle$ is a square at v_0 if and only if $w = w'$ and so by the non-degeneracy of the Weil pairing the image of $\delta(A[2])$ spans a $2g$-dimensional subspace of V_T as well. On the other hand for every $\beta' \in U$ we have $\mathrm{loc}_{v_0}(\beta') = \mathrm{loc}_{v_1}(\beta') = 0$ and $\mathrm{loc}_{w_0}(\beta') \in W_{w_0} \cap W_{w_0}^F$ by Lemma 3.25, and so the image of U in V_T is trivial. Since $\mathrm{Sel}_2(2) = U \oplus \delta(A[2])$ it follows that the dimension of V_T is exactly $2g$. The parity constraint of Lemma 3.27 now forces $\dim_2 V_T^F$ to be $2g+1$. Since we saw that $\mathrm{Sel}_2(A^F)$ contains U it now follows that $\mathrm{Sel}_2(A^F)$ is generated by U, $\delta_F(A[2])$ and one more element $\gamma \in \mathrm{Sel}_2(A^F)$. Furthermore, by adding to γ an element of $\delta(A^F[2])$ we may assume that γ is unramified over M'.

Lemma 4.13. *There exists an element $\sigma \in \Gamma_k$ such that $\gamma(\sigma) = Q_{w_0}$ and such that $\beta'(\sigma) = 0$ for every $\beta' \in U$.*

Proof. First observe that since γ is unramified over M we have that $\mathrm{loc}_{w_0}(\gamma) \in W_{w_0} \cap W_{w_0}^F$ and since the image of γ in V_T^F is orthogonal to V_T with respect to (28) we may conclude, in particular, that

$$\mathrm{inv}_{v_0}\left[\gamma \cup_\lambda \delta(P)\right] = \mathrm{inv}_{v_1}\left[\gamma \cup_\lambda \delta(P)\right]$$

for every $P \in A[2]$. Using the mutually dual bases Q_w and P_w we may write this equality as

$$\mathrm{inv}_{v_0} \sum_{w' \in M'} \left[\langle \gamma, P_{w'} \rangle_\lambda \cup \langle \delta(P), Q_{w'} \rangle_\lambda\right] = \mathrm{inv}_{v_1} \sum_{w' \in M'} \left[\langle \gamma, P_{w'} \rangle_\lambda \cup \langle \delta(P), Q_{w'} \rangle_\lambda\right].$$

Let us now plug in $P = Q_w$ for some $w \in M'$. By construction we have that $\langle \delta(Q_w), Q_{w'} \rangle_\lambda$ vanishes at both v_0 and v_1 whenever $w \neq w'$ and so we obtain

$$\mathrm{inv}_{v_0}\left[\langle \gamma, P_w \rangle_\lambda \cup \langle \delta(Q_w), Q_w \rangle_\lambda\right] = \mathrm{inv}_{v_1}\left[\langle \gamma, P_w \rangle_\lambda \cup \langle \delta(Q_w), Q_w \rangle_\lambda\right].$$

Now if $w \neq w_0$ then $\langle \delta(Q_w), Q_w \rangle_\lambda$ is unramified and non-trivial at both v_0 and v_1 and so for such w we obtain

$$\mathrm{val}_{v_0} \langle \gamma, P_w \rangle_\lambda = \mathrm{val}_{v_1} \langle \gamma, P_w \rangle_\lambda \mod 2 \tag{30}$$

while if $w = w_0$ then $\langle \delta(Q_w), Q_w \rangle_\lambda$ is unramified and non-trivial at v_0 but is trivial at v_1, and so we obtain

$$\mathrm{val}_{v_0} \langle \gamma, P_{w_0} \rangle_\lambda = 0 \mod 2$$

We now observe that $\mathrm{val}_{v_1} \langle \gamma, P_{w_0} \rangle_\lambda$ must be odd. Indeed, otherwise Equation (30) would hold for all $w \in M'$, and so there would exist a $Q \in A[2]$ such that $\gamma' = \gamma + \delta_F(Q)$ is unramified, and hence trivial, at both v_0 and v_1. It would then follow that γ' satisfies the Selmer condition of $\mathrm{Sel}_2(A)$ at all places except possibly w_0.

Since the image of γ' in V_T^F is orthogonal to the image of $\delta(Q_{w_0})$ in V_T to (28) we may conclude that γ' satisfies the Selmer condition of A at w_0 as well, i.e., $\gamma' \in U \subseteq \mathrm{Sel}_2(A) \cap \mathrm{Sel}_2(A^F)$. But this would imply that $\mathrm{Sel}_2(A^F)$ is generated by U and $\delta_F(A[2])$, contradicting the above. We may hence conclude that $\mathrm{val}_{v_1}\langle\gamma, P_{w_0}\rangle_\lambda$ is odd and so

$$\mathrm{val}_{v_0}\langle\gamma, P_w\rangle_\lambda + \mathrm{val}_{v_1}\langle\gamma, P_w\rangle_\lambda = \begin{cases} 0 \in \mathbb{Z}/2 & w \neq w_0 \\ 1 \in \mathbb{Z}/2 & w = w_0 \end{cases}.$$

It then follows that the class $\langle\gamma, P_{w_0}\rangle_\lambda \in H^1(k,\mu_2)$ does not split in the minimal field splitting $k_{\beta'}$ for all $\beta' \in U$ and splitting $\langle\gamma, P_w\rangle_\lambda$ for $w \neq w_0$. Consequently, there must exist an element $\sigma \in \Gamma_k$ such that $\beta'(\sigma) = 0 \in A[2]$ for every $\beta' \in U$ and $\langle\gamma(\sigma), P_w\rangle_\lambda = 1 \in \mu_2$ for every $w \neq w_0$, while $\langle\gamma(\sigma), P_{w_0}\rangle_\lambda$ is non-trivial. Then $\gamma(\sigma)$ must be equal to Q_{w_0}, as desired. □

Now recall that we have an element $\beta \in U$ such that $\langle\beta, Q_{w_0}\rangle_\lambda$ and $\langle\alpha, Q_{w_0}\rangle_\lambda$ are **two different non-trivial** classes in $H^1(k,\mu_2)$. It follows that for any two elements $\varepsilon_\alpha, \varepsilon_\beta \in \mu_2$ there exists an element $\tau \in \Gamma_k$ such that $\langle\alpha(\tau), Q_{w_0}\rangle_\lambda = \varepsilon_\alpha$ and $\langle\beta(\tau), Q_{w_0}\rangle_\lambda = \varepsilon_\beta$. For our purposes let us set

$$\varepsilon_\alpha = (-1)^{\langle\alpha,\gamma\rangle^{\mathrm{CT}}_{A^F}} \quad \text{and} \quad \varepsilon_\beta = (-1)^{1-\langle\beta,\gamma\rangle^{\mathrm{CT}}_{A^F}}.$$

Let $B \subseteq \mathrm{Sel}_2(A^F)$ be the subgroup generated by U and γ and let $\rho_\sigma \wedge \rho_\tau : B \times B \longrightarrow \mathbb{Z}/2$ be the alternating form constructed above. Since $\rho_\sigma(\beta') = \beta'(\sigma) = 0$ for every $\beta' \in U$ it follows that $\rho_\sigma \wedge \rho_\tau(\beta', \beta'') = 0$ for every $\beta', \beta'' \in U \subseteq B$. On the other hand, since $\rho_\tau(\gamma) = \gamma(\tau) = Q_{w_0}$ we have $\rho_\sigma \wedge \rho_\tau(\beta', \gamma) = \log_{(-1)}\langle\beta'(\tau), Q_{w_0}\rangle_\lambda$ for every $\beta' \in U$. Applying Proposition 4.11 with B the subgroup generated by U and γ and with the elements $\sigma, \tau \in \Gamma_k$ we obtain a quadratic twist $F' = k(\sqrt{a'})$ such that (with $a'' := a'a$ and $F'' := k(\sqrt{a''})$) we have

(1) $\mathrm{Sel}_2(A^{F''})$ contains U and γ and $\dim_2 \mathrm{Sel}_2(A^{F''}) = \dim_2 \mathrm{Sel}_2(A^F)$.
(2) For every $\beta', \beta'' \in U$ we have $\langle\beta', \beta''\rangle^{\mathrm{CT}}_{A^{F''}} = \langle\beta', \beta''\rangle^{\mathrm{CT}}_{A^F}$.
(3) For every $\beta' \in U$ we have $\langle\beta', \gamma\rangle^{\mathrm{CT}}_{A^{F''}} = \langle\beta', \gamma\rangle^{\mathrm{CT}}_{A^F} + (\rho_\sigma \wedge \rho_\tau)(\beta, \beta')$. In particular $\langle\alpha, \gamma\rangle^{\mathrm{CT}}_{A^{F''}} = 0$ and $\langle\beta, \gamma\rangle^{\mathrm{CT}}_{A^{F''}} \neq 0$.

Let $V \subseteq \mathrm{Sel}_2(A^{F''})$ be the subgroup consisting of those elements which are unramified over M', so that we have a direct sum decomposition $\mathrm{Sel}_2(A^{F''}) = V \oplus \delta_{F''}(A[2])$. Property (1) above implies that V is generated by U and $\gamma \notin U$. Let $V^\circ = V \cap \mathrm{Sel}_2^\circ(A^{F''})$. Since all the elements of V° are in particular orthogonal to β with respect to the Cassels-Tate pairing, Properties (2) and (3) above imply that $V^\circ \subseteq U$. Since all the elements of V° are also orthogonal to γ with respect to the Cassels-Tate pairing, Properties (2) and (3) further imply that $\beta \notin V^\circ \subseteq U$ while $\alpha \in V^\circ$. This means in particular that Condition (B4) holds for $(A^{F''}, \alpha)$. By Lemma 4.2 we have that $(A^{F''}, \alpha)$ is admissible, i.e., Condition (B1) holds as well. Finally, since $\mathrm{Sel}_2^\circ(A^{F''})$ is a direct sum of V° and the image of the 2-torsion we may now conclude that $\dim_2 \mathrm{Sel}_2^\circ(A^{F''}) < \dim_2 \mathrm{Sel}^\circ(A)$. It follows that the quadratic extension F'' has the desired properties and so the proof is complete.

□

4.4. **Proof of the main theorem.** In this section we will complete the proof of Theorem 2.8. Let k be a number field and let $A_1, \ldots, A_n$ be principally polarized simple abelian varieties over k, such that each A_i has all its 2-torsion defined over

k. For each i, let $M_i \subseteq \Omega_k$ be an extended 2-structure for A_i such that A_j has good reduction over M_j whenever $i \neq j$. Let $A = A_1 \times \ldots \times A_n$ and let $\alpha \in H^1(k, A[2])$ be a non-degenerate element which is unramified over $M = \cup_i M_i$ but which has a non-trivial image in $H^1(k_w, A[2])$ for each $w \in M$. We may uniquely write $\alpha = \sum_i \alpha_i$ with $\alpha_i \in H^1(k, A_i[2])$. Let Y_{α_i} be the 2-covering of A_i determined by α_i so that $Y_\alpha = \prod_i Y_{\alpha_i}$ is the 2-covering of A determined by α. Finally, let $X_\alpha = \mathrm{Kum}(Y_\alpha)$ be the associated Kummer surface.

of Theorem 2.8. To prove that Conjecture 1.1 holds for X_α, let us assume that the 2-primary Brauer-Manin obstruction to the Hasse principle is the only one for each Y^F_α, i.e., that $[Y^F_\alpha] \in H^1(k, A)$ is not a non-trivial divisible element of $\text{Ш}(A^F)$ for any F/k. Since $H^1(k, A) = \oplus_k H^1(k, A_i)$ and $\text{Ш}(A) = \oplus_i \text{Ш}(A_i)$ this is equivalent to saying that $[Y^F_{\alpha_i}] \in H^1(k, A_i)$ is not a non-trivial divisible element of $\text{Ш}(A^F_i)$ for any F.

In light of Lemma 4.2 we may, by possibly replacing A by a quadratic twist, assume that (A, α) is admissible. Applying Proposition 4.8 we may find a quadratic extension F/k, unramified over M, such that (A^F, α) satisfies Conditions (A1) and (A2) above. Replacing A with A^F we may assume that Conditions (A1) and (A2) already hold for (A, α). By repeated applications of Proposition 4.10 we may find a quadratic extension F'/k, unramified over M, such that $(A^{F'}, \alpha)$ satisfies Conditions (B1) and (B4) above. Replacing A with $A^{F'}$ we may assume that Conditions (B1) and (B2) already hold for (A, α). By repeated applications of Proposition 4.12 we may find a quadratic extension F''/k, unramified over M, and such that the subgroup $\mathrm{Sel}^\circ_2(A^{F''}) \subseteq \mathrm{Sel}_2(A^{F''})$ consisting of those elements which are orthogonal to all of $\mathrm{Sel}_2(A^{F''})$ with respect to the Cassels-Tate pairing is generated by $\alpha_1, ..., \alpha_n$ and the image of the 2-torsion. It then follows that $\mathrm{Sel}^\circ_2(A^{F''}_i)$ is generated by α_i and the image of the 2-torsion. Let $\text{Ш}^\circ(A^{F''}_i) \subseteq \text{Ш}(A^{F''}_i)$ be the subgroup orthogonal to all of $\text{Ш}(A^{F''}_i)[2]$ with respect to the Cassels-Tate pairing. Then we may conclude that $\text{Ш}^\circ(A^{F''}_i)$ is generated by the image of α_i, i.e., by the class $[Y^{F''}_{\alpha_i}]$ of $Y^{F''}_{\alpha_i}$. Since we assumed that $[Y^{F''}_{\alpha_i}]$ is not a non-trivial divisible element it now follows that $\text{Ш}(A^{F''}_i)\{2\}$ is finite. The Cassels-Tate pairing induces a non-degenerate self-pairing of $\text{Ш}(A^{F''}_i)\{2\}$, which is alternating in our case by Remark 3.10. This means, in particular, that if we write the abstract abelian group $\text{Ш}(A^{F''}_i)\{2\}$ as a direct sum $\oplus_i \mathbb{Z}/2^{n_i}$ of cyclic groups then for each n it will have an even number of $\mathbb{Z}/2^n$ components. Now the multiplication by 2 map induces an isomorphism $\text{Ш}(A^{F''}_i)[4]/\text{Ш}(A^{F''}_i)[2] \cong \text{Ш}^\circ(A^{F''}_i)$ and so by the above we may conclude that the 2-rank of $\text{Ш}^\circ(A^{F''}_i)$ is even. Since it is generated by a single element it must therefore vanish, implying that $[Y^{F''}_\alpha] = 0$. This means that $Y^{F''}_\alpha$ has a rational point and so X_α has a rational points as well, as desired. □

References

[BLR90] Bosch S., Lütkebohmert W. , Raynaud M., *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1990.

[BBL16] Bright M. J., Browning T. D., Loughran D., Failures of weak approximation in families, *Compositio Mathematica*, 152.7, 2016, p. 1435–1475.

[CEPT96] Chinburg T., Erez B., Pappas G., Taylor M.J., Tame actions of group schemes: integrals and slices, *Duke Mathematical Journal*, 82.2, 1996, p. 269–308.

[CTSSD98] Colliot-Thélène 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, 1998, p. 579–650.

[CT01] Colliot-Thélène J.-L., Hasse principle for pencils of curves of genus one whose jacobians have a rational 2-division point, Rational points on algebraic varieties, Birkhäuser Basel, 2001, p. 117–161.

[HS15] Harpaz Y., Skorobogatov A. N., The Hasse principle for Kummer varieties, *Algebra and Number Theory*, 10.4, 2016, p. 813-841

[HW15] Harpaz Y., Wittenberg O., On the fibration method for zero-cycles and rational points, *Annals of Mathematics*, 183.1, 2015, p. 229-295.

[HW16] Hadian M., Weidner M., On Selmer Rank Parity of Twists, *Journal of the Australian Mathematical Society*, 2016, p. 1–15.

[KMR11] Klagsbrun Z., Mazur B., Rubin K., Disparity in Selmer ranks of quadratic twists of elliptic curves, preprint arXiv:1111.2321, 2011.

[Ma72] Mazur B., Rational Points of Abelian Varieties with Values in Towers of Number Fields, *Inventiones mathematicae*, 18.3, 1972, p. 183–266.

[MR07] Mazur B., Rubin K., Finding large Selmer rank via an arithmetic theory of local constants, *Annals of Mathematics*, 166, 2007, p. 579–612.

[MR10] Mazur B., Rubin K., Ranks of twists of elliptic curves and Hilbert's tenth problem, *Inventiones Mathematicae*, 181, 2010, p. 541–575.

[Ni75] Nikulin V. V., Kummer surfaces, *Izvestiya Akademii Nauk SSSR*, Seriya Matematicheskaya 39, 1975, p. 278-293; English translation: Mathematics of the USSR-Izvestiya, 9.2, 1975, p. 261-275.

[PR11] Poonen B. Rains E., Self cup product and the theta characteristic torsor. *Math. Res. Letters*, 18, 2011, p. 1305–1318.

[PR12] Poonen B., Rains E., Random maximal isotropic subspaces and Selmer groups, *Journal of the American Mathematical Society*, 25.1, 2012, p. 245–269.

[PS99] Poonen B., Stoll M., Cassels–Tate pairing on polarized abelian varieties. *Annals of Mathematics*, 150, 1999, p. 1109–1149.

[SW95] Sarnak P., Wang L., Some hypersurfaces in $\mathbb{P}^4$ and the Hasse-principle, *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 321, 1995, p. 319–322.

[Sm14] Smeets A., Insufficiency of the étale Brauer-Manin obstruction: towards a simply connected example, preprint, arXiv:1409.6706, 2014.

[Sk09] Skorobogatov A. N., Diagonal quartic surfaces. *Explicit methods in number theory.*, K. Belabas, H.W. Lenstra, D.B. Zagier, eds. Oberwolfach report, 33, 2009, p. 76–79.

[Sk10] Skorobogatov A. N., Del Pezzo surfaces of degree 4 and their relation to Kummer surfaces, *L'Enseignement Mathématique*, 56, 2010, p. 73–85.

[SSD05] Skorobogatov A. N., Swinnerton-Dyer, P, 2-descent on elliptic curves and rational points on certain Kummer surfaces, *Advances in Mathematics*, 2005, 198.2, 448-483.

[SZ08] Skorobogatov A. N., Zarhin Y., A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces, *Journal of Algebraic Geometry*, 17, 2008, p. 481–502.

[SZ16] Skorobogatov A. N., Zarhin Y., Kummer varieties and their Brauer groups, preprint arXiv:1612.05993, 2016.

[SD95] 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.

[SD00] Swinnerton-Dyer P., Arithmetic of diagonal quartic surfaces II, *Proceedings of the London Mathematical Society*, 80.3, 2000, p. 513–544.

[Wi07] Wittenberg O., *Intersections de deux quadriques et pinceaux de courbes de genre 1*, Lecture Notes in Mathematics, Vol. 1901, Springer, 2007.

[Mu84] Mumford D., *Tata lectures on theta. II: Jacobian theta functions and differential equations*, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura, Progress in Mathematics 43, 1984.

[HN10] Halle L. H., Nicaise J, The Nron component series of an abelian variety, *Mathematische Annalen*, 348.3, 2010, p. 749–778.

[Mu91] Mumford D., *Tata lectures on theta III*, Progress in Mathematics, vol. 97, Birkhuser Boston Inc., Boston, MA, 1991. With the collaboration of Madhav Nori and Peter Norman.

[Po03] Polishchuk A., *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics, vol. 153, Cambridge University Press, Cambridge, 2003.

[Cr17] Creutz B., No transcendental Brauer-Manin obstruction on abelian varieties, preprint arXiv:1711.01541, 2017.

[Ma71] Manin Y., Le groupe de Brauer-Grothendieck en gomtrie diophantienne, Actes du Congrs International des Mathmaticiens (Nice, 1970), Gauthier-Villars, Paris, 1971, p. 401-411.

[RS17] Roulleau X., Sarti A., Construction of Nikulin configurations on some Kummer surfaces and applications, preprint arXiv:1711.05968, 2017.

[CV17] Creutz B., Viray B., Degree and the Brauer-Manin obstruction, preprint arXiv:1703.02187, 2017.