<table>
<thead>
<tr>
<th>Title</th>
<th>Instructions for use of normal K3 surfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Shimada, Ichiro</td>
</tr>
<tr>
<td>Citation</td>
<td>The Michigan Mathematical Journal, 55(2): 395-416</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2007</td>
</tr>
<tr>
<td>Doc URL</td>
<td><a href="http://hdl.handle.net/2115/30284">http://hdl.handle.net/2115/30284</a></td>
</tr>
<tr>
<td>Type</td>
<td>article</td>
</tr>
<tr>
<td>File Information</td>
<td>MMJ55-2.pdf</td>
</tr>
</tbody>
</table>
On Normal K3 Surfaces
ICHIRO SHIMADA

1. Introduction

In this paper, by a $K3$ surface we mean, unless otherwise stated, an algebraic $K3$ surface defined over an algebraically closed field.

A $K3$ surface $X$ is said to be supersingular (in the sense of Shioda [23]) if the rank of the Picard lattice $S_X$ of $X$ is 22. Supersingular $K3$ surfaces exist only when the characteristic of the base field is positive. Artin [3] showed that, if $X$ is a supersingular $K3$ surface in characteristic $p > 0$, then the discriminant of $S_X$ can be written as $-p^{2\sigma_X}$, where $\sigma_X$ is an integer with $0 < \sigma_X \leq 10$. This integer $\sigma_X$ is called the Artin invariant of $X$.

Let $\Lambda_0$ be an even unimodular $\mathbb{Z}$-lattice of rank 22 with signature $(3,19)$. By the structure theorem for unimodular $\mathbb{Z}$-lattices (see e.g. [16, Chap. V]), the $\mathbb{Z}$-lattice $\Lambda_0$ is unique up to isomorphisms. If $X$ is a complex $K3$ surface, then $H^2(X, \mathbb{Z})$ regarded as a $\mathbb{Z}$-lattice by the cup product is isomorphic to $\Lambda_0$.

For an odd prime integer $p$ and an integer $\sigma$ with $0 < \sigma \leq 10$, we denote by $\Lambda_{p,\sigma}$ an even $\mathbb{Z}$-lattice of rank 22 with signature $(1,21)$ such that the discriminant group $\text{Hom}(\Lambda_{p,\sigma}, \mathbb{Z})/\Lambda_{p,\sigma}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\otimes 2\sigma}$. Rudakov and Shafarevich [14, Sec. 1, Thm.] showed that the $\mathbb{Z}$-lattice $\Lambda_{p,\sigma}$ is unique up to isomorphisms. If $X$ is a supersingular $K3$ surface in characteristic $p$ with Artin invariant $\sigma$, then $S_X$ is $p$-elementary by [14, Sec. 8, Thm.] and of signature $(1,21)$ by the Hodge index theorem; hence $S_X$ is isomorphic to $\Lambda_{p,\sigma}$.

The primitive closure of a sublattice $M$ of a $\mathbb{Z}$-lattice $L$ is $(M \otimes \mathbb{Z} \mathbb{Q}) \cap L$, where the intersection is taken in $L \otimes \mathbb{Z} \mathbb{Q}$. A sublattice $M \subset L$ is said to be primitive if $(M \otimes \mathbb{Z} \mathbb{Q}) \cap L = M$ holds. For $\mathbb{Z}$-lattices $L$ and $L'$, we consider the following condition.

$\text{Emb}(L, L')$: There exists a primitive embedding of $L$ into $L'$.

We denote by $\mathcal{P}$ the set of prime integers. For a nonzero integer $m$, we denote by $D(m) \subset \mathcal{P}$ the set of prime divisors of $m$. We consider the following arithmetic condition on a nonzero integer $d$, a prime integer $p \in \mathcal{P} \setminus D(2d)$, and a positive integer $\sigma \leq 10$.

$$\text{Arth}(p, \sigma, d): \left(\frac{(-1)^{\sigma+1}d}{p}\right) = -1,$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Received July 19, 2006. Revision received April 17, 2007.
We make the following observations.

(i) Suppose that \( d/d' \in (Q^*)^2 \). Then, for any \( p \in \mathcal{P} \setminus \mathcal{D}(2dd') \) and any \( \sigma \), the conditions Arth\(^1\)(\( p, \sigma, d \)) and Arth\(^2\)(\( p, \sigma, d' \)) are equivalent.

(ii) For fixed \( \sigma \) and \( d \), there exists a subset \( T_{\sigma,d} \) of \((\mathbb{Z}/4d\mathbb{Z})^*\) such that, for \( p \in \mathcal{P} \setminus \mathcal{D}(2d) \), the condition Arth\(^1\)(\( p, \sigma, d \)) is true if and only if \( p \) mod \( 4d \in T_{\sigma,d} \).

The set \( T_{\sigma,d} \) is empty if and only if \((-1)^{r+1}d\) is a square integer. Otherwise, we have \(|T_{\sigma,d}| = |(\mathbb{Z}/4d\mathbb{Z})^*|/2\), and hence the set of \( p \in \mathcal{P} \setminus \mathcal{D}(2d) \) for which Arth\(^1\)(\( p, \sigma, d \)) is true has the natural density \( 1/2 \).

The main result of this paper is as follows.

**Theorem 1.1.** Let \( M \) be an even \( \mathbb{Z} \)-lattice of rank \( r = t_+ + t_- \) with signature \((t_+, t_-)\) and of discriminant \( d_M \). Suppose that \( t_+ \leq 1 \) and \( t_- \leq 19 \). Then, for a prime integer \( p \in \mathcal{P} \setminus \mathcal{D}(2d_M) \) and a positive integer \( \sigma \leq 10 \), the following statements hold.

1. If \( 2\sigma > 22 - r \), then \( \text{Emb}(M, \Lambda_{p,\sigma}) \) is false.
2. If \( 2\sigma < 22 - r \), then \( \text{Emb}(M, \Lambda_{p,\sigma}) \) and \( \text{Emb}(M, \Lambda_0) \) are equivalent.
3. If \( 2\sigma = 22 - r \), then \( \text{Emb}(M, \Lambda_{p,\sigma}) \) is true if and only if both \( \text{Emb}(M, \Lambda_0) \) and Arth\(^1\)(\( p, \sigma, d_M \)) are true.

We shall present a geometric application of Theorem 1.1. A Dynkin type is a finite formal sum of symbols \( A_l \) \((l \geq 1)\), \( D_m \) \((m \geq 4)\), and \( E_n \) \((n = 6, 7, 8)\) with nonnegative integer coefficients. For a Dynkin type

\[
R = \sum a_l A_l + \sum d_m D_m + \sum e_n E_n,
\]

we denote by \( \Sigma_R^+ \) the positive definite root lattice of type \( R \) and define \( \text{rank}(R) \) and \( \text{disc}(R) \) to be the rank and the discriminant of \( \Sigma_R^+ \):

\[
\text{rank}(R) := \sum a_l l + \sum d_m m + \sum e_n n,
\]

\[
\text{disc}(R) := \prod (l + 1)^{a_l} \cdot \prod 4^{d_m} \cdot 3^{e_n} \cdot 2^{r_+}.
\]

A normal \( K3 \) surface is a normal surface whose minimal resolution is a \( K3 \) surface. Artin [1; 2] has shown that a normal \( K3 \) surface has only rational double points as its singularities. We define the **Dynkin type** \( R_Y \) of a normal \( K3 \) surface \( Y \) to be the Dynkin type of the singular points on \( Y \). A normal \( K3 \) surface is said to be supersingular if its minimal resolution is supersingular. The **Artin invariant** \( \sigma_Y \) of a normal supersingular \( K3 \) surface \( Y \) is defined to be the Artin invariant \( \sigma_X \) of the minimal resolution \( X \) of \( Y \). Note that \( \text{rank}(R_Y) \) is equal to the total Milnor number of a normal \( K3 \) surface \( Y \). In particular, we have that \( \text{rank}(R_Y) \leq 21 \) for any \( Y \) and that \( \text{rank}(R_Y) > 19 \) holds only when \( Y \) is supersingular.

Let \( R \) be a Dynkin type, \( p \) a prime integer, and \( \sigma \) a positive integer \( \leq 10 \). We consider the following conditions.

**NK(0, R):** There exists a complex normal \( K3 \) surface \( Y \) with \( R_Y = R \).

**NK(\( p, \sigma, R \)):** There exists a normal supersingular \( K3 \) surface \( Y \) in characteristic \( p \) such that \( \sigma_Y = \sigma \) and \( R_Y = R \).

**NK'(\( p, \sigma, R \)):** Every supersingular \( K3 \) surface \( X \) in characteristic \( p \) with \( \sigma_X = \sigma \) is birational to a normal \( K3 \) surface \( Y \) with \( R_Y = R \).
Theorem 1.3. Let $R$ be a Dynkin type with $r := \text{rank}(R) \leq 19$, and let $\sigma$ be a positive integer $\leq 10$. We put $d_R := (−1)^r \text{disc}(R)$ and let $p$ be an element of $\mathcal{P} \setminus \mathcal{D}(2d_R)$.

1. If $2\sigma > 22 − r$, then $\text{NK}(p, \sigma, R)$ is false.
2. If $2\sigma < 22 − r$, then $\text{NK}(p, \sigma, R)$ and $\text{NK}(0, R)$ are equivalent.
3. If $2\sigma = 22 − r$, then $\text{NK}(p, \sigma, R)$ is true if and only if both $\text{NK}(0, R)$ and $\text{Arth}(p, \sigma, d_R)$ are true.

For each $p \in \mathcal{P}$, a supersingular K3 surface in characteristic $p$ with Artin invariant 1 is unique up to isomorphisms [12; 13]. We denote by $X_p^{(i)}$ the supersingular K3 surface in characteristic $p$ with Artin invariant 1.

Corollary 1.4. The following conditions on a Dynkin type $R$ with $r := \text{rank}(R) \leq 19$ are equivalent. We put $d_R := (−1)^r \text{disc}(R)$.

(i) There exists a complex normal K3 surface $Y$ with $R_Y = R$.
(ii) There exists a prime integer $p \in \mathcal{P} \setminus \mathcal{D}(2d_R)$ such that $X_p^{(i)}$ is birational to a normal K3 surface $Y$ with $R_Y = R$.
(iii) For every $p \in \mathcal{P} \setminus \mathcal{D}(2d_R)$, the supersingular K3 surface $X_p^{(i)}$ is birational to a normal K3 surface $Y$ with $R_Y = R$.

Let $Y$ be a normal supersingular K3 surface in characteristic $p$. It is proved in [18] that, if $\text{rank}(R_Y) = 21$, then $p \in \mathcal{D}(2\text{disc}(R_Y))$ holds. It is proved in [22] that, if $\text{rank}(R_Y) = 20$, then either $\sigma_Y = 1$ or $p \in \mathcal{D}(2\text{disc}(R_Y))$ holds. (In [22], we have also determined all Dynkin types $R$ of rank 20 of rational double points that can appear on normal supersingular K3 surfaces in characteristic $p \notin \mathcal{D}(2\text{disc}(R))$ with the Artin invariant 1.) Therefore, if $\sigma_Y > 1$, then either $\text{rank}(R_Y) \leq 19$ or $p \in \mathcal{D}(2\text{disc}(R_Y))$. Combining this consideration with Theorem 1.3, we obtain restrictions on Dynkin types of normal supersingular K3 surfaces with large Artin invariants.

Corollary 1.5. Let $Y$ be a normal supersingular K3 surface in characteristic $p$ with $\sigma_Y = 10$. Then one of the following statements holds.

(i) $\text{rank}(R_Y) \leq 1$ (i.e., $Y$ is smooth or has only one ordinary node as its singularities);
(ii) $R_Y = A_2$ and $p \mod 24 \in \{5, 11, 17, 23\}$;
(iii) $R_Y = 2A_1$ and $p \mod 8 \in \{3, 7\}$;
(iv) $p \in \mathcal{D}(2\text{disc}(R_Y))$.

Corollary 1.6. Let $Y$ be a normal supersingular K3 surface in characteristic $p$ with $\sigma_Y = 9$. Then one of the following statements holds.

(i) $\text{rank}(R_Y) \leq 3$;
(ii) $R_Y = A_4$ and $p \mod 40 \in \{3, 7, 13, 17, 23, 27, 33, 37\}$;
(iii) $R_Y = A_1 + A_3$ and $p \mod 8 \in \{3, 5\}$;
(iv) $R_Y = 2A_1 + A_2$ and $p \mod 24 \in \{5, 7, 17, 19\}$;
(v) $p \in \mathcal{D}(2\text{disc}(R_Y))$. 
We have determined the Boolean value of $NK_R$, the edges emitting from them. For a Dynkin type $R$, we can be obtained from the Dynkin diagram of $R$ by deleting some vertexes and edges from them. For a Dynkin type $R$, we denote by $S(R)$, we denote by $S(R)$, the set of Dynkin types $R'$ with $R' = R$ or $R' < R$. A $K3$ surface $X$ is birational to a normal $K3$ surface $Y$ with $R_Y = R$ if and only if there exists a configuration of $(-2)$-curves of type $R$ on $X$. Hence, if $R' \in S(R)$, then

\[ NK(0, R) \implies NK(0, R'), \quad NK(p, \sigma, R) \implies NK(p, \sigma, R'). \]

We have determined the Boolean value of $NK(0, R)$ for each Dynkin type $R$ with rank($R$) $\leq 19$, as described in the following theorem.

**Theorem 1.8.** Let $R$ be a Dynkin type of rank $\leq 19$. Then $NK(0, R)$ is true if and only if $S(R)$ does not contain any Dynkin type that appears in Table 1.

**Corollary 1.9.** Let $R$ be a Dynkin type of rank $\leq 14$. Then there exists a complex normal $K3$ surface $Y$ with $R_Y = R$.

Because $p \in D(2 \text{disc}(R))$ with rank($R$) $\leq 21$ implies that $p \leq 19$, Theorems 1.3 and 1.8 (when combined with the results of our previous papers, [18] and [22])

**Table 1** Minimal Dynkin types $R$ for which $NK(0, R)$ is false

<table>
<thead>
<tr>
<th>Rank</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>$A_4 + 11A_1$, $2A_2 + 11A_1$, $A_2 + 13A_1$</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>$3D_4 + 2A_2$, $A_6 + A_2 + 8A_1$, $A_4 + 2A_2 + 8A_1$</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>$E_8 + D_4 + 5A_1$, $E_6 + 2D_4 + 3A_1$, $E_6 + D_4 + A_2 + 5A_1$, $D_7 + 5A_2$, $D_3 + 5A_2 + 2A_1$, $3D_4 + A_4 + A_1$, $2D_4 + A_6 + A_1$, $2D_4 + A_6 + A_1$, $2A_4 + 3A_1$, $D_4 + A_6 + 5A_1$, $D_4 + 2A_2 + 5A_1$, $D_4 + A_3 + 5A_2$, $D_4 + A_3 + 5A_2$, $A_3 + 5A_1$, $A_4 + 5A_2 + 3A_1$, $A_3 + 5A_2 + 4A_1$, $7A_2 + 3A_1$, $5A_2 + 7A_1$, $7A_1$</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>$E_8 + D_4 + 2A_5$, $E_6 + 2D_4 + A_2$, $E_6 + 4A_3$, $D_3 + D_4 + 3A_3$, $D_4 + A_5 + 2A_3$, $D_4 + 2A_4 + 2A_3$, $A_7 + 5A_2 + A_1$, $A_2 + 5A_2$, $A_4 + 7A_2$, $4A_3 + 3A_2$, $4A_3 + A_2 + 4A_1$</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>$E_7 + 3A_2$, $E_7 + 3A_2 + A_1$, $D_8 + A_2$, $D_3 + 3A_1 + A_1$, $D_8 + 2A_3 + A_1$, $D_6 + 2D_3 + A_1$, $D_6 + D_3 + 2A_3 + A_2$, $D_6 + 3A_1 + A_1$, $D_6 + 4A_3 + A_1$, $D_3 + A_3 + A_1$, $D_8 + A_3 + A_1$, $3A_3 + A_3 + 2A_1$, $A_3 + 3A_3 + 2A_2 + A_1$, $3A_4 + 2A_1 + A_1$, $3A_4 + A_3 + A_2 + 2A_1$, $3A_4 + 2A_2 + 3A_1$, $A_4 + 4A_3 + A_2 + A_1$</td>
<td></td>
</tr>
</tbody>
</table>

Observe that, if $p \in D(2 \text{disc}(R))$ with rank($R$) $\leq 21$, then $p \leq 19$. We thus obtain the following corollary.

**Corollary 1.7.** The total Milnor number of a normal supersingular $K3$ surface $Y$ in characteristic $p > 19$ with Artin invariant $\sigma_Y$ is at most $22 - 2\sigma_Y$.
determine all possible configurations of rational double points on normal supersingular $K3$ surfaces in characteristic $p > 19$.

Since $17A_1$ appears in Table 1, we obtain the following result, which was proved by Nikulin [9] for the complex case. See also Section 5.1.

**Corollary 1.10**

(1) **There cannot exist seventeen disjoint $(-2)$-curves on a complex $K3$ surface.**

(2) **There exist seventeen disjoint $(-2)$-curves on a supersingular $K3$ surface only in characteristic 2.**

We remark that, in characteristic 2, there exist twenty-one disjoint $(-2)$-curves on every supersingular $K3$ surface [18; 19].

The proof of Theorems 1.1 and 1.8 is based on the theory of discriminant forms due to Nikulin [10] and the theory of $l$-excess due to Conway and Sloane [6, Chap. 15]. The same method was used in [17] to determine the list of Dynkin types $R_f$ of reducible fibers of complex elliptic $K3$ surfaces $f : X \to \mathbb{P}^1$ with a section and the torsion parts $MW_f$ of their Mordell–Weil groups.

**Remark 1.11.** Lemma 5.2 in [17] is wrong; it should be replaced with (III) and (IV) in Section 3 of this paper. However, in the actual calculation of the list of all the pairs $(R_f, MW_f)$ of complex elliptic $K3$ surfaces $f : X \to \mathbb{P}^1$ with a section, we used the correct version of [17, Lemma 5.2] and so the list presented in [17] is valid. See Remark 4.3.

The plan of this paper is as follows. In Section 2, we prove Proposition 1.2 and deduce Theorem 1.3 from Theorem 1.1. In Section 3, we review the theory of $l$-excess and discriminant forms. In Section 4, we prove Theorems 1.1 and 1.8. We conclude the paper with two remarks in Section 5: we give a simple proof of a theorem of Ogus [12, Thm. 7.10] on supersingular Kummer surfaces; and we investigate, from our point of view, the reduction modulo $p$ of a singular $K3$ surface (in the sense of Shioda and Inose [24]) defined over a number field.

**Conventions 1.12**

(1) Let $D$ be a finite abelian group. The length of $D$, denoted by $\text{leng}(D)$, is the minimal number of generators of $D$.

(2) For $l \in \mathcal{P}$ and $x \in \mathbb{Q}_l^\times$, we denote by $\text{ord}_l(x)$ the largest integer such that $l^{\text{ord}_l(x)}x \in \mathbb{Z}_l$. We put $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

(3) For a divisor $D$ on a $K3$ surface $X$, let $[D] \in S_X$ denote the class of $D$.

2. **Geometric Application**

We prove Proposition 1.2 and deduce Theorem 1.3 from Theorem 1.1.

Let $X$ be a $K3$ surface. A divisor $H$ on $X$ is called a **polarization** if $H$ is nef, $H^2 > 0$, and the complete linear system $|H|$ has no fixed components. If $H$ is a polarization of $X$, then $|H|$ is base-point free by Saint-Donat [15, Cor. 3.2] and
We introduce a notion from lattice theory. Let $L$ be an integer lattice. A vector $v$ in $L$ is called a root if $(v, v) = -2$. We denote by $\text{Roots}(L)$ the set of roots in $L$. A subset $F$ of $\text{Roots}(L)$ is called a fundamental system of roots in $L$ if (a) $F$ is a basis of the sublattice $\langle \text{Roots}(L) \rangle \subset L$ generated by $\text{Roots}(L)$ and (b) each root $v \in \text{Roots}(L)$ is written as a linear combination $v = \sum_{d \in F} k_d d$ of elements $d$ of $F$ whose coefficients $k_d$ are either all nonpositive integers or all nonnegative integers. Let $t : L \to \mathbb{R}$ be a linear form such that $t(d) \neq 0$ for any $d \in \text{Roots}(L)$. We put $(\text{Roots}(L))^+_t := \{ d \in \text{Roots}(L) \mid t(d) > 0 \}$.

hence $|H|$ defines a morphism $\Phi|_H$ from $X$ to a projective space of dimension $N := \dim|H| = H^2/2 + 1$ (see [11, Prop. 0.1]). Let

$$X \to Y|_H \to \mathbb{P}^N$$

be the Stein factorization of $\Phi|_H$. Then $X \to Y|_H$ is the minimal resolution of the normal K3 surface $Y|_H$. Conversely, let $X \to Y$ be the minimal resolution of a normal K3 surface $Y$. Let $H'$ be a hyperplane section of $Y$, and let $H$ be the pullback of $H'$ to $X$. Then $H$ is a polarization of $X$, and $Y$ is isomorphic to $Y|_H$.

**Proposition 2.1.** An element $v$ of $S_X$ is the class of a polarization if and only if $(v, v) > 0$, $v$ is nef, and the set $\{ e \in S_X \mid (v, e) = 1, (e, e) = 0 \}$ is empty.

**Proof.** See Nikulin [11, Prop. 0.1] and the argument in the proof of (4) $\Rightarrow$ (1) in Urabe [25, Prop. 1.7].

We put

$$\Xi_X := \{ v \in S_X \mid (v, v) = -2 \}, \quad \Gamma_X := \{ x \in S_X \otimes_{\mathbb{Z}} \mathbb{R} \mid (x, x) > 0 \}.$$

For $d \in \Xi_X$, we define the wall $d^\perp$ associated with $d$ by

$$d^\perp := \{ x \in S_X \otimes_{\mathbb{Z}} \mathbb{R} \mid (x, d) = 0 \}.$$

Note that the family of walls $d^\perp$ are locally finite in $\Gamma_X$. We denote by

$$\Gamma_X^0 := \{ x \in \Gamma_X \mid (x, d) \neq 0 \text{ for any } d \in \Xi_X \}$$

the complement of these walls in $\Gamma_X$. Let $W_X$ be the subgroup of the orthogonal group $O(S_X)$ of $S_X$ generated by the reflections $x \mapsto x + (x, d)d$ into the walls $d^\perp$ associated with the vectors $d \in \Xi_X$. Then the subgroup of $O(S_X)$ generated by $W_X$ and $\{ \pm 1 \}$ acts on the set of connected components of $\Gamma_X^0$ transitively. Let $A$ denote the connected component of $\Gamma_X^0$ containing the class of a very ample line bundle on $X$. Then a vector $v \in S_X$ is nef if and only if $v$ is contained in the closure of $A$ in $S_X \otimes_{\mathbb{Z}} \mathbb{R}$. Combining these considerations with Proposition 2.1, we obtain the following corollary. See also [14, Sec. 3, Prop. 3].

**Corollary 2.2.** Let $v \in S_X$ be a vector such that $(v, v) > 0$. Then there exists an isometry $\phi \in O(S_X)$ such that $\phi(mv)$ is the class of a polarization of $X$ for any integer $m \geq 2$. We introduce a notion from lattice theory. Let $L$ be a negative definite even $\mathbb{Z}$-lattice. A vector $v \in L$ is called a root if $(v, v) = -2$. We denote by $\text{Roots}(L)$ the set of roots in $L$. A subset $F$ of $\text{Roots}(L)$ is called a fundamental system of roots in $L$ if (a) $F$ is a basis of the sublattice $\langle \text{Roots}(L) \rangle \subset L$ generated by $\text{Roots}(L)$ and (b) each root $v \in \text{Roots}(L)$ is written as a linear combination $v = \sum_{d \in F} k_d d$ of elements $d$ of $F$ whose coefficients $k_d$ are either all nonpositive integers or all nonnegative integers. Let $t : L \to \mathbb{R}$ be a linear form such that $t(d) \neq 0$ for any $d \in \text{Roots}(L)$. We put

$$(\text{Roots}(L))^+_t := \{ d \in \text{Roots}(L) \mid t(d) > 0 \}.$$
An element \( d \in (\text{Roots}(L))^+_\perp \) is said to be decomposable if there exist vectors \( d_1, d_2 \in (\text{Roots}(L))^+_\perp \) such that \( d = d_1 + d_2 \); otherwise, we call \( d \) indecomposable. The following proposition is proved, for example, in Ebeling [7, Prop. 1.4].

**Proposition 2.3.** The set \( F_t \) of indecomposable elements in \( (\text{Roots}(L))^+_\perp \) is a fundamental system of roots in \( L \).

We call \( F_t \) the fundamental system of roots associated with \( t : L \rightarrow \mathbb{R} \).

Let \( H \) be a polarization of a K3 surface \( X \). The orthogonal complement \( \langle [H] \rangle_{\perp} \) of \( \langle [H] \rangle \) in \( SX \) is a negative definite even lattice. We put

\[
\Xi(X, H) := \text{Roots}(\langle [H] \rangle_{\perp}) = \langle [H] \rangle_{\perp} \cap \Xi_X.
\]

We denote by \( F(X, H) \) the set of classes of \((-2\)-curves) that are contracted by the birational morphism \( X \rightarrow Y_{[H]} \). It is obvious that \( F(X, H) \subset \Xi(X, H) \).

**Proposition 2.4.** The set \( F(X, H) \) is equal to the fundamental system of roots \( F_a \) in \( \langle [H] \rangle_{\perp} \) associated with the linear form \( \langle [H] \rangle_{\perp} \rightarrow \mathbb{R} \) given by \( v \mapsto (v, \alpha) \), where \( \alpha \) is a vector in the connected component \( A \) of \( 0_{\Gamma_X} \).

**Proof.** We denote by \( (\Xi(X, H))_a^+ \) the set of \( d \in \Xi(X, H) \) such that \( (d, \alpha) > 0 \). By the Riemann–Roch theorem, an element \( d \in (\Xi(X, H))_a^+ \) is contained in \( (\Xi(X, H))_a^+ \) if and only if \( d \) is effective. Hence \( F(X, H) \subset (\Xi(X, H))_a^+ \). Suppose that \( [E] \in F(X, H) \) were decomposable in \( (\Xi(X, H))_a^+ \), where \( E \) is a \((-2\)-curve) contracted by \( X \rightarrow Y_{[H]} \). Then there would exist \([D_1], [D_2] \in (\Xi(X, H))_a^+ \) with \( D_1 \) and \( D_2 \) being effective such that \( [E] = [D_1] + [D_2] \). Then we would have \( D_1 + D_2 \in [E] \), which is absurd. Therefore, \( [E] \) is indecomposable in \( (\Xi(X, H))_a^+ \) and hence \( F(X, H) \subset F_a \) is proved.

Conversely, let \( [D_1], \ldots, [D_m] \) be the elements of \( F_a \). Because \( F_a \subset (\Xi(X, H))_a^+ \), we can assume that \( D_1, \ldots, D_m \) are effective. We will show that each \( D_i \) is a \((-2\)-curve) contracted by \( X \rightarrow Y_{[H]} \). Let \( D_i = F_j + M_i \) be the decomposition of \( D_i \) into the sum of the fixed part \( F_j \) and the movable part \( M_i \). Since \( H \) is nef and \( D_i H = 0 \), it follows that \( F_j H = 0 \) and \( M_i H = 0 \). In particular, \( [M_i] \) is contained in the negative definite \( \mathbb{Z} \)-lattice \( \langle [H] \rangle_{\perp} \). Therefore, \( M_i \neq 0 \) would imply \( M_i^2 < 0 \), which contradicts the movability of \( M_i \). Hence we have \( D_i = F_j \). Consequently, the integral components \( E_1, \ldots, E_l \) of \( D_i \) are \((-2\)-curves). We have \( D_i = a_1 E_1 + \cdots + a_l E_l \), where \( a_1, \ldots, a_l \) are positive integers. Since \( H \) is nef and \( D_i H = 0 \), it follows that \( E_i H = \cdots = E_l H = 0 \) and hence \( E_1, \ldots, E_l \) are contracted by \( \Phi_{[H]} \). As a result, \( [E_1], \ldots, [E_l] \) are elements of \( F(X, H) \subset F_a \). Thus, for each \( k = 1, \ldots, l \), there exists a \( j_k \) such that \( [E_{j_k}] = [D_{j_k}] \). Then we have \([D_{j_1}] = a_1[D_{j_1}] + \cdots + a_l[D_{j_l}] \). Since \([D_{j_1}], \ldots, [D_{j_l}] \) form a basis of the sublattice \( (\Xi(X, H))_{[H]} \) of \( \langle [H] \rangle_{\perp} \) and since \( a_1, \ldots, a_l \) are positive integers, we must have \( l = 1, a_1 = 1 \), and \( j_1 = i \); that is, \( D_i = E_1 \). Hence \([D_i] \in F(X, H) \) holds and so \( F_a \subset F(X, H) \) is proved.

**Corollary 2.5.** The Dynkin type of the rational double points on \( Y_{[H]} \) is equal to the Dynkin type of \( \text{Roots}(\langle [H] \rangle_{\perp}) \).
Let $L$ be a $\mathbb{Z}$-lattice. We denote by $L^\vee$ the dual lattice $\text{Hom}(L, \mathbb{Z})$ of $L$. Then $L$ is embedded in $L^\vee$ as a submodule of finite index, and there exists a natural $\mathbb{Q}$-valued symmetric bilinear form on $L^\vee$ that extends the $\mathbb{Z}$-valued symmetric bilinear form on $L$. An overlattice of $L$ is a submodule $L'$ of $L^\vee$ containing $L$ such that the $\mathbb{Q}$-valued symmetric bilinear form on $L'$ takes values in $\mathbb{Z}$ on $L$. If $L$ is embedded in a $\mathbb{Z}$-lattice $L''$ of the same rank, then $L''$ is naturally embedded in $L'$ as an overlattice of $L$. Let $L$ be a negative definite even $\mathbb{Z}$-lattice. If $L'$ is an even overlattice of $L$, then Roots$(L') \supseteq$ Roots$(L)$. We put
\[ \mathcal{E}(L) := \{ L' \mid L' \text{ is an even overlattice of } L \text{ such that } \text{Roots}(L') = \text{Roots}(L) \}. \]
For a Dynkin type $R$, we denote by $\Sigma_R^-$ the negative definite root lattice of type $R$.

**Proposition 2.6.** A K3 surface $X$ is birational to a normal K3 surface $Y$ with $R_Y = R$ if and only if there exists an $M \in \mathcal{E}(\Sigma_R^-)$ such that $\text{Emb}(M, S_X)$ is true.

**Proof.** Combining Corollaries 2.2 and 2.5, we see that a K3 surface $X$ is birational to a normal K3 surface $Y$ with $R_Y = R$ if and only if there exists a vector $v \in S_X$ with $(v, v) > 0$ such that Roots$((v)^{-})$ is of type $R$, where $(v)^{-}$ is the orthogonal complement of $(v)$ in $S_X$.

Suppose that such a vector $v \in S_X$ exists. Let $M_0 \subset S_X$ be the sublattice of $S_X$ generated by Roots$((v)^{-})$. Then we have an isometry $\varphi : \Sigma_R^- \to M_0$. Let $M$ be the overlattice of $\Sigma_R^-$ corresponding by $\varphi$ to the primitive closure of $M_0$ in $S_X$. Then $M \in \mathcal{E}(\Sigma_R^-)$ and $\text{Emb}(M, S_X)$ is true.

Conversely, suppose there exists an $M \in \mathcal{E}(\Sigma_R^-)$ that admits a primitive embedding $M \hookrightarrow S_X$. Let $N$ be the orthogonal complement of $M$ in $S_X$. Since $M$ is primitive in $S_X$, the orthogonal complement of $N$ in $S_X$ coincides with $M$. Hence a wall $d^\perp$ associated with $d \in \Sigma_X$ contains $N \otimes \mathbb{Z} \mathbb{R}$ if and only if $d \in \Sigma_X \cap M = \text{Roots}(M) = \text{Roots}(\Sigma_R^-)$. We put
\[ \Gamma_N := \Gamma_X \cap (N \otimes \mathbb{Z} \mathbb{R}), \]
which is a nonempty open subset of $N \otimes \mathbb{Z} \mathbb{R}$. The family of real hyperplanes
\[ \{ d^\perp \cap (N \otimes \mathbb{Z} \mathbb{R}) \mid d \in \Sigma_X \setminus \text{Roots}(\Sigma_R^-) \} \]
in $N \otimes \mathbb{Z} \mathbb{R}$ is locally finite in $\Gamma_N$, and hence there exists $v \in \Gamma_N \cap N$ such that $v \notin d^\perp$ for any $d \in \Sigma_X \setminus \text{Roots}(\Sigma_R^-)$. Then Roots$((v)^{-}) = \text{Roots}(\Sigma_R^-)$. \hfill $\square$

**Proposition 2.7.** The condition NK(0, $R$) is true if and only if there exists an $M \in \mathcal{E}(\Sigma_R^-)$ such that $\text{Emb}(M, \Lambda_0)$ is true.

**Proof.** Suppose there exists a complex normal K3 surface $Y$ with $R_Y = R$. Let $X$ be the minimal resolution of $Y$. Then, by Proposition 2.6, there exists an $M \in \mathcal{E}(\Sigma_R^-)$ such that $\text{Emb}(M, S_X)$ is true. Since $S_X$ is primitive in $H^2(X, \mathbb{Z})$ and since $H^2(X, \mathbb{Z})$ is $\mathbb{Z}$-isometric to $\Lambda_0$, we see that $\text{Emb}(M, \Lambda_0)$ is true.

Conversely, suppose there exists an $M \in \mathcal{E}(\Sigma_R^-)$ that admits a primitive embedding $M \hookrightarrow \Lambda_0$. We choose a vector $h \in \Lambda_0$ such that $(h, h) > 0$ and denote by
S the primitive closure of the sublattice of \( \Lambda_0 \) generated by \( M \) and \( h \). Since \( M \) is primitive in \( \Lambda_0 \), the embedding \( M \hookrightarrow S \) is also primitive. Let \( T \) be the orthogonal complement of \( S \) in \( \Lambda_0 \). We put

\[
\Omega_T := \{ [\omega] \in P_+(T \otimes \mathbb{Z} \mathbb{C}) \mid (\omega, \omega) = 0, (\omega, \bar{\omega}) > 0 \},
\]

where \( [\omega] \subset T \otimes \mathbb{Z} \mathbb{C} \) is the 1-dimensional linear subspace generated by \( \omega \in T \otimes \mathbb{Z} \mathbb{C} \). Then there exists \( [\omega_0] \in \Omega_T \) such that \( \{ v \in T \mid (\omega_0, v) = 0 \} = \{ 0 \} \) and so

\[
\{ v \in \Lambda_0 \mid (\omega_0, v) = 0 \} = S. \tag{2.1}
\]

By the surjectivity of the period mapping for complex analytic \( K3 \) surfaces (see e.g. [4, Chap. VIII]), there exist an analytic \( K3 \) surface \( X \) and an isometry

\[
\phi: H^2(X, \mathbb{Z}) \to \Lambda_0
\]

of \( \mathbb{Z} \)-lattices such that \( \phi \otimes \mathbb{C} \) maps the 1-dimensional subspace \( H^{2,0}(X) \subset H^2(X, \mathbb{C}) \) to \( [\omega_0] \). By (2.1), we have \( \phi(S_X) = S \). Let \( h_X \in S_X \) be the vector such that \( \phi(h_X) = h \). Then \( (h_X, h_X) > 0 \) and hence \( X \) is algebraic. Because \( S \) and \( S_X \) are \( \mathbb{Z} \)-isometric, we see that \( \text{Emb}(M, S_X) \) is true. Thus \( X \) is birational to a normal \( K3 \) surface \( Y \) with \( K_Y = R \) by Proposition 2.6.

**Proof of Proposition 1.2 and Theorem 1.3.** By [14, Sec. 8, Thm.] and [14, Sec. 1, Thm.] (with [14, Sec. 5, Prop.] for the case of characteristic 2), the Picard lattice of a supersingular \( K3 \) surface is determined, up to isomorphisms, by the characteristic of the base field and the Artin invariant. Hence Proposition 1.2 follows from Proposition 2.6.

Note that \( d_R = (-1)^r \text{disc}(R) \) is the discriminant of \( \Sigma_R^{-} \). If \( M \) is an element of \( \mathcal{E}(\Sigma_R^{-}) \) with discriminant \( d_M \) then \( \mathcal{D}(2d_M) \subset \mathcal{D}(2d_R) \) and, for any \( p \in \mathcal{P} \setminus \mathcal{D}(2d_R) \), the conditions \( \text{Arth}(p, \sigma, d_M) \) and \( \text{Arth}(p, \sigma, d_R) \) are equivalent because \( d_R/d_M = |M/\Sigma_R^{-}|^2 \) is a square integer. Hence Theorem 1.3 follows from Propositions 2.6 and 2.7 and Theorem 1.1.

### 3. The Theory of \( l \)-excess and Discriminant Forms

See Cassels [5], Conway and Sloane [6, Chap. 15], and Nikulin [10] for the details of the results reviewed in this section.

Let \( R \) be \( \mathbb{Z}, \mathbb{Q}, \mathbb{Z}_l, \) or \( \mathbb{Q}_l \), where \( l \in \mathcal{P} \cup \{ \infty \} \). An **R-lattice** is a free \( R \)-module \( L \) of finite rank equipped with a nondegenerate symmetric bilinear form

\[
(\cdot, \cdot): L \times L \to R.
\]

We say that \( R \)-lattices \( L \) and \( L' \) are **\( R \)-isometric** and write \( L \cong L' \) if there exists an isomorphism of \( R \)-modules \( L \cong L' \) that preserves the symmetric bilinear form. We sometimes express an \( R \)-lattice \( L \) of rank \( n \) by an \( n \times n \) symmetric matrix with components in \( R \) by choosing a basis of \( L \). For example, for \( a \in R \) with \( a \neq 0 \), we denote by \( [a] \) the \( R \)-lattice of rank 1 generated by a vector \( g \) such that \( (g, g) = a \). For \( R \)-lattices \( L \) and \( L' \), we denote by \( L \oplus L' \) the orthogonal direct sum of \( L \)
and $L'$. For $s \in R \setminus \{0\}$, we denote by $sL$ the $R$-lattice obtained from an $R$-lattice $L$ by multiplying the symmetric bilinear form with $s$. Suppose that an $R$-lattice $L$ is expressed by a symmetric matrix $M$ with respect to a certain basis of $L$. Then

$$\text{disc}(L) := \det(M) \mod (R^\times)^2$$

does not depend on the choice of the basis of $L$. We say that $L$ is \textit{unimodular} if $\text{disc}(L) \in R^\times/(R^\times)^2$.

The following is proved as [5, Chap. 9, Thm. 1.2].

**Theorem 3.1.** Let $n$ be a positive integer and $d$ a nonzero integer. Suppose that, for each $l \in \mathcal{P} \cup \{\infty\}$, we are given a $\mathbb{Z}_l$-lattice $L_l$ of rank $n$ such that $\text{disc}(L_l) = d$ in $\mathbb{Z}_l/(\mathbb{Z}_l^\times)^2$. If there exists a $\mathbb{Q}$-lattice $W$ such that $W \otimes \mathbb{Q} \mathbb{Q}_l$ is $\mathbb{Q}_l$-isometric to $L_l \otimes \mathbb{Q}_l$ for each $l \in \mathcal{P} \cup \{\infty\}$, then there exists a $\mathbb{Z}$-lattice $L$ such that $L \otimes \mathbb{Z} \mathbb{Q}_l$ is $\mathbb{Z}_l$-isometric to $L_l$ for each $l \in \mathcal{P} \cup \{\infty\}$.

Let $L$ be an $R$-lattice, where $R = \mathbb{Z}$ or $\mathbb{Z}_l$ with $l \in \mathcal{P}$, and let $k$ be the quotient field of $R$. We put

$$L^\vee := \text{Hom}_R(L, R).$$

We have a natural embedding $L \hookrightarrow L^\vee$ of $R$-modules as well as a natural $k$-valued symmetric bilinear form on $L^\vee$ that extends the $R$-valued symmetric bilinear form on $L$. We define the \textit{discriminant group} $D_L$ of $L$ by

$$D_L := L^\vee/L.$$

If $L$ is a $\mathbb{Z}$-lattice, then $\text{disc}(L) = (-1)^{r_L} |D_L|$ in $\mathbb{Z}/(\mathbb{Z}^\times)^2 = \mathbb{Z}$.

Suppose that $L$ is a $\mathbb{Z}_l$-lattice. We then have an orthogonal direct sum decomposition,

$$L = \bigoplus_{v \geq 0} l^v L_v, \quad (3.1)$$

where each $L_v$ is a unimodular $\mathbb{Z}_l$-lattice. The decomposition (3.1) is called the \textit{Jordan decomposition} of $L$. The discriminant group $D_L$ of $L$ is then isomorphic to the direct product $\prod_{v \geq 1} (\mathbb{Z}/l^v \mathbb{Z})^{\text{rank}(L_v)}$. In particular, we have

$$|D_L| = l^{\sum_v \text{rank}(L_v)} \quad \text{and} \quad \text{leng}(D_L) = \text{rank}(L) - \text{rank}(L_0).$$

We define the \textit{reduced discriminant} of $L$ by

$$\text{reddisc}(L) := \prod_{v \geq 0} \text{disc}(L_v) = \text{disc}(L)/|D_L| \in \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^2.$$

Suppose that $l \neq 2$. Then we have an orthogonal direct sum decomposition,

$$L \cong \bigoplus l^v [a_v] \quad (a_v \in \mathbb{Z}_l^\times). \quad (3.2)$$

For $a \in \mathbb{Z}_l^\times$, we define

$$l\text{-excess}(l^v [a]) := \begin{cases} (l^v - 1) \mod 8 & \text{if } v \text{ is even or } a \in (\mathbb{Z}_l^\times)^2, \\ (l^v + 3) \mod 8 & \text{if } v \text{ is odd and } a \notin (\mathbb{Z}_l^\times)^2, \end{cases}$$

and define $l\text{-excess}(L) \in \mathbb{Z}/8\mathbb{Z}$ to be the sum of the $l$-excesses of the direct summands in (3.2). It has been proved that $l\text{-excess}(L)$ does not depend on the choice
of the orthogonal direct sum decomposition (3.2). Note that, if $L$ is unimodular, then l-excess($L$) = 0.

Suppose that $l = 2$. Every unimodular $\mathbb{Z}_2$-lattice is $\mathbb{Z}_2$-isometric to an orthogonal direct sum of copies of the following $\mathbb{Z}_2$-lattices:

$$[a] \quad (a \in \mathbb{Z}_2^\times), \quad U := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ or } V := \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}. $$

Hence $L$ has an orthogonal direct sum decomposition,

$$L \cong \bigoplus 2^{\nu_i} [a_i] \oplus \bigoplus 2^{\nu} U \oplus \bigoplus 2^{\nu} V, \quad (3.3)$$

where $a_i \in \mathbb{Z}_2^\times$. We put

$$2\text{-excess}(2^{\nu}[a]) := \begin{cases} (1 - a) \mod 8 & \text{if } \nu \text{ is even or } a \equiv \pm 1 \mod 8, \\ (5 - a) \mod 8 & \text{if } \nu \text{ is odd and } a \equiv \pm 3 \mod 8, \end{cases}$$

$$2\text{-excess}(2^{\nu} U) := 2 \mod 8, \quad 2\text{-excess}(2^{\nu} V) := (4 - (-1)^{\nu} 2) \mod 8$$

and define $2\text{-excess}(L) \in \mathbb{Z}/8\mathbb{Z}$ to be the sum of the 2-excesses of the direct summands in (3.3). It has been proved that 2-excess($L$) does not depend on the choice of the orthogonal direct sum decomposition (3.3). The 2-excess of a unimodular $\mathbb{Z}_2$-lattice need not be 0.

For a proof of the following theorem, see Conway and Sloane [6, Chap. 15, Thm. 8].

**Theorem 3.2.** Let $n$ be a positive integer and $d$ a nonzero integer. Suppose that, for each $l \in \mathcal{P} \cup \{\infty\}$, we are given a $\mathbb{Z}_l$-lattice $L_l$ of rank $n$ such that $\text{disc}(L_l) = d \mod (\mathbb{Z}_l^\times)^2$ in $\mathbb{Z}_l/(\mathbb{Z}_l^\times)^2$.

Then there exists a $\mathbb{Q}$-lattice $W$ such that $W \otimes_{\mathbb{Q}} \mathbb{Q}_l$ is $\mathbb{Q}_l$-isometric to $L_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ for each $l \in \mathcal{P} \cup \{\infty\}$ if and only if

$$s_+ - s_- + \sum_{l \in \mathcal{P}} l\text{-excess}(L_l) \equiv n \mod 8, \quad (3.5)$$

where $(s_+, s_-)$ is the signature of the $\mathbb{R}$-lattice $L_\infty$.

**Remark 3.3.** If $l \notin \mathcal{D}(2d)$ and $l \neq \infty$, then condition (3.4) implies that the $\mathbb{Z}_l$-lattice $L_l$ is unimodular. Hence the summation in (3.5) is in fact finite.

**Definition 3.4.** A finite quadratic form is a finite abelian group $D$ together with a map $q: D \rightarrow \mathbb{Q}/2\mathbb{Z}$ such that: (i) $q(nx) = n^2 q(x)$ for $n \in \mathbb{Z}$ and $x \in D$; and (ii) the map $b: D \times D \rightarrow \mathbb{Q}/2\mathbb{Z}$ defined by $b(x, y) := (q(x + y) - q(x) - q(y))/2$ is bilinear. A finite quadratic form $(D, q)$ is said to be nondegenerate if the symmetric bilinear form $b$ is nondegenerate.

**Remark 3.5.** Let $(D, q)$ be a finite quadratic form. Suppose that $D$ is an $l$-group, where $l \in \mathcal{P}$. Then the image of $q$ is contained in the subgroup

$$(\mathbb{Q}/2\mathbb{Z})_l := \{ t \in \mathbb{Q}/2\mathbb{Z} \mid l't = 0 \text{ for a sufficiently large } v \} = 2\mathbb{Z}[1/l]/2\mathbb{Z}$$

of $\mathbb{Q}/2\mathbb{Z}$. On the other hand, the canonical homomorphism
\[
\mathbb{Q}/2\mathbb{Z} \rightarrow (\mathbb{Q}/2\mathbb{Z}) \otimes \mathbb{Z} Z_l = \mathbb{Q}_l/2\mathbb{Z}_l
\]
induces an isomorphism \((\mathbb{Q}/2\mathbb{Z})_l \cong \mathbb{Q}_l/2\mathbb{Z}_l\). Hence we can consider \(q\) as a map to \(\mathbb{Q}_l/2\mathbb{Z}_l\).

**Definition 3.6.** For a nondegenerate finite quadratic form \((D, q)\) and \(l \in \mathcal{P}\), let
\[
D_l := \{ t \in D \mid l^r t = 0 \text{ for a sufficiently large } v \}
\]
denote the \(l\)-part of \(D\), and let \(q_l\) denote the restriction of \(q\) to \(D_l\). We call \((D, q)_l := (D_l, q_l)\) the \(l\)-part of \((D, q)\). If \(l \notin D(|D|)\), then \((D_l, q_l) = (0, 0)\). We have a decomposition
\[
(D, q) = \bigoplus_{l \in D(|D|)} (D_l, q_l)
\]
that is orthogonal with respect to the symmetric bilinear form \(b\).

Let \(R\) be \(\mathbb{Z}\) or \(\mathbb{Z}_l\) with \(l \in \mathcal{P}\), and let \(k\) be the quotient field of \(R\). An \(R\)-lattice \(L\) is said to be *even* if \((u, v) \in 2R\) holds for every \(v \in L\). Note that, if \(l\) is odd, then any \(\mathbb{Z}_l\)-lattice is even. Note also that (i) a \(\mathbb{Z}\)-lattice \(L\) is even if and only if the \(\mathbb{Z}_2\)-lattice \(L \otimes \mathbb{Z} \mathbb{Z}_2\) is even and (ii) a \(\mathbb{Z}_2\)-lattice \(L\) is even if and only if the component \(L_0\) of the Jordan decomposition \(L = \bigoplus 2^\nu L_\nu\) is \(\mathbb{Z}_2\)-isometric to an orthogonal direct sum of copies of \(U\) and \(V\).

**Definition 3.7.** For an even \(R\)-lattice \(L\), we can define a map
\[
q_L : D_L \rightarrow k/2R
\]
by \(q_L(\tilde{x}) := (x, x) \mod 2R\), where \(x \in L'\) and \(\tilde{x} := x \mod L\). When \(R = \mathbb{Z}_l\), we consider \(q_L\) as a map to \(\mathbb{Q}_l/2\mathbb{Z}_l\) by the isomorphism \(\mathbb{Q}_l/2\mathbb{Z}_l \cong (\mathbb{Q}/2\mathbb{Z})_l \subset \mathbb{Q}/2\mathbb{Z}\) in Remark 3.5. It is easy to see that the finite quadratic form \((D_L, q_L)\) is nondegenerate. We call \((D_L, q_L)\) the *discriminant form of \(L\).*

We have \(\text{leng}(D_L) \leq \text{rank}(L)\). If \(L\) is unimodular, then \((D_L, q_L) = (0, 0)\) holds. If \(b_L(\tilde{x}, \tilde{y}) := (q_L(\tilde{x} + \tilde{y}) - q_L(\tilde{x}) - q_L(\tilde{y}))/2\) is the symmetric bilinear form of \((D_L, q_L)\), then \(b_L(\tilde{x}, \tilde{y}) = (x, y) \mod \mathbb{Z}\). The following proposition is obvious.

**Proposition 3.8.** Let \(L\) be an even \(\mathbb{Z}\)-lattice and \(l\) a prime integer. Then the homomorphism \(D_L \rightarrow D_L \otimes \mathbb{Z}_l\) induced from the natural homomorphism \(L' \rightarrow L' \otimes \mathbb{Z} \mathbb{Z}_l = (L \otimes \mathbb{Z} \mathbb{Z}_l)'^\nu\) yields an isomorphism from the \(l\)-part \((D_L, q_L)_l\) of \((D_L, q_L)\) to \((D_L, q_L)_l\).

Let \((D^{(l)}, q^{(l)})\) be a nondegenerate quadratic form on a finite abelian \(l\)-group \(D^{(l)}\), and let \(n\) be a positive integer. We denote by \(\mathcal{L}^{(l)}(n, D^{(l)}, q^{(l)})\) the set of even \(\mathbb{Z}_l\)-lattices \(L\) of rank \(n\) such that \((D_L, q_L)\) is isomorphic to \((D^{(l)}, q^{(l)})\). We then denote by \(\mathcal{L}^{(l)}(n, D^{(l)}, q^{(l)}) \subset \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}_l^\nu/(\mathbb{Z}_l^\nu)^2\) the image of the map
\[
\mathcal{L}^{(l)}(n, D^{(l)}, q^{(l)}) \rightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}_l^\nu/(\mathbb{Z}_l^\nu)^2,
\]
\[
L \mapsto \varepsilon^{(l)}(L) := [\text{l-excess}(L), \text{reddisc}(L)].
\]
Let \((D, q)\) be a nondegenerate finite quadratic form, and let
\[
\mathcal{L}^{(l)}(n, D, q) := \prod_{l \in D(|D|)} \mathcal{L}^{(l)}(n, D_l, q_l)
\]
be the Cartesian product of the sets \( \mathcal{L}^{(l)}(n, D_l, q_l) \), where \((D_l, q_l)\) is the \( l \)-part of \((D, q)\) and \( l \) runs through the prime divisors of \( 2|D| \). Let \((s_+, s_-)\) be a pair of nonnegative integers such that \( s_+ + s_- = n \). We denote by \( \mathbb{L}^Z((s_+, s_-), D, q) \) the set of even \( \mathbb{Z} \)-lattices \( L \) of rank \( n \) with signature \((s_+, s_-)\) such that \((D_l, q_L)\) is isomorphic to \((D, q)\). By Proposition 3.8, we can define a map

\[
\mathbb{L}^Z((s_+, s_-), D, q) \rightarrow \mathbb{L}^Z(n, D, q),
\]

\[L \mapsto \tau^Z(L) := (\tau^{(l)}(L \otimes_{\mathbb{Z}} \mathbb{Z}_l) \mid l \in \mathcal{D}(2|D|)).\]

**Theorem 3.9.** Put \( d := (-1)^{s_+}|D| \). Then the image of \( \tau^Z \) coincides with the set of elements \((\sigma_l, \rho_l) \mid l \in \mathcal{D}(2d)\) of \( \mathbb{L}^Z(n, D, q) \) that satisfy

(i) \( \rho_l \equiv d/l^{\text{ord}(d)} \mod (\mathbb{Z}_l^x)^2 \) for each \( l \in \mathcal{D}(2d) \) and

(ii) \( s_+ - s_- + \sum_{l \in \mathcal{D}(2d)} \sigma_l \equiv n \mod 8. \)

In particular, the set \( \mathbb{L}^Z((s_+, s_-), D, q) \) is nonempty if and only if there exists an element \((\sigma_l, \rho_l) \mid l \in \mathcal{D}(2|D|)) \in \mathbb{L}^Z(n, D, q) \) that satisfies (i) and (ii).

Let \( l \in \mathcal{P} \) be an odd prime. We choose a nonsquare element \( v_l \in \mathbb{Z}_l^x \) and put \( \bar{v}_l := v_l \mod (\mathbb{Z}_l^x)^2 \), so that \( \mathbb{Z}_l^x/(\mathbb{Z}_l^x)^2 = [1, \bar{v}_l] \). We then define \( \mathbb{Z}_l \)-lattices \( S_n^{(l)} \) and \( N_n^{(l)} \) of rank \( n \) by

\[
S_n^{(l)} := [1] \oplus \cdots \oplus [1] \oplus [1],
\]

\[
N_n^{(l)} := [1] \oplus \cdots \oplus [1] \oplus [v_l].
\]

It is easy to see that \( [v_l] \oplus [v_l] \) is \( \mathbb{Z}_l \)-isometric to \([1] \oplus [1]\). Therefore, if \( T \) is a unimodular \( \mathbb{Z}_l \)-lattice of rank \( n \), then

\[
T \cong \begin{cases} 
S_n^{(l)} & \text{if } \text{disc}(T) = 1, \\
N_n^{(l)} & \text{if } \text{disc}(T) = \bar{v}_l.
\end{cases}
\]

**Proof of Theorem 3.9.** We denote by \((D_l, q_l)\) the \( l \)-part of \((D, q)\). Suppose that \( L \in \mathbb{L}^Z((s_+, s_-), D, q) \). Then \( \text{disc}(L) = d \). Since \( \text{disc}(L \otimes_{\mathbb{Z}} \mathbb{Z}_l) = d \mod (\mathbb{Z}_l^x)^2 \) and \( |D_l \otimes_{\mathbb{Z}} \mathbb{Z}_l| = |D_l| = l^{\text{ord}(d)} \) by Proposition 3.8, it follows that

\[\text{reiddisc}(L \otimes_{\mathbb{Z}} \mathbb{Z}_l) = d/l^{\text{ord}(d)} \mod (\mathbb{Z}_l^x)^2\]

for each \( l \in \mathcal{D}(2d) \). Because \( l\)-excess \((L \otimes_{\mathbb{Z}} \mathbb{Z}_l) = 0 \) for every \( l \notin \mathcal{D}(2d) \), we have

\[s_+ - s_- + \sum_{l \in \mathcal{D}(2d)} l\text{-excess}(L \otimes_{\mathbb{Z}} \mathbb{Z}_l) \equiv n \mod 8\]

by Theorem 3.2. Hence \( \tau^Z(L) \) satisfies (i) and (ii).

Conversely, suppose that \((\sigma_l, \rho_l) \mid l \in \mathcal{D}(2d)\) \in \( \mathbb{L}^Z(n, D, q) \) satisfies (i) and (ii). Then, for each \( l \in \mathcal{D}(2d) \), there is an even \( \mathbb{Z}_l \)-lattice \( L^{(l)} \in \mathbb{L}^{(l)}(n, D_l, q_l) \) such that \( l\)-excess\((L^{(l)}) = \sigma_l \) and \( \text{reiddisc}(L^{(l)}) = \rho_l \). Therefore,

\[\text{disc}(L^{(l)}) = \text{reiddisc}(L^{(l)}) \cdot |D_l| = d \mod (\mathbb{Z}_l^x)^2\]

by condition (i) and \( |D_l| = l^{\text{ord}(d)} \). For \( l \in \mathcal{P} \setminus \mathcal{D}(2d) \), we put

\[
L^{(l)} := \begin{cases} 
S_n^{(l)} & \text{if } d \in (\mathbb{Z}_l^x)^2, \\
N_n^{(l)} & \text{if } d \notin (\mathbb{Z}_l^x)^2.
\end{cases}
\]

Then \( L^{(l)} \in \mathbb{L}^{(l)}(n, D_l, q_l) = \mathbb{L}^{(l)}(n, 0, 0) \) and \( \text{disc}(L^{(l)}) = d \mod (\mathbb{Z}_l^x)^2 \). Let \( L^{(\infty)} \) be an \( \mathbb{R} \)-lattice of rank \( n \) with signature \((s_+, s_-)\); then \( \text{disc}(L^{(\infty)}) = d \mod (\mathbb{R}^x)^2 \).
Then rank \( L^{(l)} \) = 0 for \( l \in \mathcal{P} \setminus \mathcal{P}(2d) \), condition (ii) and Theorem 3.2 imply that there exists a \( \mathbb{Q} \)-lattice \( W \) of rank \( n \) such that \( W \otimes_{\mathbb{Q}} \mathbb{Q}_l \) is \( \mathbb{Q}_l \)-isometric to \( L^{(l)} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \) for any \( l \in \mathcal{P} \cup \{\infty\} \). By Theorem 3.1, there exists a \( \mathbb{Z}_l \)-lattice \( L \) of rank \( n \) such that \( L \otimes_{\mathbb{Z}_l} \mathbb{Z}_l \) is \( \mathbb{Z}_l \)-isometric to \( L^{(l)} \) for any \( l \in \mathcal{P} \cup \{\infty\} \). Looking at the places \( l = 2 \) and \( l = \infty \), we see that \( L \) is even and of signature \( (s_+ , s_- ) \). For each \( l \in \mathcal{P} \), the \( l \)-part of \( (D_l, q_L) \) is isomorphic to \( (D_l^{(l)} , q_L^{(l)} ) \cong (D_l, q_l) \) by Proposition 3.8. Therefore, \( (D_L, q_L) \) is isomorphic to \( (D, q) \).

Fix \( l \in \mathcal{P} \). We now explain how to calculate the set \( \mathcal{L}^{(n)}(D, q) \) for a nondegenerate quadratic form \( (D, q) \) on a finite abelian \( l \)-group \( D \).

**Definition 3.10.** An orthogonal direct sum decomposition
\[
(D, q) = (D', q') \oplus (D'', q'')
\]
is said to be liftable if, for any even \( \mathbb{Z}_l \)-lattice \( L \) with an isomorphism\n\[
\varphi : (D_L, q_L) \simto (D, q),
\]
there exists an orthogonal direct sum decomposition \( L = L' \oplus L'' \) such that rank \( (L') \) is equal to leng \( (D') \) and \( \varphi \) maps \( D_L \subset D_l \) to \( D' \). If this is the case, then \( \varphi \) induces isomorphisms \( (D_L', q_{L'}) \simto (D', q') \) and \( (D_L'', q_{L''}) \simto (D'', q'') \). Hence \( \tau'(L') \in \mathcal{L}^{(l)}(\text{leng}(D'), D', q') \) and \( \tau''(L'') \in \mathcal{L}^{(l)}(n - \text{leng}(D'), D'', q'') \).

For elements \( \tau := [\sigma, \rho] \) and \( \tau' := [\sigma', \rho'] \) of \( \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}^2/2\mathbb{Z}^2 \), we put
\[
\tau * \tau' := [\sigma + \sigma', \rho + \rho'].
\]
The following lemma is obvious from \( \tau^{(l)}(L' \oplus L'') = \tau^{(l)}(L') * \tau^{(l)}(L'') \).

**Lemma 3.11.** If an orthogonal direct sum decomposition \( (D, q) = (D', q') \oplus (D'', q'') \) is liftable, then \( \mathcal{L}^{(l)}(n, D, q) \) is equal to
\[
\{ \tau * \tau' \mid \tau \in \mathcal{L}^{(l)}(\text{leng}(D'), D', q'), \tau' \in \mathcal{L}^{(l)}(n - \text{leng}(D'), D'', q'') \}.
\]

**Lemma 3.12.** The decomposition \( (D, q) = (D, q) \oplus (0, 0) \) is liftable.

**Proof.** Let \( L \) be an even \( \mathbb{Z}_l \)-lattice with an isomorphism \( (D_L, q_L) \simto (D, q) \), and let \( L = \bigoplus_{v \geq 0} l^v L_v \) be the Jordan decomposition of \( L \). We put
\[
L_{\geq 1} := \bigoplus_{v \geq 1} l^v L_v.
\]
Then rank \( (L_{\geq 1}) = \text{leng}(D) \) and \( (D_L, q_L) = (D_{L \geq 1}, q_{L \geq 1}) \). Therefore, the orthogonal direct sum decomposition \( L = L_{\geq 1} \oplus L_0 \) has the required property.

**Lemma 3.13.** An orthogonal direct sum decomposition \( (D, q) = (D', q') \oplus (D'', q'') \), where \( D' \) is cyclic, is liftable.

**Proof.** Let \( l'' \) be the order of \( D' \), and let \( \gamma \) be a generator of \( D' \). Since \( (D, q) \) is nondegenerate, so is \( (D', q') \); hence the order of \( b'(\gamma, \gamma) \) in \( \mathbb{Q} / \mathbb{Z} \) is \( l'' \), where \( b' \) is the symmetric bilinear form of \( (D', q') \). Let \( L \) be an even \( \mathbb{Z}_l \)-lattice with an isomorphism \( \varphi : (D_L, q_L) \simto (D, q) \). We choose an element \( x \in L' \) such that \( \varphi(x) = \gamma \), where \( \bar{x} := x \mod L \), and put \( v := l''x \in L \). Because \( (x, x) \mod \mathbb{Z}_l \) is of order
Then of finite quadratic forms (Diophantine forms on cyclic groups. If \( l \) are elements of \( \mathbb{Z} \) are nondegenerate, the order of \( b(\gamma, \gamma) \) in \( \mathbb{Q}/\mathbb{Z} \) is of even type, if and only if \( l \) is \( \mathbb{Z}_2 \)-isometric to \( 2^a U \) or to \( 2^a V \).

**Lemma 3.16.** Suppose that \( l = 2 \). Then an orthogonal direct sum decomposition \((D, q) = (D_1, q_1) \oplus (D_2, q_2)\), where \((D_1, q_1)\) is of even type, is liftable.

**Proof.** Suppose that \( D' \) is isomorphic to \( \mathbb{Z}/2^a \mathbb{Z} \times \mathbb{Z}/2^a \mathbb{Z} \), and let \( \gamma_1, \gamma_2 \) be elements of \( D' \) of order \( 2^a \) such that \( D' = \langle \gamma_1 \rangle \times \langle \gamma_2 \rangle \). Since \((D', q')\) is of even type, the orders of \( b'(\gamma_1, \gamma_1) \) and \( b'(\gamma_2, \gamma_2) \) in \( \mathbb{Q}/\mathbb{Z} \) are less than \( 2^a \). Since \((D', q')\) is nondegenerate, the order of \( b'(\gamma_1, \gamma_2) \) in \( \mathbb{Q}/\mathbb{Z} \) must be equal to \( 2^a \). Let \( L \) be an even \( \mathbb{Z}_2 \)-lattice with an isomorphism \( \varphi: (D_L, q_L) \rightarrow (D, q) \). We choose vectors \( x_1, x_2 \in L \) such that \( \varphi(x_i) = \gamma_i \) for \( i = 1, 2 \), where \( x_i \mod L \), and put \( v_i := 2^a x_i \in L \). Then there exist \( S, T, U \in \mathbb{Z}_2 \) with \( T \in \mathbb{Z}_2 \) such that

\[
\begin{bmatrix}
(v_1, v_1) & (v_1, v_2) \\
(v_2, v_1) & (v_2, v_2)
\end{bmatrix} = 2^a \begin{bmatrix}
2S & T \\
T & 2U
\end{bmatrix}.
\]

Since \( 4SU - T^2 \in \mathbb{Z}_2 \), it follows that the components \( \xi_1, \xi_2 \) of the vector

\[
\begin{bmatrix}
\xi_1 \\
\xi_2
\end{bmatrix} := \begin{bmatrix}
2S & T \\
T & 2U
\end{bmatrix}^{-1} \begin{bmatrix}
(w, x_1) \\
(w, x_2)
\end{bmatrix}
\]

are elements of \( \mathbb{Z}_2 \) for any \( w \in L \). Moreover, \( w - \xi_1 v_1 - \xi_2 v_2 \) is orthogonal to the sublattice \( \langle v_1, v_2 \rangle \) of \( L \). Thus we obtain an orthogonal direct sum decomposition \( L = \langle v_1, v_2 \rangle \oplus \langle v_1, v_2 \rangle \) that induces \((D, q) = (D_1, q_1) \oplus (D_2, q_2)\) via \( \varphi \).

**Lemma 3.17.** If \( l \) is odd then \((D, q)\) is an orthogonal direct sum of finite quadratic forms on cyclic groups. If \( l = 2 \) then \((D, q)\) is an orthogonal direct sum of finite quadratic forms \((D_i, q_i)\); here, for each \( i \), \( D_i \) is cyclic or \((D_i, q_i)\) is of even type.

**Proof.** We proceed by induction on \( r := \text{len}(D) \). The case where \( r = 1 \) is trivial, so suppose that \( r > 1 \) and that \( D \) is isomorphic to \( \mathbb{Z}/l^{a_1} \mathbb{Z} \times \cdots \times \mathbb{Z}/l^{a_r} \mathbb{Z} \) with \( v_1 \geq \cdots \geq v_r \). If there exists an element \( \gamma \in D \) such that the order of \( b(\gamma, \gamma) \) in \( \mathbb{Q}/\mathbb{Z} \) is \( l^{a_1} \), then \( \langle \gamma \rangle \) is of order \( l^{a_1} \) and we have an orthogonal direct sum decomposition

\[
(D, q) = (\langle \gamma \rangle, q|_{\langle \gamma \rangle}) \oplus (\langle \gamma \rangle^\perp, q|_{\langle \gamma \rangle^\perp})
\]

with \( \text{len}(\langle \gamma \rangle^\perp) = r - 1 \). Suppose that the order of \( b(\gamma, \gamma) \) in \( \mathbb{Q}/\mathbb{Z} \) is strictly smaller than \( l^{a_1} \) for any \( \gamma \in D \). Since \((D, q)\) is nondegenerate, there exist elements \( \gamma_1, \gamma_2 \in D \) such that \( b(\gamma_1, \gamma_2) \in \mathbb{Q}/\mathbb{Z} \) is of order \( l^{a_1} \). If \( l \neq 2 \), then the order...
of \( b(\gamma_1 + \gamma_2, \gamma_1 + \gamma_2) \) in \( \mathbb{Q}/\mathbb{Z} \) would be \( l_{\nu} \); thus we have \( l = 2 \). We put \( D' := \langle \gamma_1 \rangle \times \langle \gamma_2 \rangle \), in which case \( (D', q|_D) \) is nondegenerate. We then put \( D'' := D'/l \), which yields an orthogonal direct sum decomposition

\[
(D, q) = (D', q|_{D'}) \oplus (D'', q|_{D''}),
\]

where \( (D', q|_{D'}) \) is of even type and\( \text{length}(D'') = r - 2 \).

Combining all our results so far, we can calculate the set \( L^{(i)}(n, D, q) \) for a positive integer \( n \) and a nondegenerate quadratic form \( (D, q) \) on a finite abelian \( l \)-group \( D \) from (I)–(IV) as follows.

(I) We have

\[
L^{(i)}(n, D, q) = \emptyset \quad \text{if} \quad n < \text{length}(D).
\]

(II) Recall that \( \mathbb{Z}_l^2/\langle \mathbb{Z}_l^2 \rangle^2 = \{1, \bar{v}_l\} \) for an odd prime \( l \). We also have \( \mathbb{Z}_l^2/\langle \mathbb{Z}_l^2 \rangle^2 = \{1, 3, 5, 7\} \). When \( n > 0 \), we have

\[
L^{(i)}(n, 0, 0) = \begin{cases} 
\{[0, 1], [0, \bar{v}_l]\} & \text{if } l \text{ is odd}, \\
\emptyset & \text{if } l = 2 \text{ and } n \text{ is odd}, \\
\{[n, 1], [n, 5]\} & \text{if } l = 2 \text{ and } n \equiv 0 \mod 4, \\
\{[n, 3], [n, 7]\} & \text{if } l = 2 \text{ and } n \equiv 2 \mod 4.
\end{cases}
\]

(III) Discriminant forms on cyclic groups. Let \( \langle \gamma \rangle \) be a cyclic group of order \( l^\nu > 1 \) generated by \( \gamma \), and let \( q \) be a nondegenerate quadratic form on \( \langle \gamma \rangle \). Because \( q \) is nondegenerate, we can write \( q(\gamma) \in \mathbb{Q}/\mathbb{Z} \) as \( a/l^\nu \mod 2\mathbb{Z} \), where \( a \) is an integer prime to \( l \). Suppose that \( l \) is odd. Then

\[
L^{(i)}(1, \langle \gamma \rangle, q) = \begin{cases} 
\{[l^\nu - 1, 1]\} & \text{if } \lambda_i(a) = 1, \\
\{[l^\nu - 1, \bar{v}_l]\} & \text{if } v \text{ is even and } \lambda_i(a) = -1, \\
\{[l^\nu + 3, \bar{v}_l]\} & \text{if } v \text{ is odd and } \lambda_i(a) = -1,
\end{cases}
\]

where \( \lambda_i : \mathbb{F}_l^\times \to \{\pm 1\} \) is the Legendre symbol. When \( l = 2 \), we have

\[
L^{(2)}(1, \langle \gamma \rangle, q) = \begin{cases} 
\{[1 - a, a]\} & \text{if } v \text{ is even}, \\
\{[1 - a, a]\} & \text{if } v \text{ is odd, } v \geq 2, \text{ and } a \equiv \pm 1 \mod 8, \\
\{[5 - a, a]\} & \text{if } v \text{ is odd, } v \geq 2, \text{ and } a \equiv \pm 3 \mod 8, \\
\{[0, 1], [0, 5]\} & \text{if } v = 1 \text{ and } a \equiv 1 \mod 4, \\
\{[2, 3], [2, 7]\} & \text{if } v = 1 \text{ and } a \equiv 3 \mod 4.
\end{cases}
\]

(IV) Discriminant forms of even type. Suppose that \( l = 2 \). Let \( \langle \gamma_1 \rangle \) and \( \langle \gamma_2 \rangle \) be cyclic groups of order \( 2^\nu \) generated by \( \gamma_1 \) and \( \gamma_2 \), where \( \nu > 0 \), and let \( q \) be a nondegenerate quadratic form on \( \langle \gamma_1 \rangle \times \langle \gamma_2 \rangle \) of even type. Then there exist integers \( u, v, w \) such that

\[
q(\gamma_1) = \frac{2u}{2^\nu} \mod 2\mathbb{Z}, \quad q(\gamma_2) = \frac{2w}{2^\nu} \mod 2\mathbb{Z}, \quad q(\gamma_1, \gamma_2) = \frac{v}{2^\nu} \mod 2\mathbb{Z}.
\]

Since \( q \) is nondegenerate, it follows that the integer \( v \) is odd. Therefore,

\[
L^{(2)}(2, \langle \gamma_1 \rangle \times \langle \gamma_2 \rangle, q) = \begin{cases} 
\{[2, 7]\} & \text{if } uw \text{ is even}, \\
\{[2, 3]\} & \text{if } v \text{ is even and } uw \text{ is odd}, \\
\{[6, 3]\} & \text{if } v \text{ is odd and } uw \text{ is odd}.
\end{cases}
\]
4. Proof of Main Theorems

**Proposition 4.1.** Let \( p \) be an odd prime. Then \( \Lambda_{p, \sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \) is \( \mathbb{Z}_2 \)-isometric to \( U^{\oplus 1} \), and \( \Lambda_{p, \sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_p \) is \( \mathbb{Z}_p \)-isometric to
\[
\begin{align*}
S_{22-2\sigma}^{(p)} \oplus pN_{2\sigma}^{(p)} & \quad \text{if } p \equiv 3 \mod 4 \text{ and } \sigma \equiv 0 \mod 2, \\
N_{22-2\sigma}^{(p)} \oplus pS_{2\sigma}^{(p)} & \quad \text{if } p \equiv 3 \mod 4 \text{ and } \sigma \equiv 1 \mod 2, \\
N_{22-2\sigma}^{(p)} \oplus pN_{2\sigma}^{(p)} & \quad \text{if } p \equiv 1 \mod 4.
\end{align*}
\]

**Proof.** Note that \( \text{disc}(\Lambda_{p, \sigma}) = -p^{2\sigma} \). For simplicity, we put \( \Lambda^{(i)} := \Lambda_{p, \sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_i \). Since \( U \oplus U \) and \( V \oplus V \) are \( \mathbb{Z}_2 \)-isometric, the even unimodular \( \mathbb{Z}_2 \)-lattice \( \Lambda^{(2)} \) is \( \mathbb{Z}_2 \)-isometric to \( U^{\oplus 1} \) or to \( U^{\oplus 1} \oplus V \). Since \( p^{2\sigma} \in (\mathbb{Z}_2^*)^2 \), we have \( \text{disc}(\Lambda^{(2)}) = -1 \) in \( \mathbb{Z}_2/(\mathbb{Z}_2^*)^2 \) and hence \( \Lambda^{(2)} \cong U^{\oplus 1} \). We thus obtain 2-excess(\( \Lambda^{(2)} \)) = 6. Since \( D_{\Lambda_{p, \sigma}} \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2\sigma} \), the \( \mathbb{Z}_p \)-lattice \( \Lambda^{(p)} \) is \( \mathbb{Z}_p \)-isometric to \( X \oplus pY \), where \( X \) is either \( S_{22-2\sigma}^{(p)} \) or \( N_{22-2\sigma}^{(p)} \), and \( Y \) is either \( S_{2\sigma}^{(p)} \) or \( N_{2\sigma}^{(p)} \). Then
\[
p\text{-excess}(\Lambda^{(p)}) = \begin{cases} 
2\sigma(p-1) \mod 8 & \text{if } Y = S_{2\sigma}^{(p)}, \\
2\sigma(p-1) + 4 \mod 8 & \text{if } Y = N_{2\sigma}^{(p)}.
\end{cases}
\]

On the other hand, from the congruence
\[
1 - 21 + 2\text{-excess}(\Lambda^{(2)}) + p\text{-excess}(\Lambda^{(p)}) \equiv 22 \mod 8
\]
in Theorem 3.9, we obtain \( p\text{-excess}(\Lambda^{(p)}) = 4 \). Hence we have
\[
Y = \begin{cases} 
S_{2\sigma}^{(p)} & \text{if } 2\sigma(p-1) \equiv 4 \mod 8, \\
N_{2\sigma}^{(p)} & \text{if } 2\sigma(p-1) \equiv 0 \mod 8.
\end{cases}
\]

From the equality
\[
-1 = \text{redisc}(\Lambda^{(p)}) = \text{disc}(X) \text{ disc}(Y) = \begin{cases} 
1 & \text{if } \text{disc}(X) = \text{disc}(Y), \\
\bar{v}_p & \text{if } \text{disc}(X) \neq \text{disc}(Y)
\end{cases}
\]
in \( \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \), we obtain the required result. \( \square \)

**Proposition 4.2.** Let \( p \) be an odd prime, and let \( (D_{p, \sigma}, q_{p, \sigma}) \) be the discriminant form of \( \Lambda_{p, \sigma} \). Then
\[
\mathcal{L}^{(p)}(n, D_{p, \sigma}, q_{p, \sigma}) = \begin{cases} 
\emptyset & \text{if } n < 2\sigma, \\
\{[4, 1]\} & \text{if } n = 2\sigma \text{ and } \sigma(p-1) \equiv 2 \mod 4, \\
\{[4, \bar{v}_p]\} & \text{if } n = 2\sigma \text{ and } \sigma(p-1) \equiv 0 \mod 4, \\
\{[4, 1], [4, \bar{v}_p]\} & \text{if } n > 2\sigma.
\end{cases}
\]

**Proof.** Let \( (\gamma) \) be a cyclic group of order \( p \) generated by \( \gamma \), and let \( q_1 \) and \( q_\nu \) be the quadratic forms on \( (\gamma) \) with values in \( \mathbb{Q}_p/2\mathbb{Z}_p = \mathbb{Q}_p/\mathbb{Z}_p \) such that \( q_1(\gamma) = 1/p \) mod \( \mathbb{Z}_p \) and \( q_\nu(\gamma) = v_\nu/p \) mod \( \mathbb{Z}_p \), respectively. Let \( \bar{v}_p \in \mathbb{Z} \) be an integer such that \( \bar{v}_p \text{ mod } p = v_\nu \text{ mod } p\mathbb{Z}_p \). As a quadratic form with values in \( \mathbb{Q}/2\mathbb{Z} \), we have \( q_1(\gamma) = (p+1)/p \) mod \( 2\mathbb{Z} \), and
condition \( (s_1) \) and \( (s_2) \) is equivalent to the condition
(See Remark 3.5.) Then \( (\langle y \rangle, q_1) \) is isomorphic to the discriminant form of the \( \mathbb{Z}_p \)-lattice \( p[1] \), and \( (\langle y \rangle, q_2) \) is isomorphic to the discriminant form of the \( \mathbb{Z}_p \)-lattice \( p[v_p] \). By Proposition 4.1, we see that \( (D_{p,\sigma}, q_{p,\sigma}) \) is isomorphic to
\[
\begin{cases}
(\langle y \rangle, q_1) \oplus (\langle y \rangle, q_2) & \text{if } \sigma(p-1) \equiv 2 \mod 4, \\
(\langle y \rangle, q_1) \oplus (\langle y \rangle, q_2) \otimes (\langle y \rangle, q_2) & \text{if } \sigma(p-1) \equiv 0 \mod 4.
\end{cases}
\]
Hence \( \mathcal{L}^{(p)}(n, D_{p,\sigma}, q_{p,\sigma}) = \emptyset \) for \( n < 2\sigma \) by (I), and \( \mathcal{L}^{(p)}(2\sigma, D_{p,\sigma}, q_{p,\sigma}) \) is equal to
\[
\mathcal{L}^{(p)}(n, D_{p,\sigma}, q_{p,\sigma}) = \emptyset \text{ if } n < 2\sigma \quad \text{by (I), and} \quad \mathcal{L}^{(p)}(2\sigma, D_{p,\sigma}, q_{p,\sigma}) \text{ is equal to}
\]
\[
\{ \{ p-1 \} \}^{2\sigma} \quad \text{if } \sigma(p-1) \equiv 2 \mod 4,
\]
\[
\{ \{ p-1 \} \}^{2\sigma} \cup \{ [4, l] \} \quad \text{if } \sigma(p-1) \equiv 0 \mod 4.
\]

by Lemmas 3.11 and 3.13 and (III). If \( n > 2\sigma \), then \( \mathcal{L}^{(p)}(n, D_{p,\sigma}, q_{p,\sigma}) \) is equal to \( \mathcal{L}^{(p)}(2\sigma, D_{p,\sigma}, q_{p,\sigma}) \) and (II). Thus we obtain the required result.

**Proof of Theorem 1.1.** By Nikulin [10, Prop. 1.5.1], the condition \( \text{Emb}(M, \Lambda_0) \) is true if and only if
\[
\mathbb{L}^Z((3 - t_+, 19 - t_-), D_M, -q_M) \neq \emptyset.
\]
Since \( p \notin \mathcal{D}(2d_M) \), the condition \( \text{Emb}(M, \Lambda_{p,\sigma}) \) is true if and only if
\[
\mathbb{L}^Z((1 - t_+, 21 - t_-), D_M \oplus D_{p,\sigma}, -q_M \oplus q_{p,\sigma}) \neq \emptyset.
\]
Observe that
\[
(1)^{3 - t_+ - t_-} |D_M| = -d_M \quad \text{and} \quad (1)^{21 - t_+ - t_-} |D_M \oplus D_{p,\sigma}| = -p^{2\sigma} d_M.
\]
By Theorem 3.9, condition (4.1) is true if and only if there exists
\[
([\sigma, \rho_i] \mid l \in \mathcal{D}(2d_M)) \in \mathcal{L}^Z(22 - r, D_M, -q_M)
\]
satisfying
\[
(c1) \quad \rho_i = -d_M/l^{\text{ord}(d_M)} \mod (\mathbb{Z}_p^x)^2 \quad \text{for each } l \in \mathcal{D}(2d_M), \quad \text{and}
\]
\[
(c2) \quad -16 + t_+ + t_- + \sum_{l \in \mathcal{D}(2d_M)} \sigma_i = 22 - r \mod 8.
\]
condition (4.2) is true if and only if there exist
\[
([\sigma_i, \rho_i]) \in \mathcal{L}^Z(22 - r, D_M, -q_M) \quad \text{and} \quad ([\sigma, \rho_p] \in \mathcal{L}^{(p)}(22 - r, D_{p,\sigma}, q_{p,\sigma})
\]
satisfying
\[
(s1) \quad \rho_i = -p^{2\sigma} d_M/l^{\text{ord}(d_M)} \mod (\mathbb{Z}_p^x)^2 \quad \text{for each } l \in \mathcal{D}(2d_M) \quad \text{and} \quad \rho_p = -d_M \mod (\mathbb{Z}_p^x)^2,
\]
and
\[
(s2) \quad -20 + t_+ + t_- + \sum_{l \in \mathcal{D}(2d_M)} \sigma_i + \sigma_p = 22 - r \mod 8.
\]
Note that, for \( l \in \mathcal{D}(2d_M) \), the condition \( \rho_i = -p^{2\sigma} d_M/l^{\text{ord}(d_M)} \mod (\mathbb{Z}_p^x)^2 \) is equivalent to the condition \( \rho_i = -d_M/l^{\text{ord}(d_M)} \mod (\mathbb{Z}_p^x)^2 \) because \( p^{2\sigma} \in (\mathbb{Z}_p^x)^2 \).
By Proposition 4.2, if \([\sigma, \rho_p] \in \mathcal{L}^{(p)}(22 - r, D_{p,\sigma}, q_{p,\sigma}) \) then \( \sigma_p = 4 \). Hence the condition “(s1) and (s2)” is equivalent to the condition
On Normal K3 Surfaces

413

“(c1) and (c2)” and \([4, -d_M] \in \mathcal{L}(p)(22 - r, D_{p, \sigma}, q_{p, \sigma})\).

By Proposition 4.2, \([4, -d_M] \in \mathcal{L}(p)(22 - r, D_{p, \sigma}, q_{p, \sigma})\) if and only if (i) \(2\sigma < 22 - r\) holds or (ii) \(2\sigma = 22 - r\) and

\[
\begin{aligned}
\sigma(p - 1) &\equiv 2 \mod 4 \text{ and } \lambda_p(-d_M) = 1 \quad \text{or} \\
\sigma(p - 1) &\equiv 0 \mod 4 \text{ and } \lambda_p(-d_M) = -1,
\end{aligned}
\]  

(4.3)

where \(\lambda_p : \mathbb{F}_p^* \to \{\pm 1\}\) is the Legendre symbol. Because (4.3) is equivalent to \(\text{Arth}(p, \sigma, d_M)\), Theorem 1.1 is proved.

\(\square\)

**Proof of Theorem 1.8.** For each Dynkin type \(R\) with \(r := \text{rank}(R) \leq 19\), we perform the following calculation.

1. We denote by \((D_R, q_R)\) the discriminant form of \(\Sigma_R^-\) and by \(\Gamma_R\) the image of the natural homomorphism \(O(\Sigma_R^-) \to O(q_R)\). (See [17, Sec. 6] for a description of the group \(\Gamma_R\).) We then make a list of all isotropic subgroups of \((D_R, q_R)\) up to the action of \(\Gamma_R\). By means of Nikulin [10, Prop. 1.4.1], the list of even overlattices of \(\Sigma_R\) up to the action of \(\Gamma_R\) is obtained. Then, by the method described in [20], we make the list \(\mathcal{E}(\Sigma_R^-)\) up to the action of \(\Gamma_R\).

2. For each \(M \in \mathcal{E}(\Sigma_R^-)\), we use Theorem 3.9 to establish whether or not \(\mathbb{L}_M := \mathbb{L}^2((3, 19 - r), D_M, -q_M)\) is empty. If we find \(M \in \mathcal{E}(\Sigma_R^-)\) such that \(\mathbb{L}_M \neq \emptyset\), then \(\text{NK}(0, R)\) is true; if \(\mathbb{L}_M = \emptyset\) for every \(M \in \mathcal{E}(\Sigma_R^-)\), then \(\text{NK}(0, R)\) is false.

\(\square\)

**Remark 4.3.** Let \(R\) be a Dynkin type with \(r := \text{rank}(R) \leq 18\), and let \(MW\) be a finite abelian group. By [17, Thm. 7.1], the following statements are equivalent.

(i) There exists a complex elliptic \(K3\) surface \(f : X \to \mathbb{P}^1\) with a section such that (a) the Dynkin type \(R_f\) of reducible fibers of \(f\) is equal to \(R\) and (b) the torsion part \(MW_f\) of the Mordell–Weil group of \(f\) is isomorphic to \(MW\).

(ii) There exists an element \(M \in \mathcal{E}(\Sigma_R^-)\) such that

\[
M/\Sigma_R^- \cong MW \quad \text{and} \quad \mathbb{L}^2((2, 18 - r), D_M, -q_M) \neq \emptyset.
\]

Therefore, once we have made the list \(\mathcal{E}(\Sigma_R^-)\) for each Dynkin type \(R\) of rank \(\leq 19\), it is an easy task to verify the list of all possible pairs \((R_f, MW_f)\) given in [17].

**Remark 4.4.** Let \(\langle h \rangle\) denote a \(\mathbb{Z}\)-lattice of rank 1 generated by a vector \(h\) with \(\langle h, h \rangle = 2\). For a Dynkin type \(R\) with \(r := \text{rank}(R) \leq 19\), we denote by \(\mathcal{Y}(R)\) the set of even overlattices \(M\) of \(\Sigma_R^- \oplus \langle h \rangle\) with the following properties:

1. \(\text{Roots}(\langle h \rangle_{\Sigma_R^-}^H) = \text{Roots}(\Sigma_R^-)\), where \(\langle h \rangle_{\Sigma_R^-}^H\) is the orthogonal complement of \(\langle h \rangle\) in \(M\); and

2. \(\{ e \in M \mid \langle h, e \rangle = 1, \langle e, e \rangle = 0 \} = \emptyset\).

By Yang [26], the following statements are equivalent.

(i) There exists a complex reduced plane curve \(C \subset \mathbb{P}^2\) of degree 6 with only simple singularities such that the Dynkin type of \(\text{Sing}(C)\) is equal to \(R\).

(ii) There exists an element \(M \in \mathcal{Y}(R)\) such that \(\mathbb{L}^2((2, 19 - r), D_M, -q_M) \neq \emptyset\). In conjunction with the proof of Theorem 1.8, we also calculated the set \(\mathcal{Y}(R)\) for each \(R\) and confirmed the validity of Yang’s list [26] of configurations of singular points of complex sextic curves with only simple singularities.
5. Concluding Remarks

5.1. Kummer Surfaces

We work over an algebraically closed field of characteristic $p > 0$ with $p \neq 2$. Let $A$ be an abelian surface with $i: A \to A$ the inversion. Then $Y_A := A/(i)$ is a normal $K3$ surface with $R_{Y_A} = 16A_1$. The minimal resolution $Km(A)$ of $Y_A$ is called the Kummer surface. We give a simple proof of the following theorem due to Ogus [12, Thm. 7.10].

**Theorem 5.1.** A supersingular $K3$ surface is a Kummer surface if and only if the Artin invariant is $1$ or $2$.

**Proof.** Since $NK(0,16A_1)$ is true and $Arth(p,3,(-1)^{16}2^{16})$ is false, Theorem 1.3 implies that $NK(p,\sigma,16A_1)$ is true if and only if $\sigma \leq 2$. Thus the “only if” part of Theorem 5.1 is proved. To show the “if” part, it is enough to prove that the minimal resolution of a normal $K3$ surface $Y$ with $R_Y = 16A_1$ is a Kummer surface.

For this purpose we use the following lemma, which can be easily checked with the aid of a computer.

**Lemma 5.2.** Let $C$ be a binary linear code of length $16$ and dimension $\geq 5$ such that the weight $wt(w)$ of every word $w$ satisfies $wt(w) \equiv 0 \mod 4$ and $wt(w) \neq 4$. Then there exists a word of weight $16$ in $C$.

We consider subgroups of the discriminant group $D_{16A_1} \cong \mathbb{F}_2^{16}$ of $\Sigma_{16A_1}$ as binary linear codes of length $16$.

**Lemma 5.3.** If $M \in E(\Sigma_{16A_1})$ satisfies $\text{leng}(DM) \leq 6$, then $M/\Sigma_{16A_1} \subset D_{16A_1}$ contains a word of weight $16$.

**Proof.** Let $C \subset D_{16A_1}$ be a linear code. Then $C$ is isotropic with respect to $q_{16A_1}$ if and only if $wt(w) \equiv 0 \mod 4$ for every $w \in C$. Suppose that $C$ is isotropic. Then the corresponding even overlattice $MC$ of $\Sigma_{16A_1}$ satisfies $\text{Roots}(MC) = \text{Roots}(\Sigma_{16A_1})$ if and only if $wt(w) \neq 4$ for every $w \in C$. Because $\text{leng}(DM_C) = 16 - 2 \dim C$ by Nikulin [10, Prop. 1.4.1], we obtain Lemma 5.3 from Lemma 5.2.

Suppose that $Y$ is a normal $K3$ surface with $R_Y = 16A_1$ and with $X \to Y$ the minimal resolution. We denote by $\Sigma_X$ the sublattice of $S_X$ generated by the classes of the $(-2)$-curves $E_1, \ldots, E_{16}$ contracted by $X \to Y$ and let $M_X$ be the primitive closure of $\Sigma_X$ in $S_X$. Then $M_X \in E(\Sigma_X)$ by Proposition 2.4. Moreover, we have $\text{leng}(DM_X) \leq 6$ because $\text{Emb}(M_X, \Lambda_{p,\sigma})$ is true, where $\sigma = \sigma_X$, and hence $\mathcal{L}^{\sigma}(22 - \text{rank}(M_X), D_{M_X} - q_{M_X}) \neq \emptyset$. By Lemma 5.3, there exists a word of weight $16$ in the code $M_X/\Sigma_X$, so $([E_1] + \cdots + [E_{16}])/2 \in M_X$. Hence there exists a double covering $A' \to X$ whose branch locus is $E_1 \cup \cdots \cup E_{16}$. Then the contraction of $(-1)$-curves on $A'$ yields an abelian surface $A$, and $X$ is isomorphic to the Kummer surface $Km(A)$. (See [12, Lemma 7.12].)
Remark 5.4. In fact, a linear code $C \subset \mathbb{F}_2^{\oplus 16}$ with the properties described in Lemma 5.2 is unique up to isomorphisms. See Nikulin [9] for the description of this code in terms of 4-dimensional affine geometry over $\mathbb{F}_2$.

5.2. Singular K3 Surfaces

A complex K3 surface $X$ is called singular (in the sense of Shioda and Inose [24]) if $S_X$ is of rank 20. Let $X$ be a singular K3 surface and $T_X$ the transcendental lattice of $X$. Then $T_X$ possesses a canonical orientation $\eta_X$ determined by the holomorphic 2-form on $X$. Shioda and Inose [24] showed that the mapping $X \mapsto (T_X, \eta_X)$ induces a bijection from the set of isomorphism classes of singular K3 surfaces to the set of $\text{SL}_2(\mathbb{Z})$-equivalence classes of positive definite even binary forms.

In [24] it is also shown that every singular K3 surface $X$ can be defined over a number field $F$. (See Inose [8] for an explicit defining equation.) For a maximal ideal $p$ of the integer ring $O_F$ of $F$, let $X(p)$ denote the reduction of $X$ at $p$.

Proposition 5.5. Suppose that a singular K3 surface $X$ is defined over a number field $F$. Let $p$ be a maximal ideal of $O_F$ with residue characteristic $p$. Suppose that $p$ is prime to $2\text{disc}(T_X)$ and that $X(p)$ is a supersingular K3 surface. Then the Artin invariant of $X(p)$ is 1, and

$$\left(\frac{-\text{disc}(T_X)}{p}\right) = -1.$$ (5.1)

Proof. Since the signature of $S_X$ is (1, 19), it follows that $\text{disc}(S_X) = -\text{disc}(T_X)$. Let $\sigma$ be the Artin invariant of $X(p)$. The reduction induces an embedding $S_X \hookrightarrow S_X(p)$. Let $M$ be the primitive closure of $S_X$ in $S_X(p)$. Then $\text{Emb}(M, \Lambda_{p,\sigma})$ is true. Since $M$ is of rank 20 and $\text{disc}(S_X)/\text{disc}(M)$ is a square integer, it follows from Theorem 1.1 that $\sigma = 1$ and that $\text{Arth}(p, 1, \text{disc}(S_X))$ is true. We thus obtain (5.1).

Remark 5.6. The converse of Proposition 5.5 is proved in [21].

References

Ichiro Shimada


Department of Mathematics
Faculty of Science
Hokkaido University
Sapporo 060-0810
Japan
shimada@math.sci.hokudai.ac.jp