AUTOMORPHISMS OF ELLIPTIC K3 SURFACES AND SALEM NUMBERS OF MAXIMAL DEGREE

HÉLÈNE ESNAULT, KEIJI OGUISO AND XUN YU

Dedicated to Professor Shing-Tung Yau on the occasion of his sixty-fifth birthday.

Abstract. Using elliptic structures, we show that any supersingular K3 surface of Artin invariant 1 in characteristic $p \neq 5$, 7, 13 has an automorphism the entropy of which is the natural logarithm of a Salem number of degree 22.

1. Introduction

If p is a prime number, there is an Artin invariant 1 supersingular K3 surface $X(p)$, defined over the congruence field $\mathbb{F}_p$. It is unique up to isomorphism (see Section 2). Since Ogus' seminal work [Ogu79], [Ogu83], this surface has been studied from various viewpoints.

In [ES13] it is shown that, as in characteristic 0, in positive characteristic the maximum of the absolute values of the algebraic integers, which are eigenvalues of an automorphism of a smooth projective surface acting on its ℓ-adic cohomology, is taken on the Néron-Severi group. Thus by analogy with complex geometry, one calls entropy the logarithm of this maximum. One knows that the entropy of an automorphism of a K3 surface is either 0 or the logarithm of a Salem number (see Section 3), then of degree at most the rank of the Néron-Severi group, thus at most 20 for projective K3 surfaces in characteristic 0.

Over $k = \bar{\mathbb{F}}_p$, Jang ([Jan14]) showed that the image of the canonical representation

$$\mathrm{Aut}\,(X(p)) \to \mathrm{GL}\,(H^0(X(p), \omega_{X(p)})) \simeq k^\times$$

is isomorphic to the cyclic group of order $p+1$. In particular, for p large, there are automorphims which are not geometrically liftable to characteristic 0. His proof relies on Ogus' Torelli theorem [Ogu83]. From this, and from Shioda's study of Mordell-Weil lattices [Sh90], it is deduced in [EO14] that for p very large, there are automorphisms of $X(p)$ of positive entropy which are not geometrically liftable to characteristic 0 (see 2.3 for the definition of this liftability notion).

The main result of this note is

Theorem 1.1. *Let $p \neq 5$, 7, 13. Then there is an automorphism $f \in \mathrm{Aut}\,(X(p))$, defined over $\bar{\mathbb{F}}_p$, the entropy of which is the logarithm of a Salem number of degree* 22.

Date: November 17, 2014.

The first author is supported by the Einstein program and the ERC Advanced Grant 226257. The second author is supported by JSPS Grant-in-Aid (S) No 25220701, JSPS Grant-in-Aid (S) No 22224001, JSPS Grant-in-Aid (B) No 22340009, and by KIAS Scholar Program.

In particular, those automorphisms are not geometrically liftable to characteristic 0. The result is known over $k = \bar{\mathbb{F}}_p$ for $p = 2$ ([BC13]) and $p = 3$ ([EO14]).

While for $p = 2$ the proof relies on the very detailed study of $X(2)$ in [DK02], and for $p = 3$, it is computer aided and relies on the explicit study of $\mathrm{Aut}(X(3))$ in [KS12], our proof of Theorem 1.1 is abstract and based on the theory of the Mordell-Weil groups of $X(p)$ by Shioda [Sh13]. We show the following strengthening of Theorem 1.1:

Theorem 1.2. *Let k be an algebraically closed field of characteristic $p \geq 0$. Let X be a K3 surface over k of Picard number $\rho = 2d \geq 4$. Assume that X has two non-isomorphic elliptic fibrations $\varphi_1 : X \to \mathbb{P}^1$ ($i = 1, 2$), such that the Mordell-Weil group $\mathrm{MW}(\varphi_1)$ of φ_1 is of maximal rank, that is $2d - 2$, and $\mathrm{MW}(\varphi_2)$ is of positive rank. Then X has an automorphism f, the entropy of which is the logarithm of a Salem number of degree $2d$.*

One deduces Theorem 1.1 from Theorem 1.2 using Shioda's theorem [Sh13]:

Theorem 1.3. *Let $p = 11$ or $p > 13$. Then $X(p)$ admits an elliptic fibration of Mordell-Weil rank $20 = 22 - 2$.*

This also explains the restriction on p in Theorem 1.1. One may think that this restriction should not appear in Theorem 1.1. More generally, it is likely that Theorem 1.2, Theorem 4.1 (mimicing [BC13]) and Theorem 4.6 could have a larger range of applications.

We do not address in this note some questions of more arithmetic flavor. We know that the Néron-Severi group of $X(p)$ is defined over $\mathbb{F}_{p^2}$ ([Sch12]). Over which field are those automorphisms of Theorem 1.1 defined? This depends on the field of definition of the Mordell-Weil groups in Theorem 1.3. Further we know that Salem numbers of bounded degree are discrete. This raises the question whether or not the minimal Salem number of degree 22 arises as the logarithm of the entropy of an automorphism on a supersingular K3 surface (see [Mc11] and references there). We also know that powers of Salem numbers are Salem numbers. Given a Salem number of degree 22 which is the power of another Salem number of degree 22, and such that its logarithm is the entropy of an automorphism f on a supersingular K3 surface, when is f itself the power of an automorphism? Finally it would be interesting to relate this work to [GMc02], [Mc02] in which the authors show that any unramified degree 22 Salem number is the logarithm of the entropy of an automorphism of a non-projective complex K3 surface.

Acknowledgement.

We thank S. Cantat, B. Gross, and C. T. McMullen for discussions. The first author thanks the department of mathematics of Harvard University for hospitality, the third author thanks T. Hibi for financial support during his stay at Osaka University.

2. Preliminaries on K3 surfaces and liftings

In this section, we fix notations and recall basic facts on K3 surfaces and liftings from [EO14] and references therein.

2.1. **K3 surfaces.** Let X be a K3 surface defined over an algebraically closed field k of characteristic $p \geq 0$, that is, X is a smooth projective surface defined over k such that $H^1(X, \mathcal{O}_X) = 0$ and the dualizing sheaf is trivial : $\omega_X \simeq \mathcal{O}_X$. We denote by $\mathrm{NS}(X)$ the Néron-Severi group of X. Then the Picard group $\mathrm{Pic}\,(X)$ is isomorphic to Néron-Severi group $\mathrm{NS}\,(X)$, which is a free $\mathbb{Z}$-module of finite rank. The rank of $\mathrm{NS}\,(X)$ is called the Picard number of X and is denoted by $\rho(X)$. It is at least 1, as X is assumed to be projective, and at most 22, the second ℓ-adic Betti number. In characteristic 0, it is at most 20 by Hodge theory. The intersection form $(*, **)$ on $\mathrm{NS}\,(X)$ is of signature $(1, \rho(X) - 1)$ and $(\mathrm{NS}\,(X), (*, **))$ is then an even hyperbolic lattice. The dual $\mathbb{Z}$-module $\mathrm{NS}\,(X)^* := \mathrm{Hom}_{\mathbb{Z}}(\mathrm{NS}\,(X), \mathbb{Z})$ is regarded as a $\mathbb{Z}$-submodule of $\mathrm{NS}\,(X) \otimes \mathbb{Q}$, containing $\mathrm{NS}\,(X)$ through the intersection form $(*, **)$ which is non-degenerate. The quotient module $\mathrm{NS}\,(X)^*/\mathrm{NS}\,(X)$ is called the discriminant group of X.

The surface X is called supersingular if $\rho(X) = 22$, the maximum possible value. (As the Tate conjecture is not yet proven for $p = 2$, one should rather say Shioda-supersingular in this case, but we consider only supersingular K3 surfaces in odd characteristic in this note).

Artin [Ar74] proved that the discriminant group $\mathrm{NS}\,(X)^*/\mathrm{NS}(X)$ of a supersingular K3 surface X is p-elementary, more precisely, as an abelian group

$$\mathrm{NS}\,(X)^*/\mathrm{NS}\,(X) \simeq (\mathbb{Z}/p)^{2\sigma(X)}$$

where $\sigma(X)$ is an integer such that $1 \leq \sigma(X) \leq 10$. The integer $\sigma(X)$ is called the Artin invariant of X. Let σ be an integer such that $1 \leq \sigma \leq 10$. Then the supersingular K3 surfaces over k with $\sigma(X) \leq \sigma$ form a $(\sigma - 1)$-dimensional family over k. There is, up to isomorphism, a unique Artin invariant 1 supersingular K3 surface $X(p)$ in each positive characteristic $p > 0$. It is defined over $\mathbb{F}_p$ and its Néron-Severi group is defined over $\mathbb{F}_{p^2}$, not over $\mathbb{F}_p$ ([Ogu79], [Sch12]). In many senses, $X(p)$ are the most special K3 surfaces. The uniqueness of $X(p)$ in particular shows that $X(p) \simeq \mathrm{Km}\,(E \times_{\mathbb{F}_p} E)$ for any supersingular elliptic curve E over $\mathbb{F}_p$ ([Ogu79], [Sh75]).

2.2. **Lifting of K3 surfaces.** Let X be a K3 surface defined over an algebraically closed field k of positive characteristic $p > 0$, and R be a discrete valuation ring with residue field k and field of fractions $K = \mathrm{Frac}\,(R)$ of characteristic 0. We call a proper flat (thus smooth) morphism of schemes $X_R \to \mathrm{Spec}\, R$, which restricts to $X \to \mathrm{Spec}(k)$, a characteristic 0 model of X/k. The generic fiber $X_K = X_R \otimes_R K$ is a K3 surface. For any field L containing K, the K3 surface $X_L = X_K \otimes_K L$ is called a lift of X over L. Characteristic 0 lifts of X are lifts over some L as above. They are unobstructed ([Del81]).

2.3. **Geometric lift of an automorphism of a K3 surface.** (See [EO14, Section 2.4]). Let X be a K3 surface defined over a perfect field k of positive characteristic $p > 0$ and $X_R \to \mathrm{Spec}\, R$ be a characteristic 0 model. Recall ([SGA6, X, App.]) that one has a *specialization homomorphism* $sp : \mathrm{Pic}(X_{\bar{K}}) \to \mathrm{Pic}(X)$ *on the Picard group*, which is defined by spreading out and restriction. It is injective as recognized in ℓ-adic cohomology, on which the specializaion is an isomorphism ([SGA4.5, V, Thm. 3.1]).

One has a *restriction homomorphism* $\mathrm{Aut}(X_R/R) \to \mathrm{Aut}(X)$. One defines the subgroup $\mathrm{Aut}^e(X_{\bar{K}}/\bar{K}) \subset \mathrm{Aut}(X_{\bar{K}}/\bar{K})$ consisting of those automorphisms which lift to some model $X_R \to \mathrm{Spec}\ R$. (Here e stands for extendable). The group law is defined by base change and the composition of automorphisms. Then the restriction homomorphism yields a *specialization homomorphism* $\iota : \mathrm{Aut}^e(X_{\bar{K}}/\bar{K}) \to \mathrm{Aut}(X/k)$. Moreover, *sp* is equivariant under ι. In addition, as automorphisms are recognized on the associated formal scheme, and $H^0(X, T_{X/k}) = 0$, the specialization homomorphism ι is injective (see [LM11, Lem. 2.3]) .

An automorphism f in $\mathrm{Aut}(X)$ is *geometrically liftable to characteristic* 0 if it is in the image of the specialization homomorphism ι for some model X_R/R.

Theorem 2.1. *(See* [EO14, Proof of Thm.6.4]*) Let X be a supersingular K3 surface and $f \in \mathrm{Aut}\,(X)$. Assume that the characteristic polynomial $f^*|\mathrm{NS}\,(X)$ is irreducible in $\mathbb{Z}[t]$. Then f is never geometrically liftable to characteristic zero.*

Proof. If f lifted geometrically to characteristic 0, say to $g \in \mathrm{Aut}\,(X_{\bar{K}})$ under $X_R \to \mathrm{Spec}\, R$, then, as explained above, the specialization map $\iota : \mathrm{NS}(X_{\bar{K}}) \hookrightarrow \mathrm{NS}(X)$ would be equivariant with respect to g^* and f^*. In particular, the minimal monic polynomial $m_g(t) \in \mathbb{Z}[t]$ of $g^*|\mathrm{NS}(X_{\bar{K}})$, which has degree ≤ 20, would divide the minimal monic polynomial $m_f(t) \in \mathbb{Z}[t]$ of $f^*|\mathrm{NS}(X)$ in $\mathbb{Z}[t]$, which is irreducible and of degree 22 by assumption, a contradiction.

□

3. Preliminaries on Salem numbers and entropy

In this section, we recall the definition of entropy and Salem numbers, again from [EO14] and the references therein.

In what follows, $L = (\mathbb{Z}^{1+t}, (*, **))$ is a hyperbolic lattice, i.e., a pair consisting of a free $\mathbb{Z}$-module of rank $1 + t$ and a $\mathbb{Z}$-valued symmetric bilinear form $(\ ,\ )$ of $\mathbb{Z}^{1+t}$ of signature $(1, t)$ with $t > 0$. For any ring K, one denotes the scalar extension of L to K by L_K.

We denote by $\mathrm{O}(L)$ the orthogonal group of the quadratic lattice L. It is an algebraic group defined over $\mathbb{Z}$. The determinant

$$\det : \mathrm{O}(L) \to \{\pm 1\}$$

is a surjective homomorphism of algebraic groups. Its kernel $\mathrm{SO}(L) \subset \mathrm{O}(L)$ is a closed index 2 algebraic subgroup, and is the identity component of $\mathrm{O}(L)$. As an algebraic group, $\mathrm{SO}(L)$ is geometrically connected. Moreover, $\mathrm{SO}(L)(\mathbb{R})$ is a connected real Lie group, has index 2 in the real Lie group $\mathrm{O}(L)(\mathbb{R})$, thus is its identity component in the real topology.

The subset

$$P := \{x \in L_{\mathbb{R}} |\ (x^2) > 0\} \subset L_{\mathbb{R}}$$

consists of two connected components $\pm C$ in the real topology. By continuity, for $g \in \mathrm{O}(L)(\mathbb{R})$, one has $g(C) = C$ or $g(C) = -C$, where the second case occurs. Thus

$$\mathrm{O}^+(L_{\mathbb{R}}) := \{g \in \mathrm{O}(L)(\mathbb{R})|\ g(C) = C\}$$

is an index 2 closed subgroup of the real Lie group $\mathrm{O}(L)(\mathbb{R})$. Thus $\mathrm{O}^+(L_{\mathbb{R}})$ is a real Lie subgroup of $\mathrm{O}(L)(\mathbb{R})$, which is not the subgroup of $\mathbb{R}$-points of an algebraic subgroup of $\mathrm{O}(L)$.

One defines

$$\mathrm{O}^+(L) := \mathrm{O}(L)(\mathbb{Z}) \cap \mathrm{O}^+(L_{\mathbb{R}})\ ,$$
$$\mathrm{SO}^+(L) := \mathrm{O}(L)(\mathbb{Z}) \cap \mathrm{O}^+(L_{\mathbb{R}}) \cap \mathrm{SO}(L)(\mathbb{R})\ .$$

The groups $\mathrm{O}^+(L)$ and $\mathrm{SO}^+(L)$ are abstract subgroups of $\mathrm{O}(L)(\mathbb{Z})$ of index at most 4.

For application for K3 surfaces, we take L to be the Néron-Severi lattice $\mathrm{NS}\,(X)$ and C to be the connected component of P containing the ample cone. Thus $\mathrm{Aut}\,(X)^*$, the representation of $\mathrm{Aut}\,(X)$ on $\mathrm{NS}\,(X)$, lies in $\mathrm{O}^+(\mathrm{NS}(X))$. Moreover,

$$\mathrm{Aut}\,(X)^{*0} := \mathrm{Aut}\,(X)^* \cap \mathrm{SO}^+(\mathrm{NS}\,(X))$$

is a subgroup of $\mathrm{Aut}^*(X)$ of index at most 2.

We call a polynomial $P(x) \in \mathbb{Z}[x]$ a *Salem polynomial* if it is irreducible, monic, of even degree $2d \geq 2$ and the complex zeroes of $P(x)$ are of the form $(1 \leq i \leq d-1)$:

$$a > 1\ ,\ 0 < a < 1\ ,\ \alpha_i, \overline{\alpha}_i \in S^1 := \{z \in \mathbb{C} \,|\, |z| = 1\} \setminus \{\pm 1\}\ .$$

Proposition 3.1. *Let $f \in \mathrm{O}^+(L)$. Then, the characteristic polynomial of f is the product of cyclotomic polynomials and at most one Salem polynomial counted with multiplicities.*

Proof. As mentioned in [EO14, Prop. 3.1], this is well-known. See [Mc02], [Og10]. □

Definition 3.2.
i) For f as in Proposition 3.1, we define the entropy $h(f)$ of f by

$$h(f) = \log(r(f)) \geq 0\ ,$$

where $r(f)$ is the spectral radius of f, that is the maximum of the absolute values of the complex eigenvalues of f acting on L.

ii) For a smooth projective surface S and an automorphism f on it, one defines the entropy $h(f)$ by

$$h(f) = \log r(f^*|\mathrm{NS}\,(S))$$

where f^* is the action on $\mathrm{NS}(S)$ induced by f.

This definition is consistent to the topological entropy of automorphisms of smooth complex projective surfaces ([ES13]).

4. Two observations from group theory

In this section, we shall prove Theorem 4.1, relying on [BH04] and [BC13], and Theorem 4.6, relying on [Og09]. They are crucial for our main theorems 1.2 and 1.1.

Theorem 4.1. *Let L be a hyperbolic lattice of even rank $2d$ and $G \subset \mathrm{SO}^+(L)$ be a subgroup. Assume that G has no G-stable $\mathbb{R}$-linear subspace of $L_{\mathbb{R}}$ other than $\{0\}$ and $L_{\mathbb{R}}$. Then there is an element $g \in G$, the characteristic polynomial of which is a Salem polynomial of degree $2d$.*

The proof below mimics [BC13, p. 15], where the authors handle the case of $L = \mathrm{NS}(X(2))$, and deduces the statement from [BH04, Prop. 1]. We slightly clarify their argument to make it fit with Theorem 4.1.

Proof. Recall [BH04, Prop. 1], in which the hyperbolicity is essential but neither the evenness of the rank L nor $G \subset \mathrm{SO}^+(L)$ are necessary assumptions:

Theorem 4.2. *Let $G \subset \mathrm{O}(L)(\mathbb{R})$ be an abstract subgroup. Assume that G has no G-stable $\mathbb{R}$-linear subspace of $L_{\mathbb{R}}$ other than $\{0\}$ and $L_{\mathbb{R}}$. Then the Zariski closure of G in $\mathrm{O}(L_{\mathbb{R}})$ contains $\mathrm{SO}(L_{\mathbb{R}})$. In particular, if in addition $G \subset \mathrm{SO}(L)(\mathbb{R})$, then its Zariksi closure in $\mathrm{SO}(L_{\mathbb{R}})$ is $\mathrm{SO}(L_{\mathbb{R}})$.*

As is well known, if L is any non-degenerate quadratic lattice, and $g \in \mathrm{SO}(L)(\mathbb{Z})$, then if the rank of L is odd, 1 is an eigenvalue of g. Indeed, if Q, M are the matrices of the form and g in a chosen basis, then ${}^tMQ(M-\mathrm{Id}) = (\mathrm{Id}-{}^tM)Q$ thus $\det(M-\mathrm{Id}) = -\det(M-\mathrm{Id}) \in \mathbb{Z}$. We use now that, in Theorem 4.1, L is of even rank:

Proposition 4.3. *There is an element $g \in \mathrm{SO}(L)(\mathbb{R})$ such that no eigenvalue of g is a root of unity.*

Proof. We may choose a real basis

$$\langle v_1, v_2, v_3, \cdots, v_{2d}\rangle$$

of $L_{\mathbb{R}}$ under which the bilinear form $(*, **)$ is represented by the matrix $Q := (1, -1, -1, \cdots, -1)$. We identify $\mathbb{R}$-linear maps and $2d \times 2d$-matrices with real entries via this basis. Consider the $\mathbb{R}$-linear map of $L_{\mathbb{R}}$ given by the matrix

$$M = P \oplus R_2 \oplus \cdots \oplus R_d$$

where

$$P = \begin{pmatrix} \sqrt{2} & 1 \\ 1 & \sqrt{2} \end{pmatrix} , \ R_i = \begin{pmatrix} \cos 2\pi\sqrt{2} & -\sin 2\pi\sqrt{2} \\ \sin 2\pi\sqrt{2} & \cos 2\pi\sqrt{2} \end{pmatrix} ,$$

for all $2 \le i \le d$. Then ${}^tMQM = Q$, $\det M = 1$ and the complex eigenvalues of M are

$$\sqrt{2} \pm 1 \ , \ e^{\pm 2\pi\sqrt{-1}\cdot\sqrt{2}} = \cos(2\pi\sqrt{2}) \pm \sqrt{-1}\sin(2\pi\sqrt{2}) \ .$$

Note that $e^{\pm 2\pi\sqrt{-1}\cdot s}$ $(s \in \mathbb{R})$ is a root of unity if and only if s is rational. Since $\sqrt{2}$ is an irrational real number, it follows that no eigenvalue of M is root of unity. Thus M satisfies all the requirements. □

Now assume that $G \subset \mathrm{SO}^+(L)$. The argument now closely follows [BC13, p. 15].

Lemma 4.4. *There are finitely many cyclotomic polynomials of degree $\le 2d$.*

Proof. This is because the number of complex numbers with $x^{(2d)!} = 1$ is at most $(2d)!$. □

Let $P_{2d} \subset \mathbb{Z}[t]$ be the set of monic polynomials of degree $2d$. Then P_{2d} is identified with the affine variety $\mathbb{A}^{2d}$ defined over $\mathbb{Z}$. The map

$$\mathrm{char} : \mathrm{SO}(L) \to P_{2d} \ , \ h \mapsto \Phi_h(t) := \det(tI_{2d} - h)$$

is a morphism of affine varieties. Let

$$u_1(t) = t-1, u_2(t) := t+1, \cdots, u_N(t)$$

be the cyclotomic polynomials in $\mathbb{Z}[t]$ of degree $\le 2d$, where N is the cardinarity of the cyclotomic polynomials of degree $\le 2d$ (Lemma 4.4). The subsets

$$P_i := \{p(t) \in P_{2d}(\mathbb{C}) \mid u_i(t)|p(t)\}$$

define proper closed algebraic subvarieties of $P_{2d} \otimes_{\mathbb{Z}} \mathbb{Q}$, thus so does their finite union

$$Q_{2d} := \cup_{i=1}^N P_i \subset P_{2d} \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

Let $g \in G$. Its characteristic polynomial $\Phi_g(t) \in \mathbb{Z}[t]$ is monic and of degree $2d$. By Proposition 3.1, $\Phi_g(t)$ is the product of cyclotomic polynomials and of at most one Salem polynomial counted with multiplicities. Thus, $\Phi_g(t)$ is a Salem polynomial of degree $2d$ if and only if $\Phi_g(t)$ is irreducible and is not a cyclotomic polynomial of degree $2d$, which is equivalent to saying that no $u_i(t)$ divides $\Phi_g(t)$ in $\mathbb{Z}[t]$. Since $\Phi_g(t)$ and $u_i(t)$ are monic polynomials in $\mathbb{Z}[t]$, it follows that no $u_i(t)$ divides $\Phi_g(t)$ in $\mathbb{Z}[t]$ if and only if no $u_i(t)$ divides $\Phi_g(t)$ in $\mathbb{C}[t]$. The last condition is, by definition, equivalent to $\Phi_g(t) \in P_{2d}(\mathbb{C}) \setminus Q_{2d}$. The following lemma completes the proof:

Lemma 4.5. *There is an element $g \in G$ such that $\Phi_g(t) \in P_{2d}(\mathbb{C}) \setminus Q_{2d}$.*

Proof. By our assumption, we can apply Theorem 4.2 to G, so the Zariski closure of G in $\mathrm{SO}(L_\mathbb{R})$ is $\mathrm{SO}(L_\mathbb{R})$. On the other hand, $\mathrm{char}^{-1}(P_{2d} \otimes_\mathbb{Z} \mathbb{Q} \backslash Q_{2d})$ is Zariski open in $\mathrm{SO}(L) \otimes_\mathbb{Z} \mathbb{Q}$, and not empty by Proposition 4.3. Thus it intersects $G \subset SO(L)(\mathbb{Q})$ non-trivially. This finishes the proof. □

This completes the proof of Theorem 4.1.

□

The following theorem is deduced from [Og09, Proof of Lem 3.6, Claim 3.8].

Theorem 4.6. *Let L be a hyperbolic lattice of signature $(1, r+1)$ with $r \geq 0$ and let $e \in L$ be a primitive element such that $(e, e) = 0$. Let $G \subset \mathrm{SO}(L)(\mathbb{Z})$ be a subgroup such that $G \simeq \mathbb{Z}^r$ as a group and such that $g(e) = e$ for all $g \in G$. Then any G-stable $\mathbb{R}$-linear subspace M of $L_\mathbb{R}$ is contained in the hypersurface $e^\perp$ in $L_\mathbb{R}$, or $M = L_\mathbb{R}$.*

Proof. Note that $G \subset \mathrm{SO}^+(L)$. Indeed, for $g \in G$, $g(e) = e$. Any small enough open ball in $L_\mathbb{R}$ in the classical topology, centered in e, meets C in an open $\mathcal{U}$, such that for any $x \in \mathcal{U}$, the distance between $g(x)$ and x is small enough so it forces $g(x)$ to lie in C.

Lemma 4.7. *There are an integral basis*

$$\langle e, w_1, \cdots, w_r \rangle$$

of $e^\perp \subset L$, so necessarily $(w_j, w_j) < 0$ for all $1 \leq j \leq r$, a $\mathbb{Q}$-basis

$$\langle e, w_1, \cdots, w_r, u \rangle$$

of $L_\mathbb{Q}$, with $(e, u) = 1$, and a finite index subgroup

$$H := \langle g_1, \cdots, g_r \rangle \simeq \mathbb{Z}^r$$

of G, such that

$$g_i = \begin{pmatrix} 1 & \mathbf{a}_i^t & c_i \\ \mathbf{0} & I_r & q_i \mathbf{e}_i \\ 0 & \mathbf{0}^t & 1 \end{pmatrix},$$

under the $\mathbb{Q}$-basis above. Here $1, 0 \in \mathbb{Q}$ are the unit and the zero, c_i and $q_i \neq 0$ are in $\mathbb{Q}$, $\mathbf{e}_i$ is the i-th unit vector of $\mathbb{Q}^r$, I_r is the $r \times r$ identity matrix, $\mathbf{0} \in \mathbb{Q}^r$ is the zero vector, $\mathbf{a}_i^t$ is the transpose of a column vector $\mathbf{a}_i \in \mathbb{Q}^r$, and simiarly for $\mathbf{0}^t$.

Proof. This is observed in [Og09, Proof of Lemma 3.6, Claim 3.8]. The essential part is that $e^\perp/\mathbb{Z}e$ is a negative definite lattice with respect to the $\mathbb{Z}$-valued bilinear form induced by $(*, **)$ and G acts on this negative definite lattice $e^\perp/\mathbb{Z}e$. Note then that

$$H := \mathrm{Ker}\big(G \to \mathrm{O}(e^\perp/\mathbb{Z}e)(\mathbb{Z})\big)$$

is a finite index subgroup of G as $\mathrm{O}(e^{\perp}/\mathbb{Z}e)(\mathbb{Z})$ is a finite group. Since $G \simeq \mathbb{Z}^r$, we have then $H \simeq \mathbb{Z}^r$ by the fundamental theorem of finitely generated abelian groups. Next choose an $\mathbb{Z}$-basis

$$\langle e, w_1, \cdots, w_r \rangle$$

of $e^{\perp}$. As $e^{\perp}$ is of signature $(0, 1, r-1)$ (degenerate lattice), it follows that $(w_i, w_i) < 0$ and $(e.w_i) = 0$, in addition to $(e^2) = 0$. Choose then $u \in L_{\mathbb{Q}}$ such that $(e.u) = 1$. Such a vector u exists as L is hyperbolic. Then,

$$\langle e, w_1, \cdots, w_r, u \rangle$$

form a $\mathbb{Q}$-basis of $L_{\mathbb{Q}}$ and the matrix representation of H with respect to the $\mathbb{Q}$-basis above is of the form

$$g = \begin{pmatrix} 1 & \mathbf{a}^t(g) & c(g) \\ \mathbf{0} & I_r & \mathbf{b}(g) \\ 0 & \mathbf{0}^t & 1 \end{pmatrix} ,$$

for all $g \in H \subset G \subset \mathrm{SO}(L)(\mathbb{Z})$. It is proved in [Og09, Claim 3.8] that the map

$$H \to \mathbb{Q}^r \ ; \ g \mapsto \mathbf{b}(g)$$

is an injective group homomorphism. This is easily checked by an explicit computation of matrices. Since $H \simeq \mathbb{Z}^r$, it follows that

$$\mathbb{Z}^r \simeq H \simeq \langle \mathbf{b}(g) | g \in H \rangle \subset \mathbb{Q}^r \ .$$

Thus, again by the fundamental theorem of finitely generated abelian groups, we obtain an $\mathbb{Z}$-basis of H with required property. □

Lemma 4.8. *There are integers i, j such that $1 \le i, j \le r$ and*

$$\mathbf{a}_j^t \cdot \mathbf{e}_i \ne 0 \ .$$

Here the right hand side is the product as matrices and we naturally identify 1×1 matrices with the entry.

Proof. Now assume to the contrary that $\mathbf{a}_j^t \cdot \mathbf{e}_i = 0$ for all i, j. Then $\mathbf{a}_j^t = 0$ for all j. Thus

$$g_j(u) = c_j e + q_j w_j + u$$

by the explicit matrix form. Then by induction one has

$$g_j^k(u) = g_j((k-1)c_j e + (k-1)w_j + u) = k(c_j e + q_j w_j) + u$$

for all positive integers k. Since g_j^k preserves intersection form, it follows that

$$(u, u) = (g^k(u), g^k(u)) = (u, u) + 2k(q_j(w_j, u) + c_j) + k^2 q_j^2 (w_j, w_j)$$

whence

$$(w_j, w_j) q_j^2 k + 2(c_j + q_j(w_j, u)) = 0$$

for all positive integers k, a contradiction to $\big((w_j, w_j) < 0,\ q_j \ne 0\big)$ in Lemma 4.7. □

To conclude the Theorem 4.6, it suffices to confirm the following:

Lemma 4.9. *Let M be a G-stable $\mathbb{R}$-linear subspace of $L_{\mathbb{R}}$. Assume that there is $v \in M_{\mathbb{R}}$ such that $v \notin e^{\perp}$ in $L_{\mathbb{R}}$. Then $M = L_{\mathbb{R}}$.*

Proof. After scaling v by an element of $\mathbb{R}^\times$, we may assume without loss of generality that

$$v = xe + \sum_{s=1}^{r} y_s w_s + u$$

where x and y_s are real numbers. Then by Lemma 4.7

$$g_i(v) = v + (\mathbf{a}_i^t \cdot \mathbf{y} + c_i)e + q_i w_i \ ,$$

where $\mathbf{y} \in \mathbb{R}^r$ is the vector whose s-th entry is y_s. But $g(v) \in M$ by the assumption and by the fact that M is $\mathbb{R}$-linear, it follows that

$$v_i := (\mathbf{a}_i^t \cdot \mathbf{y} + c_i)e + q_i w_i \in M \ .$$

By Lemma 4.7, it follows that

$$g_j(v_i) = v_i + q_i({}^t\mathbf{a}_j \cdot \mathbf{e}_i)e \ .$$

Recall from Lemma 4.7 that $q_i \neq 0$. Then, for the same reason above, it follows that

$$(\mathbf{a}_j^t \cdot \mathbf{e}_i)e \in M$$

for all $1 \leq i, j \leq r$. Thus by Lemma 4.8, $e \in M$. Combining this with $v_i \in M$, it follows that $q_i w_i \in M$ for all i. Since $q_i \neq 0$, it follows that $w_i \in M$ for all i. Combining this with $v \in M$, it follows that $u \in M$. Since e, w_i, u form a $\mathbb{Q}$-basis of $L_{\mathbb{Q}}$, thus a $\mathbb{R}$-basis of $L_{\mathbb{R}}$, it follows that $L_{\mathbb{R}} \subset M$. This finishes the proof. □

This completes the proof of Theorem 4.6. □

5. Proof of Theorems 1.2 and 1.1

First we prove Theorem 1.2. Let X be as in Theorem 1.2 after Lemma 5.2. We recall that $\mathrm{NS}\,(X)$ is a hyperbolic lattice of signature $(1, \rho(X) - 1)$.

Recall that an elliptic fibration $\varphi : X \to \mathbb{P}^1$ on the minimal surface X is a projective, surjective morphism over a field k, which has a section $O : \mathbb{P}^1 \to X$, and such that the generic fiber is a smooth curve of genus 1 over $k(\mathbb{P}^1)$. We denote by $\mathrm{MW}(\varphi)$ its Mordell-Weil group, viewed it as a subgroup of the group of the birational automorphisms $\mathrm{Bir}(X)$.

The following lemma is well known.

Lemma 5.1. *Let $\varphi : X \to \mathbb{P}^1$ be an elliptic fibration. Then*

1. $\mathrm{MW}\,(\varphi)$ *of φ is a finitely generated abelian subgroup of* $\mathrm{Aut}\,(X) \subset \mathrm{Bir}(X)$*;*
2. *the action of* $\mathrm{MW}\,(\varphi)$ *on* $\mathrm{NS}\,(X)$ *is faithful.*

We denote by $\mathrm{MW}\,(\varphi)^* \subset \mathrm{O}^+(\mathrm{NS}\,(X))$ the image of the induced representation on the Néron-Severi group $\mathrm{NS}\,(X)$ of X. Thus $\mathrm{MW}\,(\varphi) \xrightarrow{\cong} \mathrm{MW}\,(\varphi)^*$.

Proof. The group $\mathrm{MW}\,(\varphi)$ is finitey generated by [Sh90], as φ, for topological reasons, has at least one singular fiber. As X is a smooth projective minimal surface, $\mathrm{Bir}\,(X) = \mathrm{Aut}\,(X)$. This implies (1). One has $|O| = \{O\}$, where $|O|$ is the complete linear system containinig O. This is because $O \simeq \mathbb{P}^1$ and $(O, O) = -2 < 0$ as X is a K3 surface.

Let $f \in \mathrm{MW}\,(\varphi)$. If $f^*|\mathrm{NS}\,(X) = \mathrm{Id}$, then in particular, the class of O in $\mathrm{NS}(X)$ is invariant under f^*, thus $|O|$ is invariant under f, thus the section O is invariant under f. As $f \in \mathrm{MW}(\varphi)$, this implies $f = \mathrm{Id}$ on X. This proved (2). □

In the sequel, the notations are as in Section 3. We define in addition

$$\mathrm{MW}\,(\varphi)^{*0} := \mathrm{MW}\,(\varphi)^{*} \cap \mathrm{SO}^{+}(\mathrm{NS}\,(X)_{\mathbb{R}}).$$

Lemma 5.2. (i) *The group* $\mathrm{Aut}\,(X)^{*0}$ *is infinite, thus* $\mathrm{Aut}\,(X)$ *is infinite as well.*
(ii) *The abelian groups* $\mathrm{MW}\,(\varphi)$ *and* $\mathrm{MW}\,(\varphi)^{*0}$ *have the same rank.*

Proof. As $\mathrm{Aut}\,(X)^{*0} \supset \mathrm{MW}\,(\varphi)^{*0}$, (i) follows from (ii). We prove ii). By Lemma 5.1 $\mathrm{MW}\,(\varphi) \xrightarrow{\cong} \mathrm{MW}\,(\varphi)^{*}$. On the other hand, $\mathrm{SO}^{+}(\mathrm{NS}\,(X)_{\mathbb{R}})$ is a finite index subgroup of $\mathrm{O}(\mathrm{NS}\,(X))(\mathbb{R})$. Thus $\mathrm{MW}\,(\varphi)^{*0}$ is a finite index sugroup of $\mathrm{MW}\,(\varphi)^{*}$. □

Recall that X is as in Theorem 1.2. We denote by $e_1 \in \mathrm{NS}\,(X)$ the class of a fiber of φ_1.

Lemma 5.3. *X admits $g \in \mathrm{Aut}\,(X)$ such that $g^{*}(e_1) \neq e_1$ in $\mathrm{NS}\,(X)$.*

Proof. By the assumption, X admits a different elliptic fibration $\varphi_2 : X \to \mathbb{P}^1$ of positive Mordell-Weil rank. Thus, by Lemma 5.2, there is $g \in \mathrm{MW}\,(\varphi_2)$ of infinite order.

Let $f \in \mathrm{NS}\,(X)$ be the fiber class of φ_2, thus in particular, $g^{*}(f) = f$. By the Hodge index theorem, $(f + e_1, f + e_1) > 0$. Therefore $(e_1 + f)^{\perp}$ in $\mathrm{NS}\,(X)$ is a negative definite lattice.

Assume that $g^{*}(e_1) = e_1$ in $\mathrm{NS}\,(X)$. Then $g^{*}(e_1 + f) = e_1 + f$. Thus, by Lemma 5.1, g acts faithfully on $(e_1 + f)^{\perp}$. As $\mathrm{O}((e_1 + f)^{\perp})(\mathbb{Z})$ is a finite group, g is of finite order, a contradiction. This proves the Lemma. □

Definition 5.4. Consider all the elliptic fibrations $\Phi_i : X \to \mathbb{P}^1$ $(i \in I)$ on X with maximum Mordell-Weil rank $r = \rho(X) - 2$. Let $e_i \in \mathrm{NS}\,(X)$ be the class of fibers of Φ_i. Set

$$\mathcal{S} := \{e_i \in \mathrm{NS}\,(X) |\ i \in I\},$$

and denote by $\mathbb{R}\langle \mathcal{S} \rangle \subset \mathrm{NS}(X)_{\mathbb{R}}$ the real sub vectorspace spanned by $\mathcal{S}$. Note that $(e_i, e_i) = 0$, e_i are numerically effective and e_i are primitive in $\mathrm{NS}\,(X)$ for all $e_i \in \mathcal{S}$.

Lemma 5.5. *One has* $\mathbb{R}\langle \mathcal{S} \rangle \xrightarrow{\cong} \mathrm{NS}\,(X)_{\mathbb{R}}$.

Proof. Recall that $\mathcal{S} \neq \emptyset$ by our assumption. Let $e_1 \in \mathcal{S}$ be the class of Φ_1. By definition of $\mathcal{S}$, $\mathbb{R}\langle \mathcal{S} \rangle$ is $\mathrm{Aut}\,(X)$-stable. Let $g \in \mathrm{Aut}\,(X)$ with $e_2 := g(e_1) \neq e_1$ (Lemma 5.3). As $\mathcal{S}$ is stable under $\mathrm{Aut}\,(X)$, it follows that $e_2 \in \mathcal{S}$ as well.

Assume to the contrary that $\mathbb{R}\langle \mathcal{S} \rangle \neq \mathrm{NS}\,(X)_{\mathbb{R}}$. Let $G_1 \subset \mathrm{MW}\,(\Phi_1)^{*0}$ be a free abelian group of rank $r = \rho(X) - 2$. By Theorem 4.6 applied to G_1, one has $\mathbb{R}\langle \mathcal{S} \rangle \subset e_1^{\perp}$ in $\mathrm{NS}\,(X)_{\mathbb{R}}$. By the Hodge index theorem and the fact that e_i are primitive, one has $(e_1, e_2) > 0$, a contradiction. □

Lemma 5.6. *There is no* $\mathrm{Aut}\,(X)^{*0}$*-stable* $\mathbb{R}$*-linear subspace of* $\mathrm{NS}\,(X)_{\mathbb{R}}$ *other than* $\{0\}$ *and* $\mathrm{NS}\,(X)_{\mathbb{R}}$.

Proof. Let $M \neq \mathrm{NS}\,(X)_{\mathbb{R}}$ be an $\mathrm{Aut}\,(X)^{*0}$-stable $\mathbb{R}$-linear subspace of $\mathrm{NS}\,(X)_{\mathbb{R}}$. For Φ_i as in Definition 5.4, let $G_i \subset \mathrm{MW}\,(\Phi_i)^{*0}$ be a free abelian subgroup of maximal rank $r = \rho(X) - 2$ (Lemma 5.1). By Theorem 4.6 applied to G_i, it follows

$$M \subset \cap_{i \in I} e_i^{\perp} \subset \mathrm{NS}(X)_{\mathbb{R}}.$$

As the vectors e_i, for $i \in I$, generate $\mathrm{NS}\,(X)_{\mathbb{R}}$ and the intersection form is non-degenerate on $\mathrm{NS}\,(X)$, it follows that

$$\cap_{i\in I} e_i^{\perp} = \{0\}\ .$$

This proves the lemma. □

Proof of Theorem 1.2. By Lemma 5.2 and Lemma 5.6, we can apply Theorem 4.1. □

Proof of Theorem 1.1. As mentioned in the introduction, Shioda [Sh13] proved that any $X(p)$ with $p = 11$ or $p > 13$ admits an elliptic fibration $\varphi_1 : X \to \mathbb{P}^1$ with Mordell-Weil rank $20 = 22 - 2$. On the other hand, over $\mathbb{F}_p$, $X(p) \simeq \mathrm{Km}\,(E \times_{\mathbb{F}_p} E)$ for a supersingular elliptic curve E over $\mathbb{F}_p$, and the fibration $\varphi_2 : X \to \mathbb{P}^1$ induced by the first projection $E \times_{\mathbb{F}_p} E \to E$ is an elliptic fibration with Mordell-Weil rank 4 (thus positive) over $\bar{\mathbb{F}}_p$, by the formula of Mordell-Weil rank [Sh90]. In particular, these two fibrations are non-isomorphic. So, we apply Theorem 1.2 to conclude Theorem 1.1 for $p = 11$ or $p > 13$. The cases $p = 2$ and $p = 3$ are proved by [BC13] and [EO14]. This completes the proof of Theorem 1.1.

□

References

[Ar74] Artin, M.: *Supersingular $K3$ surfaces*, Ann. Sci. École Norm. Sup. **7** (1975) 543–567.

[BC13] Blanc, L., Cantat, S.: *Dynamical degrees of birational transformations of projective surfaces*, http://arxiv.org/pdf/1307.0361.pdf.

[BH04] Benoist, Y., de la Harpe, P.: *Adhérence de Zariski des groupes de Coxeter*, Compositio Math. **140**, (2004) 1357–1366.

[SGA4.5] Deligne, P.: *Séminaire de Géométrie Algébrique $4\frac{1}{2}$: Cohomologie Étale*, Lecture Notes in Mathematics **569** (1977), Springer Verlag.

[Del81] Deligne, P.: *Relèvement des surfaces $K3$ en caractéristique nulle*, Lecture Notes in Math., **868**, (1981) 58–79.

[DK02] Dolgachev, I., Kondo, S.: *A supersingular K3 surface of characteristic 2 and the Leech lattice*, Int. Math. Res. Not. **1** (2003), 1–23.

[ES13] Esnault, H., Srinivas, V.: *Algebraic versus topological entropy for surfaces over finite fields*, Osaka J. Math. **50** (2013) no3, 827–846.

[EO14] Esnault, H., Oguiso, K.: *Non-liftability of automorphism groups of a K3 surface in positive characteristic*, http://arxiv.org/pdf/1406.2761v3.pdf.

[GMc02] Gross, B., McMullen C.T.: *Automorphisms of even unimodular lattices and unramified Salem numbers*, J. Algebra **257** (2) (2002), 265–290.

[SGA6] Grothendieck, A.: *Séminaire de Géométrie Algébrique 6: Théorie des Intersections and Théorème de Riemann-Roch,* Lecture Notes in Mathematics **225** (1971), Springer Verlag.

[Jan14] Jang, J.: *Representations of the automorphism group of a supersingular K3 surface of Artin-invariant* 1 *over odd characteristic*, J. of Chungcheong Math. Soc. **27** 2 (2014), 287–295.

[KS12] S. Kondo, I. Shimada, : *The automorphism group of a supersingular K3 surface with Artin invariant 1 in characteristic 3*, http://arxiv.org/pdf/1205.6520v2.pdf.

[LM11] Lieblich, M., Maulik, D.: *A note on the cone conjecture for K3 surfaces in positive characteristic*, http://arxiv.org/pdf/1102.3377v3.pdf.

[Mc02] McMullen, C. T.: *Dynamics on $K3$ surfaces: Salem numbers and Siegel disks*, J. Reine Angew. Math. **545** (2002) 201–233.

[Mc11] McMullen, C. T.: *Automorphisms of projective K3 surfaces with minimum entropy*, http://www.math.harvard.edu/~ctm/papers/home/text/papers/pos/pos.pdf.

[Og09] Oguiso, K.: *Mordell-Weil groups of a hyperkähler manifold - a question of F. Campana*, special volume dedicated to Professor Heisuke Hironaka on his 77-th birthday, Publ. RIMS, **44** (2009) 495–506.

[Og10] Oguiso, K.: *Salem polynomials and the bimeromorphic automorphism group of a hyper-Kähler manifold*, Selected papers on analysis and differential equations, Amer. Math. Soc. Transl. Ser. **230** (2010) 201–227.

[Ogu79] Ogus, A.: *Supersingular $K3$ crystals*, Journées de Géométrie Algébrique de Rennes, Astérisque **64**, (1979), 3–86.

[Ogu83] Ogus, A.: *A crystalline Torelli theorem for supersingular $K3$ surfaces*, Progr. Math. **36** (1983) 361–394.

[Sch12] Schütt, M.: *A note on the supersingular K3 surface of Artin invariant 1*,
Journal of Pure and Applied Algebra **216** (2012), 1438-1441.

[Sh75] Shioda, T.: *Algebraic cycles on certain K3 surfaces in characteristic p*, Manifolds-Tokyo 1973 (Proc. Internat. Conf., Tokyo, 1973), 357–364. Univ. Tokyo Press, Tokyo, 1975.

[Sh90] Shioda, T.: *On the Mordell-Weil lattices*, Comm. Math. Univ. St. Paul **39** 2 (1990), 211–240.

[Sh13] Shioda, T.: *Elliptic fibrations of maximal rank on a supersingular K3 surface*, Izv. Ross. Akad. Nauk Ser. Mat. **77** (2013), 139–148; translation in Izv. Math. **77** (2013) 571–580.

Freie Universität Berlin, Arnimallee 3, 14195, Berlin, Germany
E-mail address: `esnault@math.fu-berlin.de`

Mathematical Sciences, the University of Tokyo, Meguro Komaba 3-8-1, Tokyo, Japan and Korea Institute for Advanced Study, Hoegiro 87, Seoul, 133-722, Korea
E-mail address: `oguiso@ms.u-tokyo.ac.jp`

Center for Geometry and its Applications, POSTECH, Pohang 790-784, Korea
E-mail address: `yxn100135@postech.ac.kr`