Michigan Math. J. 63 (2014), 803–844

On the Supersingular $K3$ Surface in Characteristic 5 with Artin Invariant 1

Toshiyuki Katsura, Shigeyuki Kondo, & Ichiro Shimada

Dedicated to Professor Igor V. Dolgachev on the occasion of his 70th birthday.

Abstract. We present three interesting projective models of the supersingular $K3$ surface X in characteristic 5 with Artin invariant 1. For each projective model, we determine smooth rational curves on X with the minimal degree and the projective automorphism group. Moreover, by using the superspecial Abelian surface we construct six sets of 16 disjoint smooth rational curves on X and show that they form a beautiful configuration.

1. Introduction

Let Y be a $K3$ surface defined over an algebraically closed field k, and $\rho(Y)$ the Picard number of Y. Then it is well known that $1 \leq \rho(Y) \leq 20$ or $\rho(Y) = 22$. The last case $\rho(Y) = 22$ occurs only when k is of positive characteristic. A $K3$ surface is called *supersingular* if its Picard number is 22. Let Y be a supersingular $K3$ surface in characteristic $p \geq 3$. Let S_Y denote its Néron–Severi lattice, and let $S_Y^\vee$ be the dual of S_Y. Then Artin [1] proved that $S_Y^\vee/S_Y$ is a p-elementary Abelian group of rank 2σ, where σ is an integer such that $1 \leq \sigma \leq 10$. This integer σ is called the *Artin invariant* of Y. It is known that the isomorphism class of S_Y depends only on p and σ (Rudakov and Shafarevich [26]). On the other hand, supersingular $K3$ surfaces with Artin invariant σ form a $(\sigma - 1)$-dimensional family, and a supersingular $K3$ surface with Artin invariant 1 in characteristic p is unique up to isomorphisms (Ogus [24; 25], Rudakov and Shafarevich [26]).

Supersingular $K3$ surfaces in *small* characteristic p with Artin invariant 1 are especially interesting because big finite groups act on them by automorphisms. (See Dolgachev and Keum [11].) For example, the group $\mathrm{PGL}(3, \mathbb{F}_4) \ltimes \mathbb{Z}/2\mathbb{Z}$ in case $p = 2$ or $\mathrm{PGU}(4, \mathbb{F}_9)$ in case $p = 3$ acts on the $K3$ surface by automorphisms. Moreover, these $K3$ surfaces contain a finite set of smooth rational curves on which the above group acts as symmetries. For example, in case $p = 2$, there exist 42 smooth rational curves that form a (21_5)-configuration (see Dolgachev and Kondo [12], Katsura and Kondo [16]). In case $p = 3$, the Fermat quartic surface is a supersingular $K3$ surface with Artin invariant 1, and it contains 112 lines (e.g., Katsura and Kondo [15], Kondo and Shimada [19]).

Received November 26, 2013. Revision received September 6, 2014.

Research partially supported by JSPS Grants-in-Aid for Scientific Research (C) No. 24540053, (S) No. 22224001, (C) No. 25400042.

In this paper we consider a similar problem for the supersingular $K3$ surface in characteristic 5 with Artin invariant 1. We work over an algebraically closed field k of characteristic 5 containing the finite field $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2})$. Let C_F be the Fermat sextic curve in $\mathbb{P}^2$ defined by

$$x^6 + y^6 + z^6 = 0. \tag{1.1}$$

Note that the left-hand side of equation (1.1) is a Hermitian form over $\mathbb{F}_{25}$ and the projective unitary group $\mathrm{PGU}(3, \mathbb{F}_{25})$ acts on C_F by automorphisms. Let $\pi_F : X \to \mathbb{P}^2$ be the double cover of $\mathbb{P}^2$ branched along C_F. Then X is a supersingular $K3$ surface in characteristic 5 with Artin invariant 1, on which the finite group $\mathrm{PGU}(3, \mathbb{F}_{25}) \ltimes \mathbb{Z}/2\mathbb{Z}$ acts by automorphisms (e.g., Dolgachev and Keum [11]). Let P be an $\mathbb{F}_{25}$-rational point of C_F. Then the tangent line ℓ_P to C_F at P intersects C_F at P with multiplicity 6. Hence, the pullback of ℓ_P on X splits into two smooth rational curves meeting at one point with multiplicity 3. Since the number of $\mathbb{F}_{25}$-rational points of C_F is 126, we obtain 252 smooth rational curves on X.

The main result of this paper is to exhibit three projective models of X and determine smooth rational curves of minimal degree on X with respect to the corresponding polarizations.

THEOREM 1.1. *There exist three polarizations h_F, h_1, h_2 of degree* 2, 60, 80 *on X satisfying the following conditions*:

(1) *The projective model (X, h_F) is the double cover of $\mathbb{P}^2$ branched along C_F. Here $h_F \in S_X$ is the class of the pullback of a line on $\mathbb{P}^2$ by the covering morphism $\pi_F : X \to \mathbb{P}^2$. The projective automorphism group* $\mathrm{Aut}(X, h_F)$ *of (X, h_F) is a central extension of* $\mathrm{PGU}(3, \mathbb{F}_{25})$ *by the cyclic group of order* 2 *generated by the deck-transformation of X over $\mathbb{P}^2$. The double plane (X, h_F) contains exactly* 252 *smooth rational curves of degree* 1, *on which* $\mathrm{Aut}(X, h_F)$ *acts transitively.*
(2) *The projective automorphism group of (X, h_1) is isomorphic to the alternating group $\mathfrak{A}_8$. The minimal degree of curves on (X, h_1) is* 5, *and (X, h_1) contains exactly* 168 *smooth rational curves of degree* 5, *on which* $\mathrm{Aut}(X, h_1)$ *acts transitively.*
(3) *The projective automorphism group of (X, h_2) is isomorphic to*

$$(\mathbb{Z}/2\mathbb{Z})^4 \rtimes (\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_4)$$

of order 1,152. *The minimal degree of curves on (X, h_2) is* 5, *and (X, h_2) contains exactly* 96 *smooth rational curves of degree* 5, *which decompose into two orbits under the action of* $\mathrm{Aut}(X, h_2)$.

The model (X, h_F) has been known as mentioned before. However, we give another proof of the existence of such a polarization h_F on X by using the Borcherds method [3; 4] and a geometry of the Leech lattice.

The set of the 96 smooth rational curves in Theorem 1.1(3) possesses the following remarkable property. Let $\mathcal{S}$ and $\mathcal{S}'$ be two sets of disjoint 16 smooth rational curves on a $K3$ surface. We say that $\mathcal{S}$ and $\mathcal{S}'$ form a (16_r)-configuration if every member in one set intersects exactly r members in the other set with multiplicity 1 and is disjoint from the remaining $16 - r$ members. For example, a (16_6)-configuration appears in the theory of Kummer surfaces associated to the Jacobian of a smooth curve of genus two: sixteen 2-torsion points on the Jacobian, the theta divisor, and its translations by 2-torsion points (Chapter 6 of Griffiths and Harris [13], and Dolgachev [10]).

THEOREM 1.2. *There exist six sets*

$$\mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{02}, \mathcal{S}_{10}, \mathcal{S}_{11}, \mathcal{S}_{12}$$

of disjoint 16 *smooth rational curves on X with the following properties.*

(a) *If $i \neq j$, then $\mathcal{S}_{\nu i}$ and $\mathcal{S}_{\nu j}$ form a* (16_6)*-configuration for* $\nu = 0$ *and* 1.
(b) *For* $i = 0, 1, 2$, *the sets $\mathcal{S}_{0i}$ and $\mathcal{S}_{1i}$ form a* (16_{12})*-configuration.*
(c) *If $i \neq j$, then $\mathcal{S}_{0i}$ and $\mathcal{S}_{1j}$ form a* (16_4)*-configuration.*

In fact, the set of the 96 smooth rational curves of degree 5 on (X, h_2) decomposes into the disjoint union of six sets with the properties (a), (b), (c).

Since $h_2^2 = 80$, however, it is difficult to present these curves explicitly. Instead, we construct the six sets with the properties (a), (b), (c) on the Kummer surface model of X. Let E be the elliptic curve defined by $y^2 = x^3 - 1$, and let A be the product Abelian surface $E \times E$. It is well known that X is isomorphic to the Kummer surface $\mathrm{Km}(A)$ associated with A. In Section 8, we construct these six sets explicitly on $\mathrm{Km}(A)$ by giving the pullback of rational curves by the rational map $A \cdots\to \mathrm{Km}(A)$. As a corollary of this construction, we have the following result. Let $\mathbb{P}^1$ be a projective line over $\mathbb{F}_{25}$ with an affine parameter. We define four subsets of $\mathbb{P}^1(\mathbb{F}_{25})$ as follows:

$$\begin{aligned} P_6 &= \{\infty, 0, 1, 2, 3, 4\}, \\ P_4 &= \left\{\sqrt{2}, 1 + 2\sqrt{2}, 3 + 3\sqrt{2}, 4 + 4\sqrt{2}\right\}, \\ \bar{P}_4 &= \left\{4\sqrt{2}, 1 + 3\sqrt{2}, 3 + 2\sqrt{2}, 4 + \sqrt{2}\right\}, \\ P_{12} &= \mathbb{P}^1(\mathbb{F}_{25}) \setminus (P_6 \cup P_4 \cup \bar{P}_4). \end{aligned}$$

They are mutually disjoint. See Remark 8.9 for the geometric characterization of the decomposition $\mathbb{P}^1(\mathbb{F}_{25}) = P_6 \cup P_4 \cup \bar{P}_4 \cup P_{12}$.

THEOREM 1.3. *There exist a model of* $\mathrm{Km}(A)$ *defined over* $\mathbb{F}_{25}$ *and a set $\mathcal{S}$ of the* 96 *rational curves defined over* $\mathbb{F}_{25}$ *on* $\mathrm{Km}(A)$ *that admits a decomposition into disjoint six subsets* $\mathcal{S}_{\nu i}$ ($\nu = 0, 1$ *and* $i = 0, 1, 2$) *satisfying* (a), (b), (c) *of Theorem 1.2. Moreover, any intersection point of two curves in $\mathcal{S}$ is an $\mathbb{F}_{25}$-rational point, and, for each Γ in $\mathcal{S}_{\nu i}$, the set $\Gamma(\mathbb{F}_{25})$ of $\mathbb{F}_{25}$-rational points on Γ are decomposed into the union of disjoint four sets Γ_ν, $\Gamma_{\mu i}$, $\Gamma_{\mu j}$, and $\Gamma_{\mu k}$ ($\mu \neq$ and $j \neq k \neq i \neq j$) with the following properties.*

(i) $|\Gamma_\nu| = 6$, $|\Gamma_{\mu i}| = 12$, $|\Gamma_{\mu j}| = |\Gamma_{\mu k}| = 4$.
(ii) *For any point p in Γ_ν and each $i' \neq i$, there exists exactly one curve in $\mathcal{S}_{\nu i'}$ passing through p. For any point p' in $\Gamma_{\mu i}$, there exists exactly one curve*

in $\mathcal{S}_{\mu i}$ *passing through* p'. *For any point* p'' *in* $\Gamma_{\mu j}$ (*resp.* $\Gamma_{\mu k}$), *there exists exactly one curve in* $\mathcal{S}_{\mu j}$ (*resp.* $\mathcal{S}_{\mu k}$) *passing through* p''.

(iii) *There exists an isomorphism* $\phi : \Gamma \xrightarrow{\sim} \mathbb{P}^1$ *defined over* $\mathbb{F}_{25}$ *such that* $\phi^{-1}(P_6) = \Gamma_\nu$, $\phi^{-1}(P_{12}) = \Gamma_{\mu i}$, $\phi^{-1}(P_4) = \Gamma_{\mu j}$, *and* $\phi^{-1}(\bar{P}_4) = \Gamma_{\mu k}$.

We give three different proofs of the existence of the 96 smooth rational curves mentioned in Theorem 1.2. We do not know whether such sets of 96 curves coincide under the action of the group of automorphisms of X.

By using the Borcherds method [3; 4], the groups of automorphisms of some $K3$ surfaces were calculated (Kondo [18], Keum and Kondo [17], Dolgachev and Kondo [12], Kondo and Shimada [19], Ujigawa [34]). In all cases, the Néron–Severi lattice of each $K3$ surface is isomorphic to the orthogonal complement of a root lattice in L, where L is an even unimodular lattice of signature $(1, 25)$. See Lemma 5.1 of [3], in which Borcherds gave a sufficient condition for the restrictions of standard fundamental domains of the reflection group of L to the positive cone of the $K3$ surface to be conjugate to each other under the action of the orthogonal group of the Néron–Severi lattice. Contrary to these cases, a new phenomenon occurs in the present case of the supersingular $K3$ surface in characteristic 5 with Artin invariant 1: there exist at least three nonconjugate chambers obtained by the restriction of fundamental domains (see also Section 4.6). The projective models in Theorem 1.1 correspond to these three nonconjugate chambers. This phenomenon also happens in the case of the complex Fermat quartic surface.

The plan of this paper is as follows. In Section 2, we recall some lattice theory, which will be used in this paper. Section 3 is devoted to the explanation of the Borcherds method for finding a finite polyhedron in the positive cone of a hyperbolic lattice primitively embedded into the even unimodular lattice L of signature $(1, 25)$. In Section 4, we apply this method to the case of the supersingular $K3$ surface in characteristic 5 with Artin invariant 1. In particular, by using computer, we give a proof of Theorems 1.1 and 1.2. In Section 5, by using a geometry of Leech lattice, we give another proof of Theorems 1.1 and 1.2 without using computer. In Section 6, we recall some facts on the supersingular elliptic curve in characteristic 5, and in Section 7, we investigate $\mathbb{F}_{p^2}$-rational points on the Kummer surface associated with the product of two supersingular elliptic curves. Section 8 is devoted to give another proof of Theorem 1.2 by using the Kummer surface structure of X. Moreover, we study the intersection between the 96 smooth rational curves and prove Theorem 1.3.

In Sections 4 and 8, we use computer for the proof of main results. The computational data are presented in [30].

2. Lattices

A $\mathbb{Q}$-*lattice* is a pair $(M, \langle \cdot, \cdot \rangle_M)$ of a free $\mathbb{Z}$-module M of finite rank and a nondegenerate symmetric bilinear form $\langle \cdot, \cdot \rangle_M : M \times M \to \mathbb{Q}$. We omit the bilinear form $\langle \cdot, \cdot \rangle_M$ or the subscript M in $\langle \cdot, \cdot \rangle_M$ if no confusions will occur. If $\langle \cdot, \cdot \rangle$ takes values in $\mathbb{Z}$, M is called a *lattice.* For $x \in M \otimes \mathbb{R}$, we call $x^2 = \langle x, x\rangle$ the *norm* of x. A lattice M is *even* if $x^2 \in 2\mathbb{Z}$ for all $x \in M$.

Let M be a lattice of rank r. The signature of M is the signature of the real quadratic space $M \otimes \mathbb{R}$. We say that M is *negative definite* if $M \otimes \mathbb{R}$ is negative definite, and M is *hyperbolic* if the signature is $(1, r-1)$. A *Gram matrix* of M is an $r \times r$ matrix with entries $\langle e_i, e_j\rangle$, where $\{e_1, \dots, e_r\}$ is a basis of M. The determinant of a Gram matrix of M is called the *discriminant* of M.

Let M be an even lattice, and let $M^\vee = \mathrm{Hom}(M, \mathbb{Z})$ be naturally identified with a submodule of $M \otimes \mathbb{Q}$ with extended symmetric bilinear form. We call this $\mathbb{Q}$-lattice $M^\vee$ the *dual lattice* of M. The *discriminant group* of M is defined to be the quotient $M^\vee/M$ and is denoted by A_M. The order of A_M is equal to the discriminant of M up to sign. A lattice M is called *unimodular* if A_M is trivial, whereas M is called *p-elementary* if A_M is p-elementary.

For an even lattice M, the *discriminant quadratic form* of M

$$q_M : A_M \to \mathbb{Q}/2\mathbb{Z}$$

is defined by $q_M(x \bmod M) = x^2 \bmod 2\mathbb{Z}$.

A submodule N of M is called *primitive* if M/N is torsion free. A nonzero vector $v \in M$ is called *primitive* if the submodule of M generated by v is primitive.

Let $\mathrm{O}(M)$ be the orthogonal group of a lattice M; that is, the group of isomorphisms of M preserving $\langle \cdot, \cdot \rangle$. We assume that $\mathrm{O}(M)$ acts on M from the *right,* and the action of $g \in \mathrm{O}(M)$ on $v \in M \otimes \mathbb{R}$ is denoted by $v \mapsto v^g$. Similarly, $\mathrm{O}(q_M)$ denotes the group of isomorphisms of A_M preserving q_M. There is a natural homomorphism $\mathrm{O}(M) \to \mathrm{O}(q_M)$.

Let M be a hyperbolic lattice. A *positive cone* of M is one of the two connected components of the set

$$\{x \in M \otimes \mathbb{R} \mid x^2 > 0\}.$$

Let $\mathcal{P}_M$ be a positive cone of M. We denote by $\mathrm{O}^+(M)$ the group of isometries of M preserving $\mathcal{P}_M$. Then $\mathrm{O}(M) = \mathrm{O}^+(M) \times \{\pm 1\}$. For a vector $v \in M \otimes \mathbb{R}$ with $v^2 < 0$, we define

$$(v)^\perp = \{x \in \mathcal{P}_M \mid \langle x, v\rangle = 0\},$$

which is a real hyperplane of $\mathcal{P}_M$. An isometry $g \in \mathrm{O}^+(M)$ is called a *reflection with respect to* v or a *reflection into* $(v)^\perp$ if g is of order 2 and fixes each point of $(v)^\perp$. For a lattice M, the set of (-2)-vectors is denoted by $\mathcal{R}_M$. Any element r of $\mathcal{R}_M$ defines a reflection

$$s_r : x \mapsto x + \langle x, r\rangle r$$

with respect to r. We denote by $W^{(-2)}(M)$ the group generated by the set of reflections $\{s_r \mid r \in \mathcal{R}_M\}$. Since s_r preserves $\mathcal{P}_M$, $W^{(-2)}(M)$ is a subgroup of $\mathrm{O}^+(M)$. It is obvious that $W^{(-2)}(M)$ is normal in $\mathrm{O}^+(M)$.

A negative definite even lattice M is said to be a *root lattice* if M is generated by $\mathcal{R}_M$.

3. Borcherds Method

In this section, we review the Borcherds method [3; 4] and the algorithms in [29].

We define some notions and fix some notation. Let M be an even hyperbolic lattice with a fixed positive cone $\mathcal{P}_M$. Let $\mathcal{V}$ be a set of vectors $v \in M \otimes \mathbb{R}$ with $v^2 < 0$. Suppose that the family of hyperplanes

$$\mathcal{V}^* = \{(v)^\perp \mid v \in \mathcal{V}\}$$

is locally finite in $\mathcal{P}_M$. By a $\mathcal{V}^*$*-chamber* we mean a closure in $\mathcal{P}_M$ of a connected component of

$$\mathcal{P}_M \setminus \bigcup_{v \in \mathcal{V}} (v)^\perp.$$

Let D be a $\mathcal{V}^*$-chamber. A hyperplane $(v)^\perp$ is said to be a *wall* of D if $(v)^\perp$ is disjoint from the interior of D and $(v)^\perp \cap D$ contains a nonempty open subset of $(v)^\perp$.

Recall that $\mathcal{R}_M$ is the set of vectors $r \in M$ with $r^2 = -2$. Then each $\mathcal{R}_M^*$-chamber is a fundamental domain of the action of $W^{(-2)}(M)$ on $\mathcal{P}_M$.

3.1. Conway–Borcherds Theory

Let L be an even unimodular hyperbolic lattice of rank 26. Note that L is unique up to isomorphisms. Let $\mathcal{P}_L$ be a positive cone of L. An $\mathcal{R}_L^*$-chamber will be called a *Conway chamber.* A nonzero primitive vector $w \in L$ with $w^2 = 0$ is called a *Weyl vector* if w is contained in the closure $\overline{\mathcal{P}}_L$ of $\mathcal{P}_L$ in $L \otimes \mathbb{R}$ and the even negative-definite unimodular lattice $\langle w \rangle^\perp / \langle w \rangle$ is isomorphic to the (negative-definite) Leech lattice (i.e., $\langle w \rangle^\perp / \langle w \rangle$ contains no (-2)-vectors). For a Weyl vector w, we put

$$\Delta(w) = \{r \in \mathcal{R}_L \mid \langle r, w \rangle = 1\}. \tag{3.1}$$

Conway and Sloane [8] and Conway [6] proved the following:

THEOREM 3.1. *If w is a Weyl vector, then*

$$\mathcal{D}(w) = \{x \in \mathcal{P}_L \mid \langle r, x \rangle \geq 0 \textit{ for any } r \in \Delta(w)\}$$

is a Conway chamber, and $\{(r)^\perp \mid r \in \Delta(w)\}$ is the set of walls of $\mathcal{D}(w)$. For any Conway chamber $\mathcal{D}$, there exists a unique Weyl vector w such that $\mathcal{D} = \mathcal{D}(w)$.

Let S be an even hyperbolic lattice of rank < 26. Suppose that S is primitively embedded into L. Let $\mathcal{P}_S$ be the positive cone of S that is contained in $\mathcal{P}_L$. Let R denote the orthogonal complement of S in L. For $x \in L \otimes \mathbb{R}$, we denote by

$$x \mapsto x_S \quad \text{and} \quad x \mapsto x_R$$

the projections to $S \otimes \mathbb{R}$ and $R \otimes \mathbb{R}$, respectively. Note that, if $v \in L$, then $v_S \in S^\vee$ and $v_R \in R^\vee$. We assume the following:

(i) The negative-definite lattice R cannot be embedded into the Leech lattice. (E.g., this condition is satisfied if $\mathcal{R}_R \neq \emptyset$.)

(ii) The natural homomorphism $\mathrm{O}(R) \to \mathrm{O}(q_R)$ is surjective.

We put

$$\mathcal{R}_{L|S} = \{r_S \mid r \in \mathcal{R}_L, \langle r_S, r_S\rangle < 0\}.$$

It is easy to see that the family of hyperplanes $\mathcal{R}^*_{L|S}$ is locally finite in $\mathcal{P}_S$. A Conway chamber $\mathcal{D}$ is said to be *S-nondegenerate* if $\mathcal{D}\cap\mathcal{P}_S$ contains a nonempty open subset of $\mathcal{P}_S$. If $\mathcal{D}$ is an S-nondegenerate Conway chamber, then $D = \mathcal{D}\cap\mathcal{P}_S$ is an $\mathcal{R}^*_{L|S}$-chamber of $\mathcal{P}_S$, which is called an *induced chamber.* Since $\mathcal{P}_L$ is tessellated by Conway chambers, $\mathcal{P}_S$ is tessellated by induced chambers. Since $\mathcal{R}_S$ is a subset of $\mathcal{R}_{L|S}$, any $\mathcal{R}^*_S$-chamber is a union of induced chambers. We have the following. See [29].

PROPOSITION 3.2. (1) *Any induced chamber has only a finite number of walls.*

(2) *The automorphism group* $\mathrm{Aut}(D) = \{g \in \mathrm{O}^+(S) \mid D^g = D\}$ *of an induced chamber D is a finite group.*

In [29], we have presented algorithms to calculate the set of walls and the automorphism group of an induced chamber. Moreover, by an algorithm in [29], if we have that:

- a Weyl vector $w \in L$ such that $\mathcal{D}(w)$ is S-nondegenerate and
- a wall $(v)^\perp$ of the induced chamber $D = \mathcal{D}(w)\cap\mathcal{P}_S$,

then we can calculate a Weyl vector $w' \in L$ such that $D' = \mathcal{D}(w')\cap\mathcal{P}_S$ is the induced chamber adjacent to D along the wall $(v)^\perp$.

3.2. Periods and Automorphisms of Supersingular $K3$ Surfaces

Let Y be a supersingular $K3$ surface defined over an algebraically closed field k of odd characteristic p with Artin invariant σ, and let S_Y denote the Néron–Severi lattice of Y. Since $S_Y^\vee/S_Y$ is p-elementary, we have $pS_Y^\vee \subset S_Y$. Consider the 2σ-dimensional $\mathbb{F}_p$-vector space

$$S_0 = pS_Y^\vee/pS_Y \subset S_Y \otimes_{\mathbb{Z}} \mathbb{F}_p,$$

on which we have an $\mathbb{F}_p$-valued quadratic form $Q_0 : S_0 \to \mathbb{F}_p$ defined by

$$Q_0 : px \bmod pS_Y \mapsto px^2 \bmod p \quad (x \in S_Y^\vee).$$

Let $\bar{c}_{\mathrm{DR}} : S_Y \otimes k \to H^2_{\mathrm{DR}}(Y)$ be the Chern class map. Then $\mathrm{Ker}(\bar{c}_{\mathrm{DR}})$ is a σ-dimensional isotropic subspace of $Q_0 \otimes k$. Let $\phi : S_0 \otimes k \to S_0 \otimes k$ denote the map $\mathrm{id} \otimes F_k$, where F_k is the Frobenius of k.

DEFINITION 3.3. The *period* $\mathcal{K}_Y$ of Y is defined to be $\phi^*(\mathrm{Ker}(\bar{c}_{\mathrm{DR}}))$.

Note that $\mathrm{O}(S_Y)$ acts on (S_0, Q_0) naturally. We put

$$G_Y = \{g \in \mathrm{O}(S_Y) \mid \mathcal{K}_Y^g = \mathcal{K}_Y\}.$$

We denote by $\mathcal{P}_{S_Y}$ the positive cone of S_Y containing an ample class of Y. Let $\mathrm{NC}(Y)$ denote the intersection of $\mathcal{P}_{S_Y}$ with the nef cone of Y,

$$\mathrm{NC}(Y) = \{x \in \mathcal{P}_{S_Y} \mid \langle x, C\rangle \geq 0 \text{ for any curve } C \text{ on } Y\}.$$

We put

$$\mathrm{Aut}(\mathrm{NC}(Y)) = \{g \in \mathrm{O}^+(S_Y) \mid \mathrm{NC}(Y)^g = \mathrm{NC}(Y)\}.$$

Thanks to the Torelli theorem by Ogus [24; 25] for supersingular $K3$ surfaces in odd characteristics, we see that the natural action of $\mathrm{Aut}(Y)$ on S_Y identifies $\mathrm{Aut}(Y)$ with

$$\mathrm{Aut}(\mathrm{NC}(Y)) \cap G_Y.$$

Now suppose that S_Y is embedded into L in such a way that conditions (i) and (ii) in Section 3.1 are satisfied and that the image of $\mathrm{NC}(Y)$ is contained in $\mathcal{P}_L$. It is well known that $\mathrm{NC}(Y)$ is an $\mathcal{R}^*_{S_Y}$-chamber in $\mathcal{P}_{S_Y}$. (See, e.g., Rudakov and Shafarevich [26].) Hence, $\mathrm{NC}(Y)$ is tessellated by induced chambers. For an induced chamber D contained in $\mathrm{NC}(Y)$, we put

$$\mathrm{Aut}_Y(D) = \mathrm{Aut}(D) \cap G_Y.$$

Then $\mathrm{Aut}_Y(D)$ is a finite subgroup of $\mathrm{Aut}(Y) = \mathrm{Aut}(\mathrm{NC}(Y)) \cap G_Y$. More precisely, if $v \in D \cap S_Y$ is a vector in the interior of D, then

$$h_D = \sum_{g \in \mathrm{Aut}_Y(D)} v^g$$

is an ample class, and $\mathrm{Aut}_Y(D)$ is the automorphism group $\mathrm{Aut}(Y, h_D)$ of the polarized $K3$ surface (Y, h_D). We have an algorithm to make the complete list of elements of $\mathrm{Aut}(D)$. Hence, in order to calculate $\mathrm{Aut}(Y, h_D)$, all we have to do is to calculate the action of $\mathrm{O}(S_Y)$ on the period $\mathcal{K}_Y$.

We say that two induced chambers D and D' are *G_Y-congruent* if there exists $g \in G_Y$ such that $D^g = D'$. The number of G_Y-congruence classes is finite. If we obtain the list of all G_Y-congruence classes, we can determine the automorphism group of Y. (As is explained in Introduction, in the previous works of computing automorphism groups of $K3$ surfaces using this technique, there exists only one $O^+(S_Y)$-congruence class.) See [29] and Section 4.6.

4. Proof of Theorems by Computer

In this section and the next, we prove Theorems 1.1 and 1.2 by calculating some induced chambers. In this section, we give a proof based on the algorithm presented in [29].

4.1. The Néron–Severi Lattice and the Period of X

Using the projective model (X, h_F), we calculate the Néron–Severi lattice S_X and the period $\mathcal{K}_X$ of X explicitly.

As is explained in the Introduction, the surface X contains 252 smooth rational curves Γ such that $\langle \Gamma, h_F \rangle = 1$. We call these smooth rational curves *h_F-lines*. The h_F-lines are labeled as follows. Let $\pi_F : X \to \mathbb{P}^2$ denote the double covering. Part of the $\mathbb{F}_{25}$-rational points $P_1, \dots, P_{126}$ on the Fermat curve C_F of degree 6 are given explicitly in Table 1. Let l_i be the line on $\mathbb{P}^2$ tangent to C_F at P_i. We put

$$l_1^+ = \{w = x^3, y = 3z\} \subset X,$$

Table 1 $\mathbb{F}_{25}$-rational points on C_F

$P_1 := [0:1:2]$	$P_2 := [0:1:3]$	$P_3 := [0:1:1+\sqrt{2}]$
$P_4 := [0:1:4+\sqrt{2}]$	$P_5 := [0:1:1+4\sqrt{2}]$	$P_6 := [0:1:4+4\sqrt{2}]$
$P_7 := [1:0:2]$	$P_8 := [1:0:3]$	$P_9 := [1:0:1+\sqrt{2}]$
$P_{10} := [1:0:4+\sqrt{2}]$	$P_{11} := [1:0:1+4\sqrt{2}]$	$P_{12} := [1:0:4+4\sqrt{2}]$
$P_{13} := [1:1:\sqrt{2}]$	$P_{14} := [1:1:1+2\sqrt{2}]$	$P_{15} := [1:1:4+2\sqrt{2}]$
$P_{16} := [1:1:1+3\sqrt{2}]$	$P_{17} := [1:1:4+3\sqrt{2}]$	$P_{18} := [1:1:4\sqrt{2}]$
$P_{19} := [1:2:0]$	$P_{20} := [1:3:0]$	$P_{21} := [1:4:\sqrt{2}]$
$P_{22} := [1:4:1+2\sqrt{2}]$	$P_{23} := [1:4:4+2\sqrt{2}]$	$P_{24} := [1:4:1+3\sqrt{2}]$
$P_{25} := [1:4:4+3\sqrt{2}]$	$P_{26} := [1:4:4\sqrt{2}]$	$P_{27} := [1:\sqrt{2}:1]$
$P_{28} := [1:\sqrt{2}:4]$	$P_{29} := [1:\sqrt{2}:2+2\sqrt{2}]$	$P_{30} := [1:\sqrt{2}:3+2\sqrt{2}]$
$P_{31} := [1:\sqrt{2}:2+3\sqrt{2}]$	$P_{32} := [1:\sqrt{2}:3+3\sqrt{2}]$	$P_{33} := [1:1+\sqrt{2}:0]$
$P_{34} := [1:2+\sqrt{2}:2+\sqrt{2}]$	$P_{35} := [1:2+\sqrt{2}:3+\sqrt{2}]$	$P_{36} := [1:2+\sqrt{2}:2\sqrt{2}]$
$P_{37} := [1:2+\sqrt{2}:3\sqrt{2}]$	$P_{38} := [1:2+\sqrt{2}:2+4\sqrt{2}]$	$P_{39} := [1:2+\sqrt{2}:3+4\sqrt{2}]$
…	…	…
…	…	…
$P_{124} := [1:3+4\sqrt{2}:2+4\sqrt{2}]$	$P_{125} := [1:3+4\sqrt{2}:3+4\sqrt{2}]$	$P_{126} := [1:4+4\sqrt{2}:0]$

which is an irreducible component of $\pi_F^*(l_1)$, and let l_1^- denote the other irreducible component. For $i > 1$, let l_i^+ be the irreducible component of $\pi_F^*(l_i)$ such that $\langle [l_1^+], [l_i^+] \rangle = 1$, and let l_i^- be the other irreducible component. Consider the following twenty-two h_F-lines:

$$\ell_1 = l_1^+, \quad \ell_2 = l_1^-, \quad \ell_3 = l_2^+, \quad \ell_4 = l_3^+, \quad \ell_5 = l_4^+, \quad \ell_6 = l_5^+, \quad \ell_7 = l_7^+,$$
$$\ell_8 = l_8^+, \quad \ell_9 = l_9^+, \quad \ell_{10} = l_{10}^+, \quad \ell_{11} = l_{13}^+, \quad \ell_{12} = l_{14}^+, \quad \ell_{13} = l_{15}^+,$$
$$\ell_{14} = l_{16}^+, \quad \ell_{15} = l_{17}^+, \quad \ell_{16} = l_{19}^+, \quad \ell_{17} = l_{21}^+, \quad \ell_{18} = l_{22}^+, \quad \ell_{19} = l_{24}^+,$$
$$\ell_{20} = l_{25}^+, \quad \ell_{21} = l_{27}^+, \quad \ell_{22} = l_{34}^+.$$

Their intersection matrix is of determinant -25. Hence, the classes of these h_F-lines form a basis of S_X. The Gram matrix G_S of S_X with respect to this basis $[\ell_1], \dots, [\ell_{22}]$ is given in Table 2. An element of $S_X \otimes \mathbb{R}$ is usually written as a row vector $[x_1, \dots, x_{22}]$ with respect to the basis $[\ell_1], \dots, [\ell_{22}]$, whereas when it is written with respect to the *dual* basis $[\ell_1]^\vee, \dots, [\ell_{22}]^\vee$, we use the notation $[\xi_1, \dots, \xi_{22}]^\vee$. For example, we have

$$\begin{aligned} h_F &= [1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] \\ &= [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]^\vee, \\ [l_7^-] &= [1,1,0,0,0,0,-1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] \\ &= [0,1,1,1,0,1,3,1,1,0,1,1,1,1,1,1,1,0,0,0,0,1]^\vee, \\ [l_{14}^+] &= [0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0] \\ &= [1,0,1,0,1,0,0,1,0,0,1,-2,0,0,1,1,0,1,1,0,1,1]^\vee. \end{aligned}$$

We let $\mathrm{O}(S_X)$ act on S_X from the *right,* so that we have

$$\mathrm{O}(S_X) = \{g \in \mathrm{GL}_{22}(\mathbb{Z}) \mid g \cdot \mathrm{G}_S \cdot {}^t g = \mathrm{G}_S\}.$$

Table 2 Gram matrix of S_X

−2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	−2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	−2	1	1	1	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0
1	0	1	−2	1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1
1	0	1	1	−2	1	1	1	1	1	0	1	0	0	0	1	1	0	0	1	0	0
1	0	1	1	1	−2	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
1	0	0	0	1	0	−2	0	0	1	0	0	0	0	0	0	0	1	1	1	1	0
1	0	0	0	1	0	0	−2	1	0	0	1	1	1	1	0	0	0	0	0	1	1
1	0	0	0	1	0	0	1	−2	0	1	0	1	0	0	0	1	1	1	1	0	1
1	0	0	0	1	0	1	0	0	−2	1	0	1	1	1	0	1	1	0	0	0	1
1	0	0	1	0	0	0	0	1	1	−2	1	0	0	1	1	0	1	1	0	0	0
1	0	1	0	1	0	0	1	0	0	1	−2	0	0	1	1	0	1	1	0	1	1
1	0	1	1	0	0	0	1	1	1	0	0	−2	1	0	0	1	0	0	1	0	0
1	0	1	0	0	0	0	1	0	1	0	0	1	−2	0	1	0	1	1	0	0	0
1	0	1	0	0	1	0	1	0	1	1	1	0	0	−2	0	1	0	0	1	0	0
1	0	0	0	1	0	0	0	0	0	1	1	0	1	0	−2	1	0	0	1	0	0
1	0	0	0	1	1	0	0	1	1	0	0	1	0	1	1	−2	0	1	0	1	0
1	0	1	0	0	1	1	0	1	1	1	1	0	1	0	0	0	−2	0	1	1	0
1	0	1	1	0	0	1	0	1	0	1	1	0	1	0	0	1	0	−2	0	0	0
1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	1	0	1	0	−2	1	1
1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	0	1	1	0	1	−2	0
1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	0	0	1	0	−2

The substitution $\sqrt{2} \mapsto -\sqrt{2}$ induces a permutation on the set of h_F-lines preserving the intersection form, and hence it induces an isometry of the lattice S_X, which is given by the right multiplication of the matrix in Table 3. The deck-transformation of $\pi_F : X \to \mathbb{P}^2$ also induces an isometry of S_X, which is given by

$$[\ell_1] \mapsto [\ell_2], \quad [\ell_2] \mapsto [\ell_1], \quad \text{and} \quad [\ell_i] \mapsto h_F - [\ell_i] \quad \text{for } i > 2. \tag{4.1}$$

A smooth rational curve Q on X is said to be an *h_F-conic* if $\langle h_F, Q\rangle = 2$. It is known that there exist exactly 6,300 h_F-conics on X. See [27].

Our next task is to calculate the period $\mathcal{K}_X$ of X explicitly. The discriminant group $A_S = S_X^{\vee}/S_X$ of S_X is isomorphic to $\mathbb{F}_5^2$ and is generated by

$$\alpha_1 = [\ell_3]^{\vee} \bmod S_X \quad \text{and} \quad \alpha_2 = [\ell_4]^{\vee} \bmod S_X.$$

With respect to the basis α_1, α_2, the discriminant form $q_S : A_S \to \mathbb{Q}/2\mathbb{Z}$ of S_X is given by the matrix

$$\begin{bmatrix} 2/5 & 0 \\ 0 & 4/5 \end{bmatrix}.$$

The automorphism group $\mathrm{O}(q_S)$ of (A_S, q_S) is of order 12, and, by means of the basis α_1, α_2, each element of $\mathrm{O}(q_S)$ is expressed as a right-multiplication of a 2×2 matrix in $\mathrm{GL}_2(\mathbb{F}_5)$. Consider the matrices

$$T_A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$T_B = {}^t\begin{bmatrix} 2 & 3 & 1 & 0 & 4 & 1 & 1 & 0 & 4 & 1 & 2 & 2 & 4 & 4 & 0 & 0 & 1 & 4 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & 1 & 4 & 2 & 4 & 3 & 4 & 1 & 2 & 4 & 2 & 1 & 3 & 0 & 4 & 4 & 4 & 2 & 0 & 0 \end{bmatrix}$$

Table 3 Frobenius action on S_X

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 3 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & 0 \\
0 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & 0 & 0 & 1 & 1 & -1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & -1
\end{bmatrix}
$$

of size 2×22 and 22×2, respectively. Then the action $\bar{g} \in \mathrm{O}(q_S)$ on (A_S, q_S) induced by an isometry $g \in \mathrm{O}(S_X)$ is given by

$$\bar{g} = T_A \cdot \mathrm{G}_S^{-1} \cdot g \cdot \mathrm{G}_S \cdot T_B \bmod 5. \tag{4.2}$$

Consider the two-dimensional $\mathbb{F}_5$-vector space

$$S_0 = 5S_X^{\vee}/5S_X \subset S_X \otimes_{\mathbb{Z}} \mathbb{F}_5.$$

The vector space S_0 has a basis

$$\tilde{\alpha}_1 = 5[\ell_3]^{\vee} \bmod 5S_X \quad \text{and} \quad \tilde{\alpha}_2 = 5[\ell_4]^{\vee} \bmod 5S_X,$$

with respect to which the $\mathbb{F}_5$-valued quadratic form Q_0 is given by the matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}.$$

Recall that $\bar{c}_{\mathrm{DR}} : S_X \otimes k \to H^2_{\mathrm{DR}}(X)$ is the Chern class map. Then $\mathrm{Ker}(\bar{c}_{\mathrm{DR}})$ is a one-dimensional isotropic subspace of $Q_0 \otimes k$. Therefore, we see that $\mathrm{Ker}(\bar{c}_{\mathrm{DR}})$ is either equal to $\mathcal{I}_+ = \langle (1, \sqrt{2}) \rangle$ or equal to $\mathcal{I}_- = \langle (1, -\sqrt{2}) \rangle$. Since the Frobenius map $\phi = \mathrm{id} \otimes F_k$ from $S_0 \otimes k$ to itself only interchanges $\mathcal{I}_+$ and $\mathcal{I}_-$, we conclude that the period $\mathcal{K}_X = \phi^*(\mathrm{Ker}(\bar{c}_{\mathrm{DR}}))$ of X is either $\mathcal{I}_-$ or $\mathcal{I}_+$. On the other hand, we have

$$\{\bar{g} \in \mathrm{O}(Q_0) \mid \mathcal{I}_+^{\bar{g}} = \mathcal{I}_+\} = \{\bar{g} \in \mathrm{O}(Q_0) \mid \mathcal{I}_-^{\bar{g}} = \mathcal{I}_-\},$$

and this subgroup of $\mathrm{O}(Q_0)$ is of order 6 and consists of the following elements of $\mathrm{GL}_2(\mathbb{F}_5)$:

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}2&1\\3&2\end{bmatrix},\begin{bmatrix}2&4\\2&2\end{bmatrix},\begin{bmatrix}3&1\\3&3\end{bmatrix},\begin{bmatrix}3&4\\2&3\end{bmatrix},\begin{bmatrix}4&0\\0&4\end{bmatrix}.$$

Therefore, for a given $g \in \mathrm{O}(S_X)$, we can determine whether $\mathcal{K}_X^g = \mathcal{K}_X$ or not by calculating $\bar{g}$ by means of (4.2) and see whether $\bar{g}$ is one of the six matrices above.

For example, the Frobenius isometry given in Table 3 does not preserve the period, whereas the deck-transformation isometry (4.1) does.

4.2. *Embedding S_X into L*

Let $\mathcal{P}_{S_X}$ be the positive cone of S_X containing an ample class of X. We embed S_X into the even unimodular hyperbolic lattice L of rank 26 primitively in such a way that conditions (i) and (ii) in Section 3.1 are satisfied and calculate some induced chambers contained in the $\mathcal{R}^*_{S_X}$-chamber $\mathrm{NC}(X)$.

PROPOSITION 4.1. (1) *There exists a primitive embedding $S_X \hookrightarrow L$ such that the orthogonal complement R of S_X in L satisfies conditions* (i) *and* (ii) *in Section 3.1.*

(2) *If $\iota : S_X \hookrightarrow L$ and $\iota' : S_X \hookrightarrow L$ are primitive embeddings, then there exists $g \in \mathrm{O}(L)$ such that $\iota' = g \circ \iota$.*

Proof. By Nipp's table of reduced regular primitive positive-definite quaternary quadratic forms [23], there exists a negative-definite lattice R of rank 4 with discriminant 25, and R is unique up to isomorphisms. We can choose a basis $u_1, \dots, u_4$ of R with respect to which the Gram matrix is equal to

$$\begin{bmatrix}-2&-1&0&1\\-1&-2&-1&0\\0&-1&-4&-2\\1&0&-2&-4\end{bmatrix}. \tag{4.3}$$

It is obvious that $\mathcal{R}_R$ is nonempty. By a direct computation we see that the order of $\mathrm{O}(R)$ is 72 and obtain the list of all elements of $\mathrm{O}(R)$.

The discriminant group $A_R = R^\vee/R$ of R is isomorphic to $\mathbb{F}_5^2$ and is generated by

$$\beta_1 = u_4^\vee \bmod R \quad \text{and} \quad \beta_2 = u_2^\vee \bmod R,$$

with respect to which the discriminant form $q_R : A_R \to \mathbb{Q}/2\mathbb{Z}$ of R is given by the matrix

$$\begin{bmatrix}8/5&0\\0&6/5\end{bmatrix}.$$

Hence, the order of $\mathrm{O}(q_R)$ is 12. We can check by direct computation that the natural homomorphism $\mathrm{O}(R) \to \mathrm{O}(q_R)$ is surjective.

Recall that α_1 and α_2 are the basis of $A_S = S_X^\vee/S_X \cong \mathbb{F}_5^2$ given in the previous subsection. The linear map $\delta : A_S \to A_R$ defined by $\delta(\alpha_1) = \beta_1$ and $\delta(\alpha_2) = \beta_2$

induces an isomorphism from (A_S, q_S) to $(A_R, -q_R)$. Consequently, the pull-back L of the graph

$$\{(x, \delta(x)) \mid x \in A_S\}$$

of δ by the natural projection $S_X^\vee \oplus R^\vee \to A_S \oplus A_R$ is an even unimodular hyperbolic lattice of rank 26, into which S_X and R are primitively embedded. (See Nikulin [22].)

The uniqueness of primitive embeddings $S_X \hookrightarrow L$ up to the action of $\mathrm{O}(L)$ follows from the uniqueness of the even negative-definite lattice of rank 4 with discriminant 25 and the surjectivity of $\mathrm{O}(R) \to \mathrm{O}(q_R)$. (See Nikulin [22].) □

In the following, we use the primitive embedding $S_X \hookrightarrow L$ constructed in the proof of Proposition 4.1. Let $\mathcal{P}_L$ be the positive cone containing $\mathcal{P}_{S_X}$. An element of $L \otimes \mathbb{R}$ is written in the form of a vector $[x_1, \dots, x_{26}]^\vee$ with respect to the basis $[\ell_1]^\vee, \dots, [\ell_{22}]^\vee, [u_1]^\vee, \dots, [u_4]^\vee$ of $S_X^\vee \oplus R^\vee$.

Let w be a Weyl vector of L such that the corresponding Conway chamber $\mathcal{D}(w)$ is S_X-nondegenerate, and let D denote the chamber $\mathcal{D}(w) \cap \mathcal{P}_{S_X}$ of $\mathcal{P}_{S_X}$ induced by $\mathcal{D}(w)$. We denote by $\mathcal{W}(D)$ the set of walls of D. For a wall $W \in \mathcal{W}(D)$, there exists a unique *primitive* vector $v_W \in S_X^\vee$ such that $W = (v_W)^\perp$ and $\langle v_W, u\rangle > 0$, where u is a point in the interior of D. A wall $W \in \mathcal{W}(D)$ is said to be *of type* $[a, n]$ if $\langle v_W, w_S\rangle = a$ and $\langle v_W, v_W\rangle = n$, where $w_S \in S_X^\vee$ is the projection of the Weyl vector $w \in L$. Suppose that D is contained in the $\mathcal{R}^*_{S_X}$-chamber $\mathrm{NC}(X)$. Then a wall $W \in \mathcal{W}(D)$ of type $[a, n]$ is a wall of $\mathrm{NC}(X)$ if and only if there exists an integer c such that $ac = 1$, $nc^2 = -2$, and $cv_W \in S_X$.

Let D be an induced chamber contained in $\mathrm{NC}(X)$, and let $h_D \in S_X$ be a vector contained in the interior of D that is invariant under the action of $\mathrm{Aut}(D)$. Then h_D is ample, and

$$\mathrm{Aut}_X(D) = \mathrm{Aut}(D) \cap G_X = \{g \in \mathrm{O}(S_X) \mid D^g = D, \mathcal{K}_X^g = \mathcal{K}_X\}$$

is the automorphism group of the polarized $K3$ surface (X, h_D).

4.3. *The Induced Chamber D_0*

We put

$$w_0 = h_F + u_1 \in S_X \oplus R \subset L. \tag{4.4}$$

Since w_0 is primitive in L, w_0 belongs to $\overline{\mathcal{P}}_L$, and $\langle w_0\rangle^\perp / \langle w_0\rangle$ contains no (-2)-vectors, we see that w_0 is a Weyl vector. We denote by pr_{S_X} the orthogonal projection from $L \otimes \mathbb{R}$ to $S_X \otimes \mathbb{R}$. Calculating the finite set

$$\mathrm{pr}_{S_X}(\Delta(w_0)) \cap \mathcal{R}_{L|S} = \{r_{S_X} \mid r \in \Delta(w_0), \langle r_{S_X}, r_{S_X}\rangle_{S_X} < 0\},$$

we see that $h_F = w_{0,S}$ belongs to the interior of

$$D_0 = \mathcal{D}(w_0) \cap \mathcal{P}_{S_X}.$$

Hence, the Conway chamber $\mathcal{D}(w_0)$ is S_X-nondegenerate, and D_0 is an induced chamber. The order of $\mathrm{Aut}_X(D_0)$ is 756,000, and it coincides with the automorphism group of the Fermat double sextic plane (X, h_F). The action of $\mathrm{Aut}_X(D_0) = \mathrm{Aut}(X, h_F)$ decomposes the set $\mathcal{W}(D_0)$ of walls of D_0 into the union of three orbits $O_{0,0}$, $O_{0,1}$, $O_{0,2}$ described as follows:

no.	type	card.
0	$[1, -2]$	252
1	$[1, -8/5]$	300
2	$[2, -6/5]$	15,750

The walls in the orbit $O_{0,0}$ of cardinality 252 are walls of $\mathrm{NC}(X)$, and hence they correspond to smooth rational curves on X. Let R_{252} denote the set of smooth rational curves on X corresponding to the walls in $O_{0,0}$. Then R_{252} coincides with the set of h_F-lines.

4.4. *The Induced Chamber D_1*

The $\mathrm{Aut}_X(D_0)$-orbit $O_{0,1}$ of the walls of D_0 contains a wall $(v_1)^{\perp}$, where

$$v_1 = [0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1]^{\vee} \in S_X^{\vee}.$$

We put

$$w_1 = [1, 2, 2, 1, 1, 2, 1, 2, 1, 2, 2, 1, 2, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 1, 1, 0]^{\vee} \in L.$$

Then w_1 is a Weyl vector, the Conway chamber $\mathcal{D}(w_1)$ is S_X-nondegenerate, and the induced chamber

$$D_1 = \mathcal{D}(w_1) \cap \mathcal{P}_{S_X}$$

is adjacent to D_0 along the wall $(v_1)^{\perp}$. The vector $w_{1,S} \in S_X^{\vee}$ is contained in the interior of D_1 and satisfies $w_{1,S}^2 = 12/5$. We put $h_1 = 5w_{1,S}$. Then

$$h_1 = [14, 16, -4, -6, -5, -11, 12, -8, -5, 0, 10, 8, -13, 3, -3, 5, -8, 10, 7, -2, 5, -10]$$

is a polarization of degree 60. The degree $\langle h_F, h_1 \rangle$ of the polarization h_1 with respect to h_F is 15. The automorphism group $\mathrm{Aut}_X(D_1)$ of the polarized $K3$ surface (X, h_1) is of order 20,160. The action of $\mathrm{Aut}_X(D_1)$ decomposes $\mathcal{W}(D_1)$ into the union of 18 orbits $O_{1,0}, \dots, O_{1,17}$ described as follows:

no.	type	card.	no.	type	card.
0	$[1, -2]$	168	9	$[2, -6/5]$	840
1	$[3/5, -8/5]$	8	10	$[2, -6/5]$	840
2	$[4/5, -8/5]$	15	11	$[11/5, -6/5]$	1,680
3	$[4/5, -8/5]$	15	12	$[11/5, -6/5]$	1,680
4	$[6/5, -8/5]$	70	13	$[11/5, -6/5]$	840
5	$[6/5, -8/5]$	70	14	$[11/5, -6/5]$	840
6	$[7/5, -8/5]$	168	15	$[8/5, -4/5]$	15
7	$[9/5, -6/5]$	280	16	$[8/5, -4/5]$	15
8	$[9/5, -6/5]$	280	17	$[9/5, -2/5]$	8

We confirm by computer that the action of $\mathrm{Aut}_X(D_1)$ on the orbit $O_{1,1}$ of cardinality 8 embeds $\mathrm{Aut}_X(D_1)$ into the symmetric group $\mathfrak{S}_8$. Hence, $\mathrm{Aut}_X(D_1)$ is isomorphic to the alternating group $\mathfrak{A}_8$.

The wall $(v_1)^{\perp}$ separating D_0 and D_1 is a member of the orbit $O_{1,1}$. Hence, D_1 is adjacent to eight induced chambers G_X-congruent to D_0. Moreover, we have

$$|\mathrm{Aut}_X(D_0) \cap \mathrm{Aut}_X(D_1)| = \frac{|\mathrm{Aut}_X(D_0)|}{300} = \frac{|\mathrm{Aut}_X(D_1)|}{8} = 2{,}520.$$

The walls in the orbit $O_{1,0}$ are walls of $\mathrm{NC}(X)$, and hence they correspond to smooth rational curves on X. Let R_{168} denote the set of smooth rational curves on X corresponding to the walls in $O_{1,0}$. We observe the following facts by a direct calculation.

PROPOSITION 4.2. *Any distinct two curves in R_{168} are either disjoint or intersecting at one point transversely. For any curve Γ in R_{168}, there exist exactly* 72 *curves in R_{168} that intersect Γ.*

PROPOSITION 4.3. *Among R_{168}, exactly* 126 *curves are contained in the set R_{252} of h_F-lines, whereas the other* 42 *curves are h_F-conics. The deck-transformation of $X_F \to \mathbb{P}^2$ maps $R_{252} \cap R_{168}$ to the complement $R_{252} \setminus (R_{252} \cap R_{168})$ bijectively.*

4.5. The Induced Chamber D_2

The $\mathrm{Aut}_X(D_0)$-orbit $O_{0,2}$ of the walls of D_0 contains a wall $(v_2)^{\perp}$, where

$$v_2 = [1, 1, 2, 1, 0, 1, 1, 1, 1, 1, 2, 0, 1, 1, 1, 2, 2, 1, 1, 1, 2, 2]^{\vee} \in S_X^{\vee}.$$

We put

$$w_2 = [4, 4, 7, 4, 1, 4, 4, 4, 4, 4, 7, 1, 4, 4, 4, 7, 7, 4, 4, 4, 7, 7, 2, 1, -1, 0]^{\vee} \in L.$$

Then w_2 is a Weyl vector, the Conway chamber $\mathcal{D}(w_2)$ is S_X-nondegenerate, and the induced chamber

$$D_2 = \mathcal{D}(w_2) \cap \mathcal{P}_{S_X}$$

is adjacent to D_0 along the wall $(v_2)^{\perp}$. The vector $w_{2,S} \in S_X^{\vee}$ is contained in the interior of D_2 and satisfies $w_{2,S}^2 = 16/5$. We put $h_2 = 5w_{2,S}$. Then

$$\begin{aligned} h_2 = [&14, 11, 3, 6, 21, 15, -3, 18, 6, -6, -27,\\ &0, 9, -12, 3, -15, -3, -9, -18, 12, 0, 15] \end{aligned}$$

is a polarization of degree 80. The degree $\langle h_F, h_2\rangle$ of the polarization h_2 with respect to h_F is 40. The automorphism group $\mathrm{Aut}_X(D_2)$ of the polarized $K3$ surface (X, h_2) is of order 1,152. The action of $\mathrm{Aut}_X(D_2)$ decomposes $\mathcal{W}(D_2)$ into the union of 27 orbits $O_{2,0}, \dots, O_{2,26}$ described as follows:

no.	type	card.
0	[1, −2]	48
1	[1, −2]	48
2	[2/5, −8/5]	4
3	[2/5, −8/5]	4
4	[1, −8/5]	16
5	[1, −8/5]	16
6	[8/5, −8/5]	72
7	[8/5, −8/5]	72
8	[8/5, −8/5]	64
9	[8/5, −8/5]	64
10	[8/5, −6/5]	24
11	[9/5, −6/5]	48
12	[9/5, −6/5]	48
13	[9/5, −6/5]	16
14	[9/5, −6/5]	16
15	[11/5, −6/5]	288
16	[11/5, −6/5]	288
17	[11/5, −6/5]	96
18	[11/5, −6/5]	96
19	[11/5, −6/5]	48
20	[11/5, −6/5]	48
21	[12/5, −6/5]	576
22	[12/5, −6/5]	192
23	[12/5, −6/5]	192
24	[12/5, −6/5]	144
25	[8/5, −4/5]	3
26	[8/5, −4/5]	3

The wall $(v_2)^\perp$ separating D_0 and D_2 is a member of the orbit $O_{2,10}$. Hence, D_2 is adjacent to 24 induced chambers G_X-congruent to D_0. Moreover, we have

$$|\operatorname{Aut}_X(D_0) \cap \operatorname{Aut}_X(D_2)| = \frac{|\operatorname{Aut}_X(D_0)|}{15{,}700} = \frac{|\operatorname{Aut}_X(D_2)|}{24} = 48.$$

The walls in the orbits $O_{2,0}$ and $O_{2,1}$ are walls of $\mathrm{NC}(X)$, and hence they correspond to smooth rational curves on X. Let $R_{48,0}$ and $R_{48,1}$ denote the sets of smooth rational curves on X corresponding to the walls in $O_{2,0}$ and $O_{2,1}$, respectively. We observe the following facts.

PROPOSITION 4.4. *Any distinct two curves in the union $R_{48,0} \cup R_{48,1}$ are either disjoint or intersecting at one point transversely. For $\nu = 0, 1$, the set $R_{48,\nu}$ is a union of three sets $\mathcal{S}_{\nu 0}$, $\mathcal{S}_{\nu 1}$, $\mathcal{S}_{\nu 2}$ of disjoint* 16 *smooth rational curves. Each $\mathcal{S}_{\nu j}$ contains eight h_F-lines, and the h_F-degree of the remaining eight smooth rational curves is* 4. *We can number these six sets so that they satisfy conditions* (a), (b), (c) *in Theorem 1.2.*

We remark the following fact.

PROPOSITION 4.5. *Let $\mathcal{S}$ and $\mathcal{S}'$ be sets of disjoint* 16 *smooth rational curves on X. Then there exists $g \in \operatorname{Aut}(X)$ such that $g(\mathcal{S}) = \mathcal{S}'$.*

Proof. By Nikulin [21], if $\mathcal{S}_Y$ is a set of disjoint 16 smooth rational curves on a $K3$ surface Y in characteristic $\neq 2$, then Y is a Kummer surface associated with an Abelian surface A, and $\mathcal{S}_Y$ is the set of exceptional curves of the minimal resolution $Y \to A/\langle \iota_A \rangle$. (The proof in Nikulin [21] is valid not only over $\mathbb{C}$ but also in odd characteristics.)

Let $\zeta : X \to Z$ and $\zeta' : X \to Z'$ be the contractions of the (-2)-curves in $\mathcal{S}$ and $\mathcal{S}'$, respectively. Then there exist Abelian surfaces A and A' such that $Z \cong A/\langle \iota_A \rangle$ and $Z' \cong A'/\langle \iota_{A'} \rangle$, where ι_A and $\iota_{A'}$ are the inversions of A and A', respectively. By [31], both of A and A' are superspecial. Since a superspecial Abelian surface is unique up to isomorphisms in characteristic 5 by [31], there exists an isomorphism $f : A \xrightarrow{\sim} A'$ of Abelian surfaces. Since $f \circ \iota_A = \iota_{A'} \circ f$, the isomorphism f induces $A/\langle \iota_A \rangle \xrightarrow{\sim} A'/\langle \iota_{A'} \rangle$, and therefore we obtain an isomorphism $g' : Z \xrightarrow{\sim} Z'$. Since X, Z, and Z' are birational and X is minimal, there exists $g \in \mathrm{Aut}(X)$ such that $\zeta' \circ g = g' \circ \zeta$. We obviously have $g(\mathcal{S}) = \mathcal{S}'$. □

4.6. Further Induced Chambers

We define the *level* of an induced chamber D to be the minimal nonnegative integer ℓ such that there exists a chain

$$D^{(0)} = D_0, \qquad D^{(1)}, \dots, D^{(\ell)} = D$$

from D_0 to D of induced chambers such that $D^{(i-1)}$ and $D^{(i)}$ are adjacent. The *level* of a G_X-congruence class of induced chambers is defined to be the minimum of the levels of elements of the class. We have made the list of the G_X-congruence classes of induced chambers of level < 4. The number is

level	number of G_X-congruence classes
0	1
1	2
2	12
3	328

For level 4, we found more than six thousand G_X-congruence classes, and hence we have given up the computation. The data of the induced chambers D_i of level 2 are presented in Table 4. The third column is the orbit decomposition of the (-2)-walls of D_i by the action of $\mathrm{Aut}_X(D_i)$. In level 3, we have found many induced chambers D_i with $|\mathrm{Aut}_X(D_i)| = 1$.

REMARK 4.6. In [28], various sextic double plane models of X are systematically investigated by another method.

5. Proof of Theorems by Lattice Theory

In this section, we prove Theorems 1.1 and 1.2 by using lattice theory. To do this, we give three primitive embeddings of S_X into the even unimodular lattice L of

Table 4 Induced chambers of level 2

i	$\lvert \mathrm{Aut}_X(D_i) \rvert$	orbits of (-2)-walls
3	360	[18, 60]
4	36	[6, 9, 18, 18]
5	36	[6, 9, 18, 18]
6	48	[6, 8, 12, 24]
7	48	[6, 8, 12, 24]
8	72	[3, 12, 12, 18]
9	12	[3, 6, 6, 6, 6, 12]
10	8	[2, 2, 2, 4, 4, 4, 4, 4, 8, 8]
11	2	[1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2]
12	6	[2, 2, 3, 3, 3, 3, 6, 6, 6]
13	6	[2, 2, 3, 3, 3, 3, 6, 6, 6]
14	8	[2, 4, 4, 4, 4, 8, 8]

signature $(1, 25)$ corresponding to the three cases in Theorem 1.1 and then apply the Borcherds method and a theory of the Leech lattice.

First of all, we fix the notation. We denote by Λ the unique even *negative-definite unimodular lattice of rank 24 without* (-2)-vectors; that is, Λ is the *Leech lattice.* In the following, we recall an explicit description of Λ briefly. Let $\Omega = \{\infty, 0, 1, \dots, 22\}$ be the projective line $\mathbb{P}^1(\mathbb{F}_{23})$ over the field $\mathbb{F}_{23}$. We consider the set $P(\Omega)$ of all subsets of Ω with the symmetric difference as a 24-dimensional vector space over $\mathbb{F}_2$. Let $\mathcal{C}$ be the *binary Golay code,* which is a 12-dimensional subspace of $P(\Omega)$. We call a set in $\mathcal{C}$ a *$\mathcal{C}$-set.* A $\mathcal{C}$-set consists of 0, 8, 12, 16, or 24 elements. An eight-element $\mathcal{C}$-set is called an *octad,* and a set of six tetrads is called a *sextet* if the union of any two tetrads is an octad. We denote by $\mathcal{C}(8)$ the set of all octads. Let $\mathbb{R}^{24}$ be spanned by an orthonormal basis ν_i $(i \in \Omega)$. For a subset $S \subset \Omega$, we define ν_S to be $\sum_{i \in S} \nu_i$. Then the Leech lattice Λ is the lattice generated by the vectors $2\nu_K$ for $K \in \mathcal{C}(8)$ and $\nu_\Omega - 4\nu_\infty$ with the symmetric bilinear form

$$\langle x, y \rangle = -\frac{x \cdot y}{8}.$$

PROPOSITION 5.1 (Conway [5], Section 4, Theorem 2). *A vector* $(\xi_\infty, \xi_0, \dots, \xi_{22})$ *with* $\xi_i \in \mathbb{Z}$ *is in* Λ *if and only if*:

(i) *the coordinates* ξ_i *are all congruent modulo* 2 *to* m, *say*;
(ii) *the set of i for which* ξ_i *takes any given value modulo* 4 *is a* $\mathcal{C}$-*set*;
(iii) *the coordinate-sum is congruent to* $4m$ *modulo* 8.

We denote by Λ_n the set of all vectors x in Λ with $\langle x, x \rangle = -n$. Note that $\Lambda_2 = \emptyset$.

PROPOSITION 5.2 (Conway–Sloane [9], p. 133, Table 4.13). *The complete lists of* Λ_4 *and* Λ_6 *are as follows*:

$$\Lambda_4 = \{(\pm 2^8, 0^{16}), (\pm 3, \pm 1^{23}), (\pm 4^2, 0^{22})\},$$
$$\Lambda_6 = \{(\pm 2^{12}, 0^{12}), (\pm 3^3, \pm 1^{21}), (\pm 4, \pm 2^8, 0^{15}), (\pm 5, \pm 1^{23})\},$$

where the signs are taken to satisfy the conditions in Proposition 5.1.

We fix a decomposition

$$L = U \oplus \Lambda, \tag{5.1}$$

where U is the even unimodular hyperbolic lattice of rank 2 with the Gram matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We write (m, n, λ) for a vector in L, where λ is in Λ, and m, n are integers. Then its norm is given by $2mn + \langle \lambda, \lambda \rangle$. We take a vector $w = (1, 0, 0)$ as a Weyl vector. Then a (-2)-vector r in L with $\langle r, w \rangle = 1$ is called a *Leech root*. Let $\mathcal{D}$ be the Conway chamber with respect to w. Then the automorphism group of $\mathcal{D}$,

$$\mathrm{Aut}(\mathcal{D}) = \{g \in \mathrm{O}(L) \mid \mathcal{D}^g = \mathcal{D}\},$$

is isomorphic to the affine automorphism group of Λ:

$$\mathrm{Aut}(\mathcal{D}) \cong \Lambda \rtimes \mathrm{O}(\Lambda).$$

The set of all Leech roots bijectively corresponds to the set Λ as follows (Conway–Sloane [9], Chapter 26, Theorem 3):

$$L \ni r = (-1 - \langle \lambda, \lambda \rangle / 2, 1, \lambda) \quad \longleftrightarrow \quad \lambda \in \Lambda.$$

REMARK 5.3. For Leech roots $r, r' \in L$ and the corresponding vectors λ, λ' in Λ, $\langle r, r' \rangle = 0$ if $\lambda - \lambda' \in \Lambda_4$ and $\langle r, r' \rangle = 1$ if $\lambda - \lambda' \in \Lambda_6$.

5.1. Proof of Theorem 1.1(1)

We consider the following vectors in the Leech lattice Λ:

$$A = 4\nu_\infty + \nu_\Omega, \quad B = 0, \quad C = 2\nu_{K_0}, \quad D = 4\nu_0 + \nu_\Omega, \tag{5.2}$$

where K_0 is an octad with $\infty \notin K_0$ and $0 \in K_0$. Note that

$$A^2 = D^2 = -6, \quad C^2 = -4, \quad \langle A, C \rangle = -2, \quad \langle A, D \rangle = -4, \quad \langle C, D \rangle = -3.$$

Consider the vectors in $L = U \oplus \Lambda$ defined by

$$a = -(2, 1, A), \quad b = (-1, 1, 0), \quad c = (0, 1, C), \quad d = (1, 1, D). \tag{5.3}$$

Obviously, we have

$$a^2 = b^2 = -2, \quad c^2 = d^2 = -4, \quad \langle a, b \rangle = \langle b, c \rangle = -1,$$
$$\langle a, d \rangle = 1, \quad \langle c, d \rangle = -2, \quad \langle a, c \rangle = \langle b, d \rangle = 0.$$

Let R_1 be the sublattice of L generated by a, b, c, d. Note that the Gram matrix of R_1 is the same as that given in (4.3). Obviously, R_1 is primitive in L. Let S_1 be the orthogonal complement of R_1 in L. Then the signature of S_1 is $(1, 21)$, and

$S_1^\vee/S_1 \cong R_1^\vee/R_1 \cong (\mathbb{Z}/5\mathbb{Z})^2$. Thus, S_1 is isomorphic to the Néron–Severi lattice S_X of the supersingular $K3$ surface X with Artin invariant 1 in characteristic 5.

LEMMA 5.4. *Let w' be the projection of the Weyl vector w into $S_1^\vee$. Then $w' \in S_1$ and $(w')^2 = 2$. Moreover, w' is conjugate to the class of an ample divisor under the action of $W^{(-2)}(S_1)$.*

Proof. Denote by w'' the projection of w into $R_1^\vee$. By definition (5.3) we have $\langle w'', a\rangle = -1$ and $\langle w'', b\rangle = \langle w'', c\rangle = \langle w'', d\rangle = 1$. This implies that $w'' = a - b \in R_1$. Hence, $w' = w - w'' \in S_1$ and $(w')^2 = 2$. Let r be any (-2)-vector in S_1. Then, under the embedding $S_1 \subset L$, r is a (-2)-vector in L. Therefore, $\langle r, w'\rangle = \langle r, w\rangle \neq 0$. Hence, we have the last assertion. □

Now we determine all smooth rational curves on X whose degree with respect to w' is minimal. Note that such curves correspond to all Leech roots perpendicular to R_1 under the above embedding $S_1 \subset L$.

LEMMA 5.5. *There exist exactly* 252 *Leech roots that are orthogonal to R_1.*

Proof. Let r be a Leech root perpendicular to R_1. The condition $\langle r, b\rangle = 0$ implies $r = (1, 1, \lambda)$ with $\lambda \in \Lambda_4$. Similarly, we have

$$\langle \lambda, A\rangle = -3, \quad \langle \lambda, C\rangle = -1, \quad \langle \lambda, D\rangle = -2. \tag{5.4}$$

Now we use Proposition 5.1. If $\lambda = \pm 4\nu_i \pm 4\nu_j$, then the condition $\langle \lambda, A\rangle = -3$ implies that $\lambda = 4\nu_\infty + 4\nu_i$. Then $\langle \lambda, D\rangle = -1$ or -3. This contradicts (5.4).

If $\lambda = (\pm 2^8, 0^{16})$, then the condition $\langle \lambda, A\rangle = -3$ implies that $\lambda = 2\nu_K$, where K is an octad containing ∞. The condition $\langle \lambda, D\rangle = -2$ implies that K does not contain 0, and finally the condition $\langle \lambda, C\rangle = -1$ implies that $|K_0 \cap K| = 2$.

If $\lambda = (\pm 3, \pm 1^{23})$, then we first show that the case $\lambda = (-3, \pm 1^{23})$ does not occur. Assume that $\lambda = (-3, \pm 1^{23})$. Since $\langle \lambda, A\rangle = -3$, we have $\lambda = (-3, 1^{23}) = \nu_\Omega - 4\nu_i$, $i \neq \infty$. Then $\langle \lambda, D\rangle = -1$ or -3. This contradicts condition (5.4). Now assume that $\lambda = (3, \pm 1^{23})$. Since $\langle \lambda, A\rangle = -3$, we have $\lambda = 4\nu_\infty + \nu_\Omega - 2\nu_K$, where K is an octad containing ∞. The condition $\langle \lambda, D\rangle = -2$ implies that K does not contain 0. Finally, the condition $\langle \lambda, C\rangle = -1$ implies that $|K \cap K_0| = 2$.

Thus, the desired Leech roots are

$$(1, 1, 2\nu_K) \text{ and } (1, 1, 4\nu_\infty + \nu_\Omega - 2\nu_K) = (1, 1, A - 2\nu_K),$$

where K is an octad such that $\infty \in K$, $0 \notin K$, and $|K \cap K_0| = 2$.

In the following, we show that there exist exactly 126 such octads K. Let a_1, a_2 be in $K_0 \setminus \{0\}$. Then the number of octads containing three points ∞, a_1, a_2 is 21 (see Conway [5], Theorem 11). Take two points $a_3, a_4 \in K_0 \setminus \{a_1, a_2\}$. Then there exists exactly one octad containing five points ∞, a_1, a_2, a_3, a_4. Thus, the number of octads K containing ∞, a_1, a_2 and satisfying $K \cap K_0 = \{a_1, a_2\}$ is $21 - \binom{6}{2} = 6$. Therefore, the number of octads K containing ∞ and satisfying $|K \cap K_0| = 2$ is $\binom{7}{2} \times 6 = 126$. □

THEOREM 5.6. *For a suitable identification of S_1 with S_X, (X, w') is isomorphic to (X, h_F).*

Proof. Recall that we have given a primitive embedding of S_1 into L with a Weyl vector w whose orthogonal complement is R_1 (see (5.3)). On the other hand, we have given a primitive embedding of S_X into L with a Weyl vector w_0 whose orthogonal complement is R (see (4.4)). We identify these two embeddings as follows. First, we use the decomposition $L = U \oplus \Lambda$ given in (5.1), and we may assume that R is generated by

$$u_1 = a - b, \quad u_2 = -b, \quad u_3 = -c + d, \quad u_4 = d,$$

where $\{u_1, u_2, u_3, u_4\}$ is a basis of R with the Gram matrix (4.3). Obviously, $R = R_1$. Then $S_X = R^{\perp}$. The Weyl vector $w_0 = h_F + u_1$ and u_2 generate a hyperbolic plane $U'(\cong U)$ in L, and hence we have a decomposition

$$L = U' \oplus \Lambda',$$

where $\Lambda' = U'^{\perp} \cong \Lambda$. Write $w_0 = (1, 0, 0)$ and $u_2 = (1, -1, 0)$ with respect to the decomposition $L = U' \oplus \Lambda'$. Since $\langle w_0, a\rangle = -1$ and $\langle u_2, a\rangle = 1$, we have

$$a = (-2, -1, -A'),$$

where $A' \in \Lambda'$ satisfies $A'^2 = -6$. Similarly, we have

$$\begin{aligned} b &= (-1, 1, 0), \\ c &= (0, 1, C'), \quad \text{where } C' \in \Lambda', C'^2 = -4, \\ d &= (1, 1, D'), \quad \text{where } D' \in \Lambda', D'^2 = -6, \\ \langle A', C'\rangle &= -2, \quad \langle A', D'\rangle = -4, \quad \langle C', D'\rangle = -3. \end{aligned}$$

Note that A', $B'(= 0)$, C', T' define a root lattice A_4 in Λ' in the sense of the paper [3]; that is, the following Leech roots with respect to w_0

$$(2, 1, A'), (-1, 1, 0), (1, 1, C'), (2, 1, D')$$

generate a root lattice in $U' \oplus \Lambda'$. It follows from Lemma 6.1 in [3] that $\mathrm{Aut}(\mathcal{D})$ acts transitively on the set of root lattices of type A_4, where $\mathcal{D}$ is the Conway chamber with respect to the Weyl vector $w_0 = (1, 0, 0) \in U' \oplus \Lambda'$. Since $\mathrm{Aut}(\mathcal{D})$ fixes w_0, we may assume that A', B', C', D' coincide with A, B, C, D given in (5.2). Thus, we have shown that the embedding of S_X into L is the same one given in (5.3) and hence $h_F = w'$. □

REMARK 5.7. Let $r = (1, 1, 2\nu_K)$ and $r' = (1, 1, A - 2\nu_K)$ be Leech roots as in the proof of Lemma 5.5. In the proof of Lemma 5.4, we showed that $w'' = a - b$. Hence, we have

$$w' = w - w'' = (1, 0, 0) + (2, 1, A) + (-1, 1, 0) = (2, 2, A) = r + r'.$$

Thus, we have $w' = r + r'$ and $\langle r, r'\rangle = 3$. This corresponds to the fact that the pullback of the tangent line of the Fermat sextic curve C_F at an $\mathbb{F}_{25}$-rational point under the degree two map $\pi_F : X \to \mathbb{P}^2$ splits into two smooth rational curves meeting at one point with multiplicity 3.

We know that the projective automorphism group $\mathrm{Aut}(X, w')$ is a central extension of $\mathrm{PGU}(3, \mathbb{F}_{25})$ by the cyclic group of order 2 generated by the deck-transformation of X over $\mathbb{P}^2$. Here we show that the subgroup $\mathrm{PSU}(3, \mathbb{F}_{25})$ of index 6 acts on X by using the Torelli theorem for supersingular $K3$ surfaces.

PROPOSITION 5.8. *The group* $\mathrm{PSU}(3, \mathbb{F}_{25})$ *acts on* X *by automorphisms.*

Proof. First, we see that the pointwise stabilizer of $\{A, B, C, D\}$ of $\mathrm{O}(\Lambda)$ is $\mathrm{PSU}(3, \mathbb{F}_{25})$. The pointwise stabilizer of the three points $\{A = 4\nu_\infty + \nu_\Omega, B = 0, D = 4\nu_0 + \nu_\Omega\}$ is the Higman–Sims group HS (see Conway [5], Subsection 3.5). It is known that there exist 352 vectors C' in Λ satisfying

$$A - C' \in \Lambda_6 \quad \text{and} \quad B - C', D - C' \in \Lambda_4.$$

Note that $C = 2\nu_{K_0}$ is one of them. Moreover, they form 176 pairs $\{C', D - C'\}$ (Conway [5], Subsection 3.5). It follows from the table of maximal subgroups in Atlas (p. 80 of [7]) that the stabilizer of such a pair $\{C', D - C'\}$ in HS is $\mathrm{PSU}(3, \mathbb{F}_{25}) \rtimes \mathbb{Z}/2\mathbb{Z}$ with index 176. Therefore, the pointwise stabilizer of $\{A, B, C, D\}$ is $\mathrm{PSU}(3, \mathbb{F}_{25})$. We consider $\mathrm{PSU}(3, \mathbb{F}_{25})$ as a subgroup of $\mathrm{O}(U \oplus \Lambda)$ acting trivially on U. The group $\mathrm{PSU}(3, \mathbb{F}_{25})$ preserves the projection w' of the Weyl vector w that is conjugate to an ample class of X (Lemma 5.4). On the other hand, $\mathrm{PSU}(3, \mathbb{F}_{25})$ acts on R_1 identically and hence acts trivially on $R_1^\vee/R_1 \cong S_X^\vee/S_X$. This implies that $\mathrm{PSU}(3, \mathbb{F}_{25})$ preserves the period of X. It now follows from the Torelli theorem by Ogus [24; 25] for supersingular $K3$ surfaces that $\mathrm{PSU}(3, \mathbb{F}_{25})$ can act on X by automorphisms. □

REMARK 5.9. By the direct calculation using the data of Section 4.3 and (4.2) we can confirm that the image of $\mathrm{Aut}(X, D_0)$ by the natural homomorphism $\mathrm{O}(S_X) \to \mathrm{O}(q_{S_X})$ is equal to (4.1) and hence is of order 6. Combining this fact with the proof of Proposition 5.8, we see that the kernel of $\mathrm{Aut}(X, D_0) \hookrightarrow \mathrm{O}(S_X) \to \mathrm{O}(q_{S_X})$ is isomorphic to the simple group $\mathrm{PSU}(3, \mathbb{F}_{25})$.

5.2. *Proof of Theorem 1.1(2)*

Next, we consider the following vectors in the Leech lattice Λ:

$$A = 4\nu_\infty + \nu_\Omega, \quad B = 0, \quad C = 2\nu_{K_0}, \quad D = \nu_\Omega - 4\nu_\infty, \tag{5.5}$$

where K_0 is an octad that does not contain ∞. Consider the vectors in $L = U \oplus \Lambda$ defined by

$$a = -(2, 1, A), \quad b = (-1, 1, 0), \quad c = (0, 1, C), \quad d = (0, 0, D). \tag{5.6}$$

Obviously, we have

$$a^2 = b^2 = -2, \quad c^2 = d^2 = -4, \quad \langle a, b\rangle = \langle b, c\rangle = -1,$$
$$\langle a, c\rangle = \langle b, d\rangle = 0, \quad \langle a, d\rangle = 1, \quad \langle c, d\rangle = -2.$$

Let R_2 be the sublattice of L generated by a, b, c, d. Note that the Gram matrix of R_2 is the same as that given in (4.3). Moreover, the alternating group $\mathfrak{A}_8$ of degree 8 acts on the set $\Omega = \{\infty, 0, 1, \dots, 22\}$ such that it preserves the octad K_0

and fixes the point ∞ (see Conway [5]). This action can be extended to that on Λ and hence on $L = U \oplus \Lambda$ acting trivially on U. By definition, $\mathfrak{A}_8$ fixes R_2. Let S_2 be the orthogonal complement of R_2 in L on which $\mathfrak{A}_8$ acts. Then S_2 is isomorphic to the Néron–Severi lattice S_X of the supersingular $K3$ surface X with Artin invariant 1 in characteristic 5.

LEMMA 5.10. *Let w' be the projection of the Weyl vector w into $S_2^\vee$. Then $5w' \in S_2$ and $(5w')^2 = 60$. Moreover, $5w'$ is conjugate to the class of an ample divisor on X under the action of $W^{(-2)}(S_2)$.*

Proof. Write $w = w' + w''$ where w'' is the projection of w into $R_2^\vee$. We see that $w'' = (6a - 5b - c + 2d)/5$ and $(w'')^2 = -12/5$. Since $5w'' \in R_2$ and $w^2 = 0$, we have $5w' \in S_2$ and $(w')^2 = 12/5$. The proof of the last assertion is the same as that of Lemma 5.4. □

LEMMA 5.11. *There exist exactly 168 Leech roots that are orthogonal to R_2, and $\mathfrak{A}_8$ acts transitively on these Leech roots.*

Proof. By an argument similar to the proof of Lemma 5.5, we see that the desired Leech roots correspond to (-4)-vectors

$$4\nu_\infty + \nu_\Omega - 2\nu_K$$

in Λ, where K are octads that satisfy $K \ni \infty$ and $|K \cap K_0| = 2$. We count the number of such octads K. Let a_1, a_2 be in K_0. Then the number of octads containing three points ∞, a_1, a_2 is 21 (see Conway [5], Theorem 11). Take two points $a_3, a_4 \in K_0 \setminus \{a_1, a_2\}$. Then there exists exactly one octad containing five points ∞, a_1, a_2, a_3, a_4. Thus, the number of octads K containing ∞, a_1, a_2 and satisfying $K \cap K_0 = \{a_1, a_2\}$ is $21 - \binom{6}{2} = 6$. Therefore, the number of octads K containing ∞ and satisfying $|K \cap K_0| = 2$ is $\binom{8}{2} \times 6 = 168$.

Now take such an octad K. Then the stabilizer subgroup of K in $\mathfrak{A}_8$ is the symmetry group $\mathfrak{S}_5$ of degree 5 because it has five orbits of size 1, 2, 5, 6, 10; that is,

$$\{\infty\}, \{K \cap K_0\}, \{K_0 \setminus ((K \cap K_0) \cup \{\infty\})\}, \{K \setminus (K \cap K_0)\}, \{\Omega \setminus (K \cup K_0)\}.$$

Since the index of $\mathfrak{S}_5$ in $\mathfrak{A}_8$ is 168, we have the second assertion. □

LEMMA 5.12. *The group $\mathfrak{A}_8$ acts on X by automorphisms.*

Proof. The proof is similar to that of Lemma 5.8. □

Finally, the 168 Leech roots are the classes of the 168 smooth rational curves on X because Leech roots have the minimal degree 1 with respect to the Weyl vector w. Thus, we have finished the proof of Theorem 1.1(2).

REMARK 5.13. Let $r = (1, 1, 4\nu_\infty + \nu_\Omega - 2\nu_K)$ and $r' = (1, 1, 4\nu_\infty + \nu_\Omega - 2\nu_{K'})$ be two distinct Leech roots in Lemma 5.11. Then $\langle r, r' \rangle = 0$ or 1 if and only if

$|K \cap K'| = 4$ or 2, respectively. Moreover, we see that there exist exactly 72 Leech roots r' in Lemma 5.11 with $\langle r, r' \rangle = 1$ (see Proposition 4.2).

REMARK 5.14. In both cases (1) and (2) in Theorem 1.1, the octads K satisfying $\infty \in K$ and $|K \cap K_0| = 2$ appear. In case (1), K satisfies one more condition that K does not contain 0. Here we discuss the remaining octads K; that is, K contains ∞, 0 and satisfies $|K \cap K_0| = 2$. We put

$$r = (2, 2, \lambda), \quad \lambda = 2\nu_K + \nu_\Omega - 4\nu_0,$$

where K is an octad with $K \ni \infty$, $K \ni 0$ and $|K \cap K_0| = 2$. Then $r^2 = -2$ and $r \in R_1^\perp = S_1$. Obviously, we have $\langle r, w' \rangle = \langle r, w \rangle = 2$. There exist exactly 42 octads K satisfying $K \ni \infty$, $K \ni 0$, and $|K \cap K_0| = 2$. Recall that $w' = (2, 2, A) = (2, 2, 4\nu_\infty + \nu_\Omega)$ (Remark 5.7). For each root r from the above 42 roots, put

$$r' = 2w' - r = (2, 2, 8\nu_\infty + 4\nu_0 + \nu_\Omega - 2\nu_K).$$

Then $(r')^2 = -2$ and $r' \in R_1^\perp = S_1$. Thus, the class $r + r'$ corresponds to the pullback of a conic on $\mathbb{P}^2$ tangent to the Fermat sextic C_F at six points (see Proposition 4.3).

5.3. *Proof of Theorem 1.1(3)*

Finally, we consider the following vectors in the Leech lattice Λ:

$$\begin{aligned} &A = 4\nu_\infty + \nu_\Omega, \quad B = 0, \quad C = 8\nu_\infty, \\ &D = 2(\nu_\infty + \nu_0 + \nu_1 + \nu_2) - 2(\nu_3 + \nu_5 + \nu_{14} + \nu_{17}). \end{aligned} \tag{5.7}$$

Here $K_0 = \{\infty, 0, 1, 2, 3, 5, 14, 17\}$ is an octad (see Todd [32]). Consider the vectors in $L = U \oplus \Lambda$ defined by

$$a = -(2, 1, A), \quad b = (-1, 1, 0), \quad c = (1, 2, C), \quad d = (0, 0, D). \tag{5.8}$$

Obviously, we have

$$\begin{gathered} a^2 = b^2 = -2, \quad c^2 = d^2 = -4, \quad \langle a, b \rangle = \langle b, c \rangle = -1, \\ \langle a, c \rangle = \langle b, d \rangle = 0, \quad \langle a, d \rangle = 1, \quad \langle c, d \rangle = -2. \end{gathered}$$

Let R_3 be the sublattice of L generated by a, b, c, d. Then the Gram matrix of R_3 is the same as that given in (4.3). Note that a subgroup group $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes (\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_4)$ of M_{23} acts on the set $\Omega = \{\infty, 0, 1, \dots, 22\}$ such that it preserves the sextet of tetrads determined by $\{\infty, 0, 1, 2\}$, preserves the set $\{0, 1, 2\}$ and the octad K_0, and fixes the point ∞ (see Conway [5]). This action can be extended to that on Λ and hence on $L = U \oplus \Lambda$ acting trivially on U. Let S_3 be the orthogonal complement of R_3 in L. Then S_3 is isomorphic to the Néron–Severi lattice S_X of the supersingular $K3$ surface X with Artin invariant 1 in characteristic 5.

LEMMA 5.15. *Let w' be the projection of the Weyl vector w into $S_3^\vee$. Then $5w' \in S_3$ and $(5w')^2 = 80$. Moreover, w' is conjugate to the class of an ample divisor on X under the action of $W^{(-2)}(S_3)$.*

Proof. Write $w = w' + w''$ where $w'' \in R_3^\vee$. Then $w'' = (6a - 4b - 3c + 3d)/5$ and $(w'')^2 = -16/5$. Since $5w'' \in R_3$ and $w^2 = 0$, we have $5w' \in S$ and $(w')^2 = 16/5$. The proof of the last assertion is the same as that of Lemma 5.4. □

LEMMA 5.16. *There exist exactly* 96 *Leech roots that are orthogonal to* R_3.

Proof. By an argument similar to the proof of Lemma 5.5 we see that the desired Leech roots are

$$(1, 1, A - 2\nu_K),$$

where K is an octad satisfying one of the following conditions:

(1) $|K \cap K_0| = 4$, $K \ni \infty$, and K contains exactly two points of $\{0, 1, 2\}$,
(2) $|K \cap K_0| = 2$, $K \ni \infty$, and K contains exactly one point of $\{0, 1, 2\}$.

We count the number of octads satisfying (1) or (2). In case (1), there are 21 octads containing fixed three points $\{\infty, 0, 1\}$, and among these 21 octads, five octads contain four points $\{\infty, 0, 1, 2\}$. Thus, for each two points from $\{0, 1, 2\}$, there exist exactly 16 octads, and the total is $16 \times 3 = 48$. In case (2), there are exactly 16 octads K satisfying $K \cap K_0 = \{\infty, 0\}$ (see Conway [5], Table 10.1). Thus, we have 48 octads satisfying condition (2). □

LEMMA 5.17. *The group* $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes (\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_4)$ *acts on* X *by automorphisms.*

Proof. The proof is similar to that of Lemma 5.8. □

The 96 Leech roots are the classes of the 96 smooth rational curves on X because Leech roots have the minimal degree 1 with respect to the Weyl vector w. Thus, we have finished the proof of Theorem 1.1(3).

We denote by $\mathcal{T}$ the set of 96 Leech roots in Lemma 5.16. Let $\mathcal{T}_{ij}$ be the set of Leech roots that correspond to the octads K containing the two points i, j ($i, j = 0, 1, 2$) in the proof of Lemma 5.16, case (1), and let $\mathcal{T}_i$ be the set of all Leech roots corresponding to the octads K containing the point i ($i = 0, 1, 2$) in the proof of Lemma 5.16, case (2).

THEOREM 5.18. *Each* $\mathcal{T}_i$, $\mathcal{T}_{ij}$ *consists of* 16 *mutually orthogonal Leech roots. Each Leech root in* $\mathcal{T}_i$ *(resp.* $\mathcal{T}_{ij}$*) meets exactly six Leech roots in* $\mathcal{T}_j$ *with* $j \neq i$ *(resp.* $\mathcal{T}_{kl}$ *with* $(k, l) \neq (i, j)$*) with multiplicity* 1. *In particular,* $\{\mathcal{T}_i, \mathcal{T}_j\}$ *and* $\{\mathcal{T}_{ij}, \mathcal{T}_{kl}\}$ *form a* (16_6)*-configuration. Moreover,* $\{\mathcal{T}_i, \mathcal{T}_{jk}\}$ *with* $\{i, j, k\} = \{0, 1, 2\}$ *is a* (16_{12})*-configuration, and* $\{\mathcal{T}_i, \mathcal{T}_{ij}\}$ *is a* (16_4)*-configuration.*

Proof. We put $r = (1, 1, A - 2\nu_K)$ and $r' = (1, 1, A - 2\nu_{K'}) \in \mathcal{T}$. Then $\langle r, r' \rangle = 0$ or 1 if and only if $|K \cap K'| = 4$ or 2, respectively. Since any two octads meet at 0, 2, or 4 points, $\mathcal{T}_{ij}$ consists of 16 mutually orthogonal Leech roots.

On the other hand, if $r, r' \in \mathcal{T}_i$ and $K \cap K' = \{\infty, i\}$, then the symmetric difference $K + K'$ and $\Omega + K + K'$ are dodecads. Note that $\Omega + K + K'$ contains the octad K_0. This contradicts the fact that no dodecads contain an octad. Thus, we have $|K \cap K'| = 4$, and hence $\mathcal{T}_i$ consists of 16 mutually disjoint Leech roots.

Finally, we see that an element from $\mathcal{T}_i$ or $\mathcal{T}_{ij}$ has the incidence relation with $\mathcal{T}_j$ and $\mathcal{T}_{kl}$ as desired. Since the group $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes (\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_4)$ acts transitively on each set $\mathcal{T}_i$, $\mathcal{T}_{ij}$, the assertion follows. □

By defining $\{\mathcal{S}_{ij}\}$ by

$$\mathcal{S}_{01} = \mathcal{T}_0, \quad \mathcal{S}_{02} = \mathcal{T}_1, \quad \mathcal{S}_{03} = \mathcal{T}_2, \quad \mathcal{S}_{11} = \mathcal{T}_{12}, \quad \mathcal{S}_{12} = \mathcal{T}_{02}, \quad \mathcal{S}_{13} = \mathcal{T}_{01},$$

we have finished the proof of Theorem 1.2.

6. Supersingular Elliptic Curve in Characteristic 5

We summarize some facts on the supersingular elliptic curve in characteristic 5, which we will use later. We have, up to isomorphisms, only one supersingular elliptic curve defined over an algebraically closed field k of characteristic 5, which is given by the equation

$$y^2 = x^3 - 1.$$

We denote by E a nonsingular complete model of the supersingular elliptic curve. In the affine model, let (x_1, y_1) and (x_2, y_2) be two points on E. Then, the addition

$$m : E \times E \to E$$

of E is given by

$$\begin{aligned} m^*x &= -x_1 - x_2 + \frac{(y_2 - y_1)^2}{(x_2 - x_1)^2}, \\ m^*y &= y_1 + y_2 - \frac{(y_2 - y_1)^3}{(x_2 - x_1)^3} + \frac{3(x_2y_1 - x_1y_2)}{(x_1 - x_2)}. \end{aligned} \tag{6.1}$$

We denote by $[n]_E$ the multiplication by an integer n and by E_n the group of n-torsion points of E. The multiplication $[2]_E$ is concretely given by

$$[2]_E^* x = x_1 + 1/y_1^2, \qquad [2]_E^* y = 2y_1 - 1/y_1 + 1/y_1^3.$$

We denote by Fr the relative Frobenius morphism. Then, it satisfies

$$\mathrm{Fr}^2 = [-5]_E.$$

We set $\omega = 2 + 3\sqrt{2}$. Then, ω is a primitive cube root of unity. We set

$$P_\infty = (0, \infty), \quad P_0 = (1, 0), \quad P_1 = (\omega, 0), \quad P_2 = (\omega^2, 0).$$

The point P_∞ is the zero point of E, and the group E_2 of 2-torsion points of E is

$$E_2 = \{P_\infty, P_0, P_1, P_2\}.$$

The translation T_{P_0} by the point P_0 is given by

$$T_{P_0}^*(x) = \frac{x+2}{x-1}, \qquad T_{P_0}^*(y) = \frac{2y}{(x-1)^2}.$$

We set

$$u = 2(x + T_{P_0}^*(x) - 1), \qquad v = 2\sqrt{2}(y + T_{P_0}^*(y)).$$

Then, u and v are invariant under the action of $T_{P_0}^*$, and we have

$$u = \frac{2x^2 + 3x + 1}{(x-1)}, \qquad v = \frac{2\sqrt{2}y(x^2+3x+3)}{(x-1)^2}.$$

We know that the degree of the field extension $k(x, y)/k(u, v)$ is equal to 2 and that u and v satisfy the equation $v^2 = u^3 - 1$. Therefore, we have the quotient morphism by the action of T_{P_0}:

$$\begin{aligned} \phi_{E,2} : E &\to E, \\ (x, y) &\mapsto (u, v). \end{aligned}$$

By a direct calculation we see that

$$\phi_{E,2}^2 = [-2]_E.$$

The elliptic curve E has the following automorphism γ of order 6 defined by

$$\gamma^* x = \omega x, \qquad \gamma^* y = -y.$$

We consider the endomorphism ring $\mathcal{O} = \mathrm{End}(E)$. We set $B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, as is well known, B is the quaternion division algebra with discriminant 5, and $\mathcal{O}$ is a maximal order of B. We consider the following elements of $\mathcal{O}$:

$$\omega_1 = 1, \quad \omega_2 = \gamma, \quad \omega_3 = \phi_{E,2}, \quad \omega_4 = \gamma\phi_{E,2}.$$

The multiplication is given as follows:

	γ	$\phi_{E,2}$	$\gamma\phi_{E,2}$
γ	$\gamma - 1$	$\gamma\phi_{E,2}$	$-\phi_{E,2} + \gamma\phi_{E,2}$
$\phi_{E,2}$	$-1 + \phi_{E,2} - \gamma\phi_{E,2}$	-2	$-2 + 2\gamma - \phi_{E,2}$
$\gamma\phi_{E,2}$	$-\gamma + \phi_{E,2}$	-2γ	$-2 - \gamma\phi_{E,2}$

For example, we have $\phi_{E,2}\gamma = -1 + \phi_{E,2} - \gamma\phi_{E,2}$.

The canonical involution $a \mapsto \bar{a}$ of the quaternion algebra B is given as follows:

$$\bar{\gamma} = -\gamma^2, \quad \overline{\phi_{E,2}} = -\phi_{E,2}, \quad \overline{\gamma\phi_{E,2}} = -1 - \gamma\phi_{E,2}.$$

Denoting by Tr the trace map in B, we have a 4×4 matrix $(\mathrm{Tr}\,\omega_i\omega_j)$:

$$\begin{bmatrix} 2 & 1 & 0 & 1 \\ 1 & -1 & -1 & -1 \\ 0 & -1 & -4 & -2 \\ -1 & -1 & -2 & -3 \end{bmatrix}.$$

Since the determinant of this matrix is equal to -25, we know that ω_i ($i = 1, 2, 3, 4$) is a basis of the maximal order $\mathcal{O}$:

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\gamma + \mathbb{Z}\phi_{E,2} + \mathbb{Z}\gamma\phi_{E,2}.$$

REMARK 6.1. Considering $\mathrm{Ker}(\mathrm{Fr} - 1) = E(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z}$, we have

$$\mathrm{Fr} = 1 + \phi_{E,2}\gamma(1 + \gamma) = -1 + \phi_{E,2} - 2\gamma\phi_{E,2}.$$

7. Number of $\mathbb{F}_{p^2}$-Rational Points on Km(A)

Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. We set $A = E \times E$ and denote by ι_A the inversion of A. We denote by Km(A) the Kummer surface associated with A. In this section, we compute the number N of $\mathbb{F}_{p^2}$-rational points on Km(A).

In Katsura and Kondo [15], we proved the following lemma. For the readers' convenience, we give here the proof again.

Lemma 7.1. *$E(\mathbb{F}_{p^2}) = \mathrm{Ker}[p+1]_E$. In particular, we have $|E(\mathbb{F}_{p^2})| = (p+1)^2$ and $|A(\mathbb{F}_{p^2})| = (p+1)^4$.*

Proof. A point $P \in E$ is contained in $E(\mathbb{F}_{p^2})$ if and only if $\mathrm{Fr}^2(P) = P$. Since $\mathrm{Fr}^2 = [-p]_E$, we have $\mathrm{Fr}^2(P) = P$ if and only if $[p+1]_E(P) = 0$. □

Theorem 7.2. *The number N of $\mathbb{F}_{p^2}$-rational points on* Km(A) *is equal to* $1 + 22p^2 + p^4$.

Proof. We consider the quotient morphism

$$\varpi : A \to A/\langle \iota_A \rangle.$$

By $\mathrm{Ker}[2]_A \subset \mathrm{Ker}[p+1]_A$, all 2-torsion points are defined over $\mathbb{F}_{p^2}$. Excluding the 2-torsion points, we get $\{(p+1)^4 - 16\}/2$ points of $\mathrm{Km}(A)(\mathbb{F}_{p^2})$ derived from $(p+1)$-torsion points on A. If a point P on A satisfies $\mathrm{Fr}^2(P) = \iota_A(P)$, then we have $\mathrm{Fr}^2(\varpi(P)) = \varpi(P)$ on $A/\langle \iota_A \rangle$. Therefore, $\varpi(P)$ is an $\mathbb{F}_{p^2}$-rational point on $A/\langle \iota_A \rangle$. Hence, it gives an $\mathbb{F}_{p^2}$-rational point on Km(A). Since $\mathrm{Fr}^2(P) = \iota_A(P)$ if and only if P is contained in $\mathrm{Ker}[p-1]_A$, the number of such points on A is equal to $(p-1)^4$. Excluding the 2-torsion points, we get $\{(p-1)^4 - 16\}/2$ points of $\mathrm{Km}(A)(\mathbb{F}_{p^2})$ derived from $(p-1)$-torsion points on A. Since $|\mathbb{P}^1(\mathbb{F}_{p^2})| = p^2 + 1$, we have $16(p^2+1)$ points of $\mathrm{Km}(A)(\mathbb{F}_{p^2})$ that come from the 16 exceptional curves. Therefore, in total, we have an inequality

$$N \geq \{(p+1)^4 - 16\}/2 + \{(p-1)^4 - 16\}/2 + 16(p^2+1) = 1 + 22p^2 + p^4.$$

On the other hand, we consider the congruent zeta function $Z(\mathrm{Km}(A)/\mathbb{F}_{p^2}, t)$ of Km(A). Since Km(A) is a $K3$ surface, we have

$$Z(\mathrm{Km}(A)/\mathbb{F}_{p^2}, t) = \left((1-t)(1-p^4 t)\prod_{i=1}^{22}(1-\alpha_i t)\right)^{-1}$$

with algebraic integers α_i satisfying $|\alpha_i| = p^2$. Since $\log Z(\mathrm{Km}(A)/\mathbb{F}_{p^2}, t) = Nt + \cdots$, we have

$$N = 1 + \sum_{i=1}^{22} \alpha_i + p^4 \leq 1 + \sum_{i=1}^{22} |\alpha_i| + p^4 = 1 + 22p^2 + p^4.$$

Hence, we have $N = 1 + 22p^2 + p^4$. □

Corollary 7.3. *If $p=5$, then we have* $|\mathrm{Km}(A)(\mathbb{F}_{25})| = 1{,}176$.

Remark 7.4. Let E be the nonsingular complete model of the supersingular elliptic curve defined by $y^2 = x^3 - 1$ in characteristic 5. Then, by the consideration above, a point $P = (a, b) \in E$ is contained in $E_4 \setminus E_2$ if and only if $\mathrm{Fr}^2(P) = -P$ and $b \neq 0$. Therefore, we have the following:

(i) $P \in E_2$ if and only if $b = 0$ (and hence, $a \in \mathbb{F}_{25}$);
(ii) $P \in E_4 \setminus E_2$ if and only if $a \in \mathbb{F}_{25}$ and $b \notin \mathbb{F}_{25}$;
(ii) $P \in E_6 \setminus E_2$ if and only if $a \in \mathbb{F}_{25}$ and $b \in \mathbb{F}_{25} \setminus \{0\}$.

8. Six Sets of Disjoint 16 Smooth Rational Curves on $\mathrm{Km}(A)$

In this section, we resume working in characteristic 5. Let E be the elliptic curve defined by $y^2 = x^3 - 1$, and let A be the Abelian surface $E \times E$. For brevity, we denote by Y the Kummer surface $\mathrm{Km}(A)$. As is well known (see Ogus [24]), Y is isomorphic to our supersingular $K3$ surface X with Artin invariant 1. In this section, we explicitly construct six sets

$$\mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{02}, \mathcal{S}_{10}, \mathcal{S}_{11}, \mathcal{S}_{12}$$

of disjoint 16 smooth rational curves on Y with properties (a), (b), (c) in Theorem 1.2 and prove Theorem 1.3. We denote by S_A and S_Y the Néron–Severi lattices of A and Y, respectively. It is well known that S_A is of discriminant -25.

We denote by A_2 the group of 2-torsion points of A:

$$A_2 = E_2 \times E_2.$$

We consider the following commutative diagram:

$$\begin{array}{ccc} \tilde{A} & \xrightarrow{\pi} & Y \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle \rho} \\ A & \underset{\varpi}{\longrightarrow} & A/\langle \iota_A \rangle, \end{array}$$

where b is the blow-up at the points of A_2, ϖ is the quotient morphism by $\langle \iota_A \rangle$, ρ is the minimal resolution, and π is the double covering induced by ϖ. For $P \in A_2$, we denote by E_P the exceptional curve of b over P. The homomorphism $b^* : S_A \to S_{\tilde{A}}$ identifies S_A with a sublattice of the Néron–Severi lattice $S_{\tilde{A}}$ of $\tilde{A}$, and we obtain an orthogonal decomposition

$$S_{\tilde{A}} = S_A \oplus \bigoplus_{P \in A_2} \mathbb{Z}[E_P]. \tag{8.1}$$

Let $\mathcal{T}$ denote the group of translations of A by the points in A_2. Then $\mathcal{T}$ acts on $\tilde{A}$ and hence on $S_{\tilde{A}}$. The action preserves the orthogonal decomposition (8.1), and its restriction to the factor S_A is trivial, whereas its restriction to the factor $\bigoplus \mathbb{Z}[E_P]$ is induced by the permutation representation of $\mathcal{T}$ on A_2. The inversion ι_A of A lifts to an involution $\tilde{\iota}_A$ of $\tilde{A}$, and π is the quotient map by $\langle \tilde{\iota}_A \rangle$. The homomorphism π^* induces an embedding of the lattice $S_Y(2)$ into $S_{\tilde{A}}$, where $S_Y(2)$ is the $\mathbb{Z}$-module S_Y with the symmetric bilinear form defined by $\langle x, y \rangle_{S_Y(2)} = 2\langle x, y \rangle_{S_Y}$.

For an irreducible curve Γ on A that is invariant under ι_A, we denote by $\Gamma_{\tilde{A}}$ the *strict* transform of Γ by $b : \tilde{A} \to A$ and by Γ_Y the image of $\Gamma_{\tilde{A}}$ by $\pi : \tilde{A} \to Y$ with the reduced structure. Since Γ is invariant under ι_A, the map π induces a double covering $\Gamma_{\tilde{A}} \to \Gamma_Y$. Suppose that Γ is smooth. Then we have

$$[\Gamma_{\tilde{A}}] = [b^*\Gamma] - \sum_{P \in \Gamma \cap A_2} [E_P].$$

For an endomorphism $g : E \to E$ of E, we denote by Φ_g the graph of g, that is,

$$\Phi_g = \{(P, g(P)) \mid P \in E\}.$$

We can calculate the intersection number of a curve of certain type on A with Φ_g by the following method. Suppose that H is a (hyper)elliptic curve defined by

$$v^2 = f_H(u)$$

with the involution $\iota_H : (u, v) \mapsto (u, -v)$. We consider two finite morphisms

$$\eta_i : H \to E \quad (i = 1, 2)$$

satisfying $\eta_i \circ \iota_H = \iota_E \circ \eta_i$, and we set

$$\eta = (\eta_1, \eta_2) : H \to E \times E = A.$$

We denote by $\Gamma[\eta]$ the image of η on A with the reduced structure. Suppose that η induces a birational map from H to $\Gamma[\eta]$. Using the addition $m : E \times E \to E$, we have a divisor

$$\Delta = \operatorname{Ker} m = \{(P, -P) \mid P \in E\}$$

on $A = E \times E$. From the given endomorphism $g \in \operatorname{End}(E)$ we obtain a morphism

$$(-g) \times \mathrm{id} : E \times E \to E \times E.$$

Then we have $\Phi_g = ((-g) \times \mathrm{id})^* \Delta$. We consider the morphism

$$\theta : H \xrightarrow{\eta} E \times E \xrightarrow{(-g)\times\mathrm{id}} E \times E \xrightarrow{m} E.$$

Then we have

$$\begin{aligned}\langle \Gamma[\eta], \Phi_g \rangle_{S_A} &= \deg \eta^* \Phi_g = \deg(\eta^* \circ ((-g) \times \mathrm{id})^* \Delta) \\ &= \deg(\eta^* \circ ((-g) \times \mathrm{id})^* \circ m^{-1}(P_\infty)) \\ &= \deg((m \circ ((-g) \times \mathrm{id}) \circ \eta)^*(P_\infty)) \\ &= \deg \theta. \end{aligned} \tag{8.2}$$

By the assumption $\eta_i \circ \iota_H = \iota_E \circ \eta_i$, the map η_i is written as

$$\eta_i^* x = M_i(u), \qquad \eta_i^* y = v \cdot N_i(u),$$

by some rational functions M_i and N_i of one variable u. Since $g : E \to E$ satisfies $g \circ \iota_E = \iota_E \circ g$, there exist rational functions Ψ and Ξ of one variable x such that

$$g^* x = \Psi(x), \qquad g^* y = y \cdot \Xi(x).$$

The morphism θ induces a finite morphism

$$\tilde{\theta} : H/\langle \iota_H \rangle = \mathbb{P}^1 \to E/\langle \iota_E \rangle = \mathbb{P}^1$$

from the u-line to the x-line. Using (6.1), we see that $\tilde{\theta}$ is given by the rational function

$$\tilde{\theta}^* x = -\Psi(M_1(u)) - M_2(u) + \frac{f_H(u) \cdot (N_2(u) + N_1(u) \cdot \Xi(M_1(u)))^2}{(M_2(u) - \Psi(M_1(u)))^2}.$$

Since $\deg \tilde{\theta} = \deg \theta$, we can calculate $\langle \Gamma[\eta], \Phi_g \rangle_{S_A} = \deg \theta$ simply by calculating the degree of the rational function $\tilde{\theta}^* x$ of one variable.

PROPOSITION 8.1. *Let $\gamma : E \to E$ and $\phi_{E,2} : E \to E$ be the endomorphisms defined in Section 6. Then classes of the curves*

$$B_1 = E \times \{P_\infty\}, \quad B_2 = \{P_\infty\} \times E, \quad B_3 = \Phi_{\mathrm{id}},$$
$$B_4 = \Phi_\gamma, \quad B_5 = \Phi_{\phi_{E,2}}, \quad B_6 = \Phi_{\gamma \phi_{E,2}}$$

on A form a basis of S_A, where P_∞ is the zero point of E.

Proof. The intersection numbers $\langle B_i, B_j \rangle_{S_A}$ are given by the following matrix:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 2 & 2 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 3 & 4 \\ 1 & 1 & 1 & 0 & 2 & 3 \\ 2 & 1 & 3 & 2 & 0 & 2 \\ 2 & 1 & 4 & 3 & 2 & 0 \end{bmatrix}. \tag{8.3}$$

Since its determinant is -25, the classes $[B_1], \ldots, [B_6]$ form a basis of S_A. □

REMARK 8.2. Let $\mathcal{O} = \mathrm{End}(E)$ be as in Section 6. Set $X = E \times \{P_\infty\} + \{P_\infty\} \times E$. Then X is a principal polarization on A. For a divisor L on A, we have a homomorphism

$$\phi_L : A \to \mathrm{Pic}^0(A),$$
$$x \mapsto T_x^* L - L,$$

where T_x is the translation by $x \in A$ (see Mumford [20]). We see that $\phi_X^{-1} \circ \phi_L$ is an element of $\mathrm{End}(A) = M_2(\mathcal{O})$. We set

$$H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \,\middle|\, a, d \in \mathbb{Z}, b, c \in \mathcal{O} \text{ with } c = \bar{b} \right\}.$$

Then,

$$j : S_A \to H,$$
$$L \mapsto \phi_X^{-1} \circ \phi_L$$

is a bijective homomorphism, and for $L_1, L_2 \in S_A$ such that

$$j(L_1) = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \qquad j(L_2) = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix},$$

the intersection number $\langle L_1, L_2 \rangle_{S_A}$ is given by

$$\langle L_1, L_2 \rangle_{S_A} = a_2 d_1 + a_1 d_2 - c_1 b_2 - c_2 b_1$$

(see Katsura [14] and Katsura and Kondo [15]). For two endomorphisms $\alpha_1, \alpha_2 \in \mathcal{O}$, by Katsura [14] (also see Katsura and Kondo [15]) we have

$$j((\alpha_1 \times \alpha_2)^* \Delta) = \begin{bmatrix} \bar{\alpha}_1\alpha_1 & \bar{\alpha}_1\alpha_2 \\ \bar{\alpha}_2\alpha_1 & \bar{\alpha}_2\alpha_2 \end{bmatrix}.$$

Now consider our basis $[B_1], \dots, [B_6]$ of S_A. Since we have

$$B_3 = (-\mathrm{id} \times \mathrm{id})^* \Delta, \quad B_4 = (-\gamma \times \mathrm{id})^* \Delta, \quad B_5 = (-\phi_{E,2} \times \mathrm{id})^* \Delta,$$
$$B_6 = (-\gamma\phi_{E,2} \times \mathrm{id})^* \Delta,$$

we see that

$$j(B_1) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad j(B_2) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad j(B_3) = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix},$$
$$j(B_4) = \begin{bmatrix} 1 & -\gamma^5 \\ -\gamma & 1 \end{bmatrix}, \quad j(B_5) = \begin{bmatrix} 2 & \phi_{E,2} \\ -\phi_{E,2} & 1 \end{bmatrix},$$
$$j(B_6) = \begin{bmatrix} 2 & -\phi_{E,2}\gamma^2 \\ -\gamma\phi_{E,2} & 1 \end{bmatrix}.$$

Here, as an element in $\mathcal{O}$, we use 1 for id and -1 for ι_E. Using these expressions, we can also calculate our Gram matrix (8.3) easily.

From now on, we express elements of S_A as row vectors with respect to the basis $[B_1], \dots, [B_6]$. The matrix (8.3) is then the Gram matrix of S_A with respect to this basis.

REMARK 8.3. Let $\eta : H \to A$ be as before. Note that we have

$$\langle \Gamma[\eta], B_1 \rangle_{S_A} = \deg \eta_2, \qquad \langle \Gamma[\eta], B_2 \rangle_{S_A} = \deg \eta_1. \tag{8.4}$$

By the same method we can calculate the vector representation of the class of $\Gamma[\eta]$ in S_A with respect to the basis $[B_1], \dots, [B_6]$. By the Gram matrix (8.3) we obtain the self-intersection number of $\Gamma[\eta]$ on A. Then $\Gamma[\eta]$ is smooth (i.e., η induces an isomorphism from H to $\Gamma[\eta]$) if and only if

$$\langle \Gamma[\eta], \Gamma[\eta] \rangle_{S_A} = 2(\text{the genus of } H - 1). \tag{8.5}$$

In this case, we also have

$$\eta^{-1}(A_2) = \text{the set of fixed points of } \iota_H,$$

and hence we can easily obtain the set $\Gamma[\eta] \cap A_2$. Thus, we can calculate the class of the strict transform $\Gamma[\eta]_{\tilde{A}}$ of $\Gamma[\eta]$ in $S_{\tilde{A}}$.

EXAMPLE 8.4. Note that $\mathrm{Aut}(E)$ is a cyclic group of order 6 generated by γ. For integers a and b, the pull-back $(\gamma^a \times \gamma^b)^* \Phi_g$ of the graph Φ_g of $g \in \mathrm{End}(E)$ by the action

$$(\gamma^a \times \gamma^b) : (P, Q) \mapsto (\gamma^a(P), \gamma^b(Q))$$

is equal to $\Phi_{\gamma^{-b} g \gamma^a}$. Calculating the intersection numbers $\langle (\gamma^a \times \gamma^b)^* B_i, B_j \rangle_{S_A}$, we see that the action $(\gamma^a \times \gamma^b)^*$ on S_A is given by

$$[x_1, \dots, x_6] \mapsto [x_1, \dots, x_6] \cdot G_1^a \cdot G_2^b,$$

where

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 & 0 & 0 \\ 2 & 3 & -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 & 1 & 0 \end{bmatrix}, \qquad G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

EXAMPLE 8.5. In the same way, we see that the action of the involution $(P, Q) \mapsto (Q, P)$ of A on S_A is given by

$$[x_1, \dots, x_6] \mapsto [x_1, \dots, x_6] \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & 0 & 0 \\ 3 & 3 & 0 & 0 & -1 & 0 \\ 4 & 4 & -1 & 0 & 0 & -1 \end{bmatrix}.$$

REMARK 8.6. Let $\eta : H \to A$ be as before and suppose that η is an embedding (i.e., equality (8.5) holds). Then the induced morphism

$$\bar{\eta} : H/\langle \iota_H \rangle = \mathbb{P}^1 \to Y$$

is an isomorphism from the u-line $H/\langle \iota_H \rangle$ to the (-2)-curve $\Gamma[\eta]_Y$ on Y. The morphism $\bar{\eta}$ is calculated as follows. Let (x_1, y_1) and (x_2, y_2) be the affine coordinates of the first and second factors of $A = E \times E$. Then the singular surface $A/\langle \iota_A \rangle$ is defined by

$$w^2 = (x_1^3 - 1)(x_2^3 - 1),$$

where the quotient morphism $\varpi : A \to A/\langle \iota_A \rangle$ is given by

$$((x_1, y_1), (x_2, y_2)) \mapsto (x_1, x_2, w) = (x_1, x_2, y_1 y_2).$$

Then $\rho \circ \bar{\eta} : \mathbb{P}^1 \to A/\langle \iota_A \rangle$ is given by the rational functions

$$(\rho \circ \bar{\eta})^* x_1 = M_1(u), \quad (\rho \circ \bar{\eta})^* x_2 = M_2(u), \quad (\rho \circ \bar{\eta})^* w = f_H(u) N_1(u) N_2(u).$$

Let P be a point of A_2. Suppose that the image of $\rho \circ \bar{\eta}$ passes through the node $\varpi(P)$ of $A/\langle \iota_A \rangle$. Let $Q \in H$ be the point that is mapped to P by η, and let $Q' \in H/\langle \iota_H \rangle$ be the image of Q by the quotient map $H \to H/\langle \iota_H \rangle$. The lift $\bar{\eta} : \mathbb{P}^1 \to Y$ of $\rho \circ \bar{\eta}$ at Q' is calculated as follows. Let $T_{P,A}$ denote the tangent space to A at P. Then the (-2)-curve $\pi(E_P) = \rho^{-1}(\varpi(P))$ on Y is canonically identified with the projective line $\mathbb{P}_*(T_{P,A})$ of one-dimensional linear subspaces of $T_{P,A}$, and $\bar{\eta}(Q') \in \pi(E_P)$ corresponds to the image of

$$d_Q \eta : T_{Q,H} \to T_{P,A},$$

where $T_{Q,H}$ is the tangent space to H at Q. Thus, $\bar{\eta}(Q')$ is obtained by differentiating η at Q. In particular, if $\eta : H \to A$ is defined over $\mathbb{F}_{25}$, then we can calculate the list of $\mathbb{F}_{25}$-rational points on the (-2)-curve $\Gamma[\eta]_Y$ on Y.

We consider the hyperelliptic curves defined by

$$F : v^2 = u^6 - 1 \quad \text{and} \quad G : v^2 = \sqrt{2}(u^{12} + 2u^8 + 2u^4 + 1)$$

and by the morphisms

$$\phi_{E,2} : E \to E, \qquad (u, v) \mapsto \left(\frac{2u^2 + 3u + 1}{u - 1}, \frac{2\sqrt{2}v(u^2 + 3u + 3)}{(u - 1)^2}\right),$$

$$\phi_{F,2} : F \to E, \qquad (u, v) \mapsto (u^2, v),$$

$$\phi_{F,3} : F \to E, \qquad (u, v) \mapsto \left(\frac{2u}{u^3 - 1}, \frac{v(2u^3 + 1)}{(u^3 - 1)^2}\right),$$

$$\phi_{G,3} : G \to E, \qquad (u, v) \mapsto \left(\frac{4\sqrt{2}(u + 3\sqrt{2} + 4)^2(u + 2\sqrt{2} + 4)}{f}, \frac{(4 + 4\sqrt{2})v}{f^2}\right),$$

$$\text{where } f = \big(u + \sqrt{2}\big)\big(u + 4\sqrt{2} + 1\big)\big(u + 3\sqrt{2} + 2\big),$$

$$\phi_{G,4} : G \to E, \qquad (u, v) \mapsto \left(\frac{u^4 + (1 + 4\sqrt{2})u^2 + 2}{g}, \frac{vu}{g^2}\right),$$

$$\text{where } g = u^4 + \big(1 + 2\sqrt{2}\big)u^2 + \big(4 + \sqrt{2}\big).$$

REMARK 8.7. Each of these five morphisms $\phi : H \to E$ satisfies $\iota_E \circ \phi = \phi \circ \iota_H$.

REMARK 8.8. A basis of the vector space $\mathrm{H}^0(G, \Omega^1_G)$ of regular 1-forms on the curve G is given by

$$\frac{dx}{y} - \frac{x^4\,dx}{y}, \frac{x\,dx}{y}, \frac{x^3\,dx}{y}, \frac{x^2\,dx}{y}, \frac{dx}{y} + \frac{x^4\,dx}{y}.$$

With respect to this basis, the Cartier operator $\mathcal{C}$ is given by the matrix

$$\left[\begin{array}{c|c} 3I_3 & O_{3,2} \\ \hline O_{2,3} & O_{2,2} \end{array}\right],$$

where I_3 is the 3×3 identity matrix, and $O_{a,b}$ is the $a \times b$ zero matrix. Therefore, we have $\dim \operatorname{Ker} \mathcal{C} = 2$ and $\operatorname{rank} \mathcal{C} = 3$. Hence, the Jacobian variety $J(G)$ of G is isogenous to the product of a three-dimensional ordinary Abelian variety and a superspecial Abelian surface A. In the same way, we see that the Cartier operator is zero for the curve F and that the Jacobian variety $J(F)$ of F is isomorphic to A.

REMARK 8.9. The Weierstrass points of F are $(u, v) = ((3 + 2\sqrt{2})^\nu, 0)$ for $\nu = 0, \ldots, 5$. The Weierstrass points of G are $(u, v) = (u_\nu, 0)$ for $\nu = 0, \ldots, 11$, where u_ν are

$$\pm\sqrt{2}, \pm 2\sqrt{2}, 1 \pm \sqrt{2}, 2 \pm 2\sqrt{2}, 3 \pm 3\sqrt{2}, 4 \pm 4\sqrt{2}.$$

In particular, let $E' \to \mathbb{P}^1$ (resp. $\bar{E}' \to \mathbb{P}^1$, $F' \to \mathbb{P}^1$, $G' \to \mathbb{P}^1$) be the double covering branched at the points in P_4 (resp. $\bar{P}_4$, P_6, P_{12}) defined in Theorem 1.3. Then E' and $\bar{E}'$ are isomorphic to E over $\mathbb{F}_{25}$, F' is isomorphic to F over $\mathbb{F}_{25}$, and G' is isomorphic to G over $\mathbb{F}_{25}$.

We also consider the automorphisms

$$\begin{aligned} \gamma &: E \to E, \qquad (u, v) \mapsto (\omega u, -v), \\ h_F &: F \to F, \qquad (u, v) \mapsto \left(\frac{2\sqrt{2}u + 4}{u + 2\sqrt{2}}, \frac{v}{(u + 2\sqrt{2})^3} \right), \\ h'_F &: F \to F, \qquad (u, v) \mapsto \left(\frac{2\sqrt{2}u + 1}{u + 3\sqrt{2}}, \frac{v}{(u + 3\sqrt{2})^3} \right), \\ h_G &: G \to G, \qquad (u, v) \mapsto \left(\frac{2u + 3}{u + 1}, \frac{4v}{(u + 1)^6} \right). \end{aligned}$$

Note that the morphisms $\phi_{E,2}$ and γ have already appeared in Section 6.

Let τ denote the automorphism $(P, Q) \mapsto (Q, \iota_E(P))$ of A. Note that τ lifts to an automorphism of $\tilde{A}$ and its action on $S_{\tilde{A}}$ is obtained from Examples 8.4 and 8.5. For a curve Γ on A, we denote by $\mathcal{T}(\Gamma)$ the set of translations of Γ by points in A_2. Then we define sets of curves on A by

$$\begin{aligned} \mathcal{L}_{01} &= \mathcal{T}(\Gamma[(\phi_{F,2}, \phi_{F,2} h_F)]), \\ \mathcal{L}_{02} &= \mathcal{T}(\Gamma[(\phi_{F,3}, \phi_{F,3} h'_F)]), \\ \mathcal{L}_{10,(4,3)} &= \mathcal{T}(\Gamma[(\phi_{G,4}, \phi_{G,3})]), \\ \mathcal{L}_{10,(4,4)} &= \mathcal{T}(\Gamma[(\gamma^2 \phi_{G,4}, \gamma \phi_{G,4} h_G)]), \\ \mathcal{L}_{10} &= \mathcal{L}_{10,(4,3)} \cup \tau(\mathcal{L}_{10,(4,3)}) \cup \mathcal{L}_{10,(4,4)} \cup \tau(\mathcal{L}_{10,(4,4)}), \\ \mathcal{L}_{11,(1,2)} &= \mathcal{T}(\Gamma[(\gamma^2, \gamma^2 \phi_{E,2})]), \\ \mathcal{L}_{11,(2,2)} &= \mathcal{T}(\Gamma[(\phi_{E,2}\gamma, \gamma \phi_{E,2})]), \\ \mathcal{L}_{11} &= \mathcal{L}_{11,(1,2)} \cup \tau(\mathcal{L}_{11,(1,2)}) \cup \mathcal{L}_{11,(2,2)} \cup \tau(\mathcal{L}_{11,(2,2)}), \\ \mathcal{L}_{12} &= \mathcal{T}(B_1) \cup \mathcal{T}(B_2) \cup \mathcal{T}(B_4) \cup \mathcal{T}(\Gamma[(\mathrm{id}, \gamma^2)]). \end{aligned}$$

Using the same method, we have the following list of intersection numbers.

	B_1	B_2	B_3	B_4	B_5	B_6
$\Gamma[(\phi_{F,2}, \phi_{F,2} h_F)]$	2	2	4	2	8	7
$\Gamma[(\phi_{F,3}, \phi_{F,3} h'_F)]$	3	3	6	3	5	12
$\Gamma[(\phi_{G,4}, \phi_{G,3})]$	3	4	7	4	14	15
$\Gamma[(\gamma^2 \phi_{G,4}, \gamma \phi_{G,4} h_G)]$	4	4	7	3	14	16
$\Gamma[(\gamma^2, \gamma^2 \phi_{E,2})]$	2	1	3	2	3	7
$\Gamma[(\phi_{E,2}\gamma, \gamma \phi_{E,2})]$	2	2	5	2	6	8
$\Gamma[(\mathrm{id}, \gamma^2)]$	1	1	3	1	2	2

Using this table and the Gram matrix (8.3), we obtain the following vector representations of classes of these curves:

$$\begin{aligned} [\Gamma[(\phi_{F,2}, \phi_{F,2} h_F)]] &= [2, 3, -1, 2, -1, 0], \\ [\Gamma[(\phi_{F,3}, \phi_{F,3} h'_F)]] &= [4, 6, -2, 3, -1, -1], \\ [\Gamma[(\phi_{G,4}, \phi_{G,3})]] &= [5, 6, -2, 3, -1, -1], \end{aligned}$$

$$[\Gamma[(\gamma^2\phi_{G,4}, \gamma\phi_{G,4}h_G)]] = [4, 6, -2, 4, -1, -1],$$
$$[\Gamma[(\gamma^2, \gamma^2\phi_{E,2})]] = [2, 4, -1, 1, 0, -1],$$
$$[\Gamma[(\phi_{E,2}\gamma, \gamma\phi_{E,2})]] = [3, 4, -2, 2, 0, -1],$$
$$[\Gamma[(\mathrm{id}, \gamma^2)]] = [1, 1, -1, 1, 0, 0].$$

REMARK 8.10. In particular, we see that these curves are smooth by confirming (8.5).

REMARK 8.11. Incidentally, by the vector representations of classes of our curves we have

$$j(\Gamma[(\phi_{F,2}, \phi_{F,2}h_F)]) = \begin{bmatrix} 2 & 1 + 2\gamma^2 - \phi_{E,2} \\ 1 - 2\gamma + \phi_{E,2} & 2 \end{bmatrix},$$
$$j(\Gamma[(\phi_{F,3}, \phi_{F,3}h'_F)]) = \begin{bmatrix} 3 & 2 + 3\gamma^2 - \phi_{E,2} + \phi_{E,2}\gamma^2 \\ 1 - 3\gamma + \phi_{E,2} + \gamma\phi_{E,2} & 3 \end{bmatrix},$$
$$j(\Gamma[(\phi_{G,4}, \phi_{G,3})]) = \begin{bmatrix} 3 & 1 + 3\gamma^2 - \phi_{E,2} + \phi_{E,2}\gamma^2 \\ 1 - 3\gamma + \phi_{E,2} + \gamma\phi_{E,2} & 4 \end{bmatrix},$$
$$j(\Gamma[(\gamma^2\phi_{G,4}, \gamma\phi_{G,4}h_G)]) = \begin{bmatrix} 4 & 2 + 4\gamma^2 - \phi_{E,2} + \phi_{E,2}\gamma^2 \\ 2 - 4\gamma + \phi_{E,2} + \gamma\phi_{E,2} & 4 \end{bmatrix},$$
$$j(\Gamma[(\gamma^2, \gamma^2\phi_{E,2})]) = \begin{bmatrix} 2 & 1 + \gamma^2 + \phi_{E,2}\gamma^2 \\ 1 - \gamma + \gamma\phi_{E,2} & 1 \end{bmatrix},$$
$$j(\Gamma[(\phi_{E,2}\gamma, \gamma\phi_{E,2})]) = \begin{bmatrix} 2 & 2 + 2\gamma^2 - \phi_{E,2}\gamma^2 \\ 2 - 2\gamma + \gamma\phi_{E,2} & 2 \end{bmatrix},$$
$$j(\Gamma[(\mathrm{id}, \gamma^2)]) = \begin{bmatrix} 1 & \gamma \\ -\gamma^2 & 1 \end{bmatrix}.$$

We can also use these expressions to calculate the intersection numbers.

Now we state our main result of this section.

THEOREM 8.12. *For* $\nu i = 01, 02, 10, 11, 12$, *the set*

$$\mathcal{S}_{\nu i} = \{\Gamma_Y \mid \Gamma \in \mathcal{L}_{\nu i}\}$$

is a set of disjoint 16 *smooth rational curves on* Y. *Moreover, together with the set* $\mathcal{S}_{00}$ *of the images of the* (-1)*-curves* E_P *for* $P \in A_2$ *by* $\pi : \tilde{A} \to Y$, *the six sets* $\mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{02}, \mathcal{S}_{10}, \mathcal{S}_{11}, \mathcal{S}_{12}$ *satisfy conditions* (a), (b), *and* (c) *in Theorem 1.2 and possess the properties in Theorem 1.3.*

Proof. Let $\mathcal{S}$ be the union of the six sets $\mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{02}, \mathcal{S}_{10}, \mathcal{S}_{11}, \mathcal{S}_{12}$. We have already seen that the 96 curves in $\mathcal{S}$ are (-2)-curves on Y (see Remarks 8.7 and 8.10). Since the 96 rational curves in $\mathcal{S}$ are presented explicitly, we can prove Theorem 8.12 by direct computation.

By the method in Remark 8.3, we can calculate the classes $[\Gamma_Y] \in S_Y$ of the 96 rational curves $\Gamma_Y \in \mathcal{S}$: more precisely, we calculate the vector representations of the classes $[\pi^*(\Gamma_Y)]$ of the curves $\pi^*(\Gamma_Y)$ on $\tilde{A}$ with respect to the basis $[B_1], \dots, [B_6]$ and $[E_P]$ $(P \in A_2)$. Using the Gram matrix (8.3) and the formula

$$\langle [\Gamma_Y], [\Gamma'_Y] \rangle_{S_Y} = \frac{1}{2} \langle [\pi^*(\Gamma_Y)], [\pi^*(\Gamma'_Y)] \rangle_{S_{\tilde{A}}},$$

we can calculate the intersection numbers among the curves in $\mathcal{S}$. It follows that the six sets $\mathcal{S}_{\nu i}$ satisfy conditions (a), (b), and (c) in Theorem 1.2.

Next, we calculate the list $\Gamma_Y(\mathbb{F}_{25})$ of $\mathbb{F}_{25}$-rational points by the method in Remark 8.6. It turns out that

$$\langle [\Gamma_Y], [\Gamma'_Y] \rangle_{S_Y} = |\Gamma_Y(\mathbb{F}_{25}) \cap \Gamma'_Y(\mathbb{F}_{25})|$$

for any pair Γ_Y, Γ'_Y of distinct curves in $\mathcal{S}$. Therefore, any intersection point of curves in $\mathcal{S}$ is an $\mathbb{F}_{25}$-rational point. Moreover, the properties in Theorem 1.3 can be checked directly.

For example, we consider a curve $\Gamma[\eta] \in \mathcal{L}_{10,(4,4)}$, where the morphism $\eta : G \to A$ is given by

$$\begin{aligned}
\eta^* x_1 &= \frac{(2+2\sqrt{2})(u^2+(4+3\sqrt{2})u+4\sqrt{2})(u^2+(1+2\sqrt{2})u+4\sqrt{2})}{(u+4\sqrt{2})(u+3\sqrt{2}+3)(u+2\sqrt{2}+2)(u+\sqrt{2})},\\
\eta^* y_1 &= \frac{uv}{(u+4\sqrt{2})^2(u+3\sqrt{2}+3)^2(u+2\sqrt{2}+2)^2(u+\sqrt{2})^2},\\
\eta^* x_2 &= \big(4+3\sqrt{2}\big)\big(u^2+\big(3+4\sqrt{2}\big)u+3\sqrt{2}+4\big)\\
&\quad \times \big(u^2+\big(1+4\sqrt{2}\big)u+4\sqrt{2}+3\big)\\
&\quad /\big(\big(u+4+\sqrt{2}\big)\big(u+\sqrt{2}+1\big)\big(u+2\sqrt{2}+2\big)\big(u+3\sqrt{2}+2\big)\big),\\
\eta^* y_2 &= \frac{(1+\sqrt{2})v(u+4)(u+1)}{(u+4+\sqrt{2})^2(u+\sqrt{2}+1)^2(u+2\sqrt{2}+2)^2(u+3\sqrt{2}+2)^2}.
\end{aligned}$$

The vector representation of $[\Gamma[\eta]_{\tilde{A}}] \in S_{\tilde{A}}$ is

$$[\Gamma[\eta]_{\tilde{A}}] = [4, 6, -2, 4, -1, -1] - \sum_{P \in T[\eta]} [E_P],$$

where $[4, 6, -2, 4, -1, -1] \in S_A$ is written with respect to $[B_1], \dots, [B_6]$, and

$$T[\eta] = \{P_{\infty\infty}, P_{\infty 0}, P_{\infty 1}, P_{\infty 2}, P_{0\infty}, P_{00}, P_{01}, P_{02}, P_{1\infty}, P_{12}, P_{2\infty}, P_{22}\}.$$

Here $P_{\alpha\beta}$ denotes $(P_\alpha, P_\beta) \in A_2$ for $\alpha, \beta \in \{\infty, 0, 1, 2\}$ (see Section 6). The induced isomorphism $\bar{\eta}$ from the u-line $\mathbb{P}^1 = G/\langle \iota_G \rangle$ to the (-2)-curve $\Gamma[\eta]_Y \in \mathcal{S}_{10}$ induces the bijection between the sets of $\mathbb{F}_{25}$-rational points given in Table 5. In this table, the point $\bar{\eta}(u)$ is written by the following method: If $\bar{\eta}(u)$ is not on the exceptional divisor of ρ, then the coordinates $[x_1, x_2, w]$ of $\bar{\eta}(u)$ on $A/\langle \iota_A \rangle$ defined by $w^2 = (x_1^3 - 1)(x_2^3 - 1)$ are given. (See Remark 8.6.) If $\bar{\eta}(u)$ is on the (-2)-curve $\pi(E_P) = \rho^{-1}(\varpi(P))$ corresponding to $P \in A_2$, then the point $\bar{\eta}(u)$ is written by the coordinates $[[x_1, x_2], [\xi_0, \xi_1]]$, where $[\xi_0, \xi_1]$ is the homogeneous coordinates on $\pi(E_P) = \rho^{-1}(\varpi(P)) \cong \mathbb{P}_*(T_{P,A})$ with respect to the basis $\tilde{\theta}_P, \tilde{\theta}_P$

Table 5 The map $\bar{\eta}$ on $\mathbb{F}_{25}$-rational points

$$
\begin{aligned}
\bar{\eta}(\infty) &= [2+2\sqrt{2}, 4+3\sqrt{2}, 0],\\
\bar{\eta}(0) &= [2+3\sqrt{2}, 4+3\sqrt{2}, 0],\\
\bar{\eta}(1) &= [1+3\sqrt{2}, 1, 0],\\
\bar{\eta}(2) &= [1+3\sqrt{2}, 4+3\sqrt{2}, 4+3\sqrt{2}],\\
\bar{\eta}(3) &= [1+3\sqrt{2}, 4+3\sqrt{2}, 1+2\sqrt{2}],\\
\bar{\eta}(4) &= [1+3\sqrt{2}, 2+3\sqrt{2}, 0],\\
\bar{\eta}(\sqrt{2}) &= [[\infty, 1], [1, 2\sqrt{2}]],\\
\bar{\eta}(1+\sqrt{2}) &= [[2+3\sqrt{2}, 2+2\sqrt{2}], [1, 2]],\\
\bar{\eta}(2+\sqrt{2}) &= [2\sqrt{2}, 2+\sqrt{2}, 3],\\
\bar{\eta}(3+\sqrt{2}) &= [4+4\sqrt{2}, 4+\sqrt{2}, 3],\\
\bar{\eta}(4+\sqrt{2}) &= [[2+2\sqrt{2}, 2+2\sqrt{2}], [1, 4+\sqrt{2}]],\\
\bar{\eta}(2\sqrt{2}) &= [[1, 2+3\sqrt{2}], [1, 4+2\sqrt{2}]],\\
\bar{\eta}(1+2\sqrt{2}) &= [3\sqrt{2}, 2+\sqrt{2}, 1+\sqrt{2}],\\
\bar{\eta}(2+2\sqrt{2}) &= [[\infty, 2+2\sqrt{2}], [1, 2\sqrt{2}]],\\
\bar{\eta}(3+2\sqrt{2}) &= [[1, \infty], [1, 2+\sqrt{2}]],\\
\bar{\eta}(4+2\sqrt{2}) &= [3+4\sqrt{2}, 4+\sqrt{2}, 4+4\sqrt{2}],\\
\bar{\eta}(3\sqrt{2}) &= [[1, 1], [1, \sqrt{2}]],\\
\bar{\eta}(1+3\sqrt{2}) &= [3+4\sqrt{2}, 2+4\sqrt{2}, 1+4\sqrt{2}],\\
\bar{\eta}(2+3\sqrt{2}) &= [[1, 2+2\sqrt{2}], [1, \sqrt{2}]],\\
\bar{\eta}(3+3\sqrt{2}) &= [[\infty, \infty], [1, 4+2\sqrt{2}]],\\
\bar{\eta}(4+3\sqrt{2}) &= [3\sqrt{2}, 3+4\sqrt{2}, 3],\\
\bar{\eta}(4\sqrt{2}) &= [[\infty, 2+3\sqrt{2}], [1, 3+4\sqrt{2}]],\\
\bar{\eta}(1+4\sqrt{2}) &= [[2+2\sqrt{2}, \infty], [1, 1]],\\
\bar{\eta}(2+4\sqrt{2}) &= [4+4\sqrt{2}, 2+4\sqrt{2}, 4+4\sqrt{2}],\\
\bar{\eta}(3+4\sqrt{2}) &= [2\sqrt{2}, 3+4\sqrt{2}, 1+4\sqrt{2}],\\
\bar{\eta}(4+4\sqrt{2}) &= [[2+3\sqrt{2}, \infty], [1, 2+2\sqrt{2}]].
\end{aligned}
$$

of $T_{P,A}$, where $\tilde{\theta}$ is a nonzero invariant vector field on E, which is unique up to scalar multiplications.

We put $\Gamma = \Gamma[\eta]_Y$ and present the four subsets Γ_1, Γ_{00}, Γ_{01}, Γ_{02} of $\Gamma(\mathbb{F}_{25})$ in Theorem 1.3. The set Γ_{00} of 12 points on the exceptional divisor of ρ is easily obtained from Table 5. The other sets are given as follows:

$$
\begin{aligned}
\bar{\eta}^{-1}(\Gamma_1) &= \{\infty, 0, 1, 2, 3, 4\},\\
\bar{\eta}^{-1}(\Gamma_{01}) &= \{3+\sqrt{2}, 4+2\sqrt{2}, 1+3\sqrt{2}, 2+4\sqrt{2}\},\\
\bar{\eta}^{-1}(\Gamma_{02}) &= \{2+\sqrt{2}, 1+2\sqrt{2}, 4+3\sqrt{2}, 3+4\sqrt{2}\}.
\end{aligned}
$$

For example, the unique (-2)-curve in $\mathcal{S}_{11}$ passing through $\bar{\eta}(\infty) \in \Gamma_1$ is $\Gamma[\eta']_Y$, where $\eta' : E \to A$ is given by

$$\Bigg[\Bigg[\frac{u^2 + (1+3\sqrt{2})u + 2\sqrt{2} + 1}{(u+3\sqrt{2}+4)^2}, \frac{(4+2\sqrt{2})v(u+2\sqrt{2}+4)}{(u+3\sqrt{2}+4)^3}\Bigg], \big[(2+2\sqrt{2})u, 4v\big]\Bigg],$$

and we have $\bar{\eta}'(1+3\sqrt{3}) = \bar{\eta}(\infty)$, whereas the unique (-2)-curve in $\mathcal{S}_{12}$ passing through $\bar{\eta}(\infty) \in \Gamma_1$ is $\Gamma[\eta'']_Y$, where $\eta'' : E \to A$ is given by

$$\big[\big[2+2\sqrt{2}, 0\big], [u, v]\big],$$

and we have $\bar{\eta}''(4+3\sqrt{2}) = \bar{\eta}(\infty)$. The unique (-2)-curve in $\mathcal{S}_{01}$ passing through $\bar{\eta}(3+\sqrt{2}) \in \Gamma_{01}$ is $\Gamma[\xi]_Y$, where $\xi : F \to A$ is given by

$$\Bigg[[u^2, v], \Bigg[\frac{3(u+\sqrt{2})^2}{(u+2\sqrt{2})^2}, \frac{v}{(u+2\sqrt{2})^3}\Bigg]\Bigg],$$

and we have $\bar{\xi}(4+3\sqrt{2}) = \bar{\eta}(3+\sqrt{2})$.

The details of these data for all 96 curves in $\mathcal{S}$ are presented in [30]. □

We give a remark about (16_r)-configurations on a $K3$ surface in general.

PROPOSITION 8.13. *Assume that the characteristic p of the base field is $\neq 2$. No Abelian surfaces contain any nonsingular hyperelliptic curve of genus greater than or equal to* 6.

Proof. Suppose that an Abelian surface A contains a nonsingular hyperelliptic curve C of genus g. We may assume that C is symmetric under the inversion ι of A. Then, $C \cap A_2$ must contain $2g+2$ points. Since the number of points in A_2 is 16, we have $g \leq 7$. Assume that $g = 7$. Then, we have $C \cap A_2 = A_2$. If there exists a two-torsion point x such that $T_x^* C \neq C$, then we have $C^2 = (C, T_x^* C) \geq 16$. Therefore, the genus of C is greater than or equal to $16/2 + 1 = 9$, which contradicts $g = 7$. Suppose that $T_x^* C = C$ for any $x \in A_2$. Then, the group scheme $K(C) = \operatorname{Ker} \phi_C$ contains A_2, where ϕ_C is defined in Remark 8.2. On the other hand, by the Riemann–Roch theorem we have

$$|K(C)| = \deg \phi_C = (C^2/2)^2 = (g-1)^2 = 36.$$

Since $A_2 \subset K(C)$, 36 must be divisible by 16, a contradiction. Hence, A does not contain any nonsingular hyperelliptic curve of genus 7.

Now, assume that $g = 6$. Then, since C is hyperelliptic, we have $|C \cap A_2| = 2 \times 6 + 2 = 14$. Let x be a point in A_2 that is not contained in $C \cap A_2$. Take a point $y \in C \cap A_2$. Then, we have that $C \neq T_{x-y}^* C$ and $C \cap T_{x-y}^* C \cap A_2$ contains more than or equal to 12 points. Therefore, we have $C^2 = (C, T_{x-y}^* C) \geq 12$. Hence, the genus of C must be greater than or equal to $12/2 + 1 = 7$, which contradicts $g = 6$. Consequently, A does not contain any nonsingular hyperelliptic curve of genus 6. □

REMARK 8.14. Let C be a nonsingular complete curve of genus 2, and let $J(C)$ be a Jacobian variety. Then, it is well known that on the Kummer surface $\mathrm{Km}(J(C))$, there exists a (16_6)-configuration. We also have a (16_{10})-configuration on some Kummer surfaces, using a certain hyperelliptic curve of genus 4 (see Traynard [33], Barth and Nieto [2], and Katsura and Kondo [15]). In this paper, we constructed a (16_{12})-configuration on the supersingular $K3$ surface with Artin invariant 1 in characteristic 5. This seems to be the first example of (16_{12})-configurations on a $K3$ surface. To construct the configuration, we use a hyperelliptic curve of genus 5. By Proposition 8.13, we cannot construct $(16_{2\ell})$-configurations with $\ell \geq 7$ on a Kummer surface in a similar way to our method.

REMARK 8.15. The supersingular K3 surface with Artin invariant 1 in characteristic 5 has an interesting example of a pencil of curves of genus 2. Let P be a point of $\mathbb{P}^2(\mathbb{F}_{25}) \setminus C_F(\mathbb{F}_{25})$, and let R_1 and R_2 be the points on X that are mapped to P by $\pi_F : X \to \mathbb{P}^2$. We take the blowing-up $\tilde{X}$ at the two points R_1, R_2 of X. Then, the pencil of lines passing through P induces on $\tilde{X}$ a structure of fiber space over $\mathbb{P}^1$ whose general fiber is isomorphic to a smooth complete curve C of genus 2 defined by $y^2 = x^6 - 1$. The fiber space has exactly six degenerate fibers corresponding to the tangent lines of C_F passing through P. Each degenerate fiber is a union of two smooth rational curves intersecting at one point with multiplicity 3.

Let C_1 be the nonsingular complete model of the curve defined by the equation $1 + x_1^6 + x_2^6 = 0$. $G = \mathbb{Z}/6\mathbb{Z} = \langle\theta\rangle$ with a generator θ. We denote by ξ a primitive 6th root of unity and consider the action

$$\begin{aligned} \theta : x_1 \mapsto x_1, &\qquad x_2 \mapsto \xi x_2, \\ x \mapsto \xi x, &\qquad y \mapsto y \end{aligned}$$

on the surface $C_1 \times C$. The group G also acts on the curve C_1. We set

$$w = \sqrt{-1}(x_2/x)^3 y, \qquad z = x_2/x.$$

Then, x_1, w, and z are G-invariant, and the quotient surface $(C_1 \times C)/G$ is birationally isomorphic to the surface defined by $w^2 = z^6 + 1 + x_1^6$. The fiber space structure is given by $(C_1 \times C)/G \to C_1/G$.

References

[1] M. Artin, *Supersingular $K3$ surfaces,* Ann. Sci. Éc Norm. Supér. (4) 7 (1975), 543–567.

[2] W. Barth and I. Nieto, *Abelian surfaces of type* $(1, 3)$ *and quartic surfaces with* 16 *skew lines,* J. Algebraic Geom. 3 (1994), no. 2, 173–222.

[3] R. Borcherds, *Automorphism groups of Lorentzian lattices,* J. Algebra 111 (1987), no. 1, 133–153.

[4] R. E. Borcherds, *Coxeter groups, Lorentzian lattices, and $K3$ surfaces,* Int. Math. Res. Not. IMRN 19 (1998), 1011–1031.

[5] J. H. Conway, *Three lectures on exceptional groups,* Finite simple groups (Proc. Instructional Conf. Oxford, 1969), pp. 215–247, Academic Press, London, 1971, Chapter 10 in the book "Sphere packings, lattices and groups" by Conway and Sloane.

[6] ———, *The automorphism group of the 26-dimensional even unimodular Lorentzian lattice,* J. Algebra 80 (1983), no. 1, 159–163.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups: Maximal subgroups and ordinary characters for simple groups,* Oxford University Press, Eynsham, 1985, With computational assistance from J. G. Thackray.

[8] J. H. Conway and N. J. A. Sloane, *Lorentzian forms for the Leech lattice,* Bull. Amer. Math. Soc. (N.S.) 6 (1982), no. 2, 215–217.

[9] ———, *Sphere packings, lattices and groups,* third edition, Fundamental Principles of Mathematical Sciences, 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen, and B. B. Venkov.

[10] I. Dolgachev, *Abstract configurations in algebraic geometry,* The Fano conference, pp. 423–462, Univ. Torino, Turin, 2004.

[11] I. Dolgachev and J. H. Keum, *Finite groups of symplectic automorphisms of $K3$ surfaces in positive characteristic,* Ann. of Math. (2) 169 (2009), no. 1, 269–313.

[12] I. Dolgachev and S. Kondō, *A supersingular $K3$ surface in characteristic 2 and the Leech lattice,* Int. Math. Res. Not. IMRN 1 (2003), 1–23.

[13] P. Griffiths and J. Harris, *Principles of algebraic geometry,* Wiley Classics Library, John Wiley & Sons Inc., New York, 1994, Reprint of the 1978 original.

[14] T. Katsura, *On the discriminants of the intersection form on Néron–Severi groups,* Algebraic geometry and commutative algebra, Vol. I, pp. 183–201, Kinokuniya, Tokyo, 1988.

[15] T. Katsura and S. Kondō, *Rational curves on the supersingular K3 surface with Artin invariant 1 in characteristic 3,* J. Algebra 352 (2012), 299–321.

[16] ———, *A note on a supersingular K3 surface in characteristic 2,* Geometry and arithmetic, EMS Ser. Congr. Rep., pp. 243–255, Eur. Math. Soc., Zürich, 2012.

[17] J. H. Keum and S. Kondō, *The automorphism groups of Kummer surfaces associated with the product of two elliptic curves,* Trans. Amer. Math. Soc. 353 (2001), no. 4, 1469–1487 (electronic).

[18] S. Kondō, *The automorphism group of a generic Jacobian Kummer surface,* J. Algebraic Geom. 7 (1998), no. 3, 589–609.

[19] S. Kondō and I. Shimada, *The automorphism group of a supersingular $K3$ surface with Artin invariant 1 in characteristic 3,* Int. Math. Res. Not. IMRN 7 (2014), 1885–1924.

[20] D. Mumford, *Abelian varieties,* Tata Inst. Fund. Res. Stud. Math., 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[21] V. V. Nikulin, *Kummer surfaces,* Izv. Akad. Nauk SSSR Ser. Mat. 39 (1975), no. 2, 278–293, 471,

[22] ———, *Integer symmetric bilinear forms and some of their geometric applications,* Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), no. 1, 111–177, 238, English translation: Math USSR Izv. 14 (1979), no. 1, 103–167 (1980).

[23] G. L. Nipp, *Quaternary quadratic forms,* Springer-Verlag, New York, 1991, Computer generated tables, With a 3.5″ IBM PC floppy disk. See also http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/nipp.html.

[24] A. Ogus, *Supersingular $K3$ crystals,* Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II, Astérisque, 64, pp. 3–86, Soc. Math. France, Paris, 1979.

[25] ———, *A crystalline Torelli theorem for supersingular $K3$ surfaces,* Arithmetic and geometry, Vol. II, Progr. Math., 36, pp. 361–394, Birkhäuser Boston, Boston, MA, 1983.

[26] A. N. Rudakov and I. R. Shafarevich, *Surfaces of type $K3$ over fields of finite characteristic,* Current problems in mathematics, 18, pp. 115–207, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981, Reprinted in, Shafarevich, I. R., *Collected mathematical papers,* Springer-Verlag, Berlin, 1989, 657–714.

[27] I. Shimada, *A note on rational normal curves totally tangent to a Hermitian variety,* Des. Codes Cryptogr. 69 (2013), no. 3, 299–303.

[28] ______, *Projective models of the supersingular $K3$ surface with Artin invariant 1 in characteristic 5,* J. Algebra 403 (2014), 273–299.

[29] ______, *An algorithm to compute automorphism groups of $K3$ surfaces,* preprint, 2013, arXiv:1304.7427.

[30] ______, *Supersingular $K3$ surface in characteristic 5: Computational data,* available from http://www.math.sci.hiroshima-u.ac.jp/~shimada/K3.html.

[31] T. Shioda, *Supersingular $K3$ surfaces,* Algebraic geometry, Proc. summer meeting, Univ. Copenhagen, Copenhagen, 1978, Lecture Notes in Math., 732, pp. 564–591, Springer, Berlin, 1979.

[32] J. A. Todd, *A representation of the Mathieu group M_{24} as a collineation group,* Ann. Mat. Pura Appl. (4) 71 (1966), 199–238.

[33] E. Traynard, *Sur les fonctions thêta de deux variables et les surfaces hyperelliptiques,* Ann. Sci. Éc. Norm. Supér. 3 (1907), no. 24, 77–177.

[34] M. Ujikawa, *The automorphism group of the singular $K3$ surface of discriminant 7,* Comment. Math. Univ. St. Pauli 62 (2013), no. 1, 11–29.

T. Katsura
Faculty of Science and Engineering
Hosei University
Koganei-shi, Tokyo, 184-8584
Japan

toshiyuki.katsura.tk@hosei.ac.jp

S. Kondo
Graduate School of Mathematics
Nagoya University
Nagoya, 464-8602
Japan

kondo@math.nagoya-u.ac.jp

I. Shimada
Department of Mathematics
Graduate School of Science
Hiroshima University
1-3-1 Kagamiyama,
Higashi-Hiroshima, 739-8526
Japan

shimada@math.sci.hiroshima-u.ac.jp