J. London Math. Soc. (2) 83 (2011) 659–672
doi:10.1112/jlms/jdq083

On the Brauer group of diagonal quartic surfaces

Evis Ieronymou, Alexei N. Skorobogatov and Yuri G. Zarhin

with an appendix by Sir Peter Swinnerton-Dyer

Abstract

We obtain an easy sufficient condition for the Brauer group of a diagonal quartic surface D over $\mathbb{Q}$ to be algebraic. We also give an upper bound for the order of the quotient of the Brauer group of D by the image of the Brauer group of $\mathbb{Q}$. The proof is based on the isomorphism of the Fermat quartic surface with a Kummer surface due to Mizukami.

Introduction

Let $D \subset \mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface defined by the equation

$$x_0^4 + a_1x_1^4 + a_2x_2^4 + a_3x_3^4 = 0, \qquad (1)$$

where $a_1, a_2, a_3 \in \mathbb{Q}^*$. Let $H_D \subset \mathbb{Q}^*$ be the subgroup generated by -1, 4, a_1, a_2, a_3 and the fourth powers $\mathbb{Q}^{*4}$. We write $\overline{D}$ for the surface over an algebraic closure $\overline{\mathbb{Q}}$ obtained from D by extending the ground field to $\overline{\mathbb{Q}}$, and let $\mathrm{Br}_1(D) = \mathrm{Ker}\,[\mathrm{Br}(D) \to \mathrm{Br}(\overline{D})]$. Our first main result (Corollary 3.3) states that if $\{2, 3, 5\} \cap H_D = \emptyset$, then $\mathrm{Br}(D) = \mathrm{Br}_1(D)$, that is, the Brauer group of D has no transcendental elements. Note that $\mathrm{Br}(D)$ is known to be finite modulo $\mathrm{Br}_0(D) = \mathrm{Im}\,[\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(D)]$ by a general theorem proved in [20]. The complete list of possible values of the finite abelian group $\mathrm{Br}_1(D)/\mathrm{Br}_0(D)$ can be found in the thesis of Bright [1].

Our proof is based on the crucial observation that the Fermat quartic surface $X \subset \mathbb{P}^3_{\mathbb{Q}}$ given by

$$x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0 \qquad (2)$$

is a Kummer surface, at least after an appropriate extension of the ground field. Over $\mathbb{C}$ this was first observed with some surprise in 1971 by Shafarevich and Piatetskii-Shapiro as an application of their global Torelli theorem for complex K3 surfaces [12]. In his thesis [9] (see also [10]) Mizukami constructed an explicit isomorphism between X and the Kummer surface $\mathrm{Kum}(A)$ associated with a certain abelian surface A over $\mathbb{Q}$. The details of Mizukami's construction can be found in the Appendix to this paper written by Peter Swinnerton-Dyer. There is a rational isogeny $A \to E \times E$ of degree 2, where E is the elliptic curve $y^2 = x^3 - 4x$. The Kummer surface $\mathrm{Kum}(A)$ can be given by equation (A.1) of the Appendix. Note that Mizukami's isomorphism $X \tilde{\to} \mathrm{Kum}(A)$ is only defined over $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\mu_8)$. Using [21, Proposition 1.4] we conclude that the Brauer groups $\mathrm{Br}(\overline{A})$ and $\mathrm{Br}(\overline{X})$ are isomorphic as modules under the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_8))$. This allows us to control torsion of odd order in $\mathrm{Br}(D)$ (see Theorem 3.2). The 2-primary torsion subgroup of $\mathrm{Br}(D)$ was studied in the thesis of the first named author. The result that concerns us here is [4, Theorem 5.2] which states that if $2 \notin H_D$, then the 2-primary subgroup of $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ is zero. This gives Corollary 3.3.

Received 15 December 2009; revised 1 July 2010; published online 16 March 2011.

2000 *Mathematics Subject Classification* 11D25, 14F22, 14J28.

Let us note in this connection that Bright listed many diagonal quartics D over $\mathbb{Q}$ that are everywhere locally soluble, but have no rational point of height less than 10^4, while $\mathrm{Br}_1(D) = \mathrm{Br}(\mathbb{Q})$ (see [**1**, Appendices B and C]). An inspection of his tables reveals that in all cases we have $2 \in H_D$. This hints at the possibility that a potential failure of the Hasse principle may be explained by the Brauer–Manin obstruction attached to a transcendental element of $\mathrm{Br}(D)$. See [**2**, Example 3.3] for another example of an everywhere locally soluble diagonal quartic with no algebraic Brauer–Manin obstruction and no known rational points.

As an application of Corollary 3.3 we exhibit diagonal quartic surfaces D over $\mathbb{Q}$ such that $\mathrm{Br}(D) = \mathrm{Br}(\mathbb{Q})$. Indeed, Bright's computations (see [**1**, Appendix A, case A161 and its subcases]) show that $\mathrm{Br}_1(D) = \mathrm{Br}(\mathbb{Q})$ for the following diagonal quartics D:

$$x_0^4 + 4x_1^4 + cx_2^4 - cx_3^4 = 0. \tag{3}$$

By combining this with our Corollary 3.3 we see that $\mathrm{Br}(D) = \mathrm{Br}(\mathbb{Q})$ for $c = 1, 6, 7, 9, 10, 11, \ldots$. The surfaces (3) have obvious $\mathbb{Q}$-points, e.g. $(0:0:1:1)$, and it is an interesting question whether weak approximation holds for these surfaces.

An analysis of the Galois representations on points of order 3, 5 and 16 of the lemniscatic elliptic curve E, together with Mizukami's isomorphism and [**21**, Proposition 1.4], allows one to obtain an upper bound on the size of the Brauer group of D. The second main result of this paper, Corollary 4.6, says that $\mathrm{Br}(D)/\mathrm{Br}_1(D) \subset (\mathbb{Z}/n)^2$, where $n = 2^{10} \cdot 3 \cdot 5$. Combining this with Bright's computations [**1**] we obtain that the order of $\mathrm{Br}(D)/\mathrm{Br}_0(D)$ divides $2^{25} \cdot 3^2 \cdot 5^2$. By a recent theorem of Kresch and Tschinkel [**7**, Theorem 1], this implies that the Brauer–Manin set $D(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ is effectively computable (see Corollary 4.7).

1. *Brauer group and finite morphisms*

Let k be a field of characteristic 0 with an algebraic closure $\overline{k}$ and the absolute Galois group $\Gamma_k = \mathrm{Gal}(\overline{k}/k)$. If A is an abelian group, we write A_n for the kernel of the multiplication by n map $A \to A$.

Proposition 1.1. *Let X and Y be geometrically irreducible smooth varieties over k, and let $f : Y \to X$ be a dominant, generically finite morphism of degree d. Then the kernel of the natural map $f^* : \mathrm{Br}(X) \to \mathrm{Br}(Y)$ is killed by d. In particular, for any integer $n > 1$ coprime to d, the map $f^* : \mathrm{Br}(X)_n \to \mathrm{Br}(Y)_n$ is injective.*

Proof. By a general theorem of Grothendieck (see [**8**, Example III.2.22, p. 107]) the embedding of the generic point $\mathrm{Spec}\,(k(X))$ in X induces an injective map $\mathrm{Br}(X) \hookrightarrow \mathrm{Br}(k(X))$, and similarly for Y. Since the composition of restriction and corestriction

$$\mathrm{cores}_{k(Y)/k(X)} \circ \mathrm{res}_{k(Y)/k(X)} : \mathrm{Br}(k(X)) \longrightarrow \mathrm{Br}(k(Y)) \longrightarrow \mathrm{Br}(k(X))$$

is the multiplication by d, the kernel of the natural map $f^* : \mathrm{Br}(X) \to \mathrm{Br}(Y)$ is killed by d, so our statement follows. □

Corollary 1.2. *A degree d isogeny of abelian varieties $f : A_1 \to A_2$ induces a surjective map of Γ_k-modules $f^* : \mathrm{Br}(\overline{A}_2) \to \mathrm{Br}(\overline{A}_1)$ such that $d\,\mathrm{Ker}\,(f^*) = 0$. In particular, this map induces an isomorphism on the subgroups of elements of order coprime to d.*

Proof. If $\overline{A}$ is an abelian variety over $\overline{k}$, then the Néron–Severi group $\mathrm{NS}(\overline{A})$ is torsion free. Let $r = \dim \overline{A}$ and let $\rho = \mathrm{rk}\,\mathrm{NS}(\overline{A})$. Then we have $\mathrm{Br}(\overline{A}) \simeq (\mathbb{Q}/\mathbb{Z})^m$, where $m = r(2r-1) - \rho$, and $r(2r-1)$ is the second Betti number of $\overline{A}$ (see [3, II and III, Corollary 3.4 and formula (8.9), pp. 82, 146]). By Proposition 1.1 the map $f^* : \mathrm{Br}(\overline{A}_2) \to \mathrm{Br}(\overline{A}_1)$ is a homomorphism $(\mathbb{Q}/\mathbb{Z})^m \to (\mathbb{Q}/\mathbb{Z})^m$ whose kernel is killed by d. Such a homomorphism is necessarily surjective, as shows the following well-known lemma. □

Lemma 1.3. *Any homomorphism $(\mathbb{Q}/\mathbb{Z})^m \to (\mathbb{Q}/\mathbb{Z})^m$ with finite kernel is surjective.*

Proof. Let $j : (\mathbb{Q}/\mathbb{Z})^m \to (\mathbb{Q}/\mathbb{Z})^m$ be a homomorphism such that $d\,\mathrm{Ker}\,(j) = 0$ for a positive integer d. The group $(\mathbb{Q}/\mathbb{Z})^m$ is the union of finite subgroups $F_r = ((1/r)\mathbb{Z}/\mathbb{Z})^m$ for all positive integers r. We have $j(F_{d^m r}) \subset F_{d^m r}$, moreover, the index of $j(F_{d^m r})$ in $F_{d^m r}$ divides d^m. This implies that $j(F_{d^m r})$ contains $d^m F_{d^m r} = F_r$. Since this holds for all r, the map j is surjective. □

Theorem 1.4. *Let X and Y be geometrically irreducible smooth varieties over k. Let $f : Y \to X$ be a finite flat morphism of degree d, such that $k(Y)$ is a Galois extension of $k(X)$ with Galois group G. Then $d^2\mathrm{Br}(Y)^G \subset f^*\mathrm{Br}(X)$. In particular, for any integer $n > 1$ coprime to $d = |G|$ the natural map $f^* : \mathrm{Br}(X)_n \to \mathrm{Br}(Y)_n^G$ is an isomorphism.*

Proof. Let $\mathcal{O}_X$ and $\mathcal{O}_Y$ be the structure sheaves. See [11, Lecture 10] for a construction of a natural map of coherent sheaves $f_*\mathcal{O}_Y \to \mathcal{O}_X$ which induces the norm map on the generic fibres $k(Y) \to k(X)$. The composition of the canonical map $\mathcal{O}_X \to f_*\mathcal{O}_Y$ with $f_*\mathcal{O}_Y \to \mathcal{O}_X$ sends u to u^d. The étale sheaf $\mathbb{G}_{m,X}$ is defined by setting $\mathbb{G}_{m,X}(U) = \Gamma(U, \mathcal{O}_U)^*$ for any étale morphism $U \to X$, and similarly for $\mathbb{G}_{m,Y}$. We thus obtain natural morphisms of sheaves

$$\mathbb{G}_{m,X} \longrightarrow f_*\mathbb{G}_{m,Y} \longrightarrow \mathbb{G}_{m,X},$$

whose composition sends u to u^d. Applying $\mathrm{H}^2_{\text{ét}}(X, \cdot)$ we define the maps

$$\mathrm{Br}(X) \xrightarrow{\mathrm{res}_{Y/X}} \mathrm{H}^2_{\text{ét}}(X, f_*\mathbb{G}_{m,Y}) \xrightarrow{\mathrm{cores}_{Y/X}} \mathrm{Br}(X),$$

whose composition is the multiplication by d. Note that $f^* : \mathrm{Br}(X) \to \mathrm{Br}(Y)$ is the composition of $\mathrm{res}_{Y/X}$ and the canonical map

$$\mathrm{H}^2_{\text{ét}}(X, f_*\mathbb{G}_{m,Y}) \longrightarrow \mathrm{H}^2_{\text{ét}}(Y, \mathbb{G}_{m,Y}) \tag{4}$$

from the Leray spectral sequence [8, Theorem 1.18(a)]

$$\mathrm{H}^p_{\text{ét}}(X, \mathrm{R}^q f_*\mathbb{G}_{m,Y}) \Longrightarrow \mathrm{H}^{p+q}_{\text{ét}}(Y, \mathbb{G}_{m,Y}).$$

We have $\mathrm{R}^i f_*\mathbb{G}_{m,Y} = 0$ for all $i > 0$ because f is a finite morphism [8, Corollary II.3.6]. Thus the Leray spectral sequence shows that (4) is an isomorphism. Therefore, we obtain the maps

$$\mathrm{Br}(X) \xrightarrow{\mathrm{res}_{Y/X} = f^*} \mathrm{Br}(Y) \xrightarrow{\mathrm{cores}_{Y/X}} \mathrm{Br}(X).$$

As was mentioned above, the embedding of the generic point into X induces an injective map $\mathrm{Br}(X) \hookrightarrow \mathrm{Br}(k(X))$, and a similar map for Y. By functoriality we get the following commutative diagram

$$\begin{tikzcd}
\mathrm{Br}(X) \arrow[r, hook] \arrow[d, "\mathrm{res}_{Y/X}"'] & \mathrm{Br}(k(X)) \arrow[d, "\mathrm{res}_{k(Y)/k(X)}"] \\
\mathrm{Br}(Y) \arrow[r, hook] \arrow[d, "\mathrm{cores}_{Y/X}"'] & \mathrm{Br}(k(Y)) \arrow[d, "\mathrm{cores}_{k(Y)/k(X)}"] \\
\mathrm{Br}(X) \arrow[r, hook] & \mathrm{Br}(k(X)).
\end{tikzcd} \tag{5}$$

Let $\Gamma_{k(X)} = \mathrm{Gal}(\overline{k(X)}/k(X))$ and $\Gamma_{k(Y)} = \mathrm{Gal}(\overline{k(X)}/k(Y))$, so that $\Gamma_{k(X)}/\Gamma_{k(Y)} = G$, and consider the Hochschild–Serre spectral sequence of Galois cohomology

$$\mathrm{H}^p(G, \mathrm{H}^q(\Gamma_{k(Y)}, \overline{k(X)}^*)) \Longrightarrow \mathrm{H}^{p+q}(\Gamma_{k(X)}, \overline{k(X)}^*).$$

By Hilbert's theorem 90 we have $\mathrm{H}^1(\Gamma_{k(Y)}, \overline{k(X)}^*) = 0$. We thus obtain the following exact sequence

$$\mathrm{Br}(k(X)) \longrightarrow (\mathrm{Br}(k(Y)))^G \longrightarrow \mathrm{H}^3(G, k(Y)^*).$$

The last term is an abelian group killed by $|G| = d$. This implies that for any $\alpha \in \mathrm{Br}(Y)^G$ we have $d\alpha = \mathrm{res}_{k(Y)/k(X)}(\gamma)$ for some $\gamma \in \mathrm{Br}(k(X))$. Then we have

$$d\gamma = \mathrm{cores}_{k(Y)/k(X)} \circ \mathrm{res}_{k(Y)/k(X)}(\gamma) = \mathrm{cores}_{k(Y)/k(X)}(d\alpha) = d\,\mathrm{cores}_{Y/X}(\alpha) \in \mathrm{Br}(X),$$

where the last equality is due to commutativity of the lower square of (5). From the commutativity of the upper square of (5) we finally obtain

$$d^2\alpha = d\,\mathrm{res}_{k(Y)/k(X)}(\gamma) = \mathrm{res}_{k(Y)/k(X)}(d\gamma) = \mathrm{res}_{Y/X}(d\gamma) \in f^*\mathrm{Br}(X).$$

For the last statement, the surjectivity is clear since $\mathrm{Br}(Y)_n^G \subset d^2\mathrm{Br}(Y)^G$. The injectivity follows from Proposition 1.1. □

2. *On torsion points of the lemniscata*

Let E be the lemniscatic elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$. It has complex multiplication by $\mathcal{O} = \mathbb{Z}[i]$, where $i = \sqrt{-1}$ acts on E by sending (x, y) to $(-x, iy)$. We denote by $[a + bi]$ the complex multiplication by $a + bi \in \mathbb{Z}[i]$.

Let ℓ be a prime number, $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and let $T_\ell(E)$ be the ℓ-adic Tate module of E. For a subfield $K \subset \overline{\mathbb{Q}}$ we write $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Let $\rho_\ell : \Gamma_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$ be the ℓ-adic Galois representation attached to $E/\mathbb{Q}$.

The action of $\mathcal{O}$ on $\overline{E} = E \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ endows $T_\ell(E)$ with the natural structure of an $\mathcal{O}_\ell$-module; it is known that this $\mathcal{O}_\ell$-module is free of rank 1 (see [17, Remark, p. 502]). The action of $\mathcal{O}$ on $\overline{E}$ is defined over $\mathbb{Q}(i)$, and we have

$$\rho_\ell(\Gamma_{\mathbb{Q}(i)}) \subset \mathcal{O}_\ell^* \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$$

[17, Corollary 2, p. 502], in particular, $\rho_\ell(\Gamma_{\mathbb{Q}(i)})$ is abelian. In fact, by [15, p. 302], $\rho_\ell(\Gamma_{\mathbb{Q}(i)})$ is an open subgroup of $\mathcal{O}_\ell^*$.

A prime p splits in $\mathcal{O}$ if and only if $p \equiv 1 \bmod 4$. Such a prime is uniquely written as $p = (a + bi)(a - bi)$, where $a \pm bi \equiv 1 \bmod 2 + 2i$. The principal ideals $(a + bi)$ and $(a - bi)$ of $\mathcal{O}$ are complex conjugate, with residue fields isomorphic to $\mathbb{F}_p$.

Assume that $p \neq \ell$. Since E has good reduction at p, the ℓ-adic representation $\rho_\ell : \Gamma_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$ is unramified at p. A Frobenius element $\mathrm{Fr}_p \in \rho_\ell(\Gamma_{\mathbb{Q}})$ is the image of a Frobenius automorphism at the prime p, and so Fr_p is well defined up to conjugation in $\rho_\ell(\Gamma_{\mathbb{Q}})$ (see [16, Chapter 1, Sections 1.2 and 2] for more details). The representation $\rho_\ell : \Gamma_{\mathbb{Q}(i)} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$

is unramified at $(a+bi)$ and $(a-bi)$, and the corresponding Frobenii are well-defined elements of the abelian group $\rho_\ell(\Gamma_{\mathbb{Q}(i)})$. In $\rho_\ell(\Gamma_{\mathbb{Q}})$ these two elements are conjugate by $\rho_\ell(c)$, where $c \in \Gamma_{\mathbb{Q}}$ is the complex conjugation, so they are precisely the elements of the conjugacy class of Fr_p in $\rho_\ell(\Gamma_{\mathbb{Q}})$.

A well-known fact going back to the last entry of Gauss's mathematical diary (via Deuring's interpretation on Hecke characters) is that the Frobenius element in $\rho_\ell(\Gamma_{\mathbb{Q}(i)}) \subset \mathcal{O}_\ell^*$ attached to the prime ideal $(a+bi)$ equals $a+bi$ (and similarly for $a-bi$, see [**5**, Theorem 5, p. 307] or [**14**, Proposition 4.1 and its proof, Theorem 5.6]). In what follows, Fr_p stands for either $a+bi$ or $a-bi$, for example, $\mathrm{Fr}_5 = -1+2i$ and $\mathrm{Fr}_{17} = 1+4i$.

We choose a basis of the free $\mathbb{Z}_\ell$-module $T_\ell(E)$ of rank 2 so that the image of $[i] \in \mathcal{O}$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$ is represented by the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then $\mathcal{O}_\ell \subset \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$ consists of the matrices

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

for all $a, b \in \mathbb{Z}_\ell$.

Proposition 2.1. *Let k be a Galois extension of $\mathbb{Q}(i)$.*

(a) *If the exponent of* $\mathrm{Gal}(k/\mathbb{Q}(i))$ *divides* 4, *then* $\mathrm{End}_{\Gamma_k}(E_\ell) = \mathcal{O}/\ell$ *for any prime* $\ell \geqslant 7$.

(b) *We have*

$$\mathrm{End}_{\Gamma_k}(E_5) = \begin{cases} \mathcal{O}/5 & \text{if } \sqrt[4]{5} \notin k, \\ \mathrm{End}(E_5) & \text{otherwise;} \end{cases} \qquad \mathrm{End}_{\Gamma_k}(E_3) = \begin{cases} \mathcal{O}/3 & \text{if } \sqrt[4]{-3} \notin k, \\ \mathrm{End}(E_3) & \text{otherwise.} \end{cases}$$

Proof. Let $\overline{\rho}_\ell : \Gamma_k \to \mathrm{Aut}_{\mathbb{F}_\ell}(E_\ell) \simeq \mathrm{GL}(2, \mathbb{F}_\ell)$ be the Galois representation modulo ℓ attached to E/k. Define $\Lambda \subset \Gamma_k$ as $\overline{\rho}_\ell^{-1}(\mathbb{F}_\ell^*)$, and let $M = \overline{\mathbb{Q}}^\Lambda$. If $M \neq k$, then there exists $\gamma \in \Gamma_k$ such that $\overline{\rho}_\ell(\gamma)$ has two distinct eigenvalues in $\overline{\mathbb{F}}_\ell$. The centralizer of $\overline{\rho}_\ell(\gamma)$ in $\mathrm{End}(E_\ell)$ is an $\mathbb{F}_\ell$-vector space of dimension 2 which contains $\mathcal{O}/\ell$ and so is equal to it. Hence in this case $\mathrm{End}_{\Gamma_k}(E_\ell) = \mathcal{O}/\ell$. If $M = k$, then the image of Γ_k in $\mathrm{GL}(2, \mathbb{F}_\ell)$ is the group of scalar matrices, so that $\mathrm{End}_{\Gamma_k}(E_\ell) = \mathrm{End}(E_\ell)$.

To prove (a) we note that the prime 5 splits in $\mathbb{Q}(i)$ and hence $\mathrm{Fr}_5 = -1+2i \in \mathcal{O}_\ell^*$ belongs to $\rho_\ell(\Gamma_{\mathbb{Q}(i)})$. Our assumption implies that Fr_5^4 belongs to $\rho_\ell(\Gamma_k)$. Since $\mathrm{Fr}_5^4 = -7+24i$ is not congruent to an element of $\mathbb{F}_\ell$ modulo ℓ, we see that $\overline{\rho}_\ell(\Gamma_k) \not\subset \mathbb{F}_\ell^*$ so that $\mathrm{End}_{\Gamma_k}(E_\ell) = \mathcal{O}/\ell$.

To prove (b) it suffices to show that when $k = \mathbb{Q}(i)$, then $M = k(\sqrt[4]{5})$ for $\ell = 5$, and $M = k(\sqrt[4]{-3})$ for $\ell = 3$.

Case $\ell = 5$. Since 5 splits in $\mathcal{O}$, the Γ_k-module E_5 is the direct sum of characters $\chi_1 \oplus \chi_2$ with values in $\mathbb{F}_5^*$. Then M is the fixed field of $\mathrm{Ker}\,(\chi_1\chi_2^{-1})$.

The duplication formula gives the x-coordinate of the double of a point (x, y) on E as $(x^2+1)^2/4x(x^2-1)$ (see [**18**, Chapter X, Section 6, pp. 309–310]). Using this it is easy to see that a point (x_1, y_1) such that $x_1^2 = (1+2i)^{-1}$ generates $\mathrm{Ker}\,[1-2i]$, and that a point (x_2, y_2) such that $x_2^2 = (1-2i)^{-1}$ generates $\mathrm{Ker}\,[1+2i]$. This implies that $y_1^4 = -4(1+2i)^{-3}$, $y_2^4 = -4(1-2i)^{-3}$. Then $M_1 = k(y_1)$ and $M_2 = k(y_2)$ are cyclic extensions of k of degree 4 which are linearly disjoint since M_1 is totally ramified at the principal prime ideal $(1+2i)$ and unramified at $(1-2i)$, while M_2 is totally ramified at $(1-2i)$ and unramified at $(1+2i)$. We can therefore identify $\mathrm{Gal}(M_1M_2/k)$ with $\mathrm{Gal}(M_1/k) \times \mathrm{Gal}(M_2/k)$. Let g_1 denote the generator of $\mathrm{Gal}(M_1/k) \simeq \mathbb{Z}/4$ such that $g_1(y_1) = iy_1$. We define g_2 similarly. From the above it is clear that M is the fixed subfield of $g_1g_2^{-1}$. Note that $\frac{5}{2}y_1y_2$ is fixed by $g_1g_2^{-1}$ and $(\frac{5}{2}y_1y_2)^4 = 5$. Since $[M : k] = 4$ we conclude that $M = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{5})$.

Case $\ell = 3$. Since 3 is inert in $\mathcal{O}$, it follows that Γ_k acts on E_3 by a character χ with values in $\mathbb{F}_9^*$. Recall that $\Lambda \subset \Gamma_k$ is $\chi^{-1}(\pm 1)$, and $M = \overline{\mathbb{Q}}^\Lambda$.

Applying the duplication formula we immediately see that if $P = (x, y)$ is a point of order 3 in E, then x is a root of the polynomial $f(t) = t^4 - 2t^2 - 1/3$. By Eisenstein's criterion $z^4 + 6z^2 - 3$ is irreducible over $\mathbb{Q}$, and even over k since 3 is an irreducible element of the unique factorization domain $\mathbb{Z}[i]$. The polynomial $z^4 + 6z^2 - 3$ completely splits in $k(\sqrt[4]{-3})$ since it has a root $(1 + i)a(a^2 - i)/2$, where $a = \sqrt[4]{-3}$, and $k(\sqrt[4]{-3})$ is a Galois extension of k. Hence $f(t)$ is irreducible over k with splitting field $M_1 = \mathbb{Q}(i, \sqrt[4]{-3})$. Let $M_2 = M_1(y) = M_1(\sqrt{x^3 - x})$. Since P has order 3, the points P and $[i]P$ span the $\mathbb{F}_3$-vector space E_3, so that $E_3 \subset E(M_2)$. It is clear that $[M_2 : k]$ is 8 or 4. The prime 17 splits in $\mathbb{Q}(i) = k$, and hence $1 + 4i \in \mathcal{O}_3^*$ belongs to $\rho_3(\Gamma_k)$. Since $1 + 4i$ modulo 3 has multiplicative order 8, the order of the Galois group $\mathrm{Gal}(k(E_3)/k)$ is divisible by 8. Therefore, $M_2 = k(E_3)$ is an extension of k of degree 8, $[M_2 : M_1] = 2$, and $\mathrm{Gal}(k(E_3)/k) = (\mathbb{Z}[i]/3)^* = \mathbb{F}_9^*$ is a cyclic group of order 8.

The M_1-linear automorphism of M_2 which maps y to $-y$ corresponds to the multiplication by -1 in E_3 and so belongs to Λ. Therefore $M = \overline{\mathbb{Q}}^\Lambda \subset M_1$, and in fact $M = M_1$ since $\mathbb{F}_3^*$ has index 4 in $\mathbb{F}_9^*$. Thus $M = \mathbb{Q}(i, \sqrt[4]{-3})$. □

3. *A sufficient condition for the Brauer group of D to be algebraic*

We need an easy lemma from Galois theory.

Lemma 3.1. *Let $b_i, d \in \mathbb{Q}^*$, and let $F = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{b_1}, \ldots, \sqrt[4]{b_n})$. Then $t^4 - d$ splits in F if and only if d belongs to the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*4}$ generated by the classes of -4 and the b_i, $i = 1, \ldots, n$.*

Proof. This is [**4**, Lemma 5.4]; we reproduce the proof for the convenience of the reader. The field F is a 4-Kummer extension of $\mathbb{Q}(\sqrt{-1})$, so d is a fourth power in F if and only if d belongs to the subgroup of $\mathbb{Q}(\sqrt{-1})^*/\mathbb{Q}(\sqrt{-1})^{*4}$ generated by the b_i, $i = 1, \ldots, n$. Moreover, the kernel of the natural map

$$\mathbb{Q}^*/\mathbb{Q}^{*4} \longrightarrow \mathbb{Q}(\sqrt{-1})^*/\mathbb{Q}(\sqrt{-1})^{*4}$$

is a subgroup of order 2 generated by the class of -4. □

From now on let $k = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and $F = k(\sqrt[4]{a_1}, \sqrt[4]{a_2}, \sqrt[4]{a_3})$, understood as normal subfields of $\overline{\mathbb{Q}}$.

Theorem 3.2. *Let $D \subset \mathbb{P}^3_{\mathbb{Q}}$ be the diagonal quartic surface* (1)*. Then for any prime $\ell \geqslant 7$ we have $\mathrm{Br}(\overline{D})_\ell^{\Gamma_{\mathbb{Q}}} = 0$. Moreover, if* 5 (*resp.* 3) *does not belong to the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*4}$ generated by the classes of $-1, 4, a_1, a_2, a_3$, then $\mathrm{Br}(\overline{D})_5^{\Gamma_{\mathbb{Q}}} = 0$* (*resp.* $\mathrm{Br}(\overline{D})_3^{\Gamma_{\mathbb{Q}}} = 0$).

Proof. Let X be the surface (2), and let A be the abelian surface defined in Theorem A.1. Since $D \times_{\mathbb{Q}} F \simeq X \times_{\mathbb{Q}} F$ the Γ_F-modules $\mathrm{Br}(\overline{D})$ and $\mathrm{Br}(\overline{X})$ are isomorphic. By Mizukami's isomorphism (Theorem A.1) the Fermat quartic X is isomorphic to $\mathrm{Kum}(A)$ over k, so that $\mathrm{Br}(\overline{X})$ and $\mathrm{Br}(\overline{A})$ are isomorphic as Γ_k-modules [**21**, Proposition 1.4]. Since ℓ is odd, Corollary 1.2 now implies that $\mathrm{Br}(\overline{D})_{\ell^\infty}$ and $\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^\infty}$ are isomorphic as Γ_F-modules, so it is enough to prove that $\mathrm{Br}(\overline{E} \times \overline{E})_\ell^{\Gamma_F} = 0$. The Γ_k-module $\mathrm{H}^2_{\text{ét}}(\overline{E} \times \overline{E}, \mu_\ell)$ is naturally isomorphic to $\mathbb{Z}/\ell \oplus \mathbb{Z}/\ell \oplus \mathrm{End}(E_\ell)$ (see, for example, [21, formula (17)]). The Kummer exact sequence gives rise to the well-known exact sequence of Γ_k-modules

$$0 \longrightarrow \mathrm{NS}(\overline{E} \times \overline{E})/\ell \longrightarrow \mathrm{H}^2_{\text{ét}}(\overline{E} \times \overline{E}, \mu_\ell) \longrightarrow \mathrm{Br}(\overline{E} \times \overline{E})_\ell \longrightarrow 0,$$

where $\mathrm{NS}(\overline{E} \times \overline{E})$ is the Néron–Severi group, which is isomorphic to $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathcal{O}$ as a Γ_k-module. The action of Γ_k on this module is trivial because the complex multiplication on E is defined over k. The image of $\mathrm{NS}(\overline{E} \times \overline{E})/\ell$ in $\mathrm{H}^2_{\text{ét}}(\overline{E} \times \overline{E}, \mu_\ell)$ is $\mathbb{Z}/\ell \oplus \mathbb{Z}/\ell \oplus \mathcal{O}/\ell$.

Note that ℓ is unramified in $\mathcal{O}$, thus $\mathcal{O}/\ell$ is either $\mathbb{F}_\ell \oplus \mathbb{F}_\ell$ or the field $\mathbb{F}_{\ell^2}$. In either case ℓ does not divide $|(\mathcal{O}/\ell)^*|$. Since the image G_ℓ of Γ_k in $\mathrm{Aut}(E_\ell)$ belongs to $(\mathcal{O}/\ell)^*$, we see that $|G_\ell|$ is not divisible by ℓ. It follows from Maschke's theorem that E_ℓ, $\mathrm{End}(E_\ell)$ and $\mathrm{H}^2_{\text{ét}}(\overline{E} \times \overline{E}, \mu_\ell)$ are semisimple Γ_k-modules. Therefore, we have an isomorphism of Γ_k-modules

$$\mathrm{End}(E_\ell) \cong \mathcal{O}/\ell \oplus \mathrm{Br}(\overline{E} \times \overline{E})_\ell,$$

where $\mathcal{O}/\ell$ carries trivial Γ_k-action. We conclude that $\mathrm{Br}(\overline{E} \times \overline{E})_\ell^{\Gamma_F}$ can be identified with $\mathrm{End}_{\Gamma_F}(E_\ell)/(\mathcal{O}/\ell)$. Now the desired statements follow from Proposition 2.1 by Lemma 3.1. □

Corollary 3.3. *Let $H_D \subset \mathbb{Q}^*$ be the subgroup generated by $-1, 4, a_1, a_2, a_3$ and the fourth powers $\mathbb{Q}^{*4}$. If $\{2, 3, 5\} \cap H_D = \emptyset$, then* $\mathrm{Br}(D) = \mathrm{Br}_1(D)$.

Proof. Since $\mathrm{Br}(D)$ is a torsion group, any element $\alpha \in \mathrm{Br}(D)$ can be written as $\alpha = \beta + \gamma$ where $2^m\beta = 0$ and $n\gamma = 0$ for some $m, n \in \mathbb{Z}_{\geqslant 0}$, n odd. Theorem 5.2 of [4] states that if $2 \notin H_D$, then the 2-primary subgroup of $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ is zero. Thus our condition implies that $\beta \in \mathrm{Br}_1(D)$. Also, $\gamma \in \mathrm{Br}_1(D)$ since $\mathrm{Br}(\overline{D})_n^{\Gamma_\mathbb{Q}} = 0$ by Theorem 3.2. □

4. *An upper bound for* $|\mathrm{Br}(D)/\mathrm{Br}_1(D)|$

We start with the analysis of torsion of odd order in $\mathrm{Br}(D)/\mathrm{Br}_1(D)$.

Proposition 4.1. *Let $D \subset \mathbb{P}^3_\mathbb{Q}$ be the diagonal quartic surface* (1). *Then for any odd prime ℓ we have* $\mathrm{Br}(\overline{D})_{\ell^\infty}^{\Gamma_\mathbb{Q}} = \mathrm{Br}(\overline{D})_\ell^{\Gamma_\mathbb{Q}}$.

Proof. In the beginning of the proof of Theorem 3.2 we have seen that the groups $\mathrm{Br}(\overline{D})_{\ell^\infty}$ and $\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^\infty}$ are isomorphic as Γ_F-modules. Also in the proof of Theorem 3.2 we showed that $\mathrm{Br}(\overline{E} \times \overline{E})_\ell^{\Gamma_F} = 0$ for $\ell \geqslant 7$. Thus it is enough to prove that $\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^2}^{\Gamma_F} = 0$ is killed by ℓ, where $\ell = 3$ or $\ell = 5$.

Recall that $\mathcal{O}_\ell^* \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$. Consider $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \simeq \mathrm{Mat}_2(\mathbb{Z}_\ell)$ as an $\mathcal{O}_\ell^*$-module under conjugation. Since ℓ is odd, we can decompose this module into a direct sum of $\mathcal{O}_\ell^*$-submodules $\mathcal{O}_\ell \oplus \overline{\mathcal{O}}_\ell$, where

$$\overline{\mathcal{O}}_\ell = \mathcal{O}_\ell \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \ a, b \in \mathbb{Z}_\ell \right\}.$$

We note that $[i]$ acts on $\overline{\mathcal{O}}_\ell$ by -1. Now the exact sequence of $\Gamma_{\mathbb{Q}(i)}$-modules

$$0 \longrightarrow \mathcal{O}_\ell/\ell^2 \longrightarrow \mathrm{End}(E_{\ell^2}) \longrightarrow \mathrm{Br}(\overline{E} \times \overline{E})_{\ell^2} \longrightarrow 0$$

implies that the $\Gamma_{\mathbb{Q}(i)}$-module $\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^2}$ is obtained from the $\mathcal{O}_\ell^*$-module $\overline{\mathcal{O}}_\ell/\ell^2$ via the map $\Gamma_{\mathbb{Q}(i)} \to \mathcal{O}_\ell^*$.

Since 17 splits in $\mathcal{O}$, by Gauss's result $1 + 4i \in \mathcal{O}_\ell^*$ is contained in $\rho_\ell(\Gamma_{\mathbb{Q}(i)})$. The exponent of $\mathrm{Gal}(F/\mathbb{Q}(i))$ divides 4, so we see that $(1 + 4i)^4 = 161 - 240i$ belongs to $\rho_\ell(\Gamma_F)$. Let $x \in \overline{\mathcal{O}}_\ell/\ell^2$ be an element invariant under the action of Γ_F. Then x commutes with $[161 - 240i]$. Since

240 is divisible by ℓ but not by ℓ^2 we see that ℓx is invariant under the action of $[i]$, hence $\ell x = -\ell x$. Since ℓ is odd we conclude that $\ell x = 0$. □

To estimate 2-primary torsion in $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ we need some preparations.

LEMMA 4.2. *Let G be a group of order $|G| = 2^n$, and let M be a torsion abelian 2-primary group which is a G-module. If M^G is killed by 2^m, and $M_4 \subset M^G$, then M is killed by 2^{m+n}.*

Proof. The proof is by induction on n. For $n = 1$ let g be the non-trivial element of G. If M contains an element x of exact order 2^{m+2}, then $2^m x$ has order 4 and so $2^m g(x) = 2^m x$. This implies that $2^m(x + g(x)) = 2^{m+1}x \neq 0$. However, $x + g(x) \in M^G$ and by assumption $2^m(x + g(x)) = 0$ which is a contradiction.

When $n > 1$, the group G has a proper normal subgroup $G_1 \subset G$. Applying the induction hypothesis two times, first to $(G/G_1, M^{G_1})$, and then to (G_1, M), we prove the induction step. □

PROPOSITION 4.3. *The exponent of $\mathrm{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_k}$ divides 8, and that of $\mathrm{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_F}$ divides $2^3|\mathrm{Gal}(F/k)|$.*

Proof. The prime 17 is congruent to 1 modulo 8, hence it splits completely in the cyclotomic field $k = \mathbb{Q}(\mu_8)$. Thus $\mathrm{Fr}_{17} = 1 + 4i$ is contained in $\rho_2(\Gamma_k) \subset \mathcal{O}_2^*$. In our basis of $T_2(E)$ the complex multiplication $[1 + 4i]$ is given by the matrix

$$s = \begin{pmatrix} 1 & -4 \\ 4 & 1 \end{pmatrix}.$$

For the first claim it is clearly enough to prove that for any $\alpha \in \mathrm{Br}(\overline{E} \times \overline{E})_{16}^{\Gamma_F}$ we have $8\alpha = 0$. Consider the exact sequence of Γ_k-modules

$$0 \longrightarrow \mathcal{O}/16 \longrightarrow \mathrm{End}(E_{16}) \longrightarrow \mathrm{Br}(\overline{E} \times \overline{E})_{16} \longrightarrow 0.$$

We represent α by a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{End}(E_{16}) \simeq \mathrm{Mat}_2(\mathbb{Z}/16).$$

Then $sAs^{-1} - A \in \mathcal{O}/16$, so that $sA - As \in \mathcal{O}/16$, which immediately implies that $8(a - d) = 8(c + b) = 0$. Thus $8A = 8(a + ci) \in \mathcal{O}/16$, so that $8\alpha = 0$.

To prove the second claim we note that $E_4 \subset E(k)$. Indeed, it is well known that for an elliptic curve $y^2 = (x - c_1)(x - c_2)(x - c_3)$ over $\mathbb{Q}$ the field $\mathbb{Q}(E_4)$ is an extension of $\mathbb{Q}$ obtained by joining the square roots of -1 and $c_i - c_j$ for all $i \neq j$ (see, for example, [**6**, Theorem 4.2, p. 85]). In our case $\mathbb{Q}(E_4) = \mathbb{Q}(\mu_8) = k$. This implies that $\mathrm{End}(E_4)$ is a trivial Γ_k-module, hence $\mathrm{Br}(\overline{E} \times \overline{E})_4 = \mathrm{End}(E_4)/(\mathcal{O}/4)$ is also a trivial Γ_k-module. Thus we can apply Lemma 4.2 to $G = \mathrm{Gal}(F/k)$ and $M = \mathrm{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_F}$. This completes the proof. □

PROPOSITION 4.4. *Let $D \subset \mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface (1). Then the exponent of $\mathrm{Br}(\overline{D})_{2^\infty}^{\Gamma_F}$ divides $2^4|\mathrm{Gal}(F/k)|$.*

Proof. Let X be the Fermat quartic surface (2), and let A be the abelian surface defined in Theorem A.1. Because of the isomorphism $X \times_k F \xrightarrow{\sim} D \times_k F$ we can replace D by X. By [**21**, Proposition 1.4] the Γ_F-modules $\mathrm{Br}(\overline{X})_{2^\infty}$ and $\mathrm{Br}(\overline{A})_{2^\infty}$ are isomorphic. There is a degree 2 isogeny $A \to E \times E$, so by Corollary 1.2 we have an exact sequence of Γ_F-modules

$$0 \longrightarrow (\mathbb{Z}/2)^n \longrightarrow \mathrm{Br}(\overline{E} \times \overline{E})_{2^\infty} \longrightarrow \mathrm{Br}(\overline{A})_{2^\infty} \longrightarrow 0.$$

It gives rise to the exact sequence

$$\mathrm{Br}(\overline{E}\times\overline{E})_{2^\infty}^{\Gamma_F}\longrightarrow\mathrm{Br}(\overline{A})_{2^\infty}^{\Gamma_F}\longrightarrow\mathrm{H}^1(\Gamma_F,(\mathbb{Z}/2)^n).$$

The last term is killed by 2. On the other hand, by Proposition 4.3 the exponent of $\mathrm{Br}(\overline{E}\times\overline{E})_{2^\infty}^{\Gamma_F}$ divides $2^3|\mathrm{Gal}(F/k)|$. Hence $\mathrm{Br}(\overline{A})_{2^\infty}^{\Gamma_F}$ is killed by $2^4|\mathrm{Gal}(F/k)|$. □

Corollary 4.5. *Let $D\subset\mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface* (1)*. Then the exponent of* $\mathrm{Br}(\overline{D})_{2^\infty}^{\Gamma_{\mathbb{Q}}}$ *divides* 2^{10}.

Proof. In the notation of Proposition 4.4 the Galois group $\mathrm{Gal}(F/k)$ is a quotient of $(\mathbb{Z}/4)^3$, and so $\mathrm{Br}(\overline{D})_{2^\infty}^{\Gamma_F}$ is killed by 2^{10}. Now the statement follows from the obvious inclusion $\mathrm{Br}(\overline{D})_{2^\infty}^{\Gamma_{\mathbb{Q}}}\subset\mathrm{Br}(\overline{D})_{2^\infty}^{\Gamma_F}$. □

Corollary 4.6. *Let $D\subset\mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface* (1)*. Then:*

(i) *the exponent of the group* $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ *divides* $2^{10}\cdot 3\cdot 5$;
(ii) *the order of* $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ *divides* $2^{20}\cdot 3^2\cdot 5^2$;
(iii) *the order of* $\mathrm{Br}(D)/\mathrm{Br}_0(D)$ *divides* $2^{25}\cdot 3^2\cdot 5^2$.

Proof. (i) The case of ℓ-primary torsion, where ℓ is an odd prime, follows from Theorem 3.2 combined with Proposition 4.1. The case of 2-primary torsion is dealt with in Corollary 4.5.

(ii) It is well known that $\mathrm{Pic}(\overline{D})=\mathrm{NS}(\overline{D})\simeq\mathbb{Z}^{20}$ (see, for example, [**13**, Lemma 1]). Since the second Betti number of $\overline{D}$ is 22, we conclude that $\mathrm{Br}(\overline{D})\simeq(\mathbb{Q}/\mathbb{Z})^2$ (using [**3**, II and III, Corollary 3.4 and formula (8.12), pp. 82, 147]). Thus (ii) follows from (i).

(iii) This statement follows from Bright's computations that the order of $\mathrm{Br}_1(D)/\mathrm{Br}_0(D)$ divides 2^5 (see [**1**]). □

We refer the reader to [**19**, Section 5.2], for the definition of the Brauer–Manin set $D(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.

Corollary 4.7. *Let $D\subset\mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface* (1)*. Then the Brauer–Manin set $D(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ is effectively computable.*

Proof. According to [**7**, Theorem 1] for a family of smooth projective surfaces Z over $\mathbb{Q}$ defined by explicit equations, such that $\mathrm{Pic}(\overline{Z})$ is torsion free and generated by finitely many explicitly given divisors, the Brauer–Manin set $Z(\mathbb{A}_k)^{\mathrm{Br}}$ is effectively computable whenever one has a uniform bound on the order of $\mathrm{Br}(Z)/\mathrm{Br}_0(Z)$. The geometric Picard group $\mathrm{Pic}(\overline{D})\simeq\mathbb{Z}^{20}$ of a diagonal quartic surface is generated by the obvious 48 lines on it [**13**, Lemma 1]. Thus the statement follows from Corollary 4.6. □

Appendix A. *The Fermat quartic as a Kummer surface* (*after Mizukami*)

by Sir Peter Swinnerton-Dyer

Let k be a field of characteristic different from 2. Let C be the elliptic curve over k which is a smooth projective model of the affine curve $v^2=(u^2-1)(u^2-1/2)$. The base point O of C is that point at infinity at which $v/u^2=1$.

Theorem A.1 (Mizukami [9]). *Let k be a field of characteristic not equal to 2 that contains the eighth roots of unity. Let $\tau : C \to C$ be the fixed-point free involution changing the signs of v and u. Let A be the abelian surface obtained as the quotient of $C \times C$ by the simultaneous action of τ on both factors. Then there is an isomorphism $X \xrightarrow{\sim} K = \mathrm{Kum}(A)$, where X is the Fermat quartic surface* (2).

The curves C and $C' = C/\tau$ considered as elliptic curves over $\mathbb{Q}$ have Cremona labels 64a2 and 64a1, respectively; these curves have good reduction away from 2. The short Weierstrass equation of C' is $y^2 = x^3 - 4x$, so over $\mathbb{Q}(\mu_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ the curve C' is isomorphic to the elliptic curve E with equation $y^2 = x^3 - x$. Thus there is a degree 2 isogeny $A \to E \times E$ defined over $\mathbb{Q}(\mu_8)$.

Proof of Theorem A.1. Let T be that point at infinity at which $v/u^2 = -1$. We shall need to consider two copies of C; we distinguish these and the associated variables by the subscripts 1 and 2. The involution on $C_1 \times C_2$, which reverses the signs of all four variables u_1, v_1, u_2, v_2, has no fixed points; so it is a translation by $T_1 \times T_2$ (which is the image of $O_1 \times O_2$) and $T_1 \times T_2$ must be a 2-division point. Now

$$A = C_1 \times C_2/\{O_1 \times O_2, T_1 \times T_2\}$$

is an abelian surface equipped with a map $C_1 \times C_2 \to A$ of degree 2. Its function field is the field of functions even in the four variables u_1, u_2, v_1, v_2 collectively. The involution $P \mapsto -P$ reverses the signs of u_1 and u_2; so the function field of K over a field k can be written as $k(w_1, w_2, y, z)$ where

$$w_1 = u_1^2, \quad w_2 = u_2^2, \quad y = \frac{v_1(w_2 - 1)}{v_2(w_1 - 1/2)}, \quad z = u_2/u_1.$$

(The reason for the unnatural-looking choice for y will appear at (A.4).) Thus up to birational transformation we can take K to be given by

$$y^2 = (w_1 - 1)(w_2 - 1)/(w_1 - \tfrac{1}{2})(w_2 - \tfrac{1}{2}), \quad z^2 = w_2/w_1. \tag{A.1}$$

In particular $[k(K) : k(w_1, w_2)] = 4$.

In all that follows we take ϵ to be a fixed solution of $\epsilon^4 = -1$.

We need a notation for the lines and some of the conics on the Fermat quartic surface X. (There are actually two types of conic on X, but only one of them concerns us.) Let μ and ν be odd residue classes mod 8; then the 48 lines on X can be written as

$$\begin{aligned} L_{\mu\nu} &: x_0 = \epsilon^\mu x_1, \quad x_2 = \epsilon^\nu x_3; \\ M_{\mu\nu} &: x_0 = \epsilon^\mu x_2, \quad x_1 = \epsilon^\nu x_3; \\ N_{\mu\nu} &: x_0 = \epsilon^\mu x_3, \quad x_1 = \epsilon^\nu x_2. \end{aligned}$$

(The rejection of symmetry here is deliberate, because cyclic symmetry plays no part in what follows. Note also that the notation is different to Mizukami's, and also to that of Segre.) We shall use Λ to denote any one of the three letters L, M, N. Then $\Lambda_{\alpha\beta}$ meets $\Lambda_{\gamma\delta}$ if and only if $\alpha = \gamma$ or $\beta = \delta$ but not both. Conditions for $\Lambda_{\alpha\beta}$ and $\Lambda'_{\gamma\delta}$ to meet, where Λ and Λ' are different, are as follows:

$$\begin{aligned} &L_{\alpha\beta} \text{ meets } M_{\gamma\delta} \text{ if and only if } \alpha - \beta - \gamma + \delta = 0, \\ &L_{\alpha\beta} \text{ meets } N_{\gamma\delta} \text{ if and only if } \alpha + \beta - \gamma + \delta = 0, \\ &M_{\alpha\beta} \text{ meets } N_{\gamma\delta} \text{ if and only if } \alpha + \beta - \gamma - \delta = 0. \end{aligned}$$

Now suppose that $\Lambda_{\alpha\beta}$ and $\Lambda'_{\gamma\delta}$ are two lines which meet, where Λ and Λ' are different; then the plane containing $\Lambda_{\alpha\beta}$ and $\Lambda'_{\gamma\delta}$ meets X residually in a conic, which we shall denote by

$[\Lambda_{\alpha\beta}\Lambda'_{\gamma\delta}]$. The lines $\Lambda_{\alpha\beta}$ and $\Lambda'_{\gamma\delta}$ meet this conic twice. The lines which meet it once are those which meet neither $\Lambda_{\alpha\beta}$ nor $\Lambda'_{\gamma\delta}$. Any other conic meets the plane of $[\Lambda_{\alpha\beta}\Lambda'_{\gamma\delta}]$ twice, and using the previous sentences one can work out its intersection with $[\Lambda_{\alpha\beta}\Lambda'_{\gamma\delta}]$.

If we write

$$f_{\lambda\mu\nu} = x_0 + \epsilon^{\lambda} x_1 + \epsilon^{\mu} x_2 + \epsilon^{\nu} x_3,$$

then the equations of $[L_{\alpha\beta}M_{\gamma\delta}]$ can be written as

$$\begin{aligned} x_0 - \epsilon^{\alpha}x_1 - \epsilon^{\gamma}x_2 + \epsilon^{\alpha+\delta}x_3 &= f_{\alpha+4,\gamma+4,\alpha+\delta} = 0,\\ x_0^2 + \epsilon^{\alpha+\delta}x_0x_3 + \epsilon^{2\alpha+2\delta}x_3^2 + \epsilon^{2\alpha}x_1^2 + \epsilon^{\alpha+\gamma}x_1x_2 + \epsilon^{2\gamma}x_2^2 &= 0.\end{aligned}$$

Thus the intersection of X with $f_{\alpha+4,\gamma+4,\alpha+\delta} = 0$ is

$$L_{\alpha\beta} + M_{\gamma\delta} + [L_{\alpha\beta}M_{\gamma\delta}],$$

where $\beta = \alpha - \gamma + \delta$. Similarly, the equations of $[L_{\alpha\beta}N_{\gamma\delta}]$ can be written as

$$\begin{aligned} x_0 - \epsilon^{\alpha}x_1 + \epsilon^{\alpha+\delta}x_2 - \epsilon^{\gamma}x_3 &= f_{\alpha+4,\alpha+\delta,\gamma+4} = 0,\\ x_0^2 + \epsilon^{\alpha+\delta}x_0x_2 + \epsilon^{2\alpha+2\delta}x_2^2 + \epsilon^{2\alpha}x_1^2 + \epsilon^{\alpha+\gamma}x_1x_3 + \epsilon^{2\gamma}x_3^2 &= 0.\end{aligned}$$

Thus the intersection of X with $f_{\alpha+4,\alpha+\delta,\gamma+4} = 0$ is

$$L_{\alpha\beta} + N_{\gamma\delta} + [L_{\alpha\beta}N_{\gamma\delta}],$$

where $\beta = \gamma - \alpha - \delta$.

We shall need some further intersections. If we write

$$e'_{\pm} = x_0x_3 \pm x_1x_2, \quad e''_{\pm} = x_0x_2 \pm x_1x_3,$$

then the intersections of X with the corresponding quadrics are as follows:

$$\begin{aligned} e'_{-} &= 0 : L_{11} + L_{33} + L_{55} + L_{77} + M_{11} + M_{33} + M_{55} + M_{77},\\ e'_{+} &= 0 : L_{15} + L_{37} + L_{51} + L_{73} + M_{15} + M_{37} + M_{51} + M_{73},\\ e''_{-} &= 0 : L_{17} + L_{35} + L_{53} + L_{71} + N_{11} + N_{33} + N_{55} + N_{77},\\ e''_{+} &= 0 : L_{13} + L_{31} + L_{57} + L_{75} + N_{15} + N_{37} + N_{51} + N_{73}.\end{aligned}$$

Again, if we write

$$\begin{aligned} h'_{\alpha\beta} &= x_0^2 - \epsilon^{2\alpha}x_1^2 - \epsilon^{2\beta}x_2^2 + \epsilon^{2\alpha+2\beta}x_3^2,\\ h''_{\alpha\beta} &= x_0^2 - \epsilon^{2\alpha}x_1^2 - \epsilon^{2\beta}x_3^2 + \epsilon^{2\alpha+2\beta}x_2^2,\end{aligned}$$

which only depend on α, β mod 4, then the intersection of X with $h'_{\alpha\beta} = 0$ is

$$L_{\alpha\alpha} + L_{\alpha,\alpha+4} + L_{\alpha+4,\alpha} + L_{\alpha+4,\alpha+4} + M_{\beta\beta} + M_{\beta,\beta+4} + M_{\beta+4,\beta} + M_{\beta+4,\beta+4}$$

and the intersection of X with $h''_{\alpha\beta} = 0$ is

$$L_{\alpha,-\alpha} + L_{\alpha,4-\alpha} + L_{\alpha+4,-\alpha} + L_{\alpha+4,4-\alpha} + N_{\beta\beta} + N_{\beta,\beta+4} + N_{\beta+4,\beta} + N_{\beta+4,\beta+4}.$$

Moreover, on X we have

$$h'_{13}h'_{31} = -h'_{11}h'_{33} = 2e'_{+}e'_{-}, \quad h''_{13}h''_{31} = -h''_{11}h''_{33} = 2e''_{+}e''_{-}. \tag{A.2}$$

There are a number of sets of sixteen mutually skew curves of genus 0 on X, of which a typical one is

$$\begin{aligned} &M_{51}, M_{33}, M_{15}, M_{77},\ [L_{33}M_{11}], [L_{33}M_{55}], [L_{15}M_{37}], [L_{15}M_{73}],\\ &N_{11}, N_{37}, N_{55}, N_{73},\ [L_{57}N_{15}], [L_{57}N_{51}], [L_{71}N_{33}], [L_{71}N_{77}].\end{aligned}$$

The map $X \to K$ which we shall exhibit identifies these sixteen curves with the sixteen disjoint lines on $K = \mathrm{Kum}(A)$ that correspond to the points of order 2 on A.

Now write

$$D' = 2L_{15} + M_{37} + M_{73} + [L_{31}N_{37}] + [L_{31}N_{73}]$$

and consider those principal divisors on X of degree 16 which contain D'. Four examples of them are given in the following list, which also names the associated functions of $x_0, \dots, x_3$ which give rise to them. The list is followed by rational expressions for these functions; they can of course also be written as polynomials, but the resulting formulae are unhelpful:

$$\begin{aligned}
F_1 &: D' + 2L_{73} + M_{15} + M_{51} + [L_{57}N_{15}] + [L_{57}N_{51}],\\
F_2 &: D' + 2L_{55} + M_{33} + M_{77} + [L_{71}N_{33}] + [L_{71}N_{77}],\\
F_3 &: D' + 2L_{31} + N_{37} + N_{73} + [L_{15}M_{37}] + [L_{15}M_{73}],\\
F_4 &: D' + 2L_{17} + N_{11} + N_{55} + [L_{33}M_{11}] + [L_{33}M_{55}].
\end{aligned}$$

Here we can take

$$\begin{aligned}
F_1 &= \frac{f_{727}f_{763}f_{125}f_{161}e'_+(x_0 - \epsilon x_1)(x_0 - \epsilon^7 x_1)}{e''_+(x_2 - \epsilon x_3)(x_2 - \epsilon^7 x_3)},\\
F_2 &= \frac{f_{727}f_{763}f_{327}f_{363}h'_{13}(x_2 - \epsilon^5 x_3)}{h''_{33}(x_2 - \epsilon x_3)},\\
F_3 &= f_{727}f_{763}f_{534}f_{570},\\
F_4 &= \frac{f_{727}f_{763}f_{754}f_{710}e''_- h'_{13}(x_0 - \epsilon x_1)(x_0 - \epsilon^7 x_1)}{e'_- h''_{33}(x_2 - \epsilon x_3)(x_2 - \epsilon^3 x_3)}.
\end{aligned}$$

The divisors residual to D' in the list of divisors associated with the F_i have self-intersection 0 and are linearly equivalent, so they lie in a pencil, which we denote by $\mathcal{P}'$. Hence the restrictions of any three of the F_i/F_3 to X are linearly dependent. To find their linear dependence relations, it is enough to consider, for example, their restrictions to M_{13}, and in this way we find that on X

$$F_3 = \epsilon^2 F_2 - \epsilon(1 + \epsilon^2)F_1, \quad F_4 = -\epsilon(1 + \epsilon^2)F_2 + \epsilon^2 F_1.$$

Let us also write

$$D'' = 2L_{33} + M_{11} + M_{55} + [L_{75}N_{37}] + [L_{75}N_{73}]$$

and consider those principal divisors on X of degree 16 which contain D''. The list which follows and the associated formulae correspond to the ones given above for the F_i:

$$\begin{aligned}
G_1 &: D'' + 2L_{11} + M_{33} + M_{77} + [L_{57}N_{15}] + [L_{57}N_{51}],\\
G_2 &: D'' + 2L_{37} + M_{15} + M_{51} + [L_{71}N_{33}] + [L_{71}N_{77}],\\
G_3 &: D'' + 2L_{75} + N_{37} + N_{73} + [L_{33}M_{11}] + [L_{33}M_{55}],\\
G_4 &: D'' + 2L_{53} + N_{11} + N_{55} + [L_{15}M_{37}] + [L_{15}M_{73}].
\end{aligned}$$

Here we can take

$$\begin{aligned}
G_1 &= \frac{f_{367}f_{323}f_{125}f_{161}e'_-(x_0 - \epsilon x_1)(x_0 - \epsilon^3 x_1)}{e''_+(x_2 - \epsilon^5 x_3)(x_2 - \epsilon^7 x_3)},\\
G_2 &= \frac{f_{367}f_{323}f_{327}f_{363}h'_{31}(x_0 - \epsilon^3 x_1)}{h''_{33}(x_0 - \epsilon^7 x_1)},\\
G_3 &= f_{367}f_{323}f_{754}f_{710},\\
G_4 &= \frac{f_{367}f_{323}f_{534}f_{570}e''_- h'_{31}(x_2 - \epsilon x_3)(x_2 - \epsilon^3 x_3)}{e'_+ h''_{33}(x_0 - \epsilon x_1)(x_0 - \epsilon^7 x_1)}.
\end{aligned}$$

The divisors residual to D'' in the list of divisors associated with the G_i have self-intersection 0 and are linearly equivalent, so they lie in a pencil, which we denote by $\mathcal{P}''$. Hence the restrictions of any three of the G_i/G_3 to X are again linearly dependent. To find their linear dependence relations, it is enough to consider, for example, their restrictions to M_{13}, and in this way we find that on X

$$G_3 = \epsilon(1+\epsilon^2)G_1 - \epsilon^2 G_2, \quad G_4 = -\epsilon(1+\epsilon^2)G_2 + \epsilon^2 G_1.$$

The restrictions to X of F_1G_2/F_2G_1 and F_3G_3/F_4G_4 both have divisors divisible by 2, so up to multiplication by a constant they are squares in $k(X)$. Making use of (A.2) we find that

$$\frac{F_1G_2}{F_2G_1} = 2\left(\frac{e'_+}{h'_{13}}\right)^2, \quad \frac{F_3G_3}{F_4G_4} = 2\left(\frac{e''_+}{h''_{11}}\right)^2.$$

Thus if we write

$$w_1 = \frac{\epsilon}{1+\epsilon^2}\cdot\frac{F_2}{F_1}, \quad w_2 = \frac{\epsilon}{1+\epsilon^2}\cdot\frac{G_2}{G_1}, \tag{A.3}$$

then we have

$$F_3/F_1 = \epsilon(1+\epsilon^2)(w_1-1), \quad F_4/F_1 = -2\epsilon^2(w_1-\tfrac{1}{2}),$$
$$G_3/G_1 = -\epsilon(1+\epsilon^2)(w_2-1), \quad G_4/G_1 = -2\epsilon^2(w_2-\tfrac{1}{2}).$$

In particular, we have a rational map $X \to K$ given by the equation (A.3) for w_1, w_2 together with

$$z = \epsilon^3(1+\epsilon^2)\frac{e'_+}{h'_{13}}, \quad y = 2\epsilon^2\frac{e''_+}{h''_{11}}. \tag{A.4}$$

But the curves $w_1 = \text{constant}$ and $w_2 = \text{constant}$ on X are elements of $\mathcal{P}'$ and $\mathcal{P}''$, respectively, so that their intersection has degree 4. In other words, if k contains ϵ then $[k(X):k(w_1,w_2)] = 4$; and from this it follows that the map $X \to K$ is actually birational. Since both X and K are minimal models in their birational equivalence class, any birational map $X \to K$ is a biregular isomorphism. □

Acknowledgements. We are very grateful to Tetsuji Shioda for sending us a copy of Mizukami's thesis [**9**], and to Peter Swinnerton-Dyer for the Appendix and for pointing out equation (3) to us. We thank Victor Flynn for his help with computations and Alice Silverberg for her help with references.

References

1. M. Bright, 'Computations on diagonal quartic surfaces', PhD Thesis, University of Cambridge, 2002, http://www.boojum.org.uk/maths/quartic-surfaces/thesis.pdf.
2. M. Bright, 'Brauer groups of diagonal quartic surfaces', *J. Symbolic Comput.* 41 (2006) 544–558.
3. A. Grothendieck, 'Le groupe de Brauer', *Dix exposés sur la cohomologie des schémas* (North-Holland, Amsterdam, 1968) 46–188.
4. E. Ieronymou, 'Diagonal quartic surfaces and transcendental elements of the Brauer group', *J. Inst. Math. Jussieu* 9 (2010) 769–798.
5. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd edn, Graduate Texts in Mathematics 84 (Springer, London, 1990).
6. A. Knapp, *Elliptic curves* (Princeton University Press, Princeton, NJ, 1992).
7. A. Kresch and Yu. Tschinkel, 'Effectivity of the Brauer–Manin obstructions on surfaces', Preprint, 2010, arXiv:1005.4331.
8. J. S. Milne, *Étale cohomology*, Princeton Mathematical Series 33 (Princeton University Press, Princeton, NJ, 1980).
9. M. Mizukami, 'Birational mappings from quartic surfaces to Kummer surfaces', Master Thesis, University of Tokyo, 1977 (Japanese).
10. M. Mizukami, 'Fixed point free involutions on certain nonsingular quartic surfaces', *Proceedings of the International Symposium on Algebraic Geometry*, Kyoto, 1977 (Kinokuniya, Tokyo, 1978) 589–593.
11. D. Mumford, *Lectures on curves on an algebraic surface* (Princeton University Press, Princeton, NJ, 1966).

12. I. I. Piatetskii-Shapiro and I. R. Shafarevich, ‘Torelli’s theorem for algebraic surfaces of type K3’, *Izv. Akad. Nauk SSSR Ser. Mat.* 35 (1971) 530–572 (Russian), *Math. USSR-Izv.* 5 (1971) 547–588 (English).

13. R. G. E. Pinch and H. P. F. Swinnerton-Dyer, ‘Arithmetic of diagonal quartic surfaces. I’, *L-functions and arithmetic*, London Mathematical Society Lecture Notes Series 153 (Cambridge University Press, Cambridge, 1991) 317–338.

14. K. Rubin and A. Silverberg, ‘Point counting on reductions of CM elliptic curves’, *J. Number Theory* 129 (2009) 2903–2923.

15. J.-P. Serre, ‘Propriétés galoisiennes des points d’ordre fini des courbes elliptiques’, *Invent. Math.* 15 (1972) 259–331.

16. J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 2nd edn (Addison-Wesley, Reading, MA, 1989).

17. J.-P. Serre and J. Tate, ‘Good reduction of abelian varieties’, *Ann. of Math.* 88 (1968) 492–517.

18. J. Silverman, *The arithmetic of elliptic curves* (Springer, Berlin, 1986).

19. A. Skorobogatov, *Torsors and rational points* (Cambridge University Press, Cambridge, 2001).

20. A. N. Skorobogatov and Yu. G. Zarhin, ‘A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces’, *J. Algebraic Geom.* 17 (2008) 481–502.

21. A. N. Skorobogatov and Yu. G. Zarhin, ‘The Brauer group of Kummer surfaces and torsion of elliptic curves’, *J. reine angew. Math.*, arXiv:0911.2261, to appear.

Evis Ieronymou
Ecole Polytechnique Fédérale de Lausanne
EPFL-SFB-IMB-CSAG, Station 8
CH-1015 Lausanne
Switzerland

Evis.Ieronymou@epfl.ch

Yuri G. Zarhin
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
USA
and
Institute for Mathematical Problems in Biology
Russian Academy of Sciences
Pushchino
Moscow Region
Russia

zarhin@math.psu.edu

Alexei N. Skorobogatov
Department of Mathematics
South Kensington Campus
Imperial College London
London
SW7 2BZ
United Kingdom
and
Institute for the Information Transmission Problems
Russian Academy of Sciences
19 Bolshoi Karetnyi
Moscow 127994
Russia

a.skorobogatov@imperial.ac.uk