Hasse principle for Kummer varieties

Yonatan Harpaz and Alexei N. Skorobogatov

December 17, 2015

Abstract

The existence of rational points on the Kummer variety associated to a 2-covering of an abelian variety A over a number field can sometimes be established through the variation of the 2-Selmer group of quadratic twists of A. In the case when the Galois action on the 2-torsion of A has a large image we prove, under mild additional hypotheses and assuming the finiteness of relevant Shafarevich–Tate groups, that the Hasse principle holds for the associated Kummer varieties. This provides further evidence for the conjecture that the Brauer–Manin obstruction controls rational points on K3 surfaces.

1 Introduction

The principal aim of this paper is to give some evidence in favour of the conjecture that the Brauer–Manin obstruction is the only obstruction to the Hasse principle for rational points on K3 surfaces over number fields, see [29, p. 77] and [32, p. 484]. Conditionally on the finiteness of relevant Shafarevich–Tate groups we establish the Hasse principle for certain families of Kummer surfaces. These surfaces are quotients of 2-coverings of an abelian surface A by the antipodal involution, where

(a) A is the product of elliptic curves $A = E_1 \times E_2$, or

(b) A is the Jacobian of a curve C of genus 2 with a rational Weierstraß point.

Both cases are treated by the same method which allows us to prove a more general result for the Kummer varieties attached to 2-coverings of an abelian variety A over a number field k, provided certain conditions are satisfied. By a 2-covering we understand a torsor Y for A such that the class $[Y] \in \mathrm{H}^1(k, A)$ has order at most 2. Thus Y is the twist of A by a 1-cocycle with coefficients in $A[2]$ acting on A by translations. The antipodal involution $\iota_A = [-1] : A \to A$ induces an involution $\iota_Y : Y \to Y$ and we define the Kummer variety $X = \mathrm{Kum}(Y)$ as the minimal desingularisation of Y/ι_Y, see §6 for details.

In this introduction we explain the results pertaining to cases (a) and (b) above and postpone the statement of a more general theorem until the next section. In case

(a) we have the following result, whose proof can be found at the end of Section 2. We denote by $\Delta(f)$ the discriminant of a (not necessarily monic) polynomial $f(x)$; see (3) for the classical formula for $\Delta(f)$ in the case $\deg(f) = 4$.

Theorem A *Let $g_1(x)$ and $g_2(x)$ be irreducible polynomials of degree 4 over a number field k, each with the Galois group S_4. Let w_1 and w_2 be distinct primes of k not dividing 6 such that for all $i, j \in \{1, 2\}$ the coefficients of $g_i(x)$ are integral at w_j and $\mathrm{val}_{w_j}(\Delta(g_i)) = \delta_{ij}$. Let E_i be the Jacobian of the curve $y^2 = g_i(x)$, where $i = 1, 2$. For $i = 1, 2$ assume the finiteness of the 2-primary torsion subgroup of the Shafarevich–Tate group for each quadratic twist of E_i whose 2-Selmer group has rank 1. If the Kummer surface with the affine equation*

$$z^2 = g_1(x)g_2(y) \tag{1}$$

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

We expect that the conditions of Theorem A are in a certain sense 'generic'. To illustrate this, let $\mathbb{Z}[t]_{\deg=4} \subset \mathbb{Z}[t]$ be the set of polynomials of degree 4 ordered by the maximal height of their coefficients. By a theorem of van der Waerden 100 % of polynomials in $\mathbb{Z}[t]_{\deg=4}$ have the Galois group S_4 (see [5, Thm. 1] for a statement over an arbitrary number field). For two fixed rational primes w_1, w_2 an easy sieve (or approximation) argument gives that a positive proportion of pairs $g_1, g_2 \in \mathbb{Z}[t]_{\deg=4}$ satisfy the condition $\mathrm{val}_{w_j}(\Delta(g_i)) = \delta_{ij}$. It seems plausible that 100% of pairs $g_1, g_2 \in \mathbb{Z}[t]_{\deg=4}$ satisfy this condition for some w_1, w_2. The finiteness of the Shafarevich–Tate group is a well known conjecture, established by M. Bhargava, C. Skinner and W. Zhang for a majority of elliptic curves over $\mathbb{Q}$ ordered by naïve height [2, Thm. 2]. Note finally that using [1, Thm. 1.4] one can show that the Kummer surface (1) is everywhere locally soluble for a positive proportion of pairs $g_1, g_2 \in \mathbb{Z}[t]_{\deg=4}$.

To give an explicit description of our results in case (b) we need to recall the realisation of Kummer surfaces attached to the Jacobian of a genus 2 curve as smooth complete intersections of three quadrics in $\mathbb{P}^5_k$. We mostly follow [30, Section 3]; for the classical theory over an algebraically closed field see [9, Ch. 10].

Let $f(x)$ be a separable monic polynomial of degree 5 over a field k of characteristic different from 2. Let C be the hyperelliptic curve with the affine equation $y^2 = f(x)$ and let A be the Jacobian of C. Let L be the étale k-algebra $k[x]/(f(x))$ and let $\theta \in L$ be the image of x. The 2-torsion $\mathrm{Gal}(\bar{k}/k)$-module $A[2]$ is isomorphic to $\mathrm{R}_{L/k}(\mu_2)/\mu_2$, where $\mathrm{R}_{L/k}$ is the Weil restriction of scalars. Since $[L : k]$ is odd, $A[2]$ is a direct summand of $\mathrm{R}_{L/k}(\mu_2)$. It follows that the map $\mathrm{H}^1(k, \mathrm{R}_{L/k}(\mu_2)) = L^*/L^{*2} \to \mathrm{H}^1(k, A[2])$ is surjective and induces an isomorphism $\mathrm{H}^1(k, A[2]) = L^*/k^*L^{*2}$.

Let $\lambda \in L^*$. Let $W_\lambda \subset \mathrm{R}_{L/k}(\mathbb{G}_{m,L})$ be the closed subscheme given by $z^2 = \lambda$. It is clear that W_λ is a k-torsor for $\mathrm{R}_{L/k}(\mu_2)$ whose class in $\mathrm{H}^1(k, \mathrm{R}_{L/k}(\mu_2)) = L^*/L^{*2}$ is given by λ. Let $Z_\lambda = W_\lambda/\{\pm 1\}$ be the subscheme of $\mathrm{R}_{L/k}(\mathbb{G}_{m,L})/\{\pm 1\}$ given by the same equation. We obtain that Z_λ is the k-torsor for $A[2]$ whose class in $\mathrm{H}^1(k, A[2]) = L^*/k^*L^{*2}$ is defined by λ.

Now let $Y_\lambda = (A \times Z_\lambda)/A[2]$ be the 2-covering of A obtained by twisting A by Z_λ. Then $\mathrm{Kum}(Y_\lambda)$ is the following smooth complete intersection of three quadrics in $\mathbb{P}(\mathrm{R}_{L/k}(\mathbb{A}^1_L) \times \mathbb{A}^1_k) \simeq \mathbb{P}^5_k$:

$$\mathrm{Tr}_{L/k}\left(\lambda\frac{u^2}{f'(\theta)}\right) = \mathrm{Tr}_{L/k}\left(\lambda\frac{\theta u^2}{f'(\theta)}\right) = \mathrm{Tr}_{L/k}\left(\lambda\frac{\theta^2 u^2}{f'(\theta)}\right) - \mathrm{N}_{L/k}(\lambda)u_0^2 = 0, \quad (2)$$

where u is an L-variable, u_0 is a k-variable, and $f'(x)$ is the derivative of $f(x)$ (cf. equations (7) and (8) in [30]). If $\lambda \in k^*L^{*2}$, then an easy change of variable reduces (2) to the same system of equations with $\lambda = 1$. As $Y_1 \cong A$ has a rational point this case can be excluded for the purpose of establishing the Hasse principle.

Theorem B *Let $f(x)$ be a monic irreducible polynomial of degree 5 over a number field k, and let $L = k[x]/(f(x))$. Let w be an odd prime of k such that the coefficients of $f(x)$ are integral at w and $\mathrm{val}_w(\Delta(f)) = 1$. Let A be the Jacobian of the hyperelliptic curve $y^2 = f(x)$. Assume the finiteness of the 2-primary torsion subgroup of the Shafarevich–Tate group for each quadratic twist of A whose 2-Selmer group has rank 1. Let $\lambda \in L^*$ be such that for some $r \in k^*$ the valuation of λr at each completion of L over w is even, but $\lambda \notin k^*L^{*2}$. If the Kummer surface given by (2) is everywhere locally soluble, then it has a Zariski dense set of k-points.*

Let $[\lambda] \in \mathrm{H}^1(k, A[2])$ be the class defined by λ. The conditions imposed on λ in Theorem B are equivalent to the condition that $[\lambda] \neq 0$ and $[\lambda]$ is unramified at w. Equivalently, the k-torsor Z_λ defined above has a k_w^{un}-point, where k_w^{un} is the maximal unramified extension of k_w, but no k-point.

Any Kummer surface (2) can be mapped to $\mathbb{P}^3_k$ by a birational morphism that contracts 16 disjoint rational curves onto singular points. The image of $\mathrm{Kum}(Y_\lambda)$ is a singular quartic surface $S \subset \mathbb{P}^3_k$ which is the classical Kummer surface with 16 nodes. (See [9, Section 10.3.3] and [10] for a modern account of the geometry of S over an algebraically closed field.) The group $A[2]$ acts on S by projective automorphisms and the singular locus S_{sing} is a k-torsor for $A[2]$. Then S is identified with the twist of A/ι_A by S_{sing}. The condition $\lambda \notin k^*L^{*2}$, which we use to prove the Zariski density of $S(k)$, is precisely the condition that the torsor S_{sing} is non-trivial, that is, no singular point of S is a k-point.

Theorem B is proved at the end of Section 2. The main idea of the proof of Theorems A and B is due to Swinnerton-Dyer. Let $\alpha \in \mathrm{H}^1(k, A[2])$ be the class of a 1-cocycle used to obtain Y from A. The group $\mu_2 = \{\pm 1\}$ acts on A by multiplication. As this action commutes with the action of $A[2]$ by translations we have an induced action of μ_2 on Y. For an extension F/k of degree at most 2 let T_F be the torsor for μ_2 defined by F. The quadratic twists A^F and Y^F are defined as the quotients of $A \times_k T_F$ and $Y \times_k T_F$, respectively, by the diagonal action of μ_2. We identify $A^F[2] = A[2]$ and consider Y^F as a torsor for A^F defined by the same 1-cocycle with the class $\alpha \in \mathrm{H}^1(k, A^F[2]) = \mathrm{H}^1(k, A[2])$. The projection to

the first factor defines a morphism $Y^F = (Y \times_k T_F)/\mu_2 \longrightarrow Y/\mu_2$. Thus in order to find a rational point on the Kummer variety $X = \mathrm{Kum}(Y)$ it is enough to find a rational point on Y^F for some F. 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, $\alpha \in \mathrm{H}^1(k, A^F[2])$ 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. (In the cases considered in this paper $A^F[2](k) = A[2](k) = 0$.) This implies that $Ш(A^F)[2]$ is $\mathbb{Z}/2$ or 0. In previous applications of the method [35, 31], as well as in Theorem A above, A is a product of two elliptic curves, in which case the Cassels–Tate pairing on $Ш(A^F)$ is alternating. The assumption that $Ш(A^F)$ is finite then implies that the order of $Ш(A^F)[2]$ is a square and hence $Ш(A^F)[2] = 0$. In particular, Y^F has a k-point, so that $Y^F \simeq A^F$. In this paper we consider more general principally polarised abelian varieties. The theory developed by Poonen and Stoll in [26] ensures that in the cases considered here the Cassels–Tate pairing on $Ш(A^F)$ defined using the principal polarisation is still alternating, so the proof can be concluded as before.

Swinnerton-Dyer's method was used in combination with Schinzel's Hypothesis (H) in [6, 34, 37]. For the first time the method was applied without Hypothesis (H) in [35] using Dirichlet's theorem on primes in an arithmetic progression, the only known case of (H). That work tackled diagonal cubic surfaces, which are dominated by a product of two elliptic curves with complex multiplication. The immediate precursor of our Theorem A is [31], which treats Kummer surfaces attached to products of elliptic curves, again without assuming Hypothesis (H). Central to Swinnerton-Dyer's method is a linear algebra construction that represents the Selmer group as the kernel of a symmetric bilinear form. The difficulty of operating this machinery makes implementation of the method a rather delicate task. In the present paper this linear algebra machinery is not used. Instead we use the ideas of Mazur and Rubin from [22] and especially from [21].

Let us note that given an elliptic curve E over a number field k it is not always possible to find a quadratic extension F/k such that the 2-Selmer group of E^F is spanned by a fixed class $\alpha \in \mathrm{H}^1(k, E[2])$ and the image of $E^F[2](k)$. Firstly, the parity of the rank of the 2-Selmer group of E^F can be the same for all F: this happens precisely when k is totally imaginary and E acquires everywhere good reduction over an abelian extension of k, see [8, Remark 4.9]. Secondly, over any number field k there are elliptic curves E such that for any quadratic extension F/k the difference between the 2-Selmer rank of E^F and the dimension of the $\mathbb{F}_2$-vector space $E[2](k)$ is at least the number of complex places of k, see [13, 14]. Such examples can occur when $E[2](k) \cong \mathbb{Z}/2$ and E has a cyclic isogeny of degree 4 defined over $k(E[2])$ but not over k.

In this paper we do not discuss the conjecture [29, p. 77], [32, p. 484] that rational

points on a K3 surface are dense in its Brauer–Manin set[1]. Nevertheless we make the following simple observation in the direction of Mazur's conjectures [19, 20].

Proposition 1.1. *Let $E_1, \dots, E_n$ be elliptic curves over $\mathbb{Q}$ such that $E_i[2](\mathbb{Q}) = 0$ for $i = 1, \dots, n$. Let $X = \mathrm{Kum}(\prod_{i=1}^n Y_i)$, where Y_i is a 2-covering of E_i defined by a non-zero class in $\mathrm{H}^1(\mathbb{Q}, E_i[2])$ for $i = 1, \dots, n$. Then the real topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ is a union of connected components of $X(\mathbb{R})$.*

This can be compared with the result of M. Kuwata and L. Wang [16]. See the end of Section 7 for the proof of Proposition 1.1.

The main technical result of the paper is Theorem 2.3. It is stated in Section 2 where we also show that Theorem 2.3 implies Theorems A and B. In Section 3 we systematically develop the Galois-theoretic aspect of the approach of Mazur and Rubin. We recall the necessary facts about the Kummer map for quadratic twists of abelian varieties over local fields in Section 4. In Section 5 we discuss the Selmer group and the Cassels–Tate pairing over a number field. A reduction to everywhere soluble 2-coverings is carried out in Section 6 using a known case of the fibration method. We finish the proof of Theorem 2.3 in Section 7.

While working on this paper the first named author was supported by the Fondation Sciences Mathématiques de Paris. The paper was finalised when the second named author was at the Institute for Advanced Study in Princeton where he was supported by The Charles Simonyi Endowment. We are grateful to Tim Dokchitser, Evis Ieronymou and René Pannekoek for helpful discussions, and to the referee for careful reading of the paper.

2 Main results

Let k be a field of characteristic different from 2 with a separable closure $\bar{k}$ and the Galois group $\Gamma_k = \mathrm{Gal}(\bar{k}/k)$.

Let A be an abelian variety over k. Let $K = k(A[2]) \subset \bar{k}$ be the field of definition of $A[2]$, that is, the smallest field such that $A[2](K) = A[2](\bar{k})$. Let $G = \mathrm{Gal}(K/k)$. Consider the following conditions:

(a) $A[2]$ is a simple G-module and $\mathrm{End}_G(A[2]) = \mathbb{F}_2$;
(b) $\mathrm{H}^1(G, A[2]) = 0$;
(c) there exists $g \in G$ such that $A[2]/(g-1) = \mathbb{F}_2$;
(d) there exists $h \in G$ such that $A[2]/(h-1) = 0$.

[1] A recent result of D. Holmes and R. Pannekoek [12] shows that if this conjecture is extended to all Kummer varieties, then the ranks of quadratic twists of any given abelian variety over a given number field are not bounded.

Lemma 2.1. *Let A be the Jacobian of a smooth projective curve with the affine equation $y^2 = f(x)$, where $f(x) \in k[x]$ is an irreducible separable polynomial of odd degree $m \geq 3$. If the Galois group of $f(x)$ is the symmetric group on m letters S_m, then A satisfies conditions (a), (b), (c), (d).*

Proof. It is well known that the Γ_k-module $A[2]$ is the zero-sum submodule of the vector space $(\mathbb{F}_2)^m$ freely generated by the roots of $f(x) = 0$ with the natural permutation action of Γ_k. Since m is odd, the permutation Γ_k-module $(\mathbb{F}_2)^m$ is the direct sum of $A[2]$ and the $\mathbb{F}_2$-vector space spanned by the vector $(1, \dots, 1)$.

If an S_m-submodule of $(\mathbb{F}_2)^m$ contains a vector with at least one coordinate 0 and at least one coordinate 1, then it contains the zero-sum submodule. Hence $A[2]$ is a simple S_m-module. A direct calculation with matrices shows that the $m \times m$ matrices commuting with all permutation matrices are the linear combinations of the identity and the all-1 matrix. We deduce that $\mathrm{End}_{S_m}(A[2]) = \mathbb{F}_2$, thus (a) holds.

The permutation S_m-module $(\mathbb{F}_2)^m$ is isomorphic to $\mathbb{F}_2[S_m/S_{m-1}]$. By Shapiro's lemma we have

$$\mathrm{H}^1(S_m, \mathbb{F}_2[S_m/S_{m-1}]) = \mathrm{H}^1(S_{m-1}, \mathbb{F}_2) = \mathrm{Hom}(S_{m-1}, \mathbb{F}_2) = \mathbb{F}_2.$$

Since $\mathrm{H}^1(S_m, \mathbb{F}_2) = \mathbb{F}_2$, we obtain $\mathrm{H}^1(S_m, A[2]) = 0$, so (b) holds.

If g is a cycle of length $m-1$, then $A[2]/(g-1) = \mathbb{F}_2$, so (c) is satisfied. If h is a cycle of length m, then $A[2]/(h-1) = 0$, so (d) is satisfied. □

Remark 2.2. There are other natural cases when the Galois module $A[2]$ satisfies conditions (a) to (d). Assume $\dim(A) = n > 1$. In this paper we only deal with the case when the Cassels–Tate pairing defined by a polarisation $\lambda \in \mathrm{NS}(\bar{A})^{\Gamma_k}$ is alternating. According to the results of Poonen, Stoll and Rains recalled in §5 this holds when λ lifts to a symmetric element of $\mathrm{Pic}(A)$. (This happens, for example, when A is the Jacobian of a hyperelliptic curve with a rational Weierstraß point.) In this case the pairing $A[2] \times A[2] \to \mathbb{Z}/2$ induced by λ and the Weil pairing admits a Galois invariant quadratic enhancement $q : A[2] \to \mathbb{Z}/2$ (Lemma 5.1, Remark 5.2). The 'generic' Galois action preserving q is when G is the corresponding orthogonal group $O(q) \subset \mathrm{GL}(A[2])$. It can be shown that conditions (a), (c) and (d) are always satisfied for $G = O(q)$. Condition (b) is satisfied for all $n \neq 2, 3$ when q is split (i.e., isomorphic to a direct sum of copies of the rank 2 hyperbolic space) and for all $n \neq 3, 4$ if q is non-split (see [27, Prop. 2.1]). We do not elaborate on these statements here, as we will not use them in the paper.

Let $A_1, \dots, A_r$ be abelian varieties over k. For each $i = 1, \dots, r$ let $K_i = k(A_i[2])$ and $G_i = \mathrm{Gal}(K_i/k)$. We assume the following condition.

(e) The fields $K_1, \dots, K_r$ are linearly disjoint over k.

By definition this means that $[K_1 \dots K_r : k] = \prod_{i=1}^r [K_i : k]$. Thus the Galois group of $K_1 \dots K_r$ over k is $\prod_{i=1}^r G_i$.

When k is a *number field* we shall also assume the following condition.

(f) There exist distinct odd primes $w_1, \dots, w_r$ of k such that for each $i = 1, \dots, r$ the abelian variety A_i has bad reduction at w_i and the number of geometric connected components of the Néron model of A_i at w_i is odd, whereas each A_j for $j \neq i$ has good reduction at w_i.

Let k_i^{ab} be the maximal abelian subextension of $k \subset K_i$. Equivalently, $\mathrm{Gal}(k_i^{\mathrm{ab}}/k)$ is the maximal abelian quotient G_i^{ab} of G_i. Let us finally assume the condition

(g) for each $i = 1, \dots, r$ the field k_i^{ab} is totally ramified at w_i. Equivalently, k_i^{ab} has a unique prime ideal above w_i, and G_i^{ab} coincides with the inertia subgroup of this ideal.

Let F be a field extension of k of degree at most 2. As in the introduction, we denote by A^F the quadratic twist of A by F, that is, the abelian variety over k obtained by twisting A by the quadratic character of F/k with respect to the action of μ_2 on A by multiplication. For example, if A is an elliptic curve with the Weierstraß equation $y^2 = f(x)$, then A^F is given by $y^2 = cf(x)$, where $c \in k^*$ is such that $F = k(\sqrt{c})$.

We are now ready to state the main theorem of this paper. Recall that a class in $\mathrm{H}^1(k, A[2])$ is *unramified* at a non-Archimedean place v of k if it goes to zero under the restriction map $\mathrm{H}^1(k, A[2]) \to \mathrm{H}^1(k_v^{\mathrm{nr}}, A[2])$, where k_v^{nr} is the maximal unramified extension of the completion k_v of k at v.

Theorem 2.3. *Let k be a number field. Let $A = \prod_{i=1}^r A_i$, where each A_i is a principally polarised abelian variety satisfying conditions (a), (b), (c) and (d). Assume in addition that conditions (e), (f) and (g) are satisfied. Assume that the 2-primary subgroup of the Shafarevich–Tate group $Ш(A_i^F)\{2\}$ is finite for all $i = 1, \dots, r$ and all extensions F of k with $[F : k] \leq 2$ for which the 2-Selmer group of A_i^F has rank 1. Consider the classes in $\mathrm{H}^1(k, A[2])$ that are unramified at $w_1, \dots, w_r$ and whose projection to $\mathrm{H}^1(k, A_i[2])$ is non-zero for each $i = 1, \dots, r$. If the Kummer variety of A defined by such a class is everywhere locally soluble, then it has a Zariski dense set of k-points.*

Remarks 1. If $r = 1$, then condition (d) is not needed and condition (e) is vacuous.

2. The Brauer–Manin obstruction does not appear in the conclusion of the theorem. In fact, the purely algebraic conditions (a), (b) and (e) imply that a certain part of the Brauer group is trivial, see Proposition 6.1. The problem of calculation of the full Brauer group of a Kummer variety will be addressed in a separate paper.

3. If the 2-primary torsion subgroup $Ш(A_i^F)\{2\}$ is finite, then condition (b) implies that the non-degenerate Cassels–Tate pairing on $Ш(A_i^F)\{2\}$ is alternating. See

Proposition 5.3 based on the work of Poonen–Stoll [26] and Poonen–Rains [24]. In the proof of Theorem 2.3 we use a well known consequence of this result that the number of elements of $Ш(A_i^F)[2]$ is a square.

We employ the following standard notation:
k_{w_i} is the completion of k at w_i,
$\mathcal{O}_{w_i}$ is the ring of integers of k_{w_i},
$\mathfrak{m}_{w_i}$ is the maximal ideal of $\mathcal{O}_{w_i}$, and
$\mathbb{F}_{w_i} = \mathcal{O}_{w_i}/\mathfrak{m}_{w_i}$ is the residue field.

Corollary 2.4. *Let k be a number field. For $i = 1, \dots, r$ let $f_i(x) \in k[x]$ be a monic irreducible polynomial of odd degree $n_i \geq 3$ whose Galois group is the symmetric group S_{n_i}, and let A_i be the Jacobian of the hyperelliptic curve $y^2 = f_i(x)$. Assume the existence of distinct odd primes $w_1, \dots, w_r$ of k such that $f_i(x) \in \mathcal{O}_{w_j}[x]$ and $\mathrm{val}_{w_i}(\Delta(f_j)) = \delta_{ij}$ for any $i, j \in \{1, \dots, r\}$. Assume that $Ш(A_i^F)\{2\}$ is finite for all $i = 1, \dots, r$ and all extensions F of k with $[F : k] \leq 2$ for which the 2-Selmer group of A_i^F has rank 1. Consider the classes in $\mathrm{H}^1(k, A[2])$ that are unramified at $w_1, \dots, w_r$ and whose projection to $\mathrm{H}^1(k, A_i[2])$ is non-zero for each $i = 1, \dots, r$. If the Kummer variety of A defined by such a class is everywhere locally soluble, then it has a Zariski dense set of k-points.*

Proof. Each A_i is a canonically principally polarised abelian variety which satisfies conditions (a), (b), (c), (d) by Lemma 2.1.

Let C_i be the proper, smooth and geometrically integral curve over k given by the affine equation $y^2 = f_i(x)$, so that $A_i = \mathrm{Jac}(C_i)$. As in [17, Section 4.3], a proper and flat *Weierstraß model* $\mathcal{C}_i$ over $\mathrm{Spec}(\mathcal{O}_{w_i})$ is defined as the normalisation in $C_i \times_k k_{w_i}$ of the projective line $\mathbb{P}^1_{\mathcal{O}_{w_i}}$ with the affine coordinate x. Since $2 \in \mathcal{O}_{w_i}^*$ the integral closure of $\mathcal{O}_{w_i}[x]$ in $k_{w_i}(C_i)$ is $\mathcal{O}_{w_i}[x, y]/(y^2 - f_i(x))$. The condition $\mathrm{val}_{w_i}(\Delta(f_i)) = 1$ implies that $\mathcal{C}_i$ is regular and the special fibre $\mathcal{C}_i \times_{\mathcal{O}_{w_i}} \mathbb{F}_{w_i}$ is geometrically integral with a unique singular point, which is an ordinary double point, see Cor. 6 and Remark 18 on p. 4602 of [17]. In particular, the reduction of $f_i(x)$ modulo $\mathfrak{m}_{w_i}$ has one rational double root and $n_i - 2$ simple roots. (This can also be checked directly using Sylvester's formula for the discriminant.) Now [3, Thm. 9.6.1] implies that the special fibre of the Néron model of $A_i \times_k k_{w_i}$ over $\mathrm{Spec}(\mathcal{O}_{w_i})$ is connected. If $j \neq i$, then $\mathrm{val}_{w_i}(\Delta(f_j)) = 0$, and this implies that A_j has good reduction at w_i. We conclude that (f) holds.

For each $i = 1, \dots, r$ the field $K_i = k(A_i[2])$ is the splitting field of $f_i(x)$. Since $\mathrm{Gal}(K_i/k) \cong S_{n_i}$, the alternating group is the unique non-trivial normal subgroup of $\mathrm{Gal}(K_i/k)$. Its invariant subfield is $k(\sqrt{\Delta(f_i)})$. Thus if k' is a Galois extension of k such that $k \subsetneq k' \subseteq K_i$, then $k(\sqrt{\Delta(f_i)}) \subseteq k'$. The extension $k(\sqrt{\Delta(f_i)})$ of k is ramified at w_i, so (g) holds.

Let K_i' be the compositum of the fields K_j for $j \neq i$. Since each K_i is a Galois extension of k, the field $K_i \cap K_i'$ is also a Galois extension of k. To verify (e)

we need to check that $K_i \cap K_i' = k$ for each $i = 1, \dots, r$. Otherwise, $K_i \cap K_i'$ contains $k(\sqrt{\Delta(f_i)})$ which is ramified at w_i. However, this contradicts the criterion of Néron–Ogg–Shafarevich according to which K_i' is unramified at w_i, because the abelian varieties A_j for $j \neq i$ have good reduction at this place. Thus (e) holds. □

Proof of Theorem A assuming Theorem 2.3. For $i = 1, 2$ let C_i be the curve of genus 1 given by $y^2 = g_i(x)$. Write $g_i(x) = ax^4 + bx^3 + cx^2 + dx + e$. The classical SL(2)-invariants of the corresponding quartic binary form $G_i(u, v) = v^4 g_i(u/v)$ are

$$I = 12ae - 3bd + c^2,\ J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3,\ \Delta = (4I^3 - J^2)/27. \quad (3)$$

Then the Jacobian of C_i is the elliptic curve E_i with the equation $u^2 = p_i(t)$, where $p_i(t) = t^3 - 27Ix - 27J$ is the resolvent cubic polynomial of $g_i(x)$, see [28, Prop. 3.3.6 (a)]. The 0-dimensional scheme $g_i(x) = 0$ is a k-torsor Z_i for $E_i[2]$. Then C_i can be viewed as the twist of E_i by Z_i, that is, $C_i = (E_i \times Z_i)/E_i[2]$, where $E_i[2]$ acts simultaneously on both factors. The antipodal involution acts on C_i by changing the sign of y, so the Kummer surface $\mathrm{Kum}(C_1 \times C_2)$ is the minimal desingularisation of the quotient of $C_1 \times C_2$ by the involution that acts on each component as $(x, y) \mapsto (x, -y)$. Thus $z^2 = g_1(x)g_2(y)$ defines an affine surface birationally equivalent to $\mathrm{Kum}(C_1 \times C_2)$.

Since the polynomials $g_1(x)$ and $g_2(x)$ have no roots in k, each of the torsors Z_1 and Z_2 is non-trivial. The field of definition $K_i = k(E_i[2])$ of $E_i[2]$ is the splitting field of $p_i(t)$. Hence the condition $\mathrm{Gal}(g_1) \simeq S_4$ implies $\mathrm{Gal}(K_i/k) = \mathrm{Gal}(p_i) \simeq S_3$, for $i = 1, 2$. The discriminant of the quartic $g_i(x)$ is equal to the discriminant of its resolvent cubic $p_i(t)$ up to a power of 3, and $g_i(x) \in \mathcal{O}_{w_j}[x]$ implies $p_i(t) \in \mathcal{O}_{w_j}[t]$, so the primes w_1 and w_2 satisfy the assumption in Corollary 2.4. To be in a position to appeal to that corollary we now show that Z_i is unramified at both w_1 and w_2.

Indeed, let $\mathcal{Z}_{ij} \subset \mathbb{P}^1_{\mathcal{O}_{w_j}}$ be the closed subscheme given by $G_i(u, v) = 0$, where $G_i(u, v) = v^4 g_i(u/v) \in \mathcal{O}_{w_j}[u, v]$. For $j \neq i$ the discriminant of $G_i(u, v)$ is a unit in $\mathcal{O}_{w_j}$, thus $\mathcal{Z}_{ij}$ is a finite and étale $\mathcal{O}_{w_j}$-scheme of degree 4 with the generic fibre $Z_i \times_k k_{w_j}$, hence Z_i is unramified at w_j. For $i = j$ the discriminant of $G_i(u, v)$ is a generator of the maximal ideal of $\mathcal{O}_{w_i}$. This implies that the fibre $\mathcal{Z}_{ii} \times_{\mathcal{O}_{w_i}} \mathbb{F}_{w_i}$ at the closed point of $\mathrm{Spec}(\mathcal{O}_{w_i})$ is the disjoint union of a double $\mathbb{F}_{w_i}$-point and a reduced 2-point $\mathbb{F}_{w_i}$-scheme. The latter gives rise to two sections of the morphism

$$\mathcal{Z}_{ii} \times_{\mathcal{O}_{w_i}} \mathcal{O}_{w_i}^{\mathrm{nr}} \longrightarrow \mathrm{Spec}(\mathcal{O}_{w_i}^{\mathrm{nr}}).$$

Hence Z_i is unramified at w_i. An application of Corollary 2.4 finishes the proof. □

Proof of Theorem B assuming Theorem 2.3. The condition $\mathrm{val}_w(\Delta(f)) = 1$ implies that $k(\sqrt{\Delta(f)})$ has degree 2 over k. Hence the Galois group of $f(x)$ is not a subgroup of the alternating group A_5. Any proper subgroup of S_5 which acts transitively on $\{1, 2, 3, 4, 5\}$ and is not contained in A_5, is conjugate to $\mathrm{Aff}_5 = \mathbb{F}_5 \rtimes \mathbb{F}_5^*$, the group of

affine transformations of the affine line over the finite field $\mathbb{F}_5$, see [4, Ch. XI, §166, p. 215]. Let us show that this case cannot occur. Indeed, in the proof of Corollary 2.4 we have seen that the reduction of $f(x)$ modulo $\mathfrak{m}_w$ has one rational double root and three simple roots, whereas the integral model defined by $y^2 = f(x)$ is regular. It follows that over the maximal unramified extension of k_w the polynomial $f(x)$ is the product of three linear and one irreducible quadratic polynomials. Hence the image of the inertia subgroup in Aff_5 is generated by a cycle of length 2. This is a contradiction because the elements of order 2 in Aff_5 are always products of two cycles, as they are given by affine transformations of the form $x \mapsto -x + a$.

We conclude that the Galois group of $f(x)$ is S_5. The theorem now follows from Corollary 2.4 provided we check that the relevant class in $\mathrm{H}^1(k, A[2])$ is non-zero and unramified at w.

For this it is enough to prove that the corresponding k-torsor for $A[2]$ has no k-points but has a k_w^{un}-point. This torsor is the subset $Z_\lambda \subset \mathrm{R}_{L/k}(\mathbb{G}_{m,L})/\{\pm 1\}$ given by $z^2 = \lambda$. The natural surjective map

$$\mathrm{R}_{L/k}(\mathbb{G}_{m,L}) \longrightarrow \mathrm{R}_{L/k}(\mathbb{G}_{m,L})/\{\pm 1\}$$

is a torsor for μ_2. Thus $Z_\lambda(k)$ is the disjoint union of the images of k-points of the torsors $tz^2 = \lambda$ for $\mathrm{R}_{L/k}(\mu_2)$, where $t \in k^*$. Hence $Z_\lambda(k) \neq \emptyset$ if and only if $\lambda \in k^* L^{*2}$. Next, the group $\mathrm{H}^1(k_w^{\mathrm{un}}, \mu_2)$ consists of the classes of 1-cocycles defined by 1 and π, where π is a generator of $\mathfrak{m}_w$. Hence $Z_\lambda(k_w^{\mathrm{un}})$ is the disjoint union of the images of k_w^{un}-points of the torsors $z^2 = \lambda$ and $z^2 = \pi\lambda$ for $\mathrm{R}_{L/k}(\mu_2)$. By assumption there exists an $\varepsilon \in \{0, 1\}$ such that the valuation of $\pi^\varepsilon \lambda$ at each completion of L over w is even. Then the torsor for $\mathrm{R}_{L/k}(\mu_2)$ given by $z^2 = \pi^\varepsilon \lambda$ has a k_w^{un}-point, because any unit is a square as the residue field of k_w^{un} is separably closed of characteristic different from 2. It follows that $Z_\lambda(k_w^{\mathrm{un}}) \neq \emptyset$. $\square$

3 Galois theory of finite torsors

This section develops some ideas of Mazur and Rubin, see [21, Lemma 3.5].

We shall work with groups that are semi-direct products of a group G with a semisimple G-module M. Recall that a G-module M is *simple* if it has no G-submodules except 0 and M. A G-module M is *semisimple* if M is a direct sum of simple G-modules $M = \oplus_i M_i$. The simple G-modules M_i are called the *simple factors* of M. Their isomorphism types do not depend on the presentation of M as a direct sum. Indeed, one can characterise the simple factors of M as the simple G-modules that admit a non-zero map to M or from M.

Remark 3.1. If M is a semisimple G-module, then each G-submodule of M is a direct summand of M, see, e.g., [36, 20.2]. Furthermore, each G-submodule $N \subseteq M$ is semisimple and each simple factor of N is a simple factor of M. Similarly, each

quotient G-module M/N is semisimple and each simple factor of M/N is a simple factor of M.

Lemma 3.2. *Let G be a group and let M be a semisimple G-module such that the action of G on each simple factor of M is faithful. Let $H \subseteq M \rtimes G$ be a normal subgroup. Then*
(i) *either $H \subseteq M$ or $M \subseteq H$;*
(ii) *if G/H is abelian, then $M \subseteq H$.*

Proof. (i) Suppose that M is not contained in H. The subgroup $K = H \cap M$ is normal in $M \rtimes G$, thus K is a proper G-submodule of M. The quotient G-module $N = M/K \neq 0$ is semisimple by Remark 3.1. Moreover, each simple factor of N is a simple factor of M, hence N is a faithful G-module. We identify K with the kernel of the natural surjective group homomorphism $\rho : M \rtimes G \to N \rtimes G$. Then $\rho(H)$ and N are normal subgroups of $N \rtimes G$ such that $\rho(H) \cap N = \{1\}$, hence $\rho(H)$ and N centralise each other. Thus the image of H in G acts trivially on N. But N is a faithful G-module, so the image of H in G is trivial, hence $H \subseteq M$.

(ii) By the result of (i) we just need to show that the case $H \subsetneq M$ is not possible. Indeed, since H is normal in $M \rtimes G$, in this case H is a proper G-submodule of M, so that $G/H = N \rtimes G$, where $N = M/H \neq 0$. The same argument as in the proof of (i) shows that N is a faithful G-module. By assumption G/H is abelian, so G acts trivially on N, which is a contradiction. □

Let us now set up notation and terminology for this section.

Let k be a field, $\bar{k}$ be a separable closure of k and $\Gamma_k = \mathrm{Gal}(\bar{k}/k)$. Let M be a finite Γ_k-module such that the order of M is not divisible by $\mathrm{char}(k)$. We denote by $\varphi : \Gamma_k \to \mathrm{Aut}(M)$ the action of Γ_k on M. We identify M with the group of $\bar{k}$-points of a finite étale commutative group k-scheme $\mathcal{G}_M$. A cocycle $c : \Gamma_k \to M = \mathcal{G}_M(\bar{k})$ gives rise to a twisted action of Γ_k on $\mathcal{G}_M(\bar{k})$, defined as the original action of Γ_k on M followed by the translation by c. The quotient of $\mathrm{Spec}(\bar{k}[\mathcal{G}_M])$ by the twisted action is a k-torsor of $\mathcal{G}_M$. It comes equipped with a $\bar{k}$-point corresponding to the neutral element of $\mathcal{G}_M$. Conversely, suppose we are given a k-torsor Z for $\mathcal{G}_M$. For any $z_0 \in Z(\bar{k})$ the map $c : \Gamma_k \to M$ determined by the condition $c(\gamma)z_0 = {}^{\gamma}z_0$ is a cocycle $\Gamma_k \to M$. These constructions describe a bijection between $\mathrm{H}^1(k, M)$ and the set of isomorphisms classes of k-torsors for $\mathcal{G}_M$. See [28, Section 2.1], and also [3, Ch. 6]. For $\alpha \in \mathrm{H}^1(k, M)$ we denote by Z_α the torsor for $\mathcal{G}_M$ obtained by twisting $\mathcal{G}_M$ by a 1-cocycle representing α; such a torsor is well defined up to an isomorphism of $\mathcal{G}_M$-torsors.

Definition 3.3. Let K be the smallest extension of k such that Γ_K acts trivially on M. For $\alpha \in \mathrm{H}^1(k, M)$ let K_α be the smallest extension of k such that Γ_{K_α} acts trivially on $Z_\alpha(\bar{k})$. Write $G = \mathrm{Gal}(K/k)$ and $G_\alpha = \mathrm{Gal}(K_\alpha/k)$.

Note that $K \subset K_\alpha$. Write $W_\alpha = \mathrm{Gal}(K_\alpha/K)$, then there is an exact sequence

$$1 \longrightarrow W_\alpha \longrightarrow G_\alpha \xrightarrow{\varphi} G \longrightarrow 1. \tag{4}$$

The group G of Definition 3.3 is identified with $\varphi(\Gamma_k)$, which makes M a faithful G-module. Thus we can consider the semi-direct product $M \rtimes G$. Let $\alpha \in \mathrm{H}^1(k, M)$ be a class represented by a 1-cocycle $c : \Gamma_k \to M$. If Z_α is the twist of $\mathcal{G}_M$ by c, then $M \rtimes G$ acts on $Z_\alpha(\bar{k}) \cong \mathcal{G}_M(\bar{k}) \cong M$ by affine transformations, and Γ_k acts on $Z_\alpha(\bar{k})$ by the homomorphism $(c, \varphi) : \Gamma_k \to M \rtimes G$. By the definition of K_α this homomorphism factors through an injective homomorphism $G_\alpha \to M \rtimes G$. Since M is a trivial Γ_K-module, the restriction of α to W_α defines an injective homomorphism of G-modules $\tilde{\alpha} : W_\alpha \to M$, and we have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & W_\alpha & \longrightarrow & G_\alpha & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \tilde{\alpha}} & & \downarrow{\scriptstyle (c,\varphi)} & & \downarrow{\scriptstyle =} & & \\
1 & \longrightarrow & M & \longrightarrow & M \rtimes G & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

Let $R = \mathrm{End}_G(M) = \mathrm{End}_{\Gamma_k}(M)$ be the endomorphism ring of the Γ_k-module M.

Definition 3.4. Let N be an R-module. We say that $\alpha \in N$ is *non-degenerate* if the annihilator of α in R is zero, i.e., if $r \in R$ is such that $r\alpha = 0$, then $r = 0$. Equivalently, α is non-degenerate if $R\alpha \subset N$ is a free R-module.

Remark 3.5. If M is a simple G-module, then R is a division ring by Schur's lemma, hence a finite field by Wedderburn's theorem. In this case $\alpha \in \mathrm{H}^1(k, M)$ is non-degenerate if and only if $\alpha \neq 0$. When $M = \oplus_{i=1}^r M_i$, where the G-modules M_i are simple and pairwise non-isomorphic, $R = \oplus_{i=1}^r \mathrm{End}_G(M_i)$ is a direct sum of fields. We have $\mathrm{H}^1(k, M) = \oplus_{i=1}^r \mathrm{H}^1(k, M_i)$. If we write $\alpha = \sum \alpha_i$ with $\alpha_i \in \mathrm{H}^1(k, M_i)$, then α is non-degenerate if and only if each $\alpha_i \neq 0$. When $M = N^{\oplus r}$ for a simple G-module N, the ring R is the algebra of matrices of size r with entries in the field $\mathrm{End}_G(N)$. In this case $\alpha = \sum \alpha_i$ is non-degenerate if and only if $\alpha_1, \ldots, \alpha_r$ are linearly independent in the $\mathrm{End}_G(N)$-vector space $\mathrm{H}^1(k, N)$.

Proposition 3.6. *Let M be a semisimple Γ_k-module such that $\mathrm{H}^1(G, M) = 0$. Let $\alpha \in \mathrm{H}^1(k, M)$ be a class represented by a 1-cocycle c. The following conditions are equivalent:*

(i) *the map (c, φ) is an isomorphism of groups $G_\alpha \xrightarrow{\sim} M \rtimes G$;*
(ii) *the map $\tilde{\alpha} : W_\alpha \xrightarrow{\sim} M$ is an isomorphism of G-modules;*
(iii) *$\mathrm{H}^1(G_\alpha, M)$ is a free R-module generated by α;*
(iv) *α is non-degenerate in $\mathrm{H}^1(k, M)$.*

Proof. (i)⇒(ii) Since (c, φ) is an isomorphism, for each $m \in M$ there exists $\gamma \in G_\alpha$ such that $(c, \varphi)(\gamma) = (m, 1)$. Then γ goes to $1 \in G$ and hence $\gamma \in W_\alpha$ and

$c(\gamma) = \tilde{\alpha}(\gamma) = m$. It follows that the map $\tilde{\alpha} : W_\alpha \longrightarrow M$ is surjective. Since it is also injective by construction we conclude that it is an isomorphism of G-modules.

(ii)⇒(iii) Assume that $\tilde{\alpha} : W_\alpha \xrightarrow{\sim} M$ is an isomorphism of G-modules. Then $\mathrm{Hom}_G(W_\alpha, M)$ is a free R-module with generator $\tilde{\alpha}$. The inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(G, M) \to \mathrm{H}^1(G_\alpha, M) \to \mathrm{H}^1(W_\alpha, M)^G = \mathrm{Hom}_G(W_\alpha, M) \tag{5}$$

is an exact sequence of R-modules. By assumption $\mathrm{H}^1(G, M) = 0$, so the map $\mathrm{H}^1(G_\alpha, M) \to \mathrm{Hom}_G(W_\alpha, M)$ is injective. This map sends α to a generator $\tilde{\alpha}$ of $\mathrm{Hom}_G(W_\alpha, M) = R\tilde{\alpha}$, so it is also surjective, hence an isomorphism. We obtain that $\mathrm{H}^1(G_\alpha, M)$ is a free R-module generated by α.

(iii)⇒(iv) Assume that $\mathrm{H}^1(G_\alpha, M)$ is a free R-module with generator α. By the inflation-restriction exact sequence for $\Gamma_{K_\alpha} \subseteq \Gamma_k$ the map $\mathrm{H}^1(G_\alpha, M) \to \mathrm{H}^1(k, M)$ is injective, and so (iv) holds.

(iv)⇒(i) Suppose that α is non-degenerate in $\mathrm{H}^1(k, M)$ and assume for contradiction that the map (c, φ) is not an isomorphism. Since (c, φ) is injective by construction we conclude that it is not surjective. The intersection of the image of (c, φ) with M is then a proper G-submodule $\tilde{\alpha}(W_\alpha) \subsetneq M$. Since M is semisimple, $\tilde{\alpha}(W_\alpha)$ is a direct summand of M, see Remark 3.1. It follows that there exists a non-zero element $r \in R$ such that $r\tilde{\alpha}(W_\alpha) = 0$, so that $r\tilde{\alpha} = 0$ in $\mathrm{Hom}_G(W_\alpha, M)$. From 5 we see that $r\alpha = 0$ in $\mathrm{H}^1(G_\alpha, M)$. But this is a contradiction because the map $\mathrm{H}^1(G_\alpha, M) \to \mathrm{H}^1(k, M)$ is injective and α is non-degenerate in $\mathrm{H}^1(k, M)$. □

We record an amusing corollary of this proposition.

Corollary 3.7. *Under the assumptions of Proposition 3.6, let $\alpha, \beta \in \mathrm{H}^1(k, M)$ be non-degenerate. Then the associated torsors Z_α, Z_β for $\mathcal{G}_m$ are integral k-schemes. Furthermore, the following conditions are equivalent:*

(i) *there exists an $r \in R^*$ such that $r\alpha = \beta$;*

(ii) *$R\alpha = R\beta \subset \mathrm{H}^1(k, M)$;*

(iii) *Z_α and Z_β are isomorphic as abstract k-schemes.*

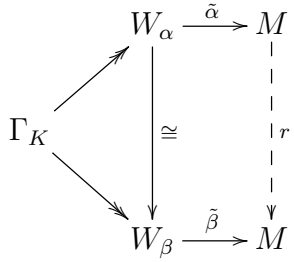
Proof. Let c be a cocycle representing α. By Proposition 3.6 the map $(c, \varphi) : G_\alpha \to M \rtimes G$ is an isomorphism. It follows that G_α acts transitively on $Z_\alpha(\bar{k})$, since already W_α acts (simply) transitively on $Z(\bar{k})$. Hence Z_α is integral. The same argument proves that Z_β is integral.

Let us now establish the equivalence of (i), (ii) and (iii). The implication (i)⇒(ii) is clear. Conversely, if $R\alpha = R\beta$, then there exist $r, s \in R$ such that $r\alpha = \beta$ and $\alpha = s\beta$. Then $sr\alpha = \alpha$ and $rs\beta = \beta$. Since α and β are non-degenerate we obtain that r and s are invertible in R, so (ii) implies (i).

We now show that (i) is equivalent to (iii). Assume (i) and take a cocycle $c : \Gamma_k \to M$ which represents α, then rc represents β. We identify $Z_\alpha(\bar{k})$ with $\mathcal{G}_m(\bar{k})$

such that Γ_k acts via its original action on $\mathcal{G}_m(\bar{k})$ followed by the translation by c. Then $Z_\beta(\bar{k})$ can be identified with $\mathcal{G}_m(\bar{k})$ such that Γ_k acts via its original action on $\mathcal{G}_m(\bar{k})$ followed by the translation by rc. Under these identifications the map $r : \mathcal{G}_m(\bar{k}) \to \mathcal{G}_m(\bar{k})$ becomes a Γ_k-equivariant map $Z_\alpha(\bar{k}) \to Z_\beta(\bar{k})$. Thus Z_α and Z_β are isomorphic as 0-dimensional k-schemes.

Finally, assume that Z_α and Z_β are isomorphic as k-schemes. Since α and β are non-degenerate we see from Proposition 3.6 that the maps $\tilde{\alpha} : W_\alpha \xrightarrow{\sim} M$ and $\tilde{\beta} : W_\beta \xrightarrow{\sim} M$ are isomorphisms of G-modules. The splitting fields K_α and K_β coincide as subfields of $\bar{k}$, so there exists an isomorphism of Γ_k-modules represented by the dotted arrow in the diagram



It is obtained as the action of an invertible element $r \in R^*$. It follows that $r\alpha$ and β have the same image in $\mathrm{H}^1(K, M)$. By assumption $\mathrm{H}^1(G, M) = 0$, hence the restriction-inflation exact sequence implies that the map $\mathrm{H}^1(k, M) \to \mathrm{H}^1(K, M)$ is injective. Thus $r\alpha = \beta$, as desired. $\square$

A continuous action of the pro-cyclic group $\hat{\mathbb{Z}}$ on a discrete module N is determined by the homomorphism $g : N \to N$ which is the action of the generator $1 \in \hat{\mathbb{Z}}$. There is a canonical isomorphism

$$\mathrm{H}^1(\hat{\mathbb{Z}}, N) \cong N/(g-1)$$

induced by sending the class of a cocycle ξ to the class of $\xi(1)$ in $N/(g-1)$.

An element $\gamma \in G_\alpha$ determines a map $f_\gamma : \hat{\mathbb{Z}} \to G_\alpha$ which sends 1 to γ, and hence an induced map

$$f_\gamma^* : \mathrm{H}^1(G_\alpha, M) \longrightarrow \mathrm{H}^1(\hat{\mathbb{Z}}, M) = M/(g-1).$$

Here we denote by g the image of γ in G (which acts on M) under the natural surjective map $G_\alpha \to G$. In particular, if $c : G_\alpha \to M$ is a cocycle representing $\alpha \in \mathrm{H}^1(G_\alpha, M)$, then $f_\gamma(\alpha)$ is equal to the class of $c(\gamma)$ in $M/(g-1)$.

Corollary 3.8. *In the assumptions of Proposition 3.6 let $\alpha \in \mathrm{H}^1(k, M)$ be non-degenerate. Take any $g \in G$ and any $x \in M/(g-1)$. Then g has a lifting $\gamma \in G_\alpha$ such that $f_\gamma(\alpha) = x$.*

Proof. Let $c : G_\alpha \to M$ be a cocycle representing α and let $m \in M$ be an element whose class in $M/(g-1)$ is x. By Proposition 3.6 the map $(c, \varphi) : G_\alpha \xrightarrow{\sim} M \rtimes G$ is an isomorphism. Hence there exists an element $\gamma \in G_\alpha$ such that $(c, \varphi)(\gamma) = (m, g)$. Then γ is a lifting of g and $c(\gamma) = m$ so that $f_\gamma(\alpha) = x$, as desired. $\square$

Corollary 3.9. *Let M be a semisimple Γ_k-module such that the induced action of G on each simple factor of M is faithful and $\mathrm{H}^1(G, M) = 0$. Let $\alpha \in \mathrm{H}^1(k, M)$ be non-degenerate. Then*
(i) *each subfield of K_α which is Galois over k is either contained in K or contains K;*
(ii) *each subfield of K_α which is abelian over k is contained in K.*

Proof. By Proposition 3.6 we have $G_\alpha \simeq M \rtimes G$. The desired result now follows directly from Lemma 3.2. $\square$

Until the end of this section we assume that k is a field of characteristic different from 2. Let $A_1, \ldots, A_r$ be abelian varieties satisfying conditions (a) and (b) of §2 and let $A = \prod_{i=1}^r A_i$. Let K_i be the splitting field of $A_i[2]$. Assume that condition (e) of §2 holds, i.e., the fields K_i are linearly disjoint over k. Let $G_i = \mathrm{Gal}(K_i/k)$. The compositum $K = K_1 \ldots K_r$ is the field of definition of $A[2]$.

We now present two applications of the results above. In the first one we consider the semisimple Γ_k-module $M = A[2] = \oplus_{i=1}^r A_i[2]$.

Proposition 3.10. *Suppose that abelian varieties $A_1, \ldots, A_r$ satisfy conditions (a) and (b), and that condition (e) holds. Let Z_i be a non-trivial k-torsor for $A_i[2]$, for each $i = 1, \ldots, r$, and let $Z = \prod_{i=1}^r Z_i$. Let L be the étale k-algebra $k[Z]$, so that $Z \cong \mathrm{Spec}(L)$. Then L is a field which contains no quadratic extension of k.*

Proof. Let $M = A[2]$ and let $\alpha \in \mathrm{H}^1(k, M)$ be the class of Z. Write $\alpha = \sum_{i=1}^r \alpha_i$, where each $\alpha_i \in \mathrm{H}^1(k, A_i[2])$ is non-zero. By condition (a) each $A_i[2]$ is simple and hence M is semisimple with simple factors $A_1[2], ..., A_r[2]$. By condition (e) the fields $K_1, \ldots, K_r$ are linearly disjoint over k, so that the Galois group $G = \mathrm{Gal}(K/k)$ is the product $G = \prod_{i=1}^r G_i$, and the $A_i[2]$ are pairwise non-isomorphic Γ_k-modules. From Remark 3.5 we see that α is non-degenerate.

For each $i = 1, \ldots, r$ we have $A_i[2]^{G_i} = 0$ and $\mathrm{H}^1(G_i, A_i[2]) = 0$ by conditions (a) and (b). The inflation-restriction exact sequence for $G_i \subset G$ then gives $\mathrm{H}^1(G, A_i[2]) = 0$, and so $\mathrm{H}^1(G, M) = 0$. Let $c : \Gamma_k \to M$ be a cocycle representing α. By Proposition 3.6 the map $(c, \varphi) : G_\alpha \xrightarrow{\sim} M \rtimes G$ is an isomorphism. Let $s : G \to G_\alpha$ be the section corresponding to the canonical section $G \to M \rtimes G$ under the isomorphism (c, φ).

By Corollary 3.7 the scheme Z_α is integral, and hence $L = k[Z_\alpha]$ is a field, whose Galois closure is K_α by definition. Moreover, $L \cong (K_\alpha)^{s(G)}$. If L contains a quadratic extension of k, then $s(G)$ is contained in a normal subgroup $H \subset G_\alpha$ of index 2. Since s is a section, the induced homomorphism $H \to G$ is surjective, so its kernel is

a G-submodule of M which is a subgroup of M of index 2. But this is a contradiction since M is semisimple and the simple factors $A_i[2]$ of M have size 4. $\square$

In the second application we consider the semisimple module $M = A_1[2]^{\oplus r}$.

Proposition 3.11. *Suppose that abelian varieties $A_1, \dots, A_r$ satisfy conditions (a) and (b), and that condition (e) holds. Let $M = A_1[2]^{\oplus r}$ be a direct sum of copies of $A_1[2]$ and let $\alpha \in \mathrm{H}^1(k, M)$ be non-degenerate. Then the fields $(K_1)_\alpha, K_2, \dots, K_r$ are linearly disjoint.*

Proof. Write $E = (K_1)_\alpha \cap K_2 \dots K_r$. In view of condition (e) it is enough to show that $E = k$. Indeed, E is a Galois subfield of $(K_1)_\alpha$, so by Corollary 3.9 we have $E \subset K_1$ or $K_1 \subset E$. In the first case $E = k$ because E is contained in $K_1 \cap K_2 \dots K_r = k$, where the equality holds by condition (e). By the same condition the second case cannot actually occur, because then $K_1 \subset E \subset K_2 \dots K_r$ which contradicts the linear disjointness of $K_1, \dots, K_r$. $\square$

4 Kummer map over a local field

Let A be an abelian variety over a local field k of characteristic zero. The Kummer exact sequence gives rise to a map $\delta : A(k) \to \mathrm{H}^1(k, A[2])$, called the Kummer map. For $x \in A(k)$ choose $\bar{x} \in A(\bar{k})$ such that $2\bar{x} = x$. Then $\delta(x)$ is represented by the cocycle that sends $\gamma \in \Gamma_k$ to ${}^\gamma\bar{x} - \bar{x} \in A[2]$.

The Weil pairing is a non-degenerate pairing of Γ_k-modules $A[2] \times A^t[2] \to \mathbb{Z}/2$. The induced pairing on cohomology followed by the local invariant of local class field theory gives a non-degenerate pairing of finite abelian groups [23, Cor. I.2.3]

$$\mathrm{H}^1(k, A[2]) \times \mathrm{H}^1(k, A^t[2]) \longrightarrow \mathrm{Br}(k)[2] \xrightarrow{\mathrm{inv}} \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

The local Tate duality implies that $\delta(A(k))$ and $\delta(A^t(k))$ are the orthogonal complements to each other under this pairing (see, e.g., the first commutative diagram in the proof of [23, I.3.2]).

When A is principally polarised, we combine the last pairing with the principal polarisation $A \xrightarrow{\sim} A^t$ and obtain a non-degenerate symmetric pairing

$$\mathrm{inv}(\alpha \cup \beta) : \mathrm{H}^1(k, A[2]) \times \mathrm{H}^1(k, A[2]) \longrightarrow \mathrm{Br}(k)[2] \xrightarrow{\mathrm{inv}} \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

It is well known that $\delta(A(k))$ is a maximal isotropic subspace of $\mathrm{H}^1(k, A[2])$, see [25, Prop. 4.11]. Note that the pairing $\mathrm{inv}(\alpha \cup \beta)$ is also defined for $k = \mathbb{R}$ and the above statements carry over to this case, cf. [23, Thm. I.2.13 (a), Remark I.3.7].

Let us recall a well known description of $\delta(A(k))$ when A has good reduction. Let κ be the residue field of k, and assume $\mathrm{char}(\kappa) = \ell \neq 2$. Then $\delta(A(k))$ is the

unramified subgroup

$$\mathrm{H}^1_{\mathrm{nr}}(k, A[2]) = \mathrm{Ker}[\,\mathrm{H}^1(\Gamma_k, A[2]) \longrightarrow \mathrm{H}^1(I, A[2])\,],$$

where $I \subset \Gamma_k$ is the inertia subgroup. By Néron–Ogg–Shafarevich the inertia acts trivially on $A[2]$, so that $\mathrm{H}^1_{\mathrm{nr}}(k, A[2]) = \mathrm{H}^1(\kappa, A[2])$. The absolute Galois group $\mathrm{Gal}(\bar{\kappa}/\kappa) = \Gamma_k/I$ is isomorphic to $\hat{\mathbb{Z}}$ with the Frobenius element as a topological generator. Thus we have a canonical isomorphism

$$\delta(A(k)) = A[2]/(\mathrm{Frob} - 1). \tag{6}$$

Since $\hat{\mathbb{Z}}$ has cohomological dimension 1, the spectral sequence

$$\mathrm{H}^p(\hat{\mathbb{Z}}, \mathrm{H}^q(I, A[2])) \Rightarrow \mathrm{H}^{p+q}(k, A[2])$$

gives rise to the exact sequence

$$0 \to A[2]/(\mathrm{Frob} - 1) \to \mathrm{H}^1(k, A[2]) \to \mathrm{Hom}(I, A[2])^{\mathrm{Frob}} \to 0.$$

The maximal abelian pro-2-quotient of I is isomorphic to $\mathbb{Z}_2$, and Frob acts on it by multiplication by ℓ. Thus $\mathrm{Hom}(I, A[2]) = A[2]$ with the natural action of Frob, so that

$$\mathrm{Hom}(I, A[2])^{\mathrm{Frob}} = A[2]^{\mathrm{Frob}} = \mathrm{Ker}(\mathrm{Frob} - 1 : A[2] \to A[2]).$$

It follows that the dimension of the $\mathbb{F}_2$-vector space $A[2]/(\mathrm{Frob} - 1)$ equals the dimension of $A[2]^{\mathrm{Frob}}$, and therefore

$$\dim \mathrm{H}^1(k, A[2]) = 2 \dim A[2]/(\mathrm{Frob} - 1). \tag{7}$$

Let us now return to the general case, where A does not necessarily have good reduction. If F/k is a quadratic extension, we write $\delta^F : A^F(k) \to \mathrm{H}^1(k, A[2])$ for the Kummer map of A^F. In the rest of this section we summarise some known results relating δ, δ^F and the norm map $\mathrm{N} : A(F) \to A(k)$.

Lemma 4.1. *We have* $\delta(\mathrm{N}(A(F))) = \delta(A(k)) \cap \delta^F(A^F(k)) \ \subset\ \mathrm{H}^1(k, A[2])$.

Proof. Cf. [15, Prop. 7] or [22, Prop. 5.2]. Let $\chi : \Gamma_k \to \{\pm 1\}$ be the quadratic character associated to F. We choose $\sigma \in \Gamma_k$ such that $\chi(\sigma) = -1$.

Suppose that $x \in A(k)$ and $y \in A^F(k)$ are such that $\delta(x) = \delta^F(y)$. Using the embedding $A^F(k) \subset A(F)$ we can consider y as a point in $A(F)$ such that ${}^{\sigma}y = -y$. If $\bar{y} \in A(\bar{k})$ is such that $2\bar{y} = y$, then $\delta^F(y)$ is represented by the cocycle that sends $\gamma \in \Gamma_k$ to

$$\chi(\gamma)\ {}^{\gamma}\bar{y} - \bar{y} = {}^{\gamma}\bar{y} - \chi(\gamma)\bar{y} \in A[2].$$

Since $\delta(x) = \delta^F(y)$ we can choose $\bar{x} \in A(\bar{k})$ such that $2\bar{x} = x$ and such that

$$\chi(\gamma)\ {}^{\gamma}\bar{y} - \bar{y} = {}^{\gamma}\bar{x} - \bar{x}.$$

We deduce that ${}^{\gamma}(\bar{x}-\bar{y}) = \bar{x} - \chi(\gamma)\bar{y}$ for every $\gamma \in \Gamma_k$. It follows that $\bar{x}-\bar{y} \in A(F)$ and ${}^{\sigma}(\bar{x}-\bar{y}) = \bar{x}+\bar{y}$. Therefore, $x = 2\bar{x} = \mathrm{N}(\bar{x}-\bar{y})$ is a norm from $A(F)$.

Conversely, suppose that $x = \mathrm{N}(z) = z + {}^{\sigma}z$ for some $z \in A(F)$. Let $y = {}^{\sigma}z - z$. Then $y \in A^F(k)$ and we claim that $\delta(x) = \delta^F(y)$. Choose $\bar{x} \in A(\bar{k})$ such that $2\bar{x} = x$ and set $\bar{y} = \bar{x} - z$. Then $2\bar{y} = x - 2z = y$ and we have $\bar{x} - \bar{y} = z$ and $\bar{x} + \bar{y} = {}^{\sigma}z$. It follows that for each $\gamma \in \Gamma_k$ we have ${}^{\gamma}(\bar{x}-\bar{y}) = \bar{x} - \chi(\gamma)\bar{y}$, and hence

$$ {}^{\gamma}\bar{x} - \bar{x} = {}^{\gamma}\bar{y} - \chi(\gamma)\bar{y}. $$

This implies $\delta(x) = \delta^F(y)$, as desired. □

Lemma 4.2. *Let A be a principally polarised abelian variety over k with bad reduction such that the number of geometric connected components of the Néron model of A is odd. If F is an unramified quadratic extension of k, then $\delta(A(k)) = \delta^F(A^F(k))$.*

Proof. Since A is principally polarised, it is isomorphic to its dual abelian variety. It follows from [18, Prop. 4.2, Prop. 4.3] that the norm map $\mathrm{N} : A(F) \to A(k)$ is surjective. By Lemma 4.1 we see that $\delta(A(k)) \subset \delta^F(A^F(k))$. Since F is unramified, the quadratic twist A^F also satisfies the assumptions of the lemma, and the same argument applied to A^F gives the opposite inclusion. □

Lemma 4.3. *Assume that the residue characteristic of k is not 2. If A is an abelian variety over k with good reduction and F is a ramified quadratic extension of k, then $\delta(A(k)) \cap \delta^F(A^F(k)) = 0$.*

Proof. In this case we have $\mathrm{N}(A(F)) = 2A(k)$. If $\dim(A) = 1$ this is proved in [22, Lemma 5.5 (ii)], and the same proof works in the general case. It remains to apply Lemma 4.1. □

5 Selmer group and Cassels–Tate pairing

Let A be an abelian variety over a field k of characteristic zero. Let $\mathrm{NS}\,(\overline{A})$ be the Néron–Severi group of $\overline{A}$. The dual abelian variety A^t represents the functor Pic^0_A. In particular, we have an exact sequence of Γ_k-modules

$$ 0 \longrightarrow A^t(\bar{k}) \longrightarrow \mathrm{Pic}(\overline{A}) \longrightarrow \mathrm{NS}\,(\overline{A}) \longrightarrow 0. \tag{8} $$

The antipodal involution $\iota_A = [-1] : A \to A$ induces an action of $\mathbb{Z}/2$ on $\mathrm{Pic}(\overline{A})$ which turns (8) into an exact sequence of $\mathbb{Z}/2$-modules. The induced action on $\mathrm{NS}\,(\overline{A})$ is trivial, see [33, p. 119]. The involution ι_A induces the involution ι_{A^t} on A^t. Since $A^t(\bar{k})$ is divisible, we obtain $\mathrm{H}^1(\mathbb{Z}/2, A^t(\bar{k})) = 0$. Thus the long exact sequence of cohomology gives an exact sequence

$$ 0 \longrightarrow A^t[2] \longrightarrow \mathrm{Pic}(\overline{A})^{[-1]^*} \longrightarrow \mathrm{NS}\,(\overline{A}) \longrightarrow 0, \tag{9} $$

cf. [24, Section 3.2]. The group $\mathrm{NS}\,(\overline{A})^{\Gamma_k}$ is canonically isomorphic to the group $\mathrm{Hom}(A, A^t)^{\mathrm{sym}}$ of self-dual k-homomorphisms of abelian varieties $A \to A^t$. A polarisation on A is an element $\lambda \in \mathrm{NS}\,(\overline{A})^{\Gamma_k}$. The polarisation is called principal if the associated morphism $\varphi_\lambda : A \to A^t$ is an isomorphism. Following [26] and [24] we shall write c_λ for the image of λ under the differential $\mathrm{NS}\,(\overline{A})^{\Gamma_k} \to \mathrm{H}^1(k, A^t[2])$ attached to (9). For example, if A is the Jacobian of a curve C and λ is the canonical principal polarisation of A, then c_λ is the image of the class of the theta characteristics torsor of C under the isomorphism $\varphi_\lambda : \mathrm{H}^1(k, A[2]) \xrightarrow{\sim} \mathrm{H}^1(k, A^t[2])$; see [24, Thm. 3.9].

Lemma 5.1. *Let A be an abelian variety over k with polarisation λ. Then c_λ belongs to the kernel of the restriction map $\mathrm{H}^1(k, A^t[2]) \to \mathrm{H}^1(K, A^t[2])$ for $K = k(A[2])$.*

Proof. Poonen and Rains [24, Section 2.1] associated to any $\mathbb{F}_2$-vector space M the group of invertible elements of the quotient $\bigwedge M / \bigwedge^{\geq 3} M$, where $\bigwedge M$ is the exterior algebra of M over $\mathbb{F}_2$. Let us denote it by $\widetilde{M}$. The homomorphism $\widetilde{M} \to M$ given by the first graded factor gives rise to the exact sequence of $\mathbb{F}_2$-vector spaces

$$0 \longrightarrow \bigwedge^2 M \longrightarrow \widetilde{M} \longrightarrow M \longrightarrow 0, \tag{10}$$

see [24], Remark 2.3 (b). If M is a Γ_k-module, then (10) is also an exact sequence of Γ_k-modules. The exact sequence dual to (10) for $M = A[2]$ fits into the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & A^t[2] & \to & \mathrm{Pic}(\overline{A})^{[-1]^*} & \to & \mathrm{NS}\,(\overline{A}) & \to & 0 \\ & & || & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{Hom}(A[2], \mathbb{F}_2) & \to & \mathrm{Hom}(\widetilde{A[2]}, \mathbb{F}_2) & \to & \mathrm{Hom}(\bigwedge^2 A[2], \mathbb{F}_2) & \to & 0 \end{array} \tag{11}$$

see [24], Prop. 3.2 and diagram (16). The left hand vertical map in (11) is induced by the Weil pairing $A[2] \times A^t[2] \to \mathbb{F}_2$.

Consider (11) as a diagram of Γ_K-modules. The commutativity of (11) implies that the differential $\mathrm{NS}\,(\overline{A})^{\Gamma_K} \to \mathrm{H}^1(K, A^t[2])$ defined by the upper row factors through the differential defined by the lower row

$$\mathrm{Hom}(\bigwedge^2 A[2], \mathbb{F}_2)^{\Gamma_K} \longrightarrow \mathrm{H}^1(K, \mathrm{Hom}(A[2], \mathbb{F}_2)).$$

But this differential is zero, since Γ_K acts trivially on $A[2]$ and hence on all the terms of the lower row of (11). $\square$

Remark 5.2. The $\mathbb{F}_2$-vector space $\mathrm{Hom}(\widetilde{M}, \mathbb{F}_2)$ can be identified with the space of *quadratic functions* $M \to \mathbb{F}_2$, see [24, Cor. 2.2]. Under this identification the map $\mathrm{Hom}(\widetilde{M}, \mathbb{F}_2) \to \mathrm{Hom}(\bigwedge^2 M, \mathbb{F}_2)$ sends a quadratic function f to its associated alternating bilinear form $f(x+y)+f(x)+f(y)$, and the kernel of this map is the space

of linear functions $M \to \mathbb{F}_2$. In the case $M = A[2]$ the element $c_\lambda \in H^1(k, A[2])$ vanishes if and only if the pairing $A[2] \times A[2] \to \mathbb{Z}/2$ induced by λ from the Weil pairing admits a Galois invariant *quadratic enhancement*. In particular, $c_\lambda = 0$ when the Galois action on $A[2]$ is trivial, which is essentially the content of Lemma 5.1.

Now let k be a number field. For a place v of k let

$$\mathrm{loc}_v : \mathrm{H}^1(k, A[2]) \longrightarrow \mathrm{H}^1(k_v, A[2])$$

be the natural restriction map. The 2-Selmer group $\mathrm{Sel}_2(A) \subset \mathrm{H}^1(k, A[2])$ is defined as the set of elements x such that $\mathrm{loc}_v(x) \in \delta(A(k_v))$ for all places v of k. If v is a place of good reduction, then the restricted map

$$\mathrm{loc}_v : \mathrm{Sel}_2(A) \longrightarrow A[2]/(\mathrm{Frob}_v - 1)$$

is the map provided by (6). For every quadratic extension F/k we have $A^F[2] = A[2]$ and hence we may consider the 2-Selmer groups $\mathrm{Sel}_2(A^F)$ of all quadratic twists A^F as subgroups of $\mathrm{H}^1(k, A[2])$. We have the well known exact sequence

$$0 \longrightarrow A(k)/2 \longrightarrow \mathrm{Sel}_2(A) \longrightarrow Ш(A)[2] \longrightarrow 0. \tag{12}$$

The Cassels–Tate pairing is a bilinear pairing

$$\langle , \rangle : Ш(A) \times Ш(A^t) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

If $Ш(A)$ is finite, then $Ш(A^t)$ is finite too and the Cassels–Tate pairing is non-degenerate, see [23, Thm. I.6.26]. A polarisation λ on A induces a homomorphism $\varphi_{\lambda *} : Ш(A) \to Ш(A^t)$.

Proposition 5.3. *Let A be an abelian variety over a number field k with a principal polarisation λ. Then condition (b) of § 2 implies that the Cassels–Tate pairing $\langle x, \varphi_{\lambda *} y \rangle$ on $Ш(A)\{2\}$ is alternating. In particular, if the 2-primary subgroup $Ш(A)\{2\}$ is finite, then the cardinality of $Ш(A)[2]$ is a square.*

Proof. By a result of Poonen and Stoll we know that $c_\lambda \in \mathrm{Sel}_2(A^t)$, see [26, Cor. 2]. If c'_λ is the image of c_λ in $Ш(A^t)[2]$, then [26, Thm. 5] says that $\langle x, \varphi_{\lambda *} x + c'_\lambda \rangle = 0$ for any $x \in Ш(A)$. Thus it is enough to prove that $c_\lambda = 0$. Lemma 5.1 implies that c_λ belongs to the image of the inflation map $\mathrm{H}^1(G, A^t[2]) \to \mathrm{H}^1(k, A^t[2])$, where $G = \mathrm{Gal}(k(A[2])/k)$ is the image of $\Gamma_k \to \mathrm{GL}(A[2])$. Since λ is a principal polarisation, φ_λ induces an isomorphism of Γ_k-modules $A[2] \xrightarrow{\sim} A^t[2]$. Now condition (b) implies $\mathrm{H}^1(G, A^t[2]) = \mathrm{H}^1(G, A[2]) = 0$, hence $c_\lambda = 0$. $\square$

6 Kummer varieties

Let A be an abelian variety over a field k of characteristic different from 2. Let Z be a k-torsor for the group k-scheme $A[2]$. Recall that the 2-covering $f : Y \to A$ associated to Z is a k-torsor for A defined as the quotient of $A \times_k Z$ by the diagonal action of $A[2]$. In other words, Y is the twisted form of A by Z with respect to the action of $A[2]$ by translations. The morphism f is induced by the first projection, and we have $Z = f^{-1}(0)$. Let L be the étale k-algebra $k[Z]$, so that $Z \cong \mathrm{Spec}(L)$.

Let $\tilde{Y}$ be the blowing-up of Z in Y. The antipodal involution $\iota_A : A \to A$ induces the map $(\iota_A, \mathrm{Id}) : A \times_k Z \to A \times_k Z$ which commutes with the action of $A[2]$ and hence induces an involution $\iota_Y : Y \to Y$. As ι_Y fixes $Z = f^{-1}(0) \subseteq Y$ it extends to an involution $\iota_{\tilde{Y}} : \tilde{Y} \to \tilde{Y}$ whose fixed point set is precisely the exceptional divisor. It is easy to see that the quotient $X = \mathrm{Kum}(Y) = \tilde{Y}/\iota_{\tilde{Y}}$ is smooth. We call X the *Kummer variety* attached to A and Z. We note that the branch locus of $\tilde{Y} \to X$ is $Z \times_k \mathbb{P}^{d-1}_k$, where $d = \dim(A)$.

Let F be an extension of k of degree at most 2. Recall that A^F denotes the quadratic twist of A by F, that is, the abelian variety over k obtained by twisting A by the quadratic character of F with respect to the action of μ_2 via the antipodal involution ι_A. Similarly, Y^F denotes the quadratic twist of Y with respect to the involution ι_Y, see §1. Since ι_A commutes with translations by the elements of $A[2]$, the quadratic twist Y^F of Y is a k-torsor for A^F. We have a natural embedding $i_F : Z \to Y^F$. Then $\tilde{Y}^F$, defined as the blowing-up of $i_F(Z)$ in Y^F, is the quadratic twist of $\tilde{Y}$ by the quadratic character of F with respect to the action of μ_2 on $\tilde{Y}$ via $\iota_{\tilde{Y}}$. We can also consider $\tilde{Y}^F$ as a quadratic twist of the 2-covering $\tilde{Y} \to X$, and consequently consider every $\tilde{Y}^F$ as a (ramified) 2-covering of X. It is clear that Y^F, and hence X, has a K-point for any extension K/k such that α is in the kernel of the natural map $\mathrm{H}^1(k, A[2]) \to \mathrm{H}^1(K, A^F)$.

We now recall a construction from [31, §5]. Let $\mathcal{Y}$ be the quotient of $\tilde{Y} \times \mathbb{G}_{m,k}$ by the action of μ_2 in which the generator $-1 \in \mu_2$ acts as the multiplication by -1 on $\mathbb{G}_m$ and by $\iota_{\tilde{Y}}$ on $\tilde{Y}$. The fibre of $\mathcal{Y}$ over $a \in \mathbb{G}_{m,k}(k)$ can be naturally identified with the quadratic twist $\tilde{Y}^F$ where $F = k(\sqrt{a})$. As in [31, §5] one may consider a smooth compactification $\mathcal{Y} \subset \mathcal{X}$ that fits into the commutaive diagram

$$\begin{array}{ccc} \mathcal{Y} & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow p \\ \mathbb{G}_{m,k} & \longrightarrow & \mathbb{P}^1_k \end{array}$$

Proposition 6.1. *Let $A = \prod_{i=1}^r A_i$ be a product of abelian varieties over k satisfying conditions (a) and (b) of §2 such that condition (e) holds. Assume in addition that the class $\alpha \in \mathrm{H}^1(k, A[2])$ of Z is non-degenerate (see Definition 3.4). Then the vertical Brauer group of $\mathcal{X}$ over $\mathbb{P}^1_k$ is the image of $\mathrm{Br}(k)$ in $\mathrm{Br}(\mathcal{X})$.*

Proof. Let t be a coordinate on $\mathbb{P}^1$ invertible on $\mathbb{G}_{m,k} \subset \mathbb{P}^1_k$. According to [31, Thm. 3] the vertical Brauer group of $\mathcal{X}$ is generated by the image of $\mathrm{Br}(k)$ and the pullbacks of the classes $(t, c) \in \mathrm{Br}(k(\mathbb{P}^1_k))$, where $c \in k^*$ becomes a square in $L = k[Z]$. By Proposition 3.10 the element c is already a square in k, hence the result. □

Proposition 6.2. *Let k be a number field. Let $A = \prod_{i=1}^r A_i$ be a product of abelian varieties over k satisfying conditions (a) and (b) of §2, and such that conditions (e) and (f) hold. Let Z be a k-torsor for $A[2]$ whose class $\alpha \in \mathrm{H}^1(k, A[2])$ is unramified at the places $w_1, \ldots, w_r$ and non-degenerate. Let Y be the attached 2-covering of A and let $X = \mathrm{Kum}(Y)$. If X is everywhere locally soluble, then there exists an extension F of k of degree at most 2 such that Y^F is everywhere locally soluble and F is split at $w_1, \ldots, w_r$.*

Proof. This is proved in [31, Lemma 6], but we give a detailed proof for the convenience of the reader. Let w be one of the places $w_1, \ldots, w_r$. By assumption $\alpha \in \mathrm{H}^1(k, A[2])$ goes to zero under the composed map

$$\mathrm{H}^1(k, A[2]) \longrightarrow \mathrm{H}^1(k_w, A[2]) \longrightarrow \mathrm{H}^1(k_w^{\mathrm{nr}}, A[2]).$$

Hence the class $[Y] \in \mathrm{H}^1(k, A)[2]$ goes to zero under the composed map

$$\mathrm{H}^1(k, A) \longrightarrow \mathrm{H}^1(k_w, A) \longrightarrow \mathrm{H}^1(k_w^{\mathrm{nr}}, A). \tag{13}$$

The second arrow in (13) is the restriction map $\mathrm{H}^1(\Gamma_{k_w}, A) \to \mathrm{H}^1(I_w, A)$, where $\Gamma_{k_w} = \mathrm{Gal}(\overline{k_w}/k_w)$ and $I_w \subset \Gamma_{k_w}$ is the inertia subgroup. By the inflation-restriction sequence we see that the class $[Y \times_k k_w] \in \mathrm{H}^1(\Gamma_{k_w}, A)$ belongs to the subgroup $\mathrm{H}^1(\Gamma_{k_w}/I_w, A(k_w^{\mathrm{nr}}))$. Let $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_w)$ be the Néron model of $A \times_k k_w$. By [23, Prop. I.3.8] we have an isomorphism

$$\mathrm{H}^1(\Gamma_{k_w}/I_w, A(k_w^{\mathrm{nr}})) = \mathrm{H}^1(\Gamma_{k_w}/I_w, \pi_0(\mathcal{A} \times_{\mathcal{O}_w} \mathbb{F}_w)),$$

where $\pi_0(\mathcal{A} \times_{\mathcal{O}_w} \mathbb{F}_w)$ is the group of connected components of the special fibre of $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_w)$. Since $2[Y] = 0$, condition (f) implies that $[Y \times_k k_w] = 0$, hence Y has a k_w-point $P_w \in Y(k_w)$. We view P_w as a point $(P_w, 1) \in \mathcal{Y}$ above $1 \in \mathbb{G}_{m,k}(k) \subset \mathbb{P}^1_k$.

For each place v of k and for each point $Q_v \in X(k_v)$ there exists an extension F_v/k_v of degree at most 2 such that Q_v lifts to $\tilde{Y}^{F_v}(k_v)$. Since X is everywhere locally soluble, we can use this observation to extend the collection of local points $(P_w, 1)$, $w \in \{w_1, \ldots, w_r\}$, to an adelic point $(P_v) \in \mathcal{Y}(\mathbb{A}_k) \subseteq \mathcal{X}(\mathbb{A}_k)$. The fibration $\mathcal{X} \to \mathbb{P}^1_k$ has only two bad fibres at 0 and ∞ (both of which are geometrically split). By Proposition 6.1 the vertical Brauer group of $\mathcal{X}$ over $\mathbb{P}^1_k$ is generated by the image of $\mathrm{Br}(k)$, therefore the desired result can now be obtained by applying the fibration method. More precisely, one proceeds as in the proof of [7, Thm. A]. (For recent reference apply [11, Thm. 9.17] with $B = 0$ and $U = \mathbb{G}_{m,k}$, which is justified in the

light of [11, Thm. 9.11].) We obtain that there exists an adelic point $(P'_v) \in \mathcal{X}(\mathbb{A}_k)$ arbitrarily close to (P_v) such that the image of (P'_v) in $\mathbb{P}^1_k(\mathbb{A}_k)$ is a k-point. Let us call it a. By the construction of (P_v) we can assume that $a \in \mathbb{G}_{m,k}(k)$ and that a is arbitrarily close to 1 in the w-adic topology for $w \in \{w_1, ..., w_r\}$. The quadratic extension $F = k(\sqrt{a})$ now satisfies the desired properties. $\square$

7 Proof of Theorem 2.3

Suppose that our Kummer variety is $X = \mathrm{Kum}(Y)$, where Y is the k-torsor for A defined by a class $\alpha \in \mathrm{H}^1(k, A[2])$. To prove the existence of a k-point on X it is enough to find a quadratic extension F of k such that α goes to 0 in $\mathrm{H}^1(k, A^F)$. We write $\alpha = \sum_{i=1}^r \alpha_i$, where $\alpha_i \in \mathrm{H}^1(k, A_i[2])$ is non-zero for each $i = 1, \ldots, r$. Let $K_i = K(A_i[2])$. For each $i = 1, \ldots, r$ we fix $g_i, h_i \in \mathrm{Gal}(K_i/k)$ satisfying conditions (c) and (d), respectively, for A_i.

By Proposition 6.2 there is a quadratic extension F of k split at $w_1, \ldots, w_r$ such that $\alpha \in \mathrm{Sel}_2(A^F)$. Replacing A with A^F we can assume without loss of generality that $\alpha \in \mathrm{Sel}_2(A)$. By doing so we preserve conditions (a), (b), (c), (d), (e) and (g) that are not affected by quadratic twisting. The extension F/k is split at $w_1, \ldots, w_r$, so replacing A by A^F also preserves condition (f) for every A_i.

Let S_0 be the set of places of k that contains all the Archimedean places and the places above 2.

Lemma 7.1. *Let S be the set of places of k which is the union of S_0 and all the places of bad reduction of A excluding $w_1, \ldots, w_r$. For each $i = 1, \ldots, r$ let $\alpha_i \in \mathrm{Sel}_2(A_i)$ be non-zero. Let $\beta \in \mathrm{Sel}_2(A_1)$ be a non-zero class such that $\beta \neq \alpha_1$. Then there exists a $q \in k^*$ such that $\mathfrak{q} = (q)$ is a prime ideal of k with the following properties:*

1. *all the places in S (including the Archimedean places) are split in $F = k(\sqrt{q})$, in particular, $\mathfrak{q} \notin S$;*
2. *A has good reduction at $\mathfrak{q}$;*
3. *$\mathrm{Frob}_\mathfrak{q}$ acts on $A_1[2]$ as g_1;*
4. *$\mathrm{Frob}_\mathfrak{q}$ acts on $A_i[2]$ as h_i, for each $i \neq 1$;*
5. *$\mathrm{loc}_\mathfrak{q}(\alpha_1) = 0$, but $\mathrm{loc}_\mathfrak{q}(\beta) \neq 0$.*

Proof. We adapt the arguments from the proof of [21, Prop. 5.1].
Let $M = A_1[2]^{\oplus 2}$ be the direct sum of two copies of $A_1[2]$. Let

$$\alpha = \alpha_1 + \beta \in \mathrm{H}^1(k, A_1[2]) \oplus \mathrm{H}^1(k, A_1[2]) = \mathrm{H}^1(k, M).$$

The splitting field of M is K_1 and the Galois action on M factors through $G_1 = \mathrm{Gal}(K_1/k)$. Let $(K_1)_\alpha$ and $(G_1)_\alpha$ be as in Definition 3.3. By Corollary 3.8 we can find a lift $\gamma \in (G_1)_\alpha$ of $g \in G_1$ such that the associated map

$$f_\gamma : \mathrm{H}^1(k, M) \longrightarrow M/(g-1) = \big(A_1[2]/(g-1)\big) \oplus \big(A_1[2]/(g-1)\big) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

sends α to the class $(0,1) \in \mathbb{Z}/2 \oplus \mathbb{Z}/2$. That is, $f_\gamma(\alpha_1, 0) = 0$, whereas $f_\gamma(0, \beta) \neq 0$.

The fields $(K_1)_\alpha, K_2, \dots, K_r$ are Galois extensions of k that are linearly disjoint by condition (e) and Proposition 3.11. Let $\mathcal{K}$ be the compositum of $(K_1)_\alpha, K_2, \dots, K_r$. This is a Galois extension of k with the Galois group $\mathrm{Gal}(\mathcal{K}/k) = (G_1)_\alpha \times \prod_{i=2}^r G_i$.

Let the modulus $\mathfrak{m}$ be the formal product of the real places of k, 8 and all the odd primes in S. Let $k_\mathfrak{m}$ be the ray class field associated to the modulus $\mathfrak{m}$. This is an abelian extension of k which is unramified away from $\mathfrak{m}$. We claim that $k_\mathfrak{m}$ and $\mathcal{K}$ are linearly disjoint over k. Indeed, $k' = k_\mathfrak{m} \cap \mathcal{K}$ is a subfield of $\mathcal{K}$ that is abelian over k and unramified at $w_1, \dots, w_r$. We note that $\mathrm{Gal}(\mathcal{K}/k)^{\mathrm{ab}} = (G_1)_\alpha^{\mathrm{ab}} \times \prod_{i=2}^r G_i^{\mathrm{ab}}$. By Corollary 3.9 we have $(G_1)_\alpha^{\mathrm{ab}} = (G_1)^{\mathrm{ab}}$. Therefore, $\mathrm{Gal}(\mathcal{K}/k)^{\mathrm{ab}} = \prod_{i=1}^r G_i^{\mathrm{ab}}$, so that k' is contained in the compositum $L = k_1^{\mathrm{ab}} \dots k_r^{\mathrm{ab}}$ of linearly disjoint abelian extensions $k_1^{\mathrm{ab}}, \dots, k_r^{\mathrm{ab}}$, where, as in §2, k_i^{ab} denotes the maximal abelian subextension of K_i/k.

Write $M = k_1^{\mathrm{ab}} \dots k_{r-1}^{\mathrm{ab}}$. The extension k_r^{ab}/k is totally ramified at w_r by condition (g), whereas k'/k and M/k are unramified at w_r (the latter by the criterion of Néron–Ogg–Shafarevich). Hence L/M is totally ramified at each prime v of M over w_r. Since $M \subset k'M \subset L$, where $k'M/M$ is unramified over v, we must have $k' \subset M$. Continuing by induction we prove that $k' = k$, as required.

It follows that $k_\mathfrak{m}\mathcal{K}$ is a Galois extension of k with the Galois group

$$\mathrm{Gal}(k_\mathfrak{m}\mathcal{K}/k) = \mathrm{Gal}(k_\mathfrak{m}/k) \times (G_1)_\alpha \times \prod_{i=2}^r G_i.$$

By Chebotarev density theorem we can find a place $\mathfrak{q}$ of k such that the corresponding Frobenius element in $\mathrm{Gal}(k_\mathfrak{m}\mathcal{K}/k)$ is the conjugacy class of $(1, \gamma, h, \dots, h)$. Then $\mathfrak{q}$ is a principal prime ideal with a totally positive generator $q \equiv 1 \bmod 8$, hence q is a square in each completion of k at a prime over 2. We also have $q \equiv 1 \bmod \mathfrak{p}$ for any odd $\mathfrak{p} \in S$. Thus all the places of S including the Archimedean places are split in $F = k(\sqrt{q})$. All other conditions are satisfied by construction. □

Proposition 7.2. *For any $\beta \in \mathrm{Sel}_2(A_1)$, $\beta \neq 0$, $\beta \neq \alpha_1$, there exists a quadratic extension F/k unramified at the places of S_0 and all the places of bad reduction of A, such that*

$$\mathrm{Sel}_2(A_1^F) \subset \mathrm{Sel}_2(A_1),\ \alpha_1 \in \mathrm{Sel}_2(A_1^F),\ \beta \notin \mathrm{Sel}_2(A_1^F),\ \mathrm{Sel}_2(A_i^F) = \mathrm{Sel}_2(A_i) \text{ for } i \neq 1.$$

Proof. Let $F = k(\sqrt{q})$ be as in Lemma 7.1. Let $i \in \{1, \dots, r\}$. Since F is split at each $v \in S$ we have $A_i^F \times_k k_v \cong A_i \times_k k_v$, so that the Selmer conditions at S

are identical for A_i and A_i^F. These conditions are also identical for all primes where both A_i and A_i^F have good reduction, and this includes the primes w_j if $j \neq i$. At w_i the extension F/k is unramified, and by condition (f) we can apply Lemma 4.2, so we obtain $\delta(A_i(k_{w_i})) = \delta^F(A_i^F(k_{w_i}))$.

It remains to check the behaviour at $\mathfrak{q}$, which is a prime of good reduction for A_i. If $i \neq 1$ then $\mathrm{Frob}_\mathfrak{q} = h$, and from condition (d) and formula (7) we deduce $\mathrm{H}^1(k_\mathfrak{q}, A_i[2]) = 0$ so the Selmer conditions for both A_i and A_i^F at $\mathfrak{q}$ are vacuous. This proves that $\mathrm{Sel}_2(A_i^F) = \mathrm{Sel}_2(A_i)$ whenever $i \neq 1$.

In the rest of the proof we work with A_1. The Selmer conditions for A_1 and A_1^F are the same at each place $v \neq \mathfrak{q}$. Thus $\mathrm{loc}_\mathfrak{q}(\alpha_1) = 0$ implies $\alpha_1 \in \mathrm{Sel}_2(A_1^F)$. Moreover, $\delta(A_1(k_\mathfrak{q})) \cap \delta^F(A_1^F(k_\mathfrak{q})) = 0$ by Lemma 4.3, hence $\beta \notin \mathrm{Sel}_2(A_1^F)$.

To prove that $\mathrm{Sel}_2(A_1^F) \subset \mathrm{Sel}_2(A_1)$ it is enough to show that for A_1 the Selmer condition at $\mathfrak{q}$ is implied by the Selmer conditions at the other places of k. Indeed, let $\xi \in \mathrm{H}^1(k, A_1[2])$ be an element satisfying the Selmer condition at each place $v \neq \mathfrak{q}$, but not necessarily at $\mathfrak{q}$. By global reciprocity the sum of $\mathrm{inv}_v(\beta \cup \xi) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ over all places of k, including the Archimedean places, is 0. Since the images of ξ and β in $\mathrm{H}^1(k_v, A_1[2])$ belong to $\delta(A_1(k_v))$ for all $v \neq \mathfrak{q}$ we obtain $\mathrm{inv}_v(\beta \cup \xi) = 0$. By the global reciprocity we deduce $\mathrm{inv}_\mathfrak{q}(\beta \cup \xi) = 0$. The non-zero element $\mathrm{loc}_\mathfrak{q}(\beta)$ generates $\delta(A_1(k_\mathfrak{q}))$, because

$$\delta(A_1(k_\mathfrak{q})) = A_1[2]/(\mathrm{Frob}_q - 1) = A_1[2]/(g-1) = \mathbb{Z}/2,$$

where we used (6) and the fact that $\mathrm{Frob}_\mathfrak{q}$ acts on $A_1[2]$ as the element g of condition (c). Since A_1 is principally polarised, $\delta(A_1(k_\mathfrak{q}))$ is a maximal isotropic subspace of $\mathrm{H}^1(k_\mathfrak{q}, A_1[2])$ (see the beginning of §4). Therefore $\mathrm{inv}_\mathfrak{q}(\beta \cup \xi) = 0$ implies that the image of ξ in $\mathrm{H}^1(k_\mathfrak{q}, A_1[2])$ lies in $\delta(A_1(k_\mathfrak{q}))$. □

End of proof of Theorem 2.3. The extension F/k is unramified at all the places where A has bad reduction, so replacing A by A^F preserves condition (f) for each A_i. Conditions (a), (b), (c), (d), (e) and (g) are not affected by quadratic twisting. By repeated applications of Proposition 7.2 we can find a quadratic extension F/k such that α_i is the only non-zero element in $\mathrm{Sel}_2(A_i^F)$, for all $i = 1, \ldots, r$. The exact sequence (12) for A_i^F shows that $Ш(A_i^F)[2]$ is of size at most 2. If the 2-primary subgroup of $Ш(A_i^F)$ is finite, then, by Proposition 5.3, the number of elements in $Ш(A_i^F)[2]$ is a square. Thus $Ш(A_i^F)[2] = 0$, so that the image of α_i in $\mathrm{H}^1(k, A_i^F)$ is 0. Then the image of α in $\mathrm{H}^1(k, A^F)$ is 0, so that $Y^F \cong A^F$ and hence $Y^F(k) \neq \emptyset$. This implies that $\tilde{Y}^F(k) \neq \emptyset$ and hence $X = \tilde{Y}/\iota_{\tilde{Y}}$ has a k-point.

It remains to prove that k-points are Zariski dense in X. Since $Y^F(k) \neq \emptyset$ we have $Y^F \simeq A^F$, so we may identify X with $\mathrm{Kum}(A^F)$. Hence it will suffice to show that $A^F(k)$ is Zariski dense in A^F. For each i the exact sequence (12) for A_i^F shows that $A_i^F(k)/2 \neq 0$. Since $A_i^F[2](k) = 0$ by condition (a), we see that $A_i^F(k)$ is infinite. The neutral connected component of the Zariski closure of $A_i^F(k)$ in A_i^F is an abelian

subvariety $B \subset A_i^F$ of positive dimension. By condition (a) we must have $B = A_i^F$. Thus the set $A_i^F(k)$ is Zariski dense in A_i^F for each $i = 1, \dots, r$, so that $A^F(k)$ is Zariski dense in A^F. $\square$

Proof of Proposition 1.1. We need to show that a real point $M \in X(\mathbb{R})$ path-connected with a rational point $P \in X(\mathbb{Q})$ can be approximated by a point in $X(\mathbb{Q})$. For each $i = 1, \dots, n$ we have the exact sequence

$$0 \longrightarrow E_i(\mathbb{Q})/2 \longrightarrow \mathrm{H}^1(\mathbb{Q}, E_i[2]) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E_i)[2] \longrightarrow 0.$$

By assumption there is a non-zero class $\alpha_i \in \mathrm{H}^1(\mathbb{Q}, E_i[2])$ that goes to the class of the torsor Y_i in $\mathrm{H}^1(\mathbb{Q}, E_i)[2]$. Recall from §6 that the fixed point set of the antipodal involution ι_Y on $Y = \prod_{i=1}^n Y_i$ is $Z = \prod_{i=1}^n Z_i$, where Z_i is a torsor for $E_i[2]$ defined by α_i. We see that in our assumptions $Z(k) = \emptyset$, thus in the notation of §6 the branch locus of the morphism $\tilde{Y} \to X$ has no $\mathbb{Q}$-points. Hence $\tilde{Y} \to X$ is unramified at P, so there exists a unique quadratic field F such that P lifts to a $\mathbb{Q}$-point $\tilde{P}$ on $Y^F = \prod_{i=1}^n Y_i^F$. The point M lifts to an $\mathbb{R}$-point $\tilde{M}$ on Y^F which is path connected with $\tilde{P}$. We recall from the introduction that each twisted torsor Y_i^F is defined by the image of α_i under the map

$$\mathrm{H}^1(\mathbb{Q}, E_i[2]) = \mathrm{H}^1(\mathbb{Q}, E_i^F[2]) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E_i^F).$$

Since $Y^F(\mathbb{Q}) \neq \emptyset$, we see that α_i is in the kernel $E_i^F(\mathbb{Q})/2$ of this map, that is, α_i comes from a $\mathbb{Q}$-point on E_i^F. By assumption $E_i[2](\mathbb{Q}) = 0$, so this point has infinite order. It follows that $\mathbb{Q}$-points of E_i are dense in the neutral connected component of $E_i(\mathbb{R})$ for each $i = 1, \dots, n$. Thus $\mathbb{Q}$-points are dense in the connected component of $Y^F(\mathbb{R})$ which contains $\tilde{P}$ and $\tilde{M}$. Hence we can find a $\mathbb{Q}$-point on $\mathrm{Kum}(Y)$ which is as close as we wish to M. $\square$

References

[1] M. Bright, T.D. Browning and D. Loughran. Failures of weak approximation in families. arXiv:1506.01817

[2] M. Bhargava, C. Skinner and W. Zhang. A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture. arXiv:1407.1826

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

[4] W. Burnside. *Theory of groups of finite order.* 2nd ed., Cambridge University Press, 1911.

[5] S.D. Cohen. The distribution of the Galois groups of integral polynomials. *Illinois J. Math.* **23** (1979) 135–152.

[6] J.-L. Colliot-Thélène, A.N. Skorobogatov and Sir P. Swinnerton-Dyer. Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. *Invent. math.* **134** (1998) 579–650.

[7] J-L. Colliot-Thélène and A.N. Skorobogatov. Descent on fibrations over $\mathbb{P}^1_k$ revisited. *Math. Proc. Camb. Phil. Soc.* **128** (2000) 383–393.

[8] T. Dokchitser and V. Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. reine angew. Math.* **658** (2011) 39–64.

[9] I. Dolgachev. *Classical algebraic geometry: a modern view.* Cambridge University Press, 2012.

[10] M.R. Gonzalez-Dorrego. $(16, 6)$ *configurations and geometry of Kummer surfaces in* $\mathbb{P}^3$. Memoirs Amer. Math. Soc. **512** (1994).

[11] Y. Harpaz and O. Wittenberg. On the fibration method for zero-cycles and rational points. *Ann. Math.* **183** (2016) 229–295.

[12] D. Holmes and R. Pannekoek. The Brauer–Manin obstruction on Kummer varieties and ranks of twists of abelian varieties. *Bull. London Math. Soc.* **47** (2015) 565–574.

[13] Z. Klagsbrun. Elliptic curves with a lower bound on 2-Selmer ranks of quadratic twists. *Math. Res. Letters* **19** (2012) 1137–1143.

[14] Z. Klagsbrun. Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion. arXiv:1201.5408

[15] K. Kramer. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.* **264** (1981) 121–135.

[16] M. Kuwata and L. Wang. Topology of rational points on isotrivial elliptic surfaces. *Internat. Math. Res. Notices* (1993), no. 4, 113–123.

[17] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.* **348** (1996) 4577–4610.

[18] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. math.* **18** (1972) 183–266.

[19] B. Mazur. The topology of rational points. *Experiment. Math.* **1** (1992) 35–45.

[20] B. Mazur. Speculations about the topology of rational points: an update. Columbia University Number Theory Seminar (New York, 1992). *Astérisque* **228** (1995) 165–182.

[21] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. math.* **181** (2010) 541–575.

[22] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Ann. Math.* **166** (2007) 579–612.

[23] J.S. Milne. *Arithmetic duality theorems*, Academic Press, 1986.

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

[25] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.* **25** (2012) 245–269.

[26] B. Poonen and M. Stoll. Cassels–Tate pairing on polarized abelian varieties. *Ann. Math.* **150** (1999) 1109–1149.

[27] C.-H. Sah. Cohomology of split group extensions, II. *J. Algebra* **45** (1977) 17–68.

[28] A. Skorobogatov. *Torsors and rational points.* Cambridge University Press, 2001.

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

[30] A. Skorobogatov. Del Pezzo surfaces of degree 4 and their relation to Kummer surfaces. *L'Enseignement Math.* **56** (2010) 73–85.

[31] A.N. Skorobogatov and Sir P. Swinnerton-Dyer. 2-descent on elliptic curves and rational points on certain Kummer surfaces. *Adv. Math.* **198** (2005) 448–483.

[32] A.N. Skorobogatov and Yu.G. Zarhin. A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces. *J. Alg. Geom.* **17** (2008) 481–502.

[33] A.N. Skorobogatov and Yu.G. Zarhin. The Brauer group of Kummer surfaces and torsion of elliptic curves. *J. reine angew. Math.* **666** (2012) 115–140.

[34] Sir P. Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces II. *Proc. London Math. Soc.* **80** (2000) 513–544.

[35] Sir P. Swinnerton-Dyer. The solubility of diagonal cubic surfaces. *Ann. Sci. École Norm. Sup.* **34** (2001) 891–912.

[36] R. Wisbauer. *Foundations of module and ring theory.* Vol. 3. CRC Press, 1991.

[37] O. Wittenberg. *Intersections de deux quadriques et pinceaux de courbes de genre 1.* Lecture Notes Math. **1901**, Springer-Verlag, 2007.

Department of Mathematics, South Kensington Campus, Imperial College, London, SW7 2BZ England, United Kingdom, and

Institute for the Information Transmission Problems, Russian Academy of Sciences, 19 Bolshoi Karetnyi, Moscow, 127994 Russia

a.skorobogatov@imperial.ac.uk

Département de Mathématiques et Applications, École Normale Supérieure, 45 rue d'Ulm, Paris 75005, France

harpaz@dma.ens.fr