Forum of Mathematics, Sigma (2017), Vol. 5, e26, 42 pages
doi:10.1017/fms.2017.16

ABELIAN n-DIVISION FIELDS OF ELLIPTIC CURVES AND BRAUER GROUPS OF PRODUCT KUMMER & ABELIAN SURFACES

ANTHONY VÁRILLY-ALVARADO[1] and BIANCA VIRAY[2]

[1] Department of Mathematics MS 136, Rice University, Houston, TX 77005, USA;
email: varilly@rice.edu

[2] University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195, USA;
email: bviray@math.washington.edu

Received 12 August 2016; accepted 21 June 2017

Abstract

Let Y be a principal homogeneous space of an abelian surface, or a K3 surface, over a finitely generated extension of $\mathbb{Q}$. In 2008, Skorobogatov and Zarhin showed that the Brauer group modulo algebraic classes $\operatorname{Br} Y/\operatorname{Br}_1 Y$ is finite. We study this quotient for the family of surfaces that are geometrically isomorphic to a product of isogenous non-CM elliptic curves, as well as the related family of geometrically Kummer surfaces; both families can be characterized by their geometric Néron–Severi lattices. Over a field of characteristic 0, we prove that the existence of a strong uniform bound on the size of the odd torsion of $\operatorname{Br} Y/\operatorname{Br}_1 Y$ is equivalent to the existence of a strong uniform bound on integers n for which there exist non-CM elliptic curves with abelian n-division fields. Using the same methods we show that, for a fixed prime ℓ, a number field k of fixed degree r, and a fixed discriminant of the geometric Néron–Severi lattice, $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)[\ell^\infty]$ is bounded by a constant that depends only on ℓ, r, and the discriminant.

1. Introduction

Let k be a field of characteristic 0, and let $\overline{k}/k$ be a fixed algebraic closure. Let Y be a smooth projective surface over k with trivial canonical sheaf $\omega_Y \cong \mathscr{O}_Y$, and let $\overline{Y} := Y \times_k \overline{k}$. The Enriques–Kodaira classification of smooth algebraic surfaces shows that $\overline{Y}$ is either a K3 surface, in which case $\mathrm{h}^1(Y, \mathscr{O}_Y) = 0$, or an abelian surface, in which case $\mathrm{h}^1(Y, \mathscr{O}_Y) = 2$.

If k is algebraically closed, the Brauer group $\operatorname{Br} Y := \mathrm{H}^2_{\mathrm{et}}(Y, \mathbb{G}_m)$ of Y is isomorphic to $(\mathbb{Q}/\mathbb{Z})^{b_2-r}$, where b_2 is the second Betti number of Y, and r denotes the rank of the Néron–Severi group of Y. In particular, $\operatorname{Br} Y$ is infinite, because k has characteristic 0 and $\omega_Y \cong \mathscr{O}_Y$ so we have $b_2 - r \geqslant 2$. In stark contrast, the group $\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$ is finite whenever k is a finitely generated extension of $\mathbb{Q}$; this is a remarkable result of Skorobogatov and Zarhin [**SZ08**]. We are interested in the existence of bounds for the size of $\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$ as Y varies in a family with fixed geometric properties.

Question 1.1. Let k be a field that is finitely generated over $\mathbb{Q}$. Let Y be a smooth projective surface over k with trivial canonical sheaf. Is there a bound for

$$\#\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$$

that is independent of Y, depending only on, say, $\mathrm{h}^1(Y, \mathscr{O}_Y)$, the geometric Néron–Severi lattice $\operatorname{NS} \overline{Y}$ (considered as an abstract lattice), and k or, if $k/\mathbb{Q}$ is finite, $[k : \mathbb{Q}]$?

Remarks 1.2.

(i) When k is a number field and Y is a K3 surface, the existence of bounds for $\#\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$ that can depend on Y has been studied previously; see [**SZ12**] and [**New16**] for the case of product Kummer surfaces, [**HKT13**] for the case of K3 surfaces of degree 2, and [**CFTTV**] for Kummer surfaces associated to Jacobians of genus 2 curves.

(ii) The Brauer group has a natural filtration

$$\operatorname{Br}_0 Y := \operatorname{im}(\operatorname{Br} k \to \operatorname{Br} Y) \subseteq \operatorname{Br}_1 Y := \ker(\operatorname{Br} Y \to \operatorname{Br} \overline{Y}) \subseteq \operatorname{Br} Y,$$

giving an injection $\operatorname{Br} Y/\operatorname{Br}_1 Y \hookrightarrow \operatorname{Br} \overline{Y}$, so we may replace $\#\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$ in Question 1.1 with $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)$. If Y is a K3 surface, $\#(\operatorname{Br}_1 Y/\operatorname{Br}_0 Y)$ is bounded above by a constant that depends only on the rank of $\operatorname{NS} \overline{Y}$ (Lemma 6.4). Therefore, bounding $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)$ is equivalent to bounding $\#(\operatorname{Br} Y/\operatorname{Br}_0 Y)$. In contrast, if Y is a principal homogeneous space of an abelian surface, then the quotient $\operatorname{Br}_1 Y/\operatorname{Br}_0 Y$ is infinite.

We study Question 1.1 for the following particular families of smooth projective surfaces:

$$\mathscr{A}_d^N := \left\{ Y/k : \omega_Y \cong \mathcal{O}_Y, \mathrm{h}^1(Y, \mathcal{O}_Y) = 2, \operatorname{NS} \overline{Y} \cong \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & d \\ 1 & d & 0 \end{pmatrix}, \right.$$
$$\left. \operatorname{Alb}^1(Y) \in \mathrm{H}^1(k, \operatorname{Alb}(Y))_N \right\},$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

$$\mathscr{K}_d := \{X/k : \omega_X \cong \mathcal{O}_X, \mathrm{h}^1(X, \mathcal{O}_X) = 0, \mathrm{NS}\,\overline{X} \cong \Lambda_d\},$$

where Λ_d denotes the Néron–Severi lattice of a Kummer surface of a product of non-CM elliptic curves that have a cyclic isogeny of degree d between them. (The lattice Λ_d is independent of the choice of elliptic curves and the cyclic isogeny of degree d, see Section 1.3.2.) Note that the surfaces in $\mathscr{A}_d^N$ are geometrically abelian (so in particular, $Y \cong \mathrm{Alb}^1(Y)$) and the surfaces in $\mathscr{K}_d$ are K3. In addition, if $d \neq d'$, then $\mathscr{K}_d \cap \mathscr{K}_{d'} = \mathscr{A}_d^N \cap \mathscr{A}_{d'}^{N'} = \emptyset$ for any integers N and N'. We prove the following theorem.

THEOREM 1.3. *Let d be a positive integer and let F be a field of characteristic* 0 *such that the symbol length of elements in* $(\mathrm{Br}\,F)[2]$ *is uniformly bounded, e.g., a number field or a p-adic field. For any positive integer n, we let n_{odd} denote the maximal odd integer that divides n. The following uniform boundedness statements are equivalent.*

(K3) *For all positive integers r, there exists a $B = B(r, d)$ such that for all fields k/F with $[k : F] \leqslant r$ and all surfaces $X/k \in \mathscr{K}_d$,*

$$\#\left(\frac{\mathrm{Br}\,X}{\mathrm{Br}_0\,X}\right)_{\mathrm{odd}} \leqslant B.$$

(Ab) *For all positive integers r', there exists a $B' = B'(r', d)$ such that for all fields k'/F with $[k' : F] \leqslant r'$ and all surfaces $Y/k \in \mathscr{A}_d^2$,*

$$\#\left(\frac{\mathrm{Br}\,Y}{\mathrm{Br}_1\,Y}\right)_{\mathrm{odd}} \leqslant B'.$$

(EC) *For all positive integers r'', there exists a $B'' = B''(r'', d)$ such that for all fields k''/F with $[k'' : F] \leqslant r''$ and all non-CM elliptic curves E/k'' with a k''-rational cyclic subgroup of order d,*

$$\mathrm{Gal}(k''(E_n)/k'')\text{ is abelian} \Rightarrow n_{\mathrm{odd}} \leqslant B''.$$

REMARK 1.4. The equivalence of **(Ab)** and **(K3)** primarily follows from a result of Skorobogatov and Zarhin [**SZ12**, Theorem 2.4 and its proof].

Theorem 1.3 reduces Question 1.1 for the odd part of the Brauer group in the case of $\mathscr{K}_d$ and $\mathscr{A}_d^2$ to a question about the existence of abelian n-division fields for n arbitrarily large. If we fix a prime ℓ and specialize to the case of a number field, then this reduction, together with results of Abramovich [**Abr96**] and Frey [**Fre94**], gives the existence of an unconditional uniform bound on the ℓ-primary part of $\#(\mathrm{Br}\,Y/\,\mathrm{Br}_1\,Y)$ and $\#(\mathrm{Br}\,X/\,\mathrm{Br}_0\,X)$.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

THEOREM 1.5. *Fix a prime integer ℓ and positive integers d, r, and v. There is a positive constant $B := B(\ell, d, r, v)$ such that for all degree r number fields k, all positive integers N with $v_\ell(N) \leqslant v$, and all surfaces $Y/k \in \mathcal{A}_d^N$, we have*

$$\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)[\ell^\infty] < B.$$

COROLLARY 1.6. *Fix a prime integer ℓ and positive integers d and r. There is a positive constant $B := B(\ell, d, r)$ such that for all degree r number fields k and surfaces $X/k \in \mathscr{K}_d$, we have*

$$\#(\operatorname{Br} X/\operatorname{Br}_0 X)[\ell^\infty] < B.$$

REMARK 1.7. Theorem 1.5 and Corollary 1.6 can be used to prove a slightly stronger version of Theorem 1.3 in the case where $F = \mathbb{Q}$. See Theorem 6.1.

If we specialize our family further, then we may use work of González-Jiménez and Lozano-Robledo [**GJLR**] to obtain precise bounds.

THEOREM 1.8. *Let d be a positive integer, let $E/\mathbb{Q}$ be a non-CM elliptic curve with a $\mathbb{Q}$-rational cyclic subgroup C of order d, let $Y = E \times E/C$, and let $X :=$ $\operatorname{Kum}(Y)$. Then*

$$\#(\operatorname{Br} Y/\operatorname{Br}_1 Y),\ \#(\operatorname{Br} X/\operatorname{Br}_1 X) \leqslant (8d)^3.$$

REMARK 1.9. Primarily by work of Mazur [**Maz78**], if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational subgroup of degree d, then $d \leqslant 163$. Thus, for any d and any Y and X as above, $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)$ and $\#(\operatorname{Br} X/\operatorname{Br}_1 X)$ are bounded above by $(8 \cdot 163)^3$.

1.1. Heuristics towards a uniform bound.

The above results might lead one to speculate that Question 1.1 has a positive answer in the case of number fields, at least for some Néron–Severi lattices. We provide some heuristic arguments in this direction.

1.1.1. The case of surfaces associated to products of isogenous non-CM elliptic curves. Let E be a non-CM elliptic curve over a number field k. Serre's Open Image Theorem states that the image of the Galois representation ρ_E attached to E is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ [**Ser72**]. In particular, there are finitely many integers n such that $k(E_n)/k$ is an abelian extension. In the same paper, Serre asked whether a *uniform* version of his Open Image Theorem is true, that is, if there exists a bound for the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \operatorname{im} \rho_E]$ that depends only on k. (Work of Mazur [**Maz78**]

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

and Bilu–Parent–Rebolledo [BPR13] strongly supports a positive answer, at least in the case $k = \mathbb{Q}$.) If there is such a bound and if, in addition, the bound can be taken to depend only on $[k : \mathbb{Q}]$ rather than k, then Theorem 6.1 proves Question 1.1 has a positive answer for $\mathscr{K}_d$ and $\mathscr{A}_d^2$. Under the same assumptions, a similar argument proves Question 1.1 has a positive answer for $\mathscr{A}_d^N$ for any N.

1.1.2. Cohomological interpretation of torsion on elliptic curves. Let E be an elliptic curve over a number field k. The torsion subgroup $E(k)_{\text{tors}}$ of the k-points is a finite abelian group. In [Man69], Manin showed that, for a fixed prime ℓ, the cardinality of the group $E(k)[\ell^\infty]$ of ℓ-primary order points of E is bounded in terms of ℓ, independent of E. Soon after, Mazur showed that, over $\mathbb{Q}$, the bound could be taken independent of ℓ and, more precisely, that there are only 15 possibilities for $E(\mathbb{Q})_{\text{tors}}$ [Maz77]. Following further progress by Kamienny [Kam92], Merel proved the strong uniform boundedness conjecture for elliptic curves: given a positive integer d, there is a constant $c := c(d)$ such that $\#E(k)_{\text{tors}} < c(d)$ for all elliptic curves E over any number field k of degree d [Mer96].

Among smooth projective curves, elliptic curves are precisely those that have trivial canonical sheaf. Surfaces with this property fall into two geometric classes: K3 surfaces and abelian surfaces. Hence, one might wonder if there is an analogous statement of Merel's theorem that holds for *both* of these classes of surfaces. The chain of group isomorphisms,

$$\begin{aligned}
E(k)_{\text{tors}} &\cong (\operatorname{Pic}^0 E)_{\text{tors}} \cong (\operatorname{Pic} E)_{\text{tors}} \\
&\cong \mathrm{H}^1_{\text{Zar}}(E, \mathscr{O}_E^\times)_{\text{tors}} \cong \mathrm{H}^1_{\text{et}}(E, \mathbb{G}_m)_{\text{tors}} \\
&\cong \operatorname{im}(\mathrm{H}^1_{\text{et}}(E, \mathbb{G}_m)_{\text{tors}} \to \mathrm{H}^1_{\text{et}}(\overline{E}, \mathbb{G}_m)_{\text{tors}}) \\
&\cong \operatorname{im}(\mathrm{H}^{\dim E}_{\text{et}}(E, \mathbb{G}_m)_{\text{tors}} \to \mathrm{H}^{\dim E}_{\text{et}}(\overline{E}, \mathbb{G}_m)_{\text{tors}}),
\end{aligned}$$

suggests that the group $\operatorname{im}(\mathrm{H}^2_{\text{et}}(Y, \mathbb{G}_m)_{\text{tors}} \to \mathrm{H}^2_{\text{et}}(\overline{Y}, \mathbb{G}_m)_{\text{tors}})$ is a plausible replacement for $E(k)_{\text{tors}}$. This group is precisely $\operatorname{im}(\operatorname{Br} Y \to \operatorname{Br} \overline{Y})$, and Skorobogatov and Zarhin's finiteness result for it is a suitable replacement for the finiteness of $E(k)_{\text{tors}}$. In this light, Question 1.1 asks whether the analogous statement of Merel's theorem holds for K3 surfaces and principal homogeneous spaces of abelian surfaces, after possibly fixing a Néron–Severi lattice; Theorem 1.5 and Corollary 1.6 are analogues of Manin's result for particular lattices.

1.1.3. Moduli of K3 surfaces with level structure. Uniform boundedness statements for torsion on elliptic curves are equivalent to statements about the lack of (noncuspidal) rational points on certain modular curves of high level.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

These curves parametrize isomorphism classes of elliptic curves with torsion data. As the level of the torsion data increases, uniform boundedness requires that the corresponding modular curves all have positive genus; having genus at least 2, that is, being of general type, is desirable in view of Faltings' Theorem. To investigate uniform boundedness of Brauer classes on K3 surfaces, one could start with the analogous purely geometric question: what is the Kodaira dimension of the moduli spaces of K3 surfaces that parametrize high-order Brauer class data?

To have a reasonable moduli theory of K3 surfaces, for example, to obtain coarse moduli spaces that are schemes of finite type over an algebraically closed field, one must first fix some polarization data. Typically, one fixes a lattice Λ of signature $(1, r)$ with $1 \leqslant r \leqslant 19$ that can be primitively embedded in the K3 lattice $U^{\oplus 3} \oplus E_8(-1)^{\oplus 2}$ and considers K3 surfaces whose geometric Néron–Severi group $\operatorname{NS} \overline{X}$ contains Λ. To these lattice-polarized moduli spaces, one adds level structures coming from the Brauer group, for example, a cyclic subgroup of order n of the Brauer group. McKinnie, Sawon, Tanimoto, and the first author show that when n is prime these moduli spaces have 3 or 4 components, depending on n and the polarization [MSTVA16]. One component is always isomorphic to a moduli space of K3 surfaces of higher degree, and, for some values of n, another is isomorphic to a moduli space of special cubic fourfolds. Kodaira dimension estimates in [GHS07, TVA15] show that such components are of general type for $n \gg 0$. This has led the first author to make the following conjecture.

Conjecture 1.10 [VA, Conjecture 5.5]. *Fix a number field k and a lattice Λ together with a primitive embedding $\Lambda \hookrightarrow U^{\oplus 3} \oplus E_8(-1)^{\oplus 2}$. Let X be a K3 surface over k such that $\operatorname{NS} \overline{X} \cong \Lambda$. Then there is a constant $B(k, \Lambda)$, independent of X, such that*

$$\#\left(\frac{\operatorname{Br} X}{\operatorname{Br}_0 X}\right) < B(k, \Lambda).$$

Recent conditional work of the first author with Abramovich [AVAa, AVAb] is aimed at exploring the plausibility of the analogous conjecture for torsion on abelian varieties.

1.2. Outline. In Section 2, we classify K3 surfaces X such that $\operatorname{NS} \overline{X} \cong \Lambda_d$. In Section 3, we build on work of Skorobogatov and Zarhin [SZ12] to relate the Brauer group of such K3 surfaces and the Brauer group of principal homogeneous spaces of abelian surfaces to Galois-equivariant homomorphisms between the n-torsion of isogenous non-CM elliptic curves. Then, we prove results on Galois-equivariant homomorphisms between the n-torsion of non-CM elliptic curves

(Section 4) and on related Galois-equivariant endomorphisms (Section 5). Finally in Section 6, we state and prove our main results.

1.3. Background and notation. For a rational prime ℓ, we write v_ℓ for the corresponding ℓ-adic valuation. For any integer n, we let $n_{\text{odd}} := n \cdot 2^{-v_2(n)}$ denote the odd part of n. Given two positive integers a and b, we let $\gcd(a, b^\infty) := \max_n\{\gcd(a, b^n)\}$.

For any abelian group G and positive integer n, we write G_n for the subgroup of n-torsion elements and G_{odd} for the subgroup of elements of odd order. If G is finite, then we write $e(G)$ for its exponent and $\#G$ for its cardinality.

Throughout, we assume that our fields have characteristic 0. For a field k, we let $\overline{k}$ denote a fixed algebraic closure and let Γ_k denote the absolute Galois group $\operatorname{Gal}(\overline{k}/k)$. For any Γ_k-module M and any quadratic character $\chi : \Gamma_k \to \mu_2$, we write

$$M^\chi := \{m \in M : \sigma(m) = \chi(\sigma)m \text{ for all } \sigma \in \Gamma_k\}.$$

If k'/k is a finite separable extension, then for any i and any Γ_k-module M we let $\operatorname{Res}_{k'/k}$ denote the restriction map $\mathrm{H}^i(\Gamma_k, M) \to \mathrm{H}^i(\Gamma_{k'}, M)$.

For any smooth projective geometrically integral variety X over a field k, we let $\overline{X}$ denote the base change of X to $\overline{k}$. We let $\operatorname{Pic} X$ denote the Picard group of X, $\operatorname{Pic}^0 X$ denote the subgroup of $\operatorname{Pic} X$ that maps to the identity component of the Picard scheme, and $\operatorname{NS} X$ denote the quotient $\operatorname{Pic} X/\operatorname{Pic}^0 X$, the Néron–Severi group of X; we use $\sim$ to denote algebraic equivalence of divisors. We write $\operatorname{Br} X := \mathrm{H}^2_{\text{et}}(X, \mathbb{G}_m)$ for the Brauer group of X, $\operatorname{Br}_1 X := \ker(\operatorname{Br} X \to \operatorname{Br} \overline{X})$ for the algebraic Brauer group of X, and $\operatorname{Br}_0 X := \operatorname{im}(\operatorname{Br} k \to \operatorname{Br} X)$ for the subgroup of constant algebras.

Let E be an elliptic curve over a field k. We write E_n for the subgroup scheme of n-torsion elements. A k-rational cyclic subgroup of E is a cyclic subgroup $C \subset E$ such that $C^{\Gamma_k} = C$; note that C is not necessarily contained in $E(k)$. If $\delta \in k^\times/k^{\times 2}$, we write E^δ for the quadratic twist associated to $\delta \in k^\times/k^{\times 2} \cong \mathrm{H}^1(k, \mu_2) \to \mathrm{H}^1(k, \operatorname{Aut} E)$. For $\phi \colon E \to E'$ an isogeny between two elliptic curves, we write $\phi^\vee$ for the dual isogeny. We call an isogeny cyclic if its kernel is a cyclic group.

Let Y/k be a principal homogeneous space of an abelian variety A. The period of Y, denoted $\operatorname{per}(Y)$, is the order of Y in the Weil–Châtelet group $\mathrm{H}^1(k, A)$.

1.3.1. Kummer surfaces. Let A be an abelian surface over k, and let $f : Y \to A$ be a 2-covering. Then $Z := f^{-1}(O)$ is a k-torsor for A_2, and the quotient $(A \times_k Z)/A_2$, where A_2 acts diagonally, is k-isomorphic to Y as a 2-covering. Thus, the antipodal involution $\iota \colon A \to A$ acts on Y fixing Z pointwise; elements of Z give rise to the singular locus S of the quotient Y/ι. Let $X := \mathrm{Bl}_S(Y/\iota)$ be the blow-up of Y/ι centred at S. The surface X can also be constructed as the quotient of the blow-up $Y' := \mathrm{Bl}_Z(Y)$ by the involution $\iota' \colon Y' \to Y'$ induced by ι. We call X the Kummer surface associated to Y (or Z) and denote it $\mathrm{Kum}\, Y$; it is a K3 surface.

Geometrically, the exceptional divisor of the blow-up map $X \to Y/\iota$ consists of 16 pairwise disjoint smooth rational curves, each with self-intersection -2. This collection of curves gives a sublattice $\mathbb{Z}^{16} \subset \mathrm{NS}\, \overline{X}$ whose saturation Λ_K is called the Kummer lattice. It is an even negative-definite rank 16 lattice of discriminant 2^6 whose isomorphism type does not depend on the choice of Y; see [Nik75]. There is an exact sequence of lattices

$$0 \to \Lambda_K \to \mathrm{NS}\, \overline{X} \to \mathrm{NS}\, \overline{Y} \to 0, \tag{1.1}$$

where the first map is the natural inclusion (see, for example, [SZ12, Remark 2]).

1.3.2. Products of elliptic curves. Of particular interest to us is the case when $\overline{Y}$ is isomorphic to a product of two elliptic curves E, E'. Let O and O' be the respective origins of E and E'. In addition to the Kummer lattice, the group $\mathrm{NS}\, \overline{X}$ contains the classes $e := [E \times \{O'\}]$ and $e' := [\{O\} \times E']$. Define the lattice

$$\Lambda_{\prod} := \Lambda_K \oplus \langle e, e' \rangle \subseteq \mathrm{NS}\, \overline{X}, \tag{1.2}$$

where $\oplus$ denotes an orthogonal direct sum and $\langle e, e' \rangle$ is isomorphic to a hyperbolic plane. Note that $\Lambda_{\prod}$ does not depend on the particular choice of E and E'.

Suppose next that E and E' are isogenous non-CM elliptic curves over k. Let d be the smallest degree of a geometric isogeny $E \to E'$; such an isogeny is necessarily cyclic [MW90, Lemma 6.2]. Define the lattice

$$\Lambda_d := \mathrm{NS}(\mathrm{Kum}(\overline{E} \times \overline{E}')).$$

The lattice Λ_d depends on the integer d, but not on the specific isogeny $E \to E'$ of degree d. Indeed, the sequence (1.1) shows that Λ_d is generated by some rational combinations of the 16 classes of (-2)-curves, and pullbacks from $\mathrm{NS}(\overline{E} \times \overline{E}')$. In turn, it is well known that the lattice $\mathrm{NS}(\overline{E} \times \overline{E}')$ is generated by the classes e, e' and the class of the graph of a degree d cyclic isogeny $E \to E'$. The intersection products of the graph with e and e' depend only on d, and not on the isogeny $E \to E'$.

REMARK 1.11. Any isomorphisms with Λ_K, $\Lambda_{\prod}$, and Λ_d are isomorphisms of abstract lattices; Λ_K, $\Lambda_{\prod}$, and Λ_d do *not* carry a Galois action.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

2. Classification of certain rank 19 K3 surfaces

The goal of this section is to classify K3 surfaces X over a number field k such that $X/k \in \mathscr{K}_d$; see Corollary 2.4 below. As a by-product, we classify surfaces $Y/k \in \mathscr{A}_d^1$; see Proposition 2.7.

PROPOSITION 2.1. *There is a positive integer M such that for any number field k, and any K3 surface X/k with* $\operatorname{NS}\overline{X}$ *containing a sublattice isomorphic to Λ_K, there is an extension k_0/k of degree at most M such that X_{k_0} is a Kummer surface.*

REMARKS 2.2.

(i) The proof of Proposition 2.1 actually proves much more – it shows that X_{k_0} is the Kummer surface of an abelian surface A whose 2-torsion is k_0-rational – at the expense of a very large bound M. It would be interesting to determine whether there is a smaller bound that yields the desired result and nothing stronger.

(ii) The proposition can be generalized to any set of fields $\mathbb{K}$ for which there is a uniform bound on the degree of a field extension required to split an order 2 element in $\operatorname{Br} k$, independent of the Brauer class and of the field $k \in \mathbb{K}$. Such a bound exists for number fields by class field theory.

THEOREM 2.3. *Let $X = \operatorname{Kum} Y$ be a Kummer surface over a field k of characteristic 0, with $Y \to A$ the 2-covering associated to X. Assume that $X \in \mathscr{K}_d$ for some positive integer d. Then there exist: a field extension L/k of degree at most 12, elliptic curves E and E' over L, and $\delta \in L^\times/L^{\times 2}$, such that:*

(1) *$A_L \cong E \times E'$; and*

(2) *there is a cyclic isogeny $\phi\colon E \to E'^{\delta}$ of degree d.*

COROLLARY 2.4. *There exists a positive integer M_0 such that, for all number fields k, all positive integers d and all surfaces $X \in \mathscr{K}_d$, there exist: a field extension L_0/k of degree at most M_0, elliptic curves E and E' over L_0, and a 2-covering $Y \to E \times E'$, such that:*

(1) *$X_{L_0} \cong \operatorname{Kum} Y$; and*

(2) *there is a cyclic isogeny $\phi\colon E \to E'$ of degree d.*

Proof. This is immediate from Theorem 2.3 and Proposition 2.1. □

We begin by proving Proposition 2.1 in Section 2.1. In Section 2.2, we study non-CM elliptic curves that are geometrically isogenous; the results therein are

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

used in Section 2.3 to classify abelian surfaces A such that $A \in \mathscr{A}_d^1$ for some d. This is used in Section 2.4 to prove Theorem 2.3.

2.1. Proof of Proposition 2.1. We use Nikulin's work on Kummer surfaces [**Nik75**], and the main idea of [**Huy16**, Lemma 17.2.6]. The group $\operatorname{NS} \overline{X}$ is finitely generated; each of its generators can be represented by a curve which is defined by finitely many equations with finitely many coefficients. Therefore, the image of the representation

$$\rho \colon \Gamma_k \to O(\operatorname{NS} \overline{X}) \hookrightarrow \mathrm{GL}_r(\mathbb{Z}), \quad r := \operatorname{rank} \operatorname{NS} \overline{X} \leqslant 20$$

is finite. Every finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$ injects into $\mathrm{GL}_r(\mathbb{F}_3)$. Furthermore, $r \leqslant 20$ so $|\mathrm{im}(\rho)|$ can be bounded by an absolute constant. Thus, for $H := \ker(\rho)$, the degree $[\overline{k}^H : k]$ can also be bounded by an absolute constant.

The hypothesis that $\operatorname{NS} \overline{X}$ contains a sublattice isomorphic to Λ_K ensures $\operatorname{NS} \overline{X}$ contains 16 pairwise disjoint (-2)-classes, represented over $\overline{k}$ by irreducible rational curves [**Nik75**, Theorem 3]. We claim that these classes can be represented by curves defined over $\overline{k}^H$. Let $[D]$ be such a class, with D an irreducible rational curve over $\overline{k}$. Since $\operatorname{Pic} \overline{X} = \operatorname{NS} \overline{X} = (\operatorname{NS} \overline{X})^H$, for $h \in H$, we have $h([D]) = [D]$, so D and ${}^hD$ are linearly equivalent irreducible curves; in particular, D and ${}^hD$ are integral elements of the linear system $|D|$. Since D is effective and $D^2 = -2$, the Riemann–Roch theorem for surfaces implies that $h^0(X, \mathscr{O}_X(D)) = 1$, so we must have ${}^hD = D$, which means that the irreducible curve D is already defined over $\overline{k}^H$.

Let $D_1, \ldots, D_{16}$ be disjoint (-2)-curves on X, each defined over $\overline{k}^H$. The class of the sum $\sum_i D_i$ is divisible by 2 in $\Lambda_K \subseteq \operatorname{NS} \overline{X} = (\operatorname{NS} \overline{X})^H$ [**Nik75**, Section 3]. The Hochschild–Serre spectral sequence

$$E_2^{p,q} := \mathrm{H}^p\big(H, \mathrm{H}^q_{\text{ét}}\big(\overline{X}, \mathbb{G}_m\big)\big) \Longrightarrow \mathrm{H}^{p+q}_{\text{ét}}\big(X_{\overline{k}^H}, \mathbb{G}_m\big) \tag{2.1}$$

gives rise to an exact sequence of low-degree terms

$$0 \to \operatorname{NS} X_{\overline{k}^H} \to (\operatorname{NS} \overline{X})^H = \operatorname{NS} \overline{X} \to \operatorname{Br} \overline{k}^H.$$

This sequence shows that the obstruction to divisibility by 2 of the class $\sum_i D_i$ in $\operatorname{NS} X_{\overline{k}^H}$ lies in $(\operatorname{Br} \overline{k}^H)_2$. Since $\overline{k}^H$ is a number field, global class field theory shows that any nontrivial element of $(\operatorname{Br} \overline{k}^H)_2$ can be represented by a quaternion algebra over $\overline{k}^H$ [**Neu13**, Theorem 3.6], and can thus be trivialized by a field extension $k_0/\overline{k}^H$ of degree at most 2. Thus, there is a divisor D' on X_{k_0} such that $\sum_i D_i \sim 2D'$, and hence a double cover morphism

$$\mathbf{Spec}(\mathscr{O}_{X_{k_0}} \oplus \mathscr{O}_{X_{k_0}}(D')) =: \widetilde{Y} \to X_{k_0}$$

branched along $\sum_i D_i$. The preimage of $\sum_i D_i$ consists of 16 pairwise disjoint rational curves with self-intersection -1. Contracting these curves gives rise to a surface Y/k_0. The classification of surfaces (see, for example, [Bea96]) implies that $\overline{Y}$ is an abelian surface, and so Y is a principal homogeneous space under its Albanese variety A. There is an involution $\widetilde{Y} \to \widetilde{Y}$ associated to the double cover $\widetilde{Y} \to X_{k_0}$, which geometrically is the $[-1]$ map and whose fixed locus consists of the preimages of $\sum_i D_i$. This involution in turn gives rise to an involution $Y \to Y$ whose fixed locus Z consists of 16 geometric points and is a torsor of A_2. Thus Y is a 2-covering and X_{k_0} is a Kummer surface. As $[\overline{k}^H : k]$ is absolutely bounded, and $[k_0 : k] \leqslant 2[\overline{k}^H : k]$, the degree of k_0/k is absolutely bounded. □

As pointed out in Remark 2.2(i), this proof actually shows that X_{k_0} is a Kummer surface of an abelian surface A such that $A_2 \subset A(k_0)$. Indeed, our determination of $\overline{k}^H$ implies that each D_i is defined over k_0 and so $Z \subset Y$ consists of 16 k_0-rational points.

2.2. Geometrically isogenous non-CM elliptic curves.

PROPOSITION 2.5. *Let E, E' be non-CM elliptic curves over a field k of characteristic* 0. *Assume that there exists a cyclic isogeny $\overline{\phi}: \overline{E} \to \overline{E}'$. Then $C := \ker \overline{\phi}$ is defined over k and there exists a $\delta \in k^\times/k^{\times 2}$ such that $E'^\delta \cong E/C$. In particular, there exists a unique cyclic isogeny $\phi_{k(\sqrt{\delta})}: E_{k(\sqrt{\delta})} \to E'_{k(\sqrt{\delta})}$ that agrees with $\overline{\phi}$.*

We begin with a lemma.

LEMMA 2.6. *Let E be a non-CM elliptic curve over a field k of characteristic* 0 *and let $C, C' \subset E$ be k-rational cyclic subgroups of order d. If E/C and E/C' are k-isomorphic, then $C = C'$.*

Proof. Let ϕ denote the quotient isogeny $E \to E/C$ and let ψ denote the composition of the quotient $E \to E/C'$ with a k-isomorphism $E/C' \xrightarrow{\sim} E/C$. Note that ϕ and ψ are both isogenies and $\ker \phi = C$ and $\ker \psi = C'$.

Now consider $\psi^\vee \circ \phi: E \to E$. This is an isogeny of degree d^2; since E is non-CM, it must be equal to $\pm[d]$. Hence $\psi = \pm\phi$ by the uniqueness of the dual isogeny and so $C' = \ker \psi = \ker \phi = C$. □

Proof of Proposition 2.5. There is a Galois extension L/k over which C is defined. Since $\overline{E}' \cong \overline{(E/C)}$ and E' is non-CM, there exists a unique $\delta \in L^\times/L^{\times 2}$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

such that $E'^{\delta}_L \cong E_L/C$. Let $\sigma \in \mathrm{Gal}(L/k)$. Then we have

$$\overline{(E_L/C)} \cong \overline{E'^{\delta}_L} \cong \overline{E'^{\sigma(\delta)}_L} \cong \overline{(E_L/\sigma(C))}.$$

Thus, Lemma 2.6 applied over $\overline{k}$ yields that $C = \sigma(C)$ for all $\sigma \in \mathrm{Gal}(L/k)$. Thus C is k-rational, and we may take $L = k$ above. This completes the proof. □

2.3. Geometric products of elliptic curves.

PROPOSITION 2.7. *Let A be an abelian surface over a field k such that $A/k \in \mathscr{A}^1_d$ for some positive integer d. Then there exist: an extension L/k with $[L : k] \in \{1, 2, 3, 4, 6, 8, 12\}$, elliptic curves E and E'/L, and $\delta \in L^\times/L^{\times 2}$ such that:*

(1) *$A_L \cong E \times E'$; and*

(2) *there exists a cyclic L-isogeny $\phi\colon E \to E'^{\delta}$ of degree d.*

LEMMA 2.8. *Let A be an abelian surface over an algebraically closed field such that $\mathrm{NS}\,A$ contains a hyperbolic plane. Then A is isomorphic to a product of elliptic curves. In addition:*

- *if $\mathrm{rank}\,\mathrm{NS}\,A = 2$, then the elliptic curves are not isogenous;*
- *if $\mathrm{rank}\,\mathrm{NS}\,A = 3$, then the elliptic curves are non-CM, isogenous, and the degree of a cyclic isogeny between them is $\frac{1}{2}\,\mathrm{disc}\,\mathrm{NS}\,A$; and*
- *if $\mathrm{rank}\,\mathrm{NS}\,A = 4$, then the elliptic curves are isogenous and CM.*

Proof. Let e_1 and e_2 generate a hyperbolic plane contained in $\mathrm{NS}\,A$, so $e_1^2 = e_2^2 = 0$ and $e_1 \cdot e_2 = 1$. Let D be a divisor on A representing the class $e_1 + e_2$. By [**Kan94**, Corollary 2.2(b)], either D or $-D$ is ample, because $D^2 > 0$; assume without loss of generality that D is ample. Using [**Kan94**, Proposition 2.3], we conclude that for $i = 1$ and 2, the class e_i is represented by a multiple $m_i E_i$ of an elliptic curve E_i, and $m_i > 0$ since $E_i \cdot D > 0$. Moreover, since $1 = e_1 \cdot e_2 = m_1 m_2 (E_1 \cdot E_2) \in m_1 m_2 \mathbb{Z}$, we have $m_i = 1$. Translating the curves E_1 and E_2 if necessary, we may assume they are elliptic subgroups of A. We may thus define a morphism of abelian varieties $\phi\colon A \to A/E_1 \times A/E_2$ using projections. Let $(P + E_1, Q + E_2) \in A/E_1 \times A/E_2$. Since $P + E_1 \sim E_1$ and $Q + E_2 \sim E_2$, and $E_1 \cdot E_2 = 1$, there exists a unique point $R \in A$ such that $\phi(R) = (P + E_1, Q + E_2)$. Hence, ϕ is an isogeny of degree 1, that is, an isomorphism.

Note that we have group isomorphisms

$$\mathrm{NS}\,A \cong \mathrm{NS}(E_1 \times E_2) \cong \mathbb{Z} \cdot [E_1] \oplus \mathbb{Z} \cdot [E_2] \oplus \mathrm{Hom}(E_1, E_2).$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

This proves all the remaining statements except for the computation of the degree of a cyclic isogeny $E_1 \to E_2$ when $\operatorname{rank} \operatorname{NS} A = 3$. Assume that $\operatorname{rank} \operatorname{NS} A = 3$. Then E_1 and E_2 are non-CM, and we have $\operatorname{Hom}(E_1, E_2) = \langle \phi \rangle$, where $\phi\colon E_1 \to E_2$ is a cyclic isogeny. The image of ϕ in $\operatorname{NS}(E_1 \times E_2)$ is the graph of ϕ and the images of $[E_1], [E_2]$ are $E_1 \times O$ and $O \times E_2$ respectively. Hence, a simple calculation shows that $\operatorname{disc} \operatorname{NS}(E_1 \times E_2) = 2 \deg(\phi)$. □

Proof of Proposition 2.7. Part (2) of the proposition follows from (1), Lemma 2.8, and Proposition 2.5. Hence, we reduce to proving (1).

Let $\mathcal{M}_{1,1} = \mathbb{A}^1$ denote the coarse moduli space of elliptic curves, parametrized by their j-invariant. The coarse moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces contains the Humbert surface $\mathcal{H}_1 := \operatorname{Sym}^2 \mathcal{M}_{1,1} \cong \mathbb{A}^2$, which is the locus of abelian surfaces with product structure. By Lemma 2.8, there exist non-CM geometrically isogenous elliptic curves E and E' over $\overline{k}$ such that $\overline{A} \cong E \times E'$. Thus the surface $\overline{A}$ gives rise to a point $x \in \mathcal{H}_1(\overline{k})$, with coordinates $(j(E) + j(E'), j(E) \cdot j(E')) \in \mathbb{A}^2(\overline{k})$. For any $\sigma \in \operatorname{Gal}(\overline{k}/k)$, we have $\sigma(\overline{A}) = \overline{A}$, so $E \times E' \cong \sigma(E \times E')$, and thus $x \in \mathcal{H}_1(k)$. Therefore, $j(E) + j(E')$ and $j(E) \cdot j(E')$ belong to k, and so there is an extension k_0/k of degree at most 2 such that $j(E)$, $j(E') \in k_0$.

Since $j(E), j(E') \in k_0$, we may assume that E, E' are defined over k_0. By Proposition 2.5, after possibly replacing E' with a quadratic twist, we may assume that E and E' are isogenous over k_0; let $\psi\colon E \to E'$ be a cyclic isogeny defined over k_0 and let $d := \deg(\psi)$. Since $\overline{A} \cong \overline{E} \times \overline{E}'$, A_{k_0} is a twist (as an abelian surface) of $E \times E'$, so corresponds to an element of $\mathrm{H}^1(k_0, \operatorname{Aut}(\overline{E} \times \overline{E}'))$. The abelian surface A_{k_0} is isomorphic to a product of elliptic curves if

$$[A_{k_0}] \in \operatorname{im}(\mathrm{H}^1(k_0, \operatorname{Aut}(\overline{E})) \times \mathrm{H}^1(k_0, \operatorname{Aut}(\overline{E}')) \to \mathrm{H}^1(k_0, \operatorname{Aut}(\overline{E} \times \overline{E}'))).$$

Thus to prove (1) it suffices to show that for any element $\varphi \in \mathrm{H}^1(k_0, \operatorname{Aut}(\overline{E} \times \overline{E}'))$, there exists an extension L/k_0 with $[L : k_0] \in \{1, 2, 3, 4, 6\}$ such that

$$\varphi_L \in \operatorname{im}(\mathrm{H}^1(L, \operatorname{Aut}(\overline{E})) \times \mathrm{H}^1(L, \operatorname{Aut}(\overline{E}')) \to \mathrm{H}^1(L, \operatorname{Aut}(\overline{E} \times \overline{E}'))).$$

Since E and E' are k_0-isogenous non-CM elliptic curves, we have

$$\begin{aligned}\operatorname{End}(\overline{E} \times \overline{E}') &= \begin{pmatrix} \operatorname{End}(\overline{E}) & \operatorname{Hom}(\overline{E}', \overline{E}) \\ \operatorname{Hom}(\overline{E}, \overline{E}') & \operatorname{End}(\overline{E}') \end{pmatrix} \\ &= \begin{pmatrix} \mathbb{Z} & \mathbb{Z}\psi^\vee \\ \mathbb{Z}\psi & \mathbb{Z} \end{pmatrix} \cong \begin{pmatrix} \mathbb{Z} & \mathbb{Z}\sqrt{d} \\ \mathbb{Z}\sqrt{d} & \mathbb{Z} \end{pmatrix} \subset \mathrm{M}_2(\mathbb{R}); \qquad (2.2)\end{aligned}$$

in particular, $\mathrm{Gal}(\overline{k}/k_0)$ acts trivially on $\mathrm{End}(\overline{E} \times \overline{E}')$ and $\mathrm{Aut}(\overline{E} \times \overline{E}')$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{R})$. Since $\mathrm{Gal}(\overline{k}/k_0)$ acts trivially, we have

$$\mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E} \times \overline{E}')) = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{k}/k_0), \mathrm{Aut}(\overline{E} \times \overline{E}')).$$

Let $\varphi \in \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{k}/k_0), \mathrm{Aut}(\overline{E} \times \overline{E}'))$ and let L be the fixed field of $\varphi^{-1}(\{\pm I\})$. Then $\operatorname{im}\mathrm{Res}_{L/k_0}(\varphi) \subset \{\pm I\}$, so

$$\mathrm{Res}_{L/k_0}(\varphi) \in \operatorname{im}(\mathrm{H}^1(L, \mathrm{Aut}(\overline{E})) \times \mathrm{H}^1(L, \mathrm{Aut}(\overline{E}')) \to \mathrm{H}^1(L, \mathrm{Aut}(\overline{E} \times \overline{E}'))).$$

Since $[L : k] = [L : k_0] \cdot [k_0 : k] \leqslant 2[L : k_0]$, it remains to show that $[L : k_0] \in \{1, 2, 3, 4, 6\}$. Note that φ yields an isomorphism $\Gamma_{k_0}/\Gamma_L \to \operatorname{im}\varphi/(\{\pm I\} \cap (\operatorname{im}\varphi))$, so

$$[L : k_0] = \#\mathrm{Gal}(L/k_0) = \#\frac{\operatorname{im}\varphi}{\{\pm I\} \cap (\operatorname{im}\varphi)}.$$

The image of φ must be a profinite subgroup of the discrete group $\mathrm{Aut}(\overline{E} \times \overline{E}')$, hence must be finite. Furthermore, by (2.2), every element of $\mathrm{Aut}(\overline{E} \times \overline{E}')$ has integer trace and determinant. Thus, the following lemma completes the proof. □

LEMMA 2.9. *Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{R})$ such that $\mathrm{Tr}(x), \det(x) \in \mathbb{Q}$ for all $x \in G$. Then G is isomorphic to a cyclic group of order $1, 2, 3, 4,$ or 6 or a dihedral group of order $4, 6, 8,$ or 12. In addition, if G is isomorphic to a dihedral group of order $4, 8$ or 12, then $-I \in G$.*

Proof. Since every compact group of $\mathrm{SL}_2(\mathbb{R})$ is conjugate to a subgroup of $\mathrm{SO}_2(\mathbb{R})$ [Iwa49, Theorem 6], $G^+ := G \cap \mathrm{SL}_2(\mathbb{R})$ is conjugate to a finite subgroup of $\mathrm{SO}_2(\mathbb{R}) \cong S^1$, so is cyclic. Therefore, G is either cyclic or an extension of $\mathbb{Z}/2\mathbb{Z}$ by a cyclic group.

Let $x \in G$. Since the trace and determinant of x are rational numbers and the minimal polynomial of x divides $T^{|G|} - 1$, the characteristic polynomial of x must be one of the following

$$(T-1)^2, \quad (T+1)^2, \quad T^2 - 1, \quad T^2 + 1, \quad T^2 + T + 1, \quad T^2 - T + 1.$$

Therefore, any $x \in G$ has order equal to $1, 2, 3, 4$ or 6, and if $x \in G \setminus G^+$, then x has order 2. Hence G is a cyclic group of order $1, 2, 3, 4$ or 6 or it is a dihedral group of order $4, 6, 8,$ or 12.

Assume that G is a dihedral group of order $4, 8$ or 12. Then G^+ is a cyclic group of even order, hence contains an element g of order 2. Since $g \in G^+$, the minimal polynomial of g must be a proper divisor of $T^2 - 1$, and so $g = -I$. □

2.4. Proof of Theorem 2.3. The exact sequence (1.1) and the isomorphism $\mathrm{NS}\,\overline{X} \cong \Lambda_d$ imply that $A \in \mathscr{A}_d^1$. Then Proposition 2.7 completes the proof. □

3. Bounds on the Brauer group in terms of Galois-invariant homomorphisms

Let Y/k be a surface such that $Y \in \mathscr{A}_d^N$ for some integers N and d, so in particular Y is a principal homogeneous space under $A := \mathrm{Alb}\, Y$. Since, as lattices, $\mathrm{NS}\,\overline{Y} \cong \mathrm{NS}\,\overline{A}$, Proposition 2.7 gives a field extension L/k of degree at most 12, and a pair of elliptic curves E and E' over L such that $A_L \cong E \times E'$.

As a first step towards bounding the n-torsion of the group $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$, we show that the group $(\mathrm{Br}\, Y/\mathrm{Br}_1\, Y)_n$ can be embedded into a group determined by Galois-invariant homomorphisms associated to E and E', after possibly extending the ground field to a field whose degree is bounded by a constant depending only on the period of Y. More precisely, we prove the following theorem.

THEOREM 3.1. *Let n be a positive integer and let Y/k be a surface in $\bigcup_{d,N} \mathscr{A}_d^N$. Let L, E, and E' be as above. There is a field extension k'/k with $[k' : k] \leqslant (\gcd(\mathrm{per}(Y), n^\infty))^4$ such that*

$$\frac{(\mathrm{Br}\, Y)_n}{(\mathrm{Br}_1\, Y)_n} \hookrightarrow \frac{\mathrm{Hom}_{L'}(E_n, E'_n)}{(\mathrm{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_{L'}}},$$

where L' denotes the compositum of k' and L. If n is relatively prime to $\mathrm{per}(Y)$ *and $L = k$, then this injection is an isomorphism.*

Work of Skorobogatov and Zarhin allows us to extend Theorem 3.1 to Kummer surfaces with geometric Néron–Severi lattice isomorphic to Λ_d. Indeed, if $X = \mathrm{Kum}\, Y$ is a Kummer surface over a field k of characteristic 0 and $\pi : \tilde{Y} \to X$ is the associated degree 2 quotient map then the proof of [SZ12, Theorem 2.4] shows that for any positive integer n, the map π^* induces an injection

$$\frac{(\mathrm{Br}\, X)_n}{(\mathrm{Br}_1\, X)_n} \hookrightarrow \frac{(\mathrm{Br}\, Y)_n}{(\mathrm{Br}_1\, Y)_n}, \tag{3.1}$$

which is an isomorphism if n is odd. (Although [SZ12, Theorem 2.4] assumes that Y is an abelian surface, the proof holds under the weaker assumption that $\overline{Y}$ is an abelian surface.) Since Y has period at most 2 and $\mathrm{NS}\,\overline{Y} \cong \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & d \\ 1 & d & 0 \end{pmatrix}$ by (1.1), we conclude the following.

COROLLARY 3.2. *Let $X = \operatorname{Kum} Y$ be a Kummer surface over a field k of characteristic 0 such that $X \in \mathscr{K}_d$ for some d, and let L, E, and E' be as above. There is a field extension k'/k with $[k' : k] \leqslant 2^4$ such that*

$$\frac{(\operatorname{Br} X)_n}{(\operatorname{Br}_1 X)_n} \hookrightarrow \frac{\operatorname{Hom}_{L'}(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_{L'}}},$$

where L' denotes the compositum of k' and L. If n is odd or Y is the trivial 2-covering, then we may take $k' = k$. If n is odd and $L = k' = k$, then this injection is an isomorphism. □

In Section 3.1 we show that if $f : Y \to A$ is an N-covering of an abelian variety, and if n is coprime to N, then $(\operatorname{Br} Y)_n/(\operatorname{Br}_1 Y)_n$ is isomorphic to $(\operatorname{Br} A)_n/(\operatorname{Br}_1 A)_n$. In Section 3.2, we use [SZ12, Proposition 3.3] to show that for an abelian surface A as above, the group $(\operatorname{Br} A)_n/(\operatorname{Br}_1 A)_n$ injects into a quotient of Galois-invariant homomorphisms between the n-torsion of two elliptic curves. We then combine these ingredients in Section 3.3 to give a proof of Theorem 3.1.

3.1. Brauer groups of N-coverings of abelian varieties.

PROPOSITION 3.3. *Let N be a positive integer, let Y and Y' be principal homogeneous spaces of an abelian variety A, both defined over k, such that there is an N-covering $f : Y' \to Y$. Then for any integer n that is coprime to N, we have*

$$f^* : \frac{(\operatorname{Br} Y)_n}{(\operatorname{Br}_1 Y)_n} \xrightarrow{\sim} \frac{(\operatorname{Br} Y')_n}{(\operatorname{Br}_1 Y')_n}.$$

Proof. Since f is a N-covering, it is dominant and finite of degree N^{2g}. Thus by [ISZ11, Proposition 1.1 and Lemma 1.3], $f^* : \operatorname{Br} \overline{Y} \to \operatorname{Br} \overline{Y}'$ is surjective with kernel killed by N^{2g}, and the kernel of $f^* : \operatorname{Br} Y \to \operatorname{Br} Y'$ is also killed by N^{2g}. This completes the proof of injectivity. We continue with the proof of surjectivity.

The above facts already imply that f^* gives an isomorphism of Galois modules $(\operatorname{Br} \overline{Y})_n \cong (\operatorname{Br} \overline{Y}')_n$ for any integer n coprime to N. Combining the above with [CTS13, Proposition 1.3], we obtain the following commutative diagram with exact rows:

$$\begin{tikzcd}
(\operatorname{Br} Y)_n \arrow[r] \arrow[d, hook, "f^*"] & (\operatorname{Br} \overline{Y})_n^{\Gamma} \arrow[r, "\delta"] \arrow[d, equal, "f^*"] & \mathrm{H}^2(k, \operatorname{Pic} \overline{Y})_n \arrow[d, "f^*"] \\
(\operatorname{Br} Y')_n \arrow[r] & (\operatorname{Br} \overline{Y}')_n^{\Gamma} \arrow[r, "\delta"] & \mathrm{H}^2(k, \operatorname{Pic} \overline{Y}')_n
\end{tikzcd}$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Let $\alpha \in (\operatorname{Br} Y')_n$ and let $\overline{\beta} \in (\operatorname{Br} \overline{Y})_n^{\Gamma}$ be such that $f^*\overline{\beta} = \overline{\alpha} := \alpha \otimes_k \overline{k}$. Since the diagram has exact rows and commutes, this implies that $f^*\delta(\overline{\beta}) = 0$. We claim that the kernel of $f^*\colon \mathrm{H}^2(k, \operatorname{Pic} \overline{Y}) \to \mathrm{H}^2(k, \operatorname{Pic} \overline{Y}')$ is an N-primary group. If so, then $\delta(\overline{\beta}) = 0$ and so $\overline{\beta} = \beta \otimes_k \overline{k}$ for some $\beta \in (\operatorname{Br} Y)_n$. Hence $f^*\beta = \alpha + \alpha_0$ for some $\alpha_0 \in (\operatorname{Br}_1 Y')_n$, which proves surjectivity.

It remains to prove the claim. We factor $f^*\colon \operatorname{Pic} \overline{Y} \to \operatorname{Pic} \overline{Y}'$ as $\operatorname{Pic} \overline{Y} \twoheadrightarrow \operatorname{im} f^* \hookrightarrow \operatorname{Pic} \overline{Y}'$ and consider the two short exact sequences

$$\begin{gathered} 0 \to \ker f^* \to \operatorname{Pic} \overline{Y} \to \operatorname{im} f^* \to 0 \quad \text{and} \\ 0 \to \operatorname{im} f^* \to \operatorname{Pic} \overline{Y}' \to \operatorname{coker} f^* \to 0. \end{gathered}$$

Since $\operatorname{coker} f^*$ and $\ker f^*$ are N-primary, both $\mathrm{H}^1(k, \operatorname{coker} f^*)$ and $\mathrm{H}^2(k, \ker f^*)$ are also N-primary. Thus, by the long exact sequences in cohomology associated to the above two short exact sequences, the kernel of the composition

$$\mathrm{H}^2(k, \operatorname{Pic} \overline{Y}) \to \mathrm{H}^2(k, \operatorname{im} f^*) \to \mathrm{H}^2(k, \operatorname{Pic} \overline{Y}')$$

is also N-primary, which completes the proof of the claim. □

3.2. Brauer groups of abelian surfaces that are geometrically products.

Let A be an abelian surface over k such that $A \in \mathscr{A}_d^1$ for some d. Then by Proposition 2.7, there exists a field extension L/k with $[L : k] \leqslant 12$ and elliptic curves E and E'/L such that $A_L = E \times E'$. Then [SZ12, Proposition 3.3] almost immediately yields the following proposition.

PROPOSITION 3.4. *Let A be an abelian surface over k such that $A \in \mathscr{A}_d^1$ for some d and let E and E' be the associated elliptic curves over the extension L as above. Then for all n we have an injection*

$$\frac{(\operatorname{Br} A)_n}{(\operatorname{Br}_1 A)_n} \hookrightarrow \frac{\operatorname{Hom}_{\Gamma_L}(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_L}}.$$

If $L = k$, then this injection is an isomorphism.

Proof. By [SZ12, Proposition 3.3], we have a canonical isomorphism

$$\frac{(\operatorname{Br} A_L)_n}{(\operatorname{Br}_1 A_L)_n} \cong \frac{\operatorname{Hom}_{\Gamma_L}(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_L}}.$$

Composing with the injection $(\operatorname{Br} A)_n/(\operatorname{Br}_1 A)_n \hookrightarrow (\operatorname{Br} A_L)_n/(\operatorname{Br}_1 A_L)_n$ induced by $\operatorname{Res}_{L/k}$ completes the proof. □

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

3.3. Proof of Theorem 3.1. Recall that $A = \operatorname{Alb} Y$. For any positive integer n, $\mathrm{H}^1(k, A_n)$ surjects onto $\mathrm{H}^1(k, A)_n$, therefore Y can be realized as a $\operatorname{per}(Y)$-covering $f\colon Y \to A$. Let $N := \gcd(\operatorname{per}(Y), n^\infty)$. Then f can be factored as an N-covering $f'\colon Y' \to A$ and a covering $f''\colon Y \to Y'$ whose degree is relatively prime to n. Since Y' is an N-covering of A, there exists a field extension k'/k with $[k' : k] \leqslant \#A_N = N^4$ such that $Y'_{k'} \cong A_{k'}$. We claim that we have the following inclusions and isomorphisms

$$\frac{(\operatorname{Br} Y)_n}{(\operatorname{Br}_1 Y)_n} \xrightarrow{(f''^*)^{-1}} \frac{(\operatorname{Br} Y')_n}{(\operatorname{Br}_1 Y')_n} \hookrightarrow \frac{(\operatorname{Br} Y'_{k'})_n}{(\operatorname{Br}_1 Y'_{k'})_n} \xrightarrow{\sim} \frac{(\operatorname{Br} A_{k'})_n}{(\operatorname{Br}_1 A_{k'})_n} \hookrightarrow \frac{\operatorname{Hom}_{L'}(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_{L'}}}.$$

From left to right, the first map is an isomorphism by Proposition 3.3, the second is an inclusion by the definition of the algebraic Brauer group, the third map is an isomorphism because $Y'_{k'} \cong A_{k'}$, and the last is an inclusion by Proposition 3.4. Furthermore, by Proposition 3.4 the last injection is an isomorphism when $L = k$. □

4. Galois-equivariant homomorphisms between E_n and E'_n

Let E and E' be non-CM elliptic curves over a field k with a geometric cyclic isogeny of degree d between them. Then by Proposition 2.5, there is $\delta \in k^\times/k^{\times 2}$ such that E and E'^δ are k-isogenous.

THEOREM 4.1. *Let E and E' be geometrically isogenous non-CM elliptic curves over a field k of characteristic 0; let d and δ be as above. For any positive integer n we have the following divisibility relations for cardinalities and exponents.*

(1) *If $\delta \in k^{\times 2}$, then*

$$\#\left(\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}}\right) \Bigg| \gcd(d, n) \cdot \#\left(\frac{\operatorname{End}_k(E'_n)}{(\operatorname{End}(\overline{E}')/n)^{\Gamma_k}}\right), \quad \text{and}$$

$$e\left(\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}}\right) \Bigg| \gcd(d, n) \cdot e\left(\frac{\operatorname{End}_k(E'_n)}{(\operatorname{End}(\overline{E}')/n)^{\Gamma_k}}\right).$$

(2) *If $\delta \notin k^{\times 2}$, then*

$$\#\left(\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}}\right) \Bigg| \gcd(2, n)^4 \cdot \gcd(d, n)^2 \cdot \#\left(\frac{\operatorname{End}_{k(\sqrt{\delta})}(E'^\delta_n)}{\operatorname{End}_k(E'^\delta)}\right),$$

and

$$e\left(\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}}\right) \Bigg| \gcd(2, n) \cdot \gcd(d, n)^2 \cdot e\left(\frac{\operatorname{End}_{k(\sqrt{\delta})}(E'^\delta_n)}{\operatorname{End}_k(E'^\delta)}\right).$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Parts (1) and (2) of Theorem 4.1 are proved in Sections 4.2 and 4.3, respectively.

4.1. Galois action on isogenies.

LEMMA 4.2. *Let E and E' be non-CM geometrically isogenous elliptic curves over a field k of characteristic* 0. *Then*

$$(\operatorname{Hom}(\overline{E},\overline{E}')/n)^{\Gamma_k} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if } E, E' \text{ are isogenous over } k \\ \mathbb{Z}/\gcd(2,n)\mathbb{Z} & \text{otherwise.} \end{cases}$$

Proof. Since $\overline{E}$ and $\overline{E}'$ are non-CM isogenous curves, $\operatorname{Hom}(\overline{E},\overline{E}') = \mathbb{Z}\phi$ where ϕ is a cyclic $\overline{k}$-isogeny. By Proposition 2.5 the action of Γ_k on $\operatorname{Hom}(\overline{E},\overline{E}')$ factors through $\operatorname{Gal}(k(\sqrt{\delta})/k)$ for some $\delta \in k^\times/k^{\times 2}$ and $\delta \in k^{\times 2}$ if and only if E and E' are k-isogenous. In the case where $\delta \notin k^{\times 2}$, then Proposition 2.5 implies that ϕ is the composition of a k-rational cyclic isogeny $\phi' \colon E \to E'^{\delta}$ with a $k(\sqrt{\delta})$-isomorphism $E'^{\delta} \to E'$. In particular, the nontrivial element of $\operatorname{Gal}(k(\sqrt{\delta})/k)$ acts on $\operatorname{Hom}(\overline{E},\overline{E}')$ by multiplication by -1. Since

$$(\mathbb{Z}/n\mathbb{Z})^{(x\mapsto -x)} = \frac{n}{\gcd(2,n)}\mathbb{Z}/n\mathbb{Z},$$

this completes the proof. □

4.2. A k-rational cyclic isogeny.

PROPOSITION 4.3. *Let n be a positive integer and let E, E' be non-CM elliptic curves over a field k of characteristic* 0. *Assume that there exists a degree d cyclic k-isogeny $\phi \colon E \to E'$. Then composition with $\phi^\vee$ induces a homomorphism*

$$\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E},\overline{E}')/n)^{\Gamma_k}} \xrightarrow{(-\circ\phi^\vee)} \frac{\operatorname{End}_k(E'_n)}{(\operatorname{End}(\overline{E}')/n)^{\Gamma_k}},$$

where the kernel is a cyclic group of order dividing $m := \gcd(d,n)$ and the cokernel is m-torsion.

Theorem 4.1(1) is a corollary of this proposition.

To prove the Proposition, we begin with two lemmas.

LEMMA 4.4. *Let E, E', E'' be elliptic curves, let $g \colon E \to E'$ be a cyclic isogeny of degree d, and let n, n' be positive integers such that $n' \gcd(d,n) = \gcd(dn',n)$.*

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Then $f \in \mathrm{Hom}(E_n, E''_n)$ *factors through* $[n'] \circ g$ *if and only if* $f \circ g^\vee \circ [n/\gcd(dn', n)] = 0 \in \mathrm{Hom}(E'_n, E''_n)$.

Proof. Assume that f factors through $[n'] \circ g$, that is, that $f = h \circ [n'] \circ g$ for some $h \in \mathrm{Hom}(E'_n, E''_n)$. Then

$$\begin{aligned} f \circ g^\vee \circ \left[\frac{n}{\gcd(dn', n)}\right] &= h \circ [n'] \circ g \circ g^\vee \circ \left[\frac{n}{\gcd(dn', n)}\right] \\ &= h \circ \left[\frac{dn'}{\gcd(dn', n)}\right] \circ [n] = 0 \end{aligned}$$

in $\mathrm{Hom}(E'_n, E''_n)$.

Now let $f \in \mathrm{Hom}(E_n, E''_n)$ be such that $f \circ g^\vee \circ [n/\gcd(dn', n)] = 0 \in \mathrm{Hom}(E'_n, E''_n)$. We show that $\ker f$ contains $\ker([n'] \circ g)$ which implies that f factors through $[n'] \circ g$. By definition of the dual isogeny, $E'_d / \ker g^\vee \cong g^\vee(E'_d) = \ker(g \colon E \to E')$. Similarly, since $n' \gcd(d, n) = \gcd(dn', n)$, we have

$$\ker([n'] \circ g \colon E_n \to E'_n) = g^\vee(E'_{n' \gcd(d,n)}) = \left(g^\vee \circ \left[\frac{n}{\gcd(dn', n)}\right]\right)(E'_n).$$

Since $f \circ g^\vee \circ [n/\gcd(dn', n)] = 0$, this gives the desired containment. □

LEMMA 4.5. *Let* n *be a positive integer and let* E, E' *be elliptic curves over* k. *Assume that there exists a cyclic degree* d k*-isogeny* $\phi \colon E \to E'$. *Then there is a short exact sequence of* Γ_k*-modules*

$$0 \to \mathrm{Hom}(\phi(E_m), E'_m) \xrightarrow{-\circ\phi\circ[n/m]} \mathrm{Hom}(E_n, E'_n) \xrightarrow{-\circ\phi^\vee} H \to 0,$$

where $m = \gcd(d, n)$ *and* $H := \{f \in \mathrm{End}(E'_n) : f \circ \phi \circ [n/m] = 0\}$.

Proof. The first map is clearly injective. Thus to prove the lemma, it suffices to compute the kernel and image of

$$(- \circ \phi^\vee) \colon \mathrm{Hom}(E_n, E'_n) \to \mathrm{End}(E'_n).$$

An application of Lemma 4.4 with $n' = 1$ and $g = \phi^\vee$ implies that the image of $(- \circ \phi^\vee)$ is equal to H. Another application of Lemma 4.4 with $n' = n/m$ and $g = \phi$ shows that the kernel of $(- \circ \phi^\vee)$ is equal to the image of $\mathrm{Hom}(\phi(E_m), E'_n)$, which completes the proof. □

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Proof of Proposition 4.3. We consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & \frac{n}{m}\mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, hook] & \mathrm{Hom}_k(\phi(E_m), E'_m) \arrow[r] \arrow[d, hook] & \ker(- \circ \phi^\vee) \arrow[d, hook] & \\
0 \arrow[r] & (\mathrm{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k} \arrow[r] \arrow[d, "(-\circ\phi^\vee)"] & \mathrm{Hom}_k(E_n, E'_n) \arrow[r] \arrow[d, "(-\circ\phi^\vee)"] & \dfrac{\mathrm{Hom}_k(E_n, E'_n)}{(\mathrm{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}} \arrow[r] \arrow[d, "(-\circ\phi^\vee)"] & 0 \\
0 \arrow[r] & (\mathrm{End}(\overline{E}')/n)^{\Gamma_k} \arrow[r] \arrow[d] & \mathrm{End}_k(E'_n) \arrow[r] \arrow[d] & \dfrac{\mathrm{End}_k(E'_n)}{(\mathrm{End}(\overline{E}')/n)^{\Gamma_k}} \arrow[r] \arrow[d] & 0 \\
 & \mathbb{Z}/m\mathbb{Z} \arrow[r] & \dfrac{\mathrm{End}_k(E'_n)}{\mathrm{Hom}_k(E_n, E'_n) \circ \phi^\vee} \arrow[r] & \mathrm{coker}(- \circ \phi^\vee) \arrow[r] & 0
\end{tikzcd}$$

We claim that this diagram is commutative and has exact rows and columns. The commutativity and exactness of the middle two rows is clear. Since E and E' are non-CM and ϕ is a k-isogeny, $\mathrm{Hom}(\overline{E}, \overline{E}') = \mathbb{Z}\phi$ and $\mathrm{End}(\overline{E}') = \mathbb{Z}$ as Galois modules. Thus the leftmost column is exact. The rightmost column is exact by definition. Taking Γ_k-invariants of the exact sequence in Lemma 4.5 gives exactness of the middle column. Since the maps in the top and bottom rows are induced by the maps in the middle two, the remaining squares commute.

The proposition is concerned with the rightmost column of the above diagram; we must prove that $\ker(- \circ \phi^\vee)$ is a cyclic group of order dividing m and that $\mathrm{coker}(- \circ \phi^\vee)$ is m-torsion. Let $f \in \mathrm{End}_k(E'_n)$ and let $a \in \mathbb{Z}$ be an inverse of d/m modulo n; then

$$[m] \circ f = f \circ [m] = f \circ [ad] = (f \circ [a] \circ \phi) \circ \phi^\vee \in \mathrm{Hom}_k(E_n, E'_n) \circ \phi^\vee.$$

Hence $\mathrm{End}_k(E'_n)/(\mathrm{Hom}_k(E_n, E'_n) \circ \phi^\vee)$ is m-torsion and thus so is $\mathrm{coker}(- \circ \phi^\vee)$.

Now consider $\mathrm{Hom}_k(\phi(E_m), E'_m)$. Since $m \mid d$, we have $\phi(E_m)$ is a cyclic group of order m. Thus after fixing a generator of $\phi(E_m)$, we have $\mathrm{Hom}(\phi(E_m), E'_m) \cong E'_m \cong (\mathbb{Z}/m\mathbb{Z})^2$ as abelian groups. Therefore, the quotient $\mathrm{Hom}_k(\phi(E_m), E'_m)/((n/m)\mathbb{Z}/n\mathbb{Z})$ is a subgroup of the cyclic group of order m.

We claim that the bottom leftmost horizontal arrow is injective. If so, then the snake lemma implies that

$$\ker(- \circ \phi^\vee) \cong \frac{\mathrm{Hom}_k(\phi(E_m), E'_m)}{(n/m)\mathbb{Z}/n\mathbb{Z}} \subset \mathbb{Z}/m\mathbb{Z},$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

as desired. To prove the claim, it suffices to show that for $b \in \mathbb{Z}$, $[b] \in \operatorname{End}(E'_n)$ is in the image of $(- \circ \phi^\vee)$ only if $m \mid b$. By Lemma 4.5, $[b]$ is in the image of $(- \circ \phi^\vee)$ if and only if $[b] \circ \phi \circ [n/m] = \phi \circ [bn/m] = 0$ on E_n. This happens if and only if $m \mid b$. □

4.3. A geometric, non k-rational isogeny.

In this section we consider the case of two non-CM geometrically isogenous elliptic curves E, E' over k that are *not* k-isogenous. By Proposition 2.5, there exists a unique nontrivial $\delta \in k^\times/k^{\times 2}$ such that E and E'^δ are k-isogenous.

PROPOSITION 4.6. *Let E and E' be non-CM geometrically isogenous elliptic curves over k, that are not isogenous over k and let $\delta \in k^\times/k^{\times 2}$ be such that E and E'^δ are k-isogenous. Let d be the degree of a cyclic isogeny between E and E'^δ. Then there is a homomorphism*

$$\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}} \to \frac{\operatorname{End}_{k(\sqrt{\delta})}(E'^\delta_n)}{\operatorname{End}_k(E'^\delta_n)}$$

whose kernel has order at most $\gcd(2,n)^4 \gcd(d,n)^2$ *and exponent at most* $\gcd(2,n)\gcd(d,n)^2$.

Theorem 4.1(2) is a corollary of this proposition.

The homomorphism in Proposition 4.6 is obtained as the composition of two homomorphisms:

$$\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}} \to \frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^\delta_n)}{\operatorname{Hom}_k(E_n, E'^\delta_n)} \quad \text{and}$$
$$\frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^\delta_n)}{\operatorname{Hom}_k(E_n, E'^\delta_n)} \to \frac{\operatorname{End}_{k(\sqrt{\delta})}(E'^\delta_n)}{\operatorname{End}_k(E'^\delta_n)}.$$

We first study each homomorphism individually.

PROPOSITION 4.7. *Let E and E' be non-CM elliptic curves over k. Assume that there exists a nontrivial $\delta \in k^\times/k^{\times 2}$ such that E and E'^δ are isogenous over k. Then there is an exact sequence.*

$$0 \to \frac{\operatorname{Hom}_k(E_n, E'_{\gcd(2,n)})}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}} \to \frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}} \to \frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^\delta_n)}{\operatorname{Hom}_k(E_n, E'^\delta_n)}$$

Proof. First let us verify that each quotient is defined. This is immediate for the middle and right quotient. The left quotient is defined by Lemma 4.2.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Over $k(\sqrt{\delta})$, E' and E'^{δ} are isomorphic. Fix a $k(\sqrt{\delta})$-isomorphism $f\colon E' \xrightarrow{\sim} E'^{\delta}$. Then we have a homomorphism

$$\operatorname{Hom}_k(E_n, E'_n) \to \frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^{\delta}_n)}{\operatorname{Hom}_k(E_n, E'^{\delta}_n)}, \quad \psi \mapsto f \circ \psi.$$

The kernel of this homomorphism consists of all maps $\psi \in \operatorname{Hom}_k(E_n, E'_n)$ such that $f \circ \psi$ is Γ_k-invariant. If $\sigma \in \Gamma_{k(\sqrt{\delta})}$, then by assumption $f^{\sigma} = f$ and $\psi^{\sigma} = \psi$. Let $\sigma \in \Gamma_k \setminus \Gamma_{k(\sqrt{\delta})}$; then $(f \circ \psi)^{\sigma} = f^{\sigma} \circ \psi^{\sigma} = -f \circ \psi$. Thus, if $(f \circ \psi)^{\sigma} = f \circ \psi$, we have $-f \circ \psi = f \circ \psi$. Since f is an isomorphism, this implies that $2\psi = 0$, or equivalently that $\operatorname{im} \psi \subset E'_{\gcd(2,n)}$. Thus, we have an exact sequence.

$$0 \to \operatorname{Hom}_k(E_n, E'_{\gcd(2,n)}) \to \operatorname{Hom}_k(E_n, E'_n) \to \frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^{\delta}_n)}{\operatorname{Hom}_k(E_n, E'^{\delta}_n)}$$

Lemma 4.2 then completes the proof. □

PROPOSITION 4.8. *Let n be a positive integer, let E, $\widetilde{E}$ be non-CM elliptic curves over a field k, let k'/k be a quadratic extension, and let χ be the quadratic character associated to k'/k. Assume that there exists a cyclic k-isogeny $\phi\colon E \to \widetilde{E}$, let $d = \deg(\phi)$, and let $m = \gcd(d, n)$. Then composition with $\phi^{\vee}$ induces a homomorphism*

$$\frac{\operatorname{Hom}_{k'}(E_n, \widetilde{E}_n)}{\operatorname{Hom}_k(E_n, \widetilde{E}_n)} \to \frac{\operatorname{End}_{k'}(\widetilde{E}_n)}{\operatorname{End}_k(\widetilde{E}_n)}.$$

Furthermore, the kernel K of this homomorphism fits in an exact sequence

$$0 \to \frac{\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)}{\operatorname{Hom}_k(\phi(E_m), \widetilde{E}_m)} \to K \to \operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)^{\chi}$$

so K is a finite abelian group with order dividing $m^2 \gcd(m, 2)$ and exponent dividing m^2.

Proof. Let $H := \{f \in \operatorname{End}(\widetilde{E}_n) : f \circ \phi \circ [n/m] = 0\}$. By Lemma 4.5, we have an exact sequence of Γ_k-modules

$$0 \to \operatorname{Hom}(\phi(E_m), \widetilde{E}_m) \to \operatorname{Hom}(E_n, \widetilde{E}_n) \to H \to 0.$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

By taking the long exact sequences in Galois cohomology for Γ_k and $\Gamma_{k'}$, we have the following commutative diagram with exact rows and columns.

$$\begin{tikzcd}
 & \operatorname{Hom}_k(\phi(E_m), \widetilde{E}_m) \arrow[r, hook, "\operatorname{Res}_{k'/k}"] \arrow[d, hook] & \operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m) \arrow[d, hook] & & \\
0 \arrow[r] & \operatorname{Hom}_k(E_n, \widetilde{E}_n) \arrow[r, "\operatorname{Res}_{k'/k}"] \arrow[d, "(-\circ\phi^\vee)"] & \operatorname{Hom}_{k'}(E_n, \widetilde{E}_n) \arrow[r] \arrow[d, "(-\circ\phi^\vee)"] & \dfrac{\operatorname{Hom}_{k'}(E_n, \widetilde{E}_n)}{\operatorname{Hom}_k(E_n, \widetilde{E}_n)} \arrow[r] \arrow[d, "(-\circ\phi^\vee)"] & 0 \\
0 \arrow[r] & H^{\Gamma_k} \arrow[r, "\operatorname{Res}_{k'/k}"] \arrow[d, "\partial_k"] & H^{\Gamma_{k'}} \arrow[r] \arrow[d, "\partial_{k'}"] & \dfrac{H^{\Gamma_{k'}}}{H^{\Gamma_k}} \arrow[r] & 0 \\
 & \mathrm{H}^1(\Gamma_k, \operatorname{Hom}(\phi(E_m), \widetilde{E}_m)) \arrow[r, "\operatorname{Res}_{k'/k}"] & \mathrm{H}^1(\Gamma_{k'}, \operatorname{Hom}(\phi(E_m), \widetilde{E}_m)) & &
\end{tikzcd}$$

Since the inclusion $H \hookrightarrow \operatorname{End}(\widetilde{E}_n)$ induces an inclusion $H^{\Gamma_{k'}}/H^{\Gamma_k} \hookrightarrow \operatorname{End}_{k'}(\widetilde{E}_n)/\operatorname{End}_k(\widetilde{E}_n)$, K is the kernel of the rightmost vertical map in the above diagram. Hence, the snake lemma applied to the middle two rows yields

$$0 \to \frac{\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)}{\operatorname{Hom}_k(\phi(E_m), \widetilde{E}_m)} \to K \to \ker(\operatorname{Res}_{k'/k} \colon \operatorname{im} \partial_k \to \operatorname{im} \partial_{k'}) \to 0.$$

By the inflation–restriction exact sequence, $\ker(\operatorname{Res}_{k'/k} \colon \operatorname{im} \partial_k \to \operatorname{im} \partial_{k'})$ is contained in $\mathrm{H}^1(\Gamma_k/\Gamma_{k'}, \operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m))$. The cocycle condition implies that the nontrivial element of $\Gamma_k/\Gamma_{k'}$ must be sent to an element of $\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)^\chi$ which yields the desired exact sequence for K.

Since $m \mid d$, we have a group isomorphism $\phi(E_m) \cong \mathbb{Z}/m\mathbb{Z}$, and so $\operatorname{Hom}(\phi(E_m), \widetilde{E}_m)$ is (non-canonically) isomorphic to $\widetilde{E}_m \cong (\mathbb{Z}/m\mathbb{Z})^2$. On the other hand, the natural inclusion $\phi(E_m) \subset \widetilde{E}_m$, together with composition by multiplication by an integer, shows that $\operatorname{Hom}_k(\phi(E_m), \widetilde{E}_m)$ contains $\mathbb{Z}/m\mathbb{Z}$. Thus $\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)/\operatorname{Hom}_k(\phi(E_m), \widetilde{E}_m)$ is a cyclic group of order dividing m.

Now we consider $\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)^\chi$. We have already shown that $\operatorname{Hom}(\phi(E_m), \widetilde{E}_m) \cong (\mathbb{Z}/m\mathbb{Z})^2$. The natural inclusion $\phi(E_m) \subset \widetilde{E}_m$ and its compositions with multiplication by an integer yield a Γ_k-homomorphism $\mathbb{Z}/m\mathbb{Z} \hookrightarrow \operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)$. However, the only such maps that satisfy $\psi^\sigma = -\psi$ are those in the image of the subgroup $(m/\gcd(m, 2))\mathbb{Z}/m\mathbb{Z}$. Thus, $\operatorname{Hom}_{k'}(\phi(E_m), \widetilde{E}_m)^\chi$ is a subgroup of $\mathbb{Z}/\gcd(m, 2)\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Hence, K is an abelian extension of a subgroup of $\mathbb{Z}/\gcd(m, 2)\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ by a subgroup of $\mathbb{Z}/m\mathbb{Z}$. □

Proof of Proposition 4.6. Consider the homomorphism φ obtained as the composition of

$$\frac{\operatorname{Hom}_k(E_n, E'_n)}{(\operatorname{Hom}(\overline{E}, \overline{E}'))/n)^{\Gamma_k}} \xrightarrow{\varphi_1} \frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, E'^{\delta}_n)}{\operatorname{Hom}_k(E_n, E'^{\delta}_n)} \quad \text{and}$$
$$\frac{\operatorname{Hom}_{k(\sqrt{\delta})}(E_n, (E')^{\delta}_n)}{\operatorname{Hom}_k(E_n, E'^{\delta}_n)} \xrightarrow{\varphi_2} \frac{\operatorname{End}_{k(\sqrt{\delta})}((E')^{\delta}_n)}{\operatorname{End}_k(E'^{\delta}_n)},$$

where φ_1 is as in Proposition 4.7 and φ_2 is as in Proposition 4.8. Hence $\ker\varphi$ is an extension of a subgroup of $\ker\varphi_2$ by $\ker\varphi_1$ and so

$$\#(\ker\varphi) \mid \#(\ker\varphi_1)\#(\ker\varphi_2) \quad \text{and} \quad e(\ker\varphi) \mid e(\ker\varphi_1)e(\ker\varphi_2).$$

The exponent and order of $\ker\varphi_2$ are bounded by Proposition 4.8, so it remains to study $\ker\varphi_1$. By Proposition 4.7,

$$\ker\varphi_1 = \frac{\operatorname{Hom}_k(E_n, E'_{\gcd(2,n)})}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}}.$$

Since $E'_{\gcd(2,n)} \cong (\mathbb{Z}/\gcd(2,n)\mathbb{Z})^2$, a choice of 2 generators for E_n determines a group isomorphism $\operatorname{Hom}(E_n, E'_{\gcd(2,n)}) \cong E'^2_{\gcd(2,n)} \cong (\mathbb{Z}/\gcd(2,n)\mathbb{Z})^4$. Hence by Lemma 4.2, $\ker\varphi_1$ is a subgroup of $(\mathbb{Z}/\gcd(2,n)\mathbb{Z})^3$. □

5. Elliptic curves and abelian representations

5.1. Galois-equivariant endomorphisms of E_n.

Let n be a positive integer and let E be an elliptic curve over a field k of characteristic 0. Let

$$\rho_{E,n} : \Gamma_k \to \operatorname{Aut}(E_n) \cong \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

denote the Galois representation coming from the action of Galois on the n-torsion of E, and let $G_{E,n}$ denote the quotient of the image of $\rho_{E,n}$ modulo scalar matrices.

The image of $\rho_{E,n}$ determines the ring of Galois-equivariant endomorphisms of E_n, namely $\operatorname{End}_k(E_n)$ is the subring of $\operatorname{End}(E_n)$ that commutes with all elements of $\rho_{E,n}(\Gamma_k)$.

PROPOSITION 5.1. *Let ℓ be a prime, let s be a positive integer, and let E be an elliptic curve over a field k of characteristic* 0. *Then*

$$\dim_{\mathbb{F}_\ell} \frac{\operatorname{End}_k(E_{\ell^s})}{\operatorname{End}_k(E_{\ell^{s-1}}) \circ [\ell]} = \begin{cases} 4 & \text{if } G_{E,\ell^s} = \{1\}, \\ 2 & \text{if } G_{E,\ell^s} \neq \{1\} \text{ and } \operatorname{im}(\rho_{E,\ell^s}) \text{ is abelian, and} \\ 1 & \text{if } \operatorname{im}(\rho_{E,\ell^s}) \text{ is nonabelian.} \end{cases}$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Corollary 5.2. *Let E be an elliptic curve over k and let n be a positive integer. Then we have an isomorphism of abelian groups*

$$\operatorname{End}_k(E_n) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times (\mathbb{Z}/n_2\mathbb{Z})^2$$

for positive integers $n_2|n_1|n$. Furthermore, n_1 is the largest integer dividing n such that $\operatorname{Gal}(k(E_{n_1})/k)$ is abelian and n_2 is the largest integer dividing n such that $\operatorname{Gal}(k(E_{n_2})/k) \subset (\mathbb{Z}/n_2\mathbb{Z})^\times$ where $a \in (\mathbb{Z}/n_2\mathbb{Z})^\times$ acts by $P \mapsto aP$. If E is non-CM, then $(\operatorname{End}_k(\overline{E})/n)^{\Gamma_k} \cong \mathbb{Z}/n\mathbb{Z}$ and hence

$$\frac{\operatorname{End}_k(E_n)}{(\operatorname{End}_k(\overline{E})/n)^{\Gamma_k}} \cong \mathbb{Z}/n_1\mathbb{Z} \times (\mathbb{Z}/n_2\mathbb{Z})^2.$$

Proof. Note that $k(E_n)$ is the compositum of $k(E_{\ell^{n(\ell)}})$ where $n(\ell) = v_\ell(n)$. Thus, we have an inclusion

$$\operatorname{Gal}(k(E_n)/k) \hookrightarrow \prod_\ell \operatorname{Gal}(k(E_{\ell^{n(\ell)}})/k) \cong \prod_\ell \operatorname{im}\rho_{E,\ell^{n(\ell)}}.$$

Furthermore, for each prime ℓ we have a surjection $\operatorname{Gal}(k(E_n)/k) \to \operatorname{Gal}(k(E_{\ell^{n(\ell)}})/k) \cong \operatorname{im}\rho_{E,\ell^{n(\ell)}}$. Hence, $\operatorname{Gal}(k(E_n)/k)$ is abelian if and only if $\operatorname{Gal}(k(E_{\ell^{n(\ell)}})/k)$ is abelian for all primes ℓ and $\operatorname{im}\rho_{E,n} \subset (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\operatorname{im}\rho_{E,\ell^{n(\ell)}} \subset (\mathbb{Z}/\ell^{n(\ell)}\mathbb{Z})^\times$ for all primes ℓ.

Since $\operatorname{End}_k(E_n) \subset \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$, the fundamental theorem of finitely generated abelian groups implies that

$$\operatorname{End}_k(E_n) \cong \mathbb{Z}/n_0\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z}$$

for unique positive integers $n_3|n_2|n_1|n_0|n$. Note that $\operatorname{End}_k(E_n)$ always contains the image of $\mathbb{Z} \hookrightarrow \operatorname{End}(E) \to \operatorname{End}(E_n)$, so $n_0 = n$. Additionally, for any prime ℓ and any positive integer s with $\ell^s \mid n$, Proposition 5.1 shows that:

(1) $\ell^s|n_2 = n_3$ if and only if $G_{E,\ell^s} = \{1\}$; and

(2) $\ell^s|n_1$ if and only if $\operatorname{im}\rho_{E,\ell^s}$ is abelian.

Combining these facts with the above arguments completes the proof. □

Corollary 5.3. *Let E be an elliptic curve over k and let n be a positive integer. Let k'/k be a field extension. Then we have an isomorphism of abelian groups*

$$\frac{\operatorname{End}_{k'}(E_n)}{\operatorname{End}_k(E_n)} \cong \mathbb{Z}\Big/\frac{n_1'}{n_1}\mathbb{Z} \times \left(\mathbb{Z}\Big/\frac{n_2'}{n_2}\mathbb{Z}\right)^2,$$

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

where n_1' (respectively n_1) is the largest integer dividing n such that $\mathrm{Gal}(k'(E_{n_1'})/k')$ *(respectively* $\mathrm{Gal}(k(E_{n_1})/k)$*) is abelian and n_2' (respectively n_2) is the largest integer dividing n such that* $\mathrm{Gal}(k'(E_{n_2'})/k') \subset (\mathbb{Z}/n_2'\mathbb{Z})^\times$ *(respectively* $\mathrm{Gal}(k(E_{n_2})/k) \subset (\mathbb{Z}/n_2\mathbb{Z})^\times$*).*

Proof. This follows from Corollary 5.2. □

The following lemma will be useful in the proof of Proposition 5.1.

LEMMA 5.4. *Let ℓ be a prime, let s be a positive integer, and let $A \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ be a non-central element. Let $\mu < s$ be the maximal non-negative integer such that $A \in \mathbb{Z}I \bmod \mathrm{M}_2(\ell^\mu\mathbb{Z}/\ell^s\mathbb{Z})$. Then the ring*

$$\frac{\{M \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z}) : AM = MA\}}{\{M \in \mathrm{M}_2(\ell^{s-\mu}\mathbb{Z}/\ell^s\mathbb{Z}) : AM = MA\}}$$

is generated by I and a matrix A' such that $\ell^\mu A' - A \in \mathbb{Z}I$.

Proof. Let $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. Since A is not in the centre of $\mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$, at least one of $\alpha - \delta$, β, or γ is nonzero modulo ℓ^s and so the quantity $\min(v_\ell(\alpha - \delta), v_\ell(\beta), v_\ell(\gamma))$ is well-defined, and is equal to $\mu < s$. An elementary algebra calculation shows that a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ commutes with A if and only if $(a - d, b, c)^T$ is in the kernel of

$$\begin{pmatrix} \beta & \delta - \alpha & 0 \\ \gamma & 0 & \delta - \alpha \\ 0 & \gamma & -\beta \end{pmatrix}.$$

Let $v_0, v_1, v_2 \in \mathbb{Z}/\ell^s\mathbb{Z}$ be such that $(\ell^\mu v_0, \ell^\mu v_1, \ell^\mu v_2) = (\alpha - \delta, \beta, \gamma)$. Note that v_0, v_1 and v_2 are unique modulo $\ell^{s-\mu}$ and at least one of v_0, v_1, v_2 is nonzero modulo ℓ. Then $(v_0, v_1, v_2)^T$ is in the kernel of the above 3×3 matrix and indeed generates the kernel modulo $(\ell^{s-\mu}\mathbb{Z}/\ell^s\mathbb{Z})^3$. Thus, any matrix M that commutes with A is such that $\ell^\mu M \in \mathbb{Z}A + \mathbb{Z}I$. This completes the proof. □

Proof of Proposition 5.1. After fixing a basis for E_{ℓ^s}, we identify $\mathrm{End}(E_{\ell^s})$ with $\mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ and $\mathrm{Aut}(E_{\ell^s})$ with $\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. If $G_{E,\ell^s} = \{1\}$, then $\mathrm{End}_k(E_{\ell^s}) = \mathrm{End}(E_{\ell^s})$ so the result is immediate.

Now assume that the image of ρ_{E,ℓ^s} is nonabelian, and let M_1 and M_2 be two elements in the image that do not commute with each other. Suppose that $\mathrm{End}_k(E_{\ell^s})/(\mathrm{End}_k(E_{\ell^{s-1}}) \circ [\ell])$ is an $\mathbb{F}_\ell$-vector space of dimension greater than

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

1 and let $A \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ be a matrix representing a non-scalar element. Since A mod ℓ is not a scalar matrix, Lemma 5.4 implies that M_1 and M_2 must both be linear combinations of I and A. As M_1 and M_2 do not commute with each other, this gives a contradiction. Hence, $\mathrm{End}_k(E_{\ell^s})/(\mathrm{End}_k(E_{\ell^{s-1}}) \circ [\ell])$ consists only of scalar matrices.

It remains to consider the case that $G_{E,\ell^s} \neq \{1\}$ and that the image of ρ_{E,ℓ^s} is abelian. Fix an element $A \in \mathrm{im}\,\rho_{E,\ell^s}$ that does not reduce to the identity in G_{E,ℓ^s}. Since $\mathrm{im}\,\rho_{E,\ell^s}$ is abelian, Lemma 5.4 implies that $\mathrm{im}\,\rho_{E,\ell^s} \mod \mathrm{M}_2(\ell\mathbb{Z}/\ell^s\mathbb{Z})$ is contained in the ring generated by I and A' where $\ell^\mu A' - A \in \mathbb{Z}I$ for a maximal μ. Hence,

$$\frac{\mathrm{End}_k(E_{\ell^s})}{\mathrm{End}_k(E_{\ell^{s-1}}) \circ [\ell]} = \frac{\{M \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z}) : A'M = MA'\}}{\{M \in \mathrm{M}_2(\ell\mathbb{Z}/\ell^s\mathbb{Z}) : A'M = MA'\}}.$$

Another application of Lemma 5.4 then shows that this quotient is 2-dimensional. □

5.2. Abelian subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$.

PROPOSITION 5.5. *Let s be a positive integer, and put $s' = \lceil s/2 \rceil$. Let ℓ be a prime, and let $H < \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ be an abelian subgroup. There exists $A' \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ with $A' \bmod \ell \notin \langle I \rangle$ such that the group $H \bmod \mathrm{M}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z})$ is contained in the ring $\langle I, A' \bmod \ell^{s'}\mathbb{Z}\rangle$. Consequently, $\#H \leqslant \ell^{3s}$.*

Proof. For $A \in H$, define $\mu_A = \max\{\mu : A \equiv \text{scalar matrix} \bmod \ell^\mu\}$, and let $\mu = \min\{\mu_A : A \in H\}$. Pick $A \in H$ such that $\mu_A = \mu$, and let $A' \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ be a matrix such that $\ell^\mu A' - A \in \mathbb{Z}I$. If $\mu < s/2$ then $s - \mu \geqslant s'$ and so Lemma 5.4 shows that $H \bmod M_2(\ell^{s-\mu}\mathbb{Z}/\ell^s\mathbb{Z})$ is contained in the ring $\langle I, A'\rangle$. On the other hand, if $\mu \geqslant s'$ then for every $A \in H$, the matrix $A \bmod \ell^{s'}\mathbb{Z}$ is a scalar matrix, by definition of μ, and so is contained in the ring $\langle I, A'\rangle$ for any matrix $A' \in \mathrm{M}_2(\mathbb{Z}/\ell^s\mathbb{Z})$.

Now we show the bound $\#H \leqslant \ell^{3s}$ holds. Let H' be the group $H \bmod \mathrm{M}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z})$. Reduction modulo $\ell^{s'}$ gives rise to an exact sequence of finite abelian groups

$$0 \to K \to H \to H' \to 0,$$

where K is the kernel of reduction. Our work above shows that an element of H' is a linear combination of I and A' with coefficients in $\mathbb{Z}/\ell^{s'}\mathbb{Z}$, and hence $\#H' \leqslant (\ell^{s'})^2$. To bound the order of K, we note that K is contained in the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) \to \mathrm{GL}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z})$. An element of this kernel has the form $I + M$ for some $M \in \mathrm{M}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z})$. Hence $\#K \leqslant (\ell^{s-s'})^4$. Putting

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

these facts together, we obtain

$$\#H \leqslant (\ell^{s'})^2 \cdot (\ell^{s-s'})^4 = (\ell^s)^2(\ell^{s-s'})^2 \leqslant (\ell^s)^2(\ell^{\lfloor s/2 \rfloor})^2 \leqslant \ell^{3s}. \qquad \square$$

COROLLARY 5.6. *Let ℓ be an odd prime, let s be a positive integer, let $s' := \lceil s/2 \rceil$, and let $H < \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ be an abelian subgroup. Then $H \bmod \mathrm{M}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z})$ is conjugate to a subgroup of one of the following groups.*

$$C_s(\ell^{s'}) := \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in (\mathbb{Z}/\ell^{s'}\mathbb{Z})^\times \right\}$$

$$C_{ns}^{t,\overline{\varepsilon}}(\ell^{s'}) := \left\{ \begin{pmatrix} x & \varepsilon\ell^t y \\ y & x \end{pmatrix} : (x, y) \in (\mathbb{Z}/\ell^{s'}\mathbb{Z})^2, x^2 - \varepsilon\ell^t y^2 \notin \ell\mathbb{Z}/\ell^{s'}\mathbb{Z} \right\},$$

$0 \leqslant t \leqslant s' - 1$,

$\overline{\varepsilon} \in (\mathbb{Z}/\ell^{s'-t}\mathbb{Z})^\times \big/ (\mathbb{Z}/\ell^{s'-t}\mathbb{Z})^{\times 2}$, $\varepsilon \in (\mathbb{Z}/\ell^{s'}\mathbb{Z})^\times$

fixed such that $\varepsilon \mapsto \overline{\varepsilon}$,

and $\varepsilon, \overline{\varepsilon}, t$ chosen such that $\varepsilon\ell^t$ is not a square

$$B_{ab}^t(\ell^{s'}) := \left\{ \begin{pmatrix} x & y \\ 0 & x + \ell^t y \end{pmatrix} : x \in (\mathbb{Z}/\ell^{s'}\mathbb{Z})^\times, y \in \mathbb{Z}/\ell^{s'}\mathbb{Z} \right\}, \quad 1 \leqslant t \leqslant s'.$$

Proof. By Proposition 5.5, $H \bmod \mathrm{M}_2(\ell^{s'}\mathbb{Z}/\ell^s\mathbb{Z}) \subset \langle I, A' \bmod \ell^{s'}\mathbb{Z} \rangle$ for some A' such that $A' \bmod \ell$ is not a scalar matrix. If we show that such an A' is conjugate to a matrix of the form

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \quad \begin{pmatrix} x & \varepsilon\ell^t y \\ y & x \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} x & y \\ 0 & x + \ell^t y \end{pmatrix}$$

(with ε, t as above), then H must be contained in $C_s(\ell^{s'})$, $C_{ns}^{t,\overline{\varepsilon}}(\ell^{s'})$ or $B_{ab}^t(\ell^{s'})$ as desired.

Since $\overline{A'} := A' \bmod \ell$ is not a scalar matrix, the minimal polynomial of $\overline{A'}$ has degree 2 and thus is equal to the characteristic polynomial of $\overline{A'}$ which is also equal to the mod ℓ reduction of the characteristic polynomial of A'. Thus by [McD78, Theorems II.4 and III.2], A' is conjugate to a matrix of the form $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ or $\begin{pmatrix} 0 & -\det(A') \\ 1 & \mathrm{tr}(A') \end{pmatrix}$, with the first case occurring if and only if the characteristic polynomial of A' has two roots in $\mathbb{Z}/\ell^s\mathbb{Z}$ that are distinct modulo ℓ.

Now assume that the characteristic polynomial of A' is reducible and the characteristic polynomial of $A' \bmod \ell$ is a square. Then the roots of the characteristic polynomial are of the form $x, x + \ell^t y$ for some $1 \leqslant t \leqslant s$, x, $y \in \mathbb{Z}/\ell^s\mathbb{Z}$; we may assume that y is invertible by taking t maximally. By the above, this is equivalent to the case where A' is conjugate to $\begin{pmatrix} 0 & -x^2 - \ell^t xy \\ 1 & 2x + \ell^t y \end{pmatrix}$.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Then we observe that

$$\begin{pmatrix} 0 & y \\ 1 & x+\ell^t y \end{pmatrix} \begin{pmatrix} 0 & -x^2 - xy\ell^t \\ 1 & 2x+\ell^t y \end{pmatrix} \begin{pmatrix} 0 & y \\ 1 & x+\ell^t y \end{pmatrix}^{-1} = \begin{pmatrix} x & y \\ 0 & x+\ell^t y \end{pmatrix},$$

so A' has the desired form.

It remains to consider the case when the characteristic polynomial of A' is irreducible in $(\mathbb{Z}/\ell^s\mathbb{Z})[T]$. In this case, since ℓ is odd, the discriminant $\operatorname{tr}(A')^2 - 4\det(A')$ is not a square. Hence, we must have

$$\det(A') = x^2 - \varepsilon\ell^t y^2,$$

where $0 \leqslant t \leqslant s-1$, ε any fixed lift of an element in $(\mathbb{Z}/\ell^{s-t}\mathbb{Z})^\times \big/ (\mathbb{Z}/\ell^{s-t}\mathbb{Z})^{\times 2}$, $y \in (\mathbb{Z}/\ell^s\mathbb{Z})^\times$ and $x = \operatorname{tr}(A')/2$. Observe that for any $c, d \in \mathbb{Z}/\ell^s\mathbb{Z}$, we have

$$\begin{pmatrix} 0 & \varepsilon\ell^t y^2 - x^2 \\ 1 & 2x \end{pmatrix} \begin{pmatrix} dy - cx & \varepsilon\ell^t cy - dx \\ c & d \end{pmatrix} = \begin{pmatrix} dy - cx & \varepsilon\ell^t cy - dx \\ c & d \end{pmatrix} \begin{pmatrix} x & \varepsilon\ell^t y \\ y & x \end{pmatrix}.$$

Since y is a unit, there exists a choice of $c, d \in \mathbb{Z}/\ell^s\mathbb{Z}$ such that $(dy - cx)d - c(\varepsilon\ell^t cy - dx) = (d^2 - \varepsilon\ell^t c^2)y \notin \ell\mathbb{Z}/\ell^s\mathbb{Z}$. Hence, A' is conjugate to a matrix of the form $\begin{pmatrix} x & \varepsilon\ell^t y \\ y & x \end{pmatrix}$. □

5.3. Modular curves. Fix a positive integer n. Let $Y(n)$ be the coarse space of the moduli stack parametrizing elliptic curves with full level-n structure up to isomorphism, that is, pairs (E, ψ), where $E \to S$ is an elliptic curve over a base scheme $S/\mathbb{Q}$ and ψ is an isomorphism

$$\psi : (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})_S \xrightarrow{\sim} E_n.$$

We do not require this isomorphism to be compatible with the Weil pairing. Two pairs (E, ψ) and (E', ψ') are isomorphic if there is an isomorphism $E \to E'$ over S such that the diagram

$$\begin{tikzcd}
(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})_S \arrow[r, "\psi"] \arrow[d, "="'] & E_n \arrow[d] \\
(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})_S \arrow[r, "\psi'"] & E'_n
\end{tikzcd}$$

commutes; we write $[E, \psi]$ for the isomorphism class of (E, ψ). The modular curve $Y(n)$ and its compactification $X(n)$, obtained by suitably adding cusps to

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

$Y(n)$, have models defined over $\mathbb{Q}$. These models are not geometrically connected because we did not insist on the compatibility of ψ with the Weil pairing. In fact, over $\overline{\mathbb{Q}}$, the curve $Y(n)_{\overline{\mathbb{Q}}}$ has $\varphi(n)$ components (here φ denotes the usual Euler totient function), one for each symplectic pairing on $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We use $j(E)$ to denote the class of a point $[E]$ in $X(1)$.

A subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ acts on $Y(n)$ by

$$h([E, \psi]) := [E, \psi \circ h] \text{ for } h \in H,$$

and this action extends uniquely to $X(n)$. The quotient $X(n)/H$ is a curve defined over $\mathbb{Q}$; conjugate subgroups give rise to isomorphic quotient curves [DR73, IV.3]. We write $\overline{[E, \psi]}$ for the image of a point $[E, \psi]$ in $X(n)/H$. Points of $X(n)/H$ are related to the Galois representation $\rho_{E,n}$ as follows.

Lemma 5.7. *Let n be a positive integer and let k be a field of characteristic* 0*. There exists a noncuspidal k-point $x \in X(n)/H$ if and only if there exists an elliptic curve E over k with $j(E) = j(x)$ such that* $\operatorname{im} \rho_{E,n}$ *is contained in H (up to conjugacy).*

Proof. By [DR73, VI, Proposition 3.2], there is a noncuspidal k-point x in $X(n)/H$ if and only if there exists an elliptic curve E over k with $j(E) = j(x)$ and an isomorphism $\psi\colon (\mathbb{Z}/n\mathbb{Z})^2 \to E_n$ such that $\overline{[E, \psi]} = x \in (X(n)/H)(k)$. Then we use the following well-known equivalence: Given an elliptic curve E over k, there exists an isomorphism $\psi\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to E_n$ such that $\overline{[E, \psi]}$ defines a k-point on $X(n)/H$ if and only if $\operatorname{im} \rho_{E,n}$ is contained in a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ conjugate to H. In the forward direction, ψ is used to identify $\mathrm{Aut}(E_n)$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ in the definition of the representation $\rho_{E,n}$. In the backward direction, $\rho_{E,n}$ is assumed to come with an identification of $\mathrm{Aut}(E_n)$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and the representation is used to construct ψ. See, for example, [RZB15, Lemma 2.1] for a proof. □

Fix a prime power ℓ^s. We define $X_s(\ell^s)$, $X_{ns}^{t,\overline{\varepsilon}}(\ell^s)$, and $X_B^t(\ell^s)$ as the quotient $X(\ell^s)/H$ by taking H to be $C_s(\ell^s)$, $C_{ns}^{t,\overline{\varepsilon}}(\ell^s)$, and $B_{ab}^t(\ell^s)$, respectively, in the notation of Section 5.2. These curves have natural forgetful maps

$$\pi_s^{\ell^s}: X_s(\ell^s) \to X(1), \quad \pi_{ns}^{\ell^s}: X_{ns}^{t,\overline{\varepsilon}}(\ell^s) \to X(1), \quad \text{and} \quad \pi_{B,t}^{\ell^s}: X_B^t(\ell^s) \to X(1)$$

to the modular curve $X(1)$.

Proposition 5.8. *Let E be an elliptic curve over a field k of characteristic* 0*, let ℓ be an odd prime, let s be a positive integer, and let $s' := \lceil s/2 \rceil$. If the extension*

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

$k(E_{\ell^s})/k$ is abelian, then $j(E) \in X(1)(k)$ is the image of a k-rational point from one of the curves $X_s(\ell^{s'})$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^{s'})$, or $X_B^t(\ell^{s'})$.

Conversely, if $j \in Y(1)(k) \subset X(1)(k)$ is the image of a k-rational point from one of the curves $X_s(\ell^s)$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^s)$, or $X_B^t(\ell^s)$, then there exists an elliptic curve E/k with $j(E) = j$, such that the field extension $k(E_{\ell^s})/k$ is abelian.

Proof. The representation ρ_{E,ℓ^s} factors through $\mathrm{Gal}(k(E_{\ell^s})/k)$, so if $k(E_{\ell^s})/k$ is an abelian extension, $\operatorname{im}\rho_{E,\ell^s}$ is an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. By Corollary 5.6, $\operatorname{im}\rho_{E,\ell^{s'}}$ is conjugate to a subgroup of $C_s(\ell^{s'})$, $C_{ns}^{t,\bar{\varepsilon}}(\ell^{s'})$, or $B_{ab}^t(\ell^{s'})$. Hence, by Lemma 5.7, there is a k-rational point on one of the curves $X_s(\ell^{s'})$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^{s'})$, or $X_B^t(\ell^{s'})$ whose image in $X(1)$ is $j(E)$. Conversely, given a k-rational point P on one of the curves $X_s(\ell^s)$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^s)$, or $X_B^t(\ell^s)$, by Lemma 5.7 there is an elliptic curve E/k whose j-invariant is the image of P in $X(1)$, and such that $\operatorname{im}\rho_{E,\ell^s}$ is conjugate to a subgroup of $C_s(\ell^s)$, $C_{ns}^{t,\bar{\varepsilon}}(\ell^s)$, or $B_{ab}^t(\ell^s)$. Therefore, $k(E_{\ell^s})/k$ is abelian. □

6. Equivalence of uniform bounds

In this section we prove the equivalence among strong uniform boundedness statements for the size of the Brauer group (modulo algebraic classes) of certain principal homogeneous spaces of abelian surfaces, for their associated K3 surfaces, for the existence of abelian n-division fields, and for rational points on certain modular curves. In addition to the results stated in Section 1, we also prove the following.

THEOREM 6.1. *Let d be a positive integer. The following uniform boundedness statements are equivalent.*

(K3) *For all positive integers r, there exists a $B = B(r, d)$ such that for all number fields k of degree at most r and all surfaces $X/k \in \mathscr{K}_d$,*

$$\#\left(\frac{\operatorname{Br} X}{\operatorname{Br}_0 X}\right) \leqslant B.$$

(Ab) *For all positive integers r', there exists a $B' = B'(r', d)$ such that for all number fields k' of degree at most r' and all $Y/k' \in \mathscr{A}_d^2$,*

$$\#\left(\frac{\operatorname{Br} Y}{\operatorname{Br}_1 Y}\right) \leqslant B'.$$

(EC) *For all positive integers r'', there exists a $B'' = B''(r'', d)$ such that for all number fields k'' of degree at most r'' and all non-CM elliptic curves E/k''*

with a k''-rational cyclic subgroup of order d,

$$\mathrm{Gal}(k''(E_n)/k'') \text{ is abelian} \Rightarrow n \leqslant B''.$$

(M) *For all positive integers r''', there exists a $B''' = B'''(r''', d)$ such that for all number fields k''' of degree at most r''' and all odd prime powers $\ell^s > B'''$, the curves $X_s(\ell^s) \times_{X(1)} X_0(d)$, $X_{ns}^{t,\overline{\varepsilon}}(\ell^s) \times_{X(1)} X_0(d)$, and $X_B^t(\ell^s) \times_{X(1)} X_0(d)$ have no non-CM, noncuspidal k'''-rational points.*

REMARK 6.2. Let r be a positive integer. If the modular curve $X_0(d)$ has no non-CM noncuspidal degree r points for d sufficiently large, then Theorem 6.1 holds without the dependence on d. Indeed if $X_0(d)$ has no non-CM noncuspidal degree r points for d sufficiently large, then **(K3)**, **(Ab)**, **(EC)**, and **(M)** trivially hold for d sufficiently large.

In Section 6.1, we show that the existence of a uniform bound on $\mathrm{Br}\, X/\mathrm{Br}_0\, X$ for K3 surfaces with fixed geometric Néron–Severi lattice reduces to a bound on the exponent of $\mathrm{Br}\, X/\mathrm{Br}_1\, X$. In Section 6.2, we show that for $Y \in \mathscr{A}_d^N$, the existence of order n elements in $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$ is related to the existence of an abelian representation of the Galois group attached to E_n, for E some elliptic curve. These results are used in Section 6.3 to prove Theorem 1.3. We prove Theorem 1.5 in Section 6.4, and use it in the proof of Theorem 6.1 in Section 6.5. Finally, we prove Theorem 1.8 in Section 6.6.

6.1. Uniform bounds on $\mathrm{Br}_1\, X/\mathrm{Br}_0\, X$.

PROPOSITION 6.3. *Let X be a K3 surface over a field k of characteristic* 0. *Then there exists a positive integer M that depends only on the exponent of* $\mathrm{Br}\, X/\mathrm{Br}_1\, X$ *such that*

$$\#\left(\frac{\mathrm{Br}\, X}{\mathrm{Br}_0\, X}\right) \leqslant M.$$

Proof. Recall that for any smooth variety W over an algebraically closed field of characteristic 0, we have the following exact sequence

$$0 \to (\mathbb{Q}/\mathbb{Z})^{b_2 - r} \to \mathrm{Br}\, W \to \bigoplus_{\ell} \mathrm{H}^3_{\mathrm{et}}(W, \mathbb{Z}_\ell(1))_{\mathrm{tors}} \to 0,$$

where b_2 denotes the second Betti number and r denotes the Picard rank. Hence, for X as in the proposition, we have $\mathrm{Br}\, \overline{X} \cong (\mathbb{Q}/\mathbb{Z})^{22-r}$.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

By the definition of $\operatorname{Br}_1 X$, we have an inclusion $\operatorname{Br} X/\operatorname{Br}_1 X \hookrightarrow \operatorname{Br} \overline{X} \cong (\mathbb{Q}/\mathbb{Z})^{22-r}$. Thus

$$\#\left(\frac{\operatorname{Br} X}{\operatorname{Br}_1 X}\right) \leqslant \left(e\left(\frac{\operatorname{Br} X}{\operatorname{Br}_1 X}\right)\right)^{22-r} \leqslant \left(e\left(\frac{\operatorname{Br} X}{\operatorname{Br}_1 X}\right)\right)^{21}.$$

The cardinality of $\operatorname{Br} X/\operatorname{Br}_0 X$ is the product of $\#(\operatorname{Br} X/\operatorname{Br}_1 X)$ and $\#(\operatorname{Br}_1 X/\operatorname{Br}_0 X)$, so it suffices to bound $\#(\operatorname{Br}_1 X/\operatorname{Br}_0 X)$. Since the geometric Picard group of a K3 surface over a characteristic zero field is free of rank at most 20, the following lemma completes the proof. □

LEMMA 6.4. *Let X be a smooth proper geometrically integral variety over a field k of characteristic* 0. *Assume that the geometric Picard group* $\operatorname{Pic} \overline{X}$ *is free of rank r. Then there exists a positive integer $M = M(r)$, independent of X such that* $\#(\operatorname{Br}_1 X/\operatorname{Br}_0 X) \mid M$.

Proof. The Hochschild–Serre spectral sequence (2.1) yields an injection

$$\frac{\operatorname{Br}_1 X}{\operatorname{Br}_0 X} \hookrightarrow \mathrm{H}^1(\Gamma_k, \operatorname{Pic} \overline{X});$$

thus it suffices to prove the existence of a constant $M = M(r)$ such that $\#\,\mathrm{H}^1(\Gamma_k, \operatorname{Pic} \overline{X}) \mid M$.

Each of the finitely many generators of $\operatorname{Pic} \overline{X}$ involves finitely many equations with finitely many coefficients, which generate a finite field extension K/k such that $\operatorname{Pic} X_K \cong \operatorname{Pic} \overline{X}$. We may assume that K/k is Galois. As $\operatorname{Pic} \overline{X}$ is free and Γ_K is profinite, the cohomology group $\mathrm{H}^1(\Gamma_K, \operatorname{Pic} \overline{X}) = \operatorname{Hom}(\Gamma_K, \operatorname{Pic} \overline{X})$ vanishes. Thus, the inflation–restriction exact sequence from group cohomology gives an isomorphism

$$\mathrm{H}^1(\operatorname{Gal}(K/k), (\operatorname{Pic} \overline{X})^{\Gamma_K}) \xrightarrow{\sim} \mathrm{H}^1(\Gamma_k, \operatorname{Pic} \overline{X}).$$

The injection $\operatorname{Pic} X_K \hookrightarrow (\operatorname{Pic} \overline{X})^{\Gamma_K}$, which comes from the exact sequence of low-degree terms of the Hochschild–Serre spectral sequence (2.1), together with the isomorphism $\operatorname{Pic} X_K \cong \operatorname{Pic} \overline{X}$ shows that $(\operatorname{Pic} \overline{X})^{\Gamma_K} \cong \operatorname{Pic} \overline{X} \cong \mathbb{Z}^r$. All together, these facts imply that the cohomology group $\mathrm{H}^1(\Gamma_k, \operatorname{Pic} \overline{X})$ has the form $\mathrm{H}^1(G, \mathbb{Z}^r)$ for some finite group G. Since $\mathrm{H}^1(G, \mathbb{Z}^r)$ is $|G|$-torsion, the long exact sequence in cohomology associated to the multiplication-by-$|G|$ map yields an isomorphism

$$\mathrm{H}^1(G, \mathbb{Z}^r) \cong \frac{(\mathbb{Z}^r/|G|)^G}{(\mathbb{Z}^r)^G/(|G|)}.$$

Therefore, $\#\,\mathrm{H}^1(G, \mathbb{Z}^r)$ divides $|G|^r$, regardless of the action of G.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

The action of G on $\mathbb{Z}^r$ factors through a finite subgroup G' of $\mathrm{GL}_r(\mathbb{Z})$, thus $\mathrm{H}^1(G, \mathbb{Z}^r) = \mathrm{H}^1(G', \mathbb{Z}^r)$. Since every finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_r(\mathbb{F}_3)$, $|G'|$, and hence $\#\mathrm{H}^1(G', \mathbb{Z}^r)$, divides a constant that depends only on r. □

6.2. Order n Brauer classes and abelian representations associated to E_n.

Let $Y/k \in \mathscr{A}_d^N$ for some d and N, and let $A = \mathrm{Alb}(Y)$. Since $\mathrm{NS}\,\overline{Y} \cong \mathrm{NS}\,\overline{A}$, by Proposition 2.7, there exists a field extension L/k of degree at most 12, a pair of elliptic curves E and E' over L and $\delta \in L^\times/L^{\times 2}$ such that:

(1) $A_L \cong E \times E'$; and

(2) there is a cyclic L-isogeny of degree d between E and E'^{δ}.

THEOREM 6.5. *Let n be a positive integer and let $Y/k \in \mathscr{A}_d^N$ for some d and N. Let L, E, E', and δ be as above. Suppose that the quotient $\mathrm{Br}\,Y/\mathrm{Br}_1\,Y$ contains an element of order n. Then there is a field extension $\tilde{k}/k$ of degree at most $(\gcd(\mathrm{per}(Y), n^\infty))^4$ such that $\mathrm{Gal}(\tilde{L}(\sqrt{\delta}, E'_{n/c})/\tilde{L}(\sqrt{\delta}))$ is abelian, where $\tilde{L}$ is the compositum of L and $\tilde{k}$ and*

$$c = \begin{cases} \gcd(d, n) & \text{if } \delta \in \tilde{L}^{\times 2}, \\ \gcd(2d^2, n) & \text{if } \delta \notin \tilde{L}^{\times 2}. \end{cases} \tag{6.1}$$

If n is relatively prime to $\mathrm{per}(Y)$, then we may take $\tilde{k} = k$.

REMARK 6.6. Theorem 6.5 also holds with E' replaced by E. Note, however, that if n/c and d are relatively prime then the two statements are equivalent, because then $E'_{n/c}$ and $E_{n/c}$ are isomorphic as $\Gamma_{L(\sqrt{\delta})}$-modules.

COROLLARY 6.7. *Let $X = \mathrm{Kum}\,Y$ be a Kummer surface over a field k of characteristic 0 such that $\mathrm{NS}\,\overline{X} \cong \Lambda_d$, and let n be a positive integer. Since $Y \in \mathscr{A}_d^2$ we have L, E, E', and δ as above.*

Suppose that the quotient $\mathrm{Br}\,X/\mathrm{Br}_1\,X$ contains an element of order n. Then there is a field extension $\tilde{k}/k$ of degree at most 16 such that $\mathrm{Gal}(\tilde{L}(\sqrt{\delta}, E'_{n/c})/\tilde{L}(\sqrt{\delta}))$ is abelian, where $\tilde{L}$ is the compositum of L and $\tilde{k}$ and c is as in (6.1). If n is odd or if X is a Kummer surface (that is, Y is the trivial 2-covering), then we may take $\tilde{k} = k$.

Proof. This follows from (3.1). □

COROLLARY 6.8. *Let X be a K3 surface over a field k of characteristic 0 such that $\mathrm{NS}\,\overline{X} \cong \Lambda_d$, and let n be a positive integer. Suppose that the quotient*

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

$\operatorname{Br} X/\operatorname{Br}_1 X$ *contains an element of order* n*. Then there is a field extension* $\tilde{L}/k$ *whose degree is uniformly bounded (independent of* X, k, d *and* n*) and an elliptic curve* E' *over* $\tilde{L}$ *such that* $\operatorname{Gal}(\tilde{L}(E'_{n/\gcd(2d^2,n)})/\tilde{L})$ *is abelian.*

Proof. By Corollary 2.4, there exist: a field L_0/k whose degree is uniformly bounded, elliptic curves E, E' over L_0, a 2-covering $Y \to E \times E'$, such that $X_{L_0} = \operatorname{Kum} Y$ and there is a cyclic isogeny $\phi\colon E \to E'$ of degree d. Hence, Corollary 6.7 implies that there is an extension $\tilde{k}/L_0$ of degree at most 16 such that $\operatorname{Gal}(\tilde{k}(E'_{n/c})/\tilde{k})$ is abelian for c as in (6.1) (since Y is a 2-covering of $E \times E'$, the extension L/L_0 associated to the Kummer X_{L_0} is the trivial extension). We have $[\tilde{k} : k] = [\tilde{k} : L_0] \cdot [L_0 : k] \leqslant 16 \cdot [L_0 : k]$. As $[L_0 : k]$ is uniformly bounded, so is $[\tilde{L} : k]$. To complete the proof, we note that if $\operatorname{Gal}(\tilde{L}(E'_{n'})/\tilde{L})$ is abelian, so is $\operatorname{Gal}(\tilde{L}(E'_{n''})/\tilde{L})$ for any divisor n'' of n'. □

Proof of Theorem 6.5. Suppose that $\operatorname{Br} Y/\operatorname{Br}_1 Y$ contains an element of order n. Then there exists an integer n' that is a power of n such that $(\operatorname{Br} Y)_{n'}/(\operatorname{Br}_1 Y)_{n'}$ has an element of order n. Hence by Theorem 3.1, there exists a field extension k'/k of degree at most $(\gcd(\operatorname{per}(Y), n^\infty))^4$ such that

$$\frac{\operatorname{Hom}_{L'}(E_{n'}, E'_{n'})}{(\operatorname{Hom}(\overline{E}, \overline{E}')/n')^{\Gamma_{L'}}}$$

contains an element of order n; here L' denotes the compositum of L and k'. Furthermore, if n is relatively prime to $\operatorname{per}(Y)$, we may take $k' = k$.

If $\delta \in L'^{\times 2}$, then Theorem 4.1 implies that

$$\frac{\operatorname{End}_{L'}(E'_{n'})}{(\operatorname{End}(\overline{E}')/n')^{\Gamma_{L'}}}$$

has an element of order $n/\gcd(d, n)$. Hence, the result follows from Corollary 5.2.

If $\delta \notin L'^{\times 2}$, then Theorem 4.1 yields an element of order $n/\gcd(n, \gcd(2, n)\gcd(d, n)^2) = n/\gcd(2d^2, n)$ in

$$\frac{\operatorname{End}_{L'(\sqrt{\delta})}(E'^{\delta}_{n'})}{\operatorname{End}_{L'}(E'^{\delta})}.$$

Again, the result follows from Corollary 5.2. □

THEOREM 6.9. *Let* n *be a positive integer, let* E' *be a non-CM elliptic curve over a field* k *of characteristic* 0*, with a* k*-rational cyclic subgroup* C *of degree* d*, and let* $E = E'/C$*. Let* W *and* W' *be principal homogeneous spaces of* E *and*

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

E', respectively, with periods coprime to n, and let $Y = W \times W'$. (Recall that then $Y \in \mathscr{A}_d^N$ for some integer N coprime to n.) If $\mathrm{Gal}(k(E'_n)/k)$ *is abelian, then* $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$ *has an element of order* $n/\gcd(d,n)$.

Proof. Since $\mathrm{Gal}(k(E'_n)/k)$ is abelian, Corollary 5.2 implies that

$$\mathrm{End}_k(E'_n)/(\mathrm{End}(\overline{E}')/n)^{\Gamma_k}$$

has an element of order n. Hence, $\mathrm{Hom}_k(E_n, E'_n)/(\mathrm{Hom}(\overline{E}, \overline{E}')/n)^{\Gamma_k}$ has an element of order $n/\gcd(d,n)$ by Proposition 4.3. Since n is coprime to $\mathrm{per}(W)\,\mathrm{per}(W')$ and $L = k$, Theorem 3.1 completes the proof. □

COROLLARY 6.10. *Let n, E, E', W, W' be as in Theorem 6.9. Suppose further that W and W' have period dividing 2, so that we may define $X := \mathrm{Kum}(W \times W')$. If* $\mathrm{Gal}(k(E'_n)/k)$ *is abelian, then* $\mathrm{Br}\, X/\mathrm{Br}_1\, X$ *has an element of order* $n_{\mathrm{odd}}/\gcd(d, n_{\mathrm{odd}})$.

Proof. This follows from [**SZ12**, Theorem 2.4] (see (3.1)). □

6.3. Proof of Theorem 1.3.

(Ab) ⇔ (K3): By Lemma 6.4, **(K3)** is equivalent to the existence of a uniform bound on $\#(\mathrm{Br}\, X/\mathrm{Br}_1\, X)$. Furthermore, by Proposition 2.1 and Remark 2.2(ii) for any $X/k \in \mathscr{K}_d$, there exists a field extension L whose degree is absolutely bounded such that X_L is a Kummer surface. Thus, the implications follow from the proof of [**SZ12**, Theorem 2.4] (see (3.1)).

(EC) ⇒ (Ab): Let r' be a positive integer, let k'/F be an extension of degree at most r, and let $Y/k' \in \mathscr{A}_d^2$. Recall that for any abelian surface A over an algebraically closed field with $\mathrm{rank}\, \mathrm{NS}\, A = 3$, $\mathrm{Br}\, A \cong (\mathbb{Q}/\mathbb{Z})^3$. As $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$ injects into $\mathrm{Br}\, \overline{Y}$ and $\overline{Y}$ is an abelian surface, bounding $\#(\mathrm{Br}\, Y/\mathrm{Br}_1\, Y)$ is equivalent to bounding the exponent of $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$.

Assume that there exists an element of order n in $\mathrm{Br}\, Y/\mathrm{Br}_1\, Y$, for some odd integer n. Then by Theorem 6.5 there exists a field extension $k'' := \tilde{L}(\sqrt{\delta})/k'$ whose degree is bounded by a constant C that is independent of Y, k', d and n and an elliptic curve E'/k'' such that E' contains a cyclic subgroup of order d and $k''(E'_{n/\gcd(d^2,n)})/k''$ is an abelian extension. Since $[k'' : F] \leqslant C \cdot [k' : F] \leqslant Cr'$, by **(EC)**,

$$n \leqslant \gcd(d^2, n) \cdot B''(Cr', d) \leqslant d^2 B''(Cr', d).$$

(Ab) ⇒ (EC): Let r'' be a positive integer, let k''/F be an extension of degree at most r'', let E/k'' be a non-CM elliptic curve with a k''-rational cyclic subgroup C of order d, and let $E' := E/C$. Let n be a positive integer such that $k''(E'_n)/k''$ is abelian. Then by Theorem 6.9, there exists $Y/k'' \in \mathscr{A}_d^2$ with an element of order $n/\gcd(d,n)$ in $\operatorname{Br} Y/\operatorname{Br}_1 Y$. Thus, by assumption

$$n_{\mathrm{odd}} \leqslant \gcd(d,n)\cdot B'(r'',d) \leqslant dB'(r'',d),$$

so we may take $B'' := dB'(r'',d)$. □

6.4. Uniform bounds on ℓ-primary parts.

Theorem 6.11. *Let ℓ be a prime integer and let r be a positive integer. There exists a positive constant $B = B(\ell, r)$ such that for all number fields L of degree at most r and all elliptic curves E/L, the extension $L(E_{\ell^s})/L$ is nonabelian whenever $s > B$.*

Proof. By Proposition 5.5 and [Abr96], for sufficiently large s, the gonality of $X(\ell^s)/H$ is greater than $2r$ for all abelian subgroups $H < \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. Fix such an $s =: s_0$. For any $s \in \mathbb{N}$, consider the set

$$J(s) := \bigcup_{\substack{H<\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})\\ H \text{ abelian}}} \bigcup_{\substack{L/k\\ [L:k]\leqslant r}} \{j(x) : x \in (Y(\ell^s)/H)(L),\ x \text{ non-CM}\}.$$

Since there are finitely many abelian subgroups $H < \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$, a result of Frey [Fre94] implies that $J(s_0)$ is a finite set.

Assume that there exists $j \in J(s_0)$. For E a non-CM elliptic curve over L, the image of $\rho_{E,\ell^{s_0}}$ is abelian if and only if the image of $\rho_{E',\ell^{s_0}}$ is abelian for any twist E' of E. Furthermore, for any non-CM elliptic curve, $\operatorname{im}\rho_{E,\ell^\infty}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ [Ser98, p. IV-11]. Thus, by Lemma 5.7, there exists a positive integer $s(j)$ such that for all $s' > s(j)$ and all abelian subgroups $H' < \mathrm{GL}_2(\mathbb{Z}/\ell^{s'}\mathbb{Z})$, there is no point on $X(\ell^{s'})/H'$ of degree at most r that maps to j. By definition of $s(j)$, we have $J(S) = \emptyset$ whenever $S > \max_{j\in J(s_0)} s(j)$. Therefore, after increasing s_0 we may assume that $J(s_0) = \emptyset$.

Assume that $J(s_0) = \emptyset$. For $s' \geqslant s_0$ and $H' < \mathrm{GL}_2(\mathbb{Z}/\ell^{s'}\mathbb{Z})$ we have $\mathbb{Q}$-morphisms

$$X(\ell^{s'})/H' \longrightarrow X(\ell^{s_0})/(H' \bmod \mathrm{M}_2(\ell^{s_0}\mathbb{Z}/\ell^{s'}\mathbb{Z})),$$

so $J(s') = \emptyset$. Thus by Lemma 5.7, for any number field L of degree at most r and any elliptic curve E/L, the extension $L(E_{\ell^s})$ is nonabelian for all $s \geqslant s_0$. Hence we obtain a bound for s that depends only on ℓ and r. □

Proof of Theorem 1.5. Let ℓ be a prime, let k be a number field of degree at most r, and let $Y/k \in \bigcup_N \mathscr{A}_d^N$. Assume that the period of Y has ℓ-valuation

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

at most v. Since $\operatorname{Br} Y/\operatorname{Br}_1 Y$ injects into $\operatorname{Br} \overline{Y} \cong (\mathbb{Q}/\mathbb{Z})^3$, in order to bound $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)[\ell^\infty]$ by a constant independent of Y, it suffices to bound the exponent of $(\operatorname{Br} Y/\operatorname{Br}_1 Y)[\ell^\infty]$ by a constant independent of Y. Assume that there exists an element of order ℓ^s in $\operatorname{Br} Y/\operatorname{Br}_1 Y$. Then by Theorem 6.5, there exists a field extension $\tilde{L}/k$ with $[\tilde{L} : k]$ bounded by $24 \cdot \ell^{4v}$ and an elliptic curve $E'/\tilde{L}$ such that the extension $\tilde{L}(E'_{\ell^s/\gcd(2d^2,\ell^s)})/\tilde{L}$ is abelian. Thus, by Theorem 6.11, $s - v_\ell(2d^2)$ must be less than $B(\ell, 24 \cdot r \cdot \ell^{4v})$, so s is bounded depending only on ℓ, v, d, and r. □

Proof of Corollary 1.6. This follows from Theorem 1.5 and [**SZ12**, Theorem 2.4] (see 3.1). □

6.5. Proof of Theorem 6.1. By Theorems 6.11 and 1.5 and Corollary 1.6 for $\ell = 2$, **(EC)**, **(Ab)**, and **(K3)** from Theorem 1.3 are equivalent, respectively, to **(EC)**, **(Ab)**, and **(K3)** from Theorem 6.1. Hence, it suffices to prove that one of these statements are equivalent to **(M)**.

(EC) ⇒ (M): Let r''' be a positive integer, let k'''/F be a field extension of degree at most r''' and consider an odd prime power ℓ^s. Suppose that at least one of the curves $X_s(\ell^s) \times_{X(1)} X_0(d)$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^s) \times_{X(1)} X_0(d)$, or $X_B^t(\ell^s) \times_{X(1)} X_0(d)$ has a non-CM, noncuspidal k'''-rational point. Then by Proposition 5.8 there exists an elliptic curve E/k''' together with a k'''-rational cyclic subgroup of order d such that $\operatorname{Gal}(k'''(E_{\ell^s})/k''')$ is abelian. Applying **(EC)** with $r'' := r'''$, there exists a $B'' = B''(r', d)$ such that $\ell^s \leqslant B''$. Take $B''' = B''$.

(M) ⇒ (EC): Let r'' be a positive integer, let k''/F be an extension of degree at most r'', let E/k'' be a non-CM elliptic curve with a k''-rational cyclic subgroup C, and let $E' := E/C$. Let n be a positive integer such that $k''(E'_n)/k''$ is abelian. Fix an odd prime ℓ and set $s := v_\ell(n)$ and $s' := \lceil s/2 \rceil$. By Proposition 5.8, the point $j(E') \in X(1)(k)$ is the image of a k''-rational point of one of the curves $X_s(\ell^{s'})$, $X_{ns}^{t,\bar{\varepsilon}}(\ell^{s'})$, or $X_B^t(\ell^{s'})$. Since E' is smooth and non-CM, the k''-rational point must be noncuspidal and non-CM. Since E' also gives rise to a k''-point on $X_0(d)$, using **(M)** with $r''' = r''$, there is a B''' such that $\ell^{s'} \leqslant B'''$. Since B''' is independent of ℓ and s', we have

$$n_{\mathrm{odd}} = \prod_{\ell > 2} \ell^s \leqslant \prod_{\ell > 2} \ell^{2s'} \leqslant \prod_{2 < \ell \leqslant B'''^2} B'''^2 =: B''_\circ.$$

Since B''' depends only on d and $r''' = r''$, $B''_\circ$ also depends only on d and r'. By Theorem 6.11, $v_2(n) \leqslant b = b(2, F, r'')$, so $n \leqslant 2^b \cdot B''_\circ =: B''$. □

6.6. Proof of Theorem 1.8. Let E be a non-CM elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational cyclic subgroup C, let $E' := E/C$, let $Y = E' \times E$, and let $X := \operatorname{Kum} Y$.

By [SZ08, Theorem 2.4], there is an injective map $\operatorname{Br} X/\operatorname{Br}_1 X \hookrightarrow \operatorname{Br} Y/\operatorname{Br}_1 Y$, thus it suffices to only bound $\#(\operatorname{Br} Y/\operatorname{Br}_1 Y)$.

Assume that $\operatorname{Br} Y/\operatorname{Br}_1 Y$ contains an element of order n. Then $\mathbb{Q}(E'_{n/\gcd(d,n)})$ is an abelian extension of $\mathbb{Q}$, by Theorem 6.5. Hence, work of González-Jiménez and Lozano-Robledo [GJLR] implies that $n/\gcd(d,n) \leqslant 8$ so $n \leqslant 8d$. Since $\operatorname{Br} Y/\operatorname{Br}_1 Y$ injects into $\operatorname{Br} \overline{Y} \cong (\mathbb{Q}/\mathbb{Z})^3$, we conclude that

$$\#\left(\frac{\operatorname{Br} Y}{\operatorname{Br}_1 Y}\right) \leqslant (8d)^3. \qquad \square$$

Acknowledgements

Question 1.1 was raised at the AIM workshop ‘Brauer groups and obstruction problems: moduli spaces and arithmetic’ in March, 2013 for the particular case of K3 surfaces [AimPL, Problem 1.5]. Lemma 6.4 was proved at the same workshop in a discussion with Max Lieblich, Andrew Obus, and the second author, among others. We thank the participants for allowing us to include this result.

We thank Brendan Hassett for many fruitful discussions, in particular, for the suggestion that we focus on these 1-parameter families. We also thank Dan Abramovich, Kęstutis Česnavičius, Max Lieblich, Ronen Mukamel, Drew Sutherland, and David Zureick-Brown for helpful conversations. The proof of Theorem 6.11 was informed by a MathOverflow post by Jeremy Rouse [JR].

We thank the anonymous referee for his or her careful reading of the paper and valuable comments.

The first author was partially supported by NSF CAREER grant DMS-1352291; the second author was partially supported by NSA Young Investigator’s Award #H98230-15-1-0054 and NSF CAREER grant DMS-1553459. This collaboration was partially supported by the Pacific Institute for Mathematical Sciences, Rice University, and the University of Washington; we thank these institutions for their support.

References

[Abr96] D. Abramovich, ‘A linear lower bound on the gonality of modular curves’, *Int. Math. Res. Not. IMRN* **20** (1996), 1005–1011.

[AVAa] D. Abramovich and A. Várilly-Alvarado, ‘Level structures on abelian varieties, Kodaira dimensions, and Lang’s conjecture’, Preprint, 2016, arXiv:1601.02483.

[AVAb] D. Abramovich and A. Várilly-Alvarado, ‘Level structures on abelian varieties and Vojta’s conjecture’, *Compos. Math.* **153** (2017), 373–394. With an Appendix by K. Madapusi Pera.

[AimPL] ‘AimPL: Brauer groups and obstruction problems’, available at http://aimpl.org/brauermoduli.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

[Bea96] A. Beauville, *Complex Algebraic Surfaces*, 2nd edn, London Mathematical Society Student Texts, 34 (Cambridge University Press, Cambridge, 1996). Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid.

[BPR13] Yu. Bilu, P. Parent and M. Rebolledo, 'Rational points on $X_0^+(p^r)$', *Ann. Inst. Fourier (Grenoble)* **63**(3) (2013), 957–984. (English, with English and French summaries).

[CTS13] J.-L. Colliot-Thélène and A. N. Skorobogatov, 'Descente galoisienne sur le groupe de Brauer', *J. Reine Angew. Math.* **682** (2013), 141–165. (French, with English and French summaries).

[CFTTV] V. Contoral-Farfán, Y. Tang, S. Tanimoto and E. Visse, 'Effective bounds for Brauer groups of Kummer surfaces over number fields', Preprint, 2016, arXiv:1606.06074.

[DR73] P. Deligne and M. Rapoport, 'Les schémas de modules de courbes elliptiques', in *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics, 349 (Springer, Berlin, 1973), 143–316 (French).

[Fre94] G. Frey, 'Curves with infinitely many points of fixed degree', *Israel J. Math.* **85**(1–3) (1994), 79–83.

[GJLR] E. González-Jiménez and Á. Lozano-Robledo, 'Elliptic curves with abelian division fields', *Math. Z.* **283**(3–4) (2016), 835–859.

[GHS07] V. Gritsenko, K. Hulek and G. K. Sankaran, 'The Kodaira dimension of the moduli of K3 surfaces', *Invent. Math.* **169**(3) (2007), 519–567.

[HKT13] B. Hassett, A. Kresch and Y. Tschinkel, 'Effective computation of Picard groups and Brauer–Manin obstructions of degree two K3 surfaces over number fields', *Rend. Circ. Mat. Palermo (2)* **62**(1) (2013), 137–151, doi:10.1007/s12215-013-0116-8.

[Huy16] D. Huybrechts, *Lectures on K3 surfaces*, Cambridge Studies in Advanced Mathematics, 158 (Cambridge University Press, Cambridge, 2016).

[ISZ11] E. Ieronymou, A. N. Skorobogatov and Y. G. Zarhin, 'On the Brauer group of diagonal quartic surfaces', *J. Lond. Math. Soc. (2)* **83**(3) (2011), 659–672. With an appendix by Peter Swinnerton-Dyer.

[Iwa49] K. Iwasawa, 'On some types of topological groups', *Ann. of Math. (2)* **50** (1949), 507–558.

[Kam92] S. Kamienny, 'Torsion points on elliptic curves and q-coefficients of modular forms', *Invent. Math.* **109**(2) (1992), 221–229.

[Kan94] E. Kani, 'Elliptic curves on abelian surfaces', *Manuscripta Math.* **84**(2) (1994), 199–223.

[Man69] Ju. I. Manin, 'The p-torsion of elliptic curves is uniformly bounded', *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 459–465 (Russian).

[MW90] D. W. Masser and G. Wüstholz, 'Estimating isogenies on elliptic curves', *Invent. Math.* **100**(1) (1990), 1–24, doi:10.1007/BF01231178; MR 1037140.

[Maz77] B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186, (1978).

[Maz78] B. Mazur, 'Rational isogenies of prime degree (with an appendix by D. Goldfeld)', *Invent. Math.* **44**(2) (1978), 129–162.

[McD78] B. R. McDonald, 'Similarity of matrices over Artinian principal ideal rings', *Linear Algebra Appl.* **21**(2) (1978), 153–162.

[MSTVA16] K. McKinnie, J. Sawon, S. Tanimoto and A. Várilly-Alvarado, 'Brauer groups on K3 surfaces and arithmetic applications', in *Brauer Groups and Obstruction Problems:*

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press

Moduli Spaces and Arithmetic, Progress in Mathematics, 320 (Birkhäuser, Cham, Switzerland, 2017), 177–218.

[Mer96] L. Merel, 'Bornes pour la torsion des courbes elliptiques sur les corps de nombres', *Invent. Math.* **124**(1–3) (1996), 437–449 (French).

[Neu13] J. Neukirch, *Class Field Theory*, (Springer, Heidelberg, 2013). The Bonn lectures, edited and with a foreword by Alexander Schmidt. Translated from the 1967 German original by F. Lemmermeyer and W. Snyder; Language editor: A. Rosenschon.

[New16] R. Newton, 'Transcendental Brauer groups of products of CM elliptic curves', *J. Lond. Math. Soc. (2)* **93**(2) (2016), 397–419, doi:10.1112/jlms/jdv058; MR 3483120.

[Nik75] V. V. Nikulin, 'On Kummer surfaces', *Izv. Akad. Nauk SSSR Ser. Mat.* **39**(2) (1975), 278–293. 471 (Russian).

[JR] J. Rouse, 'What are the strongest conjectured uniform versions of Serre's Open Image Theorem?', MathOverflow. URL: http://mathoverflow.net/q/203837 (version: 2015-05-02).

[RZB15] J. Rouse and D. Zureick-Brown, 'Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois', *Res. Number Theory* **1** (2015), 1–34.

[Ser72] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15**(4) (1972), 259–331 (French).

[Ser98] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Research Notes in Mathematics, 7 (A K Peters, Ltd., Wellesley, MA, 1998), with the collaboration of Willem Kuyk and John Labute; revised reprint of the 1968 original.

[SZ08] A. N. Skorobogatov and Y. G. Zarhin, 'A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces', *J. Algebraic Geom.* **17**(3) (2008), 481–502.

[SZ12] A. N. Skorobogatov and Y. G. Zarhin, 'The Brauer group of Kummer surfaces and torsion of elliptic curves', *J. Reine Angew. Math.* **666** (2012), 115–140.

[TVA15] S. Tanimoto and A. Várilly-Alvarado, 'Kodaira dimension of moduli of special cubic fourfolds', *J. Reine Angew. Math.* to appear, doi:10.1515/crelle-2016-0053.

[VA] A. Várilly-Alvarado, 'Arithmetic of K3 surfaces', in *Geometry Over Nonclosed Fields* (Springer, New York, 2017), 197–248.

https://doi.org/10.1017/fms.2017.16 Published online by Cambridge University Press