Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sajad SALAMI et Arman SHAMSI ZARGAR

Generators and splitting fields of certain elliptic $K3$ surfaces

Tome 38, nº 2 (2026), p. 317-339.

https://doi.org/10.5802/jtnb.1363

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **38** (2026), 317–339

Generators and splitting fields of certain elliptic $K3$ surfaces

par Sajad SALAMI et Arman SHAMSI ZARGAR

Résumé. Soit $k \subset \mathbb{C}$ un corps de nombres et $\mathcal{E}$ une courbe elliptique définie sur $k(t)$ qui est isomorphe à la fibre générique d'une surface elliptique $\pi : \mathcal{S}_{\mathcal{E}} \to \mathbb{P}^1_k$. Pour tout sous-corps $\mathcal{K} \subseteq \mathbb{C}$ de k, l'ensemble $\mathcal{E}(\mathcal{K}(t))$ des points rationnels de $\mathcal{E}$ est un groupe abélien de type fini. Le corps de décomposition de $\mathcal{E}$ défini sur $k(t)$ est la plus petite extension finie $\mathcal{K} \subset \mathbb{C}$ de k telle que $\mathcal{E}(\mathbb{C}(t)) \cong \mathcal{E}(\mathcal{K}(t))$. Dans cet article, nous considérons les surfaces elliptiques $K3$ définies sur $k = \mathbb{Q}$ de fibre générique donnée par l'équation de Weierstrass $\mathcal{E}_n : y^2 = x^3 + t^n + 1/t^n$, $1 \leq n \leq 6$, déterminons le corps de décomposition $\mathcal{K}_n$ et trouvons un ensemble explicite de générateurs linéairement indépendants pour $\mathcal{E}_n(\mathcal{K}_\backslash(t))$ pour $1 \leq n \leq 6$.

Abstract. Let $k \subset \mathbb{C}$ be a number field and $\mathcal{E}$ be an elliptic curve defined over $k(t)$ that is isomorphic to the generic fiber of an elliptic surface $\pi : \mathcal{S}_{\mathcal{E}} \to \mathbb{P}^1_k$. For any extension $\mathcal{K} \subseteq \mathbb{C}$ of k, the set $\mathcal{E}(\mathcal{K}(t))$ of $\mathcal{K}(t)$-rational points of $\mathcal{E}$ is known to be a finitely generated abelian group. The splitting field of $\mathcal{E}$ defined over $k(t)$ is the smallest finite extension $\mathcal{K} \subset \mathbb{C}$ of k such that $\mathcal{E}(\mathbb{C}(t)) \cong \mathcal{E}(\mathcal{K}(t))$. In this paper, we consider the elliptic $K3$ surfaces defined over $k = \mathbb{Q}$ with the generic fiber given by the Weierstrass equation $\mathcal{E}_n : y^2 = x^3 + t^n + 1/t^n$, $1 \leq n \leq 6$, and determine the splitting field $\mathcal{K}_n$, and find an explicit set of linearly independent generators for $\mathcal{E}_n(\mathcal{K}_\backslash(t))$ for $1 \leq n \leq 6$.

1. Introduction and main results

Let k be a number field and $\mathcal{E}$ be an elliptic curve defined over $k(t)$, the rational function field of the projective line $\mathbb{P}^1_k$ over k, that is isomorphic to the generic fiber of an elliptic surface $\pi : \mathcal{S}_{\mathcal{E}} \to \mathbb{P}^1_k$. Given any subfield $\mathcal{K} \subseteq \mathbb{C}(t)$, the set $\mathcal{E}(\mathcal{K})$ of $\mathcal{K}$-rational points of $\mathcal{E}$ is known to be a finitely generated abelian group that has a lattice structure called the Mordell–Weil lattice [7, 8, 13].

By the splitting field of $\mathcal{E}$ over $k(t)$, we mean the smallest finite extension $\mathcal{K} \subset \mathbb{C}$ of k, such that $\mathcal{E}(\mathbb{C}(t)) \cong \mathcal{E}(\mathcal{K}(t))$. It is a well-known fact that $\mathcal{K}|k$

Manuscrit reçu le 28 octobre 2023, révisé le 7 décembre 2025, accepté le 3 mars 2026.
2020 *Mathematics Subject Classification.* 14J27, 11G05.
Mots-clefs. Elliptic surface, Mordell–Weil lattice, Splitting field.

is a Galois extension with the finite Galois group $G = \mathrm{Gal}(\mathcal{K}|k)$. Moreover, the G-invariant elements of $\mathcal{E}(\mathcal{K}(t))$ are the $\mathcal{E}(k(t))$-rational points [7].

In this paper, we consider $k = \mathbb{Q}$ and the elliptic $K3$ surfaces over $\mathbb{Q}(t)$ with a generic fiber given by the following equation

$$\mathcal{E}_n : y^2 = x^3 + t^n + \frac{1}{t^n}, \text{ for } 1 \le n \le 6.$$

The structure of Mordell–Weil lattice of $\mathcal{E}_n$ over $\mathbb{C}(t)$ is studied by T. Shioda in [10, 12] and by A. Kumar and M. Kuwata in [1] with a more general setting, for all $1 \le n \le 6$. We notice that $\mathcal{E}_n$ is a special member, considering $\alpha = \beta = 0$, of the generic fiber of a more general family $K3$ surface defined by

$$y^2 = x^3 - 3\alpha x + \left(t^n + \frac{1}{t^n} - 2\beta\right).$$

In particular, the invariants of the Mordell–Weil lattices of $\mathcal{E}_n$ are determined by T. Shioda in [12, Theorem 2.4], and a generic form of their generators is described in [12, Theorem 2.6]. For the convenience of readers, we compiled those results as Theorem 2.1 in Section 2.

The main aims of this paper are to determine the splitting field $\mathcal{K}_n \subset \mathbb{C}$ of $\mathcal{E}_n$ and provide an explicit set of linearly independent generators of $\mathcal{E}_n(\mathcal{K}_n(t))$ for each $1 \le n \le 6$. Let r_n be the rank of $\mathcal{E}_n(\mathbb{C}(t))$, and ζ_m be a fixed m-th root of unity. In Table 1.1, we listed all m-th roots of unity and algebraic quantities that we used throughout the paper.

Table 1.1. Notation

$\mathrm{i} = \sqrt{-1}$	$\epsilon_1 = 2 + \sqrt{3}$	$\epsilon_1' = 2 - \sqrt{3}$
$\zeta_3 = \dfrac{\sqrt{3}\mathrm{i} - 1}{2}$	$\epsilon_2 = 11\sqrt{2} + 9\sqrt{3}$	$\epsilon_2' = -11\sqrt{2} + 9\sqrt{3}$
$\zeta_5 = \dfrac{\sqrt{5} - 1 + \sqrt{2}\sqrt{5+\sqrt{5}}\mathrm{i}}{4}$	$\epsilon_3 = \sqrt{2} + 5\mathrm{i}$	$\epsilon_3' = \sqrt{2} - 5\mathrm{i}$
$\zeta_6 = \dfrac{1 + \sqrt{3}\mathrm{i}}{2}$	$\epsilon_4 = 1 - \zeta_{12}$	$\beta_0 = 2^{\frac{1}{6}}$
$\zeta_8 = \dfrac{\sqrt{2}(1+\mathrm{i})}{2}$	$\epsilon_5 = \dfrac{\sqrt{3} - \sqrt{5}}{2}(\zeta_{12} + \zeta_{12}^{10})$	$\beta_1 = \left(3 + 2\sqrt{3}\right)^{\frac{1}{4}}$
$\zeta_{12} = \dfrac{\sqrt{3} + \mathrm{i}}{2}$	$\epsilon_6 = \dfrac{1 + \sqrt{5}}{2}\zeta_{12}$	$\beta_2 = \left(3 - 2\sqrt{3}\right)^{\frac{1}{4}}$

The Mordell–Weil lattice $\mathcal{E}_1(\mathbb{C}(t))$ is of rank $r_1 = 0$, as demonstrated in [11, Theorem 1.1]. In the rest of this section, we provide a list of our main results for each of the cases $2 \le n \le 6$.

Theorem 1.1. *The Mordell–Weil lattice $\mathcal{E}_2(\mathbb{C}(t))$ is isomorphic to $\mathcal{E}_2(\mathcal{K}_2(t))$ with (rank) $r_2 = 4$, where $\mathcal{K}_2 = \mathbb{Q}(\zeta_3, 2^{1/3})$ is a number field of degree 6* *with the defining minimal polynomial* $g_2(x) = x^6 + 108$. *Moreover, a set of linearly independent generators of* $\mathcal{E}_2(\mathcal{K}_2(t))$ *consists of the four points*

$$P_1 = \left(2^{\frac{1}{3}}, t + \frac{1}{t}\right), \qquad P_2 = \left(2^{\frac{1}{3}}\zeta_3, t + \frac{1}{t}\right),$$
$$P_3 = \left(-2^{\frac{1}{3}}, t - \frac{1}{t}\right), \quad P_4 = \left(-2^{\frac{1}{3}}\zeta_3^2, t - \frac{1}{t}\right).$$

Theorem 1.2. *The Mordell–Weil lattice* $\mathcal{E}_3(\mathbb{C}(t))$ *is isomorphic to* $\mathcal{E}_3(\mathcal{K}_3(t))$ *with* $r_3 = 8$, *where* $\mathcal{K}_3 = \mathbb{Q}(\zeta_3, (3+3\sqrt{3})^{1/4})$ *is a number field of degree* 16 *with the defining minimal polynomial* $g_3(x)$ *given by* (4.2). *Moreover, a set of eight linearly independent generators of* $\mathcal{E}_3(\mathcal{K}_3(t))$ *consists of the points*

$$P_j = (x_j(t), y_j(t)) = \left(\frac{a_j t^2 + b_j t + a_j}{t}, \ \frac{c_j t^2 + d_j t + c_j}{t}\right)$$

and $P_{j+4} = \zeta_3 \cdot P_j = (x_j(\zeta_3 t), y_j(\zeta_3 t))$ *for* $j = 1, 2, 3, 4$, *where* a_j, b_j, c_j *and* d_j *are given in Subsection 4.2.*

For $n = 4, 6$, we consider the automorphism of $\mathcal{E}_n(\mathbb{C}(t))$ given by

$$\phi_n : (x(t), y(t)) \longrightarrow (-x(\zeta_{2n}t), y(\zeta_{2n}t)\mathrm{i}).$$

Theorem 1.3. *The Mordell–Weil lattice* $\mathcal{E}_4(\mathbb{C}(t))$ *is isomorphic to* $\mathcal{E}_4(\mathcal{K}_4(t))$ *with* $r_4 = 12$, *where* $\mathcal{K}_4$ *is a number field of degree* 24 *with the defining minimal polynomial* $g_4(x)$ *given by* (5.2). *Moreover, a set of twelve linearly independent generators of* $\mathcal{E}_4(\mathcal{K}_4(t))$ *contains the points*

$$P_j = (x_j(t), y_j(t)) = \left(\frac{a_j t^2 + b_j t + a_j}{t}, \frac{t^4 + c_j t^3 + (d_j + 2)t^2 + c_j t + 1}{t^2}\right),$$

and $P_{j+6} = \phi_4(P_j) = (-x_j(\zeta_8 t), \mathrm{i}y_j(\zeta_8 t))$ *for* $j = 1, \ldots, 6$, *where* a_j, b_j, c_j *and* d_j *are given in Subsection 5.1.*

Theorem 1.4. *The Mordell–Weil lattice* $\mathcal{E}_5(\mathbb{C}(t))$ *is isomorphic to* $\mathcal{E}_5(\mathcal{K}_5(t))$ *with* $r_5 = 16$, *where* $\mathcal{K}_5$ *is a number field of degree 192 with the defining minimal polynomial given in* [4, min-pols]. *Moreover, a set of sixteen linearly independent generators of* $\mathcal{E}_5(\mathcal{K}_5(t))$ *consists of the points* $P_j = (x_j(t), y_j(t))$ *with*

$$x_j(t) = \frac{t^4 + a_j t^3 + (b_j + 2)t^2 + a_j t + 1}{u_j^2 t^2},$$
$$y_j(t) = \frac{t^6 + c_j t^5 + (d_j + 3)t^4 + (2c_j + e_j)t^3 + (d_j + 3)t^2 + c_j t + 1}{u_j^3 t^3},$$

and $P_{j+8} = (x_j(\zeta_5 t), y_j(\zeta_5 t))$ *for* $j = 1, \ldots, 8$, *where* a_j, b_j, c_j, d_j, e_j *and* u_j*'s are given in* [4, Points-5].

We would like to mention that the points given by Theorem 1.4 provide sixteen linearly independent generators of the Mordell–Weil lattice of the Shioda's rank 68 elliptic surface, as described in [5, Theorem 1.1 (11)].

Theorem 1.5. *The Mordell–Weil lattice $\mathcal{E}_6(\mathbb{C}(t)) \cong \mathcal{E}_6(\mathcal{K}_6(t))$ has rank $r_6 = 16$, where $\mathcal{K}_6$ is a number field of degree 96 with the defining minimal polynomial $g_6(x)$ given in* [4, min-pols]*. Moreover, a set of sixteen linearly independent generators consists of $P_j = (x_j(t), y_j(t))$ with*

$$x_j(t) = \frac{a_{j,0}t^4 + a_{j,1}t^3 + a_{j,2}t^2 + a_{j,1}t + a_{j,0}}{t^2},$$
$$y_j(t) = \frac{b_{j,0}t^6 + b_{j,1}t^5 + b_{j,2}t^4 + b_{j,3}t^3 + b_{j,2}t^2 + b_{j,1}t + b_{j,0}}{t^3},$$

in which, for $j = 1, \ldots, 8$, we have $a_{j,0} = a_j$, $b_{j,0} = c_j$, and

$$a_{j,1} = b_j - 2\sqrt{2}a_j, \qquad a_{j,2} = g_j + 4a_j - \sqrt{2}b_j,$$
$$b_{j,1} = c_j + d_j - 3\sqrt{2}, \qquad b_{j,2} = d_j + 9c_j + e_j - 2\sqrt{2},$$
$$b_{j,3} = h_j - 8\sqrt{2}c_j - \sqrt{2}e_j + 4d_j,$$

and the points $P_{j+8} = \phi_6(P_j)$, where the coefficients $a_j, b_j, c_j, d_j, e_j, g_j$ and h_j are given in [4, Points-6]*.*

In [6], we explicitly determined the generators and splitting fields of the Shioda's elliptic surface given by $y^2 = x^3 + t^m + 1$ for integers $2 \leq m \leq 12$ defined over $\mathbb{Q}(t)$. Furthermore, in [5], the first-named author did a similar study for the particular case $m = 360$ which is known to have rank 68 over $\mathbb{C}(t)$.

The rest of paper is organized as follows. Prior to proving the main results, we provide the preliminary facts on the Mordell–Weil lattice of $\mathcal{E}_n$ in the next section. Then, in Section 3, we provide a general algorithmic approach for proofs of our results. We prove Theorems 1.1 and 1.2 in Section 4. In the last three sections, we respectively demonstrate proofs of Theorems 1.3, 1.4 and 1.5.

In our computations, we used the mathematical softwares Maple [2], and PARI/GP [3].

2. Shioda's results on Mordell–Weil lattice of $\mathcal{E}_n$

In this section, we recall some of the known results by T. Shioda on the elliptic $K3$ surfaces $\mathcal{E}_n$ defined over $\mathbb{Q}(t)$ from [12].

For a given lattice $(L, \langle\, , \rangle)$ and an integer $m \geq 2$, we let $L[m]$ be a lattice with the height pairing $m \cdot \langle\, , \rangle$. We denote by M_n the Mordell–Weil lattice $\mathcal{E}_n(\mathbb{C}(t))$, which does not have torsion part, see [12, Lemma 5.2]. It is clear that $\mathcal{E}_n$ is obtained from $\mathcal{E}_1$ by the base change $t \to t^n$. Hence, we let $N_n = M_1[n]$ for each $2 \leq n \leq 6$.

In order to study the lattice M_n, as in [12], we will consider the Mordell–Weil lattice $M'_n = \mathcal{E}'_n(\mathbb{C}(s))$ of the rational elliptic surface $\mathcal{E}'_n : y^2 = x^3 + f_n(s)$, where $f_n(s)$ is a polynomial defined as follows:

$$f_n(s) = \begin{cases} s^2 - 2 & n = 2, \\ s^3 - 3s & n = 3, \\ s^4 - 4s^2 + 2 & n = 4, \\ s^5 - 5s^3 + 5s & n = 5, \\ s^6 - 6s^4 + 9s^2 - 2 & n = 6. \end{cases}$$

We denote by $\mathcal{K}'_n$ the splitting field of $\mathcal{E}'_n$ over $\mathbb{Q}(s)$ for $1 \le n \le 6$, which is determined in the next sections. The Mordell–Weil rank of M'_n is $2, 4, 6, 8, 8$ and we have $M'_n \cong \{0\}, A_2^*, D_4^*, E_6^*, E_8, E_8$, respectively. Here, A_2^* indicates the dual lattice of the root lattice A_2, etc.

The following theorem is the main result of T. Shioda on the invariants and generators of the Mordell–Weil lattice of $\mathcal{E}_n$.

Theorem 2.1. *With the above notations, the invariants of $M_n = \mathcal{E}_n(\mathbb{C}(t))$ are given in Table 2.1, where μ_n denotes the length of minimal sections.*

Table 2.1. Invariants of the lattices M_n

n	1	2	3	4	5	6
r_n	0	4	8	12	16	16
$\det(M_n)$	1	$2^4/3^2$	$3^4/4^2$	$4^4/3^2$	5^4	6^4
μ_n	-	$4/3$	2	$8/3$	4	4

Moreover, the lattice M_n is generated by the points $P = (x(t), y(t))$ with the coordinates

$$x(t) = \frac{a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4}{t^2},$$
$$y(t) = \frac{b_0 + b_1 t + b_2 t^2 + b_3 t^3 + b_4 t^4 + b_5 t^5 + b_6 t^6}{t^3},$$

$a_i, b_j \in \mathbb{C}$. More precisely, for $n = 2$, a set of linearly independent generators of M_2 is given by $(\alpha, t + 1/t)$ and $(\alpha', t - 1/t)$, where α and α' run over the roots of the cubic polynomials $u^3 - 2$ and $u^3 + 2$, respectively. For $n > 2$, the lattice M_n is generated by the following set of points:

(i) *in the cases $n = 3, 5$:*

$$\left(x'\left(t + \frac{1}{t}\right), y'\left(t + \frac{1}{t}\right)\right) \text{ and } \left(x'\left(\zeta_n t + \frac{1}{\zeta_n t}\right), y'\left(\zeta_n t + \frac{1}{\zeta_n t}\right)\right),$$

(ii) *in the cases* $n = 4, 6$*:*

$$\left(x'\left(t+\frac{1}{t}\right), y'\left(t+\frac{1}{t}\right)\right)$$

and

$$\left(-x'\left(\zeta_{2n}t+\frac{1}{\zeta_{2n}t}\right), y'\left(\zeta_{2n}t+\frac{1}{\zeta_{2n}t}\right)\mathrm{i}\right),$$

where $\big(x'(s), y'(s)\big)$ *belongs to a generating set of* M_n' *with the coordinates*

$$x'(s) = a_0 + a_1 s + a_2 s^2 \text{ and } y'(s) = b_0 + b_1 s + b_2 s^2 + b_3 s^3,$$

$a_i, b_j \in \mathbb{C}$*.*

In [12, Theorem 2.5], T. Shioda proved the above theorem, but he did not determine exactly the coefficients or splitting fields $\mathcal{K}_n$, which is our main task in this paper. We refer the reader to see the proofs of Theorems 2.4 and 2.6 in [12]. Here, we just provide a sketch of the main idea of the proofs.

Letting $T = t^n$, $w = T + 1/T$, and $L_n = M_n'[2]$ for $1 \leq n \leq 6$, and considering the elliptic surface $\mathcal{E}_0 : y^2 = x^3 + w$ over $\mathbb{C}(w)$, we have $\mathcal{E}_0 \cong \mathcal{E}_1$, hence $M_n = \mathcal{E}_0(\mathbb{C}(t))$, $L_n = \mathcal{E}_0(\mathbb{C}(s))$, and $N_n = \mathcal{E}_0(\mathbb{C}(T))$. We note that $\mathbb{C}(t)$ is a Galois extension of $\mathbb{C}(w)$ with the Galois group $G = \langle \tau_0, \tau_n \rangle$ with $\tau_0 : t \to 1/t$ and $\tau_n : t \to \zeta_n t$, where ζ_n is an n-th root of unity. In the terminology of Galois Theory, the fields $\mathbb{C}(s)$ and $\mathbb{C}(T)$ correspond to the subgroups $\langle \tau_0 \rangle$ and $\langle \tau_n \rangle$, and the invariant sublattices of M_n are L_n and N_n, respectively.

By [12, Lemmata 7.2 and 7.3], we have $L_n \cap N_n = \{0\}$, and $L_n \oplus N_n$ is an orthogonal direct sum of lattices. Moreover, if we let $\widetilde{L}_n = \tau_n(L_n) \subseteq M_n$, then $\widetilde{L}_n = \mathcal{E}_0(\mathbb{C}(s'))$ with $s' = \tau_n(s) = \zeta_n t + 1/\zeta_n t$ such that $L_n \cap \widetilde{L}_n = \{0\}$ for odd n and $L_n \cap \widetilde{L}_n \cong M_2'$ otherwise. In [12, Lemma 7.4], it is proved that $M_n = L_n + \widetilde{L}_n$ for $n = 3, 5$ and $\det(M_n)$ is equal to $3^4/4^2$ for $n = 3$, and 5^4 for $n = 5$. In the cases $n = 4, 6$, denoting the fourth root of unity by i, redefining $\widetilde{L}_n$ as the image of L_n by the following automorphism

$$\phi_n : (x(t), y(t)) \longrightarrow (-x(\zeta_{2n}t), y(\zeta_{2n}t)\mathrm{i}),$$

of M_n, and using [12, Lemma 7.5], we have $L_n \cap \widetilde{L}_n = \{0\}$ and the lattice $L_n + \widetilde{L}_n$ has determinant $4^4/3^2$ for $n = 4$ and 6^4 for $n = 6$. Therefore, one may conclude that $N_n \oplus L_n \oplus \widetilde{L}_n$ is a sublattice of finite index in M_n for $n = 4, 6$.

3. An algorithmic approach to proofs of our main theorems

In this section, we provide an algorithmic approach for proofs of the main results of the paper. Indeed, we make use of the Shioda's results presented in Theorem 2.1 to determine the splitting field $\mathcal{K}_n$ of $\mathcal{E}_n$ and a set of linearly independent generators of $\mathcal{E}_n(\mathcal{K}_n)$.

Algorithm 1 Computation of the splitting field and generators of $\mathcal{E}_n(\mathcal{K}_n)$

Require: The defining equation of $\mathcal{E}_n$ over $\mathbb{Q}(t)$ of rank r_n over $\mathbb{C}(t)$.
Ensure: Splitting field $\mathcal{K}_n \subset \mathbb{C}$ of $\mathcal{E}_n$ and a set of linearly independent generators for $\mathcal{E}_n(\mathcal{K}_n)$.

1: *Determine the splitting field $\mathcal{K}'_n$ and generators of the rational elliptic surface $\mathcal{E}'_n$*
   (i) Define $\mathcal{E}'_n : y^2 = x^3 + f_n(s)$ over $\mathbb{Q}(s)$ of rank r'_n over $\mathbb{C}(s)$.
   (ii) Take $(x'(s), y'(s)) = (a_0 + a_1 s + a_2 s^2, b_0 + b_1 s + b_2 s^2 + b_3 s^3)$.
   (iii) Substitute in $\mathcal{E}'_n$ to generate a set of equations in a_i and b_j defining an ideal in $\mathbb{Q}[a_0, \ldots, b_3]$.
   (iv) Find the fundamental polynomial of the ideal using the `UnivariatePolynomial` command in the `PolynomialIdeals` package of Maple.
   (v) Use PARI/GP to find the minimal polynomial $g'_n(x)$ of $\mathcal{K}'_n$.
   (vi) Using the determinant conditions, select appropriate roots to obtain linearly independent generators of the Mordell–Weil lattice $\mathcal{E}'_n(\mathcal{K}'_n)$.

2: *Determine $\mathcal{K}_n$ and generators of $\mathcal{E}_n(\mathcal{K}_n)$*
   (i) Use PARI/GP to find the minimal polynomial $g_n(x)$ of $\mathcal{K}_n = \mathcal{K}'_n(\zeta_m)$.
   (ii) Set $m = n$ for $n = 3, 5$ and $m = 2n$ for $n = 4, 6$.
   (iii) Transform $(x'(s), y'(s)) \in \mathcal{E}'_n(\mathcal{K}'_n)$ to the points in $\mathcal{E}_n(\mathcal{K}_n)$ using the transformations in Theorem 2.1.

4. The cases $\mathcal{E}_2$ and $\mathcal{E}_3$

We consider the Mordell–Weil lattices of the cases $\mathcal{E}_2$ and $\mathcal{E}_3$ in this section.

4.1. Proof of Theorem 1.1. The structure of Mordell–Weil lattice of $\mathcal{E}_2$ over $\mathbb{C}(t)$ is treated in [11, Theorem 6.1] and [12, Theorem 7.1].

In the case of $\mathcal{E}_2$, by Theorem 2.1, a set of linearly independent generators can be found of the form $(a, bt + c + d/t)$. Substituting these points in the equation of $\mathcal{E}_2$ leads to $c = 0$, $b, d \in \{\pm 1\}$. If b and d have the same sign, then $a^3 - 2 = 0$ and otherwise $a^3 + 2 = 0$. Hence, there are totally six points and one can check that the Gram matrix of the points P_1, P_2, P_3, P_4 given in the statement of Theorem 1.1 is

$$R_2 = \frac{2}{3}\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix},$$

which has determinant $2^4/3^2$ as desired (cf. Table 2.1). The splitting field $\mathcal{K}_2$ is equal to an extension of $\mathbb{Q}$ which includes the roots of $a^3-2=0$ and otherwise $a^3+2=0$, say $\mathcal{K}_2=\mathbb{Q}(\zeta_3, 2^{1/3})$ with the defining minimal polynomial $g_2(x)=x^6+108$.

4.2. Proof of Theorem 1.2. We consider the rational elliptic surface $\mathcal{E}'_3 : y^2 = x^3 - (s^3 - 3s)$. According to the Shioda's results given in Section 2, the rank of $\mathcal{E}'_3(\mathbb{C}(s))$ is equal to 4 and $\mathcal{E}'_3(\mathbb{C}(s)) \cong D_4^*$. To find a set of linearly independent generators, we consider the points $Q=(as+b, cs+d)$ and substitute the coordinates in the equation of $\mathcal{E}'_3 : y^2 = x^3 - (s^3-3s)$. It follows that

$$a^3+1=0, \quad c^2-3a^2b=0, \quad -3ab^2+2cd+3=0, \quad d^2-b^3=0. \tag{4.1}$$

Form the second and third equations, one obtains that $b=c^2/3a^2$, and $d=-(c^4+1)/6c$. Substituting these in the last equality of (4.1) gives $c^8-54c^4-243=0$ with theroots

$$\begin{aligned} c = \pm\sqrt{3}\left(3+2\sqrt{3}\right)^{\frac{1}{4}}, &\quad \pm\frac{\sqrt{2}(1+\mathrm{i})}{2}\left(3-2\sqrt{3}\right)^{\frac{1}{4}}, \\ \pm\sqrt{3}\left(3+2\sqrt{3}\right)^{\frac{1}{4}}\mathrm{i}, &\quad \pm\frac{\sqrt{2}(1-\mathrm{i})}{2}\left(3-2\sqrt{3}\right)^{\frac{1}{4}}. \end{aligned}$$

The above eight roots together with the three roots $a=-1, (1\pm\sqrt{3}\mathrm{i})/2$ of $a^3+1=0$ determine 24 points on $\mathcal{E}'_3$ generating the Mordell–Weil lattice $\mathcal{E}'_3(\mathbb{C}(s))$. The points with $a=-1$ generate a sublattice isomorphic to the unit matrix of degree 4. By straight computations and similar argument as in [9, Section 6], one can check that the four points $Q_j=(a_js+b_j, c_js+d_j)$ generate $\mathcal{E}'_3(\mathbb{C}(s))$, where their coefficients are

$$\begin{aligned}
&a_1=-1, && b_1=3^{\frac{1}{4}}\epsilon_1^{\frac{1}{2}}, && c_1=3^{\frac{5}{8}}\epsilon_1^{\frac{1}{4}}, && d_1=-3^{\frac{3}{8}}\epsilon_1^{\frac{3}{4}},\\
&a_2=-1, && b_2=-3^{\frac{1}{4}}\epsilon_1^{\frac{1}{2}}, && c_2=3^{\frac{5}{8}}\epsilon_1^{\frac{1}{4}}\mathrm{i}, && d_2=3^{\frac{3}{8}}\epsilon_1^{\frac{3}{4}}\mathrm{i},\\
&a_3=-1, && b_3=3^{\frac{1}{4}}\epsilon_1'^{\frac{1}{2}}\mathrm{i}, && c_3=3^{\frac{5}{8}}\zeta_8\epsilon_1'^{\frac{1}{4}}, && d_3=-3^{\frac{3}{8}}\zeta_8\epsilon_1'^{\frac{3}{4}},\\
&a_4=\zeta_6, && b_4=3^{\frac{1}{4}}\zeta_3^2\epsilon_1^{\frac{1}{2}}, && c_4=3^{\frac{5}{8}}\epsilon_1^{\frac{1}{4}}, && d_4=-3^{\frac{3}{8}}\epsilon_1^{\frac{3}{4}}.
\end{aligned}$$

The Gram matrix of the points Q_j's is given by

$$R'_3=\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 1\\ 0 & 2 & 0 & 1\\ 0 & 0 & 2 & 1\\ 1 & 1 & 1 & 2 \end{pmatrix},$$

which has determinant 1/4. Thus, the splitting field $\mathcal{K}_3'$ of $\mathcal{E}_3'$ over $\mathbb{Q}(t)$ is the compositum of the fields defined by the polynomials $a^3+1=0$ and $c^8-54c^4-243=0$, including the field $\mathbb{Q}(\zeta_3,(3+3\sqrt{3})^{1/4})$.

Using Theorem 2.1, and substituting $s=t+1/t$ and $s=\zeta_3 t+1/\zeta_3 t$ in the coordinates of Q_j's for $j=1,2,3,4$, we obtain

$$P_j=(x(t),y(t))=\left(\frac{a_jt^2+b_jt+a_j}{t},\ \frac{c_jt^2+d_jt+c_j}{t}\right),$$
$$P_{j+4}=(x(\zeta_3t),y(\zeta_3t))=\left(\frac{a_j\zeta_3^2t^2+b_j\zeta_3t+a_j}{\zeta_3t},\ \frac{c_j\zeta_3^2t^2+d_j\zeta_3t+c_j}{\zeta_3t}\right).$$

Using PARI/GP, we obtain that the defining minimal polynomial of $\mathcal{K}_3$, including $\mathbb{Q}(\zeta_6,(3+3\sqrt{3})^{1/4})$, is equal to the compositum of the fields defined by $x^3-1=0$, $x^3+1=0$ and $x^8-54x^4-243=0$, leading to

$$\begin{aligned}(4.2)\quad g_3(x)=x^{16}&+8x^{15}+36x^{14}+112x^{13}+158x^{12}-144x^{11}-836x^{10}\\&+86040x^5-1144x^9+3051x^8+14624x^7+45820x^6\\&+109130x^4+91912x^3-60552x^2-94600x+49141.\end{aligned}$$

By properties of height pairing, we have

$$\langle P_i,P_{i+j}\rangle=-\frac{1}{2}\langle P_i,P_j\rangle\ (1\le i,j\le 4).$$

Using this fact and the matrix R_3', one can see that the Gram matrix of the eight points $P_1,\dots,P_8$ is equal to

$$R_3=\frac{1}{2}\begin{pmatrix}4&0&0&2&-2&0&0&-1\\0&4&0&2&0&-2&0&-1\\0&0&4&2&0&0&-2&-1\\2&2&2&4&-1&-1&-1&-2\\-2&0&0&-1&4&0&0&2\\0&-2&0&-1&0&4&0&2\\0&0&-2&-1&0&0&4&2\\-1&-1&-1&-2&2&2&2&4\end{pmatrix},$$

which has determinant $3^4/4^2$ as desired. We refer the reader to [4, check-3] for details on the computations of this section.

5. The case $\mathcal{E}_4$

In this section, we prove Theorem 1.3 using the following result on the rational elliptic surface $\mathcal{E}_4'$.

Theorem 5.1. *The splitting field $\mathcal{K}_4'$ of the rational elliptic surface*

$$\mathcal{E}_4' : y^2 = x^3 - \left(s^4 - 4s^2 + 2\right),$$

is a number field of degree 24 defined by the defining minimal polynomial given by (5.2). Moreover, the Mordell–Weil lattice $\mathcal{E}_4'(\mathcal{K}_4'(s))$ is generated by the points

$$Q_j = \left(a_j s + b_j, s^2 + c_j s + d_j\right),$$

for $j = 1, \ldots, 6$, where a_j, b_j, c_j, d_j are given in the next subsection.

5.1. Proof of Theorem 5.1. The discriminant of $\mathcal{E}_4'$ is $-27\left(s^4-4s^2+2\right)^2$. Hence, the singular fibers of $\mathcal{E}_4'$ are of type II over the roots of $s^4 - 4s^2 + 2$ and of type IV over $s = \infty$. Then, Shioda–Tate's formula shows that the Mordell–Weil rank of $\mathcal{E}_4'(\mathbb{C}(s))$ is equal to 6 and $\mathcal{E}_4'(\mathbb{C}(s)) \cong E_6^*$. Based on [9, Theorem 10.5], a set of six linearly independent generators of $\mathcal{E}_4'(\mathbb{C}(s))$ can be found of the set of 27 rational points $Q = \left(as+b,\ s^2+cs+d\right)$. Substituting these in the equation of $\mathcal{E}_4'$ leads to

$$\begin{aligned} 2c - a^3 = 0, &\quad 3a^2b - c^2 - 2d - 4 = 0,\\ 3ab^2 - 2cd = 0, &\quad\quad\quad b^3 - d^2 + 2 = 0. \end{aligned}$$

From the first two equations, we get

$$c = \frac{a^3}{2}, \quad d = -\frac{1}{8}\left(a^6 - 12a^2b + 16\right) \tag{5.1}$$

and two polynomials in b with coefficients in the ring $\mathbb{Q}[a]$ as

$$\begin{aligned} p_1 &= 24ab^2 - 12a^5b + a^9 + 16a^3,\\ p_2 &= -64b^3 + 144a^4b^2 - 24a^2\left(a^6 + 16\right)b + a^{12} + 32a^6 + 128. \end{aligned}$$

Taking the resultant respect to b of p_1 and p_2 gives a polynomial of degree 27 of the form $\Phi(a) = a^3\Phi_1(a)\Phi_2(a)$, where

$$\Phi_1(a) = a^{12} - 352a^6 - 128 \text{ and } \Phi_2(a) = a^{12} - 32a^6 + 3456.$$

By (5.1) and using the roots of $\Phi(a)$, we obtain coefficients of the 27 points $Q = \left(as + b, s^2 + cs + d\right)$ in $\mathcal{E}_4'(\mathbb{C}(t))$. The factors of degree 12 of $\Phi(a)$ can be decomposed as

$$\begin{aligned} \Phi_1(a) &= \prod_{\ell=0}^{5}\left(a - 2^{\frac{7}{12}}\zeta_{12}^{2\ell}\epsilon_2^{\frac{1}{6}}\right)\prod_{\ell=0}^{5}\left(a - 2^{\frac{7}{12}}\zeta_{12}^{2\ell+1}{\epsilon_2'}^{\frac{1}{6}}\right),\\ \Phi_2(a) &= \prod_{\ell=0}^{5}\left(a - 2^{\frac{7}{12}}\zeta_{12}^{2\ell}\epsilon_3^{\frac{1}{6}}\right)\prod_{\ell=0}^{5}\left(a - 2^{\frac{7}{12}}\zeta_{12}^{2\ell+1}{\epsilon_3'}^{\frac{1}{6}}\right). \end{aligned}$$

Thus, the splitting field $\mathcal{K}_4'$ of $\mathcal{E}_4'$ is equal to the compositum of the splitting fields of the polynomials $\Phi_1(a)$ and $\Phi_2(a)$, which has the following minimal polynomial:

$$\begin{aligned} g_4(x) = x^{24} &- 12x^{22} + 114x^{20} - 664x^{18} + 2856x^{16} \\ &- 8928x^{14} + 21196x^{12} - 33576x^{10} + 35484x^8 \\ &- 20544x^6 + 5832x^4 - 720x^2 + 36. \end{aligned} \tag{5.2}$$

Thus, $\mathcal{E}_4'(\mathbb{C}(s)) \cong \mathcal{E}_4'(\mathcal{K}_4'(s))$ and by straight height computations and the determinant of the lattice $\mathcal{E}_4'(\mathbb{C}(s)) \cong E_6^*$, we obtain its six linearly independent generators $Q_j = (a_j s + b_j, s^2 + c_j s + d_j)$ with the coefficients

$$\begin{array}{llll}
a_1 = 0, & b_1 = 2^{\frac{1}{3}}, & c_1 = 0, & d_1 = -2, \\
a_2 = 2^{\frac{7}{12}}\epsilon_2^{\frac{1}{6}}, & b_2 = 2^{\frac{5}{6}}\left(\sqrt{2}+\sqrt{3}\right), & c_2 = 2^{\frac{3}{4}}\epsilon_2^{\frac{1}{2}}, & d_2 = 6 + 3\sqrt{6}, \\
a_3 = 2^{\frac{7}{12}}\epsilon_3^{\frac{1}{6}}, & b_3 = \dfrac{2^{\frac{1}{3}}\epsilon_3^{\frac{2}{3}}(\epsilon_3 \mathrm{i} + 1)}{9}, & c_3 = 2^{\frac{3}{4}}\epsilon_3^{\frac{1}{2}}, & d_3 = 2 + \sqrt{2}\mathrm{i}, \\
a_4 = 0, & b_4 = 2^{\frac{1}{3}}\zeta_3, & c_4 = 0, & d_4 = -2, \\
a_5 = 2^{\frac{7}{12}}\zeta_{12}\epsilon_2'^{\frac{1}{6}}, & b_5 = 2^{\frac{5}{6}}\zeta_6^5\epsilon_2'^{\frac{2}{3}}\left(\sqrt{2}+\sqrt{3}\right), & c_5 = 2^{\frac{3}{4}}\epsilon_2'^{\frac{1}{2}}\mathrm{i}, & d_5 = 6 - 3\sqrt{6}, \\
a_6 = 2^{\frac{7}{12}}\epsilon_3^{\frac{1}{6}}\zeta_6, & b_6 = \dfrac{-2^{\frac{1}{3}}\epsilon_3^{\frac{2}{3}}(\epsilon_3 - \mathrm{i})}{9\zeta_{12}}, & c_6 = -2^{\frac{3}{4}}\epsilon_3^{\frac{1}{2}}, & d_6 = 2 + \sqrt{2}\mathrm{i}.
\end{array}$$

The Gram matrix of the points $Q_1, \ldots, Q_6$ is given by

$$R_4' = \frac{1}{3}\begin{pmatrix} 4 & -2 & 1 & -2 & 1 & -2 \\ -2 & 4 & 1 & 1 & 1 & 1 \\ 1 & 1 & 4 & -2 & 1 & 1 \\ -2 & 1 & -2 & 4 & -2 & 1 \\ 1 & 1 & 1 & -2 & 4 & -2 \\ -2 & 1 & 1 & 1 & -2 & 4 \end{pmatrix},$$

which is of determinant $1/3$. Therefore, they are linearly independent generators of $\mathcal{E}_4'(\mathcal{K}_4'(s))$.

5.2. Proof of Theorem 1.3. Considering Theorem 2.1 and substituting $s = t + 1/t$ in the coordinates of the points $Q_j = (a_j s + b_j, s^2 + c_j s + d_j)$ in $\mathcal{E}_4'(\mathcal{K}_4'(s))$, we obtain

$$P_j = \left(\frac{a_j t^2 + b_j t + a_j}{t}, \frac{t^4 + c_j t^3 + (d_j + 2)t^2 + c_j t + 1}{t^2}\right)$$

and their images $P_{j+6} = \phi_4(P_j)$, under the automorphism ϕ_4 of $\mathcal{E}_4$, with the coordinates

$$x(P_{j+6}) = -\frac{(1+\mathrm{i})a_j t^2 + 2b_j t + (2-2\mathrm{i})a_j}{2t},$$
$$y(P_{j+6}) = \frac{\mathrm{i}t^4 + (1+\mathrm{i})c_j t^3 + (4+2d_j)t^2 + (2-2\mathrm{i})c_j t - 4\mathrm{i}}{2t^2},$$

for $j = 1, \ldots, 6$, which all together generates $\mathcal{E}_4(\mathbb{C}(t)) \cong \mathcal{E}_4(\mathcal{K}_4(t))$, where $\mathcal{K}_4 = \mathcal{K}'_4(\zeta_8) = \mathcal{K}'_4$, because the compositum of the polynomials $g_4(x)$ and $x^8 - 1$ leads to the same number field. The Gram matrix of the points $P_1, \ldots, P_{12} \in \mathcal{E}_4(\mathcal{K}_4(t))$ is given by

$$R_4 = \frac{1}{3}\begin{pmatrix} 8 & -4 & 2 & -4 & 2 & -4 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 8 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 8 & -4 & 2 & 2 & 0 & 0 & 0 & -3 & 0 & 0 \\ -4 & 2 & -4 & 8 & -4 & 2 & 0 & 0 & 3 & 0 & 0 & 0 \\ 2 & 2 & 2 & -4 & 8 & -4 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 2 & 2 & 2 & -4 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & -4 & 2 & -4 & 2 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 8 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 3 & 0 & 0 & 2 & 2 & 8 & -4 & 2 & 2 \\ 0 & 0 & -3 & 0 & 0 & 0 & -4 & 2 & -4 & 8 & -4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & -4 & 8 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 2 & 2 & 2 & -4 & 8 \end{pmatrix},$$

whose determinant is $4^4/3^2$ as desired. Therefore, the proof of Theorem 1.3 is completed. We refer the reader to see [4, check-4] for the computations of this section.

6. The case $\mathcal{E}_5$

In this section, we prove Theorem 1.4 using the following result on the splitting field and a set of linearly independent generators of

$$\mathcal{E}'_5 : y^2 = x^3 + s^5 - 5s^3 + 5s,$$

over $\mathbb{C}(s)$.

Theorem 6.1. *The splitting field $\mathcal{K}'_5$ of $\mathcal{E}'_5$ is defined by the minimal polynomial of degree* 96 *given in* [4, min-pols], *that includes* $\mathbb{Q}(\zeta_{12}, 5^{1/24}, (\epsilon_4\epsilon_5)^{1/2})$.

Moreover, the lattice $\mathcal{E}_5'(\mathcal{K}_5'(s))$ *is generated by the points*

$$Q_j = (x_j(s), y_j(s)) = \left(\frac{s^2 + a_j s + b_j}{u_j^2}, \frac{s^3 + c_j s^2 + d_j s + e_j}{u_j^3}\right),$$

for $j = 1, \dots, 8$, *where* a_j, b_j, c_j, d_j, e_j *are given in* [4, check-5], *and the constants* u_j*'s are*

$$\begin{aligned} u_1 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5^{-1})^{\frac{1}{2}}\mathrm{i}, & u_2 &= 5^{\frac{1}{24}}(\epsilon_4^{-1}\epsilon_5)^{\frac{1}{2}}\mathrm{i}, & u_3 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5)^{\frac{1}{2}}\mathrm{i}, \\ u_4 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5)^{-\frac{1}{2}}\mathrm{i}, & u_5 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5^{-1})^{\frac{1}{2}}\epsilon_6\mathrm{i}, & u_6 &= 5^{\frac{1}{24}}(\epsilon_4^{-1}\epsilon_5)^{\frac{1}{2}}\epsilon_6\mathrm{i}, \\ u_7 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5)^{\frac{1}{2}}\epsilon_6^{-1}\mathrm{i}, & u_8 &= 5^{\frac{1}{24}}(\epsilon_4\epsilon_5\epsilon_6)^{-\frac{1}{2}}\mathrm{i}. \end{aligned}$$

6.1. Proof of Theorem 6.1. Since $\mathcal{E}_5'(\mathbb{C}(s))$ is isomorphic to E_8, there are 240 points $Q \in \mathcal{E}_5'(\mathbb{C}(s))$, corresponding to the 240 minimal roots of E_8, of the form

$$Q = \left(\frac{s^2 + as + b}{u^2}, \frac{s^3 + cs^2 + ds + e}{u^3}\right),$$

for suitable constants $a, b, c, d, e, u \in \mathbb{C}$. Substituting the coordinates of Q in the equation of $\mathcal{E}_5'$, we get the following six relations:

$$\begin{aligned} 2c - 3a - u^6 &= 0, & 2d - 3a^2 + c^2 - 3b &= 0, \\ 2e - a^3 - 6ab + 2cd + 5u^6 &= 0, & 3b^2 + 3a^2 b - 2ce - d^2 &= 0, \\ 3ab^2 + 5u^6 - 2de &= 0, & b^3 - e^2 &= 0. \end{aligned} \tag{6.1}$$

By the first three relations, we obtain c, d, e in terms of a, b and u as

$$c = \frac{3a + u^6}{2}, \quad d = \frac{3a^2 - c^2 + 3b}{2}, \quad e = \frac{a^3 + 6ab - 2cd - 5u^6}{2}.$$

Using Maple, we calculate the fundamental polynomial of the ideal generated by the equations (6.1) of degree 240 in the variable u, see [4, check-5].

Letting $V = u^{12}$, the polynomial $\Phi(V)$ decomposes into four irreducible factors in $\mathbb{Z}[V]$ over $\mathbb{Q}$, namely,

$$\begin{aligned} \Phi_1(V) &= V^4 - 56700V^3 - 1204210V^2 - 283500V + 25, \\ \Phi_2(V) &= V^4 + 6660V^3 - 685810V^2 - 91320300V + 25, \\ \Phi_3(V) &= V^4 - 1260V^3 + 1178590V^2 - 4592700V + 13286025, \\ \Phi_4(V) &= V^8 - 24300V^7 + 280019230V^6 \\ &\quad - 18498253500V^5 + 569262158025V^4 + 5919441120000V^3 \\ &\quad + 28673969152000V^2 + 796262400000V + 10485760000. \end{aligned}$$

Then, one can decompose all polynomials Φ_1, Φ_2, Φ_3 and Φ_4 over the field $k_0 = \mathbb{Q}(\mathrm{i}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\zeta_{12}, \sqrt{5})$ into the product of linear factors as given below,

$$\begin{aligned}
\Phi_1(V) &= (V - v_1)(V - v_1^{\sigma})(V - v_1^{\tau})(V - v_1^{\sigma\tau}),\\
\Phi_2(V) &= (V - v_2)(V - v_2^{\sigma})(V - v_2^{\tau})(V - v_2^{\sigma\tau}),\\
\Phi_3(V) &= (V - v_3)(V - v_3^{\sigma})(V - v_3^{\tau})(V - v_3^{\sigma\tau}),\\
\Phi_4(V) &= (V - v_4)(V - v_4^{\sigma})(V - v_4^{\tau})(V - v_4^{\sigma\tau})\\
&\qquad \times (V - \overline{v_4})(V - \overline{v_4}^{\sigma})(V - \overline{v_4}^{\tau})(V - \overline{v_4}^{\sigma\tau}),
\end{aligned}$$

where $\overline{z}$ gives the conjugate of any complex number z, and the maps σ and τ change respectively the signs of $\sqrt{3}$, $\sqrt{5}$, and v_1, v_2, v_3 and v_4 are as follows:

$$\begin{aligned}
v_1 &= \left(3660\sqrt{5} - 8190\right)\sqrt{3} - 6344\sqrt{5} + 14175,\\
v_2 &= \left(-420\sqrt{5} - 990\right)\sqrt{3} - 784\sqrt{5} - 1665,\\
v_3 &= 315 - 440\mathrm{i} + (140 - 198\mathrm{i})\sqrt{5},\\
v_4 &= \frac{\left(3510 - 3300\mathrm{i} - (1560 - 1485\mathrm{i})\sqrt{5}\right)\sqrt{3}}{2} + \frac{6075}{2} - 2860\mathrm{i}\\
&\qquad - (1350 - 1287\mathrm{i})\sqrt{5}.
\end{aligned}$$

Hence, the 240 roots of the fundamental polynomial $\Phi(u^{12})$ of $\mathcal{E}'_5$ are of the form $u = v^{1/12}\zeta_{12}^{\ell}$ for $\ell = 0, 1, \ldots, 11$, where v varies on the set of 20 roots of $\Phi(V)$. This means that the splitting field $\mathcal{K}'_5$ of $\mathcal{E}'_5$ includes the field $k_0(v_i^{1/12} : i = 1, 2, 3, 4)$. For each root of $\Phi(u)$, using the equations (6.1), one can determine the coefficients a, b, c, d, e and hence a rational point $Q \in \mathcal{E}'_5(\mathcal{K}'_5(s))$ such that $sp_\infty(Q) = u$, where sp_∞ is the specialization map from $\mathcal{E}'_5(\mathcal{K}'_5(s))$ to the additive group of $\mathcal{K}'_5$. Indeed, it maps $Q \in \mathcal{E}'_5(\mathcal{K}'_5(s))$ to the intersection point of the section (Q) and the fiber over ∞ which lies in the smooth part of the additive singular fiber $\pi^{-1}(\infty)$.

Since $\mathcal{E}'_5$ has no reducible fiber and all the 240 sections Q_j's corresponding to the roots of $\Phi(u)$ are points in $\mathcal{E}'_5(\mathcal{K}'_5(s))$ with polynomial coordinates, we have $\langle Q_j, Q_j\rangle = 2$ and $\langle Q_{j_1}, Q_{j_2}\rangle = 1 - (Q_{j_1} \cdot Q_{j_2})$, where $(Q_{j_1} \cdot Q_{j_2})$ denotes the intersection number for any $1 \leq j_1 \neq j_2 \leq 2$. Assuming $x_j = x(Q_j)$ and $y_j = y(Q_j)$, the number $(Q_{j_1} \cdot Q_{j_2})$ can be computed by the following formula:

$$\begin{aligned}
(Q_{j_1} \cdot Q_{j_2}) &= \deg(\gcd(x_{j_1} - x_{j_2}, y_{j_1} - y_{j_2}))\\
&\qquad + \min\{2 - \deg(x_{j_1} - x_{j_2}), 3 - \deg(y_{j_1} - y_{j_2})\}.
\end{aligned}$$

Using this formula and considering the determinant conditions, we obtain a subset of eight points with unimodular height paring matrix. In order to describe those points, we consider the following roots of $\Phi(V)$:

$$v_1=\sqrt{5}\zeta_{12}^6\epsilon_4^6\epsilon_5^{-6},\qquad v_1^\sigma=\sqrt{5}\zeta_{12}^6\epsilon_4^{-6}\epsilon_5^6,\qquad v_1^\tau=\sqrt{5}\zeta_{12}^6\epsilon_4^6\epsilon_5^6,$$
$$v_1^{\sigma\tau}=\sqrt{5}\zeta_{12}^6\epsilon_4^{-6}\epsilon_5^{-6},\qquad v_2=\sqrt{5}\zeta_{12}^6\epsilon_4^6\epsilon_5^{-6}\epsilon_6^{12},\qquad v_2^\sigma=\sqrt{5}\zeta_{12}^6\epsilon_4^{-6}\epsilon_5^6\epsilon_6^{12},$$
$$v_2^\tau=\sqrt{5}\zeta_{12}^6\epsilon_4^6\epsilon_5^6\epsilon_6^{-12},\quad v_2^{\sigma\tau}=\sqrt{5}\zeta_{12}^6\epsilon_4^{-6}\epsilon_5^{-6}\epsilon_6^{-12}.$$

Hence, the roots $v_1, v_1^\sigma, v_1^\tau, v_1^{\sigma\tau}, v_2, v_2^\sigma, v_2^\tau$ and $v_2^{\sigma\tau}$ correspond to the eight points

$$Q_j=\left(\frac{s^2+a_js+b_j}{u_j^2},\frac{s^3+c_js^2+d_js+e_j}{u_j^3}\right)\in\mathcal{E}_5'(\mathcal{K}_5'(s)),$$

for $j=1,\dots,8$, where a_j,b_j,c_j,d_j,e_j are given in [4, check-5] and u_j's are given as follows:

$$u_1=v_1^{\frac{1}{12}},\quad u_2=(v_1^\sigma)^{\frac{1}{12}},\quad u_3=(v_1^\tau)^{\frac{1}{12}},\quad u_4=(v_1^{\sigma\tau})^{\frac{1}{12}},$$
$$u_5=v_2^{\frac{1}{12}},\quad u_6=(v_2^\sigma)^{\frac{1}{12}},\quad u_7=(v_2^\tau)^{\frac{1}{12}},\quad u_8=(v_2^{\sigma\tau})^{\frac{1}{12}}.$$

Applying the specialization map $sp_\infty:\mathcal{E}_5'(\mathcal{K}_5')\to(\mathcal{K}_5')^+$ to these points and dividing the images by u_1, we obtain the following subset of the field $\mathcal{K}_5'$,

$$\left\{1,\frac{u_j}{u_1}:j=2,\dots,8\right\}=\left\{1,\epsilon_4^{-1}\epsilon_6,\epsilon_6,\epsilon_4^{-1},\epsilon_5,\epsilon_4^{-1}\epsilon_5\epsilon_6,\epsilon_5^{-1}\epsilon_6,\epsilon_4^{-1}\epsilon_5^{-1}\right\},$$

which is easy to see that they are linearly independent over $\mathbb{Q}$. Thus, the points $Q_1,\dots,Q_8$ form a linearly independent subset generating a sublattice of rank 8 in $\mathcal{E}_5'(\mathcal{K}_5'(s))$. The Gram matrix of these eight points is equal to the following unimodular matrix:

$$R_5'=\begin{pmatrix}2&0&0&-1&0&0&0&0\\0&2&-1&0&0&0&1&-1\\0&-1&2&0&0&0&0&0\\-1&0&0&2&-1&-1&0&0\\0&0&0&-1&2&0&0&-1\\0&0&0&-1&0&2&-1&0\\0&1&0&0&0&-1&2&0\\0&-1&0&0&-1&0&0&2\end{pmatrix}.$$

Thus, the points Q_j's for $j=1,\dots,8$ generate the whole group $\mathcal{E}_5'(\mathcal{K}_5'(s))$ as desired. Using PARI/GP, we obtain that $\mathcal{K}_5'$ is a number field of degree 96 with the defining minimal polynomial $g_5'(x)$ given in [4, min-pols].

Therefore, the proof of Theorem 6.1 is finished.

6.2. Proof of Theorem 1.4. First, we note that the splitting field of the elliptic $K3$ surface $\mathcal{E}_5$ over $\mathbb{Q}(t)$ is equal to $\mathcal{K}_5 = \mathcal{K}_5'(\zeta_5)$, where $\mathcal{K}_5'$ is the splitting field of $\mathcal{E}_5'$ over $\mathbb{Q}(s)$. The field $\mathcal{K}_5$ is defined by the polynomial $g_5(x)$ of degree 192 with the huge coefficients given in [4]. Indeed $\mathcal{K}_5$ is the compositum of the polynomial $g_5'(x)$ and the cyclotomic polynomial of order 5, because $x^5 - 1 = (x-1)\big(x^4 + x^3 + x^2 + x + 1\big)$.

Letting $s = t + 1/t$, the rational elliptic surface $\mathcal{E}_5'$ over $\mathcal{K}_5(s)$ is isomorphic to $\mathcal{E}_5$ over $\mathcal{K}_5(t)$ as a quadratic extension of $\mathcal{K}_5(s)$. Hence, the linearly independent generators

$$Q_j = \left(\frac{s^2 + a_j s + b_j}{u_j^2}, \frac{s^3 + c_j s^2 + d_j s + e_j}{u_j^3} \right)$$

of $\mathcal{E}'(\mathcal{K}_5(s))$ lead to the points $P_j = (x_j(t), y_j(t)) \in \mathcal{E}_5(\mathcal{K}_5(t))$ of the form given in the statement of Theorem 1.4 with the constants a_j, b_j, c_j, d_j, e_j and u_j's, for $j = 1, \ldots, 8$, provided in [4].

Furthermore, by letting $s = \zeta_5 t + 1/\zeta_5 t$ and following the same argument as above, we obtain the points $P_{j+8} = \big(x_j(\zeta_5 t), y_j(\zeta_5 t)\big)$ for $j = 1, \ldots, 8$. We note that the points $P_j' = \big(t^2 x(P_j), t^3 y(P_j)\big)$ belong to the Mordell–Weil lattice of the elliptic $K3$ surface $\mathcal{E} : y^2 = x^3 + t\big(t^{10} + 1\big)$, which is birational to $\mathcal{E}_5$ over $\mathcal{K}_5(t)$. Since the P_j''s have no intersection with the zero section of $\mathcal{E}$, we have $\langle P_j', P_j' \rangle = 4$, and $\langle P_{j_1}', P_{j_2}' \rangle = 2 - (P_{j_1}' \cdot P_{j_2}')$, for $1 \le j_1 \ne j_2 \le 16$. The intersection number $(P_{j_1}' \cdot P_{j_2}')$ can be computed by

$$\begin{aligned}(P_{j_1}' \cdot P_{j_2}') = {} & \deg(\gcd(x_{j_1} - x_{j_2}, y_{j_1} - y_{j_2})) \\ & + \min\{4 - \deg(x_{j_1} - x_{j_2}), 6 - \deg(y_{j_1} - y_{j_2})\}.\end{aligned}$$

Thus, we obtain the following Gram matrix R_5 of the height pairing for the points P_j''s and hence for the P_j's:

$$R_5 = \begin{pmatrix}
4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 2 & 0 & 0 & 1 \\
0 & 4 & 2 & 0 & 0 & 0 & -2 & 2 & 0 & -2 & -1 & 1 & 0 & 2 & 2 & -1 \\
0 & 2 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 2 & 0 \\
2 & 0 & 0 & 4 & 2 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 \\
0 & 0 & 0 & 2 & 4 & 0 & 0 & 2 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & 0 & 4 & 2 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & -1 & 1 \\
0 & -2 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 2 & 2 & 0 & 0 & -1 & -2 & 0 \\
0 & 2 & 0 & 0 & 2 & 0 & 0 & 4 & 1 & -1 & 0 & 2 & 0 & 1 & 0 & -2 \\
-2 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & -2 & -1 & 1 & 0 & 2 & 2 & -1 & 0 & 4 & 2 & 0 & 0 & 0 & -2 & 2 \\
0 & -1 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 0 & 0 & 4 & 2 & 2 & 0 & 0 \\
2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 2 \\
0 & 2 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 2 & 0 & 4 & 2 & 0 \\
0 & 2 & 2 & 0 & 0 & -1 & -2 & 0 & 0 & -2 & 0 & 0 & 0 & 2 & 4 & 0 \\
1 & -1 & 0 & 2 & 0 & 1 & 0 & -2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 4
\end{pmatrix}.$$

One can check that its determinant is equal to 5^4 as desired, which shows that the points P_j's for $j = 1, \ldots, 16$ form a set of linearly independent generators of $\mathcal{E}_5$ over $\mathcal{K}_5(t)$. We refer the reader to see [4, check-5] for the computations of this section, and [4, Points-5] for the list of the sixteen points in $\mathcal{E}_5(\mathcal{K}_5(t))$.

7. The case $\mathcal{E}_6$

We prove Theorem 1.5 on the elliptic $K3$ surface $\mathcal{E}_6 : y^2 = x^3 + t^6 + 1/t^6$ over $\mathbb{C}(t)$ in this section. To do this, first we determine the splitting field $\mathcal{K}'_6$ and find a set of linearly independent generators for the Mordell–Weil lattice of the rational elliptic surface $\mathcal{E}'_6 : y^2 = x^3 + f_6(s)$, where

$$f_6(s) = s^6 - 6s^4 + 9s^2 - 2 = (s^2 - 2)(s^4 - 4s^2 + 1).$$

To simplify the computations, we set $\widetilde{s} = s - \sqrt{2}$ to obtain the rational elliptic surface

$$\widetilde{\mathcal{E}}'_6 : y^2 = x^3 + f'_6(\widetilde{s}), \tag{7.1}$$

where

$$f'_6(\widetilde{s}) = \widetilde{s}(\widetilde{s} - 2\sqrt{2})(\widetilde{s}^2 - \sqrt{2}\widetilde{s} - 1)(\widetilde{s}^2 - 3\sqrt{2}\widetilde{s} + 3).$$

It is easy to see that $\widetilde{\mathcal{E}}'_6$ is birational to $\mathcal{E}'_6$ over $\mathbb{Q}(\sqrt{2})$, and we have $\widetilde{\mathcal{E}}'_6(\mathbb{C}(\widetilde{s})) \cong \mathcal{E}'_6(\mathbb{C}(s)) \cong E_8$. Hence, there exist exactly 240 points in $\widetilde{\mathcal{E}}'_6(\mathbb{C}(\widetilde{s}))$ of the form

$$\widetilde{Q} = (a\widetilde{s}^2 + b\widetilde{s} + g,\ c\widetilde{s}^3 + d\widetilde{s}^2 + e\widetilde{s} + h) \tag{7.2}$$

corresponding to the points $Q = (x, y) \in \mathcal{E}'_6(\mathbb{C}(s))$ with

$$\begin{aligned} x(s) &= as^2 + (b - 2\sqrt{2}a)s + g + (2a - \sqrt{2}b), \\ y(s) &= cs^3 + (d - 3\sqrt{2}c)s^2 + (6c - 2\sqrt{2}d + e)s \\ &\quad + h - \sqrt{2}(2c - \sqrt{2}d + e). \end{aligned} \tag{7.3}$$

It is clear that the splitting field $\mathcal{K}'_6$ of $\mathcal{E}'_6$ is a quadratic extension by $\sqrt{2}$ of the splitting field of $\widetilde{\mathcal{E}}'_6$, which is denoted by $\widetilde{\mathcal{K}}'_6$ and includes $\mathbb{Q}(\sqrt{2})$ as a subfield. We have the following result on $\widetilde{\mathcal{K}}'_6$ and the set of linearly independent generators of $\widetilde{\mathcal{E}}'_6(\widetilde{\mathcal{K}}'_6(\widetilde{s}))$.

Theorem 7.1. *The splitting field $\widetilde{\mathcal{K}}'_6$ of $\widetilde{\mathcal{E}}'_6$ is a number field of degree* 96 *with the defining minimal polynomial given in* [4, min-pols]*. Moreover, the lattice $\widetilde{\mathcal{E}}'_6(\widetilde{\mathcal{K}}'_6(\widetilde{s}))$ is generated by*

$$\widetilde{Q}_j = (a_j\widetilde{s}^2 + b_j\widetilde{s} + u_j^2,\ c_j\widetilde{s}^3 + d_j\widetilde{s}^2 + e_j\widetilde{s} + u_j^3), \quad j = 1, \ldots, 8,$$

where a_j, b_j, c_j, d_j, e_j and u_j are given in [4, check-6].

In the next subsection, we prove the above theorem and in Subsection 7.2 we provide the complete proof of Theorem 1.5.

7.1. Proof of Theorem 7.1. We first determine the fundamental polynomial of $\widetilde{\mathcal{E}}'_6$ over $\mathbb{Q}(\sqrt{2})$. Substituting the coordinates of $\widetilde{Q} \in \widetilde{\mathcal{E}}'_6(\widetilde{\mathcal{K}}'_6(\widetilde{s}))$, given by (7.2), in the equation (7.1) of $\widetilde{\mathcal{E}}'_6$ and letting $g = u^2, h = u^3$, we get the following six relations:

$$\begin{aligned}
a^3 - c^2 + 1 &= 0,\\
3a^2b - 2cd - 6\sqrt{2} &= 0,\\
3a^2u^2 + 3ab^2 - 2ce - d^2 + 24 &= 0,\\
6abu^2 - 2cu^3 + b^3 - 2de - 16\sqrt{2} &= 0,\\
3au^4 + 3b^2u^2 - 2du^3 - e^2 - 3 &= 0,\\
3bu^4 - 2eu^3 + 6\sqrt{2} &= 0.
\end{aligned}$$

Using Maple, one can compute the fundamental polynomial $\Phi(u)$ of the ideal generated by the above equations, which is a polynomial of degree 240 in terms of u up to a constant. By taking $v = u^2$, we obtain a polynomial $\Phi(v)$ in $\mathbb{Z}[v]$ which can be decomposed into nine irreducible factors, namely,

$$\Phi(v) = \prod_{i=1}^{9} \Phi_i(v).$$

The first six factors of $\Phi(v)$ can be decomposed as follows:

$$\begin{aligned}
\Phi_1(v) &= v^3 - 2 = (v - \beta_0^2)(v - \beta_0^2\zeta_3)(v - \beta_0^2\zeta_3^2),\\
\Phi_2(v) &= v^4 - 6v^2 - 3 = (v - \beta_1^2)(v + \beta_1^2)(v - \mathrm{i}\beta_2^2)(v + \mathrm{i}\beta_2^2),\\
\Phi_3(v) &= v^3 + 12v^2 + 12v + 6 = (v - v_{31})(v - v_{32})(v - v_{33}),\\
\Phi_4(v) &= v^8 + 6v^6 + 39v^4 - 18v^2 + 9\\
&= (v + \zeta_3\beta_1^2)(v - \zeta_3\beta_1^2)(v + \zeta_6\beta_1^2)(v - \zeta_6\beta_1^2)\\
&\qquad \times (v + \zeta_{12}\epsilon'_1\beta_1^2)(v - \zeta_{12}\epsilon'_1\beta_1^2)(v + \zeta_{12}^{11}\epsilon'_1\beta_1^2)(v - \zeta_{12}^{11}\epsilon'_1\beta_1^2),\\
\Phi_5(v) &= v^6 - 12v^5 + 132v^4 - 132v^3 + 72v^2 - 72v + 36\\
&= (v - v_{51})(v - v_{51}^{\gamma})(v - v_{52})(v - v_{52}^{\gamma})(v - v_{53})(v - v_{53}^{\gamma}),\\
\Phi_6(u) &= v^8 - 48v^7 + 168v^6 - 912v^5 + 1272v^4\\
&\qquad - 1152v^3 + 864v^2 - 576v + 144\\
&= (v - v_{61})(v - v_{61}^{\gamma})(v - v_{62})(v - v_{62}^{\gamma})(v - v_{63})\\
&\qquad \times (v - v_{63}^{\gamma})(v - v_{64})(v - v_{64}^{\gamma})
\end{aligned}$$

with

$$\begin{aligned}
v_{31} &= -\big(2\beta_0^4+3\beta_0^2+4\big), \quad v_{32} = 2\beta_0^4\zeta_6^5+3\beta_0^2\zeta_6-4,\\
v_{33} &= 2\beta_0^4\zeta_6+3\beta_0^2\zeta_6^5-4,\\
v_{51} &= \big(2\beta_0^4+3\beta_0^2+4\big)\zeta_6, \quad v_{52} = 2\beta_0^4\zeta_6-3\beta_0^2+4\zeta_6^5,\\
v_{53} &= -2\beta_0^4+3\beta_0^2\zeta_6+4\zeta_6^5,\\
v_{61} &= \sqrt{3}\beta_1^4+2\sqrt{2}\mathrm{i}\beta_1^3-(2\sqrt{3}+1)\beta_1^2-\sqrt{2}(\sqrt{3}+3)\mathrm{i}\beta_1,\\
v_{62} &= \sqrt{3}\beta_1^4+2\sqrt{2}\beta_1^3+\big(2\sqrt{3}+1\big)\beta_1^2+\sqrt{2}\big(\sqrt{3}+3\big)\beta_1,\\
v_{63} &= -\sqrt{3}\beta_1^4+\sqrt{2}\big(3\sqrt{3}-5\big)(\mathrm{i}+1)\beta_1^3+\big(5\sqrt{3}-8\big)\mathrm{i}\beta_1^2\\
&\qquad +\sqrt{2}\big(-3+2\sqrt{3}\big)(\mathrm{i}-1)\beta_1+12,\\
v_{64} &= -\sqrt{3}\beta_1^4+\sqrt{2}\big(3\sqrt{3}-5\big)(\mathrm{i}-1)\beta_1^3-\big(5\sqrt{3}-8\big)\mathrm{i}\beta_1^2\\
&\qquad +\sqrt{2}\big(-3+2\sqrt{3}\big)(\mathrm{i}+1)\beta_1+12,
\end{aligned}$$

where γ changes the sign of $\sqrt{2}$. One can check that the other three factors of $\Phi(v)$, say $\Phi_7(v)$, $\Phi_8(v)$ and $\Phi_9(v)$ of degrees 16, 24 and 48 respectively, can be completely decomposed over $\mathbb{Q}(\mathrm{i},\beta_0,\beta_1)$. For example, the seventh factor is the following degree 16 polynomial:

$$\begin{aligned}
\Phi_7(v) = v^{16} &+ 48v^{15}+2136v^{14}+6240v^{13}-16824v^{12}\\
&+32256v^{11}+564480v^{10}+815040v^{9}+477360v^{8}\\
&-6912v^{7}-248832v^{6}-338688v^{5}-100224v^{4}\\
&+165888v^{3}+207360v^{2}+82944v+20736,
\end{aligned}$$

and one of its roots is equal to

$$v_7 = \frac{1}{2}\big(v_{73}\beta_1^3+v_{72}\beta_1^2+v_{71}\beta_1+v_{70}\big), \tag{7.4}$$

where

$$\begin{aligned}
v_{70} &= 3\big((1+2\mathrm{i})\sqrt{3}-(2+3\mathrm{i})\big), \quad v_{71} = -\beta_0^3\big((5\mathrm{i}-1)\sqrt{3}+(3-9\mathrm{i})\big),\\
v_{72} &= (5\mathrm{i}-8)\sqrt{3}+(15-8\mathrm{i}), \qquad v_{73} = 2\beta_0^3\big((4+\mathrm{i})\sqrt{3}-(7+2\mathrm{i})\big).
\end{aligned}$$

We cite [4, check-6] to see the complete decomposition of all factors of $\Phi(v)$. Thus, the field $\mathcal{K}_6'$ is an extension of $\mathbb{Q}(\mathrm{i},\beta_0,\beta_1)$, with a defining minimal polynomial of degree 96 with huge coefficients, see [4, min-pols].

By a direct search for the eight roots among 240 root of $\Phi(u)$ and considering the determinant conditions on the Gram matrix of corresponding points, we find the following roots:

$$\begin{aligned}
&u_1 = \beta_0, \quad u_2 = \zeta_6\beta_0, \quad u_3 = \beta_1, \quad u_4 = \zeta_8\beta_1,\\
&u_5 = v_{32}^{\frac{1}{2}}, \quad u_6 = \zeta_{12}\beta_1, \quad u_7 = v_{61}^{\frac{1}{2}}, \quad u_8 = v_7^{\frac{1}{2}}.
\end{aligned}$$

These provide the following eight points generating $\widetilde{\mathcal{E}}'_6(\widetilde{\mathcal{K}}'_6(\widetilde{s}))$:

$$\widetilde{Q}_j = \left(a_j\widetilde{s}^2 + b_j\widetilde{s} + g_j,\ c_j\widetilde{s}^3 + d_j\widetilde{s}^2 + e_j\widetilde{s} + h_j\right),\ j = 1, \ldots, 8,$$

where $a_j, b_j, c_j, d_j, g_i, h_i$ are given in [4, check-6].

Applying the specialization map $sp_0 : \mathcal{E}'_6(\mathcal{K}'_6(\widetilde{s})) \to (\mathcal{K}'_6)^+$, defined by

$$P \longmapsto sp_0(P) = \frac{1}{u} = \frac{x(P)}{y(P)}\bigg|_{\tilde{s}=0},$$

to the above points and multiplying the images by u_1, we obtain

$$\left\{1, \frac{u_j}{u_1} : j = 2, \ldots, 8\right\} \subset \mathcal{K}'_6,$$

which can be checked that they are linearly independent over $\mathbb{Q}$. Thus the points $\widetilde{Q}_1, \ldots, \widetilde{Q}_8$ form a linearly independent subset generating a sublattice of rank 8 in $\mathcal{E}'_6(\mathcal{K}'_6(\widetilde{s}))$. Moreover, the Gram matrix of the points $\widetilde{Q}_1, \ldots, \widetilde{Q}_8$ is equal to the following unimodular matrix:

$$R'_6 = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 & -1 & 1 \\ 1 & 1 & 0 & 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 2 \end{pmatrix}.$$

Finally, one can use (7.3) to get the points $Q_j = (x_j, y_j) \in \mathcal{E}'_6\big(\mathcal{K}'_6(s)\big)$ with

$$\begin{aligned} x_j(s) &= a_j s^2 + (b_j - 2\sqrt{2}a_j)s + u_j^2 + (2a_j - \sqrt{2}b_j), \\ y_j(s) &= c_j s^3 + (d_j - 3\sqrt{2}c_j)s^2 + (6c_j - 2\sqrt{2}d_j + e_j)s \\ &\qquad + u_j^3 - \sqrt{2}(2c_j - \sqrt{2}d_j + e_j). \end{aligned}$$

7.2. Proof of Theorem 1.5. The splitting field of the elliptic $K3$ surface $\mathcal{E}_6$ over $\mathbb{Q}(t)$ is equal to $\mathcal{K}_6 = \mathcal{K}'_6(\zeta_{12}) = \mathcal{K}'_6$, where $\mathcal{K}'_6$ is the splitting field of $\mathcal{E}'_6 : y^2 = x^3 + f_6(s)$ over $\mathbb{Q}(s)$.

Letting $s = t + 1/t$, one can see that the rational elliptic surface $\mathcal{E}'_6$ over $\mathcal{K}_6(s)$ is isomorphic to $\mathcal{E}_6$ over $\mathcal{K}_6(t)$ as a quadratic extension of $\mathcal{K}_6(s)$. Hence, the eight linearly independent generators $Q_j = (x_j(s), y_j(s)) \in$

$\mathcal{E}'(\mathcal{K}_6(s))$ give the points $P_j = (x_j(t), y_j(t)) \in \mathcal{E}_6(\mathcal{K}_6(t))$ with

$$x_j(t) = \frac{a_{j,4}t^4 + a_{j,3}t^3 + a_{j,2}t^2 + a_{j,1}t + a_{j,0}}{t^2},$$
$$y_j(t) = \frac{b_{j,6}t^6 + b_{j,5}t^5 + b_{j,4}t^4 + b_{j,3}t^3 + b_{j,2}t^2 + b_{j,1}t + b_{j,0}}{t^3},$$

where

$$\begin{aligned} &a_{j,0} = a_{j,4} = a_j, && a_{j,1} = a_{j,3} = b_j - 2\sqrt{2}a_j,\\ &a_{j,2} = u_j^2 + 4a_j - \sqrt{2}b_j, &&\\ &b_{j,0} = b_{j,6} = c_j, && b_{j,1} = b_{j,5} = c_j + d_j - 3\sqrt{2},\\ &b_{j,2} = b_{j,4} = d_j + 9c_j + e_j - 2\sqrt{2}, && b_{j,3} = u_j^3 - 8\sqrt{2}c_j - \sqrt{2}e_j + 4d_j. \end{aligned}$$

The constants a_j, b_j, c_j, d_j, e_j and u_j's for $j = 1, \ldots, 8$, are the same as in the previous subsection ([4, check-6]).

Furthermore, letting $s = \zeta_{12}t + 1/\zeta_{12}t$, and following the same fashion as above, we obtain the points $P_{j+8} = (x_{j+8}(t), y_{j+8}(t))$ for $j = 1, \ldots, 8$ with

$$x_{j+8}(t) = \frac{1}{\zeta_6 t^2}\sum_{i=0}^{4} a_{j+8,i}t^i \text{ and } y_{j+8}(t) = \frac{\mathrm{i}}{t^3}\sum_{i=0}^{6} b_{j+8,i}t^i,$$

where

$$\begin{aligned} a_{j+8,4} &= \zeta_3 a_{j+8,0} = \zeta_3 a_j,\\ a_{j+8,3} &= \zeta_6 a_{j+8,1} = 2\sqrt{2}\zeta_6 a_j + b_j,\\ a_{j+8,2} &= \zeta_6\big(a_j + \sqrt{2}b_j + g_j\big),\\ b_{j+8,6} &= -b_{j+8,0} = c_j,\\ b_{j+8,5} &= b_{j+8,1} = \zeta_{12}^5\big(3\sqrt{2}c_j + d_j\big),\\ b_{j+8,4} &= b_{j+8,2} = \zeta_3\big(9c_j + 2\sqrt{2}d_j + e_j\big),\\ b_{j+8,3} &= \big(8\sqrt{2}c_j + 4d_j + \sqrt{2}e_j + h_j\big)\mathrm{i}. \end{aligned}$$

We note that the points $P'_j = (\zeta_{12}^2 t^2 x(P_j), \zeta_{12}^3 t^3 y(P_j))$ belong to the Mordell–Weil lattice of $\mathcal{F} : y^2 = x^3 + t^{12} + 1$, which is birational to $\mathcal{F}_6$ over $\mathbb{C}(t)$. See [14] for more details. Having polynomial coordinates, the P'_j's have no intersection with the zero sections of $\mathcal{F}$, we get that $\langle P'_j, P'_j\rangle = 4$, $\langle P'_{j_1}, P'_{j_2}\rangle = 2 - (P'_{j_1} \cdot P'_{j_2})$, and for any $1 \le j_1 \ne j_2 \le 16$, the intersection number $(P'_{j_1} \cdot P'_{j_2})$ can be computed by

$$\begin{aligned}(P'_{j_1} \cdot P'_{j_2}) = {}&\deg(\gcd(x_{j_1} - x_{j_2}, y_{j_1} - y_{j_2}))\\ &+ \min\{4 - \deg(x_{j_1} - x_{j_2}), 6 - \deg(y_{j_1} - y_{j_2})\}.\end{aligned}$$

Thus, we obtain the following Gram matrix R_6 with determinant $2^4 \cdot 3^4$ of the height pairing for the P_j''s and hence for the P_j's:

$$R_6 = \begin{pmatrix}
4 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 4 & 0 & 0 & -2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 4 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
2 & 2 & 0 & 0 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & -2 & 2 & 0 & 4 & 2 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 2 & 0 & 2 & 4 & 2 & 0 & 0 & 0 & -1 & -2 & 0 & 0 & -1 \\
0 & 0 & 2 & 0 & 2 & 0 & 2 & 4 & 0 & 0 & 0 & -1 & -1 & -1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & -2 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & 0 & 0 & 0 & 4 & 0 & 2 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -2 & -1 & 2 & 2 & 0 & 0 & 4 & 0 & 0 & 2 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -2 & 2 & 0 & 4 & 2 & 0 \\
0 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 2 & 4 & 2 \\
0 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 4
\end{pmatrix}.$$

Thus, the points P_j's, $j = 1, \ldots, 16$, form a set of linearly independent generators of $\mathcal{E}_6$ over $\mathcal{K}_6(t)$. We refer the reader to see [4, check-6] for all computations in this section.

References

[1] A. KUMAR & M. KUWATA, "Elliptic $K3$ surfaces associated with the product of two elliptic curves: Mordell–Weil lattices and their fields of definition", *Nagoya Math. J.* **228** (2017), p. 124-185.

[2] MAPLESOFT, A DIVISION OF WATERLOO MAPLE INC. , "Maple", 2025, `https://www.maplesoft.com`.

[3] THE PARI GROUP, "PARI/GP version `2.17.3`", 2025, available from `http://pari.math.u-bordeaux.fr/`.

[4] S. SALAMI, "Checking codes for computations", `https://github.com/sajadsalami/K3Surface-Check-Codes`, 2025.

[5] ———, "The splitting field and generators of the elliptic surface $Y^2 = X^3 + t^{360} + 1$", 2025, `https://arxiv.org/abs/2512.25009`.

[6] S. SALAMI & A. SHAMSI ZARGAR, "The splitting fields and generators of Shioda's elliptic surfaces $y^2 = x^3 + t^m + 1$ (I)", 2025, `https://arxiv.org/abs/2512.16578`.

[7] M. SCHÜTT & T. SHIODA, *Mordell–Weil lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 70, Springer, 2019, xvi+431 pages.

[8] T. SHIODA, "On the Mordell–Weil lattices", *Comment. Math. Univ. St. Pauli* **39** (1990), no. 2, p. 211-240.

[9] ———, "Construction of elliptic curves with high rank via the invariants of the Weyl groups", *J. Math. Soc. Japan* **43** (1991), no. 4, p. 673-719.

[10] ———, "A note on $K3$ surfaces and sphere packings", *Proc. Japan Acad., Ser. A* **76** (2000), no. 5, p. 68-72.

[11] ———, "Correspondence of elliptic curves and Mordell–Weil lattices of certain elliptic $K3$'s", in *Algebraic cycles and motives. Vol. 2. Selected papers of the EAGER conference, Leiden, Netherlands, Aug. 30–Sep. 3, 2004 on the occasion of the 75th birthday of Prof. J. P. Murre*, London Mathematical Society Lecture Note Series, vol. 344, Cambridge University Press, 2007, p. 319-339.

[12] ———, "$K3$ surfaces and sphere packings", *J. Math. Soc. Japan* **60** (2008), no. 4, p. 1083-1105.

[13] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.

[14] H. Usui, "On the Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + t^m + 1$. IV", *Comment. Math. Univ. St. Pauli* **57** (2008), no. 1, p. 23-63.

Sajad Salami
Institute of Mathematics and Statistics,
State University of Rio de Janeiro,
Rio Janeiro, RJ, Brazil
E-mail: sajad.salami@ime.uerj.br
URL: https://sites.google.com/a/ime.uerj.br/sajadsalami/home

Arman Shamsi Zargar
Department of Mathematics and Applications,
Faculty of Mathematical Sciences,
University of Mohaghegh Ardabili, Ardabil, Iran
E-mail: zargar@uma.ac.ir