European Journal of Mathematics (2024) 10:36
https://doi.org/10.1007/s40879-024-00745-1

RESEARCH ARTICLE

$K3$ surfaces, cyclotomic polynomials and orthogonal groups

Eva Bayer-Fluckiger[1]

In memory of Nikolai Vavilov

Received: 11 February 2024 / Revised: 7 April 2024 / Accepted: 12 April 2024 /
Published online: 30 May 2024
© The Author(s) 2024

Abstract

Let X be a complex projective $K3$ surface and let T_X be its transcendental lattice; the characteristic polynomials of isometries of T_X induced by automorphisms of X are powers of cyclotomic polynomials. Which powers of cyclotomic polynomials occur? The aim of this note is to answer this question, as well as related ones, and give an alternative approach to some results of Kondō, Machida, Oguiso, Vorontsov, Xiao and Zhang; this leads to questions and results concerning orthogonal groups of lattices.

Keywords $K3$ surfaces · Orthogonal groups

Mathematics Subject Classification 14J28 · 20G30

1 Introduction

If X is a projective $K3$ surface over the complex numbers; we denote by S_X its Picard lattice and by T_X its transcendental lattice; if $a\colon X \to X$ is an automorphism, then a induces an isometry a^* of the lattice $H^2(X, \mathbf{Z})$, and the characteristic polynomial of the restriction of a^* to T_X is a power of a cyclotomic polynomial (see Proposition 2.1).

Let m, r be integers with $m \geqslant 3$ and $r \geqslant 1$, and let $C = \Phi_m^r$ (where Φ_m is the m-th cyclotomic polynomial).

Proposition 1.1 *Assume that* $\deg(C) \leqslant 20$. *Then there exists an automorphism* $a\colon X \to X$ *of a projective* $K3$ *surface* X *such that the characteristic polynomial of the restriction of* a^* *to* T_X *is equal to* C.

✉ Eva Bayer-Fluckiger
eva.bayer@epfl.ch

[1] EPFL-FSB-MATH, Station 8, 1015 Lausanne, Switzerland

We denote by $\mathrm{Aut}(X)$ the group of automorphisms of the $K3$ surface X, and by $\mathrm{Aut}_{\mathrm{s}}(X)$ the subgroup of $\mathrm{Aut}(X)$ acting trivially on T_X. We have the exact sequence

$$1 \to \mathrm{Aut}_{\mathrm{s}}(X) \to \mathrm{Aut}(X) \to M_X \to 1,$$

where M_X is a finite cyclic group (see Nikulin [18, Theorem 10.1.2]); we denote by m_X the order of M_X.

Corollary 1.2 *Let $m \geqslant 4$ be an even integer such that $\varphi(m) \leqslant 20$. Then there exists a projective $K3$ surface X with $m_X = m$.*

It is well known that there exist $K3$ surfaces X with $m_X = 1, 2$ (see for instance [11, Corollary 15.2.12]), but as far as we know, the following question is open.

Question 1.3 Let $m > 1$ be an odd integer. Does there exist a projective $K3$ surface X with $m_X = m$?

In [15], Machida and Oguiso obtain several results on related topics; see Remark 11.5, Proposition 12.1 and Remark 13.2 for details.

Following Vorontsov [23] and Kondō [12], we consider automorphisms that act trivially on the Picard lattice. Let N_X be the kernel of $\mathrm{Aut}(X) \to \mathrm{O}(S_X)$; this is a finite cyclic group that can be identified with a subgroup of M_X; we denote by n_X the order of N_X. The following proposition is proved in Sect. 5.

Proposition 1.4 *There exists an automorphism $a\colon X \to X$ of a projective $K3$ surface X such that a^* is the identity on S_X and that the characteristic polynomial of the restriction of a^* to T_X is equal to C if and only if the following conditions hold:*

(i) *$C(-1)$ is a square.*
(ii) *If $C(1) = 1$, then $\deg(C) \equiv 4 \pmod 8$.*

The possible values of n_X can be deduced from Proposition 1.4, extending previous results of Vorontsov [23], Kondō [12], and Oguiso–Zhang [20]; see Sect. 13. Note that n_X divides m_X, since N_X can be identified with a subgroup of M_X. This suggests the following question.

Question 1.5 What are the possible values of the pairs (m_X, n_X)?

The proofs of the above propositions use some arithmetic results (see below), as well as the surjectivity of the period map, the strong Torelli theorem, and some results of McMullen [17].

The arithmetic results are valid in a greater generality than the one needed for the applications to $K3$ surfaces. For instance, in order to prove Proposition 1.4, we introduce the following property, called property (P2):

(P2) Let $R, S \geqslant 0$ be integers such that such that $R \equiv S \pmod 8$, and set $N = R + S$; suppose that $\deg(C) < N$.

Let $c \geqslant 0$ be an even integer with $c \leqslant \deg(C)$ such that $c \leqslant R$ and $\deg(C) - c \leqslant S$.

Definition 1.6 We say that *property* (P2) *holds* if there exist an even, unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ such that

- The characteristic polynomial of t is $C(X)(X-1)^{N-\deg(C)}$.
- The signature of the sublattice $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$.

In application to $K3$ surfaces, we have $R = 3$, $S = 19$ and $c = 2$, and Proposition 1.4 is a consequence of the following result.

Theorem 1.7 *Property* (P2) *holds if and only if the following conditions are satisfied:*

(i) $C(-1)$ *is a square.*
(ii) *If* $C(1) = 1$*, then* $\deg(C) \equiv 2c \pmod 8$.

In particular, Property (P2) always holds if $C(-1)$ is a square and $C(1) > 1$.

If m is an odd prime number, this can be deduced from a result of Brandhorst and Cattaneo [6, Theorem 1.1]. Note that Theorem 1.7 gives a partial answer to a question of this paper (see [6, Outlook]).

With the same notation, we introduce property (P1).

Definition 1.8 We say that *property* (P1) *holds* if there exist an even, unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ such that

(i) The characteristic polynomial of t is divisible by C.
(ii) The signature of the sublattice $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$.

Theorem 1.9 *If* $C(1)C(-1) > 1$*, then property* (P1) *holds.*

If $C(1) = C(-1) = 1$ and $R = 0$ or $S = 0$, then property (P1) does not always hold, but the *indefinite* case seems to be open.

Question 1.10 Does property (P1) always hold when $R > 0$ and $S > 0$?

A modified version of this property is used to prove Proposition 1.1. A more tractable question is to ask for isometries of *finite order*; this leads to the following definition.

Definition 1.11 We say that *property* (P1$'$) *holds* if there exist an even, unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ of finite order such that

- The characteristic polynomial of t is divisible by C.
- The signature of the sublattice $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$.

Note that properties (P1) and (P1$'$) are equivalent if $R = 0$ or $S = 0$, since then all isometries are of finite order. If $R > 0$ and $S > 0$, it is possible that property (P1) always holds — however, this is not the case for property (P1$'$), as shown by the following example.

Example 1.12 Let $C = \Phi_{60}$, and set $R = 3$, $S = 19$ and $c = 2$. Then

- Property (P1) holds (see Example 9.4).
- Property (P1$'$) does not hold (see Proposition 12.2).

The fact that property (P1$'$) does not hold implies the well-known result that there does not exist a projective $K3$ surface X having an automorphism $a \in \mathrm{Aut}(X)$ of *finite order* such that a^* induces multiplication by a primitive 60-th root of unity on T_X; see Machida and Oguison [15], Xiao [25], and Zhang [26]; see also Proposition 12.1.

It can be useful to replace "of finite order" by "of *order m*". This point of view is taken by several authors; see the paper of Brandhorst [5] and the references therein; see also Sects. 6, 7 and 8.

The paper is organized as follows. The first two sections are mainly preliminary, recalling notions and results on $K3$ surfaces and isometries of lattices; Sects. 3 and 9 also recall some results of [2, 3], and give some examples that are used in the paper. Theorem 1.7 is proved in Sect. 4 (see Theorem 4.6), and Proposition 1.4 in Sect. 5 (see Proposition 5.1). A stronger form of Theorem 1.9 is in Sect. 6, see Theorem 6.1. Proposition 1.1 is proved in Sects. 10 and 11. The last section concerns the possible values of m_X and n_X, a discussion of some results of Kondō and Vorontsov, as well as a generalization of these results, and some open questions.

The proofs use results of [2, 3], of McMullen, [17], and of Takada [22].

2 *K*3 surfaces

We recall some notation and basic facts on $K3$ surfaces and their automorphisms; see [11, 13] for details.

A $K3$ surface X is a simply-connected compact complex surface with trivial canonical bundle. We have the Hodge decomposition

$$H^2(X, \mathbf{C}) = H^{2,0}(X) \oplus H^{1,1}(X) \oplus H^{0,2}(X)$$

with $\dim H^{2,0} = \dim H^{0,2} = 1$ and $\dim H^{1,1} = 20$. The *Picard lattice* of X is by definition

$$S_X = H^2(X, \mathbf{Z}) \cap H^{1,1}(X).$$

The intersection form $H^2(X, \mathbf{Z}) \times H^2(X, \mathbf{Z}) \to \mathbf{Z}$ of X is an even unimodular lattice of signature $(3, 19)$. Such a form is unique up to isomorphism (see for instance [21, Chapter V, Theorem 5]). The *transcendental lattice* T_X is by definition the primitive sublattice of $H^2(X, \mathbf{Z})$ of minimal rank such that $T_X \otimes_{\mathbf{Z}} \mathbf{C}$ contains $H^{2,0}(X) \oplus H^{0,2}(X)$. Assume that X is *projective*; then lattices S_X and T_X are orthogonal to each other, and the orthogonal sum $S_X \oplus T_X$ is of finite index in $H^2(X, \mathbf{C})$, the signature of S_X is $(1, \rho_X - 1)$, and the signature of T_X is $(2, 20 - \rho_X)$, where ρ_X is the rank of S_X.

If $a \colon X \to X$ is an automorphism, then $a^* \colon H^2(X, \mathbf{C}) \to H^2(X, \mathbf{C})$ respects the Hodge decomposition and is an isometry of the intersection form; hence a^* is also an isometry of the lattices S_X and T_X.

The following is a result of Oguiso [19, Theorem 2.4].

Proposition 2.1 *Let $a\colon X \to X$ be an automorphism of a projective $K3$ surface. Then the minimal polynomial of the restriction of a^* to T_X is a cyclotomic polynomial.*

Proof The minimal polynomial of the restriction of a^* to T_X is irreducible (see Oguiso [19, Theorem 2.4 (1)]). Since X is projective, $a^*|T_X$ is of finite order (cf. Nikulin [18, Theorem 10.1.2], [19, Theorem 2.4 (4)], or [11, Corollary 3.3.4 or Corollary 15.1.10]), hence its minimal polynomial is a cyclotomic polynomial. □

3 Isometries of lattices

In this section we summarize some notions and results from [2, 3, 10] in the special cases needed in this paper.

A *lattice* is a pair (L, q), where L is a free $\mathbf{Z}$-module of finite rank, and $q\colon L \times L \to \mathbf{Z}$ is a symmetric bilinear form; it is *unimodular* if $\det(q) = \pm 1$, and *even* if $q(x, x)$ is an even integer for all $x \in L$. The following lemma is well known.

Lemma 3.1 (See e.g., [21, Chapter V, Corollary 1]) *Let L be an even unimodular lattice of signature (r, s). Then $r \equiv s \pmod 8$.*

Let $n \geqslant 1$ be an integer and let $F \in \mathbf{Z}[x]$ be a monic polynomial of degree $2n$ such that $F(x) = x^{2n}F(x^{-1})$. We say that F *satisfies condition* (C1) if $|F(1)|$, $|F(-1)|$ and $(-1)^n F(1)F(-1)$ are squares.

Lemma 3.2 (Gross–McMullen, [10, Theorem 6.1] or [3, Corollary 2.3]) *Let L be an even unimodular lattice and let $t\colon L \to L$ be an isometry with characteristic polynomial F. Then F satisfies condition* (C1).

Assume that F is a *product of cyclotomic polynomials*, and that $F(1) \neq 0$ or $F(-1) \neq 0$. Let us write $F = F_1F_0$, where $F_1 \in \mathbf{Z}[x]$ is a monic polynomial such that $F_1(1)F_1(-1) \neq 0$, and $F_0(x) = (x - 1)^{n_+}$ or $F_0(x) = (x + 1)^{n_-}$, where $n_+, n_- \geqslant 0$ are integers. Set $D_0 = (-1)^n F_1(1)F_1(-1)$. Let I be the set of irreducible factors of F over $\mathbf{Q}$.

Following [3], we associate to F a finite group G_F; we start by defining a set $\Pi_{f,g}$ for all $f, g \in I$, as follows. We say that a monic polynomial h is $(\pm)$-*symmetric* if $h(x) = \pm x^{\deg(h)}h(x^{-1})$. We also use the terminology *symmetric* for $(+)$-symmetric.

If $f, g \in I$ are such that $\deg(f) \geqslant 2$, $\deg(g) \geqslant 2$, then $\Pi_{f,g}$ is the set of prime numbers p such that $f \pmod p$ and $g \pmod p$ have a common irreducible $(\pm)$-symmetric factor in $\mathbf{F}_p[x]$.

If $f \in I$ is such that $\deg(f) \geqslant 2$, then $\Pi_{f,x-1}$ is the set of prime numbers p such that $f \pmod p$ is divisible by $x - 1$ in $\mathbf{F}_p[x]$, and that if $n^+ = 2$, then $D_0 \neq -1$ in $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$.

If $f \in I$ is such that $\deg(f) \geqslant 2$, then $\Pi_{f,x+1}$ is the set of prime numbers p such that $f \pmod p$ is divisible by $x + 1$ in $\mathbf{F}_p[x]$, and that if $n^- = 2$, then $D_0 \neq -1$ in $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$.

Let $C(I)$ be the set of maps $c\colon I \to \mathbf{Z}/2\mathbf{Z}$, let $C_0(I)$ the set of $c \in C(I)$ such that $c(f) = c(g)$ if $\Pi_{f,g} \neq \varnothing$; note that $C_0(I)$ is an abelian group. Let G_F be the quotient of $C_0(I)$ by the subgroup of constant maps.

Example 3.3 Let $F(x) = \Phi_{15}^2(x)\Phi_3(x)(x-1)^2$. We have $5 \in \Pi_{\Phi_{15},\Phi_3}$ and $3 \in \Pi_{\Phi_3(x),x-1}$, hence $G_F = 0$.

When F has no linear factors, then G_F is already defined in [2], and several examples are given in [2, Section 25]. Here is another example that will be used in the proof of Proposition 10.5.

Example 3.4 Let $F = \Phi_{60}\Phi_{12}$. The resultant of Φ_{60} and Φ_{12} is 5^4, and the polynomials Φ_{60} and Φ_{12} (mod 5) have the common irreducible factors x^2+2x+4 and x^2+3x+4 in $\mathbf{F}_5[x]$. These polynomials are not $(\pm)$-symmetric, hence $\Pi_{\Phi_{60},\Phi_{12}} = \varnothing$, and $G_F = \mathbf{Z}/2\mathbf{Z}$.

The following is proved in [3, Corollary 12.4].

Theorem 3.5 *Let $r, s \geqslant 0$ be integers such that $r \equiv s \pmod 8$ and that $r+s = \deg(F)$. If $G_F = 0$, then there exists an even unimodular lattice of signature (r, s) having an isometry with characteristic polynomial F.*

We need a more precise result: it is not enough to fix the signature of the lattice, we also need information about the *signature map* of the isometry. We recall this notion from [3, Sections 3 and 4].

Definition 3.6 Let V be a finite-dimensional vector space over $\mathbf{R}$ and let $q\colon V \times V \to \mathbf{R}$ be a non-degenerate quadratic form. Let $t\colon V \to V$ be an isometry of q. If $f \in \mathbf{R}[X]$, set $V_f = \operatorname{Ker}(f(t))$ and let q_f be the restriction of q to V_f. Let

$$\operatorname{sign}_t\colon \mathbf{R}[X] \to \mathbf{N} \times \mathbf{N}$$

be the map sending $f \in \mathbf{R}[X]$ to the signature of (V_f, q_f), where $\mathbf{N}$ is the set of all nonnegative integers; it is called the *signature map of the isometry t*. The signature of q is called the *maximum* of the signature map, and the characteristic polynomial of t the *polynomial associated to the signature map*.

Example 3.7 Let $a\colon X \to X$ be an automorphism of a projective $K3$ surface, and suppose that $a^*|S_X$ is the identity and that the characteristic polynomial of the restriction of a^* to T_X is C. Let ρ_X be the rank of S_X and let τ be the signature map of a^*. Then we have $\tau(x-1) = (1, \rho_X - 1)$ and $\tau(C) = (2, \deg(C) - 2)$. Note that $\deg(C) = 22 - \rho_X$, hence we also have $\tau(C) = (2, 20 - \rho_X)$.

Theorem 3.8 ([3, Corollary 12.3]) *Let $r, s \geqslant 0$ be integers such that $r \equiv s \pmod 8$ and that $r + s = \deg(F)$. Let τ be a signature map of maximum (r, s) and associated polynomial F. If $G_F = 0$, then there exists an even unimodular lattice having an isometry with signature map τ.*

4 Cyclotomic polynomials and property (P2)

The aim of this section is to prove Theorem 1.7 from the introduction. We start by recalling some basic properties of cyclotomic polynomials. Recall that Φ_m denotes the m-th cyclotomic polynomial and that $\deg(\Phi_m) = \varphi(m)$.

Lemma 4.1 *Let m be an integer with $m \geqslant 3$. We have*

(i) *If m is a power of 2, then $\Phi_m(1) = \Phi_m(-1) = 2$.*
(ii) *Let p be a prime number with $p \neq 2$ and let $k \geqslant 1$ be an integer. If $m = p^k$, then $\Phi_m(1) = p$ and $\Phi_m(-1) = 1$; if $m = 2p^k$, then $\Phi_m(1) = 1$ and $\Phi_m(-1) = p$.*
(iii) *In all other cases, $\Phi_m(1) = \Phi_m(-1) = 1$.*
(iv) *If $\Phi_m(1) = \Phi_m(-1) = 1$, then* $\deg(\Phi_m) \equiv 0 \pmod 4$.

Proof (i) Let $m = 2^k$ for some integer $k \geqslant 2$. Then $\Phi_m(x) = x^{2^k-1} + 1$, hence $\Phi_m(1) = \Phi_m(-1) = 2$.
(ii) We have $\Phi_p(x) = x^{p-1} + \cdots + x + 1$, and $\Phi_{p^k}(x) = \sum_{i=0,\ldots,p-1} x^{ip^{k-1}}$ for all integers $k \geqslant 1$ (see for instance [14, Chapter IV, Section 1] or [9, Chapter VI, Section 1]). Hence $\Phi_{p^k}(1) = p$ and $\Phi_{p^k}(-1) = 1$ for all $r \geqslant 1$. We have $\Phi_{2p^k}(x) = \Phi_{p^k}(-x)$, hence $\Phi_{2p^k}(1) = 1$ and $\Phi_{2p^k}(-1) = p$ for all $k \geqslant 1$.
(iii) Suppose that m is divisible by at least two distinct prime numbers. Then $\Phi_m(1) = 1$ by [24, Proposition 2.8]. We have $\Phi_m(-1) = \Phi_{2m}(1)$, therefore the same result implies that $\Phi_m(-1) = 1$.
(iv) If $\Phi_m(1) = \Phi_m(-1) = 1$, then by (i) and (ii) the integer m is not of the form p^k or $2p^k$ for some prime number p. Therefore m is divisible by 4 and by an odd prime number, or by two distinct odd prime numbers. This implies that $\varphi(m)$ is divisible by 4, hence $\deg(\Phi_m) \equiv 0 \pmod 4$. □

Lemma 4.2 *Let $C = \Phi_m^r$ where m, r are integers with $m \geqslant 3$ and $r \geqslant 1$. If $C(1)$ and $C(-1)$ are both squares, then* $\deg(C)$ *is divisible by* 4.

Proof If $C(1) = C(-1) = 1$, then Lemma 4.1 (iv) implies that $\deg(C)$ is divisible by 4. Suppose that $C(1)C(-1) \neq 1$. Then by Lemma 4.1 we have $m = p^k$ or $m = 2p^k$ for some prime number p, and hence $\Phi_m(1) = p$ or $\Phi_m(-1) = p$ (see Lemma 4.1 (i) and (ii)). This implies that r is even, and since $\deg(\Phi_m)$ is even, the degree of C is divisible by 4. □

We now recall some notation from the introduction:

- $C = \Phi_m^r$ where m, r are integers with $m \geqslant 3$ and $r \geqslant 1$,
- $R, S \geqslant 0$ are integers such that $R \equiv S \pmod 8$ and $\deg(C) < R + S$. Set $N = R + S$.

Theorem 1.7 is a consequence of Lemmas 4.3 and 4.5.

Lemma 4.3 *Let L be an even unimodular lattice of signature (R, S), and let $t \colon L \to L$ be an isometry with characteristic polynomial $C(x)(x-1)^{N-\deg(C)}$. Let $(c, \deg(C) - c)$ be the signature of the sublattice* $\mathrm{Ker}(C(t))$. *Then*

- *$C(-1)$ is a square.*
- *If $C(1) = 1$, then* $\deg(C) \equiv 2c \pmod 8$.

Moreover, if $C(1) = 1$, then the sublattice $\mathrm{Ker}(C(t))$ *is unimodular.*

Proof Set $F(x) = C(x)(x-1)^{N-\deg(C)}$. Then by Lemma 3.2 the polynomial F satisfies condition (C1); this implies that $|F(-1)|$ is a square. Note that $N - \deg(C)$ is even, hence $|C(-1)|$ is a square. Since C is a power of a cyclotomic polynomial, we have $C(-1) \geqslant 0$ (cf. Lemma 4.1), hence $C(-1)$ is a square, and hence (i) holds.

Set $L_1 = \operatorname{Ker}(C(t))$ and let L_2 be the orthogonal complement of L_1 in L. If $C(1) = 1$, then the polynomials $x-1$ and C are relatively prime over $\mathbf{Z}$ (i.e. the resultant of $x-1$ and C is equal to 1); this implies that $L = L_1 \oplus L_2$, and hence the lattices L_1 and L_2 are both even and unimodular. Therefore $\deg(C) - c \equiv c \pmod 8$, hence $\deg(C) \equiv 2 \pmod 8$, and therefore (ii) holds. □

Lemma 4.4 (i) *If $C(1)$ and $C(-1)$ are both squares, then* $\deg(C) \equiv 0 \pmod 4$.
(ii) *If $C(1)$ and $C(-1)$ are both squares, then condition* (C1) *holds for C.*

Let $c \geqslant 0$ be an even integer such that $c \leqslant \deg(C)$, $c \leqslant R$ and $\deg(C) - c \leqslant S$. We have

(iii) *If $N = \deg(C) + 2$ and $\deg(C) \equiv 0 \pmod 4$, then $\deg(C) \equiv 2c \pmod 8$.*

Proof If $C(1)$ and $C(-1)$ are both squares, then Lemma 4.2 implies that $\deg(C)$ is divisible by 4, hence (i) holds. Set $\deg(C) = 2n$; then n is even, hence $C(1)$, $C(-1)$ and $(-1)^n C(1)$ and $C(-1)$ are all squares, therefore condition (C1) holds for C and this implies (ii).

Let us prove (iii). Since $\deg(C)$ is divisible by 4 and $\deg(C) = N-2$, we have $N \equiv 2 \pmod 4$, and therefore R and S are both odd integers. Since $\deg(C) = N-2$, the inequalities $c \leqslant R$ and $\deg(C) - c \leqslant S$ imply that $R - 2 \leqslant c \leqslant R$; since R and S are odd, this implies that $c = R-1$ and $\deg(C) - c = S - 1$. We have $R \equiv S \pmod 8$ by hypothesis, hence $\deg(C) - c \equiv c \pmod 8$, as claimed. □

Lemma 4.5 *Let $c \geqslant 0$ be an even integer such that $c \leqslant \deg(C)$, $c \leqslant R$ and $\deg(C) - c \leqslant S$. Suppose that the following conditions hold:*

(i) *$C(-1)$ is a square.*
(ii) *If $C(1) = 1$, then $\deg(C) \equiv 2c \pmod 8$.*

Then there exist an even unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ such that

- *The characteristic polynomial of t is $C(x)(x-1)^{N-\deg(C)}$.*
- *The signature of the sublattice $\operatorname{Ker}(C(t))$ is $(c, \deg(C) - c)$.*

Proof Set $F(x) = C(x)(x-1)^{N-\deg(C)}$. By (i), the polynomial F satisfies condition (C1).

Suppose that $C(1) > 1$, and note that by Lemma 4.1 this implies that $m = p^k$ for some prime number p. If $C(1) > 1$ and $\deg(C) < N - 2$, then with the notation of Sect. 3 we have $n^+ \neq 2$, hence $\Pi_{\Phi_m(x), x-1} = \{p\}$. Suppose now that $C(1) > 1$, that $\deg(C) = N-2$, and that $C(1)$ is not a square. Then we have $D_0 \neq -1$ in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$, hence $\Pi_{\Phi_m(x), x-1} = \{p\}$ in this case as well. Therefore in both cases we have $G_F = 0$. By Theorem 3.8, there exist an even, unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ with characteristic polynomial F and signature map τ satisfying $\tau(C) = (c, \deg(C) - c)$. Let $L_1 = \operatorname{Ker}(C(t))$ and let L_2 be the sublattice of L of fixed points by t.

It remains to consider the cases where $C(1)$ is a square, and either $C(1) = 1$ or $\deg(C) = N - 2$.

If $C(1)$ is a square, then by Lemma 4.4 condition (C1) holds for C. Moreover, we have $\deg(C) - c \equiv c \pmod 8$. If $C(1) = 1$, this follows from (ii), and if $\deg(C) = N - 2$, from Lemma 4.4 (i) and (iii).

The polynomial C is a power of an irreducible polynomial, hence the group G_C is trivial, and therefore in both cases we can apply Theorem 3.5, and conclude that there exist an even unimodular lattice L_1 of signature $(c, \deg(C) - c)$ and an isometry $t_1 \colon L_1 \to L_1$ of characteristic polynomial C (note that this also follows from [4, Theorem A]). Let L_2 be an even unimodular lattice of signature $(R-c, S-\deg(C)-c)$, and let $t_2 \colon L_2 \to L_2$ be the identity. Set $L = L_1 \oplus L_2$ and $t = (t_1, t_2)$.

The lattice L is even unimodular and of signature (R, S), and t is an isometry of L with the required properties. □

The following is a reformulation of Theorem 1.7 from the introduction.

Theorem 4.6 *There exist an even unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ such that*

- *The characteristic polynomial of t is $C(x)(x-1)^{N-\deg(C)}$.*
- *The signature of the sublattice $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$ if and only if the following conditions are satisfied:*
  - (i) *$C(-1)$ is a square.*
  - (ii) *If $C(1) = 1$, then $\deg(C) \equiv 2c \pmod 8$.*

Proof This is an immediate consequence of Lemmas 4.3 and 4.5. □

Notation If L is a lattice, we denote by $L^{\#}$ its dual lattice, and set $\Delta(L) = L^{\#}/L$.

Definition 4.7 Let p be a prime number. We say that a lattice L is *p-elementary* if $p\Delta(L) = 0$.

Proposition 4.8 *Let L be a unimodular lattice of rank N and let $t \colon L \to L$ be an isometry with characteristic polynomial $C(x)(x-1)^{N-\deg(C)}$. Set $L_C = \mathrm{Ker}(C(t))$ and let L_0 be the orthogonal complement of L_C in L. Then we have*

(i) *If $C(1) = 1$, then L_C and L_0 are both unimodular.*

(ii) *If $C(1) > 1$, then L_C and L_0 are both p-elementary, where p is such that $\Phi_m(1) = p$.*

Proof (i) Lemma 4.3 implies that L_C is unimodular, hence L_0 is also unimodular.
(ii) The action of t endows L with a structure of $\mathbf{Z}[\Gamma]$-module with Γ infinite cyclic; this action stabilizes L_C and L_0, hence also $\Delta(L_C)$ and $\Delta(L_0)$. Since L is unimodular, the $\mathbf{Z}[\Gamma]$-modules $\Delta(L_C)$ and $\Delta(L_0)$ are isomorphic.

Lemma 4.1 implies that $C = \Phi_m^r$ with $m = p^k$ for some integer k. Therefore t acts on L_C by $t(x) = \alpha.x$ where α is the image of x in $\mathbf{Z}[x]/(\Phi_{p^k})$. On the other hand, t acts as the identity on L_0. Since the $\mathbf{Z}[\Gamma]$-modules $\Delta(L_C)$ and $\Delta(L_0)$ are isomorphic, this implies that $p\Delta(L_C) = 0$ and $p\Delta(L_0) = 0$. □

5 Automorphisms acting trivially on Picard lattices

We now prove Proposition 1.4 from the introduction. Let m, r be integers with $m \geqslant 3$ and $r \geqslant 1$ and let $C = \Phi_m^r$. Assume that $\deg(C) \leqslant 20$.

Proposition 5.1 *There exists an automorphism $a\colon X \to X$ of a projective $K3$ surface X such that a^* is the identity on S_X and that the characteristic polynomial of the restriction of a^* to T_X is equal to C if and only if the following conditions hold:*

(i) *$C(-1)$ is a square.*
(ii) *If $C(1) = 1$, then* $\deg(C) \equiv 4 \pmod 8$.

If $C(1) = 1$, then the lattice T_X is unimodular. Moreover, the $K3$ surface is unique up to isomorphism if and only if C is a cyclotomic polynomial (*i.e.* $r = 1$).

Proof Let $a\colon X \to X$ be an automorphism of a projective $K3$ surface such that $a^*|S_X$ is the identity, and that the characteristic polynomial of $a^*|T_X$ is equal to C. Applying Lemma 4.3 with $L = H^2(X, \mathbf{Z})$, $t = a^*$, $N = 22$, $R = 3$, $S = 19$, and $c = 2$ shows that (i) and (ii) hold.

Conversely, assume that (i) and (ii) hold, and set

$$F(x) = C(x)(x-1)^{22-\deg(C)}.$$

By Lemma 4.5 with $N = 22$, $R = 3$, $S = 19$ and $c = 2$ there exist an even unimodular lattice L of signature $(3, 19)$ and an isometry $t\colon L \to L$ with characteristic polynomial F such that the signature of the sublattice $L_1 = \mathrm{Ker}(C(t))$ is $(2, \deg(C) - 2)$. Let $L_1 = \mathrm{Ker}(C(t))$ and let L_2 be the sublattice of L of fixed points by t.

Let $V \subset L_1 \otimes_{\mathbf{Z}} \mathbf{R}$ be a 2-dimensional subspace of signature $(2, 0)$ and stable by t; for a generic choice of V, the intersection of L with the orthogonal of V is equal to L_2. The restriction of t to V has determinant 1. Since t_2 is the identity, it is positive in the sense of McMullen [17, Section 2]. By [17, Theorem 6.1], there exist a projective $K3$ surface X and an automorphism $a\colon X \to X$ such that $a^* = t$, that $S_X = L_2$ and $T_X = L_1$. Therefore a^* is the identity on S_X and the restriction of a^* to T_X has characteristic polynomial C. If moreover $C(1) = 1$, then by Lemma 4.3 the lattice T_X is unimodular.

If $r = 1$, then the uniqueness of the $K3$ surface up to isomorphism follows from a result of Brandhorst [5, Theorem 1.2]. If $r > 1$, then varying the choice of the subspace V gives rise to an infinite family of $K3$ surfaces. □

Corollary 5.2 *Let $a\colon X \to X$ be an automorphism of a projective $K3$ surface X such that a^* is the identity on S_X and that the characteristic polynomial of the restriction of a^* to T_X is equal to C. Then one of the following holds:*

(i) *T_X and S_X are unimodular.*
(ii) *T_X and S_X are p-elementary, where p is a prime number such that $\Phi_m(1) = p$.*

Proof This is an immediate consequence of Proposition 4.8. □

Note that this implies that $p \leqslant 19$, hence we have the following

Corollary 5.3 *If a projective $K3$ surface X has a non-trivial automorphism that induces the identity on S_X, then the lattices T_X and S_X are either both unimodular or both p-elementary with $p \leqslant 19$.*

6 Cyclotomic polynomials and isometries of finite order

We keep the notation of Sect. 4; in particular, $C = \Phi_m^r$ where m, r are integers with $m \geqslant 3$ and $r \geqslant 1$. The following result implies Theorem 1.9 from the introduction; it is actually a *strengthening* of Theorem 1.9, since it implies the existence of an isometry is of order m.

Theorem 6.1 *Suppose that $C(1)C(-1) > 1$. Then there exist an even, unimodular lattice L of signature (R, S) and an isometry $t : L \to L$ of order m such that*

- *The characteristic polynomial of t is divisible by C.*
- *The signature of the sublattice $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$.*

Proof If $C(1) > 1$ and $C(-1)$ is a square, then this follows from Theorem 4.6.

Suppose that $C(-1) > 1$ and that $C(1)$ is a square. In this case, set $F(X) = C(X)(X + 1)^{N - \deg(C}$. Since $C(1)$ is a square, the polynomial F satisfies condition (C1).

If $\deg(C) < N - 2$, then with the notation of Sect. 3 we have $n^- \neq 2$, hence $\Pi_{\Phi_m(x), x-1} \neq \varnothing$; this implies that $G_F = 0$. Suppose now that $\deg(C) = N - 2$ and that $C(-1)$ is not a square. Note that by Lemma 4.1 this implies that $m = 2p^k$ for some odd prime number p; with the notation of Sect. 3, we have $D_0 \neq -1$ in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$, hence $\Pi_{\Phi_m(x), x-1} = \{p\}$. This implies that $G_F = 0$ in this case as well. By Theorem 3.8, there exist an even, unimodular lattice L of signature (R, S) and an isometry $t : L \to L$ with characteristic polynomial F and signature map τ satisfying $\tau(C) = (c, \deg(C) - c)$.

Suppose now that $C(-1)$ is a square and $\deg(C) = N - 2$; then Lemma 4.4 implies that condition (C1) holds for C and that $\deg(C) - c \equiv c \pmod 8$. The polynomial C is a power of an irreducible polynomial, hence the group G_C is trivial, and therefore we can apply Theorem 3.5, and conclude that there exist an even unimodular lattice L_1 of signature $(c, \deg(C) - c)$ and an isometry $t_1 : L_1 \to L_1$ of characteristic polynomial C (note that this also follows from [4, Theorem A]). Let L_2 be an even unimodular lattice of signature $(R - c, S - \deg(C) - c)$ and let $t_2 : L_2 \to L_2$ be the identity. Set $L = L_1 \oplus L_2$ and $t = (t_1, t_2)$; then $t : L \to L$ has the required properties.

Finally, suppose that $C(1)$ and $C(-1)$ are both non-squares. In this case, $C(1) = C(-1) = 2$, and $C = \Phi_{2^k}$ for some integer k (see Lemma 4.1). Suppose first that $N > \deg(C) + 2$. Set $F(x) = C(x)(x + 1)^2(x - 1)^{N - \deg(C) - 2}$. We have $\Pi_{C, x-1} = \Pi_{x-1, x+1} = \{2\}$ (see [3, Sections 7 and 12]), hence $G_F = 0$. Therefore by [3, Corollary 12.3], there exist exists an even, unimodular lattice L of signature (R, S) and an isometry $t : L \to L$ with characteristic polynomial F and signature map τ satisfying $\tau(C) = (c, \deg(C) - c)$. Assume now that $N = \deg(C) + 2$ and set $F(x) = C(x)(x + 1)(x - 1)$. By Takada [22, Theorem 6.11], there exist a lattice L and an isometry $t : L \to L$ with the required properties. □

It remains to treat the case where $C(1) = C(-1) = 1$; if $\deg(C) \equiv 2c \pmod 8$, then Theorem 4.6 implies the following

Corollary 6.2 *Suppose that* $C(1) = 1$ *and that* $\deg(C) \equiv 2c \pmod 8$. *Then there exist an even unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ of order m such that*

- *The characteristic polynomial of t is divisible by C.*
- *The signature of the sublattice* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

The condition $C(1) = C(-1) = 1$ implies that $\deg(C) \equiv 0 \pmod 4$ (see Lemma 4.1 (i)), and c is an even integer; hence we have either $\deg(C) \equiv 2c \pmod 8$ or $\deg(C) \equiv c \pmod 8$. The first case is covered by Corollary 6.2, therefore we have the following two cases to consider

(a) $c \equiv 0 \pmod 4$ and $\deg(C) \equiv 4 \pmod 8$,
(b) $c \equiv 2 \pmod 4$ and $\deg(C) \equiv 0 \pmod 8$.

We treat these cases in the next sections; the following results will be useful.

Lemma 6.3 *Let $t \colon L \to L$ be an isometry of a lattice L such that*

- *The characteristic polynomial of t is divisible by C.*
- *The signature of the sublattice* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

If $\deg(C) \equiv 0 \pmod 4$ *and* $c \equiv 2 \pmod 4$, *then L is indefinite.*

Proof Indeed, the sublattice $\mathrm{Ker}(C(t))$ is indefinite: since $\deg(C) \equiv 0 \pmod 4$ and $c \equiv 2 \pmod 4$, we have $c \neq \deg(C)$ and $c \neq 0$. □

Proposition 6.4 *Let $m \geqslant 3$ be an integer and let p be a prime number that does not divide m. The following are equivalent:*

(a) *The polynomial Φ_m has a symmetric irreducible factor mod p.*
(b) *The prime ideals of $\mathbf{Q}(\zeta_m + \zeta_m^{-1})$ above p are inert in $\mathbf{Q}(\zeta_m)$.*
(c) *The subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p contains -1.*

Proof The equivalence of (a) and (b) follows from [24, Proposition 2.14]. Let us prove that (b) and (c) are equivalent. Let G be the Galois group of $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ and let P be a prime ideal of $\mathbf{Q}(\zeta_m)$ above p. The decomposition group G_P is by definition $\{g \in, G \mid g(P) = P\}$. Since G is abelian, this group only depends on the prime number p; set $G_P = G_p$. Condition (b) holds if and only if the element of G induced by $\zeta_m \to \zeta_m^{-1}$ is contained in G_p. Let $f \colon G \to (\mathbf{Z}/m\mathbf{Z})^\times$ be an isomorphism; then $f(G_p)$ is the subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p. This implies the equivalence of (b) and (c). □

Corollary 6.5 *Let m, p be distinct prime numbers. If p is not a square modulo m then the polynomial Φ_m has a symmetric irreducible factor mod p.*

Proof We have $p^{(m-1)/2} = \pm 1$. If $p^{(m-1)/2} = 1$, then p is a square modulo m, hence $p^{(m-1)/2} = -1$. This implies that the subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by p contains -1, and hence by Proposition 6.4 the polynomial Φ_m has a symmetric irreducible factor mod p. □

We start by noting that if N is sufficiently large, then property (P1′) holds.

Proposition 6.6 *Suppose that* $C(1) = C(-1) = 1$. *Let p be a prime number such that* $\Pi_{\Phi_{mp},\Phi_m} = \{p\}$. *If* $N > \deg(C) + \varphi(mp)$*, then there exist an even unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ of order mp such that*

- *The characteristic polynomial of t is divisible by C.*
- *The signature of the sublattice* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

Proof Set $F(x) = C(x)\Phi_{mp}(x)(x-1)^k$ with $k = N - \deg(C) - \varphi(mp)$. The polynomial F satisfies condition (C1). Since $\Pi_{\Phi_{mp},\Phi_m} = \{p\}$, we have $G_F = 0$. Therefore by Theorem 3.8 there exist a lattice L and an isometry t with the required properties.

Note that Proposition 6.4 implies that there exist infinitely many prime numbers p such that $\Pi_{\Phi_{mp},\Phi_m} = \{p\}$. In the following sections, we give conditions on N for the existence of an isometry *of order m*. □

7 $C(1) = C(-1) = 1$ and $c \equiv 0 \pmod 4$

We keep the notation of the previous sections and assume in addition that $C(1) = C(-1) = 1$; this implies that $\deg(C) \equiv 0 \pmod 4$ (see Lemma 4.1 (i)). Suppose that $c \equiv 0 \pmod 4$.

Corollary 6.2 implies that if $\deg(C) \equiv 0 \pmod 8$, then there exists an even, unimodular lattice L of signature (R, S) having an isometry $t \colon L \to L$ of order m such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$.

Suppose that $\deg(C) \equiv 4 \pmod 8$; then r is odd, and Lemma 4.1 implies that m is of one of the following forms:

- $m = 4p^k$ where p is a prime number with $p \equiv 3 \pmod 4$ and $k \geqslant 1$ is an integer;
- $m = p^k q^s$ where p and q are distinct prime numbers with $\equiv 3 \pmod 4$ and $k, s \geqslant 1$ are integers;
- $m = 2p^k q^s$ where p and q are distinct prime numbers with $\equiv 3 \pmod 4$ and $k, s \geqslant 1$ are integers.

Lemma 7.1 $N \geqslant \deg(C) + 4$.

Proof Let us show that $N \neq \deg(C) + 2$. Set $c' = \deg(C) - c$. We have $c \leqslant R$, $c' \leqslant S$ and $N = R + S$, $\deg(C) = c + c'$; moreover, c and c' are even. Therefore if $N = \deg(C) + 2$, then $R = c + 1$ and $S = c' + 1$. We have $R \equiv S \pmod 8$, hence this implies that $c \equiv c' \pmod 8$; but $\deg(C) = c + c'$ is congruent to $4 \pmod 8$, so this is impossible. Since N and $\deg(C)$ are both even, this implies that $N \geqslant \deg(C) + 4$, as claimed. □

Proposition 7.2 *Suppose that $m = 4p^k$ where p is a prime number with $p \equiv 3 \pmod 4$ and $k \geqslant 1$ is an integer. Then there exist an even unimodular lattice L of signature (R, S) and an isometry $t \colon L \to L$ of order m such that*

- *The characteristic polynomial of t is divisible by C.*

- *The signature of the sublattice* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

Proof Set $F = C\Phi_4^2(x-1)^{N-\deg(C)-4}$; note that Lemma 7.1 implies that $N-\deg(C)-4 \geqslant 0$, and that F satisfies condition (C1). Since $p \equiv 3 \pmod 4$, Φ_4 is irreducible mod p, and therefore $\Pi_{\Phi_m,\Phi_4} = \{p\}$. This implies that $G_F = 0$, and hence by Theorem 3.8 there exist a lattice L and an isometry t with the required properties.

If p and q are distinct prime numbers $\equiv 3 \pmod 4$, then by quadratic reciprocity either p is a square modulo q or q is a square modulo p, and these cases are mutually exclusive. Therefore we may assume that p is a square modulo q. □

Proposition 7.3 *Suppose that* $m = p^k q^s$ *or* $2p^k q^s$ *where* p *and* q *are distinct prime numbers with* $p, q \equiv 3 \pmod 4$ *and* $k, s \geqslant 1$ *are integers, and assume that* p *is a square modulo* q. *Suppose that* $N \geqslant \deg(C) + (p-1)p^{k-1} + 2$. *Then there exist an even unimodular lattice* L *of signature* (R, S) *and an isometry* $t\colon L \to L$ *of order* m *such that*

- *The characteristic polynomial of* t *is divisible by* C.
- *The signature of the sublattice* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

Proof Set $N' = N - \deg(C) - (p-1)p^{k-1} - 2$; set $F(x) = C(x)\Phi_{p^k}(x)(x-1)^{N'}$ if $m = p^k q^s$, and $F(x) = C(x)\Phi_{2p^k}(x)(x+1)^{N'}$ if $m = 2p^k q^s$. The polynomial F satisfies condition (C1), and Lemma 4.1 implies that $G_F = 0$. Theorem 3.8 implies that there exist a lattice L and an isometry t with the required properties. □

8 $C(1) = C(-1) = 1$ and $c \equiv 2 \pmod 4$

We keep the notation of Sect. 4; in particular, $C = \Phi_m^r$ where m, r are integers with $m \geqslant 3$ and $r \geqslant 1$. The case where $C(1)C(-1) > 1$ is covered by Theorem 6.1.

Assume now that $C(1) = C(-1) = 1$ and that $c \equiv 2 \pmod 4$. Since $C(1) = C(-1) = 1$, by Lemma 4.1 we have $\deg(C) \equiv 0 \pmod 4$; hence Lemma 6.3 implies that if $t\colon L \to L$ is an isometry of a lattice such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$, then L is indefinite. This implies that $R > 0$ and $S > 0$; recall that since $R \equiv S \pmod 8$, there exists up to isomorphism a unique even, unimodular lattice of signature (R, S) (see for instance [21, Chapter V]); we denote it by $\Lambda_{R,S}$.

In the applications to $K3$ surfaces, we have $R = 3$, $S = 19$, and $c = 2$.

Note that the case where $\deg(C) \equiv 4 \pmod 8$ was already handled in Corollary 6.2.

Proposition 8.1 *If* $\deg(C) \equiv 4 \pmod 8$ *then the lattice* $\Lambda_{R,S}$ *has an isometry* t *of order* m *such that the signature of* $\mathrm{Ker}(C(t))$ *is* $(c, \deg(C) - c)$.

Proof Indeed, we are assuming that $c \equiv 2 \pmod 4$, hence the hypothesis $\deg(C) \equiv 4 \pmod 8$ implies that $\deg(C) \equiv 2c \pmod 8$. Therefore by Corollary 6.2 there exist an even, unimodular lattice L and an isometry $t\colon L \to L$ of order m such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$. By Lemma 6.3, such a lattice is indefinite, hence L is isomorphic to $\Lambda_{R,S}$. □

Suppose that $\deg(C) \equiv 0 \pmod 8$. Recall that $N = R + S$. Using the results of [3] (in particular, Theorem 3.8) and Proposition 6.4 it is possible to determine the values of N for which $\Lambda_{R,S}$ has an isometry t of order m such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$; since this would be quite long, we only give some partial results that will be useful for the for the proof of Proposition 1.1.

Proposition 8.2 *Let $m = 2^n p$ with $n \geqslant 2$ and p be a prime number such that $p \equiv 3, 5 \pmod 8$, or $m = pq$ with p and q distinct prime numbers such that p is not a square modulo q. Suppose that $N \geqslant \deg(C) + p + 1$; set $M = N - \deg(C) - p + 1$ and $F(x) = C(x)\Phi_p(x)(x-1)^M$. Then $\Lambda_{R,S}$ has an isometry t with characteristic polynomial F such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$ and that the signature of $\mathrm{Ker}((t-1)^M)$ is $(1, M-1)$.*

Proof Since $C(1) = C(-1) = 1$, the polynomial F satisfies condition (C1). We have $G_F = 0$; indeed, by Corollary 6.5 we have $\Pi_{\Phi_m,\Phi_p} = \{2\}$ if $m = 2^n p$ and $\Pi_{\Phi_m,\Phi_p} = \{q\}$ if $m = pq$; moreover, $\Pi_{\Phi_p(x),x-1} = \{p\}$. Therefore by Theorem 3.8 there exists an isometry with the required properties. □

Proposition 8.3 *Let $m = 2pq$ with p and q distinct prime numbers such that p is not a square modulo q. Suppose that $N \geqslant \deg(C)+p+1$; set $M = N - \deg(C) - p - 1$ and $F(x) = C(x)\Phi_{2p}(x)(x+1)^2(x-1)^M$. Then $\Lambda_{R,S}$ has an isometry t with characteristic polynomial F such that the signature of $\mathrm{Ker}(C(t))$ is $(c, \deg(C) - c)$ and that the signature of $\mathrm{Ker}((t-1)^M)$ is $(1, M-1)$.*

Proof We have $\Pi_{\Phi_m,\Phi_{2p}} = \{q\}$ by Corollary 6.5, $\Pi_{\Phi_{2p}(x),x+1} = \{p\}$, $\Pi_{x+1,x-1} = \{2\}$, hence $G_F = 0$. The polynomial F satisfies condition (C1). Therefore by Theorem 3.8 there exists an isometry with the required properties. □

9 Salem polynomials and isometries of lattices

A *Salem polynomial* is a monic irreducible polynomial $S \in \mathbf{Z}[X]$ such that $S(X) = X^{\deg(S)}S(X^{-1})$ and that S has exactly two roots outside the unit circle, both positive real numbers.

Example 9.1 Let n be an integer $\geqslant 0$ and set

$$S_n(X) = X^6 - nX^5 - X^4 + (2n-1)X^3 - X^2 - nX + 1.$$

The polynomials S_n are Salem polynomials (see [16, Section 4] or [10, Section 7, Example 1]); we have $S_n(1) = -1$ and $S_n(-1) = 1$.

If $a\colon X \to X$ is an automorphism of a projective $K3$ surface, then the characteristic polynomial of $a^*\colon H^2(X, \mathbf{C}) \to H^2(X, \mathbf{C})$ is either a product of cyclotomic polynomials or it is of the form SC, where S is a Salem polynomial and C a product of cyclotomic polynomials (see [16, Theorem 3.2 and Corollary 3.3]).

We recall some notions and results from [3, Sections 7 and 12].

Notation 1 Let S be a Salem polynomial such that $S(1) = -1$ and $S(-1) = 1$, and let C be a cyclotomic polynomial. Let $\Pi_{S,C}$ be the set of prime numbers p such that $S \pmod p$ and $C \pmod p$ have a common irreducible symmetric factor in $\mathbf{F}_p[x]$.

Example 9.2 Let $S_2(x) = x^6 - 2x^5 - x^4 + 3x^3 - x^2 - 2x + 1$ (cf. Example 9.1) and let $C = \Phi_{60}$. The polynomials $S_2 \pmod{359}$ and $C \pmod{359}$ have the common irreducible factor $x^2 - 15x + 1$ in $\mathbf{F}_{359}[x]$; this polynomial is symmetric, hence $359 \in \Pi_{S,C}$.

Notation Let $F = SC$ for S and C as in Notation 1. We define a group G_F as in [3, Section 7] (see also Sect. 3); we have $G_F = 0$ if $\Pi_{S,C} \neq \varnothing$, and $G_F = \mathbf{Z}/2\mathbf{Z}$ if $\Pi_{S,C} = \varnothing$.

Proposition 9.3 *Let S be a Salem polynomial such that $S(1) = -1$ and $S(-1) = 1$, and let C be a cyclotomic polynomial; set $F = SC$. Suppose that $\deg(F) = 22$, that condition* (C1) *holds for F, and that $G_F = 0$. Then the lattice $\Lambda_{3,19}$ has an isometry t of signature map τ satisfying $\tau(C) = (2, \deg(C) - 2)$.*

Proof This is a consequence of [3, Corollary 12.3]. □

Example 9.4 Let $S(x) = S_2(x) = x^6 - 2x^5 - x^4 + 3x^3 - x^2 - 2x + 1$, and $C = \Phi_{60}$; set $F = SC$. We have $359 \in \Pi_{S,C}$ (cf. Example 9.2), therefore $G_F = 0$. Condition (C1) holds for F, hence by Proposition 9.3 the lattice $\Lambda_{3,19}$ has an isometry t with characteristic polynomial F such that the signature of $\mathrm{Ker}(C(t))$ is $(2, 14)$.

Example 9.5 Let $C = \Phi_{30}^2$ and $S_1(x) = x^6 - x^5 - x^4 + x^3 - x^2 - x + 1$, as in Example 9.1. We have $3 \in \Pi_{S_1,\Phi_{30}}$, hence $G_{S_1C} = 0$. Proposition 9.3 implies that $\Lambda_{3,19}$ has an isometry t such that the signature of $\mathrm{Ker}(C(t))$ is $(2, 14)$.

Example 9.6 Let $C = \Phi_{10}^4$. We have $S_0(x) = x^6 - x^4 - x^3 - x^2 + 1$ (cf. Example 9.1) and $3 \in \Pi_{S_0,\Phi_{10}}$, hence $G_{S_0C} = 0$. Proposition 9.3 implies that $\Lambda_{3,19}$ has an isometry t such that the signature of $\mathrm{Ker}(C(t))$ is $(2, 14)$.

Remark 9.7 The sets $\Pi_{S,C}$ of the above examples were computed by PARI GT.

Notation Let C be a cyclotomic polynomial and let S_n be as in Example 9.1. Let $N(C)$ be the set of integers $n \geqslant 0$ such that $\Pi_{C,S_n} \neq \varnothing$.

Example 9.8 Let $C = \Phi_{60}$. We have $0, 2, 5, 6, 7, \ldots \in N(C)$.

Question 9.9 Let C be a cyclotomic polynomial. Is the set $N(C)$ infinite?

10 Proof of Proposition 1.1—first part

In this section and the next one, we prove Proposition 1.1 from the introduction. Let m, r be integers with $m \geqslant 3$ and $r \geqslant 1$, and let $C = \Phi_m^r$. Assume that $\deg(C) \leqslant 20$.

Proposition 10.1 *There exists an automorphism $a\colon X \to X$ of a projective $K3$ surface X such that the characteristic polynomial of the restriction of a^* to T_X is equal to C.*

The proof of the proposition is divided into several parts, according to the value of m. Note first that if $m = p^k$ for some prime number $p \neq 2$, then Proposition 10.1 follows from Proposition 5.1.

Proposition 10.2 *Suppose that $m = p^k$ where p is a prime number, $p \neq 2$, and $k \geqslant 1$ is an integer. Then there exists an automorphism $a\colon X \to X$ of a projective $K3$ surface X such that the characteristic polynomial of the restriction of a^* to T_X is equal to C.*

Proof We have $C(1) = p^r$ and $C(-1) = 1$, hence Proposition 5.1 implies the existence of an automorphism $a\colon X \to X$ of a projective $K3$ surface X with the required properties. □

Proposition 10.3 *Suppose that $m = 2p^k$ where p is a prime number, and $k \geqslant 1$ is an integer. Suppose that r is even and that* $\deg(C) \equiv 4 \pmod 8$. *Then there exists an automorphism $a\colon X \to X$ of a projective $K3$ surface X such that the characteristic polynomial of the restriction of a^* to T_X is equal to C.*

Proof We have $C(1) = 1$ and $C(-1) = p^r$; since r is even, $C(-1)$ is a square, hence the conditions of Proposition 5.1 are satisfied; therefore this implies the existence of an automorphism $a\colon X \to X$ of a projective $K3$ surface X with the required properties. □

In the remaining cases, the proofs use modified versions of the results of the previous sections. The following lemma is based on results of McMullen in [17], and will be used in the proof of Proposition 10.1. Recall from [17, Section 2] that an isometry of a hyperbolic lattice is said to be *positive* if it stabilizes a chamber.

Lemma 10.4 *Let* (L, q) *be an even unimodular lattice of signature* $(3, 19)$ *and let $t\colon L \to L$ be an isometry of L. Let L_1 and L_2 be mutually orthogonal sublattices of L such that $L_1 \oplus L_2$ is of finite index in L, that $t(L_1) = L_1$, $t(L_2) = L_2$, that the signature of L_1 is* $(2, \operatorname{rank}(L_1) - 2)$ *and the signature of L_2 is* $(1, \operatorname{rank}(L_2) - 1)$. *Suppose moreover that the restriction of t to L_2 preserves a connected component of* $\{x \in L_2 \otimes_{\mathbf{Z}} \mathbf{R} \mid q(x, x) > 0\}$. *Then we have*

(i) *The lattice L has an isometry $t'\colon L \to L$ such that the restriction of t' to L_2 is positive, and that t' and t coincide on L_1.*
(ii) *Let $V \subset L_1 \otimes_{\mathbf{Z}} \mathbf{R}$ be a 2-dimensional subspace of signature* $(2, 0)$ *and stable by t such that the intersection of L with the orthogonal of V is equal to L_2 and that the restriction of t to V is in* $\mathrm{SO}(V)$. *Then there exist a projective $K3$ surface X and an automorphism $a\colon X \to X$ such that $T_X \simeq L_1$, $S_X \simeq L_2$, and $a^*|T_X = t$.*

Proof (i) Set $t_1 = t|L_1$ and $t_2 = t|L_2$. For $i = 1, 2$, set $\overline{L}_i = L_i^{\#}/L_i$, and let $\overline{q}_i$ and $\overline{t}_i$ be the induced symmetric bilinear forms and isometries; since L is unimodular, we have $(\overline{L}_1, \overline{q}_1, \overline{t}_1) \simeq (\overline{L}_2, -\overline{q}_2, \overline{t}_2)$. If L_2 has no roots, then t_2 is a positive isometry in the sense of McMullen [17, Section 2]; otherwise, let ρ be an element of the Weyl group of L_2 such that $\rho \circ t_2$ is positive. Set $t_2' = t_2$ in the first case, and $t_2' = \rho \circ t_2$ in the second one. The elements of the Weyl group of L_2 induce the identity on $\overline{L}_2$, hence we have $(\overline{L}_1, \overline{q}_1, \overline{t}_1) \simeq (\overline{L}_2, -\overline{q}_2, \overline{t}_2')$. This implies that there exists an isometry $t'\colon L \to L$ such that $t'|L_1 = t_1$ and $t'|L_2 = t_2'$; the isometry t_2' is positive, and this implies (i).

(ii) Applying [17, Theorem 6.1] to the isometry $t' \colon L \to L$ constructed in part (i), we conclude that there exist a projective $K3$ surface X with $T_X \simeq L_1$, $S_X \simeq L_2$, and an automorphism $a \colon X \to X$ such that $a^* = t'$. By construction, we have $t'|L_1 = t|L_1$, hence the restriction of a^* to T_X is equal to $t|L_1$. □

Proposition 10.5 *Suppose that $C(1) = C(-1) = 1$. Then there exists an automorphism $a \colon X \to X$ of a projective $K3$ surface X such that the characteristic polynomial of the restriction of a^* to T_X is equal to C.*

Proof If $\deg(C) \equiv 4 \pmod 8$, then this follows from Proposition 5.1. Suppose that $\deg(C) \equiv 0 \pmod 8$, and that $m \neq 30, 60$. Then we have $m = 15, 20, 24$ and $r = 1$ or 2, or $m = 40, 48$ and $r = 1$. By Proposition 8.2 the lattice $\Lambda_{3,19}$ has an isometry t such that the characteristic polynomial of t is divisible by C and by $(x-1)^4$, and that the signature of $\mathrm{Ker}(C(t))$ is $(2, \deg(C) - 2)$. The same property holds for $m = 30$ and $r = 1$ by Proposition 8.3. If $m = 60$, then by Example 9.4, the lattice $\Lambda_{3,19}$ has an isometry t such that the characteristic polynomial of t is CS_2; if $m = 30$ and $r = 2$, then this holds for CS_1 by Example 9.5.

Set $L_1 = \mathrm{Ker}(C(t))$ and let L_2 be the orthogonal complement of L_1 in L. The hypotheses of Lemma 10.4 are fulfilled; hence by Lemma 10.4 there exist a projective $K3$ surface X with $T_X = L_1$ and an automorphism $a \colon X \to X$ such that the characteristic polynomial of the restriction of a^* to T_X is equal to C. □

Proposition 10.6 *Let p be a prime number, let $r, k \geqslant 0$ be integers, and let $C = \Phi^r_{2p^k}$. Suppose that $\deg(C) \leqslant 16$, or r is even and $\deg(C) \leqslant 20$. Then there exists an automorphism $a \colon X \to X$ of a projective $K3$ surface X such that the characteristic polynomial of the restriction of a^* to T_X is equal to C.*

Proof The hypothesis implies that $C(1) = 1$ (if $p \neq 2$) or $C(1) = 2^r$ (if $p = 2$) and $C(-1) = p^r$. If r is odd, set $C'(x) = (x+1)^2(x-1)^{20-\deg(C)}$. If $C = \Phi_5^4$, set $C = S_0$ (cf. Example 9.1). Then CC' satisfies condition (C1) and $G_{CC'} = 0$, hence by Theorem 3.8 the lattice $\Lambda_{3,19}$ has an isometry with characteristic polynomial CC' such that the signature of $\mathrm{Ker}(C(t))$ is $(2, \deg(C) - 2)$. If r is even and $p = 2$ or deg $(C) \equiv 4 \pmod 8$, then the existence of such an isometry (with C' a power of $x - 1$) follows from Proposition 5.1. We conclude as in the proof of Proposition 10.5. □

11 Proof of Proposition 1.1—continued

The aim of this section is to prove Proposition 1.1 (that is, Proposition 10.1) in the remaining cases; the results are stated in a more general setting than needed.

Notation Let q be a prime number. If $V = (V, b)$ is a quadratic form over $\mathbf{Q}_q$, we denote by $d(V) \in \mathbf{Q}_q^\times / \mathbf{Q}_q^{\times 2}$ its determinant and by $w(V) \in \mathrm{Br}_2(\mathbf{Q}_q)$ its Hasse–Witt invariant.

Lemma 11.1 *Let V be a quadratic form over $\mathbf{Q}_2$. Then V contains an even, unimodular $\mathbf{Z}_2$-lattice if and only if*

- $\dim(V) \equiv 2 \pmod 4$*,* $d(V) = -1$ *and* $w(V) = 0$ *or* $d(V) = 3$ *and* $d(V) = 1$*;*
- $\dim(V) \equiv 0 \pmod 4$*,* $d(V) = 1$ *and* $w(V) = 1$ *or* $d(V) = 5$ *and* $d(V) = 0$*.*

Proof Let $H = \langle 1, -1 \rangle$ and $N = \langle 2, 6 \rangle$. By [8, Proposition 5.2], we see that V contains an even, unimodular $\mathbf{Z}_2$-lattice if and only if V is an orthogonal sum of copies of H and N; the lemma follows by computing the invariants of these orthogonal sums. □

Notation Let K be a field, and let E be an étale K-algebra with a K-linear involution $\sigma : E \to E$; set $E_0 = \{x \in E \mid \sigma(x) = x\}$. Let $\lambda \in E_0^{\times}$. We denote by b_λ the quadratic form $b_\lambda : E \times E \to K$ given by $b_\lambda(x, q) = \mathrm{Tr}_{E/K}(\lambda x \sigma y)$.

Proposition 11.2 *Let* p *be a prime number,* $p \neq 2$*, let* $r, k \geqslant 0$ *be integers, and let* $C = \Phi_{2p^k}^r$*. Suppose that if* r *is even, then* $\deg(C) \equiv 4 \pmod 8$*. The lattice* $(L, q) = \Lambda_{3,19}$ *has an isometry* t *with characteristic polynomial* CC'*, where* $C'(x) = (x^2 - 1)(x - 1)^{20-\deg(C)}$*, such that the sublattice* $\mathrm{Ker}(C(t))$ *has signature* $(2, 18)$ *and that the restriction of* t *to* $\mathrm{Ker}(C'(t))$ *stabilizes one of the connected components of* $\{x \in \mathrm{Ker}(C'(t)) \otimes_{\mathbf{Z}} \mathbf{R} \mid q(x, x) > 0\}$*.*

Proof Set $2n = 22 - \deg(C)$, and let U be the $\mathbf{Q}$-vector space with basis $e_1, \ldots, e_n, f_1, \ldots, f_n$; let $Q : U \times U \to \mathbf{Q}$ be the orthogonal sum of the quadratic form equal to $\langle 2, -2p^r \rangle$ on the subspace generated by e_1 and f_1, and of the diagonal form $\langle -2, \ldots, -2 \rangle$ on the subspace generated by e_i, f_j for $i, j \neq 1$. Let $T : U \to U$ be the isometry of Q given by $T(f_1) = -f_1$ and by $T(e_i) = e_i$ for all i, $T(f_i) = f_i$ if $i \neq 1$.

Suppose first that r is even. Since $C(1) = 1, C(-1) = p^r$ and $\deg(C) \equiv 0 \pmod 4$, the polynomial satisfies condition (C1). Moreover, $G_F = 0$, since C is a power of an irreducible polynomial. We are assuming that $\deg(C) \equiv 4 \pmod 8$, hence $\deg(C) - 2 \equiv 2 \pmod 8$. Therefore Theorem 3.8 implies that $\Lambda_{2,\deg(C)-2}$ has an isometry T' with characteristic polynomial C. Note that (U, Q) contains a lattice isomorphic to $\Lambda_{1,2n-1}$ stable by T, hence $\Lambda_{3,19}$ has an isometry with the required properties.

Assume now that r is odd. Set $F = \mathbf{Q}[x]/(\Phi_{2p^k})$ and let $\alpha \in F$ be the image of x. Let $\sigma_F : F \to F$ be the involution induced by $\alpha \mapsto \alpha^{-1}$ and let F_0 be the fixed field of this involution. Let E_0 be an extension of F_0 of degree r that is linearly independent of F over F_0, and set $E = E_0 \otimes_{F_0} F$. Then E is a field, and the characteristic polynomial of $\alpha \in E$ is equal to $C = \Phi_{2p^k}^r$. Let σ be the extension of σ_F to E.

If q is a prime number, set $E_q = E \otimes_{\mathbf{Q}} \mathbf{Q}_q$ and $(E_q)_0 = E_0 \otimes_{\mathbf{Q}} \mathbf{Q}_q$. With the notation of [4], let $\lambda_p \in (E_p)_0^{\times}$ be such that $\partial(E_p, b_{\lambda_p}, \alpha) = -\partial(U, Q, T)$; if $q \neq p$, let $\lambda_q \in (E_q)_0^{\times}$ be such that $\partial(E_q, b_{\lambda_q}, \alpha) = 0$ and that (E_q, b_{λ_q}) contains an even, unimodular $\mathbf{Z}_q$-lattice stabilized by α; this is possible by [4, Propositions 7.1 and 9.1] and the fact that $\det(E_q, b_{\lambda_q}) = p$ and $\deg(C) \equiv p - 1 \pmod 4$. Let $\lambda_\infty \in \mathbf{R}^{\times}$ be such that the signature of $(E \otimes_{\mathbf{Q}} \mathbf{R}, b_{\lambda_\infty})$ is equal to $(2, \deg(C) - 2)$.

For all prime numbers q, set $U_q = (U, Q) \otimes_{\mathbf{Q}} \mathbf{Q}_q$ and $W_q = (E_q, b_{\lambda_q})$; we have $d(U_q) = p$ and $d(W_q) = -p$. Note that this implies that $w(W_q \oplus U_q) = w(W_q) + W(U_q)$. If $q \neq 2, p$, we have $w(W_q) = w(U_q) = 0$.

Set $W_\infty = (E \otimes_{\mathbf{Q}} \mathbf{R}, b_{\lambda_\infty})$ and set $w(W_\infty) = w_2(W_\infty)$ in $\mathrm{Br}_2(\mathbf{R})$. We have $w(W_\infty) = 0 \iff p \equiv 3 \pmod 4 \iff n \equiv 0 \pmod 2$ and $w(W_\infty) = 1 \iff p \equiv 1 \pmod 4 \iff n \equiv 1 \pmod 2$.

By construction, $W_p \oplus U_p$ contains a unimodular lattice, hence $w(W_p) = w(U_p)$, and we have $w(U_p) = 0 \iff p \equiv \pm 1 \pmod 8$.

Together with Lemma 11.1, this allows us to compute $w(W_q)$ for all q, as follows.

Assume first that $p \equiv 3 \pmod 4$. Then $w(W_\infty) = 0$ and

$$w(W_p) = 0 \iff p \equiv 7 \pmod 8.$$

By Lemma 11.1, we have

$$w(W_2) = 0 \iff p \equiv 7 \pmod 8.$$

Since $w(W_q) = 0$ if $q \neq 2, p$, the sum of the invariants $w(W_q)$ (for q a prime number) and $w(W_\infty)$ is 0.

Suppose that $p \equiv 1 \pmod 4$. Then $w(W_\infty) = 1$ and

$$w(W_p) = 0 \iff p \equiv 1 \pmod 8.$$

By Lemma 11.1, we have

$$w(W_2) = 0 \iff p \equiv 5 \pmod 8.$$

Again, since $w(W_q) = 0$ if $q \neq 2, p$, the sum of the invariants $w(W_q)$ (for q a prime number) and $w(W_\infty)$ is 0.

We have $w_2(E_q, b_{\lambda_q}) = w(b_1) + \mathrm{cor}_{E_q/\mathbf{Q}_q}(\lambda_q, d)$ for all prime numbers q (see [3, Proposition 5.4]). Let $\mathcal{V}$ be the set of all places of $\mathbf{Q}$; since b_1 is a global form, the above argument shows that $\sum_{v \in \mathcal{V}} \mathrm{cor}_{E_v/\mathbf{Q}_v}(\lambda_p, d) = 0$. By [3, Theorem 9.6], this implies that there exists $\lambda \in E_0^\times$ such that $(E, b_\lambda) \otimes_{\mathbf{Q}} \mathbf{Q}_q \simeq (E_p, b_{\lambda_p})$ for all q.

Let (V, B, t) be the orthogonal sum of (E, b_λ, α) and (U, Q, T). Set $V_2 = (V, B) \otimes_{\mathbf{Q}} \mathbf{Q}_2$. We have $d(V) = -1$ and $w(V_2) = w(W_2) + w(U_2)$. Recall that $\deg(C) \equiv p - 1 \pmod 4$, hence $\dim(W_2) \equiv p - 1 \pmod 4$; we have $\dim(U) = 22 - \deg(C)$, hence $\dim(U) \equiv p + 1 \pmod 4$. This implies that

If $p \equiv 1 \pmod 4$, then

$$w(U_2) = 0 \iff p \equiv 1 \pmod 8 \quad \text{and} \quad w(W_2) = 0 \iff p \equiv 5 \pmod 8.$$

If $p \equiv 3 \pmod 4$, then

$$w(U_2) = 0 \iff p \equiv 3 \pmod 8 \quad \text{and} \quad w(W_2) = 0 \iff p \equiv 7 \pmod 8.$$

In both cases, we have $w(W_2) + w(U_2) = 1$, hence $w(V_2) = 1$.

The quadratic form V has determinant -1, signature $(3, 19)$, $w(V_2) = 1$ and all the other Hasse–Witt invariants of V are trivial. This implies that V is isomorphic to $\Lambda_{3,19} \otimes_{\mathbf{Z}} \mathbf{Q}$. The characteristic polynomial of t is CC'. The quadratic form V contains an even unimodular lattice stabilized by t everywhere locally; this is clear by construction at all prime numbers $q \neq 2$, and for $q = 2$ it follows from Takada [22, Theorem 4.2]. The intersection of these lattices is an even unimodular lattice stabilized by the isometry t; this lattice is isomorphic to $\Lambda_{3,19}$. By construction, t has the required properties. □

Proposition 11.3 *Let $C = \Phi^r_{2^k}$ with $k = 2$ and $r = 9$ or $k = 3$ and $r = 5$. Then the lattice $(L, q) = \Lambda_{3,19}$ has an isometry t with characteristic polynomial CC', where $C'(x) = (x^2 - 1)(x - 1)^{20-\deg(C)}$, such that the sublattice $\mathrm{Ker}(C(t))$ has signature $(2, 18)$ and that the restriction of t to $\mathrm{Ker}(C'(t))$ stabilizes one of the connected components of $\{x \in \mathrm{Ker}(C'(t)) \otimes_{\mathbf{Z}} \mathbf{R} \mid q(x, x) > 0\}$.*

Proof Set $E = \mathbf{Q}/[x]/(\Phi_{2^k})$ with $k = 2$ or $k = 4$. We denote by $x \mapsto \overline{x}$ the complex conjugation and let E_0 be the fixed subfield of E: we have $E_0 = \mathbf{Q}$ if $r = 2$ and $E_0 = \mathbf{Q}(\sqrt{2})$ if $k = 4$.

Suppose first that $k = 2$, and let $X = (X, q_X, t_X)$ be defined by $X = E, q_X(x, y) = \mathrm{Tr}_{E/\mathbf{Q}}(\frac{1}{2}x\overline{y})$; let t_X be induced by multiplication by $i = \zeta_4$; note that t_X is an isometry of q_X with characteristic polynomial Φ_4. Let $W_2 = (W_2, q_2, t_2)$ be the orthogonal sum of a copy of X with 9 copies of $-X$. We have $\dim(W_2) = 18$, $d(W_2) = 1$, and $w(W_2) = 0$. The signature of W_2 is $(2, 16)$, and the characteristic polynomial of t_2 is Φ_4^9.

Let U_2 be the $\mathbf{Q}$-vector space of basis e_1, e_2, f_1, f_2 and $q_2 \colon U_2 \times U_2 \to \mathbf{Q}$ be the quadratic form such that $q_2(e_1, e_1) = 1$ and $q_2(f_1, f_1) = q_2(e_2, e_2) = q_2(f_2, f_2) = -1$. Let $t_2 \colon U_2 \to U_2$ be the isometry given by $t_2(f_2) = -f_2$ and $t_2(e_i) = e_i$ for $i = 1, 2$, $t_2(f_2) = f_2$. We have $\dim(U_2) = 4$, $d(U_2) = -1$, $w(U_2) = 1$ at 2 and ∞, and 0 elsewhere.

If $k = 2$, we set $(V, q, t) = (W_2, q_2, t_2) \oplus (U_2, q_2, t_2)$. The signature of V is $(3, 19)$, and $d(V) = -1$, $w(V) = 1$ at 2 and ∞, and 0 elsewhere. The characteristic polynomial of t is $\Phi_4^9(x)(x^2 - 1)(x - 1)^2$.

Assume now that $k = 4$. Let $X = (X, q_X, t_X)$ be defined by $X = E$, $q_X(x, y) = \mathrm{Tr}_{E/\mathbf{Q}}\big(\frac{\sqrt{2}}{4}x\overline{y}\big)$; let t_X be induced by multiplication by ζ_8; note that t_X is an isometry of q_X with characteristic polynomial Φ_8. Let $Y = (Y, q_Y, t_Y)$ be defined by $Y = E$, $q_Y(x, y) = \mathrm{Tr}_{E/\mathbf{Q}}\big(\frac{1}{4}x\overline{y}\big)$; let t_Y be induced by multiplication by ζ_8. Let $W_4 = (W_4, q_4, t_4)$ be the orthogonal sum of X with 4 copies of $-Y$. We have $\dim(W_4) = 20$, $d(W_2) = 1$, and $w(W_2) = 1$ at 2 and at ∞, and 0 elsewhere. The signature of W_2 is $(2, 18)$, and the characteristic polynomial of t_2 is Φ_8^5.

Let U_2 be the $\mathbf{Q}$-vector space of basis e_1, f_1 and $q_2 \colon U_2 \times U_2 \to \mathbf{Q}$ be the quadratic form such that $q_2(e_1, e_1) = 1$ and $q_2(f_1, f_1) = -1$. Let $t_2 \colon U_2 \to U_2$ be the isometry given by $t_2(f_2) = -f_2$ and $t_2(e_1) = e_1$. We have $\dim(U_2) = 2$, $d(U_2) = -1$, $w(U_2) = 0$.

If $k = 2$, we set $(V, q, t) = (W_2, q_2, t_2) \oplus (U_2, q_2, t_2)$. The signature of V is $(3, 19)$, and $d(V) = -1$, $w(V) = 1$ at 2 and ∞, and 0 elsewhere. The characteristic polynomial of t is $\Phi_4^9(x)(x^2 - 1(x - 1)^2)$.

If $k = 4$, we set $(V, q, t) = (W_4, q_4, t_4) \oplus (U_4, q_4, t_4)$. The signature of V is $(3, 19)$, and $d(V) = -1$, $w(V) = 1$ at 2 and ∞, and 0 elsewhere. The characteristic polynomial of t is $\Phi_8^5(x)(x^2 - 1)$.

In both cases, (V, q, t) contains an even unimodular lattice stabilized by t everywhere locally; at the prime 2, this follows from Takada [22, Theorem 4.2]. Let L be the intersection of these lattices; L is stabilized by t, and we have $L \simeq \Lambda_{3,19}$. □

Proof of Proposition 10.1 If $m = p^k$ where p is a prime number with $p \neq 2$, then the proposition follows from Proposition 10.2; if $C(1) = C(-1)$, then from Proposition 10.5. Suppose that $C = \Phi^r_{2p^k}$. If r is even of if $\deg(C) \leqslant 16$, it is a consequence of Proposition 10.6. Suppose that r is odd and that $\deg(C) = 18$ or 20; apply Proposition 11.2 f $p \neq 2$, and Proposition 11.3 if $p = 2$. □

Proposition 10.1 implies the following result.

Corollary 11.4 *Let m be an integer such that $m \geqslant 1$ and that $\varphi(m) \leqslant 20$. Then there exists an automorphism $a \colon X \to X$ of a projective $K3$ surface X inducing multiplication by a primitive m-th root of unity on T_X.*

Proof For $m = 1$, we can take the identity, and there are many examples of automorphisms of projective $K3$ surfaces X inducing $-\mathrm{id}$ on T_X (see for instance [11, Corollary 15.2.12]). Suppose that $m \geqslant 3$, and let $C = \Phi_m$; Proposition 10.1 implies that there exists an automorphism $a \colon X \to X$ of a projective $K3$ surface such that the characteristic polynomial of $a^*|T_X$ is equal to C; hence $a^*|T_X$ acts by multiplication by a primitive m-th root of unity. □

Remark 11.5 Corollary 11.4 follows from results of Machida–Oguiso [15], Xiao [25], and Zhang [26] when $m \neq 60$; more precisely, they prove the existence of an automorphism $a \colon X \to X$ of *finite order* inducing multiplication by a primitive m-th root of unity on T_X. They also show that this is not the case for $m = 60$; in the next section we give another proof of this result.

12 The primitive 60-th roots of unity

The following result was proved by Machida–Oguiso [15], Xiao [25], and Zhang [26].

Proposition 12.1 *There does not exist any automorphism of finite order of a projective $K3$ surface inducing multiplication by a primitive* 60*-th root of unity on its transcendental lattice.*

The aim of this section is to give another proof of Proposition 12.1. Set $C = \Phi_{60}$.

Proposition 12.2 *Let L be an even unimodular lattice of signature* (3, 19)*. The lattice L does not have any isometry $t \colon L \to L$ having the following properties:*

(i) *The characteristic polynomial of t is CC', where C' is a product of cyclotomic polynomials.*
(ii) *The signature of the sublattice $L_C = \mathrm{Ker}(C(t))$ of L is* (2, 14).

The main ingredient of the proof of Proposition 12.2 is the following lemma.

Lemma 12.3 *Set $C' = \Phi_{12}$ and let M be an even unimodular lattice of signature* $(2, 18)$. *The lattice M does not have any isometry $t: M \to M$ having the following properties:*

(i) *The characteristic polynomial of t is CC'.*
(ii) *The signature of the sublattice $M_C = \mathrm{Ker}(C(t))$ of M is* $(2, 14)$.

We give two proofs of this lemma; the first one is based on some results of [3], the second one is a direct proof.

First proof of Lemma 12.3 Set $F = CC'$ and note that F satisfies condition (C1). By Example 3.4, we have $G_F = \mathbf{Z}/2\mathbf{Z}$.

Set $I = \{C, C'\}$. Since $G_F = \mathbf{Z}/2\mathbf{Z}$, we have $C_0(I) = C(I)$. Let $c: I \to \mathbf{Z}/2\mathbf{Z}$ be such that $c(C) = 1$ and $c(C') = 0$, and let $c': I \to \mathbf{Z}/2\mathbf{Z}$ be such that $c'(C) = 0$ and $c'(C') = 1$.

As in [3, Sections 9 and 12], we define a homomorphism $\epsilon_F^{\text{finite}}: C(I) \to \mathbf{Z}/2\mathbf{Z}$.

Let τ be a signature map with characteristic polynomial F and maximum $(2, 18)$ such that $\tau(C) = (2, 14)$ and $\tau(C') = (0, 4)$, and let $\epsilon_\tau^\infty: C(I) \to \mathbf{Z}/2\mathbf{Z}$ be the associated homomorphism (see [3, Sections 9 and 12]). We obtain a homomorphism $\epsilon_\tau: G_F \to \mathbf{Z}/2\mathbf{Z}$ by setting $\epsilon_\tau = \epsilon_F^{\text{finite}} + \epsilon_\tau^\infty$. By [3, Theorem 12.1], there exists an even unimodular lattice M having an isometry $t: M \to M$ with properties (i) and (ii) if and only if $\epsilon_\tau = 0$.

With the notation of [3, Section 9], we have $a_\tau^\infty(C) = 1$ and $a_\tau^\infty(C') = 0$. This implies that $\epsilon_\tau^\infty(c) = 1$ and $\epsilon_\tau^\infty(c') = 0$.

Similarly, let τ' be a signature map with characteristic polynomial F and maximum $(2, 18)$ such that $\tau(C) = (0, 16)$ and $\tau(C') = (2, 2)$, and let $\epsilon_\tau^\infty: C(I) \to \mathbf{Z}/2\mathbf{Z}$ be the associated homomorphism. We have $a_{\tau'}^\infty(C) = 0$ and $a_{\tau'}^\infty(C') = 1$, hence $\epsilon_{\tau'}^\infty(c) = 0$ and $\epsilon_{\tau'}^\infty(c') = 1$. We obtain a homomorphism $\epsilon_{\tau'}: G_F \to \mathbf{Z}/2\mathbf{Z}$ by setting $\epsilon_{\tau'} = \epsilon_F^{\text{finite}} + \epsilon_{\tau'}^\infty$.

Both C and C' satisfy condition (C 1), and since they are irreducible, we have $G_C = G_{C'} = 0$. Therefore by Theorem 3.5 there exists an even unimodular lattice N of signature $(0, 16)$ having an isometry with characteristic polynomial C, and an even unimodular lattice N' of signature $(2, 2)$ having an isometry with characteristic polynomial C'. The lattice $N \oplus N'$ is even unimodular of signature $(2, 18)$, and has an isometry of characteristic polynomial F and of signature map τ'. Applying [3, Theorem 12.1], this implies that $\epsilon_{\tau'} = 0$. Since $\epsilon_{\tau'} = \epsilon_F^{\text{finite}} + \epsilon_{\tau'}^\infty$, we have $\epsilon_F^{\text{finite}}(c) = 0$ and $\epsilon_F^{\text{finite}}(c') = 1$.

On the other hand, we have $\epsilon_\tau = \epsilon_F^{\text{finite}} + \epsilon_\tau^\infty$, and this implies that $\epsilon_\tau \neq 0$; therefore there does not exist any even unimodular lattice M having an isometry $t: M \to M$ with properties (i) and (ii). □

The second proof of Lemma 12.3 uses the notion of Hasse–Witt invariant of a quadratic form.

Notation Let K be a field of characteristic $\neq 2$, let V be a finite-dimensional K-vector space, and let $q: V \times V \to K$ be a non-degenerate quadratic form. The Hasse–Witt invariant of q is denoted by $w_2(q)$; it is an element of $\mathrm{Br}_2(K)$.

If K is a p-adic field or $\mathbf{R}$, then $\mathrm{Br}_2(K)$ is a group of order two, that we identify with $\{0, 1\}$; see [21, Chapitre IV] for the properties of Hasse–Witt invariants of quadratic forms that are needed here.

Second proof of Lemma 12.3 Set $F = CC'$. Suppose that the even unimodular lattice (M, q) of signature $(2, 18)$ has an isometry $t \colon M \to M$ with characteristic polynomial F, and let us show that (ii) does not hold.

Set $M_1 = \mathrm{Ker}(C(t))$ and let q_1 be the restriction of q to $M_1 \times M_1$; similarly, set $M_2 = \mathrm{Ker}(C'(t))$ and let q_2 be the restriction of q to $M_2 \times M_2$. Set $V = M \otimes_{\mathbf{Z}} \mathbf{Q}$, $V_1 = M_1 \otimes_{\mathbf{Z}} \mathbf{Q}$, and $V_2 = M_2 \otimes_{\mathbf{Z}} \mathbf{Q}$. Since C and C' are distinct irreducible polynomials, the quadratic space (V, q) is the orthogonal sum of (V_1, q_1) and (V_2, q_2).

The resultant of C and C' is 5^4. This implies that if p is a prime number with $p \neq 5$, then $(M, q) \otimes_{\mathbf{Z}} \mathbf{Z_p}$ is the orthogonal sum of $(M_1, q_1) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ and $(M_2, q_2) \otimes_{\mathbf{Z}} \mathbf{Z}_p$; therefore the $\mathbf{Z_p}$-lattices $(M_1, q_1) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ and $(M_2, q_2) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ are unimodular.

Let p be a prime number $p \neq 2, 5$. Since $(V_1, q_1) \otimes_{\mathbf{Q}} \mathbf{Q}_p$ and $(V_2, q_2) \otimes_{\mathbf{Q}} \mathbf{Q}_p$ contain unimodular $\mathbf{Z}_p$-lattices, we have $w_2(q_1) = w_2(q_2) = 0$ in $\mathrm{Br}_2(\mathbf{Q}_p)$.

Let U be the hyperbolic plane; if n is an integer with $n \geqslant 1$, we denote by U^n the orthogonal sum of n copies of U. Since $(M_1, q_1) \otimes_{\mathbf{Z}} \mathbf{Z}_2$ and $(M_2, q_2) \otimes_{\mathbf{Z}} \mathbf{Z}_2$ are unimodular, we have $(M_1, q_1) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq U^8 \otimes_{\mathbf{Z}} \mathbf{Z}_2$ and $(M_2, q_2) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq U^2 \otimes_{\mathbf{Z}} \mathbf{Z}_2$ (see for instance [8, Proposition 5.2]). This implies that $w_2(q_1) = 0$ and $w_2(q_2) = 1$ in $\mathrm{Br}_2(\mathbf{Q}_2)$.

Let K be the cyclotomic field of the 12-th roots of unity and let K_0 be its maximal real subfield. The prime 5 is inert in the extension $K_0/\mathbf{Q}$, and splits in K/K_0. This implies that there exists a degree 2 polynomial $f \in \mathbf{Z}_5[x]$ such that $C' = ff^*$ in $\mathbf{Z}_5[x]$, where $f^*(x) = x^2 f(x^{-1})$, and such that $f \neq f^*$. Let us denote by t_2 the restriction of t to V_2, and note that $\mathrm{Ker}(f(t_2))$ is an isotropic subspace of dimension 2 of $V_2 \otimes_{\mathbf{Q}} \mathbf{Q}_5$; this implies that $(V_2, q_2) \otimes_{\mathbf{Q}} \mathbf{Q}_5 \simeq U^2 \otimes_{\mathbf{Q}} \mathbf{Q}_5$, and therefore $w_2(q_2) = 0$ in $\mathrm{Br}_2(\mathbf{Q}_5)$.

Suppose that (ii) holds. Then the signature of (V_1, q_1) is $(2, 14)$, and the signature of (V_2, q_2) is $(0, 4)$; hence $w_2(q_2) = 0$ in $\mathrm{Br}_2(\mathbf{R})$. This leads to a contradiction, since $w_2(q_2) = 1$ in $\mathrm{Br}_2(\mathbf{Q}_2)$, and $w_2(q_2) = 0$ in $\mathrm{Br}_2(\mathbf{Q}_p)$ for all prime numbers p with $p \neq 2$. □

Proof of Proposition 12.2 Let C' be a product of cyclotomic polynomials and let $t \colon L \to L$ be an isometry with characteristic polynomial CC', and set $F = CC'$. Suppose first that C' is not divisible by Φ_{12}. Then C and C' are relatively prime over $\mathbf{Z}$. Indeed, $\deg(C') = 6$, and if Φ is a cyclotomic polynomial of degree $\leqslant 6$ such that Φ is not relatively prime to C over $\mathbf{Z}$, then $\Phi = \Phi_{12}$; this follows from the values of the resultants of cyclotomic polynomials, see for instance [1]. Since C and C' are relatively prime over $\mathbf{Z}$, the lattice L is the orthogonal sum of the even unimodular lattices L_C and $\mathrm{Ker}(C'(t))$. If (ii) holds, then the signature of L_C is $(2, 14)$; this contradicts the fact that L_C is an even unimodular lattice.

Assume now that Φ_{12} divides C'. The polynomial F satisfies condition (C1); this implies that $C' = \Phi_{12} C''$ such that the irreducible factors of C'' are in $\{x - 1, x + 1\}$. Therefore C'' is relatively prime over $\mathbf{Z}$ to $C\Phi_{12}$. Set $M = \mathrm{Ker}(C\Phi_{12}(t))$ and $M' = \mathrm{Ker}(C''(t))$. The lattice L is the orthogonal sum of M and M', hence both these lattices are even and unimodular. This implies that the signature of M' is $(1, 1)$, and hence the signature of M is $(2, 14)$. By Lemma 12.3, this is impossible. □

Proof of Proposition 12.1 Let $a\colon X \to X$ be an automorphism of a projective $K3$ surface such that a^* induces multiplication by a primitive 60-th root of unity on T_X. This implies that the characteristic polynomial of $a^*|T_X$ is equal to Φ_{60}. Assume that a is of finite order. Then the characteristic polynomial of $a^*|S_X$ is a product of cyclotomic polynomials. Since $T_X = \mathrm{Ker}(\Phi_{60}(a^*))$, the signature of the lattice $\mathrm{Ker}(\Phi_{60}(a^*))$ is $(2, 14)$. Proposition 12.2 implies that this is impossible, hence no such automorphism exists. □

13 Two cyclic groups

Recall from the introduction that if X is a projective $K3$ surface, we have the exact sequences

$$1 \to \mathrm{Aut}_s(X) \to \mathrm{Aut}(X) \to M_X \to 1$$

and

$$1 \to N_X \to \mathrm{Aut}(X) \to \mathrm{O}(S_X),$$

where M_X and N_X are finite cyclic groups, of order m_X, respectively n_X. The group N_X can be identified to a subgroup of M_X, hence n_X divides m_X.

The question of determining the possible values of m_X and n_X was raised by Huybrechts in [11, p. 336]; the characterization of the pairs (m_X, n_X) is also of interest.

The values of n_X were studied much earlier, by Vorontsov [23], Kondō [12], and Oguiso–Zhang [20]; assuming that $\mathrm{rank}(T_X) = \varphi(n_X)$, they give a complete list of these values (see Corollary 13.6 below).

We start with the integers m_X. The following is Corollary 1.2 from the introduction.

Corollary 13.1 *Let $m \geqslant 2$ be an even integer such that $\varphi(m) \leqslant 20$. Then there exists a projective $K3$ surface X with $m_X = m$.*

Proof There exist projective $K3$ surfaces X with $m_X = 2$, see for instance [11, Corollary 15.2.12]. Suppose that $m \geqslant 4$. By Proposition 10.1 there exist a projective $K3$ surface X and an automorphism $a\colon X \to X$ such that the characteristic polynomial of the restriction of a^* to T_X is Φ_m. Since m is even, we have $m_X = m$. □

Remark 13.2 In [15], Machida and Oguiso consider a related problem; they are interested in the images of the *finite subgroups* of $\mathrm{Aut}(X)$ in M_X. Their results imply that there exist projective $K3$ surfaces X with $m_X = 28, 30, 32, 34, 38, 40, 42, 44, 48, 54$ and 66 (see [15, Proposition 4]).

The possible values of n_X can be deduced from Proposition 5.1. As we will see, it is enough to consider $K3$ surfaces X such that $\mathrm{rank}(T_X) = \varphi(n_X)$ or $\mathrm{rank}(T_X) = 2\varphi(n_X)$.

Proposition 13.3 *Let m be an integer with $m \geqslant 1$ and $\varphi(m) \leqslant 20$. The following are equivalent:*

(i) *There exists a projective $K3$ surface X such that $n_X = m$.*
(ii) *There exists a projective $K3$ surface X such that $n_X = m$ and* $\mathrm{rank}(T_X) = \varphi(m)$ *or* $\mathrm{rank}(T_X) = 2\varphi(m)$.

This will be proved at the end of the section.

We start with the case where C is a cyclotomic polynomial, i.e. when the rank of T_X is $\varphi(n_X)$.

Corollary 13.4 *Let m be an integer such that $m \geqslant 3$ and that $\varphi(m) \leqslant 20$; set $C = \Phi_m$. There exists a projective $K3$ surface X such that $n_X = m$ and the rank of T_X is $\varphi(n_X)$ if and only if the following conditions hold:*

(i) $C(-1) = 1$.
(ii) *If* $C(1) = 1$, *then* $m \equiv 0 \pmod 2$ *and* $\deg(C) \equiv 4 \pmod 8$.

The $K3$ surface is unique up to isomorphism. Moreover, the lattice T_X is unimodular if and only if $C(1) = 1$, and p-elementary with $p = C(1)$ if $C(1) > 1$.

Proof Suppose that conditions (i) and (ii) hold. Then by Proposition 5.1, there exists an automorphism $a\colon X \to X$ of a projective $K3$ surface such that the restriction of a^* is the identity and that the characteristic polynomial of $a^*|T_X$ is equal to C; this implies that m divides n_X. Since $C = \Phi_m$, the rank of T_X is equal to $\varphi(m)$; hence $\varphi(m) = \varphi(n_X)$. Suppose that $C(1) > 1$; then $m = p^r$, where p is an odd prime number (cf. Lemma 4.1). Then either $n_X = m$ or $n_X = 2m$; but Φ_{2p^r} does not satisfy (i), hence $n_X \neq 2p^r$, and this implies that $n_X = m$. Assume now that $C(1) = 1$. By (ii), we have $m \equiv 0 \pmod 2$; since m divides n_X and $\varphi(m) = \varphi(n_X)$, this implies that $n_X = m$.

Conversely, suppose that there exists a projective $K3$ surface X such that $n_X = m$ and $\mathrm{rank}(T_X) = \varphi(m)$, and let a be a generator of the cyclic group N_X. Then the restriction of a^* to S_X is the identity and the characteristic polynomial of $a^*|T_X$ is equal to C. Therefore Proposition 5.1 (i) implies that $C(-1)$ is a square; since C is a cyclotomic polynomial, we have $C(-1) = 1$, hence (i) holds. Proposition 5.1 (ii) implies that if $C(1) = 1$, then $\deg(C) \equiv 4 \pmod 8$. Moreover, the hypothesis $C(1) = 1$ implies that T_X is unimodular; this implies that $n_X \equiv 0 \pmod 2$, hence $m \equiv 0 \pmod 2$, and therefore (ii) holds.

The uniqueness of the $K3$-surface follows from Proposition 5.1. If $C(1) = 1$ then T_X is unimodular (cf. Proposition 5.1). Conversely, suppose that T_X is unimodular; then C satisfies condition (C1). Since C is a cyclotomic polynomial, this implies that $C(1) = 1$. If $C(1) > 1$, then by Proposition 5.2 the lattice T_X is p-elementary with $p = C(1)$. Conversely, if T_X is p-elementary, then by Proposition 5.1 we have $C(1) > 1$. □

Using Corollary 13.4, we recover the lists of Vorontsov [23] and Kondō [12], as follows. Set

$$A = \{12,\ 28,\ 36,\ 42,\ 44,\ 66\} \quad \text{and} \quad B = \{3,\ 9,\ 27,\ 5,\ 25,\ 7,\ 11,\ 13,\ 17,\ 19\}.$$

Lemma 13.5 *Let m be an integer such that $m \geqslant 3$ and that $\varphi(m) \leqslant 20$. Then we have*

$$m \in A \iff \Phi_m(1) = \Phi_m(-1) = 1,\ m \text{ is even, and } \deg(C) \equiv 4 \pmod 8,$$
$$m \in B \iff \Phi_m(-1) = 1 \text{ and } \Phi_m(1) > 1.$$

Proof This follows from Lemma 4.1. □

Combining Corollary 13.4 and Lemma 13.5, we obtain

Corollary 13.6 (Kondō, Vorontsov) *Let $m \in A \cup B$. Then there exists a projective $K3$ surface X such that $n_X = m$ and that the rank of $T_X(X)$ is equal to $\varphi(n_X)$. Moreover, X is unique up to isomorphism, and*

$$n_X \in A \iff \text{the lattice } T_X \text{ is unimodular},$$
$$n_X \in B \iff \text{the lattice } T_X \text{ is } p-\text{elementary with } p = \Phi_{n_X}(1).$$

Proof See [12, 23]; this also follows from Corollary 13.4 and Lemma 13.5. □

We now consider the case where $\operatorname{rank}(T_X) = 2\varphi(n_X)$.

Corollary 13.7 *Let m be an integer such that $m \geqslant 3$, that $m \equiv 0 \pmod 2$, and that $\varphi(m) \leqslant 10$. Suppose that if $\Phi_m(1) = 1$, then $\varphi(m) \equiv 2 \pmod 4$. Then there exist infinitely many projective $K3$ surfaces X such that $n_X = m$, and that* $\operatorname{rank}(T_X) = 2\varphi(m)$.

Proof Set $C = \Phi_m^2$ and note that C satisfies conditions (i) and (ii) of Proposition 5.1. Therefore there exist infinitely many projective $K3$ surfaces X having automorphisms $a \colon X \to X$ such that $a^*|S_X$ is the identity, and that the characteristic polynomial of $a^*|T_X$ is C. If m is a power of 2, then $m = n_X$. Otherwise, we have $m = 2m'$ where $m' = 3, 7, 9$ or 11; therefore $n_X = m$ or $n_X = 2m = 4m'$.

If Y is a $K3$ surface with $n_Y = 4m'$ and $\operatorname{rank}(T_Y) = 2\varphi(m) = \varphi(4m')$, then Y has an automorphism $b \colon Y \to Y$ such that $b^*|T_Y$ is the identity and the characteristic polynomial of $b^*|T_Y$ is $C' = \Phi_{4m'}$; by Corollary 13.4, the surface Y is unique up to isomorphism.

Therefore there exist infinitely many non-isomorphic projective $K3$ surfaces X such that $n_X = m$. □

Set $C = \{4, 6, 8, 14, 16, 18, 22\}$.

Lemma 13.8 *Let m be an integer such that $m \geqslant 3$ and that $\varphi(m) \leqslant 10$. We have*

$$m \in C \iff m \text{ is even, and if } \Phi_m(1) = 1, \text{ then } \varphi(m) \equiv 2 \pmod 4.$$

Proof This follows from Lemma 4.1. □

Corollary 13.7 and Lemma 13.8 imply the following

Corollary 13.9 *If $m \in C$, then there exist infinitely many projective $K3$ surfaces X such that $n_X = m$, and that* $\operatorname{rank}(T_X) = 2\varphi(n_X)$.

Finally, we show that Corollaries 13.4 and 13.7 characterize the possible values of n_X. We start with a lemma.

Lemma 13.10 *Let m, r be integers with $m \geqslant 3$ and $r \geqslant 1$, and let $C = \Phi_m^r$. Conditions* (i) *and* (ii) *of Proposition 5.1 hold for C if and only if*

(i) $r \equiv 1 \pmod 2$*,* $\Phi_m(-1) = 1$ *and if* $\Phi_m(1) = 1$*, then* $\varphi(m) \equiv 4 \pmod 8$.
(ii) $r \equiv 2 \pmod 4$*, and if* $\Phi_m(1) = 1$*, then* $\varphi(m) \equiv 2 \pmod 4$.
(iii) $r \equiv 0 \pmod 4$*, and* $\Phi(1) > 1$.

Proof This is a straightforward verification, using Lemma 4.1. □

Corollary 13.11 *Let m be an integer such that $m \geqslant 3$ and that $\varphi(m) \leqslant 20$. There exists a projective $K3$ surface X with $n_X = m$ and* $\mathrm{rank}(T_X) = r\varphi(n_X)$ *if and only if*

(i) $r = 1$ *and* $m \in A \cup B$.
(ii) $r = 2$ *and* $m \in C \cup \{3, 5, 7, 11\}$.
(iii) $r = 3$ *and* $m \in \{3, 5, 7, 9, 12\}$.
(iv) $r = 4$ *and* $m \in \{3, 4, 5, 8\}$.
(v) $r = 5$ *and* $m \in \{3, 5\}$.
(vi) $r = 6$ *or* 10 *and* $m \in \{3, 4, 6\}$.
(vii) $r = 8$ *and* $m \in \{3, 4\}$.
(viii) $r = 7$ *or* 9 *and* $m = 3$.

Proof This follows from Proposition 5.1 and Lemma 13.10. □

Corollary 13.12 *Let m be an integer such that $m \geqslant 3$ and that $\varphi(m) \leqslant 20$. There exists a projective $K3$ surface X with $n_X = m \iff m \in A \cup B \cup C$.*

Proof This is an immediate consequence of Corollary 13.11. □

Proof of Proposition 13.3 It is clear that (ii)⇒(i). Suppose (i). Then by Corollary 13.12, we have $n_X \in A \cup B \cup C$, and (i) follows from Corollaries 13.6 and 13.9. □

Notation If X is a $K3$ surface, set $r_X = \frac{\mathrm{rank}(T_X)}{\varphi(n_X)}$ and $t_X = \frac{\mathrm{rank}(T_X)}{\varphi(m_X)}$.

Corollary 13.11 characterizes the possible pairs (n_X, r_X). This suggests the following question.

Question 13.13 What are the possibilities for (n_X, m_X, r_X, t_X)?

Huybrechts asked for explicit examples of $K3$ surfaces with $m_X > n_X$ (see [11, Remark 15.1.13]). The following construction is due to Brandhorst and Elkies [7].

Example 13.14 Let X be the $K3$ surface constructed by Brandhorst and Elkies in [7]. This surface has an automorphism $a \colon X \to X$ such that the characteristic polynomial of $a^*|T_X$ is Φ_{14} (see [7, Section 3]), hence $m_X = 14$. Since $14 \notin A \cup B$, we have $n_X \neq 14$, therefore $n_X < m_X$.

This implies that $n_X = 7, 2$ or 1. The results of Vorontsov [23] and Oguiso–Zhang [20] imply that up to isomorphism, there exists a unique projective $K3$ surface Y such that $\mathrm{rank}(T_Y) = 6$ and $n_Y = 7$ (note that this also follows from Proposition 13.4); the discriminant of S_Y is equal to 7 (see [20, Lemma 1.3]). For the $K3$ surface X constructed by Brandhorst and Elkies, the discriminant of S_X is 7.13^2, hence X and Y are not isomorphic; therefore $n_X \neq 7$. One can show that $n_X = 1$.

Funding Open access funding provided by EPFL Lausanne

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The author declares no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Apostol, T.M.: Resultants of cyclotomic polynomials. Proc. Amer. Math. Soc. **24**(3), 457–462 (1970)
2. Bayer-Fluckiger, E.: Isometries of lattices and Hasse principles. J. Eur. Math. Soc. https://doi.org/10.4171/JEMS/1334
3. Bayer-Fluckiger, E.: Automorphisms of $K3$ surfaces, signatures, and isometries of lattices (2022). arXiv:2209.06698v3 (to appear in J. Eur. Math. Soc.)
4. Bayer-Fluckiger, E., Taelman, L.: Automorphisms of even unimodular lattices and equivariant Witt groups. J. Eur. Math. Soc. **22**, 3467–3490 (2020)
5. Brandhorst, S.: The classification of purely non-symplectic automorphisms of high order on $K3$ surfaces. J. Algebra **533**, 229–265 (2019)
6. Brandhorst, S., Cattaneo, A.: Prime order isometries of unimodular lattices and automorphisms of ihs manifolds. Int. Math. Res. Not. **2023**(18), 15584–15638 (2023). arXiv:1912.07119v3
7. Brandhorst, S., Elkies, N.D.: Equations for a K3 Lehmer map. J. Algebraic Geom. **32**(4), 641–675 (2023). arXiv:2103.1510v2
8. Belolipetsky, M., Gan, W.T.: The mass of unimodular lattices. J. Number Theory **114**(2), 221–237 (2005)
9. Fröhlich, A., Taylor, M.: Algebraic Number. Theory Cambridge Studies in Advanced Mathematics, vol. 27. Cambridge University Press, Cambridge (1993)
10. Gross, B.H., McMullen, C.T.: Automorphisms of even unimodular lattices and unramified Salem numbers. J. Algebra **257**(2), 265–290 (2002)
11. Huybrechts, D.: Lectures on $K3$ Surfaces. Cambridge Studies in Advanced Mathematics, vol. 158. Cambridge University Press, Cambridge (2016)
12. Kondō, S.: Automorphisms of algebraic $K3$ surfaces which act trivially on Picard groups. J. Math. Soc. Japan **44**(1), 75–98 (1992)
13. Kondō, S.: $K3$ Surfaces. Tracts in Mathematics, vol. 32. European Mathematical Society, Berlin (2020)
14. Lang, S.: Algebraic Number Theory. Graduate Texts in Mathematics, vol. 110, 2nd edn. Springer, New York (1994)
15. Machida, N., Oguiso, K.: On $K3$ surfaces admitting finite non-symplectic group actions. J. Math. Sci. Univ. Tokyo **5**(2), 273–297 (1998)
16. McMullen, C.T.: Dynamics on $K3$ surfaces: Salem numbers and Siegel disks. J. Reine Angew. Math. **545**, 201–233 (2002)
17. McMullen, C.T.: Automorphisms of projective K3 surfaces with minimum entropy. Invent. Math. **203**(1), 179–215 (2016)
18. Nikulin, V.V.: Quotient-groups of groups of automorphisms of hyperbolic forms by subgroups generated by 2-reflections. Algebro-geometric applications. J. Soviet Math. **22**(4), 1401–1475 (1983)
19. Oguiso, K.: Bimeromorphic automorphism groups of non-projective hyperkähler manifolds–a note inspired by C. T. McMullen. J. Differ. Geom. **78**(1), 163–191 (2008)

20. Oguiso, K., Zhang, D.-Q.: On Vorontsov's theorem on $K3$ surfaces with non-symplectic group actions. Proc. Amer. Math. Soc. **128**(6), 1571–1580 (2000)
21. Serre, J.-P.: Cours d'Arithmétique. Le Mathématicien, No. 2. Presses Universitaires de France, Paris (1977)
22. Takada, Y.: Lattice isometries and K3 surface automorphisms: Salem numbers of degree 20. J. Number Theory **252**, 195–242 (2023)
23. Vorontsov, S.P.: Automorphisms of even lattices arising in connection with automorphisms of algebraic $K3$-surfaces. Vestnik Moskov. Univ. Ser. I Mat. Mekh. **1983**(2), 19–21 (1983) (in Russian)
24. Washington, L.C.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, vol. 83, 2nd edn. Springer, New York (1997)
25. Xiao, G.: Non-symplectic involutions of a $K3$ surface (1995). arXiv:alg-geom/9512007
26. Zhang, D.-Q.: Automorphisms of $K3$ surfaces. In: Chen, Z. et al. (eds.) Proceedings of the International Conference on Complex Geometry and Related Fields. AMS/IP Studies in Advanced Mathematics, vol. 39. American Mathematical Society, Providence, pp. 379–392 (2007)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.