TRANSCENDENTAL LATTICES
AND SUPERSINGULAR REDUCTION LATTICES
OF A SINGULAR $K_3$ SURFACE

ICHIRO SHIMADA

Abstract. A $K_3$ surface $X$ defined over a field $k$ of characteristic 0 is called singular if the Néron-Severi lattice $\text{NS}(X)$ of $X \otimes \bar{k}$ is of rank 20. Let $X$ be a singular $K_3$ surface defined over a number field $F$. For each embedding $\sigma : F \hookrightarrow \mathbb{C}$, we denote by $T(X^{\sigma})$ the transcendental lattice of the complex $K_3$ surface $X^{\sigma}$ obtained from $X$ by $\sigma$. For each prime $p$ of $F$ at which $X$ has a supersingular reduction $X_p$, we define $L(X, p)$ to be the orthogonal complement of $\text{NS}(X)$ in $\text{NS}(X_p)$. We investigate the relation between these lattices $T(X^{\sigma})$ and $L(X, p)$. As an application, we give a lower bound for the degree of a number field over which a singular $K_3$ surface with a given transcendental lattice can be defined.

1. Introduction

For a smooth projective surface $X$ defined over a field $k$, we denote by $\text{Pic}(X)$ the Picard group of $X$, and by $\text{NS}(X)$ the Néron-Severi lattice of $X \otimes \bar{k}$, where $\bar{k}$ is the algebraic closure of $k$. When $X$ is a $K_3$ surface, we have a natural isomorphism $\text{Pic}(X \otimes \bar{k}) \cong \text{NS}(X)$. We say that a $K_3$ surface $X$ in characteristic 0 is singular if $\text{NS}(X)$ is of rank 20, while a $K_3$ surface $X$ in characteristic $p > 0$ is supersingular if $\text{NS}(X)$ is of rank 22. It is known ([17], [30], [31]) that every complex singular $K_3$ surface is defined over a number field.

For a number field $F$, we denote by $\text{Emb}(F)$ the set of embeddings of $F$ into $\mathbb{C}$, by $\mathbb{Z}_F$ the integer ring of $F$, and by $\pi_F : \text{Spec} \mathbb{Z}_F \to \text{Spec} \mathbb{Z}$ the natural projection. Let $X$ be a singular $K_3$ surface defined over a number field $F$, and let $\mathcal{X} \to U$ be a smooth proper family of $K_3$ surfaces over a non-empty open subset $U$ of $\text{Spec} \mathbb{Z}_F$ such that the generic fiber is isomorphic to $X$. We put

$$d(X) := \text{disc}(\text{NS}(X)).$$

Remark that we have $d(X) < 0$ by the Hodge index theorem. For $\sigma \in \text{Emb}(F)$, we denote by $X^{\sigma}$ the complex analytic $K_3$ surface obtained from $X$ by $\sigma$. The transcendental lattice $T(X^{\sigma})$ of $X^{\sigma}$ is defined to be the orthogonal complement of $\text{NS}(X) \cong \text{NS}(X^{\sigma})$ in the second Betti cohomology group $H^2(X^{\sigma}, \mathbb{Z})$, which we regard as a lattice by the cup-product. Then $T(X^{\sigma})$ is an even positive-definite lattice of rank 2 with discriminant $-d(X)$. For a closed point $p$ of $U$, we denote by $X_p$ the reduction of $\mathcal{X}$ at $p$. Then $X_p$ is a $K_3$ surface defined over the finite field

Received by the editors November 8, 2006 and, in revised form, April 16, 2007.
2000 Mathematics Subject Classification. Primary 14J28; Secondary 14J20, 14H52.
©2008 American Mathematical Society
Reverts to public domain 28 years from publication

909
If $\Lambda \in L$ is an integer, we denote by $\mathcal{S}_p(\Lambda) := \{ \pi \in U \mid \pi_\pi(p) = p \text{ and } X_\pi \text{ is supersingular} \}$. For each $\pi \in \mathcal{S}_p(\Lambda)$, we have the specialization homomorphism

$$\rho_\pi : \text{NS}(X) \to \text{NS}(X_\pi),$$

which preserves the intersection pairing (see [2 Exp. X], [11 §4] or [12 §20.3]), and hence is injective. We denote by $L(\chi, p)$ the orthogonal complement of $\text{NS}(X)$ in $\text{NS}(X_\pi)$, and call $L(\chi, p)$ the supersingular reduction lattice of $\chi$ at $p$. Then $L(\chi, p)$ is an even negative-definite lattice of rank 2. We will see that, if $p \nmid 2d(X)$, then the discriminant of $L(\chi, p)$ is $-p^2d(X)$. For an odd prime integer $p$ not dividing $x \in \mathbb{Z}$, we denote by

$$\chi_p(x) := \left( \frac{x}{p} \right) \in \{1, -1\}$$

the Legendre character. In [26 Proposition 5.5], we have proved the following. (See Theorem-Definition 1.0.4 for the definition of the Artin invariant.)

**Proposition 1.0.1.** Suppose that $p \nmid 2d(X)$.

1. If $\chi_p(d(X)) = 1$, then $\mathcal{S}_p(\Lambda)$ is empty.
2. If $\pi \in \mathcal{S}_p(\Lambda)$, then the Artin invariant of $X_\pi$ is 1.

The first main result of this paper, which will be proved in Proposition 5.5, is as follows:

**Theorem 1.** There exists a finite set $N$ of prime integers containing the prime divisors of $2d(X)$ such that the following holds:

$$(1.0.1) \quad p \notin N \Rightarrow \mathcal{S}_p(\Lambda) = \begin{cases} \emptyset & \text{if } \chi_p(d(X)) = 1, \\ \pi_\pi^{-1}(p) & \text{if } \chi_p(d(X)) = -1. \end{cases}$$

We put $\mathbb{Z}_\infty := \mathbb{R}$. Let $R$ be $\mathbb{Z}$ or $\mathbb{Z}_l$, where $l$ is a prime integer or $\infty$. An $R$-lattice is a free $R$-module $\Lambda$ of finite rank with a non-degenerate symmetric bilinear form $(\ ,\ ) : \Lambda \times \Lambda \to R$.

The discriminant $\text{disc}(\Lambda) \in R/(R^\times)^2$ of an $R$-lattice $\Lambda$ is the determinant modulo $(R^\times)^2$ of a symmetric matrix expressing $(\ ,\ )$.

A $\mathbb{Z}$-lattice is simply called a lattice. For a lattice $\Lambda$ and a non-zero integer $n$, we denote by $\Lambda[n]$ the lattice obtained from $\Lambda$ by multiplying the symmetric bilinear form $(\ ,\ )$ by $n$. A lattice $\Lambda$ is said to be even if $(v,v) \in 2\mathbb{Z}$ holds for any $v \in \Lambda$. Let $\Lambda$ and $\Lambda'$ be lattices. We denote by $\Lambda \perp \Lambda'$ the orthogonal direct sum of $\Lambda$ and $\Lambda'$. A homomorphism $\Lambda \to \Lambda'$ preserving the symmetric bilinear form is called an isometry. Note that an isometry is injective because of the non-degeneracy of the symmetric bilinear forms. An isometry $\Lambda \to \Lambda'$ (or a sublattice $\Lambda$ of $\Lambda'$) is said to be primitive if the cokernel $\Lambda'/\Lambda$ is torsion-free. The primitive closure of a sublattice $\Lambda \to \Lambda'$ is the intersection of $\Lambda \otimes \mathbb{Q}$ and $\Lambda'$ in $\Lambda' \otimes \mathbb{Q}$. For an isometry $\Lambda \to \Lambda'$, we put

$$(\Lambda \to \Lambda')^\perp := \{ x \in \Lambda' \mid (x,y) = 0 \text{ for all } y \in \Lambda \}.$$ 

Note that $(\Lambda \to \Lambda')^\perp$ is primitive in $\Lambda'$. Let $r$ be a positive integer, and $d$ a non-zero integer. We denote by $\mathcal{L}(r,d)$ the set of isomorphism classes of lattices of rank $r$ with discriminant $d$, and by $[\Lambda] \in \mathcal{L}(r,d)$ the isomorphism class of a lattice $\Lambda$. If $[\Lambda] \in \mathcal{L}(r,d)$, then we have $[\Lambda[n]] \in \mathcal{L}(r, n^r d)$, and the map $\mathcal{L}(r,d) \to \mathcal{L}(r, n^r d)$...
given by $[\Lambda] \mapsto [\Lambda[n]]$ is injective. We denote by $\mathcal{L}^{\text{even}}(r, d)$ (resp. $\mathcal{L}^{\text{pos}}(r, d)$) the set of isomorphism classes in $\mathcal{L}(r, d)$ of even lattices (resp. of positive-definite lattices). We recall the notion of genera of lattices. See [3], for example, for details. Two lattices $\Lambda$ and $\Lambda'$ are said to be in the same genus if $\Lambda \otimes \mathbb{Z}_l$ and $\Lambda' \otimes \mathbb{Z}_l$ are isomorphic as $\mathbb{Z}_l$-lattices for any $l$ (including $\infty$). If $\Lambda$ and $\Lambda'$ are in the same genus, then we have $\text{rank}(\Lambda) = \text{rank}(\Lambda')$ and $\text{disc}(\Lambda) = \text{disc}(\Lambda')$. Therefore the set $\mathcal{L}(r, d)$ is decomposed into the disjoint union of genera. For each non-zero integer $n$, $\Lambda$ and $\Lambda'$ are in the same genus if and only if $\Lambda[n]$ and $\Lambda'[n]$ are in the same genus. Moreover, if $\Lambda''$ is in the same genus as $\Lambda[n]$, then there exists $\Lambda'$ in the same genus as $\Lambda$ such that $[\Lambda''] = [\Lambda'[n]]$ holds. Therefore, for each genus $\mathcal{G} \subset \mathcal{L}(r, d)$, we can define the genus $\mathcal{G}[n] \subset \mathcal{L}(r, n'd)$ by

$$\mathcal{G}[n] := \{ [\Lambda[n]] \mid [\Lambda] \in \mathcal{G} \}.$$  

The map from the set of genera in $\mathcal{L}(r, d)$ to the set of genera in $\mathcal{L}(r, n'd)$ given by $\mathcal{G} \mapsto \mathcal{G}[n]$ is injective. Suppose that $\Lambda$ and $\Lambda'$ are in the same genus. If $\Lambda$ is even (resp. positive-definite), then so is $\Lambda'$. Hence $\mathcal{L}^{\text{even}}(r, d)$ and $\mathcal{L}^{\text{pos}}(r, d)$ are also disjoint unions of genera. We say that a genus $\mathcal{G} \subset \mathcal{L}(r, d)$ is even (resp. positive-definite) if $\mathcal{G} \subset \mathcal{L}^{\text{even}}(r, d)$ (resp. $\mathcal{G} \subset \mathcal{L}^{\text{pos}}(r, d)$) holds.

We review the theory of discriminant forms due to Nikulin [20]. Let $\Lambda$ be an even lattice. We put $\Lambda' := \text{Hom}(\Lambda, \mathbb{Z})$. Then $\Lambda$ is embedded into $\Lambda'$ naturally as a submodule of finite index, and there exists a unique $\mathbb{Q}$-valued symmetric bilinear form on $\Lambda'$ that extends the $\mathbb{Z}$-valued symmetric bilinear form on $\Lambda$. We put

$$D_\Lambda := \Lambda'/\Lambda,$$

which is a finite abelian group of order $|\text{disc}(\Lambda)|$, and define a quadratic form

$$q_\Lambda : D_\Lambda \to \mathbb{Q}/2\mathbb{Z}$$

by $q_\Lambda(x + \Lambda) := (x, x) + 2\mathbb{Z}$ for $x \in \Lambda'$. The finite quadratic form $(D_\Lambda, q_\Lambda)$ is called the discriminant form of $\Lambda$.

**Theorem-Definition 1.0.2** (Corollary 1.9.4 in [20]). Let $\Lambda$ and $\Lambda'$ be even lattices. Then $\Lambda$ and $\Lambda'$ are in the same genus if and only if the following hold:

(i) $\Lambda \otimes \mathbb{Z}_\infty$ and $\Lambda' \otimes \mathbb{Z}_\infty$ are isomorphic as $\mathbb{Z}_\infty$-lattices, and

(ii) the finite quadratic forms $(D_\Lambda, q_\Lambda)$ and $(D_{\Lambda'}, q_{\Lambda'})$ are isomorphic.

Therefore, for an even genus $\mathcal{G}$, we can define the discriminant form $(D_\mathcal{G}, q_\mathcal{G})$ of $\mathcal{G}$.

Next, we define Rudakov-Shafarevich lattices.

**Theorem-Definition 1.0.3** (Section 1 of [23]). For each odd prime $p$ and a positive integer $\sigma \leq 10$, there exists, uniquely up to isomorphism, an even lattice $\Lambda_{p, \sigma}$ of rank 22 with signature $(1, 21)$ such that the discriminant group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2\sigma}$. We call $\Lambda_{p, \sigma}$ a Rudakov-Shafarevich lattice.

**Theorem-Definition 1.0.4** (Artin [1], Rudakov-Shafarevich [23]). For a supersingular K3 surface $Y$ in odd characteristic $p$, there exists a positive integer $\sigma \leq 10$, which is called the Artin invariant of $Y$, such that $\text{NS}(Y)$ is isomorphic to the Rudakov-Shafarevich lattice $\Lambda_{p, \sigma}$.

We denote by $(D_{p, \sigma}^{\text{RS}}, q_{p, \sigma}^{\text{RS}})$ the discriminant form of the Rudakov-Shafarevich lattice $\Lambda_{p, \sigma}$. The finite quadratic form $(D_{p, \sigma}^{\text{RS}}, q_{p, \sigma}^{\text{RS}})$ has been calculated explicitly in our previous paper [26] Proof of Proposition 4.2].
Our second main result, which will be proved in [2] is as follows:

**Theorem 2.** Let $X$ be a singular K3 surface defined over a number field $F$, and let $X \to U$ be a smooth proper family of K3 surfaces over a non-empty open subset $U$ of $\text{Spec} \mathbb{Z}_F$ such that the generic fiber is isomorphic to $X$. We put $d(X) := \text{disc}(\text{NS}(X))$.

(T) There exists a unique genus $G_\mathbb{C}(X) \subset L(2, -d(X))$ such that $[T(X^\sigma)]$ is contained in $G_\mathbb{C}(X)$ for any $\sigma \in \text{Emb}(F)$. This genus $G_\mathbb{C}(X)$ is determined by the properties that it is even, positive-definite, and that the discriminant form is isomorphic to $(D_{\text{NS}(X)}, -q_{\text{NS}(X)})$.

(L) Let $p$ be a prime integer not dividing $2d(X)$. Suppose that $S_p(X) \neq \emptyset$. Then there exists a unique genus $G_p(X) \subset L(2, -d(X))$ such that $[L(X, p)]$ is contained in $G_p(X)[-p]$ for any $p \in S_p(X)$. This genus $G_p(X)$ is determined by the properties that it is even, positive-definite, and that the discriminant form of $G_p(X)[-p]$ is isomorphic to $(D_{\text{NS}_p(X)}, -q_{\text{NS}_p(X)})$. To ease notation, we put

$$M[a, b, c] := \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}.$$ 

Let $D$ be a negative integer. We then put

$$(1.0.2) \quad Q_D := \{ M[a, b, c] \mid a, b, c \in \mathbb{Z}, \quad a > 0, \quad b > 0, \quad b^2 - 4ac = D \},$$

$$(1.0.3) \quad Q_D^* := \{ M[a, b, c] \in Q_D \mid \gcd(a, b, c) = 1 \}.$$ 

The group $\text{GL}_2(\mathbb{Z})$ acts on $Q_D$ from the right by $(M, g) \mapsto g^T M g$ for $M \in Q_D$ and $g \in \text{GL}_2(\mathbb{Z})$, and the subset $Q_D$ of $Q_D$ is stable by this action. We put

$$\mathcal{L}_D := Q_D / \text{GL}_2(\mathbb{Z}), \quad \mathcal{L}_D^* := Q_D^* / \text{GL}_2(\mathbb{Z}),$$

$$\tilde{\mathcal{L}}_D := Q_D / \text{SL}_2(\mathbb{Z}), \quad \tilde{\mathcal{L}}_D^* := Q_D^* / \text{SL}_2(\mathbb{Z}).$$

Then we have a natural identification

$$\mathcal{L}_D = \mathcal{L}_{\text{pos}}^2(2, -D) \cap \mathcal{L}_{\text{even}}(2, -D),$$

and $\tilde{\mathcal{L}}_D$ is regarded as the set of isomorphism classes of even positive-definite oriented lattices of rank 2 with discriminant $-D$.

Let $S$ be a complex K3 surface or a complex abelian surface. Suppose that the transcendental lattice $T(S) := (\text{NS}(S) \hookrightarrow H^2(S, \mathbb{Z}))^\perp$ of $S$ is of rank 2. Then $T(S)$ is even, positive-definite and of discriminant $-d(S)$, where $d(S) := \text{disc}(\text{NS}(S))$. By the Hodge structure

$$T(S) \otimes \mathbb{C} = H^{2,0}(S) \oplus H^{0,2}(S)$$

of $T(S)$, we can define a **canonical orientation** on $T(S)$ as follows. An ordered basis $(e_1, e_2)$ of $T(S)$ is said to be positive if the imaginary part of $(e_1, \omega_S)/(e_2, \omega_S) \in \mathbb{C}$ is positive, where $\omega_S$ is a basis of $H^{2,0}(S)$. We denote by $\tilde{T}(S)$ the oriented transcendental lattice of $S$, and by $[\tilde{T}(S)] \in \mathcal{L}_{d(S)}$ the isomorphism class of $\tilde{T}(S)$.

We have the following important theorem due to Shioda and Inose [30]:

**Theorem 1.0.5 ([30]).** The map $S \mapsto [\tilde{T}(S)]$ gives rise to a bijection from the set of isomorphism classes of complex singular K3 surfaces $S$ to the set of isomorphism classes of even positive-definite oriented lattices of rank 2.
If a genus \( G \subset L_D \) satisfies \( G \cap L^*_D \neq \emptyset \), then \( G \subset L^*_D \) holds. Therefore \( L^*_D \) is a disjoint union of genera. For a genus \( G \subset L_D \), we denote by \( \bar{G} \) the pull-back of \( G \) by the natural projection \( \bar{L}_D \to L_D \), and call \( \bar{G} \subset \bar{L}_D \) a lifted genus.

A negative integer \( D \) is called a fundamental discriminant if it is the discriminant of an imaginary quadratic field.

Our third main result, which will be proved in §6.6 and 6.7, is as follows:

**Theorem 3.** Let \( S \) be a complex singular K3 surface. Suppose that \( D := \text{disc}(\text{NS}(S)) \) is a fundamental discriminant, and that \([T(S)]\) is contained in \( L_D^* \).

(T) There exists a singular K3 surface \( X \) defined over a number field \( F \) such that \( \{ [\bar{T}(X^\sigma)] \mid \sigma \in \text{Emb}(F) \} \) is equal to the lifted genus in \( \bar{L}_D^* \) that contains \([\bar{T}(S)]\). In particular, there exists \( \sigma_0 \in \text{Emb}(F) \) such that \( X^{\sigma_0} \) is isomorphic to \( S \) over \( \mathbb{C} \).

(L) Suppose further that \( D \) is odd. Then there exists a smooth proper family \( \mathcal{X} \to U \) of K3 surfaces over a non-empty open subset \( U \) of \( \text{Spec}\mathbb{Z}_F \), where \( F \) is a number field, such that the following hold:

(i) the generic fiber \( X \) of \( \mathcal{X} \to U \) satisfies the property in (T) above,
(ii) if \( p \in \pi_F(U) \), then \( p \not\equiv D \), and
(iii) if \( p \in \pi_F(U) \) and \( \chi_p(D) = -1 \), then \( S_p(X) = \pi_F^{-1}(p) \) holds, and the set \( \{ [L(X, \mathfrak{p})] \mid \mathfrak{p} \in S_p(X) \} \) coincides with a genus in \( L(2, -p^2D) \).

Suppose that \( D \) is a negative fundamental discriminant. The set \( \bar{L}_D^* \) and its decomposition into lifted genera are very well understood by the work of Gauss. We review the theory briefly. We put \( K := \mathbb{Q}(\sqrt{D}) \), and denote by \( I_D \) the multiplicative group of non-zero fractional ideals of \( K \), by \( \mathcal{P}_D \subset I_D \) the subgroup of non-zero principal fractional ideals, and by \( Cl_D := I_D/\mathcal{P}_D \) the ideal class group of \( K \). Let \( I \) be an element of \( I_D \). We denote by \([I] \in Cl_D \) the ideal class of \( I \). We put

\[
N(I) := [\mathbb{Z}_K : nI]/n^2,
\]

where \( n \) is an integer \( \neq 0 \) such that \( nI \subset \mathbb{Z}_K \), and define a bilinear form on \( I \) by

\[
(x, y) := (x\bar{y} + y\bar{x})/N(I) = \text{Tr}_{K/\mathbb{Q}}(x\bar{y})/N(I).
\]

We say that an ordered basis \((\omega_1, \omega_2)\) of \( I \) as a \( \mathbb{Z} \)-module is positive if

\[
(\omega_1\bar{\omega}_2 - \omega_2\bar{\omega}_1)/\sqrt{D} > 0.
\]

By the bilinear form [10.24] and the orientation [10.3], the \( \mathbb{Z} \)-module \( I \) of rank 2 obtains a structure of an even positive-definite oriented lattice with discriminant \(-D\). The isomorphism class of this oriented lattice is denoted by \( \psi(I) \in \bar{L}_D \). For the following, see [5] Theorems 5.2.8 and 5.2.9] and [7] Theorem 3.15, for example.

**Proposition 1.0.6.** (1) The map \( \psi : I_D \to \bar{L}_D \) defined above induces a bijection \( \Psi : Cl_D \cong \bar{L}_D^* \) with the inverse given by the following. Let \([A] \in \bar{L}_D^* \) be represented by \( M[a, b, c] \in \mathcal{Q}_D^* \), and let \( I \in I_D \) be the fractional ideal generated by \( \omega_1 = (-b + \sqrt{D})/2 \) and \( \omega_2 = a \). Then \( \psi([I]) = [\psi(I)] \) is equal to \([A]\).

(2) Let \([I]\) and \([J]\) be elements of \( Cl_D \). Then \( \Psi([I]) \) and \( \Psi([J]) \) are in the same lifted genus if and only if \([I][J]^{-1} \) is contained in \( \mathcal{Q}_D^2 := \{ x^2 \mid x \in Cl_D \} \). In particular, every lifted genus in \( \bar{L}_D^* \) consists of the same number of isomorphism classes, and the cardinality is equal to \( |Cl_D^2| \).
Using Theorems 1.0.5 and 3(T), we obtain the following:

**Corollary 4.** Let \( S \) be a complex singular \( K3 \) surface such that \( D := \text{disc(}\text{NS}(S)\text{)} \) is a fundamental discriminant and such that \( |T(S)| \) is contained in \( \mathcal{L}_D^* \). Let \( Y \) be a \( K3 \) surface defined over a number field \( L \) such that \( Y^{\tau_0} \) is isomorphic to \( S \) over \( \mathbb{C} \) for some \( \tau_0 \in \text{Emb}(L) \). Then we have \( |L : \mathbb{Q}| \geq |\text{Cl}_D^2| \).

**Proof.** Let \( X \) be the \( K3 \) surface defined over a number field \( F \) given in Theorem 3(T). Then the complex \( K3 \) surfaces \( X^{\sigma_0} \) and \( Y^{\tau_0} \) are isomorphic over \( \mathbb{C} \), and hence there exists a number field \( M \subset \mathbb{C} \) containing both of \( \sigma_0(F) \) and \( \tau_0(L) \) such that \( X \otimes M \) and \( Y \otimes M \) are isomorphic over \( M \). Therefore, for each \( \sigma \in \text{Emb}(F) \), there exists \( \tau \in \text{Emb}(L) \) such that \( X^\sigma \) is isomorphic to \( Y^\tau \) over \( \mathbb{C} \).

Since there exist exactly \( |\text{Cl}_D^2| \) isomorphism classes of complex \( K3 \) surfaces among \( X^\sigma \) (\( \sigma \in \text{Emb}(F) \)), we have \( |\text{Emb}(L)| \geq |\text{Cl}_D^2| \). \( \square \)

The proof of Theorem 2 is in fact an easy application of Nikulin’s theory of discriminant forms, and is given in [2]. The main tool of the proof of Theorems 1 and 3 is the Shioda-Inose-Kummer construction [30]. This construction forms a singular \( K3 \) surface \( Y \) from a pair of elliptic curves \( E' \) and \( E \). Shioda and Inose [30] proved that, over \( \mathbb{C} \), the transcendental lattices of \( Y \) and \( E' \times E \) are isomorphic. We present their construction in our setting, and show that, over a number field, the supersingular reduction lattices of \( Y \) and \( E' \times E \) are also isomorphic under certain assumptions. The supersingular reduction lattice of \( E' \times E \) is calculated by the specialization homomorphism \( \text{Hom}(E', E) \rightarrow \text{Hom}(E'_p, E_p) \). In [3] we investigate the Hom-lattices of elliptic curves. After examining the Kummer construction in [4] and the Shioda-Inose construction in [5] we prove Theorems 1 and 3 in [6].

For Theorem 3(T), we use the Shioda-Mitani theory [33]. For Theorem 3(L), we need a description of embeddings of \( \mathbb{Z}_K \) into maximal orders of a quaternion algebra over \( \mathbb{Q} \). We use Dorman’s description [9], which we expound in [10].

In [22], Shafarevich studied, by means of the Shioda-Inose-Kummer construction, number fields over which a singular \( K3 \) surface with a prescribed Néron-Severi lattice can be defined, and proved a certain finiteness theorem.

The supersingular reduction lattices and their relation to the transcendental lattice were first studied by Shioda [32] for certain \( K3 \) surfaces. Thanks are due to Professor Tetsuji Shioda for stimulating conversations and many comments.

After the first version of this paper appeared on the e-print archive, Schütt [24] has succeeded in removing the assumptions in Theorem 3(T) and Corollary 4 that \( D = \text{disc(}\text{NS}(S)\text{)} \) be a fundamental discriminant, and that \( |T(S)| \) be in \( \mathcal{L}_D^* \). Interesting examples of singular \( K3 \) surfaces defined over number fields are also given in [24 §7].

Applications of Theorem 3(T) to topology and its generalization by Schütt [24] are given in [27] and [28].

The author expresses gratitude to the referee for many comments and suggestions improving the exposition.

Let \( W \) be a Dedekind domain. For \( P \in \text{Spec} W \), we put

\[
\kappa_p := \begin{cases} 
\text{the quotient field of } W & \text{if } P \text{ is the generic point,} \\
W/p & \text{if } P \text{ is a closed point } p.
\end{cases}
\]
2. Proof of Theorem 2

2.1. The discriminant form of an orthogonal complement. The following can be derived from [20] Proposition 1.5.1. We give a simple and direct proof.

**Proposition 2.1.1.** Let \( L \) be an even lattice, and \( M \subset L \) a primitive sublattice. We put \( N := (M \hookrightarrow L)^\bot \). Suppose that \( \text{disc}(M) \) and \( \text{disc}(L) \) are prime to each other. Then there exists an isomorphism

\[
(D_N, q_N) \cong (D_L, q_L) \oplus (D_M, -q_M)
\]

of finite quadratic forms. In particular, we have \( \text{disc}(N) = \text{disc}(L)\text{disc}(M) \).

**Proof.** We put \( d_L := |\text{disc}(L)| = |D_L| \). The multiplication by \( d_L \) induces an automorphism \( \delta_L : D_M \cong D_M \) of \( D_M \) by the assumption. We regard \( L, M, N \) and \( L^\vee, M^\vee, N^\vee \) as submodules of \( L \otimes \mathbb{Q} = (M \otimes \mathbb{Q}) \oplus (N \otimes \mathbb{Q}) \). First we show that

\[
(2.1.1)
\]

\[ L^\vee \cap M^\vee = M. \]

The inclusion \( \supseteq \) is obvious. Suppose that \( x \in L^\vee \cap M^\vee \). Then we have \( d_L x \in L \). Since \( M \) is primitive in \( L \), we have \( L \cap M^\vee = M \), and hence \( \delta_L(x + M) = 0 \) holds in \( D_M \). Because \( \delta_L \) is an automorphism of \( D_M \), we have \( x \in M \). Next we show that the composite of natural homomorphisms

\[
(2.1.2)
\]

\[
L \hookrightarrow L^\vee \twoheadrightarrow M^\vee \twoheadrightarrow D_M
\]

is surjective. Let \( \xi \in D_M \) be given. There exists \( \eta \in D_M \) such that \( \delta_L(\eta) = \xi \). Since \( L^\vee \twoheadrightarrow M^\vee \) is surjective by the primitivity of \( M \hookrightarrow L \), there exists a \( y \in L^\vee \) that is mapped to \( \eta \). Then \( x := d_L y \) is in \( L \) and is mapped to \( \xi \). We define a homomorphism \( \tau : D_N \to D_L \oplus D_M \) as follows. Let \( x \in N^\vee \) be given. Since \( L^\vee \twoheadrightarrow N^\vee \) is surjective by the primitivity of \( N \hookrightarrow L \), there exists a \( z \in L^\vee \) that is mapped to \( x \). Let \( y \in M^\vee \) be the image of \( z \) by \( L^\vee \twoheadrightarrow M^\vee \). We put

\[
\tau(x + N) := (z + L, y + M).
\]

The well-definedness of \( \tau \) follows from the formula (2.1.1). Since \( z = (y, x) \) in \( L^\vee \subset M^\vee \oplus N^\vee \), we have \( q_N(x + N) = q_L(z + L) - q_M(y + M) \). The injectivity of \( \tau \) follows from \( L \cap N^\vee = N \). Since the homomorphism (2.1.2) is surjective, the homomorphism \( \tau \) is also surjective. \( \square \)

2.2. The cokernel of the specialization isometry. Let \( W \) be a Dedekind domain with the quotient field \( F \) being a number field, and let \( \mathcal{X} \to U := \text{Spec} W \) be a smooth proper family of K3 surfaces. We put \( X := \mathcal{X} \otimes F \). In this subsection, we do not assume that \( \text{rank}(\text{NS}(X)) = 20 \). Let \( \mathfrak{p} \) be a closed point of \( U \) such that \( X_0 := \mathcal{X} \otimes \kappa_{\mathfrak{p}} \) is supersingular. We consider the specialization isometry

\[
\rho : \text{NS}(X) = \text{Pic}(X \otimes \overline{F}) \hookrightarrow \text{NS}(X_0) = \text{Pic}(X_0 \otimes \overline{\kappa_{\mathfrak{p}}}),
\]

whose definition is given in [2] Exp. X] or [11] §4]. We put \( p := \text{char} \kappa_{\mathfrak{p}} \).

**Proposition 2.2.1.** Every torsion element of \( \text{Coker}(\rho) \) has order a power of \( p \).

**Proof.** We denote by \( \overline{F} \) the completion of \( F \) at \( \mathfrak{p} \), and by \( \hat{\mathcal{X}} \) the valuation ring of \( \overline{F} \) with the maximal ideal \( \hat{\mathfrak{p}} \). Let \( \hat{L} \) be a finite extension of \( \overline{F} \) with the valuation ring \( \hat{B} \), the maximal ideal \( \hat{m} \), and the residue field \( \kappa_{\hat{m}} \) such that there exist natural isomorphisms \( \text{Pic}(X \otimes \hat{L}) \cong \text{NS}(X) \) and \( \text{Pic}(X_0 \otimes \kappa_{\hat{m}}) \cong \text{NS}(X_0) \). Then \( \rho \) is obtained from the restriction isomorphism

\[
\text{Pic}(\mathcal{X} \otimes \hat{B}) \cong \text{Pic}(X \otimes \hat{L})
\]
to the generic fiber, whose inverse is given by taking the closure of divisors, and the restriction homomorphism
\[(2.2.1) \quad \text{Pic}(\mathcal{X} \otimes \hat{\mathcal{X}}) \to \text{Pic}(X_0 \otimes \kappa_{\mathfrak{m}})\]
to the central fiber. Therefore it is enough to show that the order of any torsion element of the cokernel of the homomorphism (2.2.1) is a power of $p$. We put
\[\mathcal{Y} := \mathcal{X} \otimes \hat{\mathcal{X}} \quad \text{and} \quad Y_n := \mathcal{Y} \otimes (\hat{\mathcal{X}}/\mathfrak{m}^{n+1}).\]
Let $\hat{Y}$ be the formal scheme obtained by completing $\mathcal{Y}$ along $Y_0 = X_0 \otimes \kappa_{\mathfrak{m}}$. Note that $(\mathcal{Y}, Y_0)$ satisfies the effective Lefschetz condition $\text{Leff}(\mathcal{Y}, Y_0)$ in [15, Exp. X]. (See [16, Theorem 9.7 in Chap. II].) Hence, by [15, Proposition 2.1 in Exp. XI], we have $\text{Pic}(\mathcal{Y}) \cong \text{Pic}(\hat{Y})$. On the other hand, we have $\text{Pic}(\hat{Y}) = \text{proj} \lim \text{Pic}(Y_n)$ by [16, Exercise 9.6 in Chap. II]. Let $\mathcal{O}_n$ denote the structure sheaf of $Y_n$. From the natural exact sequence $0 \to \mathcal{O}_0 \to \mathcal{O}_n^{\times} \to \mathcal{O}_n^{\times} \to 1$ (see [15, Exp. XI]), we obtain an exact sequence
\[0 \to \text{Pic}(Y_{n+1}) \to \text{Pic}(Y_n) \to H^2(Y_0, \mathcal{O}_0).\]
In particular, the projective limit of $\text{Pic}(Y_n)$ is equal to $\bigcap_n \text{Pic}(Y_n)$. Since every non-zero element of $H^2(Y_0, \mathcal{O}_0)$ is of order $p$, every torsion element of $\text{Pic}(Y_0)/\bigcap_n \text{Pic}(Y_n)$ is of order a power of $p$. \hfill \square

Let $\text{NS}(X)$ be the primitive closure of $\text{NS}(X)$ in $\text{NS}(X_0)$. Then the index of $\text{NS}(X)$ in $\text{NS}(X)$ is a divisor of $\text{disc}(\text{NS}(X))$. Therefore we obtain the following:

**Corollary 2.2.2.** If $p$ does not divide $\text{disc}(\text{NS}(X))$, then the specialization isometry $\rho : \text{NS}(X) \to \text{NS}(X_0)$ is primitive.

**Remark 2.2.3.** Artin [1, §1] showed a similar result over an equal characteristic base. Note that the definition of supersingularity in [1, Definition (0.3)] differs from ours.

### 2.3. Proof of Theorem 2

Let $X \to \text{Spec} F$ and $\mathcal{X} \to U$ be as in the statement of Theorem 2. Note that $\text{NS}(X)$ is of signature $(1, 19)$, while the lattice $H^2(X^\sigma, \mathbb{Z})$ is even, unimodular and of signature $(3, 19)$ for any $\sigma \in \text{Emb}(F)$. Hence $T(X^\sigma)$ is even, positive-definite of rank 2, and its discriminant form is isomorphic to $(D_{\text{NS}(X)}, -q_{\text{NS}(X)})$ by Proposition 2.1.1. Therefore $[T(X^\sigma)]$ is contained in the genus $\mathcal{G} \subset \mathcal{L}_{d(X)}$ characterized by $(D_\mathcal{G}, q_\mathcal{G}) \cong (D_{\text{NS}(X)}, -q_{\text{NS}(X)})$.

Let $p$ be a point of $\mathcal{S}_p(\mathcal{X})$ with $p/2d(X)$. Since the Artin invariant of $X_p$ is 1 by Proposition 1.0.1, we have $\text{NS}(X_p) \cong \Lambda_{p, 1}$ by Theorem 1.0.4. Therefore $L(\mathcal{X}, p)$ is even and negative-definite of rank 2. On the other hand, Corollary 2.2.2 implies that the specialization isometry $\rho$ is primitive, and hence the discriminant form of $L(\mathcal{X}, p)$ is isomorphic to $(D_{\text{NS}(X)}, -q_{\text{NS}(X)}) \oplus (D_{\text{NS}(X)}, -q_{\text{NS}(X)})$ by Proposition 2.1.1. It remains to show that there exists $[M] \in \mathcal{L}_{d(X)}$ such that $L(\mathcal{X}, p) \cong M[-p]$, or equivalently, we have $(x, y) \in p\mathbb{Z}$ for any $x, y \in L(\mathcal{X}, p)$. This follows from the following lemma, whose proof was given in [29].

**Lemma 2.3.1.** Let $p$ be an odd prime integer, and $L$ an even lattice of rank 2. If the $p$-part of $D_L$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, then $(x, y) \in p\mathbb{Z}$ holds for any $x, y \in L$. 

3. Hom-lattice

3.1. Preliminaries. Let $E'$ and $E$ be elliptic curves defined over a field $k$. We denote by $\text{Hom}_k(E', E)$ the $\mathbb{Z}$-module of homomorphisms from $E'$ to $E$ defined over $k$, and put

$$\text{Hom}(E', E) := \text{Hom}_k(E' \otimes \bar{k}, E \otimes \bar{k}),$$

$$\text{End}(E) := \text{Hom}(E, E) \quad \text{and} \quad \text{End}(E') := \text{Hom}(E', E) = \text{End}^k(E \otimes \bar{k}).$$

The Zariski tangent space $T_O(E)$ of $E$ at the origin $O$ is a one-dimensional $k$-vector space, and hence $\text{End}_k(T_O(E))$ is canonically isomorphic to $k$. By the action of $\text{End}_k(E)$ on $T_O(E)$, we have a representation

$$\text{Lie} : \text{End}_k(E) \to \text{End}_k(T_O(E)) = k.$$

According to §3.4, we work over an algebraically closed field $k$. For an elliptic curve $E$, we denote by $\text{Hom}_k(E', E)$ the subfield $k$ of $\text{Hom}(E', E)$ by

$$(f, g) := \deg(f + g) - \deg(f) - \deg(g).$$

We consider the product abelian surface

$$A := E' \times E.$$

Let $O' \in E'$ and $O \in E$ be the origins. We put

$$(3.1.1) \quad \xi := [E' \times \{O\}] \in \text{NS}(A), \quad \eta := [\{O'\} \times E] \in \text{NS}(A),$$

and denote by $U(A)$ the sublattice of $\text{NS}(A)$ spanned by $\xi$ and $\eta$, which is even, unimodular and of signature $(1, 1)$. The following is classical. See [37], for example.

Proposition 3.1.1. The lattice $\text{NS}(A)$ is isomorphic to $U(A)$ ⊥ $\text{Hom}(E', E)[-1]$. In particular, the lattice $\text{Hom}(E', E)$ is even and positive-definite.

One can easily prove the following propositions by means of, for example, the results in §9 in Chap. III and §3.

Proposition 3.1.2. Suppose that $\text{char} k = 0$. Then the following are equivalent:

(i) $\text{rank}(\text{Hom}(E', E)) = 2$.
(ii) $E'$ and $E$ are isogenous over $k$, and $\text{rank}(\text{End}(E')) = 2$.
(iii) There exists an imaginary quadratic field $K$ such that both of $\text{End}(E') \otimes \mathbb{Q}$ and $\text{End}(E) \otimes \mathbb{Q}$ are isomorphic to $K$.

Proposition 3.1.3. Suppose that $\text{char} k > 0$. Then the following are equivalent:

(i) $\text{rank}(\text{Hom}(E', E)) = 4$.
(ii) $E'$ and $E$ are isogenous over $k$, and $\text{rank}(\text{End}(E')) = 4$.
(iii) Both of $E'$ and $E$ are supersingular.

3.2. The elliptic curve $E'$. To the end of §3.4, we work over an algebraically closed field $k$. For an elliptic curve $E$, we denote by $k(E)$ the function field of $E$.

Definition 3.2.1. Two non-zero isogenies $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ are isomorphic if there exists an isomorphism $\psi : E_1 \cong E_2$ such that $\psi \circ \phi_1 = \phi_2$ holds, or equivalently, if the subfields $\phi_1^*k(E_1)$ and $\phi_2^*k(E_2)$ of $k(E)$ are equal.

For a non-zero endomorphism $a \in \text{End}(E)$, we denote by $E^a$ the image of $a$; that is, $E^a$ is an elliptic curve isomorphic to $E$ with an isogeny $a : E \to E^a$. The function field $k(E^a)$ is canonically identified with the subfield $a^*k(E) = \{a^*f \mid f \in k(E)\}$ of $k(E)$, and we have $[k(E) : k(E^a)] = \deg a$. 
**Definition 3.2.2.** Let \( J \subset \text{End}(E) \) be a non-zero left-ideal of \( \text{End}(E) \). We denote by \( k(E^J) \subset k(E) \) the composite of the subfields \( k(E^a) \) for all non-zero \( a \in J \). Then \( k(E^J) \) is a function field of an elliptic curve \( E^J \). We denote by
\[
\phi^J : E \rightarrow E^J
\]
the isogeny corresponding to \( k(E^J) \hookrightarrow k(E) \).

**Remark 3.2.3.** Let \( a, b \in \text{End}(E) \) be non-zero. Since \( ba(x) = b(a(x)) \), we have the canonical inclusions \( k(E^{ba}) \subset k(E^a) \subset k(E) \). Hence, if the left ideal \( J \) is generated by non-zero elements \( a_1, \ldots, a_t \), then \( k(E^J) \) is the composite of \( k(E^{a_1}), \ldots, k(E^{a_t}) \).

**Remark 3.2.4.** The isogeny \( \phi^J : E \rightarrow E^J \) is characterized by the following properties: (i) every \( a \in J \) factors through \( \phi^J \), and (ii) if every \( a \in J \) factors through an isogeny \( \psi : E \rightarrow E' \), then \( \phi^J \) factors through \( \psi \).

### 3.3. The Hom-lattice in characteristic 0

In this subsection, we assume that \( k = \bar{k} \) is of characteristic 0, and that the conditions in Proposition 3.1.2 are satisfied.

We denote by \( D \) the discriminant of the imaginary quadratic field \( K \) in the condition (iii) of Proposition 3.1.2. Note that \( \text{End}(E) \) is isomorphic to a \( \mathbb{Z} \)-subalgebra of \( \mathbb{Z}_K \) with \( \mathbb{Z} \)-rank 2, and that there exist two embeddings of \( \text{End}(E) \) into \( \mathbb{Z}_K \) as a \( \mathbb{Z} \)-subalgebra that are conjugate over \( \mathbb{Q} \). Each embedding \( \text{End}(E) \hookrightarrow \mathbb{Z}_K \) is an isometry of lattices, where \( \mathbb{Z}_K \) is considered as a lattice by the formula (3.1.4), because the dual endomorphism corresponds to the conjugate element over \( \mathbb{Q} \).

**Proposition 3.3.1.** There exist non-zero integers \( m \) and \( n \) such that
\[
m^2 \text{disc}(\text{Hom}(E', E)) = -n^2 D. \tag{3.3.1}
\]

**Proof.** There exists a non-zero isogeny \( \alpha : E \rightarrow E' \). Then the map \( g \mapsto g \circ \alpha \) induces an isometry \( \Phi_\alpha \) from \( \text{Hom}(E', E) [\deg \alpha] \) to \( \text{End}(E) \). Putting \( m := \deg \alpha \) and \( n := [\mathbb{Z}_K : \text{End}(E)] \cdot |\text{Coker} \Phi_\alpha| \), we obtain the equality (3.3.1). \( \square \)

**Definition 3.3.2.** Since \( k = k \), we have \( \text{Lie} : \text{End}(E) \rightarrow k \). Suppose that an embedding \( i : K \hookrightarrow k \) is fixed. Then an embedding \( \iota : \text{End}(E) \hookrightarrow \mathbb{Z}_K \) as a \( \mathbb{Z} \)-subalgebra is called \( \text{Lie-normalized} \) if \( \text{Lie} : \text{End}(E) \rightarrow k \) coincides with the composite of \( \iota : \text{End}(E) \hookrightarrow \mathbb{Z}_K \), the inclusion \( \mathbb{Z}_K \hookrightarrow k \) and \( i : K \hookrightarrow k \).

**Definition 3.3.3.** Suppose that \( k = \mathbb{C} \), and that \( \text{End}(E) \cong \mathbb{Z}_K \). We fix an embedding \( K \hookrightarrow \mathbb{C} \). Let \( \Lambda \subset \mathbb{C} \) be a \( \mathbb{Z} \)-submodule of rank 2 such that \( E \cong \mathbb{C}/\Lambda \) as a Riemann surface. For an ideal class \([I]\) of \( \mathbb{Z}_K \) represented by a fractional ideal \( I \subset K \subset \mathbb{C} \), we denote by \([I] \ast E\) the complex elliptic curve \( \mathbb{C}/I^{-1}\Lambda \), where \( I^{-1}\Lambda \) is the \( \mathbb{Z} \)-submodule of \( \mathbb{C} \) generated by \( x\lambda \) (\( x \in I^{-1}, \lambda \in \Lambda \)). When \( I \subset \mathbb{Z}_K \), we have \( I^{-1}\Lambda \supset \Lambda \), and the identity map \( \text{id}_\mathbb{C} \) of \( \mathbb{C} \) induces an isogeny
\[
an \phi^J : E = \mathbb{C}/\Lambda \rightarrow [I] \ast E = \mathbb{C}/I^{-1}\Lambda.
\]

**Proposition 3.3.4.** Suppose that \( k = \mathbb{C} \), and that \( \text{End}(E) \cong \mathbb{Z}_K \). For an ideal \( J \subset \text{End}(E) \), the isogeny \( \phi^J : E \rightarrow E^J \) is isomorphic to \( an \phi^J : E \rightarrow [J] \ast E \), where \( J \) is regarded as an ideal of \( \mathbb{Z}_K \) by the Lie-normalized isomorphism \( \text{End}(E) \cong \mathbb{Z}_K \).

**Proof.** Suppose that \( E = \mathbb{C}/\Lambda \). We choose \( \Lambda' \subset \mathbb{C} \) such that \( E^J = \mathbb{C}/\Lambda' \) and such that \( \phi^J : E = \mathbb{C}/\Lambda \rightarrow E^J = \mathbb{C}/\Lambda' \) is given by \( \text{id}_\mathbb{C} \). For a non-zero \( a \in J \), we have \((1/a)\Lambda \supset \Lambda \) and there exists a canonical isomorphism \( E^a = \mathbb{C}/(1/a)\Lambda \) such that \( a : E \rightarrow E^a \) is given by \( \text{id}_\mathbb{C} \). Therefore \( \Lambda' \) is the largest \( \mathbb{Z} \)-submodule of \( \mathbb{C} \) that is contained in \((1/a)\Lambda\) for any non-zero \( a \in J \). Hence we have \( \Lambda' = J^{-1}\Lambda \). \( \square \)
LATTICES OF A SINGULAR $K3$ SURFACE

From this analytic description of $\phi^J : E \to E^J$, we obtain the following, which holds in any field of characteristic 0.

**Proposition 3.3.5.** Suppose that char $k = 0$ and that $\text{End}(E) \cong \mathbb{Z}_K$. Let $J$ be an ideal of $\text{End}(E)$. Then $\text{End}(E^J)$ is also isomorphic to $\mathbb{Z}_K$. Moreover, deg $\phi^J$ is equal to $|\text{End}(E)/J|$, and the image of the map

$$\Phi^J : \text{Hom}(E^J, E) \to \text{End}(E)$$

given by $g \mapsto g \circ \phi^J$ coincides with $J$.

3.4. The Hom-lattice of supersingular elliptic curves. In this subsection, we assume that $k = \bar{k}$ is of characteristic $p > 0$, and that the conditions in Proposition 3.1.3 are satisfied. In particular, $E$ is a supersingular elliptic curve.

We denote by $B$ the quaternion algebra over $\mathbb{Q}$ that ramifies exactly at $p$ and $\infty$. It is well known that $B$ is unique up to isomorphism. We denote by $x \mapsto x^*$ the canonical involution of $B$. Then $B$ is equipped with a positive-definite $\mathbb{Q}$-valued symmetric bilinear form defined by

$$(x, y) := xy^* + yx^*. \tag{3.4.1}$$

A subalgebra of $B$ is called an order if its $\mathbb{Z}$-rank is 4. An order is said to be maximal if it is maximal among orders with respect to the inclusion. If $R$ is an order of $B$, then the bilinear form (3.4.1) takes values in $\mathbb{Z}$ on $R$, and $R$ becomes an even lattice. It is known that $R$ is maximal if and only if the discriminant of $R$ is $p^2$. The following are the classical results due to Deuring [8]. (See also [18, Chapter 13, Theorem 9].)

**Proposition 3.4.1.** There exists a maximal order $R$ of $B$ such that $\text{End}(E)$ is isomorphic to $R$ as a $\mathbb{Z}$-algebra. The canonical involution of $R$ corresponds to the involution $\phi \mapsto \phi^*$ of $\text{End}(E)$, where $\phi^*$ is the dual endomorphism. Hence the lattice $\text{End}(E)$ is isomorphic to the lattice $R$, and we have $\text{disc}(\text{End}(E)) = p^2$.

Conversely, we have the following:

**Proposition 3.4.2.** Let $R$ be a maximal order of $B$. Then there exists a supersingular elliptic curve $E_R$ such that $\text{End}(E_R)$ is isomorphic to $R$ as a $\mathbb{Z}$-algebra.

We fix an isomorphism $\text{End}(E) \otimes \mathbb{Q} \cong B$ such that $\text{End}(E)$ is mapped to a maximal order $R$ of $B$. Let $J$ be a non-zero left-ideal of $\text{End}(E)$. Consider the left- and right-orders

$$O_l(J) := \{ x \in B \mid xJ \subset J \}, \quad O_r(J) := \{ x \in B \mid Jx \subset J \}$$

of $J$. Since $O_l(J)$ contains $R$ and $R$ is maximal, $O_l(J)$ is maximal, and hence $O_r(J)$ is also maximal by [22, Theorem (21.2)]. In other words, $J$ is a normal ideal of $B$. We denote by $\text{nr}(J)$ the greatest common divisor of the integers

$$\text{nr}(\phi) := \phi \phi^* = \text{deg} \phi \quad (\phi \in J). \tag{3.4.2}$$

(See [22, Corollary (24.12)].) Then, by [22, Theorem (24.11)], we have

$$\text{nr}(J)^2 = |R/J|. \tag{3.4.3}$$

On the other hand, Deuring [8, (2.3)] proved the following:
Proposition 3.4.3. The image of the map $\Phi^J : \text{Hom}(E^J, E) \to \text{End}(E)$ given by $g \mapsto g \circ \phi^J$ is equal to $J$.

Proof. By Remark 3.2.4, we have $J \subseteq \text{Im} \Phi^J$. Suppose that there exists $a \in \text{Im} \Phi^J$ such that $a \notin J$. Let $J'$ be the left-ideal of $\text{End}(E)$ generated by $J$ and $a$. Then we have $\text{nr}(J') < \text{nr}(J)$ by formula (3.4.2). On the other hand, since $a$ factors through $\phi^J$, we have $k(E^a) \subset k(E^J)$ and hence $k(E^{J'}) = k(E^J)$. This contradicts Deuring’s formula (3.4.3).

Proposition 3.4.4. Let $\psi : E \to E''$ be a non-zero isogeny, and let

$$\psi : \text{Hom}(E'', E) \to \text{End}(E)$$

be the homomorphism of $\mathbb{Z}$-modules given by $g \mapsto g \circ \psi$. We denote by $J_\psi$ the image of $\psi$, which is a left-ideal of $\text{End}(E)$. Then $\psi$ is equal to $\phi^{J_\psi}$.

Proof. Since $k(E^{\psi}) \subset k(E'')$ as subfields of $k(E)$ for any non-zero $g \in \text{Hom}(E'', E)$, we have $k(E^{J_\psi}) \subset k(E'')$, and hence $\phi^{J_\psi} : E \to E^{J_\psi}$ factors through $\psi : E \to E''$. The greatest common divisor of the degrees of $g \in \text{Hom}(E'', E)$ is 1 by Proposition 3.4.1. The specialization isometry of $E$ is equal to $\phi^{J_\psi}$. We note by $\psi(J_\psi) = \text{nr} \psi$ by the definition of $\text{nr}$. Since $\deg \phi^{J_\psi} = \text{nr}(J_\psi)$ by Deuring’s formula (3.4.3), we have $\psi = \phi^{J_\psi}$ and $E'' = E^{J_\psi}$.

Corollary 3.4.5. The map $J \mapsto \phi^J$ establishes a one-to-one correspondence between the set of non-zero left-ideals of $\text{End}(E)$ and the set of isomorphism classes of non-zero isogenies from $E$.

Proposition 3.4.6. Let $E'$ and $E$ be supersingular. Then the discriminant of the lattice $\text{Hom}(E', E)$ is equal to $p^2$.

Proof. Since $E'$ and $E$ are isogenous, there exists a non-zero left-ideal $J$ of $\text{End}(E)$ such that $E' \cong E^J$. Then we have an isomorphism $\text{Hom}(E', E) \cong J$ of $\mathbb{Z}$-modules given by $g \mapsto g \circ \phi^J$, and hence we have $\text{Hom}(E', E)[\deg \phi^J] \cong J$ as a lattice, from which we obtain

$$\text{disc}(\text{Hom}(E', E)) = \frac{\text{disc}(J)}{(\deg \phi^J)^2} = \frac{\text{disc}(\text{End}(E)) \cdot [\text{End}(E) : J]^2}{(\deg \phi^J)^2} = \text{disc}(\text{End}(E))$$

by the formula (3.4.2) and (3.4.3). Thus we have $\text{disc}(\text{Hom}(E', E)) = p^2$ by Proposition 3.4.1.

3.5. The specialization isometry of Hom-lattices. Let $E$ be an elliptic curve defined over a finite extension $L \subset \overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ such that the $j$-invariant $j(E) \in L$ is integral over $\mathbb{Z}_p$. This condition is satisfied, for example, if $\text{rank}(\text{End}(E)) = 2$. Then $E$ has potentially good reduction; that is, there exist a finite extension $M \subset \overline{\mathbb{Q}}_p$ of $L$ and a smooth proper morphism $\mathcal{E}_M \to \text{Spec} \mathbb{Z}_M$ over the valuation ring $\mathbb{Z}_M$ of $M$ such that $\mathcal{E}_M \otimes M$ is isomorphic to $E \otimes M$. Let $E_0$ be the central fiber of $\mathcal{E}_M$. Then we have a specialization isometry

$$\rho : \text{End}(E) \hookrightarrow \text{End}(E_0),$$

which is obtained from the specialization isometry $\text{NS}(E \times E) \hookrightarrow \text{NS}(E_0 \times E_0)$ and Proposition 3.4.1. The following follows, for example, from the existence and the uniqueness of the Néron model [35 Chap. IV].

Proposition 3.5.1. The isomorphism class of $E_0$ over $\overline{\mathbb{F}}_p$ and the specialization isometry $\rho$ do not depend on the choice of $M$ and $\mathcal{E}_M$. 
Replacing $L$ by a finite extension if necessary, we assume that
\[ \text{End}(E) = \text{End}_L(E), \]
so that $\text{Lie} : \text{End}(E) \to L$ is defined.

Let $E'$ be another elliptic curve defined over a finite extension $L' \subset \mathbb{Q}_p$ of $\mathbb{Q}_p$ such that $j(E') \in L'$ is integral over $\mathbb{Z}_p$. Then we have a specialization isometry $\rho' : \text{End}(E') \to \text{End}(E'_0)$, where $E'_0$ is the central fiber of a Néron model of $E'$. Replacing $L'$ by a finite extension, we assume that $\text{End}(E') = \text{End}_L(E')$. The following is easy to prove.

**Proposition 3.5.2.** Suppose that there exists a $g \in \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $E = g(E')$. Then there exist isomorphisms $\text{End}(E) \cong \text{End}(E')$ and $\text{End}(E_0) \cong \text{End}(E'_0)$ induced from $g$ such that the following diagram is commutative:

\[
\begin{array}{ccc}
\mathbb{Q}_p & \rightarrow & L \\
\downarrow g & & \downarrow \text{Lie} \\
\mathbb{Q}_p & \rightarrow & L' \rightarrow \text{End}(E') \\
\downarrow \rho & & \downarrow \rho' \\
\text{End}(E) & \rightarrow & \text{End}(E_0) \\
\end{array}
\]

Suppose that $\text{End}(E) \otimes \mathbb{Q}$ is isomorphic to an imaginary quadratic field $K$. The following result is again due to Deuring [8]. (See also [18, Chapter 13, Theorem 12].)

**Proposition 3.5.3.** The elliptic curve $E_0$ is supersingular if and only if $p$ is inert or ramifies in $K$.

We now work over $\overline{\mathbb{Q}}_p$ and assume that $\text{End}(E)$ is isomorphic to $\mathbb{Z}_K$. Suppose that $E_0$ is supersingular. We put $R := \text{End}(E_0)$. Let $J$ be an ideal of $\text{End}(E)$ and consider the elliptic curve $E^J$. Since $\text{End}(E^J)$ is also isomorphic to $\mathbb{Z}_K$ by Proposition 3.3.5, the reduction $(E^J)_0$ of $E^J$ is supersingular by Proposition 3.5.3 and we have a reduction
\[ \rho(\phi^J) : E_0 \to (E^J)_0 \]
of the isogeny $\phi^J : E \to E^J$. On the other hand, we have the left-ideal $R \cdot \rho(J)$ of $R$ generated by $\rho(J) \subset R$, and the associated isogeny
\[ \phi^{R_J} : E_0 \to (E_0)^{R\rho(J)}. \]

**Proposition 3.5.4.** The isogenies $\rho(\phi^J)$ and $\phi^{R_J}$ are isomorphic.

**Proof.** We choose $a_1, \ldots, a_t \in J$ such that $J$ is generated by $a_1, \ldots, a_t$ and such that $[\text{End}(E) : J]$ is equal to the greatest common divisor of $\text{deg} \ a_1, \ldots, \text{deg} \ a_t$. By Proposition 3.3.5, we have $\text{deg} \ \rho(\phi^J) = \text{deg} \ \phi^J = [\text{End}(E) : J]$. By Deuring’s formula (3.4.3), we see that $\text{deg} \ \phi^{R_J}$ is a common divisor of $\text{deg} \ \rho(a_i) = \text{deg} \ a_i$ for $i = 1, \ldots, t$, and hence $\text{deg} \ \phi^{R_J}$ divides $\text{deg} \ \rho(\phi^J)$. On the other hand, the left-ideal $R \cdot \rho(J)$ is generated by $\rho(a_1), \ldots, \rho(a_t)$, and hence, by Remarks 3.2.2 and 3.2.4, we see that $\phi^{R_J}$ factors through $\rho(\phi^J)$. Therefore we obtain $\rho(\phi^J) = \phi^{R_J}$. \qed

By Proposition 3.5.4, the following diagram is commutative:

\[
\begin{array}{ccc}
\text{Hom}(E^J, E) & \to & \text{Hom}((E^J)_0, E_0) \\
\phi^J & & \phi^{R_J} \\
\text{End}(E) & \to & \text{End}(E_0),
\end{array}
\]
where the horizontal arrows are the specialization isometries. By Propositions 3.3.6 and 3.4.3, we obtain the following:

**Proposition 3.5.5.** We put \( d_J := \deg \phi^J = \deg \rho(\phi^J) = \deg \phi^{RJ} \). Then we have an isomorphism of lattices

\[
(\text{Hom}(E^J, E) \hookrightarrow \text{Hom}((E^J)_0, E_0)) \cong (J \rightarrow R \cdot \rho(J))^\perp,
\]

where, on the right-hand side, \( J \) and \( R \cdot \rho(J) \) are regarded as sublattices of the lattices \( \text{End}(E) \cong \mathbb{Z}_K \) and \( \text{End}(E_0) = R \), respectively, and \( J \rightarrow R \cdot \rho(J) \) is given by the specialization isometry \( \rho : \text{End}(E) \hookrightarrow R \).

Finally, we state the lifting theorem of Deuring [8]. See also [18, Chapter 13, Theorem 14] and [13, Proposition 2.7].

**Proposition 3.5.6.** Let \( E_0 \) be a supersingular elliptic curve defined over a field \( \kappa_0 \) of characteristic \( p \), and \( \alpha_0 \) an endomorphism of \( E_0 \). Then there exist a smooth proper family of elliptic curves \( \mathcal{E} \rightarrow \text{Spec} \mathbb{Z}_L \) over the valuation ring \( \mathbb{Z}_L \) of a finite extension \( L \) of \( \mathbb{Q}_p \) and an endomorphism \( \alpha \) of \( \mathcal{E} \) over \( \mathbb{Z}_L \) such that \( (\mathcal{E}, \alpha) \otimes \kappa_p \) is isomorphic to \( (E_0, \alpha_0) \otimes \kappa_0 \), where \( p \) is the closed point of \( \text{Spec} \mathbb{Z}_L \).

### 3.6. Application of Tate’s theorem [36]

In this subsection, we prove the following result, which was used in the proof of Proposition 3.4.4.

**Proposition 3.6.1.** Let \( E' \) and \( E \) be supersingular elliptic curves. Then the greatest common divisor of the degrees of \( g \in \text{Hom}(E', E) \) is 1.

**Proof.** Without loss of generality, we can assume that \( E' \) and \( E \) are defined over a finite field \( \mathbb{F}_q \) of characteristic \( p \). Replacing \( \mathbb{F}_q \) by a finite extension, we can assume that \( \text{End}(E') = \text{End}_{\mathbb{F}_q}(E') \), \( \text{End}(E) = \text{End}_{\mathbb{F}_q}(E) \) and \( \text{Hom}(E', E) = \text{Hom}_{\mathbb{F}_q}(E', E) \) hold. Let \( l \) be a prime integer \( \neq p \), and consider the \( l \)-adic Tate module \( T_l(E') \) of \( E' \). By the famous theorem of Tate [36], we see that

\[
\text{End}_{\text{Gal}(\mathbb{F}_l/\mathbb{F}_q)}(T_l(E')) \cong \text{End}_{\mathbb{F}_q}(E') \otimes \mathbb{Z}_l = \text{End}(E') \otimes \mathbb{Z}_l
\]

is of rank 4, and hence we can assume that the \( q \)-th power Frobenius morphism \( \text{Frob}_{E'} \) acts on \( T_l(E') \) as a scalar multiplication by \( \sqrt{q} \). In the same way, we can assume that \( \text{Frob}_E \) acts on \( T_l(E) \) as a scalar multiplication by \( \sqrt{q} \). Then, by the theorem of Tate [36] again, we have a natural isomorphism

\[
\text{Hom}(E', E) \otimes \mathbb{Z}_l \cong \text{Hom}(T_l(E'), T_l(E)) \cong \text{End}_{\mathbb{Z}_l}(\mathbb{Z}_l^{\oplus 2}).
\]

Hence there exists a \( g \in \text{Hom}(E', E) \) such that \( \deg g \) is not divisible by \( l \). Therefore the greatest common divisor of the degrees of \( g \in \text{Hom}(E', E) \) is a power of \( p \). Let \( F : E' \rightarrow E^{(p)} \) be the \( p \)-th power Frobenius morphism of \( E' \). If the degree of \( g : E' \rightarrow E \) is divisible by \( p \), then \( g \) factors as \( g' \circ F \) with \( \deg g' = \deg g/p \). Therefore it is enough to show the following:

**Claim.** For any supersingular elliptic curve \( E \) in characteristic \( p \), there exists a \( g \in \text{Hom}(E, E^{(p)}) \) such that \( \deg g \) is prime to \( p \).

Note that \( j(E) \in \mathbb{F}_{p^2} \) and \( j(E^{(p)}) = j(E)^p \). By Proposition 3.5.6 there exists an elliptic curve \( E^\sharp \) defined over a finite extension \( L \) of \( \mathbb{Q}_p \) such that \( \text{End}(E^\sharp) \) is of rank 2 and such that \( E^\sharp \) has a reduction isomorphic to \( E \) at the closed point \( p \) of \( \mathbb{Z}_L \). We assume that \( L \) is Galois over \( \mathbb{Q}_p \), and fix an embedding \( L \rightarrow \mathbb{C} \). Then \( \text{End}(E^\sharp) \) is an order \( \mathcal{O} \) of an imaginary quadratic field, and \( E^\sharp \otimes \mathbb{C} \) is isomorphic to \( \mathbb{C}/I \) as a Riemann surface for some invertible \( \mathcal{O} \)-ideal \( I \). Note...
that \( j(E^2) \) is a root of the Hilbert class polynomial of the order \( O \) (\cite{14} Proposition 13.2). There exists an element \( \gamma \in \text{Gal}(L/\mathbb{Q}_p) \) such that

\[
j(E^2)^\gamma \equiv j(E^2)^p \mod p.
\]

We put \( E^\flat := (E^\#)^\gamma \). Then \( E^\flat \) has a reduction isomorphic to \( E^{(p)} \) at \( p \), and we have \( E^\flat \otimes \mathbb{C} \cong \mathbb{C}/J \) as a Riemann surface for some invertible \( O \)-ideal \( J \). The degree of homomorphisms in \( \text{Hom}(E^\flat, E^\flat) = \text{Hom}(\mathbb{C}/I, \mathbb{C}/J) \) is given by a primitive binary form corresponding to the ideal class of the proper \( O \)-ideal \( I \). By \cite{14} Theorem 7.7, we see that \( \text{Hom}(E^\flat, E^\flat) \) has an element whose degree is prime to \( p \). Since the specialization homomorphism \( \text{Hom}(E^\flat, E^\flat) \to \text{Hom}(E, E^{(p)}) \) preserves the degree, we obtain the proof. \( \square \)

4. Kummer construction

We denote by \( k \) an algebraically closed field of characteristic \( \neq 2 \).

4.1. Double coverings. We work over \( k \). Let \( W \) and \( Z \) be smooth projective surfaces, and \( \phi : W \to Z \) a finite double covering. Let \( \iota : W \cong W \) be the deck-transformation of \( W \) over \( Z \). Then we have homomorphisms

\[
\phi_* : \text{NS}(W) \to \text{NS}(Z) \quad \text{and} \quad \phi^* : \text{NS}(Z) \to \text{NS}(W).
\]

Let \( \text{NS}(W)_Q^+ \subset \text{NS}(W) \otimes \mathbb{Q} \) be the eigenspace of \( \iota_* \) with the eigenvalue 1. We put

\[
\text{NS}(W)^+ := \text{NS}(W) \cap \text{NS}(W)_Q^+.
\]

When the base field \( k \) is \( \mathbb{C} \), we assume that \( H^2(W, \mathbb{Z}) \) and \( H^2(Z, \mathbb{Z}) \) are torsion-free, so that they can be regarded as lattices. We have homomorphisms

\[
\phi_* : H^2(W, \mathbb{Z}) \to H^2(Z, \mathbb{Z}) \quad \text{and} \quad \phi^* : H^2(Z, \mathbb{Z}) \to H^2(W, \mathbb{Z}).
\]

Note that \( \phi^* \) preserves the Hodge structure. We define \( H^2(W, \mathbb{Z})^+ := H^2(W, \mathbb{Z}) \cap H^2(W, \mathbb{Q})^+ \) in the same way as \( \text{NS}(W)^+ \).

Lemma 4.1.1. The homomorphism \( \phi_* \) induces an isometry

\[
\phi_*^+ : \text{NS}(W)^+ \otimes \mathbb{Q} \to \text{NS}(Z)
\]

with a finite 2-elementary cokernel. When \( k = \mathbb{C} \), \( \phi_* \) induces an isometry

\[
\phi_*^+ : H^2(W, \mathbb{Z})^+ \otimes \mathbb{Q} \to H^2(Z, \mathbb{Z})
\]

with a finite 2-elementary cokernel that preserves the Hodge structure.

Proof. The proof follows immediately from the following:

\[
\phi^* \circ \phi_*(w) = w + \iota_*(w), \quad \phi_* \circ \phi^*(z) = 2z, \quad \iota_* \circ \phi^*(z) = \phi^*(z),
\]

\[
(\phi^*(z_1), \phi^*(z_2)) = 2(z_1, z_2), \quad (\iota_*(w_1), \iota_*(w_2)) = (w_1, w_2).
\]

The inverse of the isomorphism \( \phi_*^+ \otimes \mathbb{Q} \) is given by \((1/2)\phi^* \otimes \mathbb{Q}\). \( \square \)
4.2. Disjoint \((-2)\)-curves. We continue to work over \(k\). Let \(C_1, \ldots, C_m\) be \((-2)\)-curves on a \(K3\) surface \(X\) that are disjoint from each other, \(\Delta \subset \text{NS}(X)\) the sublattice generated by \([C_1], \ldots, [C_m]\), and \(\Delta \subset \text{NS}(X)\) the primitive closure of \(\Delta\). The discriminant group \(D_\Delta\) of \(\Delta\) is isomorphic to \(\mathbb{F}_2^m\) with basis

\[ \gamma_i := -[C_i]/2 + \Delta \quad (i = 1, \ldots, m). \]

For \(x = x_1 \gamma_1 + \cdots + x_m \gamma_m \in D_\Delta\), we denote by \(\text{wt}(x)\) the Hamming weight of \(x\), that is, the number of \(x_i \in \mathbb{F}_2\) with \(x_i \neq 0\). Then \(q_\Delta : D_\Delta \to \mathbb{Q}/2\mathbb{Z}\) is given by

\[ q_\Delta(x) = (-\text{wt}(x)/2) + 2\mathbb{Z} \in \mathbb{Q}/2\mathbb{Z}. \]

**Lemma 4.2.1.** We put \(H_\Delta := \Delta \cap D_\Delta\). Then, for every \(x \in H_\Delta\), we have \(\text{wt}(x) \equiv 0 \text{ mod } 4\) and \(\text{wt}(x) \neq 4\).

**Proof.** Since \(H_\Delta\) is totally isotropic with respect to \(q_\Delta\), we have \(\text{wt}(x) \equiv 0 \text{ mod } 4\) for any \(x \in H_\Delta\). Let \(\gamma : X \to Y\) be the contraction of \(C_1, \ldots, C_m\), and \(L_Y\) a very ample line bundle on the normal \(K3\) surface \(Y\). Then \([\{C_1\}, \ldots, [C_m]\]\) is a fundamental system of roots in the root system of type \(mA_1\). (See [26, Proposition 2.4].) If there were \(x \in H_\Delta\) with \(\text{wt}(x) = 4\), then there would exist a vector \(r\) in the set \(\{\gamma_i\}_{i=1}^m\) such that \(r \neq \pm [C_i]\) for any \(i\), which is a contradiction. \(\square\)

4.3. Double Kummer pencil. Let \(E'\) and \(E\) be elliptic curves defined over \(k\). We put \(A := E' \times E\), and denote by \(\text{Km}(A)\) the Kummer surface associated with \(A\); that is, \(\text{Km}(A)\) is the minimal resolution of the quotient surface \(A/\langle \iota_A \rangle\), where \(\iota_A : A \cong A\) is the inversion automorphism \(x \mapsto -x\). Let \(u'_i\) and \(u_j\) \((1 \leq i, j \leq 4)\) be the points of order \(\leq 2\) in \(E'\) and \(E\), respectively, and let \(\beta_A : A \to A\) be the blowing-up of \(A\) at the fixed points \((u'_i, u_j)\) of \(\iota_A\). Let \(\varphi_A : \tilde{A} \to \text{Km}(A)\) denote the natural finite double covering. The involution \(\iota_A\) lifts to an involution \(\tilde{i}_A\) of \(\tilde{A}\), and \(\varphi_A\) is the quotient morphism \(\tilde{A} \to \tilde{A}/\langle \tilde{i}_A \rangle = \text{Km}(A)\).

**Definition 4.3.1.** The diagram

\[ \begin{array}{ccc} \text{Km}(A) & \xrightarrow{\varphi_A} & \tilde{A} \xrightarrow{\beta_A} A = E' \times E \\ \end{array} \]

is called the *Kummer diagram* of \(E'\) and \(E\). We denote by \(E_{ij} \subset \text{Km}(A)\) the image by \(\varphi_A\) of the exceptional curve of \(\beta_A\) over the point \((u'_i, u_j)\) in \(A\), and by \(F_j\) and \(G_i\) the image by \(\varphi_A\) of the strict transforms of \(E' \times \{u_j\}\) and \(\{u'_i\} \times E\), respectively. These \((-2)\)-curves \(E_{ij}\), \(F_j\) and \(G_i\) on \(\text{Km}(A)\) form the configuration depicted in Figure 4.3.1, which is called the *double Kummer pencil* (see [30]).

Let \(B_{16} \subset \text{NS}(\tilde{A})\) be the sublattice generated by the classes of the sixteen \((-2)\)-curves contracted by \(\beta_A\). Then we have

\[ \text{NS}(\tilde{A}) = \text{NS}(A) \perp B_{16} = U(A) \perp \text{Hom}(E', E)[-1] \perp B_{16}. \]

Since \(\tilde{i}_A\) acts on \(\text{NS}(\tilde{A})\) trivially, we see that \(\varphi_A\) induces an isometry

\[ (\varphi_A)^\perp : U(A)[2] \perp \text{Hom}(E', E)[-2] \perp B_{16}[2] \to \text{NS}(\text{Km}(A)) \]

with a finite 2-elementary cokernel. Hence we obtain the following:

**Proposition 4.3.2.** We have \(\text{rank}(\text{NS}(\text{Km}(A))) = 18 + \text{rank}(\text{Hom}(E', E))\).
Proposition 4.3.3. The lattice \( N \) of curves in the double Kummer pencil, and we have

\[
\tilde{\eta} = 2[\xi] + \sum_{\mu=1}^4 [E_{\mu j}] \quad \text{and} \quad \tilde{\xi} = 2[\tilde{\xi}] + \sum_{\nu=1}^4 [E_{\nu i}],
\]

and they are orthogonal to \([E_{ij}]\). We have \(\tilde{\xi}^2 = \tilde{\eta}^2 = 0\) and \(\tilde{\xi}\tilde{\eta} = 2\). We then put

\[
N(Km(A)) := \langle \tilde{\xi}, \tilde{\eta} \rangle \perp \langle [E_{ij}] \mid 1 \leq i, j \leq 4 \rangle \subset NS(Km(A)),
\]

which is the image of \(U(A)[2] \perp B_{16}[2]\) by the isometry \((\varphi_A)^+\), and we denote by \(\overline{N}(Km(A)) \subset NS(Km(A))\) the primitive closure of \(N(Km(A))\).

**Proposition 4.3.3.** The lattice \(\overline{N}(Km(A))\) is generated by the classes of \((-2)\)-curves in the double Kummer pencil, and we have \([\overline{N}(Km(A)) : N(Km(A))] = 2^7\). In particular, we have \(\text{disc}(N(Km(A))) = -2^4\).

**Proof.** For simplicity, we put \(N := N(Km(A))\) and \(\overline{N} := \overline{N}(Km(A))\). Let \(N' \subset NS(Km(A))\) be the sublattice generated by \([E_{ij}], [F_j]\) and \([G_i]\). It is obvious from the equalities (4.3.1) that \(N'\) is contained in \(\overline{N}\), and it is easy to calculate that \([N' : N] = 2^7\). We will show that \(N' = \overline{N}\). Let \(\tilde{\xi}', \tilde{\eta}'\) and \([E_{ij}]'\) (\(1 \leq i, j \leq 4\)) be the basis of \(N'\) dual to the basis \(\tilde{\xi}, \tilde{\eta}\) and \([E_{ij}]\) (\(1 \leq i, j \leq 4\)) of \(N\). The discriminant group \(D_N = N'/N\) is isomorphic to \(\mathbb{F}_2^{18}\) with basis \(\tilde{\xi}', \tilde{\eta}'+N\) and \([E_{ij}]'+N\). With respect to this basis, we write an element of \(D_N\) by \([x, y, z_{11}, ..., z_{44}]\) with \(x, y, z_{ij} \in \mathbb{F}_2\). Then \(q_N : D_N \to \mathbb{Q}/2\mathbb{Z}\) is given by

\[
q_N([x, y, z_{11}, ..., z_{44}]) = (xy - \text{wt}([z_{11}, ..., z_{44}])/2) + 2\mathbb{Z},
\]

where \(\text{wt}([z_{11}, ..., z_{44}])\) is the Hamming weight of \([z_{11}, ..., z_{44}]\) in \(\mathbb{F}_2^{16}\). We put \(H' := N'/N\) and \(H := \overline{N}/\overline{N}\). Then we have \(H' \subseteq H\). By Lemma 4.2.1, if a code word \([0, 0, z_{11}, ..., z_{44}]\) is in \(H\), then \(\text{wt}([z_{11}, ..., z_{44}]) \neq 4\) holds. We can confirm by computer that every element \(v\) of the finite abelian group \(D_N\) of order \(2^{18}\) satisfies the following: if \(v \notin H'\), then the linear code \((H', v) \subset D_N\) spanned by \(H'\) and \(v\) is either not totally isotropic with respect to \(q_N\), or containing \([0, 0, z_{11}, ..., z_{44}]\) with \(\text{wt}([z_{11}, ..., z_{44}]) = 4\). Therefore \(H = H'\) holds. 

\[\square\]
4.4. The transcendental lattice of $\text{Km}(A)$. In this subsection, we work over $\mathbb{C}$. Then we have $H^2(\bar{A}, \mathbb{Z}) = H^2(A, \mathbb{Z}) \perp B_{16}$. Since $\iota_A$ acts on $H^2(\bar{A}, \mathbb{Z})$ trivially, we have an isometry

$$(\varphi_A)^+ : H^2(A, \mathbb{Z})[2] \perp B_{16}[2] \hookrightarrow H^2(\text{Km}(A), \mathbb{Z})$$

with a finite 2-elementary cokernel. We put

$$P(A) := (U(A) \perp B_{16} \hookrightarrow H^2(\bar{A}, \mathbb{Z}))^\perp = (U(A) \hookrightarrow H^2(A, \mathbb{Z}))^\perp$$

and

$$Q(\text{Km}(A)) := (\overline{\mathcal{N}}(\text{Km}(A)) \hookrightarrow H^2(\text{Km}(A), \mathbb{Z}))^\perp.$$

**Proposition 4.4.1.** The isometry $(\varphi_A)^+$ induces the following commutative diagram, in which the horizontal isomorphisms of lattices preserve the Hodge structure:

$$(4.4.1) \quad \begin{array}{ccc} T(A)[2] & \cong & T(\text{Km}(A)) \\ \downarrow & & \downarrow \\ P(A)[2] & \cong & Q(\text{Km}(A)). \end{array}$$

**Proof:** First we prove that $(\varphi_A)^+$ induces $P(A)[2] \cong Q(\text{Km}(A))$. By the definition of $N(\text{Km}(A))$, the isometry $(\varphi_A)^+$ maps $(U(A) \perp B_{16})[2]$ to $N(\text{Km}(A))$ isomorphically, and hence $(\varphi_A)^+$ induces an isometry from $P(A)[2]$ to $Q(\text{Km}(A))$ with a finite 2-elementary cokernel. Since $U(A) \perp B_{16}$ and $H^2(\bar{A}, \mathbb{Z})$ are unimodular, we have $\text{disc}(P(A)[2]) = 2^4$. Since $H^2(\text{Km}(A), \mathbb{Z})$ is unimodular and $\text{disc}(\overline{\mathcal{N}}(\text{Km}(A))) = -2^4$ by Proposition 4.3.3, we have $\text{disc}(Q(\text{Km}(A))) = 2^4$. Therefore the isometry $P(A)[2] \hookrightarrow Q(\text{Km}(A))$ is in fact an isomorphism.

By definition, we have $T(A) \subset P(A)$ and $T(\text{Km}(A)) \subset Q(\text{Km}(A))$. Since $(\varphi_A)^+$ preserves the Hodge structure, the isomorphism $P(A)[2] \cong Q(\text{Km}(A))$ induces $T(A)[2] \cong T(\text{Km}(A))$. \qed

**Remark 4.4.2.** The isomorphism $T(A)[2] \cong T(\text{Km}(A))$ was proved in [21, §4] using the sublattice $\langle [E_{ij}] \mid 1 \leq i, j \leq 4 \rangle$ instead of $N(\text{Km}(A))$. We need the diagram (4.4.1) for the proof of Proposition 4.5.2.

4.5. The supersingular reduction lattice of $\text{Km}(A)$. Let $W$ be either a number field, or a Dedekind domain with the quotient field $F$ being a number field. We assume that 2 is invertible in $W$. Let $\mathcal{E}'$ and $\mathcal{E}$ be smooth proper families of elliptic curves over $U := \text{Spec} W$. We put $\mathcal{A} := \mathcal{E}' \times_U \mathcal{E}$.

**Definition 4.5.1.** A diagram

$$(\mathcal{K}) : \quad \text{Km}(A) \leftarrow \bar{A} \rightarrow \mathcal{A} = \mathcal{E}' \times_U \mathcal{E}$$

of schemes and morphisms over $U$ is called the Kummer diagram over $U$ of $\mathcal{E}'$ and $\mathcal{E}$ if the following hold:

(i) $\text{Km}(A)$ and $\mathcal{A}$ are smooth and proper over $U$,

(ii) $\bar{A} \rightarrow \mathcal{A}$ is the blowing-up along the fixed locus (with the reduced structure) of the inversion automorphism $\iota_A : \mathcal{A} \rightarrow \mathcal{A}$ over $U$, and

(iii) $\text{Km}(A) \rightarrow \bar{A}$ is the quotient morphism by a lift $\tilde{\iota}_A$ of $\iota_A$.

In this subsection, we consider the case where $W$ is a Dedekind domain. Suppose that the Kummer diagram $(\mathcal{K})$ over $U$ of $\mathcal{E}'$ and $\mathcal{E}$ is given. Then, at every point $P$ of $U$ (closed or generic, see the definition (1.0.6)), the diagram $(\mathcal{K}) \otimes \tilde{\kappa}_P$ is the Kummer diagram of the elliptic curves $\mathcal{E}' \otimes \tilde{\kappa}_P$ and $\mathcal{E} \otimes \tilde{\kappa}_P$. 


Let \( p \) be a closed point of \( U \) with \( \kappa := \kappa_p \) being of characteristic \( p \). Note that \( p \neq 2 \) by the assumption \( 1/2 \in W \). We put

\[
E' := \mathcal{E}' \otimes \overline{\mathbb{F}}, \quad E := \mathcal{E} \otimes \overline{\mathbb{F}}, \quad A := E' \times E = A' \otimes \overline{\mathbb{F}} \quad \text{and} \quad A_0 := E_0' \times E_0 = A \otimes \overline{\mathbb{k}}.
\]

(4.5.1)

Then we have \( \text{Km}(A) \otimes \overline{\mathbb{F}} = \text{Km}(A) \) and \( \text{Km}(A) \otimes \overline{\mathbb{k}} = \text{Km}(A_0) \). We assume that

\[
\text{rank}(\text{Hom}(E', E)) = 2 \quad \text{and} \quad \text{rank}(\text{Hom}(E_0', E_0)) = 4.
\]

Then, by Proposition 4.3.2, we see that \( \text{Km}(A) \) is singular and \( \text{Km}(A_0) \) is supersingular. We consider the supersingular reduction lattices

\[
L(A, p) := (\text{NS}(A) \hookrightarrow \text{NS}(A_0))^\perp \quad \text{and} \quad L(\text{Km}(A), p) := (\text{NS}(\text{Km}(A)) \hookrightarrow \text{NS}(\text{Km}(A)_0))^\perp.
\]

Note that, by Proposition 3.1.1, we have

\[
L(A, p) = (\text{Hom}(E', E) \hookrightarrow \text{Hom}(E_0', E_0))^\perp[-1].
\]

**Proposition 4.4.1.** Suppose that \( p \) is prime to \( \text{disc}(\text{NS}(\text{Km}(A))) \). Then the Kummer diagram \((\mathcal{K})\) induces an isomorphism \( L(A, p)[2] \cong L(\text{Km}(A), p) \).

We use the following lemma, whose proof is quite elementary and is omitted:

**Lemma 4.5.3.** Let \( \rho : \Lambda_1 \hookrightarrow \Lambda_2 \) be an isometry of lattices. Suppose that \( \rho \) maps a sublattice \( N_1 \) of \( \Lambda_1 \) to a sublattice \( N_2 \) of \( \Lambda_2 \). For \( i = 1, 2 \), we put \( M_i := (N_i \hookrightarrow \Lambda_i)^\perp \). If \( \text{rank}(N_1) = \text{rank}(N_2) \), then \( \rho \) maps \( M_1 \) into \( M_2 \) and we have

\[
(M_1 \hookrightarrow M_2)^\perp = (N_1 \hookrightarrow N_2)^\perp.
\]

**Proof of Proposition 4.5.2.** Note that the double Kummer pencil is defined on \( \text{Km}(A) \) and is flat over \( U \). Hence, by Proposition 4.3.3, the specialization isometry

\[
\rho_{\text{Km}(A)} : \text{NS}(\text{Km}(A)) \hookrightarrow \text{NS}(\text{Km}(A)_0)
\]

maps \( \overline{\text{N}}(\text{Km}(A)) \) to \( \overline{\text{N}}(\text{Km}(A)_0) \) isomorphically. We put

\[
\Sigma(\text{Km}(A)) := (\overline{\text{N}}(\text{Km}(A)) \hookrightarrow \text{NS}(\text{Km}(A)))^\perp \quad \text{and} \quad \Sigma(\text{Km}(A)_0) := (\overline{\text{N}}(\text{Km}(A)_0) \hookrightarrow \text{NS}(\text{Km}(A)_0))^\perp.
\]

Then \( \rho_{\text{Km}(A)} \) maps \( \Sigma(\text{Km}(A)) \) to \( \Sigma(\text{Km}(A)_0) \), and we have

\[
L(\text{Km}(A), p) = (\Sigma(\text{Km}(A)) \hookrightarrow \Sigma(\text{Km}(A)_0))^\perp
\]

by Lemma 4.5.3. The isometry \( (\varphi_A)^\perp \) maps \((U(A) \subset B_16)[2] \subset \text{NS}(A)[2] \) to \( \overline{\text{N}}(\text{Km}(A)) \) isomorphically. Hence \( (\varphi_A)^\perp \) induces an isometry

\[
\text{Hom}(E', E)[-2] \hookrightarrow \Sigma(\text{Km}(A))
\]

with a finite 2-elementary cokernel. In the same way, we see that \( (\varphi_{A_0})^\perp \) induces an isometry

\[
\text{Hom}(E_0', E_0)[-2] \hookrightarrow \Sigma(\text{Km}(A)_0)
\]

with a finite 2-elementary cokernel. By the equalities (4.5.4) and (4.5.5), it is enough to show that the isometries (4.5.4) and (4.5.5) are isomorphisms.
To show that \(\text{(4.5.4)}\) is an isomorphism, we choose an embedding \(\sigma\) of \(\overline{\mathcal{T}}\) into \(\mathbb{C}\), and consider the analytic manifolds \(E^\sigma, E', A^\sigma, A\) and \(\text{Km}(A^\sigma) = \text{Km}(A)\). By Proposition 3.4.6, we have

\[
\text{Hom}(E^\sigma, E')[-1] = P(A^\sigma) \cap \text{NS}(A^\sigma) = (T(A^\sigma) \hookrightarrow P(A^\sigma))^\perp,
\]

where \(P(A^\sigma)\) is the lattice defined in the previous subsection. By the definition of \(\Sigma(\text{Km}(A))\), we have

\[
\Sigma(\text{Km}(A)^\sigma) = Q(\text{Km}(A)^\sigma) \cap \text{NS}(\text{Km}(A)^\sigma) = (T(\text{Km}(A)^\sigma) \hookrightarrow Q(\text{Km}(A)^\sigma))^\perp,
\]

where \(Q(\text{Km}(A)^\sigma)\) is the lattice defined in the previous subsection. Therefore, from \((4.4.1)\), we see that the analytic Kummer diagram \((\mathcal{K})^\sigma\) induces

\[
\text{Hom}(E^\sigma, E')[-2] \cong \Sigma(\text{Km}(A)^\sigma).
\]

Hence the isometry \((4.5.4)\) is an isomorphism.

Since \(p/2\) \(\text{disc}(\text{NS}(\text{Km}(A)))\), the Artin invariant of \(\text{Km}(A_0)\) is 1 by Proposition 1.0.1 and hence \(\text{disc}(\text{NS}(\text{Km}(A_0)))\) is equal to \(-p^2\). By Proposition 1.3.3, we have \(\text{disc}(\overline{\mathcal{N}}(\text{Km}(A_0))) = -2^4\), and hence we obtain \(\text{disc}(\Sigma(\text{Km}(A_0))) = 2^4p^2\) by Proposition 2.1.1. On the other hand, we have \(\text{disc}(\text{Hom}(E_0, E_0)[-2]) = 2^4p^2\) by Proposition 3.4.6. Comparing the discriminants, we conclude that the isometry \((4.5.5)\) is an isomorphism. \(\square\)

5. **Shioda-Inose construction**

We continue to denote by \(k\) an algebraically closed field of characteristic \(\neq 2\).

### 5.1. **Shioda-Inose configuration.**

Let \(Z\) be a K3 surface defined over \(k\).

**Definition 5.1.1.** We say that a pair \((C, \Theta)\) of reduced effective divisors on \(Z\) is a **Shioda-Inose configuration** if the following hold:

- (i) \(C\) and \(\Theta\) are disjoint,
- (ii) \(C = C_1 + \cdots + C_8\) is an ADE-configuration of \((-2)\)-curves of type \(E_8\),
- (iii) \(\Theta = \Theta_1 + \cdots + \Theta_8\) is an ADE-configuration of \((-2)\)-curves of type \(8A_1\),
- (iv) there exists a class \([\mathcal{L}] \in \text{NS}(Z)\) such that \(2[\mathcal{L}] = [\Theta]\).

Let \((C, \Theta)\) be a Shioda-Inose configuration on \(Z\). Then there exists a finite double covering \(\varphi_Y : \overline{Y} \to Z\) that branches exactly along \(\Theta\) by the condition (iv). Let \(T_i \subset \overline{Y}\) be the reduced part of the pull-back of \(\Theta_i\) by \(\varphi_Y\), which is a \((-1)\)-curve on \(\overline{Y}\), and let \(\beta_Y : \overline{Y} \to Y\) be the contraction of \(T_1, \ldots, T_8\). Then \(Y\) is a K3 surface. Let \(i_Y : Y \hookrightarrow \overline{Y}\) be the deck-transformation of \(\overline{Y}\) over \(Z\). Then \(i_Y\) is the lift of an involution \(i_Y : Y \cong Y\) of \(Y\), which has eight fixed points.

**Definition 5.1.2.** The diagram

\[
(\mathcal{S}Y) : Y \xrightarrow{i_Y} \overline{Y} \xrightarrow{\varphi_Y} Z
\]

is called the **Shioda-Inose diagram** associated with the Shioda-Inose configuration \((C, \Theta)\) on \(Z\). We call \(Y\) a **Shioda-Inose surface of\( Z\).**

We denote by \(\Gamma \subset \text{NS}(Z)\) the sublattice generated by \([C_1], \ldots, [C_8]\). Then \(\Gamma\) is a negative-definite root lattice of type \(E_8\). In particular, \(\Gamma\) is unimodular. We then denote by \(M(Z) \subset \text{NS}(Z)\) the sublattice generated by \([\Theta_1], \ldots, [\Theta_8]\), and by \(\overline{M}(Z)\) the primitive closure of \(M(Z)\) in \(\text{NS}(Z)\). Note that \(\overline{M}(Z)\) and \(\Gamma\) are orthogonal in \(\text{NS}(Z)\). By condition (iv) of the Shioda-Inose configuration, \(\overline{M}(Z)\) contains the
class $|\mathcal{L}| = |\Theta|/2$. In fact, we can see that $\mathcal{M}(Z)$ is generated by $M(Z)$ and $|\mathcal{L}|$ from the following equality [30] Lemma 3.4:

\[(5.1.1) \quad \text{disc}(\mathcal{M}(Z)) = 2^6.\]

Note that one can also prove the equality (5.1.1) easily using Lemma 4.3.3 in the same way as the proof Proposition 4.3.3. We then put \(\Xi(Z) := (\Gamma \perp \mathcal{M}(Z) \hookrightarrow \text{NS}(Z))^\perp.\)

Next we define several sublattices of \(\text{NS}(\bar{Y})\) and \(\text{NS}(Y)\). Since \(\varphi_Y\) is étale in a neighborhood of \(C \subset Z\) and \(C\) is simply connected, the pull-back of \(C\) by \(\varphi_Y\) consists of two connected components \(C^[1]\) and \(C^[2]\). Let \(\Gamma^[1]\) and \(\Gamma^[2]\) be the sublattices of \(\text{NS}(\bar{Y})\) generated by the classes of the irreducible components of \(C^[1]\) and \(C^[2]\), respectively. We put

\[\bar{\Gamma} := \Gamma^[1] \perp \Gamma^[2].\]

The sublattice \(\bar{\Gamma}\) is mapped by \(\beta_Y\) isomorphically to a sublattice of \(\text{NS}(Y)\), which we will denote by the same letter \(\bar{\Gamma}\). We denote by \(B_8 \subset \text{NS}(\bar{Y})\) the sublattice generated by the classes of the \((-1)\)-curves \([T_1], \ldots, [T_8]\). Then \(B_8\) is orthogonal to \(\bar{\Gamma}\), and we have a canonical isomorphism \(\text{NS}(Y) \cong \text{NS}(\bar{Y}) \perp B_8\). We put

\[\Pi(Y) := (\bar{\Gamma} \perp B_8 \hookrightarrow \text{NS}(\bar{Y}))^\perp = (\bar{\Gamma} \hookrightarrow \text{NS}(Y))^\perp.\]

Since \(\bar{\Gamma}\) and \(B_8\) are unimodular, we have

\[\text{NS}(\bar{Y}) = \bar{\Gamma} \perp B_8 \perp \Pi(Y) \quad \text{and} \quad \text{NS}(Y) = \bar{\Gamma} \perp \Pi(Y).\]

The action of \(i_Y\) on \(\text{NS}(\bar{Y})\) and the action of \(i_Y\) on \(\text{NS}(Y)\) preserve the orthogonal direct-sum decompositions (5.1.4), and the action of \(i_Y\) is trivial on \(B_8\). We put

\[\bar{\Gamma}^+ := \bar{\Gamma} \cap \bar{\Gamma}^+_Q \quad \text{and} \quad \Pi(Y)^+ := \Pi(Y) \cap \Pi(Y)^+_Q,\]

where \(\bar{\Gamma}^+_Q\) (resp. \(\Pi(Y)^+_Q\)) is the eigenspace of \((i_Y)_*\) on \(\bar{\Gamma} \otimes \mathbb{Q}\) (resp. \(\Pi(Y) \otimes \mathbb{Q}\)) with the eigenvalue 1. Since \(i_Y\) acts on \(\bar{\Gamma}\) by interchanging \(\Gamma^[1]\) and \(\Gamma^[2]\), we have \(\text{rank}(\bar{\Gamma}^+) = 8\). By Lemma 4.3.1 we see that \(\varphi_Y\) induces an isometry

\[(\varphi_Y)^+_*: \bar{\Gamma}^+[2] \perp B_8[2] \perp \Pi(Y)^+[2] \hookrightarrow \text{NS}(Z)\]

with a finite \(2\)-elementary cokernel. Since \((\varphi_Y)^+_*\) induces an isometry \(\bar{\Gamma}^+[2] \hookrightarrow \Gamma\) with a finite \(2\)-elementary cokernel and an isomorphism \(B_8[2] \cong M(Z)\), we obtain the following:

\textbf{Proposition 5.1.3.} (1) We have

\[\text{rank}(\text{NS}(Y)) = 16 + \text{rank}(\Pi(Y)) \geq \text{rank}(\text{NS}(Z)) = 16 + \text{rank}(\Pi(Y)^+).\]

(2) If \(\text{rank}(\text{NS}(Z))\) is equal to \(\text{rank}(\text{NS}(Y))\), then \((\varphi_Y)^+_*\) induces an isometry \(\Pi(Y)[2] \hookrightarrow \Xi(Z)\) with a finite \(2\)-elementary cokernel.

\section{The transcendental lattice of the Shioda-Inose surface.}

In this subsection, we work over \(\mathbb{C}\). Note that we have \(H^2(\bar{Y}, Z) = H^2(Y, Z) \perp B_8\). We consider the isometry

\[(\varphi_Y)^+*: H^2(\bar{Y}, Z)^+[2] \hookrightarrow H^2(Z, Z)\]

with a finite \(2\)-elementary cokernel. We put

\[R(Y) := (\bar{\Gamma} \perp B_8 \hookrightarrow H^2(\bar{Y}, Z))^\perp = (\bar{\Gamma} \hookrightarrow H^2(Y, Z))^\perp \quad \text{and} \quad S(Z) := (\Gamma \perp \mathcal{M}(Z) \hookrightarrow H^2(Z, Z))^\perp.\]
**Proposition 5.2.1.** The isometry \((\varphi_Y)_+^*\) induces the following commutative diagram, in which the horizontal isomorphisms of lattices preserve the Hodge structure:

\[
\begin{array}{ccc}
T(Y)[2] & \cong & T(Z) \\
\downarrow & & \downarrow \\
R(Y)[2] & \cong & S(Z).
\end{array}
\]

**Proof.** First we prove \(R(Y)[2] \cong S(Z)\). Since \(\tilde{\Gamma}\) and \(B_8\) are unimodular, we have

\[
H^2(\tilde{\Gamma}, \mathbb{Z}) = \tilde{\Gamma} \perp B_8 \perp R(Y).
\]

The action of \(i_Y\) on \(H^2(\tilde{\Gamma}, \mathbb{Z})\) preserves the decomposition \((5.2.2)\) and is trivial on \(B_8\). Since \(\text{rank}(\tilde{\Gamma}^+) = 8\) and \(\text{rank}(H^2(\tilde{\Gamma}, \mathbb{Z})^+) = 22\), we see that \(i_Y\) acts on \(R(Y)\) trivially. (This fact was also proved in \([30, \text{Lemma 3.2}]\).) We thus obtain an isometry

\[
(\varphi_Y)_+^* : \tilde{\Gamma}^+[2] \perp B_8[2] \perp R(Y)[2] \hookrightarrow H^2(\mathbb{Z}, \mathbb{Z})
\]

with a finite 2-elementary cokernel. Since \((\varphi_Y)_+^*\) maps \(\tilde{\Gamma}^+[2]\) to \(\Gamma\) and \(B_8[2]\) to \(M(Z)\) with finite 2-elementary cokernels, it induces an isometry from \(R(Y)[2]\) to \(S(Z)\) with a finite 2-elementary cokernel. From the decomposition \((5.2.2)\), we have \(\text{disc}(R(Y)[2]) = -2^6\). Since \(\text{disc}(M(Z)) = 2^6\) by the equality \((5.1.1)\), we have \(\text{disc}(S(Z)) = -2^6\). Therefore the isometry \(R(Y)[2] \hookrightarrow S(Z)\) is in fact an isomorphism.

The proof of the isomorphism \(T(Y)[2] \cong T(Z)\) is completely parallel to the second paragraph of the proof of Proposition \(4.4.1\). \(\square\)

**Remark 5.2.2.** The isomorphism \(T(Y)[2] \cong T(Z)\) is due to Shioda and Inose \([30]\). We need the diagram \((5.2.1)\) for the proof of Proposition \(5.3.2\).

**Corollary 5.2.3.** In characteristic 0, we have \(\text{rank}(\text{NS}(Y)) = \text{rank}(\text{NS}(Z))\) and \(2^{22-r} \text{disc}(\text{NS}(Y)) = \text{disc}(\text{NS}(Z))\), where \(r := \text{rank}(\text{NS}(Y)) = \text{rank}(\text{NS}(Z))\).

5.3. The supersingular reduction lattice of the Shioda-Inose surface. Let \(W\) be either a number field, or a Dedekind domain with the quotient field \(F\) being a number field such that \(1/2 \in W\). Let \(Z\) be a smooth proper family of \(K3\) surfaces over \(U := \text{Spec} W\).

**Definition 5.3.1.** A diagram

\[
(\mathcal{S}I) : \mathcal{Y} \hookrightarrow \tilde{\mathcal{Y}} \twoheadrightarrow Z
\]

of schemes and morphisms over \(U\) is called a **Shioda-Inose diagram** over \(U\) if there exists a pair of reduced effective divisors \((\mathcal{C}, \Theta)\) of \(Z\) such that the following hold:

(i) \(\mathcal{C}\) and \(\Theta\) are flat over \(U\),

(ii) \(\mathcal{Y}\) and \(\tilde{\mathcal{Y}}\) are smooth and proper over \(U\),

(iii) at each point \(P\) of \(U\) (closed or generic, see the definition \((1.0.6)\)), the pair of divisors \((\mathcal{C} \otimes \tilde{\kappa}_P, \Theta \otimes \tilde{\kappa}_P)\) is a Shioda-Inose configuration on \(Z \otimes \tilde{\kappa}_P\),

(iv) \(\tilde{\mathcal{Y}} \rightarrow Z\) is a finite double covering that branches exactly along \(\Theta\), and

(v) \(\mathcal{Y} \rightarrow \tilde{\mathcal{Y}}\) is a contraction of the inverse image of \(\Theta\) in \(\tilde{\mathcal{Y}}\).

In this subsection, we consider the case where \(W\) is a Dedekind domain. Suppose that a Shioda-Inose diagram \((\mathcal{S}I)\) over \(U\) is given. Then, at every point \(P\) of \(U\), the diagram \((\mathcal{S}I) \otimes \tilde{\kappa}_P\) is a Shioda-Inose diagram of \(Z \otimes \tilde{\kappa}_P\).
Let \( p \) be a closed point of \( U \) with \( \kappa := \kappa_p \) being of characteristic \( p \). Note that \( p \neq 2 \) by the assumption \( 1/2 \in W \). We put
\[
Y := Y \otimes \mathcal{F}, \quad \tilde{Y} := \tilde{Y} \otimes \mathcal{F}, \quad Z := Z \otimes \mathcal{F},
\]
\[
Y_0 := Y \otimes \mathcal{F}, \quad \tilde{Y}_0 := \tilde{Y} \otimes \mathcal{F}, \quad Z_0 := Z \otimes \mathcal{F}.
\]
We assume that \( Z \) is singular and \( Z_0 \) is supersingular. Then \( Y \) is singular and \( Y_0 \) is supersingular by Proposition 5.1.3. We consider the supersingular reduction lattices
\[
L(Z, p) := (\text{NS}(Z) \hookrightarrow \text{NS}(Z_0))^\perp \quad \text{and} \quad L(Y, p) := (\text{NS}(Y) \hookrightarrow \text{NS}(Y_0))^\perp.
\]
By Corollary 5.2.3, we have \( 4 \text{disc}(\text{NS}(Y)) = \text{disc}(\text{NS}(Z)) \). Since \( p \) is odd, the following are equivalent: (i) \( \not\mid \text{disc}(\text{NS}(Z)) \), and (ii) \( \not\mid \text{disc}(\text{NS}(Y)) \).

**Proposition 5.3.2.** Suppose that \( p \) satisfies the conditions (i) and (ii) above. Then the Shioda-Inose diagram \((ST)\) induces an isomorphism \( L(Y, p)[2] \cong L(Z, p) \).

**Proof.** Recall the definition of \( \Pi \). Since the specialization isometry \( \text{NS}(Y) \hookrightarrow \text{NS}(Y_0) \) maps \( \tilde{\Gamma} \subset \text{NS}(Y) \) to \( \tilde{\Gamma} \subset \text{NS}(Y_0) \) isomorphically, it maps \( \Pi(Y) \) to \( \Pi(Y_0) \), and we have
\[
L(Y, p) = (\Pi(Y) \hookrightarrow \Pi(Y_0))^\perp
\]
by Lemma 4.5.3. Recall the definition of \( \Xi \). Since the specialization isometry \( \text{NS}(Z) \hookrightarrow \text{NS}(Z_0) \) maps \( \Gamma \subset \text{NS}(Z) \) to \( \tilde{\Gamma} \subset \text{NS}(Z_0) \) and \( M(Z) \subset \text{NS}(Z) \) to \( M(Z_0) \subset \text{NS}(Z_0) \) isomorphically, it maps \( \Xi(Z) \) to \( \Xi(Z_0) \), and we have
\[
L(Z, p) = (\Xi(Z) \hookrightarrow \Xi(Z_0))^\perp
\]
by Lemma 4.5.3. By Proposition 5.1.3, we have the isometries
\[
(5.3.2) \quad \Pi(Y)[2] \hookrightarrow \Xi(Z) \quad \text{and} \quad \Pi(Y_0)[2] \hookrightarrow \Xi(Z_0)
\]
with finite 2-elementary cokernels induced by \((ST)\otimes \mathcal{F}((ST)\otimes \mathcal{F})\), and \((ST)\otimes \mathcal{F}((ST)\otimes \mathcal{F})\), respectively. It is therefore enough to show that both of the isometries in (5.3.2) are isomorphisms.

We choose an embedding \( \sigma \) of \( \mathcal{F} \) into \( \mathbb{C} \), and consider the transcendental lattices \( T(Y^\sigma) \) and \( T(Z^\sigma) \). We have
\[
\Pi(Y) \cong \Pi(Y^\sigma) = R(Y^\sigma) \cap \text{NS}(Y^\sigma) = (T(Y^\sigma) \hookrightarrow R(Y^\sigma))^\perp \quad \text{and} \quad \Xi(Z) \cong \Xi(Z^\sigma) = S(Z^\sigma) \cap \text{NS}(Z^\sigma) = (T(Z^\sigma) \hookrightarrow S(Z^\sigma))^\perp,
\]
where \( R(Y^\sigma) \) and \( S(Z^\sigma) \) are the lattices defined in the previous subsection. Since the analytic Shioda-Inose diagram \((ST)^\sigma\) induces the commutative diagram (5.2.1) for \( Y^\sigma \) and \( Z^\sigma \), we see that the first isometry of (5.3.2) is an isomorphism.

By Proposition 1.0.1, we have \( \text{disc} (\text{NS}(Y_0)) = \text{disc} (\text{NS}(Z_0)) = -p^2 \). Since \( \tilde{\Gamma} \) is unimodular, we have \( \text{disc}(\Pi(Y_0)) = -p^2 \) by Proposition 2.1.1 and hence \( \text{disc}(\Pi(Y_0)[2]) \) is equal to \( -2^6p^2 \). Since \( \Gamma \) is unimodular and \( \text{disc}(M(Z_0)) = 2^6 \) by the equality (5.1.1), we see that \( \text{disc}(\Xi(Z_0)) \) is equal to \( -2^6p^2 \) by Proposition 2.1.1 again. Therefore the second isometry of (5.3.2) is also an isomorphism. \( \Box \)
6. Proof of Theorems 1 and 3

6.1. Preliminaries. In this subsection, we quote fundamental facts in algebraic geometry from Grothendieck’s FGA [14, no. 221]. See also [10, Chap. 5].

Let $S$ be a noetherian scheme, and let $W$ and $Z$ be schemes flat and projective over $S$. We denote by $\text{Mor}_S(W, Z)$ the functor from the category $\text{Sch}_S$ of locally noetherian schemes over $S$ to the category of sets such that, for an object $T$ of $\text{Sch}_S$, we have

$$\text{Mor}_S(W, Z)(T) = \text{the set of } T\text{-morphisms from } W \times_S T \text{ to } Z \times_S T.$$ 

Then we have the following ([14, no. 221, Section 4], [10, Theorem 5.23]):

**Theorem 6.1.1.** The functor $\text{Mor}_S(W, Z)$ is representable by an open subscheme $\text{Mor}_S(W, Z)$ of the Hilbert scheme $\text{Hilb}_{W \times_S Z/S}$ parameterizing closed subschemes of $W \times_S Z$ flat over $S$.

Let $F$ be a number field, and let $X$ and $Y$ be smooth projective varieties defined over $F$. By the flattening stratification ([10, Theorem 5.12], [19, Lecture 8]), we have a non-empty open subset $U$ of $\text{Spec } \mathbb{Z}_F$ and smooth projective $U$-schemes $X$ and $Y$ such that the generic fibers $X \times_U F$ and $Y \times_U F$ are isomorphic to $X$ and $Y$, respectively. We will consider the schemes

$$\text{Mor}_V(X_V, Y_V) = \text{Mor}_U(X, Y) \times_U V$$

for non-empty open subsets $V$ of $U$, where $X_V := X \times_U V$ and $Y_V := Y \times_U V$.

**Proposition 6.1.2.** Let $\varphi : X \to Y$ be an $F$-morphism. Then there exist a non-empty open subset $V \subset U$ and a $V$-morphism $\varphi_V : X_V \to Y_V$ that extends $\varphi$. If $\tilde{\varphi}_V : X_V \to Y_V$ is a morphism over a non-empty open subset $V' \subset U$ that extends $\varphi$, then $\tilde{\varphi}_V|_{V \cap V'} = \varphi_V|_{V \cap V'}$ holds, where $\tilde{\varphi}_V|_{V \cap V'}$ and $\varphi_V|_{V \cap V'}$ denote the restrictions of $\tilde{\varphi}_V$ and $\varphi_V$ to $X_V \cap Y_V$.

**Proof.** We denote by $[\varphi] : \text{Spec } F \to \text{Mor}_U(X, Y)$ the $U$-morphism corresponding to $\varphi : X \to Y$. Let $\Phi$ be the Hilbert polynomial of the graph $\Gamma(\varphi) \subset X \times_F Y$ of $\varphi$ with respect to a relatively ample invertible sheaf $\mathcal{O}(1)$ of $X \times_U Y \to U$, so that $[\varphi]$ is an $F$-rational point of $\text{Mor}_U(X, Y) \cap H^\Phi$, where $H^\Phi := \text{Hilb}_{X \times_U Y/U}^\Phi$ is the Hilbert scheme parameterizing closed subschemes of $X \times_U Y$ flat over $U$ with the Hilbert polynomial of fibers with respect to $\mathcal{O}(1)$ being equal to $\Phi$. Since $H^\Phi$ is projective over $U$, the morphism $[\varphi]|_{V'} : U \to H^\Phi$. Since $\text{Mor}_U(X, Y) \cap H^\Phi$ is open in $H^\Phi$, there exists a non-empty open subset $V$ of $U$ such that $[\varphi]$ extends to a $U$-morphism

$$[\varphi]|_V : V \to \text{Mor}_U(X, Y).$$

Hence the existence of a morphism $\tilde{\varphi}_V : X_V \to Y_V$ extending $\varphi$ over some non-empty open subset $V \subset U$ is proved. The equality $\tilde{\varphi}_V|_{V \cap V'} = \varphi_V|_{V \cap V'}$ follows from the fact that $H^\Phi \to U$ is separated.

We call $\tilde{\varphi}_V$ the extension of $\varphi$ over $V$. By the uniqueness of the extension, we obtain the following:

**Corollary 6.1.3.** Let $Z$ be a smooth projective $U$-scheme with the generic fiber $Z$. Let $\psi : Y \to Z$ be an $F$-morphism, and let $\tilde{\psi}_V : Y_V \to Z_V$ be the extension of $\psi$ over a non-empty open subset $V' \subset U$. Then $([\tilde{\psi}_V]|_{V \cap V'}) \circ ([\varphi]|_{V \cap V'})$ is the extension of $\psi \circ \varphi : X \to Z$ over $V \cap V'$. 

Applying Corollary \[6.1.3\] to an \(F\)-isomorphism and its inverse, we obtain the following, which plays a key role in the proof of Theorem \[1\].

**Corollary 6.1.4.** If \(X\) and \(Y\) are isomorphic over \(F\), then there exists a non-empty open subset \(V \subset U\) such that \(\mathcal{X}_V\) and \(\mathcal{Y}_V\) are isomorphic over \(V\).

We give three applications that will be used in the proof of Proposition \[6.3.2\].

**Example 6.1.5.** Let \(\beta\) be an \(F\)-rational point of \(Y\), and \(\varphi : X \to Y\) the blowing-up of \(Y\) at \(\beta\), which is defined over \(F\). By shrinking \(U\) if necessary, we can assume that \(\beta\) is the generic fiber of a closed subscheme \(Q \subset Y\) that is smooth over \(U\). Let \(\beta_U : X' \to Y\) be the blowing-up of \(Y\) along \(Q\), which is defined over \(U\). Then the restriction \(\beta_\eta : X' \to Y\) of \(\beta_U\) to the generic fiber \(X'\) of \(X'\) to \(Y\) is isomorphic to \(\varphi\); that is, there exists an \(F\)-isomorphism \(\tau : X' \cong X\) such that \(\beta_\eta = \beta \circ \tau\). Hence, by Corollaries 6.1.3 and 6.1.4, there exists a non-empty open subset \(V \subset U\) such that the restriction \(\beta_V : X'_V \to Y_V\) of \(\beta_U\) to \(X'_V\) coincides with the composite of the \(V\)-isomorphism \(\tau_V : X'_V \cong X_V\) and the extension \(\hat{\varphi}_V : X_V \to Y_V\) of \(\varphi\) over \(V\).

**Example 6.1.6.** Let \(D\) be a reduced smooth divisor of \(Y\) such that every irreducible component \(D_i\) of \(D\) is defined over \(F\). By shrinking \(U\) if necessary, we can assume that each \(D_i\) is the generic fiber of a closed subscheme \(D_i \subset Y\) that is smooth over \(U\). We can also assume that these \(D_i\) are mutually disjoint. Then \(D := \sum D_i\) is smooth over \(U\).

**Proposition 6.1.7.** Let \(\varphi : X \to Y\) be an \(F\)-morphism that is a double covering branching exactly along \(D\). Then there exists an open subset \(V \neq \emptyset\) of \(U\) such that the extension of \(\varphi\) over \(V\) is a double covering of \(\mathcal{Y}_V\) branching exactly along \(\mathcal{D}_V\).

**Proof.** Let \(L\) be an invertible sheaf on \(Y\) defined by the exact sequence

\[
0 \to \mathcal{O}_Y \to \varphi_* \mathcal{O}_X \to L^{-1} \to 0.
\]

Then \(L\) is defined over \(F\), and we have an isomorphism

\[
\rho : L \otimes \mathcal{O}_Y(D) \simeq \mathcal{O}_Y(D)
\]

on \(Y\) that corresponds to the double covering \(\varphi\) in the way described in [3, Chap. 0]. There exist a non-empty open subset \(V\) of \(U\) and an invertible sheaf \(L\) on \(\mathcal{Y}_V\) such that \(L \otimes \mathcal{O}_Y(D)\) is isomorphic to \(\mathcal{O}_Y(D)\). We consider the invertible sheaves

\[
\mathcal{M} := \operatorname{Hom}_{\mathcal{O}_Y(V)}(L \otimes \mathcal{O}_Y(V), \mathcal{D}_V) \quad \text{and} \quad M := \operatorname{Hom}_{\mathcal{O}_Y}(L \otimes \mathcal{O}_Y, \mathcal{D}_Y(D))
\]

on \(\mathcal{Y}_V\) and \(Y\), respectively. Then we have \(M = \mathcal{M} \otimes \mathcal{O}_Y(V) \cong \mathcal{O}_Y(V)\). By [10, Proposition 9.3 in Chap. III], the restriction homomorphisms

\[
H^0(\mathcal{Y}_V, \mathcal{M}) \to H^0(Y, M) \quad \text{and} \quad H^0(\mathcal{Y}_V, M^{-1}) \to H^0(Y, M^{-1})
\]

to the generic fiber \(Y\) induce isomorphisms

\[
H^0(\mathcal{Y}_V, \mathcal{M}) \otimes_R F \cong H^0(Y, M) \quad \text{and} \quad H^0(\mathcal{Y}_V, M^{-1}) \otimes_R F \cong H^0(Y, M^{-1}),
\]

where \(R := \Gamma(V, \mathcal{O}_Y)\). Hence, by shrinking \(V = \operatorname{Spec} R\), we have elements \(f \in H^0(\mathcal{Y}_V, \mathcal{M})\) and \(g \in H^0(\mathcal{Y}_V, M^{-1})\) that restrict to \(\rho\) and \(\rho^{-1}\), respectively. Then the composites \(f \circ g\) and \(g \circ f\), considered as elements of \(H^0(\mathcal{Y}_V, \mathcal{M} \otimes M^{-1}) = R\), are mapped to the \(1 \in H^0(Y, M \otimes M^{-1}) = F\). Since \(R \to F\), we see that \(f\) and \(g\) are isomorphisms. Thus \(\rho\) extends to an isomorphism

\[
\tilde{\rho} : L \otimes \mathcal{O}_Y(V) \simeq \mathcal{O}_Y(V,D).\]
By means of \( \bar{\rho} \), a double covering \( \delta_V : \mathcal{X}_V' \to \mathcal{Y}_V \) that branches exactly along \( \Theta \) is constructed as a closed subscheme of the line bundle on \( \mathcal{Y}_V \) corresponding to the invertible sheaf \( \mathcal{L} \). By construction, the restriction \( \delta_{\bar{\rho}} : X' \to Y \) of \( \delta_V \) to the generic fiber is isomorphic to \( \varphi : X \to Y \). By Corollaries [6.1.3] and [6.1.4] it follows that, making \( V \) smaller if necessary, we have a \( V \)-isomorphism \( \mathcal{X}_V' \cong \mathcal{X}_V \) under which \( \delta_V \) coincides with the extension \( \bar{\varphi}_V \) of \( \varphi \) over \( V \).

**Example 6.1.8.** In this example, we assume \( 1/2 \in R := \Gamma(U, \mathcal{O}_U) \). Let \( \iota : X \to X \) be an involution defined over \( F \), and \( \varphi : X \to Y \) the quotient morphism by the group \( \langle i \rangle \). Suppose that the extension \( \iota_U : X \to X \) of \( \iota \) over \( U \) exists. Then \( \iota_U \) is an involution over \( U \) by Corollary [6.1.3]. Let \( q_U : \mathcal{X} \to \mathcal{Y} \) be the quotient morphism by the group \( \langle \iota_U \rangle \), which is defined over \( U \) by \( 1/2 \in R \). Then, by Corollaries [6.1.3], [6.1.4] and Lemma [6.1.9], we have a non-empty open subset \( V \subset U \) and a \( V \)-isomorphism \( \mathcal{Y}_V \cong \mathcal{Y}_V' \) under which the extension \( \bar{\varphi}_V \) of \( \varphi \) over \( V \) coincides with the restriction \( q_U : \mathcal{X}_V \to \mathcal{Y}_V' \) of \( q_U \) to \( \mathcal{X}_V \).

**Lemma 6.1.9.** Let \( A \) be an \( R \)-algebra on which an involution \( i \) acts. Then we have \( A^{(i)} \otimes_R F = (A \otimes_R F)^{(i)} \), where \( A^{(i)} := \{ a \in A | i(a) = a \} \).

*Proof.* Since \( 1/2 \in R \), we see that the \( R \)-module \( A \) is the direct-sum of \( A^{(i)} = \{(a + i(a))/2 | a \in A \} \) and \( \{(a - i(a))/2 | a \in A \} \). \( \square \)

6.2. Shioda-Inose configuration on \( \text{Km}(E' \times E) \). The following result is due to Shioda and Inose [30]. We briefly recall the proof.

**Proposition 6.2.1.** Let \( E' \) and \( E \) be elliptic curves defined over an algebraically closed field \( k \) of characteristic \( 0 \). Then there exists a Shioda-Inose configuration \((C, \Theta)\) on the Kummer surface \( \text{Km}(E' \times E) \).

*Proof.* Let \( E_{ij}, E_j \) and \( G_i \) \( (1 \leq i, j \leq 4) \) be the \((-2)\)-curves in the double Kummer pencil (Figure [4.3.1]) on \( \text{Km}(E' \times E) \). We consider the divisor

\[(6.2.1) \quad H := E_{12} + 2F_2 + 3E_{32} + 4G_3 + 5E_{31} + 6F_1 + 3E_{21} + 4E_{41} + 2G_4,\]

and let \( C \) be the reduced part of \( H - E_{12} \):

\[(6.2.2) \quad C := F_2 + E_{32} + G_3 + E_{31} + F_1 + E_{21} + E_{41} + G_4,\]

which is an ADE-configuration of \((-2)\)-curves of type \( \mathbb{E}_8 \). The complete linear system \( |H| \) defines an elliptic pencil

\[\Phi : \text{Km}(E' \times E) \to \mathbb{P}^1\]

with a section \( G_1 \). Since \( HE_{13} = 0 \) and \( HE_{14} = 0 \), each of \( E_{13} \) and \( E_{14} \) is contained in a fiber of \( \Phi \). We put \( t_0 := \Phi(H) \), \( t_1 := \Phi(E_{13}) \) and \( t_2 := \Phi(E_{14}) \). Note that \( t_0 \neq t_1 \neq t_2 \neq t_0 \), because \( H, E_{13} \) and \( E_{14} \) intersect \( G_1 \) at distinct points. By [30] Theorem 1], the fibers of \( \Phi \) over \( t_1 \) and \( t_2 \) are either \( (a) \) of type \( \mathbb{I}_b^+ \) and \( \mathbb{I}_a^- \) with \( b_1 + b_2 \leq 2 \), or \( (b) \) of type \( \mathbb{I}_0^+ \) and \( \mathbb{I}_0^- \). Hence there exist exactly eight \((-2)\)-curves \( \Theta_1, \ldots, \Theta_8 \) in \( \Phi^{-1}(t_1) \) and \( \Phi^{-1}(t_2) \) that appear in the fiber with odd multiplicity. We denote by \( \Theta \) the sum of \( \Theta_1, \ldots, \Theta_8 \). Let \( \Delta \) be a projective line, and \( f : \Delta \to \mathbb{P}^1 \) the double covering that branches exactly at \( t_1 \) and \( t_2 \). Let \( \bar{Y} \) be the normalization of \( \text{Km}(E' \times E) \times_{\mathbb{P}^1} \Delta \). Then \( \bar{Y} \to \text{Km}(E' \times E) \) is a finite double covering that branches exactly along \( \Theta \). Hence \((C, \Theta)\) is a Shioda-Inose configuration. \( \square \)
6.3. The SIK diagram. Let \( W \) be either a number field, or a Dedekind domain with the quotient field \( F \) being a number field such that \( 1/2 \in W \).

**Definition 6.3.1.** Let \( \mathcal{E}' \) and \( \mathcal{E} \) be smooth proper families of elliptic curves over \( U := \text{Spec} \, W \). We put \( A := \mathcal{E}' \times_U \mathcal{E} \). A diagram

\[
(\text{SIK}) : \mathcal{Y} \leftarrow \tilde{\mathcal{Y}} \rightarrow \text{Km}(A) \leftarrow \tilde{A} \rightarrow A
\]

of schemes and morphisms over \( U \) is called an SIK diagram of \( \mathcal{E}' \) and \( \mathcal{E} \) if the left half \( \mathcal{Y} \leftarrow \tilde{\mathcal{Y}} \rightarrow \text{Km}(A) \) is a Shioda-Inose diagram over \( U \), and the right half \( \text{Km}(A) \leftarrow \tilde{A} \rightarrow A \) is the Kummer diagram of \( \mathcal{E}' \) and \( \mathcal{E} \) over \( U \).

**Proposition 6.3.2.** Let \( E' \) and \( E \) be elliptic curves defined over a number field \( L \).

1. There exist a finite extension \( F \) of \( L \) and an SIK diagram

\[
(\text{SIK})_F : \mathcal{Y} \leftarrow \tilde{\mathcal{Y}} \rightarrow \text{Km}(A) \leftarrow \tilde{A} \rightarrow A := (E' \times E) \otimes F
\]

of \( E' \otimes F \) and \( E \otimes F \) over \( F \).

2. Moreover, there exist a non-empty open subset \( U \) of \( \text{Spec} \, \mathbb{Z}_F[1/2] \), smooth proper families \( \mathcal{E}' \) and \( \mathcal{E} \) of elliptic curves over \( U \) with the generic fibers being isomorphic to \( E' \otimes F \) and \( E \otimes F \), respectively, and an SIK diagram

\[
(\text{SIK})_U : \mathcal{Y} \leftarrow \tilde{\mathcal{Y}} \rightarrow \text{Km}(A) \leftarrow \tilde{A} \rightarrow A := \mathcal{E}' \times_U \mathcal{E}
\]

of \( \mathcal{E}' \) and \( \mathcal{E} \) over \( U \) such that \( (\text{SIK})_U \otimes F \) is equal to the SIK diagram \( (\text{SIK})_F \) over \( F \) in (1) above.

**Proof.** Our argument for the proof of the assertion (1) is similar to [K0] [6]. Let \( F \) be a finite extension of \( L \) such that every 2-torsion point \( Q_{ij} := (u'_i, u'_j) \) of \( A := (E' \times E) \otimes F \) is rational over \( F \). Then the blowing-up \( \tilde{A} \rightarrow A \) and the involution \( \iota_A \) of \( \tilde{A} \) are defined over \( F \). Therefore the quotient morphism \( \tilde{A} \rightarrow \text{Km}(A) \) is defined over \( F \), and every irreducible component of the double Kummer pencil on \( \text{Km}(A) \) is rational over \( F \). Since the divisor \( H \) is defined over \( F \), the elliptic pencil \( \Phi \) on \( \text{Km}(A) \) is defined over \( F \). Moreover, the points \( t_1, t_2 \in \mathbb{P}^1 \) are \( F \)-rational. Replacing \( F \) by a finite extension, we can assume that \( Y \) is defined over \( F \), and that \( \Theta_1, \ldots, \Theta_8 \) are rational over \( F \). Then the \((-1)\)-curves \( T_1, \ldots, T_8 \) on \( \tilde{Y} \) are rational over \( F \), and the contraction \( \tilde{Y} \rightarrow Y \) is defined over \( F \). Moreover, the image \( R_i \in Y \) of \( T_i \subset Y \) is an \( F \)-rational point of \( Y \). Thus we have obtained an SIK diagram \( (\text{SIK})_F \) of \( E' \) and \( E \) over \( F \), and the assertion (1) is proved. Moreover, \( (\text{SIK})_F \) has the following properties:

(i) Each of the centers \( Q_{ij} \) of the blowing-up \( \tilde{A} \rightarrow A \) is rational over \( F \), and each of the centers \( R_i \) of the blowing-up \( Y \leftarrow \tilde{Y} \) is rational over \( F \).

(ii) Each irreducible component of the double Kummer pencil on \( \text{Km}(A) \) is rational over \( F \). In particular, each irreducible component \( C_i \) of the \( E_8 \)-configuration \( C \) is rational over \( F \). (See [6.2.1].)

(iii) Each irreducible component \( \Theta_i \) of the branch curve of the double covering \( \tilde{Y} \rightarrow \text{Km}(A) \) is rational over \( F \).

We choose a non-empty open subset \( U \) of \( \text{Spec} \, \mathbb{Z}_F[1/2] \), construct smooth proper families \( \mathcal{E}' \) and \( \mathcal{E} \) of elliptic curves over \( U \) with the generic fibers being isomorphic to \( E' \otimes F \) and \( E \otimes F \), respectively, and make a diagram \( (\text{SIK})_U \) of schemes and morphisms over \( U \) such that each scheme is smooth and projective over \( U \) and such
that \((SIK)_U \otimes F\) is equal to the \(SIK\) diagram \((SIK)_F\) over \(F\). We will show that, after deleting finitely many closed points from \(U\), the diagram \((SIK)_U\) becomes an \(SIK\) diagram over \(U\). Note that, since \(\mathcal{E}'\) and \(\mathcal{E}\) are families of elliptic curves (that is, with a section over \(U\)), the inversion automorphism \(\iota_A\) of \(A\) is defined over \(U\).

We can make \(U\) so small that the following hold:

- Each \(Q_{ij} \in A\) is the generic fiber of a closed subscheme \(Q_{ij}\) of \(A\) that is smooth over \(U\), and these \(Q_{ij}\) are mutually disjoint. Then \(\bigcup Q_{ij}\) is the fixed locus of \(\iota_A\), and \(\tilde{A} \to A\) is the blowing-up along \(\bigcup Q_{ij}\) by Example 6.1.5.
- The involution \(\iota_A\) of \(\tilde{A}\) extends to an involution \((\iota_A')_\mathbb{Y}\) of \(\tilde{A}\) over \(U\), which is a lift of \(\iota_A\) by Corollary 6.1.3. By Example 6.1.8 the morphism \(\text{Km}(A) \to \tilde{A}\) is the quotient morphism by \((\iota_A')_\mathbb{Y}\).
- Each \(\Theta_i \subset \text{Km}(A)\) is the generic fiber of a closed subscheme \(\Theta_i\) of \(\text{Km}(A)\) that is smooth over \(U\). By the specialization isometry from \(\text{NS}(\text{Km}(A))\) to \(\text{NS}(\text{Km}(A) \otimes \kappa_P)\) for closed points \(p\) of \(U\), we see that these \(\Theta_i\) are mutually disjoint. By Example 6.1.8 the morphism \(\mathbb{Y} \to \text{Km}(A)\) is a double covering branching exactly along \(\Theta = \bigcup \Theta_i\).
- Each irreducible component \(C_i\) of \(C\) is the generic fiber of a closed subscheme \(C_i\) of \(\text{Km}(A)\) that is smooth over \(U\). We put \(C := \bigcup C_i\). Considering the specialization isometry \(\text{NS}(\text{Km}(A)) \to \text{NS}(\text{Km}(A) \otimes \kappa_P)\) for closed points \(p\) of \(U\), we see that \(C\) is a flat family of \(\mathbb{E}_8\)-configurations of \((-2)\)-curves over \(U\), and that \(\Theta\) and \(C\) are disjoint. Hence \((C, \Theta) \otimes \kappa_P\) is a Shioda-Inose configuration on \(\text{Km}(A) \otimes \kappa_P\) for every point \(P\) of \(U\).
- Each \(R_i \in Y\) is the generic fiber of a closed subscheme \(R_i\) of \(Y\) that is smooth over \(U\), and these \(R_i\) are mutually disjoint. The morphism \(\tilde{Y} \to Y\) is the blowing-up along \(\bigcup R_i\) by Example 6.1.3.

Hence \((SIK)_U\) is an \(SIK\) diagram over \(U\). \(\Box\)

We consider the \(SIK\) diagram \((SIK)_U\) over a non-empty open subset \(U \subset \text{Spec} \mathbb{Z}_p[1/2]\), and the \(SIK\) diagram \((SIK)_F = (SIK)_U \otimes F\) over \(F\), as in Proposition 6.3.2 (Remark that we have changed the notation from 4.5.1 and 5.3.1 to \(Y := Y \otimes F, E' := E' \otimes F, E := E \otimes F\)). By the isomorphisms of Propositions 4.4.1 and 5.2.3 we obtain the following:

**Proposition 6.3.3.** For each \(\sigma \in \text{Emb}(F)\), the diagram \((SIK) \otimes \mathbb{C}\) obtained from \((SIK) \otimes F\) by \(\sigma : F \to \mathbb{C}\) induces an isomorphism of lattices \(T(Y') \cong T(A')\) that preserves the Hodge structure.

We assume the following, which are equivalent by Proposition 4.3.2 and Corollary 5.2.3 (i) \(\text{rank} \text{Hom}(E', E)) = 2\). (ii) \(\text{Km}(A)\) is singular. (iii) \(Y\) is singular.

**Proposition 6.3.4.** We put \(d(Y) := \text{disc}(\text{NS}(Y))\). There exists a finite set \(N\) of prime integers containing the prime divisors of \(2d(Y)\) such that the following holds:

\[
(6.3.1) \quad p \not\in N \Rightarrow S_p(Y) = \begin{cases} 0 & \text{if } \chi_p(d(Y)) = 1, \\ \pi_F^{-1}(p) & \text{if } \chi_p(d(Y)) = -1. \end{cases}
\]

**Proof.** By Proposition 6.1.2 there exists an imaginary quadratic field \(K\) such that \(K \cong \text{End}(E') \otimes \mathbb{Q} \cong \text{End}(E) \otimes \mathbb{Q}\). We denote by \(D\) the discriminant of \(K\). We choose \(N\) in such a way that \(N\) contains all the prime divisors of \(2d(Y)/D\), and that
if $p \not\in N$, then $\chi_{p^{-1}}(p) \subset U$ holds. By Propositions 6.3.3 and 5.1.1, we have
\[
d(Y) := \text{disc}(\text{NS}(Y)) = -\text{disc}(T(Y^\sigma)) = -\text{disc}(T(\sigma)) = \text{disc}(\text{NS}(A)) = -\text{disc}(\text{Hom}(E', E)).
\]
By Proposition 6.3.3 we have $m^2d(Y) = n^2D$ for some non-zero integers $m$ and $n$. We can assume that $\gcd(m, n) = 1$. Then any $p \not\in N$ is prime to $mn$, and hence
\[p \not\in N \Rightarrow \chi_p(d(Y)) = \chi_p(D)
\]
holds. Let $p$ be a prime integer not in $N$. If $\chi_p(d(Y)) = 1$, then $S_p(Y) = \emptyset$ by Proposition 1.0.1. Suppose that $\chi_p(d(Y)) = -1$, and let $p$ be a point of $\pi_{F^{-1}}(p) \subset U$. Since $\chi_p(D) = -1$, both of $E'_p := E' \otimes \kappa_p$ and $E_p := E \otimes \kappa_p$ are supersingular by Proposition 3.5.3, and hence $\text{Km}(A) \otimes \kappa_p = \text{Km}(E'_p \times E_p)$ is supersingular by Propositions 3.1.1 and 4.3.2. By Proposition 5.1.3, we see that $Y \otimes \kappa_p$ is also supersingular. Hence $\pi_{F^{-1}}(p) = S_p(Y)$ holds. \qed

From the equality (6.3.2) and Propositions 6.3.2, 6.3.3, we obtain the following:

**Proposition 6.3.5.** Let $N$ be a finite set of prime integers with the properties given in Proposition 6.3.2. Suppose that $p \not\in N$ satisfies $\chi_p(d(Y)) = -1$, and let $p$ be a point of $\pi_{F^{-1}}(p) = S_p(Y)$.

Then the diagram $(\SIK)_Y$ induces an isomorphism of lattices
\[
L(Y, p) \cong (\text{Hom}(E', E) \hookrightarrow \text{Hom}(E'_p, E_p)) \downarrow [-1],
\]
where $E'_p := E' \otimes \kappa_p$ and $E_p := E \otimes \kappa_p$.

**6.4. Shioda-Mitani theory.** In this subsection, we work over $\mathbb{C}$, and review the Shioda-Mitani theory [33] on product abelian surfaces. Let $M[a, b, c]$ be a matrix in the set $Q_D$ defined in (1.0.3), where $D = b^2 - 4ac$ is a negative integer. Let $\sqrt{D} \in \mathbb{C}$ be in the upper half-plane, and put
\[
\tau' := (-b + \sqrt{D})/(2a), \quad \tau := (b + \sqrt{D})/2.
\]
We consider the complex elliptic curves
\[
anE' := \mathbb{C}/(\mathbb{Z} + Z\tau'), \quad anE := \mathbb{C}/(\mathbb{Z} + Z\tau).
\]

**Proposition 6.4.1** ([33]). The oriented transcendental lattice $\tilde{T}(anE' \times anE)$ of the product abelian surface $anE' \times anE$ is represented by $M[a, b, c] \in Q_D$.

Suppose that $D$ is a negative fundamental discriminant and that $M[a, b, c]$ is in the set $Q_D$ defined in (1.0.3). We put $K := \mathbb{Q}(\sqrt{D}) \subset \mathbb{C}$. Then
\[
I_0 := \mathbb{Z} + Z\tau'
\]
is a fractional ideal of $K$, and $\mathbb{Z} + Z\tau$ is equal to $\mathbb{Z}_K$.

**Proposition 6.4.2** (4.14 in [33]). Let $J_1$ and $J_2$ be fractional ideals of $K$. Then the product abelian surface $\mathbb{C}/J_1 \times \mathbb{C}/J_2$ is isomorphic to $anE' \times anE$ if and only if $|J_1||J_2| = |I_0|$ holds in the ideal class group $Cl_D$.

Recall the definition of $\Psi : Cl_D \cong \tilde{L}_D^*$ in Proposition 1.0.6. The image of $[I_0] \in Cl_D$ by $\Psi$ is represented by $M[a, b, c]$. Hence we obtain the following:

**Corollary 6.4.3.** For fractional ideals $J_1$ and $J_2$ of $K$, we have
\[
[T(\mathbb{C}/J_1 \times \mathbb{C}/J_2)] = \Psi([J_1][J_2]).
\]
6.5. **Proof of Theorem** [1] Let \( X \to \text{Spec} \ F \) and \( \mathcal{X} \to U \) be as in [1]. We choose \( \sigma \in \text{Emb}(F) \), and let \( M[a,b,c] \in Q_d(X) \) be a matrix representing \([\tilde{T}(X^\sigma)]\in \tilde{L}_{d(X)}\), where \( d(X) := \text{disc}(\text{NS}(X)) \). We define complex elliptic curves \( ^aE' \) and \( ^aE \) by (6.4.1) and (6.4.2). Then there exist elliptic curves \( E' \) and \( E \) defined over a number field \( L \subset \mathbb{C} \) such that \( E' \otimes \mathbb{C} \) and \( E \otimes \mathbb{C} \) are isomorphic to \( ^aE' \) and \( ^aE \), respectively. By replacing \( L \) with a finite extension, if necessary, we have an \( \text{SIK} \) diagram

\[
\mathcal{Y} \leftarrow \tilde{\mathcal{Y}} \to \text{Km}(A) \leftarrow \tilde{A} \to A := \mathcal{E}' \times_{U_L} \mathcal{E}
\]

over a non-empty open subset \( U_L \) of \( \text{Spec} \ Z_L[1/2] \) such that the generic fibers of \( \mathcal{E}' \) and \( \mathcal{E} \) are isomorphic to \( E' \) and \( E \), respectively. We put

\[
A := A \otimes L = E' \times E \text{ and } Y := \mathcal{Y} \otimes L.
\]

Then we see from Proposition [6.4.1] that \([\tilde{T}(A \otimes \mathbb{C})]\) is represented by the matrix \( M[a,b,c] \). Therefore we have \([\tilde{T}(A \otimes \mathbb{C})] = [\tilde{T}(X^\sigma)]\). On the other hand, we have \([\tilde{T}(Y \otimes \mathbb{C})] = [\tilde{T}(A \otimes \mathbb{C})]\) by Proposition [6.3.3]. Hence we obtain

\[
[\tilde{T}(Y \otimes \mathbb{C})] = [\tilde{T}(X^\sigma)].
\]

By the Torelli theorem for \( K3 \) surfaces [21] or the Shioda-Inose theorem (Theorem [1.0.5]), the complex \( K3 \) surfaces \( Y \otimes \mathbb{C} \) and \( X^\sigma \) are isomorphic. Hence \( d(Y) := \text{disc}(\text{NS}(Y)) \) is equal to \( d(X) \). Moreover, there exists a number field \( M \subset \mathbb{C} \) containing both of \( \sigma(F) \subset \mathbb{C} \) and \( L \subset \mathbb{C} \) such that \( X \otimes M \) and \( Y \otimes M \) are isomorphic over \( M \). Then \( \mathcal{X} \times \text{Spec} \ Z_M \) and \( \mathcal{Y} \times \text{Spec} \ Z_M \) are isomorphic over the generic point of \( \text{Spec} \ Z_M \), and hence there exists a non-empty open subset \( V \) of \( \text{Spec} \ Z_M \) such that

\[
\mathcal{X}_V := \mathcal{X} \otimes V \text{ and } \mathcal{Y}_V := \mathcal{Y} \otimes V
\]

are isomorphic over \( V \) by Corollary [6.1.4]. Let

\[
\pi_{M,F} : \text{Spec} \ Z_M \to \text{Spec} \ Z_F \text{ and } \pi_{M,L} : \text{Spec} \ Z_M \to \text{Spec} \ Z_L
\]

be the natural projections. By deleting finitely many closed points from \( V \), we can assume that \( \pi_{M,F}(V) \subset U \) and \( \pi_{M,L}(V) \subset U_L \). Then we have

\[
\pi_{M,F}^{-1}(S_p(\mathcal{X})) \cap V = S_p(\mathcal{X}_V) = S_p(\mathcal{Y}_V) = \pi_{M,L}^{-1}(S_p(\mathcal{Y})) \cap V
\]

for any \( p \in \pi_M(V) \). We choose a finite set \( N \) of prime integers in such a way that the following hold:

(i) \( N \) contains all the prime divisors of \( 2d(X) = 2d(Y) \),

(ii) if \( p \notin N \), then \( \pi_{M,F}^{-1}(p) \subset U \), and hence \( \pi_{M,F}^{-1}(p) \subset U_L \) hold,

(iii) \( N \) satisfies the condition [6.3.1] for \( \mathcal{Y} \).

Then \( N \) satisfies the condition [1.0.1] for \( \mathcal{X} \). Hence Theorem [1] is proved.

6.6. **Proof of Theorem** [3](T). Let \( S \) be as in the statement of Theorem [3]. Since \( D = \text{disc}(\text{NS}(S)) \) is assumed to be a fundamental discriminant, there exists an imaginary quadratic field \( K \) with discriminant \( D \). We fix an embedding \( K \hookrightarrow \mathbb{C} \) once and for all. For a finite extension \( L \) of \( K \), we denote by \( \text{Emb}(L/K) \) the set of embeddings of \( L \) into \( \mathbb{C} \) whose restrictions to \( K \) are the fixed one.

We recall the theory of complex multiplications. See [35, Chap. II], for example, for the details. Let \( \overline{Q} \subset \mathbb{C} \) be the algebraic closure of \( Q \) in \( \mathbb{C} \), and let \( \mathcal{E}\mathcal{L}\mathcal{L}(Z_K) \) be the set of \( \overline{Q} \)-isomorphism classes \([E]\) of elliptic curves \( E \) defined over \( \overline{Q} \) such that
End\( (E) \cong \mathbb{Z}_K \). Then \( \mathcal{ELL}(\mathbb{Z}_K) \) consists of \( h \) elements, where \( h \) is the class number \( |Cl_D| \) of \( \mathbb{Z}_K \). We denote by

\[
\alpha_1, \ldots, \alpha_h \in \overline{\mathbb{Q}} \subset \mathbb{C}
\]

the \( j \)-invariants \( j(E) \) of the isomorphism classes \( [E] \in \mathcal{ELL}(\mathbb{Z}_K) \), and put

\[
\Phi_D(t) := (t - \alpha_1) \cdots (t - \alpha_h).
\]

Then \( \Phi_D(t) \) is a polynomial in \( \mathbb{Z}[t] \), which is called the \textit{Hilbert class polynomial} of \( \mathbb{Z}_K \). It is known that \( \Phi_D(t) \) is irreducible in \( K[t] \). The field \( H := K(\alpha_1) \subset \mathbb{C} \) is the maximal unramified abelian extension of \( K \), which is called the \textit{Hilbert class field} of \( K \). We define an action of \( Cl_D \) on \( \mathcal{ELL}(\mathbb{Z}_K) \) by

\[
[I] \ast [E] := [C/I^{-1}I_E] \quad \text{for } [I] \in Cl_D \text{ and } [E] \in \mathcal{ELL}(\mathbb{Z}_K),
\]

where \( I_E \subset K \) is a fractional ideal such that \( E \cong \mathbb{C}/I_E \). On the other hand, for an elliptic curve \( E \) defined over \( \overline{\mathbb{Q}} \) and \( \gamma \in \text{Gal}(\overline{\mathbb{Q}}/K) \), we denote by \( E^\gamma \) the elliptic curve obtained from \( E \) by letting \( \gamma \) act on the defining equation for \( E \). Then \( \text{Gal}(\overline{\mathbb{Q}}/K) \) acts on \( \mathcal{ELL}(\mathbb{Z}_K) \) by \( [E]^\gamma := [E^\gamma] \). The following is the central result in the theory of complex multiplications.

**Theorem 6.6.1.** There exists a homomorphism \( F : \text{Gal}(\overline{\mathbb{Q}}/K) \to Cl_D \) such that \( [E]^\gamma = F(\gamma) \ast [E] \) holds for any \( [E] \in \mathcal{ELL}(\mathbb{Z}_K) \) and \( \gamma \in \text{Gal}(\overline{\mathbb{Q}}/K) \). Moreover, this homomorphism \( F \) induces an isomorphism \( \text{Gal}(H/K) \cong Cl_D \).

We put \( H := K[t]/(\Phi_D) \), and denote by \( \alpha \in H \) the class of \( t \in K[t] \) modulo the ideal \( (\Phi_D) \). Then we have \( \text{Emb}(H/K) = \{\sigma_1, \ldots, \sigma_h\} \), where \( \sigma_i \) is given by \( \sigma_i(\alpha) = \alpha_i \). Moreover, we have \( H = \sigma_1(H) = \cdots = \sigma_h(H) \in \mathbb{C} \). Let \( E_\alpha \) be an elliptic curve defined over \( H \) such that

\[
j(E_\alpha) = \alpha \in H.
\]

A construction of such an elliptic curve is given, for example, in [23, §1 in Chap. III]. For each \( \sigma_i \in \text{Emb}(H/K) \), we denote by \( E_\alpha^{\sigma_i} \) the elliptic curve defined over \( H = \sigma_i(H) \subset \overline{\mathbb{Q}} \) obtained from \( E_\alpha \) by applying \( \sigma_i \) to the coefficients of the defining equation. Then we have \( j(E_\alpha^{\sigma_i}) = \alpha_i \in H \), and there exists a unique ideal class \( [I_i] \in Cl_D \) of \( K \) such that \( E_\alpha^{\sigma_i} \cong \mathbb{C}/I_i \). Moreover, we have

\[
\mathcal{ELL}(\mathbb{Z}_K) = \{[E_\alpha^{\sigma_1}], \ldots, [E_\alpha^{\sigma_h}]\} \quad \text{and} \quad Cl_D = \{[I_1], \ldots, [I_h]\}.
\]

Since \( \text{Gal}(H/K) \) is abelian, there exists a canonical isomorphism \( \text{Gal}(H/K) \cong \text{Gal}(H/K) \), which we will denote by \( \gamma \mapsto \tilde{\gamma} \). By Theorem 6.6.1 we have an isomorphism \( \text{Gal}(H/K) \cong Cl_D \) denoted by \( \gamma \mapsto [I_i] \) such that

\[
E_\alpha^{\sigma_i, \gamma} = (E_\alpha^{\sigma_i})^{\gamma} = (E_\alpha^{\sigma_i})^{\tilde{\gamma}} \cong \mathbb{C}/I_i^{-1}I_i
\]

holds for any \( i = 1, \ldots, h \) and any \( \gamma \in \text{Gal}(H/K) \).

There exist a finite extension \( F \) of \( H \) and a non-empty open subset \( U \) of \( \text{Spec} \mathbb{Z}_F[1/2] \) such that, for each \( \gamma \in \text{Gal}(H/K) \), there exist smooth proper families of elliptic curves \( \mathcal{E}_\gamma \) and \( \mathcal{E}_\alpha \) over \( U \) whose generic fibers are isomorphic to \( E_\alpha^{\gamma} \otimes F \) and \( E_\alpha \otimes F \), respectively, and an \( \text{SIK} \) diagram

\[
(SIK)^\gamma : Y^\gamma \leftarrow \tilde{Y}^\gamma \rightarrow \text{Km}(\mathcal{A}^\gamma) \leftarrow \tilde{A}^\gamma \rightarrow \mathcal{A}^\gamma := \mathcal{E}_\gamma \times_U \mathcal{E}_\alpha
\]
of $E_\alpha$ and $E_\alpha$ over $U$. We then put $Y^\gamma := \mathcal{Y}^\gamma \otimes F$ and $A^\gamma := \mathcal{A}^\gamma \otimes F$. Let $\sigma$ be an element of $\text{Emb}(F/K)$. If the restriction of $\sigma$ to $H$ is equal to $\sigma_i$, then we have the following equalities in $\tilde{L}_D^*$:

$$[\tilde{T}((Y^\gamma)^\sigma)] = [\tilde{T}((A^\gamma)^\sigma)] = [\tilde{T}(E_\alpha^\sigma \times E_\alpha^\sigma)]$$

by Proposition 6.3.3

$$= [\tilde{T}(E_\alpha^\sigma \times E_\alpha^\sigma)]$$

by (6.6.2)

$$= \Psi([I_i]^{-1}[I_i]^2)$$

by Corollary 6.4.3

Note that the restriction map $\text{Emb}(F/K) \to \text{Emb}(H/K)$ is surjective. Therefore, the following equalities in $\tilde{L}_D^*$ holds so that $\text{Lie} : \text{End}(F) \to \text{End}(E_\alpha)$ contains $\phi$.

$$\phi : \text{End}(F) \to \text{End}(E_\alpha)$$

We consider pairs $(\gamma, \alpha)$ such that two such pairs $(\gamma, \alpha)$ are isomorphic.

$$\gamma : \mathcal{Y}^\gamma \otimes F$$

and $\alpha$ isomorphic to a maximal order of $\mathcal{Z}$ and $\alpha$ is a root of $\Phi_D$ and $F$ contains $K$, we have the Lie-normalized isomorphism $\text{End}(E_\alpha) \cong \mathbb{Z}_K$.

We consider the $\text{SIK}$ diagram $(\text{SIK})^{\gamma(S)}$ smaller if necessary, we can assume the following:

(i) $U = \pi_F^{-1}(\pi_F(U))$, and $p \not\parallel 2D$ for any $p \in \pi_F(U)$,

(ii) if $p \in \pi_F(U)$, then $\Phi_D(t) \bmod p$ has no multiple roots in $\overline{\mathbb{F}}_p$, and

(iii) for $p \in \pi_F(U)$, we have the following equivalence:

$$\chi_p(D) = -1 \iff S_p(\mathcal{X}) \neq \emptyset \iff S_p(\mathcal{X}) = \pi_F^{-1}(p).$$

Let $p$ be a prime integer in $\pi_F(U)$ such that $\chi_p(D) = -1$, so that $S_p(\mathcal{X}) = \pi_F^{-1}(p)$. We show that, under the assumption that $D$ is odd, the set of isomorphism classes of supersingular reduction lattices $\{[L(\mathcal{X}, \varphi)] | p \in \pi_F^{-1}(p)\}$ coincides with a genus.

Let $B$ denote the quaternion algebra over $\mathbb{Q}$ that ramifies exactly at $p$ and $\infty$. We consider pairs $(R, Z)$ of a $\mathbb{Z}$-algebra $R$ and a subalgebra $Z \subset R$ such that $R$ is isomorphic to a maximal order of $B$ and such that $Z$ is isomorphic to $\mathbb{Z}_K$. We say that two such pairs $(R, Z)$ and $(R', Z')$ are isomorphic if there exists an isomorphism $\varphi : R \cong R'$ satisfying $\varphi(Z) = Z'$. We denote by $\mathcal{R}$ the set of isomorphism classes $[R, Z]$ of these pairs. Next we consider pairs $(R, \rho)$ of a $\mathbb{Z}$-algebra $R$ isomorphic to a maximal order of $B$ and an embedding $\rho : \mathbb{Z}_K \hookrightarrow R$ as a $\mathbb{Z}$-subalgebra. We say
that two such pairs \((R, \rho)\) and \((R', \rho')\) are isomorphic if there exists an isomorphism \(\varphi : R \cong R'\) satisfying \(\varphi \circ \rho = \rho'\). We denote by \(\widehat{\mathcal{R}}\) the set of isomorphism classes \([R, \rho]\) of these pairs. For an embedding \(\rho : \mathbb{Z}_K \hookrightarrow R\), we denote by \(\bar{\rho}\) the composite of the non-trivial automorphism of \(\mathbb{Z}_K\) and \(\rho\). The natural map

\[
\Pi_{\mathcal{R}} : \widehat{\mathcal{R}} \rightarrow \mathcal{R}
\]

given by \([R, \rho] \mapsto [R, \rho(\mathbb{Z}_K)]\) is surjective, and its fiber consists either of two elements \([R, \rho]\) and \([R, \bar{\rho}]\), or of a single element \([R, \rho] = [R, \bar{\rho}]\).

Let \(p\) be a point of \(\pi_F^{-1}(p)\). We denote by \(F[p]\) the completion of \(F\) at \(p\), and put

\[
E[p] := E_\alpha \otimes F[p] \quad \text{and} \quad E_p := E_\alpha \otimes \kappa_p.
\]

Then we have canonical isomorphisms

\[
(6.7.3) \quad \text{End}_{F[p]}(E[p]) \cong \text{End}(E[p]) \cong \text{End}(E_\alpha)
\]

by the assumption (6.7.1), and hence \(\text{Lie} : \text{End}(E[p]) \rightarrow F[p]\) is defined. We put

\[
R_p := \text{End}(E_p),
\]

which is isomorphic to a maximal order of \(B\) by Proposition 3.4.1 and denote by

\[
\rho_p : \text{End}(E[p]) \hookrightarrow R_p
\]

the specialization isometry. Using the isomorphisms (6.7.3) and the Lie-normalized isomorphism (6.7.2), we obtain an element \([R_p, \rho_p]\) of \(\widehat{\mathcal{R}}\). We denote by

\[
\bar{r} : S_p(\mathcal{X}) \rightarrow \widehat{\mathcal{R}}
\]

the map given by \(p \mapsto [R_p, \rho_p]\).

**Lemma 6.7.1.** The map \(\bar{r}\) is surjective.

**Proof.** First we show that the map \(r := \Pi_{\mathcal{R}} \circ \bar{r}\) from \(S_p(\mathcal{X})\) to \(\mathcal{R}\) is surjective. Let \([R, Z]\) be an element of \(\mathcal{R}\). By Proposition 3.4.2, there exists a supersingular elliptic curve \(C_0\) in characteristic \(p\) with an isomorphism \(\psi : \text{End}(C_0) \cong R\). Let \(\alpha_0 \in \text{End}(C_0)\) be an element such that the subalgebra \(\mathbb{Z} + \mathbb{Z} \alpha_0\) corresponds to \(Z \subset R\) by \(\psi\). By Proposition 3.5.3, there exists a lift \((C, \alpha)\) of \((C_0, \alpha_0)\), where \(C\) is an elliptic curve defined over a finite extension of \(\mathbb{Q}_p\). Since \(\mathbb{Z} + \mathbb{Z} \alpha \subseteq \text{End}(C)\) is isomorphic to \(\mathbb{Z}_K\), we have \(\text{End}(C) \cong \mathbb{Z}_K\), and hence the \(j\)-invariant of \(C\) is a root of the Hilbert class polynomial \(\Phi_D\) in \(\mathbb{Q}_p\). Since the set of roots of \(\Phi_D\) in \(\mathbb{Q}_p\) is in one-to-one correspondence with \(\pi_F^{-1}(p)\) by the assumption (ii) on \(U\), and \(U\) contains \(\pi_F^{-1}(p)\) by the assumption (i) on \(U\), there exists \(p \in \pi_F^{-1}(p) \subset U\) such that

\[
j(E[p]) = j(C).
\]

By applying Proposition 3.5.2 with \(g = \text{id}\), we have \(r(p) = [R, Z]\). To prove that \(\bar{r}\) is surjective, therefore, it is enough to show that, for each \(p \in \pi_F^{-1}(p)\), there exists \(p' \in \pi_F^{-1}(p)\) such that \([R_{p'}, \rho_{p'}] = [R_p, \rho_p]\) holds in \(\widehat{\mathcal{R}}\). We choose an element \(g \in \text{Gal}(F/\mathbb{Q})\) such that the restriction of \(g\) to \(K\) is the non-trivial element of
Gal\(\mathbb{K}/\mathbb{Q}\), and let \(\mathfrak{p}'\) be the image of \(\mathfrak{p}\) by the action of \(g\) on \(\pi_{\mathfrak{p}}^{-1}(p)\). Consider the diagram

\[
\begin{array}{cccc}
F[\mathfrak{p}] & \xrightarrow{\text{Lie}} & \text{End}(E[\mathfrak{p}]) & \xrightarrow{\rho_{\mathfrak{p}}} & \text{End}(E) \\
\downarrow I & \xrightarrow{\lambda} & \downarrow \lambda' & \xrightarrow{\rho_{\mathfrak{p}}} & \downarrow \lambda' \\
F[\mathfrak{p}'] & \xrightarrow{\text{Lie}} & \text{End}(E[\mathfrak{p}']) & \xrightarrow{\rho_{\mathfrak{p}'}_+} & \text{End}(E'),
\end{array}
\]

where \(\lambda\) and \(\lambda'\) are the canonical isomorphisms \((6.7.3)\), and the vertical isomorphisms \(f_{g}, e_{g}\) and \(E_{g}\) are given by the action of \(g\). Then we have \(e_{g} \circ \lambda = \lambda' \circ \lambda\), where \(\lambda'\) is the composite of the non-trivial automorphism of \(\text{End}(E_{\alpha}) \cong \mathbb{Z}_{K}\) and \(\lambda'\). By Proposition \(3.5.2\) we have \(E_{g} \circ \rho_{\mathfrak{p}} = \rho_{\mathfrak{p}'} \circ e_{g}\), and hence \([R_{\mathfrak{p}'}, \rho_{\mathfrak{p}'}] = [R_{\mathfrak{p}}, \rho_{\mathfrak{p}}]\). \(\square\)

Suppose that the ideal class \([I_{\gamma}(S)] \in \text{Cl}_{D}\) is represented by an ideal \(J \subset \mathbb{Z}_{K}\). We can regard \(J\) as an ideal of \(\text{End}(E_{\alpha})\) by the Lie-normalized isomorphism \(6.7.2\). By \([7, \text{Corollary 7.17}]\), we can choose \(J \subset \mathbb{Z}_{K}\) in such a way that \(d_{J} := \deg \phi_{J} = [\text{End}(E_{\alpha}): J]\) is prime to \(D\). (See Remark \(6.7.3\) \((2)\).) For any \(\sigma_{i} \in \text{Emb}(H/K)\), we have the following isomorphisms of complex elliptic curves:

\[
(E_{\alpha}^{\gamma}(S))^{\sigma_{i}} \cong \mathbb{C}/I_{\gamma}(S)^{-1}I_{i} \quad \text{by} \quad (6.6.2)
\]

\[
\cong \mathbb{C}/J^{-1}I_{i} \quad \text{by} \quad [J] = [I_{\gamma}(S)]
\]

\[
\cong (E_{\alpha}^{\gamma}(S))^{J} \quad \text{by} \quad E_{\alpha}^{\gamma}(S) \cong \mathbb{C}/I_{i} \text{ and Proposition } 3.3.4
\]

\[
\cong (E_{\alpha}^{J})^{\sigma_{i}} \quad \text{since the construction of } E \to E^{J} \text{ is algebraic.}
\]

Hence we have

\[
(6.7.4) \quad (E_{\alpha}^{\gamma}(S))^{J} \otimes \overline{\mathcal{F}} \cong E_{\alpha}^{J} \otimes \overline{\mathcal{F}}.
\]

We then consider \(J\) as an ideal of \(\text{End}(E_{[\mathfrak{p}]}\) by the canonical isomorphisms \((6.7.3)\), and we consider the left ideal \(R_{\mathfrak{p}}\rho_{\mathfrak{p}}(J)\) of \(R_{\mathfrak{p}}\) generated by \(\rho_{\mathfrak{p}}(J)\). From the isomorphism \((6.7.4)\), we obtain an isomorphism

\[
E_{\alpha}^{\gamma}(S) \otimes \overline{\mathcal{F}}[\mathfrak{p}] \cong E_{[\mathfrak{p}]}^{J} \otimes \overline{\mathcal{F}}[\mathfrak{p}].
\]

Then, by Proposition \(3.5.3\) we have

\[
E_{\alpha}^{\gamma}(S) \otimes \overline{\mathcal{F}}[\mathfrak{p}] \cong E_{[\mathfrak{p}]}^{R_{\mathfrak{p}}\rho_{\mathfrak{p}}(J)} \otimes \overline{\mathcal{F}}[\mathfrak{p}].
\]

Therefore we have the following equalities in the set \(L_{p^{2}d_{J}D}\):

\[
[L(X, \mathfrak{p})[-d_{J}]] = [(\text{Hom}(E[\mathfrak{p}]^{J}, E[\mathfrak{p}]) \hookrightarrow \text{Hom}(E_{p}^{R_{\mathfrak{p}}\rho_{\mathfrak{p}}(J), E_{p}})^{\perp} [d_{J}])] \quad \text{by Proposition } 6.3.5
\]

\[
= [(J \hookrightarrow R_{\mathfrak{p}}\rho_{\mathfrak{p}}(J)^{\perp})] \quad \text{by Proposition } 3.5.5
\]

By the surjectivity of the map \(\overline{r}\), we complete the proof of Theorem \((3.\text{L})\) by the following proposition, which will be proved in the next section.
Proposition 6.7.2. Let $J$ be an ideal of $\mathbb{Z}_K$. Suppose that $D$ is odd and that $d_J = N(J) = [\mathbb{Z}_K : J]$ is prime to $D$. Then the set

$$\{ (J \hookrightarrow R_{\rho}(J))^{-1} \mid [R, \rho] \in \tilde{R} \}$$

coincides with a genus in $L_{p^2d_J^2D}$.

Remark 6.7.3. (1) We make use of the assumption that $D$ is odd in Theorem [3.L] only in the proof of Proposition 6.7.2. (2) The condition $\gcd(N(J), D) = 1$ is assumed only in order to simplify the proof of Proposition 6.7.2.

7. The maximal orders of a quaternion algebra

Let $K$, $D$, $p$, $B$ and $\tilde{R}$ be as in the previous section. We assume that $D$ is odd. We describe the set $\tilde{R}$ following Dorman [9], and prove Proposition 6.7.2.

7.1. Dorman’s description of $\tilde{R}$. Note that $D$ is a square-free negative integer satisfying $D \equiv 1 \mod 4$. We choose a prime integer $q$ that satisfies

$$(7.1.1) \quad \chi_l(-pq) = 1 \quad \text{for all prime divisors } l \text{ of } D.$$

Then the $\mathbb{Q}$-algebra

$$B := \{ [\alpha, \beta] \mid \alpha, \beta \in K \}, \quad \text{where } [\alpha, \beta] := \left( \frac{\alpha}{\beta}, \frac{\beta}{\alpha} \right),$$

is a quaternion algebra that ramifies exactly at $p$ and $\infty$. The canonical involution of $B$ is given by $[\alpha, \beta]^* = [\bar{\alpha}, -\bar{\beta}]$. Hence the bilinear form (3.4.1) on $B$ is given by

$$(7.1.2) \quad ([\alpha, \beta], [\alpha', \beta']) = \text{Tr}_{K/\mathbb{Q}}(\alpha\alpha') + pq\text{Tr}_{K/\mathbb{Q}}(\beta\beta').$$

Note that we have

$$(7.1.3) \quad [\gamma, 0][\alpha, \beta] = [\gamma\alpha, \gamma\beta] \quad \text{and} \quad [\alpha, \beta][\gamma, 0] = [\gamma\alpha, \gamma\beta].$$

For simplicity, we use the following notation:

$$[S, T] := \{ [\alpha, \beta] \in B \mid \alpha \in S, \beta \in T \} \quad \text{for subsets } S \text{ and } T \text{ of } K.$$

For $u \in B^\times$, we denote by $\theta_u : B \cong B$ the inner automorphism $\theta_u(x) := uxu^{-1}$. We have a natural embedding $\iota : K \hookrightarrow B$ given by $\iota(\alpha) := [\alpha, 0]$. By the Skolem-Noether theorem (for instance, see Chapter 8 of [3]), we see that, if $\iota' : K \hookrightarrow B$ is another embedding as a $\mathbb{Q}$-algebra, then there exists a $u \in B^\times$ such that $\theta_u \circ \iota = \iota'$ holds. On the other hand, we have $\theta_u \circ \iota = \iota$ if and only if $u \in [K^\times, 0]$. Hence we have a canonical identification

$$\tilde{R} \cong [K^\times, 0] \setminus \mathbf{R},$$

where $\mathbf{R}$ is the set of maximal orders $R$ of $B$ such that $R \cap [K, 0] = [\mathbb{Z}_K, 0]$ holds. We will examine the set $\mathbf{R}$.

For a $\mathbb{Z}$-submodule $\Lambda \subset B$ of rank 4, we put

$$N_B(\Lambda) := ([\mathbb{Z}_K, \mathbb{Z}_K] : n\Lambda]/n^4,$$

where $n$ is a non-zero integer such that $n\Lambda \subset [\mathbb{Z}_K, \mathbb{Z}_K]$. An order $R$ of $B$ is maximal if and only if $R$ is of discriminant $p^2$ as a lattice. Since the discriminant of $[\mathbb{Z}_K, \mathbb{Z}_K]$ is $p^2q^2|D|^2$, we obtain the following.
Lemma 7.1.1. An order $R$ of $B$ is maximal if and only if $N_B(R) = 1/(q|D|)$.

We denote by $\text{pr}_2 : B \to K$ the projection given by $\text{pr}_2([\alpha, \beta]) := \beta$.

Lemma 7.1.2. Let $R$ be an element of $\mathbf{R}$. Then $M_R := \text{pr}_2(R)$ is a fractional ideal of $K$ with $N(M_R) = 1/(q|D|)$.

Proof. It is obvious that $M_R \subset K$ is a finitely generated $\mathbb{Z}_K$-module by the formula (7.1.3). Since $[K,0] \cap R = [\mathbb{Z}_K,0]$, we have $N(M_R) = N_B(R) = 1/(q|D|)$ by Lemma 7.1.1.

From the condition (7.1.1) on $q$, $x_p(D) = -1$ and $D \equiv 1 \mod 4$, we deduce that $q$ splits completely in $K$. We choose an ideal $Q \subset \mathbb{Z}_K$ such that $(q) = Q\overline{Q}$. We also denote by $D$ the principal ideal $(\sqrt{D}) \subset \mathbb{Z}_K$. Let $R$ be an element of $\mathbf{R}$. By Lemma 7.1.2 the fractional ideal

$$I_R := \mathcal{D}QM_R \quad (M_R := \text{pr}_2(R))$$

satisfies $N(I_R) = 1$. Since $[K,0] \cap R = [\mathbb{Z}_K,0]$, we can define a map $f_R : M_R \to K/\mathbb{Z}_K$ by $f_R(\beta) := \alpha + \mathbb{Z}_K$ for $[\alpha, \beta] \in R$. By the formula (7.1.3), we see that $f_R$ is a homomorphism of $\mathbb{Z}_K$-modules, and we have $f_R(\gamma\beta) = f_R(\gamma\beta)$ for any $\gamma \in \mathbb{Z}_K$ and $\beta \in M_R$. Therefore $f_R(\sqrt{D}\beta) = \sqrt{D}f_R(\beta) = 0$ holds for any $\beta \in M_R$. Thus $f_R$ induces a homomorphism

$$\tilde{f}_R : M_R/\mathcal{D}M_R \to \mathcal{D}^{-1}/\mathbb{Z}_K$$

de torsion $\mathbb{Z}_K$-modules.

Lemma 7.1.3. The homomorphism $\tilde{f}_R$ is an isomorphism.

Proof. Since $|M_R/\mathcal{D}M_R| = |\mathcal{D}^{-1}/\mathbb{Z}_K| = |D|$, it is enough to show that $\tilde{f}_R$ is injective. Let $\mathcal{F}$ be the fractional ideal such that $\text{Ker}(f_R) = \mathcal{F}M_R = \mathcal{F}Q^{-1}I_R$. Suppose that $\beta, \beta' \in \text{Ker}(f_R)$. Then $[0, \beta] \in R$ and $[0, \beta'] \in R$ hold, and hence $[0, \beta] \cdot [0, \beta'] = [-pq\beta\overline{\beta}, 0]$ is also in $R$. From $[K,0] \cap R = [\mathbb{Z}_K,0]$, we have $-pq\beta\overline{\beta} \in \mathbb{Z}_K$. Since $N(I_R) = 1$, we have

$$pq(\mathcal{F}Q^{-1}I_R)(\mathcal{F}Q^{-1}I_R) = p\mathcal{F}\mathcal{F} \subset \mathbb{Z}_K.$$  

Since $\text{gcd}(p, D) = 1$ and $\mathbb{Z}_K \subset \mathcal{F} \subset \mathcal{D}^{-1}$, we have $\mathcal{F} = \mathbb{Z}_K$. 

Since $\tilde{f}_R$ is an isomorphism, there exists a unique element $\mu_R + \mathcal{D}M_R = \mu_R + Q^{-1}I_R \in M_R/\mathcal{D}M_R$ such that $\tilde{f}_R(\mu_R + Q^{-1}I_R) = (1/\sqrt{D}) + \mathbb{Z}_K$.

Lemma 7.1.4. For any $\beta \in M_R$, we have

$$f_R(\beta) = pq\sqrt{D}\mu_R\beta + \mathbb{Z}_K = pq\sqrt{D}\mu_R\beta + \mathbb{Z}_K.$$ 

Proof. For $\beta \in M_R$, we have $[0, \sqrt{D}\beta] \in R$. Since $[1/\sqrt{D}, \mu_R] \in R$, we have $[0, \sqrt{D}\beta] \cdot [1/\sqrt{D}, \mu_R] = [-pq\sqrt{D}\mu_R\beta, -\beta] \in R$ and $[1/\sqrt{D}, \mu_R] \cdot [0, \sqrt{D}\beta] = [pq\sqrt{D}\mu_R\beta, \beta] \in R$,

from which the desired description of $f_R$ follows. 

□
Lemma 7.1.5. Let $I$ be a fractional ideal with $N(I) = 1$, and let $x, x' \in D^{-1}Q^{-1}I$ satisfy $x' - x \equiv Q^{-1}I$. Then we have $qD|x|^2 \equiv Z$ and $qD|x'|^2 \equiv qD|x|^2 \mod D$.

Proof. Since $I_T = Z_K$, we have

$$qD|x|^2 \equiv qD(D^{-2}Q^{-1}I Q^{-1}) \cap Q = Z_K \cap Q = Z.$$ 

We put $x' = x + y$ with $y \in Q^{-1}I$. Then we have $q|y|^2 \in Z_K \cap Q = Z$. Since $D$ is odd, we have $D^{-1} \cap Q = Z$, and hence $q(x+y) \in D^{-1} \cap Q = Z$ holds. □

We define $T$ to be the set of all pairs $(I, \mu + Q^{-1}I)$, where $I$ is a fractional ideal of $K$ such that $N(I) = 1$, and $\mu + Q^{-1}I$ is an element of $D^{-1}Q^{-1}I/Q^{-1}I$ such that

$$pqD|\mu|^2 \equiv 1 \mod D.$$ 

Then we have a map $\tau : R \to T$ given by

$$\tau(R) := (I_R, \mu_R + Q^{-1}I_R) \in T.$$ 

Proposition 7.1.6. The map $\tau$ is a bijection.

Proof. The maximal order $R$ is uniquely recovered from $(I_R, \mu_R + Q^{-1}I_R)$ by

$$R = \{ [\alpha, \beta] \mid \beta \in D^{-1}Q^{-1}I_R, \alpha \equiv pq\sqrt{D\overline{\mu\beta}} \mod Z_K \}.$$ 

Hence $\tau$ is injective. Let an element $t := (I, \mu + Q^{-1}I)$ of $T$ be given. We put $M_t := D^{-1}Q^{-1}I$, and define $f_t : M_t \to D^{-1}/Z_K$ by

$$f_t(\beta) := pq\sqrt{D\overline{\mu\beta}} + Z_K.$$ 

Note that the definition of $f_t$ does not depend on the choice of the representative $\mu$ of $\mu + Q^{-1}I$. Since $M_t \cap [K, 0] = [Z_K, 0]$, we show that $Z_K$ is closed under the product. Since $f_t$ is a homomorphism of $Z_K$-modules, we have $[Z_K, 0]R_t = R_t$. By the formula (7.1.4), we have $R_t[Z_K, 0] = R_t$. Hence it is enough to prove that

$$[pq\sqrt{D\overline{\mu\beta}}, \beta']\cdot [pq\sqrt{D\overline{\mu\beta'}}, \beta'] = [p^2q^2D|\mu|\overline{\beta\beta'} - pq\beta\overline{\beta'}, pq\sqrt{D\mu(\overline{\beta}\beta' - \overline{\beta'}\beta)}]$$

is in $R_t$ for any $\beta, \beta' \in M_t$. Because

$$pq\beta\overline{\beta'} \in pqM_t \overline{\beta} = (p/D) \quad \text{and} \quad 1 - pqD|\mu|^2 \equiv 0 \mod D,$$

we have a congruence $pq\beta\overline{\beta'} \equiv p^2q^2D|\mu|^2\beta\overline{\beta'} \mod Z_K$. Hence

$$f_t(pq\sqrt{D\mu(\overline{\beta}\beta' - \overline{\beta'}\beta)}) \equiv p^2q^2D|\mu|^2\beta\overline{\beta'} \mod Z_K.$$ 

Therefore $R_tR_t = R_t$ is proved, and hence $R_t$ is an order. Because $N(M_t) = 1/(q|D|)$, we see that $R_t$ is maximal by Lemma 7.1.1. Hence $R_t \in R$. □
Proof of Proposition 6.7.2. Let $I \in \mathcal{I}$ denote the group of fractional ideals $I$ with $N(I) = 1$. We put

$$
P_I := I \cap P_D$$

and $C_1 := I_1 / P_1$.

Then $C_1$ is a subgroup of the ideal class group $Cl_D = \mathcal{I}_D / P_D$. Since the homomorphism $\mathcal{I}_D \to \mathcal{I}_1$ given by $I \mapsto I^{-1}$ is surjective and $|I|^{-1}$ is equal to $|I|^2$ in $Cl_D$, we see that the subgroup $C_1$ of $Cl_D$ is equal to $C_1^2$.

Lemma 7.1.7. The map $R \mapsto [I_R]$ from $R$ to $C_1 = C_1^2$ is surjective.

Proof. We will show that, for each $I \in \mathcal{I}_1$, there exists $\mu \in D^{-1}Q^{-1}I$ such that $pq\mu^2 \equiv 1 \mod D$ holds. Since $\mathcal{T} = Z_K$, there exists an ideal $A \subset Z_K$ such that $A + \bar{A} = Z_K$ and $I = AA^{-1}$. Since $A$ and $\bar{A}$ have no common prime divisors, the norm $n := N(A)$ is prime to $D$. Hence there exists an integer $m$ such that $nm \equiv 1 \mod D$ holds. By the condition (7.1.1) on $q$, there exists an integer $z$ such that $-pqz^2 \equiv 1 \mod D$ holds. Therefore we have an element

$$
zm \in \bar{A} \subset A \subset I \subset Q^{-1}I
$$

such that $-pq(zm)^2 \equiv 1 \mod D$. Then the element $\mu := zm/\sqrt{D}$ of $D^{-1}Q^{-1}I$ satisfies $pq\mu^2 = -pq(zm)^2 \equiv 1 \mod D$. \hfill \Box

7.2. Proof of Proposition 6.7.2. Let $J$ be a non-zero ideal in $Z_K$ such that $d_J := N(J)$ is prime to $D$. Then we have

$$(\mathcal{J} \cap \mathcal{D}) = \mathcal{J} \mathcal{D}.$$  

Lemma 7.2.1. Let $R$ be an element of $R$, and let $RJ$ denote the left-ideal of $R$ generated by $|J,0| \subset R$. Then we have

$$(J \mapsto RJ)^\perp = [0, Q^{-1}I_R\mathcal{J}],$$

where $[0, Q^{-1}I_R\mathcal{J}]$ is the lattice such that the underlying $Z$-module is $Q^{-1}I_R\mathcal{J} \subset K$ and such that the bilinear form is given by $(x,y) := pq \text{Tr}_{K/\mathbb{Q}}(xy)$.

Proof. For simplicity, we put $M := M_R$, $I := I_R$, $f := f_R$ and $\mu := \mu_R$. Since $J \otimes \mathbb{Q} = K$ and $B = [K,0] \perp [0,K]$ by (7.1.2), we see that $(J \mapsto RJ)^\perp$ is equal to $[0,K] \cap RJ$. Let $\gamma, \gamma'$ be a basis of $J$ as a $Z$-module. For an element $x \in K$, we have the following equivalence:

$$(0, x) \in RJ$$

$\Leftrightarrow$ there exist $[\alpha, \beta], [\alpha', \beta'] \in R$ such that $\alpha \gamma + \alpha' \gamma' = 0$ and $\beta \gamma + \beta' \gamma' = x$

$\Leftrightarrow$ there exist $\beta, \beta' \in M$ and $a, a' \in Z_K$ such that $\beta \gamma + \beta' \gamma' = x$ and $pq\sqrt{D}\mu(\beta \gamma + \beta' \gamma') + a \gamma + a' \gamma' = 0$

$\Leftrightarrow$ $x \in \mathcal{J}M$ and $pq\sqrt{D}\mu \in J$.

Suppose that $x \in \mathcal{J}M$ and $pq\sqrt{D}\mu \in J$. Then we have $f(x) = 0$ by Lemma 7.1.4 and hence

$$
x \in \mathcal{J}M \cap \text{Ker}(f) = \mathcal{J}DM = Q^{-1}I \mathcal{J}
$$

by Lemma 7.1.3 and the equality (7.2.1). Conversely, suppose that $x \in Q^{-1}I \mathcal{J}$. Then we have $x \in \mathcal{J}M$. On the other hand, there exist $\xi, \xi' \in Q^{-1}I$ such that
x = ξγ + ξ′. Since ξ, ξ′ ∈ DM, we have f(ξ) = f(ξ′) = 0, and hence both of
pq√Dμξ and pq√Dμξ′ are in ZK. Therefore we have

pq√Dμξ = (pq√Dμξ)γ + (pq√Dμξ′)γ′ ∈ J,

and thus [0, x] ∈ RJ holds.

We define an orientation of the Z-module Q−1JR ⊂ K by (1.0.5). Then, for
each R ∈ R, we obtain an oriented lattice [0, Q−1JR] of discriminant

(pq)2 · N(Q−1JR)2 · disc(ZK) = −p2d3D.

On the other hand, recall that Ψ([Q−1JR]) ∈ ĖD is represented by an oriented
lattice such that the underlying Z-module is Q−1JR ⊂ K and such that the bilinear
form is given by

(x, y) = \frac{1}{N(Q−1JR)} \Tr_{K/Q}(x y) = \frac{q}{d} \Tr_{K/Q}(x y).

Therefore the isomorphism class of the oriented lattice (J ↪ RJ)⊥ = [0, Q−1JR]
is equal to

Ψ([Q−1JR])|RJ| ∈ Ėp2d3D.

Thus Proposition [6.7.2] is proved.
[11] W. Fulton. Rational equivalence on singular varieties. *Inst. Hautes Études Sci. Publ. Math.*, 45:147–167, 1975. MR0404257 (53:8060)

[12] W. Fulton. Intersection theory, volume 2 of Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer-Verlag, Berlin, second edition, 1998. MR1644323 (99d:14003)

[13] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985. MR772491 (86j:11041)

[14] A. Grothendieck. *Fondements de la géométrie algébrique. [Extraits du Séminaire Bourbaki, 1957–1962.]* Secrétariat mathématique, Paris, 1962. MR0146040 (26:3566)

[15] A. Grothendieck. Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux (SGA 2). North-Holland Publishing Co., Amsterdam, 1968, Séminaire de Géométrie Algébrique du Bois-Marie, 1962, Advanced Studies in Pure Mathematics, Vol. 2, also available from http://arxiv.org/abs/math.AG/0511279. MR2171939 (2006f:14004)

[16] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57:3116)

[17] H. Inose. Defining equations of singular K3 surfaces and a notion of isogeny. In *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, pages 495–502, Tokyo, 1978. Kinokuniya Book Store. MR578868 (81h:14021)

[18] S. Lang. *Elliptic functions*, volume 112 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate. MR890960 (88c:11028)

[19] D. Mumford. *Lectures on curves on an algebraic surface*. With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59. Princeton University Press, Princeton, N.J., 1966. MR0209285 (35:187)

[20] V. V. Nikulin. Integer symmetric bilinear forms and some of their geometric applications. Math USSR-Izv. 14 (1979), no. 1, 103–167 (1980). MR525944 (80i:10031)

[21] I. I. Pjatecki˘ı-ˇSapiro and I. R. ˇSafareviˇc. Torelli’s theorem for algebraic surfaces of type K3. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:530–572, 1971. Reprinted in I. R. Shafarevich, Collected Mathematical Papers, Springer-Verlag, Berlin, 1989, pp. 516–557. MR633161 (83c:14027)

[22] I. Reiner. Maximal orders, volume 28 of London Mathematical Society Monographs. New Series. The Clarendon Press, Oxford University Press, Oxford, 2003. MR1972204 (2004c:16026)

[23] A. N. Rudakov and I. R. Shafarevich. Surfaces of type K3 over fields of finite characteristic. In *Current problems in mathematics, Vol. 18*, pages 115–207. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981. Reprinted in I. R. Shafarevich, Collected Mathematical Papers, Springer-Verlag, Berlin, 1989, pp. 657–714. MR633161 (83c:14027)

[24] M. Sch¨utt. Fields of definition for singular K3 surfaces. *Commun. Number Theory Phys.* 1 (2007), 307–321. MR2346573

[25] I. R. Shafarevich. On the arithmetic of singular K3-surfaces. In *Algebra and analysis (Kazan, 1994)*, pages 103–108. de Gruyter, Berlin, 1996. MR1465448 (98h:14041)

[26] I. Shimada. Correspondence of elliptic curves and Mordell-Weil lattices of certain K3 surfaces. *Complex analysis and algebraic geometry*, pages 119–136. Iwanami Shoten, Tokyo, 1977. MR0441982 (56:371)

[27] I. Shimada. On arithmetic Zariski pairs in degree 6. Preprint, 2006. To appear in Adv. Geom. http://arxiv.org/abs/math.AG/0611596.

[28] I. Shimada. Non-homeomorphic conjugate complex varieties. Preprint, 2007. http://arxiv.org/abs/math.AG/0701115.

[29] I. Shimada and De-Qi Zhang. Dynkin diagrams of rank 20 on supersingular K3 surfaces. Preprint, 2005. http://www.math.sci.hokudai.ac.jp/~shimada/preprints.html.

[30] T. Shioda and H. Inose. On singular K3 surfaces. In *Complex analysis and algebraic geometry*, pages 119–136. Iwanami Shoten, Tokyo, 1977. MR0441982 (56:371)

[31] T. Shioda. The elliptic K3 surfaces with with a maximal singular fibre. *C. R. Math. Acad. Sci. Paris*, 337(7):461–466, 2003. MR2023754 (2005c:14046)

[32] T. Shioda and N. Mitani. Singular abelian surfaces and binary quadratic forms. In *Classification of algebraic varieties and compact complex manifolds*, pages 259–287. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974. MR0392289 (52:3174)

[33] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[34] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994. MR1312368 (96b:11074)
[36] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966. MR 0206004 (34:5829)

[37] A. Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064, Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948. MR 0029522 (10:621d)

Department of Mathematics, Faculty of Science, Hokkaido University, Sapporo 060-0810, Japan

E-mail address: shimada@math.sci.hokudai.ac.jp

Current address: Department of Mathematics, Graduate School of Science, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 Japan

E-mail address: shimada@math.sci.hiroshima-u.ac.jp