POINTS DEFINED OVER CYCLIC CUBIC EXTENSIONS ON AN ELLIPTIC CURVE AND GENERALIZED KUMMER SURFACES

MASATO KUWATA

1. Introduction

Let E be an elliptic curve defined over a number field k. The Mordell-Weil theorem asserts that $E(k)$, the group of k-rational point, is a finitely generated abelian group. If E and k are given in an explicit form, it is often possible to determine the rank of $E(k)$, though at present we do not dispose of any algorithm that guarantees the determination. In this paper we fix E once and for all and study the behavior of the rank of the group $E(K_\lambda)$ as we vary K_λ through a certain family of finite extensions of k.

One case that has been well studied is the case where K_λ runs through the family of quadratic extensions of k. If E is an elliptic curve over k given by the Weierstrass equation $y^2 = x^3 + Ax + B$, and d is a nonzero element of k, the quadratic twist of E by d, noted E_d, is given by the equation $dy^2 = x^3 + Ax + B$. Since we have the relation $\operatorname{rank} E(k(\sqrt{d})) = \operatorname{rank} E(k) + \operatorname{rank} E_d(k)$, studying the behavior of the rank of the group $E(k(\sqrt{d}))$, as $k(\sqrt{d})$ varies through all the quadratic extensions of k, is equivalent to studying the family of quadratic twists $\{E_d\}_{d\in k^\times/(k^\times)^2}$.

In this paper we consider all the *cyclic cubic* extensions of k instead of considering quadratic extensions. In the quadratic case it is very easy to find values of d such that $\operatorname{rank} E_d(k)$ is positive. Gouvêa and Mazur[4] found lower bounds for the number of times $\operatorname{rank} E_d(\mathbb{Q})$ is ≥ 2. In our case, however, it is not clear whether or not there exists a cyclic cubic extension K such that $\operatorname{rank} E(K)$ is positive. The purpose of this paper is to show that once we find one such extension, we are able to find many other such extensions by a geometric method. Our main theorem is

Theorem 1.1. *Let E be an elliptic curve defined over a number field k. If there is a cyclic cubic extension K_0 over k such that the Mordell-Weil group $E(K_0)$ is positive, then there exists an infinite family $\{K_\lambda\}$ of cyclic cubic extensions of k such that the rank of $E(K_\lambda)$ is positive.*

Unlike the quadratic case, we do not dispose of such a curve E_{K_λ} defined over k for each cyclic cubic extension K_λ such that k-rational points on E_{K_λ} correspond K_λ-rational points on E. Instead, we will show that there is a

Date: November, 1999.

Key words and phrases. Elliptic curves, $K3$ surfaces, Kummer surfaces.

$K3$ surface S_E such that k-rational points on S_E correspond points on E defined over some cyclic cubic extension of k. The surface S_E is obtained as the minimal desingularization of the quotient surface $(E \times E)/\langle\rho\rangle$, where ρ is the automorphism of order 3 given by $(P, Q) \mapsto (-P-Q, P)$. The surface S_E is an example of generalized Kummer surfaces (see Definition 3.2). We will show that S_E possesses a fibration $\pi : S_E \to \mathbf{P}^1$ whose fiber C_t at the generic point t on $\mathbf{P}^1$ is a curve of genus 1 with an involution ι. This fibration is essential for the proof of our main theorem.

It turns out that the fibration π has two sections defined over $k(\sqrt{-3})$, and if we choose one of them as the 0-section, the other becomes a section of infinite order. Thus, we have

Theorem 1.2. *Let E be an elliptic curve defined over a number field k containing $\sqrt{-3}$. Then there exist infinitely many cyclic cubic extensions K_λ such that* $\operatorname{rank} E(K_\lambda)$ *is positive.*

When the base field k is a real field, then, we can show a result on S_E of somewhat different nature. In §5 we show that the family of surfaces $\{S_E\}$ satisfies Mazur's conjecture on the topology of rational points(see [8][9][2]) in its original form. More precisely, we have

Theorem 1.3. *Let E be an elliptic curve defined over a number field k embedded in the field of real numbers $\mathbb{R}$. Let S_E be the generalized Kummer surface obtained from the quotient $(E \times E)/\langle g\rangle$ as above. If $S_E(k)$ is Zariski dense in S_E, then the closure of $S_E(k)$ with respect to the ordinary topology of $\mathbb{R}$ is open in $S_E(\mathbb{R})$.*

As a matter of fact, this result was the original aim of the author, who sought for the results similar to an earlier result in [7] on the Kummer surfaces of product type.

Assuming the Birch and Swinnerton-Dyer conjecture, our problem may be translated to the vanishing of the twist the L-function by cubic Dirichlet characters. Kisilevsky and Fearnley have been studying from this point of view, and they obtained similar results as those contained in this paper using other methods. For more detail, see the upcoming thesis of Fearnley.

As Fearnley's numerical results suggest, we generally feel that we should be able to prove the existence of many rational points on S_E for any E without any other assumptions. At present, however, we are unable to find, in general, a point on S_E that satisfies the hypothesis of Theorem 1.1. In §7 we provide a few examples where we show the existence of many k-rational points on S_E starting from a torsion point of E.

The nature of our proof of Theorem 1.1 does not provide us a quantitative result, unfortunately. It is desirable to obtain some quantitative result, but the technical difficulty is greater than that of quadratic case.

The author would like to thank Hershy Kisilevsky and Jack Fearnley for useful conversations, which took place in the hospitable environment the CICMA provided him during his stay in Montreal.

2. Permutation action on the self product of an algebraic variety

Let X be an algebraic variety defined over a number field k, namely, a geometrically integral scheme of finite type over $\operatorname{Spec} k$. Let $\bar{k}$ be an algebraic closure of k, which we fix once and for all. We denote by $G = \operatorname{Gal}(\bar{k}/k)$ its Galois group. Throughout this paper, a point means a geometric point, i.e., a $\bar{k}$-valued point. This is the same as a closed point of the scheme $X \times_k \operatorname{Spec} \bar{k}$.

Let Γ be a finite group, and n its order. Write $\Gamma = \{g_1, g_2, \ldots, g_n\}$, which fixes a bijection between Γ and $\{1, 2, \ldots, n\}$. The left translation $L_g : x \mapsto gx$ induces a homomorphism from Γ to the symmetric group S_n, and we let Γ act on the variety $X^n = X \times \cdots \times X$ via this homomorphism. More precisely, define a permutation $\pi_g \in S_n$ by the formula $gg_i = g_{\pi_g(i)}$, and define an action of $g \in \Gamma$ by

$$g \cdot (P_1, P_2, \ldots, P_n) = (P_{\pi_{g^{-1}(1)}}, P_{\pi_{g^{-1}(2)}}, \ldots, P_{\pi_{g^{-1}(n)}}).$$

Let $Y = X^n/\Gamma$ be its quotient variety (cf. [11, Ch. II, §7 and Ch. III, §12)]). It is obvious that the Γ-action on X^n commutes with the Galois action on X^n. Thus, Y is a variety defined over k. We denote by $[P_1, \ldots, P_n]$ the class of $(P_1, \ldots, P_n)$ in Y.

Let $(X^n)^\circ$ be the open set of X^n consisting of points whose stabilizer in Γ is reduced to the identity element. The group Γ acts on $(X^n)^\circ$ freely. Let Y° the quotient of $(X^n)^\circ$ by Γ.

Lemma 2.1. *A point $[P_1, \ldots, P_n]$ in Y° is a k-rational point if and only if there is a Galois extension K of k such that*

1. *for all i, P_i is defined over K, and*
2. *there is an injective homomorphism $\rho : \operatorname{Gal}(K/k) \to \Gamma$ such that*

$$(\sigma(P_1), \ldots, \sigma(P_n)) = \rho(\sigma)^{-1} \cdot (P_1, \ldots, P_n)$$

for all $\sigma \in \operatorname{Gal}(K/k)$.

Proof. Suppose $[P_1, \ldots, P_n] \in Y^\circ$ is a k-rational point. This is equivalent to say that for any $\sigma \in G$ there exist $g_\sigma \in \Gamma$ such that $(\sigma(P_1), \ldots, \sigma(P_n)) = g_\sigma \cdot (P_1, \ldots, P_n)$. We first claim that g_σ is unique. Indeed, if g'_σ is another element satisfying the same property, then $g_\sigma^{-1} g'_\sigma$ fixes the point $(P_1, \ldots, P_n)$. But Γ acts freely on $(X^n)^\circ$, which implies $g_\sigma^{-1} g'_\sigma$ is the identity. We thus have a map $\operatorname{Gal}(\bar{k}/k) \to \Gamma$ given by $\sigma \mapsto g_\sigma$. It is easy to see that this is an anti-homomorphism; i.e., we have $g_{\sigma\tau} = g_\tau g_\sigma$. Thus we obtain a homomorphism $\tilde{\rho}$ by defining $\sigma \mapsto g_\sigma^{-1}$.

Let $\operatorname{Stab}_G(P_i)$ be the stabilizer of P_i under the Galois action on X. We claim that $\operatorname{Stab}_G(P_1) = \operatorname{Stab}_G(P_2) = \cdots = \operatorname{Stab}_G(P_n)$. To show this choose $h \in \Gamma$ such that $g_1 = hg_i$, and let τ be any element of $\operatorname{Stab}_G(P_1)$. Then the first coordinate of $\tau h(P_1, \ldots, P_n)$ is $\tau(P_i)$, while the first coordinate of $h\tau(P_1, \ldots, P_n)$ is P_i. Since τ and h commute, we deduce that $\tau(P_i) = P_i$. This shows that $\operatorname{Stab}_G(P_1)$ is contained in $\operatorname{Stab}_G(P_i)$. Exchanging the rolls of 1 and i, the same argument shows that $\operatorname{Stab}_G(P_i)$ is also contained in $\operatorname{Stab}_G(P_1)$. This shows that $\operatorname{Stab}_G(P_1) = \operatorname{Stab}_G(P_i)$ for any i. It follows from this that $\operatorname{Stab}_G(P_i)$ is the kernel of the G-action on the set $\{P_1, \dots, P_n\}$. In particular, $\operatorname{Stab}_G(P_i)$ is a normal subgroup of finite index in $G = \operatorname{Gal}(\bar{k}/k)$. This implies that there is a Galois extension K of k such that $\operatorname{Stab}_G(P_i) = \operatorname{Gal}(\bar{k}/K)$. This means that P_i is defined over K for all i. Since $\operatorname{Stab}_G(P_i)$ is also the kernel of the homomorphism $\tilde{\rho}$, we have an injective homomorphism $\rho : \operatorname{Gal}(K/k) \simeq \operatorname{Gal}(\bar{k}/k) \big/ \operatorname{Gal}(\bar{k}/K) \to \mathit{\Gamma}$ induced by $\tilde{\rho}$. This homomorphism ρ satisfies the condition 2. □

Next we consider the above situation when X is an abelian variety A. For any X, the diagonal $D = \{(P, P, \dots, P) \mid P \in X\}$ of X^n is a subvariety invariant under the $\mathit{\Gamma}$-action. If $X = A$ is an abelian variety (or more generally, a commutative group variety), then D is a subgroup of A^n, and we may define the complement D' of D in A^n to be

$$D' = \{(P_1, P_2, \dots, P_n) \mid \sum_{i=1}^{n} P_i = O\}.$$

Then D' is a subgroup of A^n invariant under $\mathit{\Gamma}$-action. Moreover we have a degree n isogeny φ given by

$$\begin{array}{cccc} \varphi : & A^n & \longrightarrow & D \times D' \\ & (P_1, \dots, P_n) & \longmapsto & \Big(\big(\sum_{i=0}^{n} P_i, \dots, \sum_{i=0}^{n} P_i\big), \big(P_1 - \sum_{i=0}^{n} P_i, \dots, P_n - \sum_{i=0}^{n} P_i\big) \Big). \end{array}$$

Its dual isogeny $\hat{\varphi} : D \times D' \to A^n$ is defined by

$$\begin{array}{cccc} \hat{\varphi} : & D \times D' & \longrightarrow & A^n \\ & \big((R, \dots, R), (P_1, \dots, P_n)\big) & \longmapsto & (P_1 + nR, \dots, P_n + nR). \end{array}$$

Since φ and $\hat{\varphi}$ commute with the $\mathit{\Gamma}$-action, we obtain two maps

$$\bar{\varphi} : Y \to (D \times D')/\mathit{\Gamma}, \qquad \bar{\hat{\varphi}} : (D \times D')/\mathit{\Gamma} \to Y$$

such that $\bar{\hat{\varphi}} \circ \bar{\varphi}$ is the map $\overline{[n]}$ induced from the multiplication-by-n map $[n]$ of A^n.

3. Generalized Kummer surface S_E

In this section we apply the results of the previous section to the case where X is an elliptic curve E defined over a number field k and $\mathit{\Gamma}$ is a cyclic group of order 3. Let g be a generator of $\mathit{\Gamma}$ and set $g_i = g^{i-1}$ for $i = 1, 2, 3$. Then the action of g on E^3 is given by

$$g \cdot (P, Q, R) = (R, P, Q).$$

Identify D' with $E \times E$ through the map $(P, Q, R) \mapsto (P, Q)$. Its inverse is given by $(P, Q, -P - Q)$. Through this identification g acts on $E \times E$ by

$$g \cdot (P, Q) = (-P - Q, P).$$

Let $\overline{S}_E$ be the quotient of $E \times E$ by this action. As before, we denote by $[P, Q]$ the class of (P, Q).

It is easy to see that the fixed point set is $\{(P, P) \mid P \in E[3]\}$, where $E[3]$ is the subgroup of all the 3-torsion points in E. It is not difficult to see that $\overline{S}_E$ has a quotient singularity of type A_2 at the image of each fixed point.

Proposition 3.1. *The set of rational points of $\overline{S}_E$ consists of points of the form:*

1. $[P, Q]$*, where* P*,* $Q \in E(k)$*;*
2. $[P, \sigma(P)]$*, where P is a point defined over a certain cyclic cubic extension L over k, satisfying the relation $P + \sigma(P) + \sigma^2(P) = O$, where σ is an element of its Galois group* $\mathrm{Gal}(L/k)$*.*

Proof. If $[P, Q]$ is not the image of a fixed point, the assertion follows from Lemma 2.1. If P is a 3-torsion point, $[P, P]$ is defined over k if and only if P is defined over k. So, this is included in the first case. □

Let S_E be the minimal desingularization of $\overline{S}_E$. We will see that S_E is a $K3$ surface, and thus S_E is an example of a generalized Kummer surface, the definition of which is as follows.

Definition 3.2. Let A be an abelian surface, and G a finite group of automorphisms of A. If A/G is birational to a $K3$ surface, then its minimal desingularization is called a generalized Kummer surface.

Our basic references to this subject are Bertin[1] and Katsura[5].

We would like to study the geometry of S_E in more detail. To this end, we fix a Weierstrass model of E and consider it as a curve in $\mathbf{P}^2$. Namely, suppose that E is given by the equation

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{1}$$

Then, as is well known, three points P, Q and R satisfy $P + Q + R = O$ if and only if P, Q and R are collinear. Let $(\mathbf{P}^2)^*$ be the dual space of $\mathbf{P}^2$, namely, the space of all the lines in $\mathbf{P}^2$. For points P and Q in $\mathbf{P}^2$ we denote by ℓ_{PQ} the line passing through P and Q. As usual, we understand that ℓ_{PP} is the tangent line passing through P. Consider the map

$$\begin{aligned} \lambda : E \times E &\longrightarrow (\mathbf{P}^2)^* \\ (P, Q) &\longmapsto \ell_{PQ}. \end{aligned}$$

If we set $R = -P-Q$, then $\ell_{PQ} = \ell_{RP} = \ell_{QR}$. This shows that λ is invariant under the $\mathit{\Gamma}$-action, and thus we obtain a map $\bar{\lambda} : \overline{S}_E \to (\mathbf{P}^2)^*$, which sends a class $[P, Q]$ of $\overline{S}_E$ to the line ℓ_{PQ}. It is easy to see that $\bar{\lambda}^{-1}(\ell_{PQ})$ consists of two classes, $[P, Q]$ and $[Q, P]$. In $\overline{S}_E$ the classes $[P, Q]$ and $[Q, P]$ coincide if and only if $P = Q$, $P = -2Q$ or $Q = -2P$. In other words $[P, Q] = [Q, P]$ if and only if ℓ_{PQ} is a tangent line to the curve E. This shows that $\overline{S}_E$ is a double cover or $(\mathbf{P}^2)^*$ ramifying along the dual curve $E^* = \{L \in (\mathbf{P}^2)^* \mid L \text{ is tangent to } E\ \}$. Choosing an isomorphism between $(\mathbf{P}^2)^*$ and $\mathbf{P}^2$, and we consider E^* as a plane curve. It is easy to see that E^* is an irreducible curve of degree 6, and it has 9 nodes corresponding to the tangent lines at 9 inflection points of E. Summing all up, we have

Proposition 3.3. *The quotient surface $\overline{S}_E = (E \times E)/\langle g \rangle$ may be regarded as a double cover of the projective plane $\mathbf{P}^2$ ramifying along an irreducible curve of degree 6. As a consequence $\overline{S}_E$ is birational to a $K3$ surface and its minimal desingularization S_E is a generalized Kummer surface.* □

4. A pencil of curves of genus 1 on S_E

Consider the map $\nu : E \to \overline{S}_E$ given by $P \mapsto [P, O]$. This is an injective map, and we have an embedding $\tilde{\nu} : E \to S$. Let $D_{\nu(E)}$ be the divisor associated with the image of ν. Then the complete linear system $|D_{\nu(E)}|$ determines a pencil of curves of genus 1, or equivalently, a fibration $\pi : S_E \to \mathbf{P}^1$. In what follows we write an explicit equation for the surface $\overline{S}_E$ and this elliptic pencil. To this end, we consider the function field $k(E)$ of E as the field generated by the functions x and y satisfying the relation

$$y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

Consider the function δ on $E \times E$ given by

$$\delta(P, Q) = \bigl(x(P) - x(Q)\bigr)\bigl(x(R) - x(P)\bigr)\bigl(x(Q) - x(R)\bigr),$$

where $R = -P - Q$. It is clear that δ is invariant under the $\mathit{\Gamma}$-action, and thus δ is in the function field of $\overline{S}_E$. Define functions t and u by

$$t(P, Q) = \frac{y(P) - y(Q)}{x(P) - x(Q)}, \qquad u(P, Q) = \frac{x(P)y(Q) - x(Q)y(P)}{x(P) - x(Q)}.$$

Since t signifies the slope of the line ℓ_{PQ} and u signifies its y-section, we see that these functions are invariant under the $\mathit{\Gamma}$-action. Clearly $k(t, u)$ can be considered as the function field of $(\mathbf{P}^2)^*$, as a line is determined by its slope and y-section.

Consider the cubic equation in x obtained by eliminating y from (2) and the equation of the line ℓ_{PQ}, i.e., $y = tx + u$. The function δ^2 is nothing but the discriminant $\Delta(u, t)$ of this cubic equation. We thus obtain the relation $\delta^2 = \Delta(u, t)$.

The surface in$\mathbb{A}^3 = \{(t, u, \delta)\}$ determined by $\delta^2 = \Delta(u, t)$ is a double cover of $(\mathbf{P}^2)^*$ ramifying along the curve $\Delta(u, t) = 0$. But the condition $\Delta(u, t) = 0$ is exactly the condition that the line ℓ_{PQ} is tangent to the elliptic curve E. Thus, $\Delta(u, t) = 0$ is an equation of the dual cure E^* in $\mathbf{P}^2 \simeq (\mathbf{P}^2)^*$, and $\delta^2 = \Delta(u, t)$ is an equation of the double cover of $\mathbf{P}^2$ ramifying along E^*. We thus obtain an affine equation of $\overline{S}_E$.

For simplicity we write the explicit result only in the case where $a_1 = a_2 = a_3 = 0$, $a_4 = A$, and $a_6 = B$.

Proposition 4.1. *Suppose that E is given by the equation $y^2 = x^3 + Ax + B$. Then the surface S_E is birational to the affine surface in $\mathbb{A}^3$ defined by the* *equation*

$$(3)\quad \delta^2 = -27u^4 - 4t^3u^3 - (30At^2 - 54B)u^2 - 4t(At^4 - 9t^2 - 6A^2)u \\ + 4Bt^6 + A^2t^4 - 18ABt^2 - (4A^3 + 27B^2).$$

□

Consider the map $\pi : \overline{S}_E \to \mathbf{P}^1$ associated with the projection $(t, u, \delta) \mapsto t$. The fiber at $t = \infty$ corresponds exactly the image of the embedding $P \to [P, O]$, and thus the fibration π coincides with the pencil of curves of genus 1 at the beginning of this section.

Remark 4.2. The surface S_E possesses two obvious involutions, $[P, Q] \mapsto [Q, P]$ and $[P, Q] \mapsto [-P, -Q]$. In terms of the equation (3) the former corresponds to $(t, u, \delta) \mapsto (t, u, -\delta)$, while the latter corresponds to $(t, u, \delta) \mapsto (-t, -u, \delta)$.

Let C_t be the fiber of π at the generic point t of $\mathbf{P}^1$. This is nothing but the curve of genus 1 defined over the function field $k(t)$ given by the equation (3).

The coefficient of u^4 in the right-hand side of (3) is constant, -27. Thus, the curve C_t has two points at infinity defined over $k(\sqrt{-3})$. In other words, if k contains $\sqrt{-3}$, C_t has a rational point and it is an elliptic curve over $k(t)$. However, if k does not contain $\sqrt{-3}$, we cannot consider C_t as an elliptic curve. Instead, we have to consider its Jacobian J_t.

Using an algorithm for calculating an equation of the Jacobian of the curve given by a quartic equation (see Connell[3]), we see that J_t is given by the equation

$$J_t \ : \ Y^2 = X^3 + \big(At^8 + 18Bt^6 - 18A^2t^4 - 54ABt^2 - 9(A^3 + 9B^2)\big)x \\ + \big(Bt^{12} - 4A^2t^{10} - 45ABt^8 - 270B^2t^6 + 135A^2Bt^4 \\ - 54A(2A^3 + 9B^2)t^2 - 243B(A^3 + 6B^2)\big).$$

Proposition 4.3. *The elliptic surface associated with the curve J_t has eight singular fibers of type* I_3 *located at t satisfying*

$$(4)\qquad t^8 + 18At^4 + 108Bt^2 - 27A^2 = 0.$$

The Mordell-Weil group $J_t(\bar{k}(t))$ contains an point of infinite order γ_1 given by

$$\gamma_1 = \Big(-\frac{1}{27}t^6 + 5At^2 - 9B, \frac{\sqrt{-3}}{243}t(t^8 + 162At^4 - 2916Bt^2 - 2187A^2)\Big).$$

If E does not have complex multiplication, then $J_t(\bar{k}(t))$ is isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},$$

and $J_t(\bar{k}(t))/J_t(\bar{k}(t))_{tors}$ is generated by γ_1. All the points in $J_t(\bar{k}(t))$ are defined already over $k(E[3])(t)$.

Proof. It is easy to determine the singular fibers using Tate's algorithm. Over $k(\sqrt{-3})$, C_t and J_t are isomorphic. Using an algorithm in [3], we can write an isomorphism which send one of the two points at infinity on C_t to the origin of J_t and the other to γ_1. Using an algorithm in [6], we calculate the height of γ_1, which turns out to be 3. This implies that it has infinite order.

In order to determine the Mordell-Weil group of J_t, we consider the quotient surface by the involution induced from the involution on C_t given by $(t, u, \delta) \mapsto (-u, -t, \delta)$. In terms of equation, the induced involution on J_t is given by $(t, X, Y) \mapsto (-t, X, Y)$. So, we set $T = t^2/3$, and consider the elliptic curve J_T defined over $k(T)$. Its Kodaira-Néron model is a rational elliptic surface with four I_3 fibers. The classification of rational elliptic surfaces due to Oguiso and Shioda[12] shows that there is only one such surface up to isomorphism over $\bar{k}$. It is known that the surface given by the Hasse cubic

$$H_\mu : x^3 + y^3 + z^3 = 3\mu xyz$$

is such a surface. As is well-known, it is the modular elliptic surface associated with the full modular group $\mathit{\Gamma}(3)$. The Mordell-Weil group $H_\mu(\bar{k}(t))$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and if we choose $(x : y : z) = (1 : -1 : 0)$ as the origin, then $H_\mu(\bar{k}(t))$ is generated by $(1 : 0 : -1)$ and $(1 : (-1+\sqrt{-3})/2 : 0)$.

The polynomial obtained from (4) by the substitution $T = t^2/3$ is nothing but the 3-division polynomial of E (see Silverman[Ch. III, p.105][15]). The singular fibers of H_μ are located at μ satisfying $\mu^3 = 1$ and $\mu = \infty$. We thus have a linear transformation $l : T \mapsto \mu = l(T)$ defined over $k(E[3])$ such that four roots of $3T^4 + 6AT^2 + 12BT - A^2 = 0$ are sent to the third roots of unity and the infinity, and we have an isomorphism between J_T and H_μ which extends the linear transformation l of the base. It is easy to see that this isomorphism is also defined over $k(E[3])$. Therefore, $J_T(k(E[3])(T))$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. This implies $J_t(k(E[3])(t))$ contains the subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Since all the singular fibers of J_t are of type I_3, any torsion point of $J_t(\bar{k}(t))$ must be 3-torsion. Thus, the torsion subgroup of $J_t(\bar{k}(t))$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and all of the torsion points are defined over $k(E[3])(t)$.

If E does not have a complex multiplication, then the Picard number of S_E, i.e., the rank of the Néron-Severi group of S_E, is 19. Using the Shioda-Tate formula ([14]), we conclude that the rank of $J_t(\bar{k}(t))$ is 1.

Suppose that γ_1 and the torsion subgroup do not generate $J_t(\bar{k}(t))$. Then there is a point γ_2 of infinite order such that $n\gamma_2 + \theta = \gamma_1$, where n is an integer greater than 1 and θ is a torsion point. This implies $n^2\hat{h}(\gamma_2) = \hat{h}(\gamma_1) = 3$, where $\hat{h}$ is the canonical height. A result in [6] shows that the lower bound for the canonical height of a nontorsion point on $J_t(\bar{k}(t))$is $1/3$. Thus, n must be 3. If $\hat{h}(\gamma_2) = 1/3$, then the formula for calculating $\hat{h}$ from the local heights implies that the section associated to γ_2 in the elliptic surface associated to the curve J_t must intersect with the nonidentity components of all the singular fibers. Since $\hat{h}(\gamma_2 + \theta) = 1/3$ for any 3-torsion point θ, and $\gamma_2 + \theta$ must satisfy the same condition as above. However, there is a singular fiber such that θ passes nonidentity component, and at such a singular fiber one of γ_2, $\gamma_2 + \theta$ and $\gamma_2 + 2\theta$ must intersect with the identity component, which is a contradiction. This concludes the proof. □

Remark 4.4. We note that J_T is isomorphic to one of the curves considered in Rubin-Silverberg[13, §4.1]. Namely, J_T is the family of all elliptic curves whose 3-torsion subgroups are isomorphic to $E[3]$ as Galois modules with symplectic structure.

5. Proof of Theorem 1.1

We begin by proving some lemmas that are necessary later in the proof.

Consider the surface defined by (3) together with the fibration $(t, u, \delta) \mapsto t$. Suppose we have infinitely many k-rational points $\gamma_n = (u_n, t_0, \delta_n)$ for a fixed t_0. For each n, the point γ_n corresponds to a class $[P_n, Q_n]$ in S_E. Let K_n be the field over which P_n and Q_n are defined. We already know that $K_n = k$ or K_n/k is a cyclic cubic extension of k.

Lemma 5.1. *Suppose that $t_0 \neq 0$, and that the fiber $\pi^{-1}(t_0)$ is a good fiber. Then the compositum of all K_n is an infinite extension of k.*

Proof. For each n the cubic polynomial $x^3 + Ax + B - (t_0x + u_n)^2$ in x factors into three linear terms over K_n. Conversely, finding a k-rational point (u, t_0, δ) on the surface (3) is finding u in k such that $x^3 + Ax + B - (tx + u)^2$ factors completely over some cubic cyclic field L. This is equivalent to finding a point (ξ_1, ξ_2, ξ_3, t) on the curve given by

$$\begin{cases} \xi_1 + \xi_2 + \xi_3 = t^2, \\ \xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1 = A - 2tu, \\ \xi_1\xi_2\xi_3 = u^2 - B. \end{cases}$$

By eliminating xi_3 and u, we obtain a plane curve of degree 4. A calculation shows that this degree 4 curve is nonsingular if and only if $t_0 \neq 0$ and $t^8 + 18At^4 + 108Bt^2 - 27A^2 \neq 0$. If that is the case, the genus of the curve is 3. Thus, by a theorem of Faltings, it has only finitely many K-rational points for each fixed number field K. Therefore, the compositum of all K_n cannot be a number field. □

In the case where k contains $\sqrt{-3}$, Lemma 5.1 and Proposition 4.3 proves the following statement, which is stronger than Theorem 1.1.

Theorem 5.2. *Let E be an elliptic curve defined over a number field k containing $\sqrt{-3}$. Then there exist infinitely many cyclic cubic extensions K_λ such that the Mordell-Weil group $E(K_\lambda)$ has positive rank.* □

We need another lemma for the general case.

Lemma 5.3. *Let S be a smooth surface and C a smooth curve both defined over k. Let $\pi : S \to C$ be a fibration defined over k such that the generic fiber is a curve of genus 1 with an involution ι with a fixed point. Suppose that the set of k-rational points, $S(k)$, is Zariski dense in S, then there exist infinitely many k-rational points P on C such that the fiber $\pi^{-1}(P)$ contains infinitely many k-rational points.*

Proof. Let $\pi' : J \to C$ be the Jacobian fibration associated with $\pi : S \to C$. There is a map $f : S \to J$ of degree 4 defined over k sending a point $P \in S$ to the divisor class $(P) - (\iota(P))$. Since f is dominant, the image of $S(k)$ by f is Zariski dense.

By Merel's theorem on the bound for the torsion points defined over a number field on an elliptic curve ([10]), the set consisting of all the k-rational torsion points of all the fibers is contained in a proper Zariski closed set. Thus if we denote by $f(S(k))'$ the set consisting of all the points in the image of $f(S(k))$ that have infinite order, then $f(S(k))'$ is still Zariski dense in J. This means that there are infinitely many k-rational points P on C such that the fiber ${\pi'}^{-1}(P)$ contains points in $f(S(k))'$. For such P the $\pi^{-1}(P)$ contains infinitely many k-rational points. □

Proof of Theorem 1.1. Let $P \in E(K_0)$ be a point of infinite order. First, we show that the set of k-rational points in S_E is Zariski dense in S_E.

If P is defined already over k, then consider the set $\{[mP, nP] \mid n, m \in \mathbb{Z}\}$. This is clearly a Zariski dense set in $E \times E$. We thus assume that P is not defined over k. Let σ be a generator of $\mathrm{Gal}(L/k)$. Then $R = P + \sigma(P) + \sigma^2(P)$ is a point defined over k. If R is a point of infinite order, then we are in the previous case. If not, replacing P by nP if necessary, we may assume that $P + \sigma(P) + \sigma^2(P) = O$. We consider $E(K_0)$ as an $\mathrm{End}_k(E)$-module, and we claim that P and $\sigma(P)$ are $\mathrm{End}_k(E)$-linearly independent, except when E has complex multiplication over $\mathbb{Q}(\sqrt{-3})$ and k contains $\sqrt{-3}$.

Suppose $[\alpha]$ and $[\beta]$ two nonzero endomorphsims of E defined over k, and suppose we have the relation

$$[\alpha]P + [\beta]\sigma(P) = O. \tag{5}$$

Apply σ to both sides of (5). Since σ commutes with $[\alpha]$ and $[\beta]$, we have another relation

$$[\alpha]\sigma(P) + [\beta](-P - \sigma(P)) = O. \tag{6}$$

Eliminating $\sigma(P)$ from (5) and (6), we obtain

$$\big([\alpha]^2 + [\alpha][\beta] + [\beta]^2\big)P = O.$$

This occurs only when E has complex multiplication by $\mathbb{Q}(\sqrt{-3})$. Moreover, since $[\alpha]$ is defined over k, $\sqrt{-3}$ must be contained in k. We thus verified the claim. The case where k contains $\sqrt{-3}$ has been treated already. In what follows we assume $\sqrt{-3} \notin k$.

Next we claim that the subgroup $\{(nP, n\sigma(P)) \mid n \in \mathbb{Z}\}$ is Zariski dense in $E \times E$. Let F be the Zariski closure of this subgroup. Suppose F does not equal S_E, then F is a closed subgroup of dimension 1 in $E \times E$. Let F^0 be the connected component of F containing the identity. We then have two isogenies ϕ_1 and ϕ_2 from F^0 to E, corresponding to two projections $E \times E \to E$. Choose $m \in \mathbb{Z}$ such that $(mP, m\sigma(P))$ is in F^0. Let $\hat{\phi}_1$ be the dual isogeny of ϕ_1. Consider the endomorphism $\phi_2\hat{\phi}_1$ of E. We have

$$\begin{aligned}\phi_2\hat{\phi}_1(mP) &= \phi_2\hat{\phi}_1\phi_1((mP, m\sigma(P))) \\ &= \phi_2((dmP, dm\sigma(P))) \qquad (d = \deg \phi_1) \\ &= dm\sigma(P).\end{aligned}$$

This contradicts the independence of P and $\sigma(P)$.

Since the projection map $E \times E \to \overline{S}_E$ is a dominant map, the set $\{[nP, n\sigma(P)] \mid n \in \mathbb{Z}\}$ is also Zariski dense in S_E. We thus proved that $S_E(k)$ is Zariski dense in all cases.

The fibration $\pi : \overline{S}_E \to \mathbf{P}^1$ constructed in §4 satisfies the hypotheses of Lemma 5.3. Thus, there exist infinitely many $t \in \mathbf{P}^1$ such that the fiber $\pi^{-1}(t)$ has infinitely many k-rational points. In particular, we have at least one such t such that $t \neq 0$ and $\pi^{-1}(t)$ is a good fiber. Then Lemma 5.1 implies that there exist infinitely many different cyclic cubic extension K_λ such that the elliptic curve E possesses a point P_λ defined over K_λ.

In order to complete the proof we have to show that P_λ has infinite order except for finite number of λ. But this is true because the bound of the order of torsion points given by Merel's theorem depends only on the degree of the field. □

6. Topology of rational points on S_E

In this section we suppose that the base field k is embedded in the field of real numbers. Using a result of Waldschmidt[16], we have

Lemma 6.1. *If the hypothesis of Theorem 1.3 holds, the closure with respect to the ordinary topology of the set of K_0-rational points is open in $(E \times E)(\mathbb{R})^0$, the identity component of the set of $\mathbb{R}$-rational points in $E \times E$.*

Proof. Suppose that P is a k-rational point of infinite order in $E(k)^0$. Then the set $R_1 = \{(nP, mP) \mid n, m \in \mathbb{Z}\}$ is clearly dense in $(E \times E)(\mathbb{R})^0$. Otherwise, the proof of Theorem 1.1 shows that $E \times E$ has a point $(P, \sigma(P))$ of infinite order. Note that K_0 being a cyclic cubic extension of a real field k, it is also a real field. Therefore, $(2P, 2\sigma(P))$ is always in $(E \times E)(k)^0$. By a result of Waldschmidt[16, Chapter IV, Proposition 1.2], we see that the set $R_2 = \{(2nP, 2m\sigma(P)) \mid n \in \mathbb{Z}\}$ is dense in $(E \times E)(\mathbb{R})^0$.

If E has a K_0-rational point Q in the nonidentity component of $E(\mathbb{R})$, then $(O, Q) + R_i$, $(O, Q) + R_i$ and $(Q, Q) + R_i$, $i = 1, 2$, are dense in the three nonidentity components of $(E \times E)(k)$. This concludes the proof. □

Proof of Theorem 1.3. Since the degree of the projection map $E \times E \to \overline{S}_E$ is odd, the inverse image of $\overline{S}_E(\mathbb{R})$ is nothing but the set $(E \times E)(\mathbb{R})$. More precisely, if $E(\mathbb{R})$ has two connected components, then $\overline{S}_E(\mathbb{R})$ has two connected components, and the inverse image of the component containing $[O, O]$ is the identity component $(E\times E)(k)^0$. The inverse image of the other component is the union of thee nonidentity components of $(E \times E)(k)$. If $E(\mathbb{R})$ has only one connected component, then both $(E\times E)(k)$ and $\overline{S}_E(\mathbb{R})$. It thus suffices to show that the $(E \times E)(k)$ is open in $E \times E$, but this has been done in Lemma 6.1. □

7. Examples

In this section the base field k is the field of rational numbers $\mathbb{Q}$. Let us consider the universal elliptic curve having a point of order 6. It is given by the equation

$$y^2 + (1-s)xy + s(s+1)y = x^3 - s(s+1)x^2.$$

When $s \neq 0$, -1 or $-1/9$, this is an elliptic curve and the point $P = (0,0)$ is a point of order 6. The line passing through P, $2P$ and $3P$ is given by $y = sx$. Consider the curve in $\mathbb{A}^2 = \{(u,\delta)\}$ with two parameters s and t given by

$$\delta^2 = \operatorname{disc}\bigl((tx+u)^2 + (1-s)x(tx+u)s(s+1)y - x^3 + s(s+1)x^2\bigr),$$

where $\operatorname{disc}(f)$ stands for the discriminant of f with respect to x. When $t = s$, it has two points $(u,\delta) = (0, \pm s^4(s+1))$. Choosing one of them, say $(0, -s^4(s+1))$, as the origin, we can convert the equation into Weierstrass form:

$$\begin{aligned}(7)\quad y^2 + (8s + 2s^2 + 2)xy - 4s(7s+1)(s-2)(s+1)^2y \\ = x^3 - 2s(s+1)(2s^2-4-s)x^2 + 108s^4(s+1)^2x \\ - 216s^5(2s^2-4-s)(s+1)^3.\end{aligned}$$

This is an elliptic curve if and only if

$$s(1+9s)(2s+1)(s+1)(s^4+3s^3+4s^2+1) \neq 0.$$

The point $(0, s^4(s+1))$ is sent to the point $\gamma_1 = \bigl(2s(s+1)(2s^2-4-s), 0\bigr)$.

Lemma 7.1. *For all $s \in \mathbb{Q}$ such that* (7) *is an elliptic curve, the point $\bigl(2s(s+1)(2s^2-4-s), 0\bigr)$ is a point of infinite order. When $s = -1/2$, then* (7) *is not an elliptic curve, but* $(3/2, 0)$ *is still a point of infinite order.*

Proof. We consider (7) as the curve defined over $\mathbb{Q}(s)$, and calculate $n\gamma_1$, $n = 1, 2, ..10, 12$. For all those n we observe that the denominator of the x-coordinate of $n\gamma_1$ does not vanish for any value of s except for $s = 0$. For $s = -1/2$ the group is isomorphic to $\mathbb{Q}^*$. Thus, it suffices to see that it is not a 2-torsion point. □

Theorem 7.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational 6-torsion point. Then there exist infinitely many cyclic cubic extensions K_λ such that the Mordell-Weil group $E(K_\lambda)$ has positive rank.* □

Remark 7.3. We may replace a 6-torsion point by a n-torsion point $n = 7, 8, 9, 10, 12$. However, the point (u, δ) obtained from a 5-torsion point becomes a 2-torsion point.

References

1. J. Bertin, *Reseaux de Kummer et surfaces de $K3$*, Invent. Math. **93** (1988), 267–284.
2. J.-L. Colliot-Télène, H. P. F. Swinnerton-Dyer, and A. N. Skorobogatov, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), 113–135.
3. I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra **145** (1992), 463–467.
4. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
5. T. Katsura, *Generalized Kummer surfaces and their unirationality in characteristic p*, J. Fac. Sci., Univ. Tokyo, Sect. I A **34** (1987), 1–41.
6. M. Kuwata, *Canonical height and elliptic K3 surfaces*, J. Number Theory **36** (1990), 399–406.
7. M. Kuwata and L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Duke Intl. Math. Res. Notices (1993), 113–123.
8. B. Mazur, *The topology of rational points*, Experimental Mathematics **1** (1992), 35–45.
9. ______, *Speculations about the topology of rational points: an update*, Columbia University Number Theory Seminar, New York 1992, Astérisque, vol. 128, 1995, pp. 165–181.
10. L. Mérel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math **124** (1996), 437–449.
11. D. Mumford, *Abelian varieties*, Oxford University Press, 1970.
12. K. Oguiso and T. Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, Comment. Math. Univ. Sancti Pauli **40** (1991), 83–99.
13. K. Rubin and A. Silverberg, *Famillies of elliptic curves with constant mod p representations*, Conference on Elliptic Curves and Modular Forms, Hong Kong, December 18–21, 1993, Intl. Press, 1995, pp. 148–161.
14. T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.
15. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, New York, 1986.
16. M. Waldschmidt, *Topologie des points rationnels*, Lecture notes of the graduate couse given in 1994/95, Université de P. et M. Curie (Paris VI), 1995.

Département de Mathématiques, Université de Caen, B.P. 5186, F-14032 Caen Cedex, France

E-mail address: kuwata@math.unicaen.fr