Corrigendum to “Odd order Brauer–Manin obstruction on diagonal quartic surfaces”

Evis Ieronymou and Alexei N. Skorobogatov

Abstract

We correct a mistake in our paper “Odd order Brauer–Manin obstruction on diagonal quartic surfaces” published in *Advances in Mathematics* **270** (2015) 181–205.

1 Errata

The assertion made in the sentence in lines 27–29 on page 202 of [2] is incorrect. This invalidates Proposition 5.13, Lemma 5.16, Corollary 5.17, Proposition 5.19, and thus also statement (ii) of Theorem 1.2 in the case $\ell = 3$, the second statement of Corollary 1.3 and statement (1) of Corollary 1.5. The second sentence of the abstract should be replaced by the sentence “We calculate the obstruction to weak approximation provided by the elements of odd order in the Brauer group”. The following should be removed from the introduction: “and always obstructs weak approximation” (page 183, lines 12–13) and the text on page 184, lines 20–25, starting with “In the same way...” and finishing with “$9|yzw$.)”

2 Corrections

Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$ with complex multiplication by $\mathbb{Z}[\sqrt{-1}]$. For $m \in \mathbb{Q}^*$ we write E^m for the quartic twist $y^2 = x^3 - mx$ of E. Let E_3^m be the 3-torsion subgroup of E^m considered as a $\Gamma_{\mathbb{Q}}$-module. Complex multiplication defines an injective homomorphism of rings $\mathbb{Z}[\sqrt{-1}]/3 \cong \mathbb{F}_9 \to \mathrm{End}(E_3^m)$. The action of $\Gamma_{\mathbb{Q}(\sqrt{-1})}$ on E_3^m factors through the surjective homomorphism $\Gamma_{\mathbb{Q}(\sqrt{-1})} \to \mathbb{F}_9^*$ which is the composition of $\psi_m : \Gamma_{\mathbb{Q}(\sqrt{-1})} \to \mathbb{Z}[\sqrt{-1}]$ with the reduction modulo 3, where

$$\psi_m(\mathrm{Frob}_\pi) = \overline{\left(\frac{m}{\pi}\right)_4}\,\pi$$

for any primary prime $\pi \in \mathbb{Z}[\sqrt{-1}]$ which is coprime to m, see [4, Exercise 2.34]. It follows that the image G of $\Gamma_{\mathbb{Q}} \to \mathrm{GL}(E_3^m)$ is the normaliser of the non-split maximal torus $\mathbb{F}_9^* \rtimes \mathbb{Z}/2$, so G is a 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, cf. page 189 of [2]. We note that $\mathrm{H}^1(G, E_3^m) = 0$, because G is a finite 2-group and E_3^m is a vector space over $\mathbb{F}_3$. We also note that $\mathrm{End}_G(E_3^m) = \mathbb{F}_3$, hence E_3^m is an irreducible representation of G over $\mathbb{F}_3$.

Let $m_1, m_2 \in \mathbb{Q}^*$. We denote by $\mathrm{Hom}(E_3^{m_2}, E_3^{m_1})^-$ the subgroup of $\mathrm{Hom}(E_3^{m_2}, E_3^{m_1})$ consisting of the homomorphisms which anti-commute with $[\sqrt{-1}]$, so that $\mathrm{End}(E_3^m) = \mathbb{Z}[\sqrt{-1}]/3 \oplus \mathrm{End}(E_3^m)^-$. By Lemma 4.2 of [2] and the remark after it, the $\Gamma_{\mathbb{Q}}$-module $\mathrm{End}(E_3)^-$ is the quartic twist of $\Gamma_{\mathbb{Q}}$-module $\mathbb{Z}[\sqrt{-1}]/3$ by the class of -3^3 in $\mathbb{Q}^*/\mathbb{Q}^{*4}$. Then the argument of [2, Prop. 3.3] shows that the $\Gamma_{\mathbb{Q}}$-module $\mathrm{Hom}(E_3^{m_2}, E_3^{m_1})^-$ is the quartic twist of $\mathbb{Z}[\sqrt{-1}]/3$ by the class of $-3^3(m_1m_2)^{-1}$ in $\mathbb{Q}^*/\mathbb{Q}^{*4}$. If $m_1, m_2 \in \mathbb{Q}^*$ are such that $-3m_1m_2 \in \langle -4\rangle\mathbb{Q}^{*4}$, then we obtain an isomorphism of $\Gamma_{\mathbb{Q}}$-modules $\varphi : E_3^{m_2} \to E_3^{m_1}$. Since $\mathrm{End}_G(E_3^m) = \mathbb{F}_3$, it is unique up to sign.

Lemma 2.1 *For any $m \in \mathbb{Q}_3^*$ the image of $\Gamma_{\mathbb{Q}_3} \to \mathrm{GL}(E_3^m)$ is G.*

Proof. Multiplying m by a fourth power in $\mathbb{Q}_3^*$, which produces an isomorphic elliptic curve, we can assume that $m \in \mathbb{Q}^*$. Let $L = \mathbb{Q}(E_3^m)$ be the field of definition of E_3^m over $\mathbb{Q}$, so that $G = \mathrm{Gal}(L/\mathbb{Q})$. The Galois group $\Gamma_{\mathbb{Q}}$ acts on $\mathbb{Z}[\sqrt{-1}]/3 \subset \mathrm{End}(E_3^m)$ by complex conjugation, so $\sqrt{-1} \in L$. Next, $\Gamma_{\mathbb{Q}(\sqrt{-1})}$ acts on $\mathrm{End}(E_3^m)^-$ via the quartic character attached to -3^3m^2, hence $F = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{-3^3m^2}) \subset L$. We obtain a surjective homomorphism

$$\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-1})) \cong \mathbb{Z}/8 \longrightarrow \mathrm{Gal}(F/\mathbb{Q}(\sqrt{-1})) \cong \mathbb{Z}/4$$

and a compatible surjective homomorphism

$$\pi : G = \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/8 \rtimes \mathbb{Z}/2 \longrightarrow \mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/4 \rtimes \mathbb{Z}/2.$$

Fix an inclusion $\Gamma_{\mathbb{Q}_3} \subset \Gamma_{\mathbb{Q}}$. Let $K = \mathbb{Q}_3(E_3^m)$ be the field of definition of E_3^m over $\mathbb{Q}_3$, and let $H = \mathrm{Gal}(K/\mathbb{Q}_3)$. We need to prove that the inclusion $H \subset G$ is an equality. Note that $F_3 = F \otimes \mathbb{Q}_3 = \mathbb{Q}_3(\sqrt{-1}, \sqrt[4]{3})$ is a Galois extension of $\mathbb{Q}_3$ with the Galois group $\mathrm{Gal}(F_3/\mathbb{Q}_3) = \mathrm{Gal}(F/\mathbb{Q})$. The same arguments as above show that $F_3 \subset K$. Thus H is a subgroup of G such that $\pi(H) = \mathbb{Z}/4 \rtimes \mathbb{Z}/2$. The intersection $H \cap \mathbb{Z}/8 \subset G$ has least 4 elements, and thus contains $\mathrm{Ker}\,(f)$. Hence $H = G$. $\square$

Lemma 2.1 implies that $E_3^m(\mathbb{Q}_3) = 0$ for any $m \in \mathbb{Q}_3^*$. The topological group $E^m(\mathbb{Q}_3)$ contains $\mathbb{Z}_3$ as a subgroup of finite index not divisible by 3, so $E^m(\mathbb{Q}_3)/3 \cong \mathbb{F}_3$. Recall that the Kummer map embeds $E^m(\mathbb{Q}_3)/3$ into $\mathrm{H}^1(\mathbb{Q}_3, E_3^m)$ as a maximal isotropic subspace for the non-degenerate symmetric bilinear form induced by the Weil pairing:

$$\cup : \ \mathrm{H}^1(\mathbb{Q}_3, E_3^m) \times \mathrm{H}^1(\mathbb{Q}_3, E_3^m) \longrightarrow \mathrm{Br}(\mathbb{Q}_3)[3] \xrightarrow{\sim} \frac{1}{3}\mathbb{Z}/\mathbb{Z} \qquad (1)$$

where the last arrow is the local invariant inv_3. In particular, $\mathrm{H}^1(\mathbb{Q}_3, E_3^m)$ is a 2-dimensional vector space over $\mathbb{F}_3$. For $P \in E^m(\mathbb{Q}_3)$ we write $\chi_P \in \mathrm{H}^1(\mathbb{Q}_3, E_3^m)$ for the image of P under the Kummer map.

If $m_1, m_2 \in \mathbb{Q}_3^*$ are such that $\pm 3m_1m_2 \in \mathbb{Q}_3^{*4}$, then there is an isomorphism of $\Gamma_{\mathbb{Q}_3}$-modules $\varphi : E_3^{m_2} \to E_3^{m_1}$, which is unique up to sign. Indeed, we can assume $m_1, m_2 \in \mathbb{Q}^*$ and $-3m_1m_2 \in \langle -4\rangle \mathbb{Q}^{*4}$. The isomorphism of $\Gamma_{\mathbb{Q}}$-modules $\varphi : E_3^{m_2} \to E_3^{m_1}$ is also an isomorphism of $\Gamma_{\mathbb{Q}_3}$-modules. By Lemma 2.1, $\mathrm{End}_G(E_3^m) = \mathbb{F}_3$ implies $\mathrm{End}_{\mathbb{Q}_3}(E_3^m) = \mathbb{F}_3$, so any such isomorphism is unique up to sign. We define a bilinear pairing

$$[\ ,\ ] :\ E^{m_1}(\mathbb{Q}_3)\ \times E^{m_2}(\mathbb{Q}_3) \longrightarrow \frac{1}{3}\mathbb{Z}/\mathbb{Z}, \qquad [P,Q] = \chi_P \cup \varphi_*(\chi_Q),$$

where $P \in E^{m_1}(\mathbb{Q}_3)$, $Q \in E^{m_2}(\mathbb{Q}_3)$, and $\varphi_* : \mathrm{H}^1(\mathbb{Q}_3, E_3^{m_2}) \to \mathrm{H}^1(\mathbb{Q}_3, E_3^{m_1})$ is the isomorphism induced by φ.

The following statement replaces the erroneous Proposition 5.13 of [2].

Proposition 2.2 *The pairing* $[\ ,\ ]$ *is trivial if the* 3*-adic valuation of* m_1 *or* m_2 *is zero modulo* 4*, otherwise* $[P,Q] \neq 0$ *as long as* $P \notin 3E^{m_1}(\mathbb{Q}_3)$ *and* $Q \notin 3E^{m_2}(\mathbb{Q}_3)$*.*

Proof. Let $P \in E^{m_1}(\mathbb{Q}_3)$ be a point not divisible by 3 in $E^{m_1}(\mathbb{Q}_3)$, and similarly for $Q \in E^{m_2}(\mathbb{Q}_3)$. Then $\chi_P \neq 0$ and $\chi_Q \neq 0$. The subspace of $\mathrm{H}^1(\mathbb{Q}_3, E_3^{m_1})$ spanned by χ_P is maximal isotropic for the non-degenerate symmetric pairing (1). It follows that $[P,Q] = 0$ if and only if $\chi_P = \pm\varphi_*(\chi_Q)$. Let Z_P be the $\mathbb{Q}_3$-torsor for $E_3^{m_1}$ defined as the inverse image of $P \in E^{m_1}(\mathbb{Q}_3)$ under the multiplication by 3 map, so that Z_P represents the class $\chi_P \in \mathrm{H}^1(\mathbb{Q}_3, E_3^{m_1})$. We define Z_Q similarly for Q, so that χ_Q is the class of Z_Q in $\mathrm{H}^1(\mathbb{Q}_3, E_3^{m_2})$. Since $\mathrm{H}^1(G, E_3^m) = 0$ and $\mathrm{End}_G(E_3^m) = \mathbb{F}_3$, we can use [1, Cor. 3.3] which implies that $\chi_P = \pm\varphi_*(\chi_Q)$ if and only if Z_P and Z_Q are isomorphic as $\mathbb{Q}_3$-schemes. By *loc. cit.* these schemes are connected, so this is equivalent to an isomorphism $\mathbb{Q}_3[Z_P] \cong \mathbb{Q}_3[Z_Q]$ of field extensions of $\mathbb{Q}_3$. For each $m = \pm 3^n$, $n = 0, 1, 2, 3$, write $k_m = \mathbb{Q}_3[Z_P]$; indeed, up to isomorphism, this field depends only on m and not on P.

It is well known that the quotient of E^m by the degree 2 isogeny with the kernel $\{0, (0,0)\}$ is isomorphic to E^{-4m}. This isogeny sends a generator of $E^m(\mathbb{Q}_3)/3$ to a generator of $E^{-4m}(\mathbb{Q}_3)/3$ and induces an isomorphism of corresponding torsors for the group scheme $E_3^m \cong E_3^{-4m}$. This produces an isomorphism $k_m \cong k_{-m}$ of field extensions of $\mathbb{Q}_3$.

It remains to examine the four fields k_1, k_3, k_9 and k_{27} and to decide whether k_1 and k_{27} are isomorphic extensions of $\mathbb{Q}_3$, and similarly for k_3 and k_9. We can write $k_m = \mathbb{Q}_3[t]/(f_m(t))$, where the polynomial $f_m(t)$ of degree 9 is given on page 201 of [2]. For $m = 1$ we choose the point $P \in E^m(\mathbb{Q}_3)$ with $x_P = 1/9$ and in each of the other cases we choose $x_P = 1$. Consider the following Eisenstein polynomials

$$f(t) = t^9 + 6t + 6, \quad g(t) = t^9 + 6t^7 + 3, \quad h(t) = t^9 + 3t^5 + 3.$$

A computation performed with [3] shows that

$$k_1 \cong k_{27} \cong \mathbb{Q}_3[t]/(f(t)), \quad k_3 \cong \mathbb{Q}_3[t]/(g(t)), \quad k_9 \cong \mathbb{Q}_3[t]/(h(t)),$$

and these three fields are pairwise non-isomorphic extensions of $\mathbb{Q}_3$. $\square$

We now give a correction for Theorem 1.2 (ii) in the case $\ell = 3$.

By [2, Thm. 1.1] any diagonal quartic surface $D \subset \mathbb{P}^3_{\mathbb{Q}}$ with an element of order 3 in $\mathrm{Br}(D)/\mathrm{Br}_0(D)$ is given by

$$ax^4 + by^4 = cz^4 + dw^4, \tag{2}$$

where $a, b, c, d \in \mathbb{Q}^*$ are such that $-3abcd \in \langle -4 \rangle \mathbb{Q}^{*4}$. By renaming the variables and multiplying coefficients a, b, c, d by fourth powers of rational numbers and by a common rational number, we can arrange that the 3-adic valuation of a, b, c, d is of one of the following types:

$$\text{(I)} \ \ (0, 0, 0, 3) \qquad \text{or} \qquad \text{(II)} \ \ (0, 0, 1, 2).$$

For an abelian group B we denote by B_{odd} the subgroup of B consisting of the elements of finite odd order.

Theorem 2.3 *Let D be a diagonal quartic surface over $\mathbb{Q}$ with $D(\mathbb{Q}_3) \neq \emptyset$ and an element $\mathcal{A} \in \mathrm{Br}(D)_3$ which is not in $\mathrm{Br}_0(D)$.*

When D is of type (I)*, the map* $\mathrm{ev}_{\mathcal{A},3}$ *is constant. When D is of type* (II)*, the map* $\mathrm{ev}_{\mathcal{A},3}$ *is surjective.*

Assume $D(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. Then $D(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(D)_{\mathrm{odd}}} = D(\mathbb{A}_{\mathbb{Q}})$ when D is of type (I)*, and $\emptyset \neq D(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(D)_{\mathrm{odd}}} \neq D(\mathbb{A}_{\mathbb{Q}})$ when D is of type* (II)*.*

Proof. We can assume that D is given by (2), where the 3-adic valuations of a, b, c, d are of type (I) or (II). After a renaming of variables and multiplication of coefficients by ± 1, we can assume that in case (I) we have

(I) $a, b \in 1 + 3\mathbb{Z}_3$, $c \in \mathbb{Z}_3^*$, $d \in 27\mathbb{Z}_3^*$,

see [2, Lemma 5.18]. Using the condition $D(\mathbb{Q}_3) \neq \emptyset$, in case (II) we arrange that

(II) $a \in 1 + 3\mathbb{Z}_3$, $b \in -1 + 3\mathbb{Z}_3$, $c \in 3\mathbb{Z}_3^*$, $d \in 9\mathbb{Z}_3^*$.

Since $\mathcal{A}(L)$ is a locally constant function of $L \in D(\mathbb{Q}_3)$ in the 3-adic topology of $D(\mathbb{Q}_3)$, for the purpose of calculating $\mathrm{ev}_{\mathcal{A},3}(D(\mathbb{Q}_3))$ we can assume that L has coordinates $(x, y, z, w) \in (\mathbb{Z}_3)^4$ not all divisible by 3 such that $f = ax^4 + by^4 \neq 0$ and $xyzw \neq 0$. A straightforward calculation shows that in case (I) we have $f \in \mathbb{Z}_3^*$.

Let $m_1 = 4ab(f/x^2y^2)^2$ and $m_2 = 4cd(f/z^2w^2)^2$. The curve E^{m_1} contains the $\mathbb{Q}_3$-point $P = (-4ab, 4abx^{-2}y^{-2}(ax^4 - by^4))$, and E^{m_2} contains the $\mathbb{Q}_3$-point $Q = (-4cdz^2w^2, 4cdz^{-2}w^{-2}(cz^4 - dw^4))$, see page 192 of [2].

By Theorem 1.1 and formula (6) on page 188 of [2], there is a non-zero homomorphism of $\Gamma_{\mathbb{Q}}$-modules $\varphi : E_3^{4cd} \to E_3^{4ab}$, which is unique up to sign. Furthermore, φ is an isomorphism, see page 192 of [2]. By [2, Thm. 1.1] we have $\mathrm{Br}(D)/\mathrm{Br}_0(D) \cong \mathbb{Z}/3$, hence modifying $\mathcal{A}$ by an element of $\mathrm{Br}_0(D)$ we can assume without loss of generality that, up to sign, $\mathcal{A}$ is constructed from φ as described on page 193 of [2]. The $\Gamma_{\mathbb{Q}_3}$-modules $E_3^{m_2}$ and $E_3^{m_1}$ are isomorphic; we fix an isomorphism which is induced by φ. Then, by formula (9) of [2], we have

$$\mathrm{inv}_3(\mathcal{A}(L)) = [P, Q] \ \in \ \frac{1}{3}\mathbb{Z}/\mathbb{Z}.$$

If D is of type (I), then $f \in \mathbb{Z}_3^*$ and hence the class of m_1 in $\mathbb{Q}_3^*/\mathbb{Q}_3^{*4}$ is 1. It follows from Proposition 2.2 that the map $\mathrm{ev}_{\mathcal{A},3}$ is identically zero.

If D is of type (II), then in the course of the proof of Proposition 5.19 of [2] (page 204) we have exhibited a point $L \in D(\mathbb{Q}_3)$ such that $f \in 3\mathbb{Z}_3^*$ and neither P nor Q is divisible by 3. In this case neither m_1 nor m_2 is in $\mathbb{Z}_3^*/\mathbb{Z}_3^{*4}$, hence $\mathrm{inv}_3(\mathcal{A}(L)) \neq 0$ by Proposition 2.2. We have also exhibited a point $L' \in D(\mathbb{Q}_3)$ such that $\mathcal{A}(L') = 0$. Since $\mathrm{ev}_{\mathcal{A},3}(D(\mathbb{Q}_3))$ is a subset of $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$ stable under the change of sign [2, Cor. 5.2], we conclude that $\mathrm{ev}_{\mathcal{A},3}$ is surjective in this case.

Now assume $D(\mathbb{A}_\mathbb{Q}) \neq \emptyset$. The map $\mathrm{ev}_{\mathcal{A},p}$ is identically zero for any $p \neq \ell$ by [2, Prop. 5.5]. The same is true for the infinite place. This gives the last statement of the theorem. □

The authors are very grateful to Chris Wuthrich and Martin Bright for their help with calculations.

References

[1] Y. Harpaz and A.N. Skorobogatov. Hasse principle for generalised Kummer varieties. Preprint, 2015.

[2] E. Ieronymou and A.N. Skorobogatov. Odd order Brauer–Manin obstruction on diagonal quartic surfaces. *Adv. Math.* **270** (2015) 181–205.

[3] J.W. Jones and D.P. Roberts. Database of local fields. Available at `https://math.la.asu.edu/~jj/localfields/`

[4] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Grad. Texts in Math., vol. 151, Springer-Verlag, 1994.