Math. Proc. Camb. Phil. Soc. (2019), **166**, 523–542
doi:10.1017/S0305004118000087
First published online 27 March 2018

On the arithmetic of a family of degree - two K3 surfaces

BY FLORIAN BOUYER

School of Mathematics,
*Howard House, Queen's Avenue, BS*81*SD*
University of Bristol.
e-mail: f.j.s.c.bouyer@gmail.com

EDGAR COSTA

Department of Mathematics,
Dartmouth College
27 *N. Main Street,* 6188 *Kemeny Hall, Hanover, NH* 03755-3551 *U.S.A.*
e-mail: edgarcosta@math.dartmouth.edu

DINO FESTI

Institut für Mathematik,
Johannes Gutenberg–Universität Mainz
Staudingerweg 9, 55128 *Mainz, Germany.*
e-mail: dinofesti@gmail.com

CHRISTOPHER NICHOLLS

Mathematical Institute,
University of Oxford
*Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX*2 6*GG.*
e-mail: christopher.nicholls@balliol.ox.ac.uk

AND MCKENZIE WEST

Department of Mathematics,
1200 *Academy Street, Kalamazoo MI 49006, U.S.A.*
Kalamazoo College
e-mail: mckenzie.west@kzoo.edu

(*Received* 19 *June* 2017; *revised* 7 *February* 2018)

Abstract

Let $\mathbb{P}$ denote the weighted projective space with weights $(1, 1, 1, 3)$ over the rationals, with coordinates x, y, z and w; let $\mathcal{X}$ be the generic element of the family of surfaces in $\mathbb{P}$ given by

$$X\colon w^2 = x^6 + y^6 + z^6 + tx^2y^2z^2.$$

The surface $\mathcal{X}$ is a K3 surface over the function field $\mathbb{Q}(t)$. In this paper, we explicitly

compute the geometric Picard lattice of $\mathcal{X}$, together with its Galois module structure, as well as derive more results on the arithmetic of $\mathcal{X}$ and other elements of the family X.

1. *Introduction*

K3 surfaces are sometimes called "surfaces of intermediate type", as they are neither birational to $\mathbb{P}^2$ nor of general type; that is, they lie between those surfaces whose arithmetic and geometry is well understood and those surfaces whose arithmetic and geometry is still largely obscure, occupying a position similar to elliptic curves among curves. Even though interest in K3 surfaces has recently increased, very basic questions about their arithmetic are still unanswered. For example, it is not known if there are K3 surfaces with finitely many rational points, or if there are K3 surfaces with rational points that are not Zariski dense.

An important tool in understanding the arithmetic and the geometry of a K3 surface is its Picard lattice. The Picard lattice encodes information about the existence of elliptic fibrations, the potential density of rational points and, if the surface is defined over a global field, also the existence of a Brauer–Manin obstruction to the Hasse principle on the surface.

Let $\mathbb{P} = \mathbb{P}_{\mathbb{Q}}(1, 1, 1, 3)$ denote the weighted projective space over $\mathbb{Q}$ with weights $(1, 1, 1, 3)$ and coordinates x, y, z and w; let $\mathbb{A}^1$ denote the affine line over $\mathbb{Q}$, with coordinate t. Consider the following family of degree-two K3 surfaces

$$X\colon w^2 = x^6 + y^6 + z^6 + tx^2y^2z^2 \subset \mathbb{P} \times \mathbb{A}^1.$$

Let $\mathcal{X}$ be the generic element of the family, and let $\overline{\mathcal{X}}$ denote its base change to $\overline{\mathbb{Q}(t)}$. Then $\mathcal{X}$ is a K3 surface over the field $\mathbb{Q}(t)$ (see Proposition 2·1). In this paper we explicitly compute the geometric Picard lattice of $\mathcal{X}$, together with its Galois module structure.

THEOREM 1·1. *The geometric Picard lattice* $\operatorname{Pic}\overline{\mathcal{X}}$ *is isometric to the unique (up to isometries) lattice with rank* 19*, signature* $(1, 18)$*, determinant* $2^5 \cdot 3^3$*, and discriminant group isomorphic to* $\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/12\mathbb{Z})^2$.

We prove Theorem 1·1 as follows. In Section 2, we prove some geometric results about $\mathcal{X}$, and find an explicit set of divisors on $\overline{\mathcal{X}}$. In Section 3, we use these results to show that the geometric Picard number of $\mathcal{X}$ is 19, and we use the aforementioned set of explicit divisors on $\overline{\mathcal{X}}$ to generate a rank 19 sublattice of the geometric Picard lattice of $\mathcal{X}$. Finally, using a technique originating from [**ST10**], we prove that the two lattices coincide.

We then use the explicit description of $\operatorname{Pic}\overline{\mathcal{X}}$ to prove a number of results about the geometry and the arithmetic of all the elements of the family X, as shown in Section 4. We also use Theorem 1·1 to obtain information about the elements of a larger, in fact 4-dimensional, family of K3 surfaces (cf. Remark 4·6).

2. *Geometry*

In this section we investigate the geometry of $\mathcal{X}$. First we show that $\mathcal{X}$ is a K3 surface, then we exhibit an explicit elliptic fibration on it. We then compute a subgroup of $\operatorname{Aut}\overline{\mathcal{X}}$. Finally, we write down a set of explicit divisors on $\overline{\mathcal{X}}$; these divisors play a crucial role in the proof of the main theorem.

Let us first fix notation. In this and also the following sections, if Y is a scheme over a field k, we denote by $Y_{\bar{k}}$ the base change of Y to an algebraic closure of k. For convenience

we write $\overline{\mathcal{X}}$ instead of $\mathcal{X}_{\overline{\mathbb{Q}(t)}}$. We denote by ζ_{12} a primitive 12th root of unity, and for $n = 3, 4, 6$ we define ζ_n as the nth primitive root of unity given by $\zeta_{12}^{12/n}$. Furthermore, if k is a field, we denote by $\mathbb{P}_k$ the weighted projective space $\mathbb{P}_k(1, 1, 1, 3)$ over k, with coordinates x, y, z, w of weight 1, 1, 1, 3, respectively. We also denote by $\mathbb{A}^1_k$ the affine line over k, with coordinate t.

We can now view the family X as a threefold over $\mathbb{Q}$ together with a fibration to the affine line. Using the notation above, X is the threefold

$$X\colon w^2 = x^6 + y^6 + z^6 + tx^2y^2z^2 \subseteq \mathbb{P}_{\mathbb{Q}} \times \mathbb{A}^1_{\mathbb{Q}} \tag{2·1}$$

over $\mathbb{Q}$. The fibration is the map $p\colon X \to \mathbb{A}^1$ defined by $((x_0 : y_0 : z_0 : w_0), t_0) \mapsto t_0$.

Let t_0 be a point in $\mathbb{A}^1_k$ where k is an algebraic extension of $\mathbb{Q}$. The fiber $p^{-1}(t_0) \subset \mathbb{P}_k \times \mathbb{A}^1_k$ naturally embeds into $\mathbb{P}_k$, and we denote its image inside $\mathbb{P}_k$ by $X_{t_0,k}$; we also denote by $B_{t_0,k}$ the plane sextic curve in $\mathbb{P}^2_k$ defined by

$$B_{t_0}\colon x^6 + y^6 + z^6 + t_0x^2y^2z^2 = 0. \tag{2·2}$$

PROPOSITION 2·1. *Let t_0 be a point of $\mathbb{A}^1_{\overline{\mathbb{Q}}}$. If $t_0^3 \neq -27$, then $X_{t_0,\overline{\mathbb{Q}}}$ is a K3 surface. If $t_0^3 = -27$, then $X_{t_0,\overline{\mathbb{Q}}}$ is birational to a K3 surface. Furthermore, the surface $\mathcal{X}$ is a K3 surface over the function field $\mathbb{Q}(t)$.*

Proof. By definition, $X_{t_0,\overline{\mathbb{Q}}}$ is the image inside $\mathbb{P}_{\overline{\mathbb{Q}}}$ of the fiber of X above $t_0 \in \mathbb{A}^1_{\overline{\mathbb{Q}}}$, that is, the surface defined by the equation

$$X_{t_0,\overline{\mathbb{Q}}}\colon w^2 = x^6 + y^6 + z^6 + t_0x^2y^2z^2 \subseteq \mathbb{P}_{\overline{\mathbb{Q}}}.$$

Then $X_{t_0,\overline{\mathbb{Q}}}$ is a double cover of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ ramified above the sextic curve $B_{t_0,\overline{\mathbb{Q}}}$, defined in (2·2). The curve $B_{t_0,\overline{\mathbb{Q}}}$ admits singular points if and only if $t_0^3 = -27$.

Hence, if $t_0^3 \neq -27$, the curve $B_{t_0,\overline{\mathbb{Q}}}$ is smooth and so $X_{t_0,\overline{\mathbb{Q}}}$ is a double cover of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ ramified above a smooth sextic curve and is thus a K3 surface.

Assume now that $t_0^3 = -27$ or, equivalently, $t_0 \in \{-3, -3\zeta_3, -3\zeta_3^2\}$. One sees that $X_{-3,\overline{\mathbb{Q}}}$ has twelve ordinary double points: $(1 : \zeta_6^j : \zeta_6^k : 0)$, where $j + k \equiv 0 \bmod 3$. For $i = 1, 2$, the map $(x : y : z : w) \mapsto (\zeta_3^i x : y : z : w)$ gives an isomorphism $X_{-3,\overline{\mathbb{Q}}} \to X_{-3\zeta_3^i,\overline{\mathbb{Q}}}$. So also $X_{t_i,\overline{\mathbb{Q}}}$ has twelve ordinary double points, namely the points $(1 : \zeta_6^j : \zeta_6^k : 0)$, such that $j + k \equiv i \bmod 3$. Recall that blow ups of points preserve the cohomological groups (cf. [**Har77**, proposition V·3·4]) and that resolutions of ordinary double points preserve the canonical divisor (cf. [**BHPVdV04**, theorem III·7·2]). Hence, by blowing up the singular points of $X_{t_i,\overline{\mathbb{Q}}}$ we obtain a K3 surface.

Finally, the surface $\mathcal{X}$ is the fiber of X above the generic point of $\mathbb{A}^1_{\mathbb{Q}}$ and so, by the first part of the proof, $\mathcal{X}$ is a K3 surface over the function field $\mathbb{Q}(t)$.

Remark 2·2. As noticed by Noam Elkies, $\mathcal{X}$ is isogenous to an elliptic K3 surface $\mathcal{Y}$. Both the isogeny and the elliptic fibration of $\mathcal{Y}$ can be explicitly written down, as follows.

The composition of the Cremona transformation $(x : y : z : w) \mapsto (yz : xz : xy : w)$ with the map $(x : y : z : w) \mapsto (x^2 : y^2 : z^2 : w)$ is a rational map from $\mathcal{X}$ to the surface defined by

$$w^2 = (yz)^3 + (xz)^3 + (xy)^3 + t(xyz)^2$$

inside $\mathbb{P}_{\mathbb{Q}(t)}(4, 4, 4, 3) \cong \mathbb{P}_{\mathbb{Q}(t)}$. Notice that this is a $4 : 1$ map not defined at $(1\colon 0\colon 0\colon 0)$, $(0\colon 1\colon 0\colon 0)$, and $(0\colon 0\colon 1\colon 0)$.

Set $z = ry$ to project along $(1\colon 0\colon 0\colon 0)$; for each r, we get

$$w^2 = y^3((r^3+1)x^3 + r^2tx^2y + (ry)^3).$$

Now let us restrict to the affine patch given by $y \neq 0$ or, equivalently, $y = 1$. Then we can write the above equation as

$$w^2 = ((r^3+1)x^3 + r^2tx^2 + r^3).$$

The $3:1$ map $\mathbb{A}^2(x,w) \times \mathbb{A}^1(r) \to \mathbb{A}^2(u,v) \times \mathbb{A}^1(s)$ defined by

$$((x,w),r) \mapsto ((x\,r^4(r^3+1),\, w\,r^6(r^3+1)), r^3)$$

sends the variety defined by the above equation to the variety

$$\mathcal{Y} : v^2 = u^3 + ts^2u^2 + s^5(1+s)^2, \tag{2·3}$$

a one parameter family of elliptic surfaces over the s-line. The composition of these maps is a $12:1$ map from $\mathcal{X}$ to $\mathcal{Y}$.

PROPOSITION 2·3. *The surface $\mathcal{X}$ is isogenous to the Kummer surface associated to the abelian surface $E \times E$, where E is an elliptic curve with j-invariant $-(4t)^3$. For example, we can take E to be*

$$E : y^2 + xy = x^3 + \frac{36}{1728 + (4t)^3}x + \frac{1}{1728 + (4t)^3}.$$

Proof. Under the change of coordinates $v \mapsto v - s^2t/3$ we can rewrite $\mathcal{Y}$ in (2·3) as

$$u^2 = v^3 - \frac{1}{3}s^4t^2v + s^5\left(s^2 + \frac{2}{27}s(27+t^3) + 1\right),$$

which matches the Inose fibration

$$Z_{A,B} : y^2 = x^3 - 3As^4x + s^5(t^2 - 2Bs + 1), \tag{2·4}$$

with $A = t^2/9$ and $B = (-t^3-27)/27$. In [**Ino78**], Inose showed that $Z_{A,B}$ is isogenous to the Kummer surface associated to the product of two elliptic curves E_1 and E_2, where

$$A^3 = j(E_1)j(E_2)/12^6, \quad B^2 = \left(1 - j(E_1)/12^3\right)\left(1 - j(E_2)/12^3\right).$$

See also [**SS10**, section 13·5]. In our case, we have $j(E_1) = j(E_2) = -(4t)^3$.

Remark 2·4. This result came only after explicitly computing the Picard lattice. Nevertheless, being independent of those computations, it can be used to more easily obtain some of our results. In particular, it implies Corollary 2·5.

COROLLARY 2·5. *The family X is not isotrivial.*

Proof. Since two elliptic curves are isomorphic if and only if they have the same j-invariant, Proposition 2·3 implies that two fibers X_{t_0} and X_{t_1} are isomorphic if and only if $t_0^3 = t_1^3$. Hence, there exist smooth fibers that are not isomorphic.

Automorphisms are important in order to understand the geometry of a surface. Following [**Fes16**, section 3·2], we present a subgroup of $\mathrm{Aut}\,\overline{\mathcal{X}}$. We make use of this subgroup later, to find more divisors on $\overline{\mathcal{X}}$ and generate a large sublattice of the Picard lattice.

Let $\sigma \in S_3$ be a permutation of the set $\{x, y, z\}$ and let ψ_σ be the corresponding automorphism on $\mathbb{P}_{\overline{\mathbb{Q}}}$:

$$\psi_\sigma : (x : y : z : w) \longmapsto (\sigma(x) : \sigma(y) : \sigma(z) : w).$$

Further, for $i, j, k \in \mathbb{Z}/6\mathbb{Z}$, such that $2(i + j + k) \equiv 0 \bmod 6$, consider the following automorphism of $\mathbb{P}_{\overline{\mathbb{Q}}}$:

$$\psi_{i,j,k} : (x : y : z : w) \longmapsto \left(\zeta_6^i x : \zeta_6^j y : \zeta_6^k z : w\right).$$

Remark 2·6. Since w has weight 3, we have $(\zeta_6^2 x : \zeta_6^2 y : \zeta_6^2 z : w) = (x : y : z : w)$, and thus $\psi_{i,j,k} = \psi_{i+\ell,j+\ell,k+\ell}$ for $\ell \equiv 0 \bmod 2$.

Let H_1 denote the group formed by the automorphisms ψ_σ, for $\sigma \in S_3$; let H_2 denote the group formed by the automorphisms $\psi_{i,j,k}$, for $i, j, k \in \mathbb{Z}/6\mathbb{Z}$, such that $2(i + j + k) \equiv 0 \bmod 6$; finally, let H denote the subgroup of $\operatorname{Aut}\mathbb{P}_{\overline{\mathbb{Q}}}$ generated by H_1 and H_2, that is

$$H := \langle H_1, H_2 \rangle \subseteq \operatorname{Aut}\mathbb{P}_{\overline{\mathbb{Q}}}. \tag{2·5}$$

Let α and β be two elements of H_1 and H_2, respectively. One can easily see that the automorphism given by $\alpha^{-1}\beta\alpha$ is an element of H_2. We can then define an action of H_1 on H_2 by sending $(\alpha, \beta) \in H_1 \times H_2$ to $\alpha^{-1}\beta\alpha \in H_2$. Let $H_1 \ltimes H_2$ denote the semidirect product of H_1 and H_2, with H_1 acting on H_2 as described above. It is easy to see that $H = H_1 \ltimes H_2$.

The following results describe H_1, H_2 and H as abstract groups. For a positive integer n, let μ_n denote the multiplicative group of nth roots of unity. Let $\Sigma \subset \mu_6^3$ be the subgroup of $\mu_6^3 = \mu_6 \times \mu_6 \times \mu_6$ defined by

$$\Sigma := \{(\zeta, \xi, \theta) \in \mu_6^3 \ : \ \zeta\xi\theta = \pm 1\}.$$

Remark 2·7. The group Σ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times 3\mathbb{Z}/6\mathbb{Z}$. To see this, let (ζ, ξ, θ) be an element of Σ. Since $\zeta, \xi, \theta \in \mu_6$, there are $i, j, k \in \{0, 1, ..., 5\}$ such that $\zeta = \zeta_6^i, \xi = \zeta_6^j, \theta = \zeta_6^k$; since $\zeta\xi\theta = \pm 1$, we have that $i + j + k \in \{0, 3\}$. Then the map $\Sigma \to \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times 3\mathbb{Z}/6\mathbb{Z}$ given by

$$(\zeta, \xi, \theta) \longrightarrow (i, j, i + j + k)$$

is well defined and is in fact an isomorphism of groups.

Let $\Delta : \mu_3 \hookrightarrow \mu_6^3$ be the embedding defined by

$$\Delta : \zeta \longrightarrow (\zeta, \zeta, \zeta).$$

It is easy to see that the image of Δ is a subgroup of Σ. Let N denote the quotient group

$$N := \Sigma / \operatorname{im}(\Delta). \tag{2·6}$$

Remark 2·8. As an easy exercise in group theory, one can show that the group N is isomorphic to the group $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$.

LEMMA 2·9. *The following statements hold*:

(i) *H_1 is isomorphic to the symmetric group S_3;*

(ii) *H_2 is isomorphic to the group N defined in* (2·6);

(iii) *H is isomorphic to $S_3 \ltimes N$, where the action of S_3 on N is given by permuting the coordinates of the elements of N.*

Proof.

(i) Follows from the definition of H_1.

(ii) Let (ζ, ξ, θ) be an element of Σ and let i, j, k be defined as in Remark 2·7. Then $i + j + k \in \{0, 3\}$ or, equivalently, $2(i + j + k) \equiv 0 \mod 6$. We can then consider the map $\Sigma \to H_2$ given by

$$(\zeta, \xi, \theta) \longmapsto \psi_{i,j,k}.$$

The map is clearly surjective; by Remark 2·6, it follows that the kernel is the subgroup $\{(0, 0, 0), (2, 2, 2), (4, 4, 4)\}$; so

$$H_2 \cong \Sigma/\{(0, 0, 0), (2, 2, 2), (4, 4, 4)\} = N,$$

concluding the proof.

(iii) The statement follows by combining points *i)* and *ii)* and the observation that $H = H_1 \ltimes H_2$.

LEMMA 2·10. *The group H injects into* $\operatorname{Aut}\overline{\mathcal{X}}$.

Proof. First notice that all the elements of H extend to automorphisms of $\mathbb{P}_{\overline{\mathbb{Q}(t)}}$. The maps ψ_σ and $\psi_{i,j,k}$ map $\mathcal{X}$ to itself, as the automorphisms fix the defining equation of X. For any given non-trivial $h \in H$, its fixed points are contained in a hyperplane, hence it cannot act trivially on $\overline{\mathcal{X}}$. Hence, the group homomorphism $H \to \operatorname{Aut}\overline{\mathcal{X}}$ given by first extending an automorphism $h \in H \subset \operatorname{Aut}\mathbb{P}_{\overline{\mathbb{Q}}}$ to $\mathbb{P}_{\overline{\mathbb{Q}(t)}}$ and then restricting it to $\overline{\mathcal{X}}$ is injective.

In what follows we will make no distinction between the group H and its image inside $\operatorname{Aut}\overline{\mathcal{X}}$.

Remark 2·11. Since the elements of H are defined over $\mathbb{Q}(\zeta_6) \subset \overline{\mathbb{Q}}$, using the same argument as in Lemma 2·10, one can show that for any $t_0 \in \mathbb{A}^1$, the group H is a subgroup of the automorphism group $\operatorname{Aut} X_{t_0,\overline{\mathbb{Q}}}$.

Finally, we produce a specific set of divisors on $\overline{\mathcal{X}}$. In Section 3, we show that this set of divisors, together with a particular subgroup of isometries of $\operatorname{Pic}\overline{\mathcal{X}}$, generates the full Picard lattice of $\overline{\mathcal{X}}$.

As in [**EJ08**, construction 4], to produce a set of divisors, we use the fact that $\mathcal{X}$ is a double cover of $\mathbb{P}^2_{\mathbb{Q}(t)}$ branched above the curve

$$\mathcal{B}\colon x^6 + y^6 + z^6 + tx^2y^2z^2 = 0 \subset \mathbb{P}^2_{\mathbb{Q}(t)}.$$

We produce a set of divisors on $\overline{\mathcal{X}}$ by searching for conics in $\mathbb{P}^2_{\overline{\mathbb{Q}(t)}}$ that intersect $\mathcal{B}_{\overline{\mathbb{Q}(t)}}$ with even multiplicity everywhere; the pullback of such conics to the surface $\overline{\mathcal{X}}$ splits into two components. For each of these conics, we take a component of the pullback. In this way, we find the set Ω of divisors on $\overline{\mathcal{X}}$, given by

$$\Omega = \{B_1, B_2, B_3, B_4, B_5\}, \tag{2·7}$$

where

$$B_1\colon \begin{cases} x^2+y^2+\zeta_3 z^2 & =0\\ w-\beta_1 xyz & =0\end{cases}$$

$$B_2\colon \begin{cases} x^2+\zeta_3 y^2+\zeta_3^2 z^2 & =0\\ w-\beta_0 xyz & =0\end{cases}$$

$$B_3\colon \begin{cases} 2xy-c_1 z^2 & =0\\ x^3-y^3-w & =0\end{cases}$$

$$B_4\colon \begin{cases} c_0\delta x^2-2(9c_0^2+3tc_0-2t^2)xy+2\delta y^2-\delta z^2 & =0\\ (x^3+a_4x^2y+b_4xy^2+c_4y^3)(c_0^2c_1+2)-2w & =0\end{cases}$$

$$B_5\colon \begin{cases} a_5x^2+c_5(y^2+z^2)+yz & =0\\ r_5x^3+v_5xyz-w & =0.\end{cases}$$

Here, $\beta_i \in \overline{\mathbb{Q}(t)}$ satisfy $\beta_i^2 = t+3\zeta_3^i$, for $i=0,1,2$; the elements $c_0, c_1, c_2 \in \overline{\mathbb{Q}(t)}$ are the three roots of x^3+tx^2+4; the element δ is $4\zeta_4\beta_0\beta_1\beta_2$; and the remaining constants are expressed in terms of β_i, c_j and δ as follows:

$$\begin{aligned}
a_4 &= \frac{9c_0+6t}{4(t^3+27)}\delta,\\
b_4 &= -c_0^2-tc_0,\\
c_4 &= \frac{18-3t^2c_0-3tc_0^2}{8(t^3+27)},\\
a_5 &= \frac{\zeta_{12}(-\zeta_6+2)}{9}(\beta_0\beta_1+\beta_0\beta_2+\beta_1\beta_2+t),\\
c_5 &= \frac{\zeta_{12}(\zeta_6-2)}{3},\\
r_5 &= \frac{\zeta_{12}(\zeta_6-2)}{9}(2\beta_0\beta_1\beta_2+(2t-3)\beta_0+(2t-3\zeta_3)\beta_1+(2t+3\zeta_6)\beta_2),\\
v_5 &= -\beta_0-\beta_1-\beta_2.
\end{aligned}$$

Remark 2·12. In the rest of the paper, we abuse notation and use the symbols B_i, for $i=1,\ldots,5$, to denote both the divisor B_i as well as its class inside $\operatorname{Pic}\overline{\mathcal{X}}$.

Remark 2·13. By definition, B_i is one of the two irreducible components on the pullback of a certain smooth conic $C_i \subset \mathbb{P}^2_{\overline{\mathbb{Q}(t)}}$ on $\overline{\mathcal{X}}$. Thus B_i is isomorphic to the conic C_i, and so B_i has genus 0.

Note that the divisors in Ω are not defined over $\mathbb{Q}(t)$. Denote by L the Galois closure of the minimal field extension of $\mathbb{Q}(t)$ over which Ω is defined. We refer to Appendix B for the definition of L and the computation of the Galois group $\operatorname{Gal}(L/\mathbb{Q}(t))$, which we use later on.

Let S be a K3 surface defined over a field k and let K be a field extension of k. Let D be a class in $\operatorname{Pic}\overline{S}$. In what follows, we say that D *can be defined over* K if D contains a divisor on $\overline{S}$ whose defining equations have coefficients in K.

Remark 2·14. By exploiting the symmetry of the equation defining $\mathcal{B}$, it is easy to find the divisors B_1, B_2, B_3. However, finding the divisors B_4 and B_5 is more challenging. To

find them, we specialise the surface $\mathcal{X}$, find divisors on the specialisation, and then try to lift them to $\mathcal{X}$. More explicitly, we choose $t_0 \in \mathbb{Z}$, and specialise the surface $\mathcal{X}$ to the surface X_{t_0}. We then reduce X_{t_0} modulo a prime of good reduction, p, to get the surface $X_{t_0,p}$ (see Section 3 for more details). Then, with the help of a computer, we iterate over all conics over $\mathbb{F}_p$ that are everywhere bi-tangent to the ramification locus of $X_{t_0,p}$. We look for those conics whose components of the pull-back on $X_{t_0,p}$, together with the specialisations of B_1, B_2 and B_3, generate a lattice inside $\mathrm{Pic}\left(X_{t_0,p}\right)_{\overline{\mathbb{F}_p}}$ with higher rank or smaller determinant than the lattice generated by B_1, B_2 and B_3 of $\mathcal{X}$. For each such curve, we lift it to a number field. By repeating this process for different values of t_0, we are able to interpolate these divisors in terms of t. For more details, see [**Fes16**, remarks 3·5·1 and 3·5·2].

Remark 2·15. There are many other ways to write down divisors on $\mathcal{X}$. For example, we could have looked for lines that are tri-tangent to $\mathcal{B}$. Unfortunately, such lines do not exist over $\mathbb{Q}(t)$. A Gröbner bases computation shows that such lines only exist on the fibers above the zeros of the polynomial

$$t(t^3 + 5^3)(8t^3 + 33^3). \tag{2·8}$$

Another possibility is to take advantage of the fact that $\mathcal{X}$ is a double cover of the degree-one del Pezzo surface

$$Y : \ w = x^6 + y^6 + z^3 + tx^2y^2z \subset \mathbb{P}_{\mathbb{Q}(t)}(1, 1, 2, 3).$$

It is well known that $\mathrm{Pic}\, Y_{\overline{\mathbb{Q}(t)}}$ is a rank 9 lattice, generated by the 240 exceptional curves on $Y_{\overline{\mathbb{Q}(t)}}$. These divisors do not play a relevant role in our approach, though this has been useful in other situations (e.g., [**KT04**]).

3. *The Picard lattice of* $\overline{\mathcal{X}}$

Even though there are some theoretical algorithms to compute the geometric Picard lattice of a K3 surface, none are computationally feasible. For example, an effective version of the Kuga–Satake construction for degree-two K3 surfaces in [**HKT13**] yields a theoretical algorithm, but there are no explicit examples of this. Another algorithm is given in [**PTvL15**, section 8·6.]. The paper [**Cha14**] presents an algorithm to compute the rank of the geometric Picard lattice, conditional on the Hodge conjecture for $X \times X$; the algorithm computes a sublattice of finite index, which therefore has the same rank. These methods rely on finding linearly independent divisors on X. However, there is no known practical algorithm to do this on a K3 surface.

In this section, we use the results presented in Section 2 to explicitly compute the geometric Picard lattice of $\mathcal{X}$. Using the divisors in the set $\mathbf{\Omega}$, defined in (2·7), we explicitly compute a sublattice Λ of $\mathrm{Pic}\,\overline{\mathcal{X}}$. Finally, we show that Λ is in fact equal to $\mathrm{Pic}\,\overline{\mathcal{X}}$.

We first compute the geometric Picard number.

PROPOSITION 3·1. *The surface* $\mathcal{X}$ *has geometric Picard number* $\rho\left(\overline{\mathcal{X}}\right) = 19$.

Proof. From Proposition 2·3, we have that $\overline{\mathcal{X}}$ is isomorphic to the Kummer surface associated to the square of an elliptic curve with j-invariant $-(4t)^3$. If A is an abelian surface, with Kummer surface $\mathrm{Kum}(A)$, then we have $\rho(\mathrm{Kum}(A)) = 16 + \rho(A)$ (see [**Huy16**, section 17·1]). Also, we have $\rho(A) = \dim(\mathrm{End}(A) \otimes \mathbb{Q})^{\dagger}$, where the superscript $\dagger$ denotes those endomorphisms that are invariant under the Rosati involution. For a product of elliptic

curves, we have

$$(\mathrm{End}(E_1 \times E_2) \otimes \mathbb{Q})^\dagger \cong (\mathrm{End}(E_1) \otimes \mathbb{Q})^\dagger \times (\mathrm{End}(E_2) \otimes \mathbb{Q})^\dagger \times \mathrm{Hom}(E_1, E_2).$$

See [**Mum70**, section 21] for more details. Therefore,

$$\begin{aligned} \rho(\overline{\mathcal{X}}) &= 16 + \rho(E \times E) \\ &= 18 + \mathrm{rk}\,\mathrm{End}(E) \\ &\geqslant 19. \end{aligned}$$

In the other direction, from Corollary 2·5, we have that X is a 1-dimensional non-isotrivial family of K3 surfaces. Thus, from [**Dol96**, corollary 3·2], it follows that $\rho(\overline{\mathcal{X}})$ is at most $20 - 1 = 19$.

Recall that H is the subgroup of $\mathrm{Aut}\,\overline{\mathcal{X}}$ defined in Section 2. The group $\mathrm{Aut}\,\overline{\mathcal{X}}$ induces a natural action on the group of divisors on $\overline{\mathcal{X}}$, so we define the set

$$H \cdot \Omega = \{hB \mid h \in H,\ B \in \Omega\}, \tag{3·1}$$

given by the union of the orbits of the elements of Ω under the action of $H \subset \mathrm{Aut}\,\overline{\mathcal{X}}$. Recall that all the divisors in Ω are defined over a certain Galois extension L of $\mathbb{Q}(t)$. By construction, ζ_6 lies in L and so, since all the automorphisms in H are defined over $\mathbb{Q}(\zeta_6)(t)$, it follows that all the elements in $H \cdot \Omega$ are defined over L.

The divisors in $H \cdot \Omega$ generate a sublattice of $\mathrm{Pic}\,\overline{\mathcal{X}}$, say

$$\Lambda := \langle H \cdot \Omega \rangle \subseteq \mathrm{Pic}\,\overline{\mathcal{X}}. \tag{3·2}$$

This sublattice can be explicitly computed, as shown by the following results.

Remark 3·2. To show that $\rho \geqslant 19$ in Proposition 3·1, we could alternatively just compute the rank of the sublattice $\Lambda \subset \mathrm{Pic}\,\overline{\mathcal{X}}$.

3·1. *Computing the sublattice* Λ.

We first introduce some notation and state some preliminary results. For this, we follow [**Fes16**, subsection 3·3·3].

Let $t_0 \in \mathbb{Z}$ be an integer and fix an integral model Ξ_{t_0} for the surface X_{t_0} (the fiber of X above t_0). Let $p \in \mathbb{Z}$ be a prime of good reduction for Ξ_{t_0}, and let $\mathbb{F}_p$ denote the field with p elements.

Let L_{t_0} be the number field obtained by specializing the field L to $t = t_0$; let $\mathcal{O}_{t_0}$ denote the ring of integers of L_{t_0}, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_{t_0}$ lying above p. Let $\kappa(\mathfrak{p})$ be the residue field $\mathcal{O}_{t_0}/\mathfrak{p}$. The field $\kappa(\mathfrak{p})$ is isomorphic to $\mathbb{F}_{p^m}$, for some $m > 0$.

Let $X_{t_0,p}$ denote the reduction of Ξ_{t_0} modulo p. Let $B_{t_0,p} \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ denote the branch locus of $X_{t_0,p}$.

Let D be one of the divisors on $\mathcal{X}$ in $H \cdot \Omega$, and let $\overline{D}$ denote its Zariski closure inside X. Then $\overline{D}$ is a divisor on X. We define D_{t_0} to be the specialisation of $\overline{D}$ at t_0; that is, the divisor on X_{t_0} obtained by taking the fiber of $\overline{D}$ above t_0.

Note that for some divisors in $H \cdot \Omega$, there are values of $t_0 \in \overline{\mathbb{Q}}$ such that the divisor cannot be specialised to $t = t_0$; for example, B_4 cannot be specialised to $t = -3$. Assume that D can be specialised to t_0 and that $\mathfrak{p} \in \mathcal{O}_{t_0}$ is a prime of good reduction for Ξ_{t_0}. Then let $\overline{D_{t_0}}$ be the Zariski closure of D_{t_0} inside Ξ_{t_0}. We define $D_{t_0,\mathfrak{p}}$ to be the reduction modulo $\mathfrak{p}$ of $\overline{D_{t_0}}$. The curve $D_{t_0,\mathfrak{p}}$ is a divisor on $X_{t_0,\mathfrak{p}} = (X_{t_0,p})_{\kappa(\mathfrak{p})}$. Note that the procedure of going from a

divisor on $\mathcal{X}$ to a divisor on $X_{t_0,\mathfrak{p}}$ consists of a single step, repeated twice: taking the closure of a divisor on the generic fiber of a family and specializing it to a special fiber.

LEMMA 3·3. *Using the same notation as above, and assuming that D and D' are two divisors on $\mathcal{X}$ that can be specialised to $t_0 \in \mathbb{Z}$, we have the following equality of intersection numbers*:

$$D \cdot D' = D_{t_0,\mathfrak{p}} \cdot D'_{t_0,\mathfrak{p}}$$

Proof. Using [**MP12**, proposition 3·6] and [**EJ11**, theorem 1·4], one immediately gets that the reduction of $\mathcal{X}$ to $X_{t_0,p}$ induces an embedding $\mathrm{Pic}\,\overline{\mathcal{X}} \hookrightarrow \mathrm{Pic}(X_{t_0,\mathfrak{p}})_{\overline{\kappa(\mathfrak{p})}}$ that is injective, compatible with the intersection product, and has torsion-free cokernel. The result follows.

See [**Huy16**, proposition 17·2·10, remark 17·2·11], and [**vL07**, proposition 6·2] for more details.

COMPUTATION 3·4. *The lattice Λ is isometric to the lattice*

$$U \oplus E_8(-1) \oplus A_5(-1) \oplus A_2(-1) \oplus A_2(-4).$$

In particular, Λ has rank 19*, determinant* $2^5 \cdot 3^3$*, signature* $(1, 18)$ *and discriminant group isomorphic to* $\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/12\mathbb{Z})^2$.

See Appendix A for the definition of the lattices U, $E_8(-1)$, $A_5(-1)$, $A_2(-1)$, $A_2(-4)$, the direct sum of lattices, and the discriminant group of a lattice.

Proof. The main step is to compute the intersection matrix for the generators of Λ; that is, to calculate the intersection numbers $D \cdot D'$ for all pairs D, D' in the set $H \cdot \Omega$.

For self intersection numbers, we use the adjunction formula:

$$D \cdot D = 2g(D) - 2 = -2, \qquad \text{for } D \in H \cdot \Omega,$$

as D is isomorphic to a plane conic, and so it has genus zero.

For pairs of distinct D, D' in $H \cdot \Omega$, directly computing the intersection number $D \cdot D'$ over an algebraic extension of a function field can be computationally very expensive. Instead, using Lemma 3·3, we reduce all the computations to computations over finite fields. Fix an integer $t_0 \in \mathbb{Z}$, and an integral model for X_{t_0}. Let p be a prime of good reduction for the fixed integral model of X_{t_0} and, recalling the notation introduced before, let L_{t_0} be the specialisation of L to t_0, $\mathcal{O}_{t_0}$ be the ring of integers of L_{t_0} and $\mathfrak{p}$ be a prime of $\mathcal{O}_{t_0}$ lying above p. Using Lemma 3·3, if D, D' are two divisors on $\mathcal{X}$, then $D \cdot D' = D_{t_0,\mathfrak{p}} \cdot D'_{t_0,\mathfrak{p}}$. Since all divisors $D \in H \cdot \Omega$ are defined over L, all the divisors $D_{t_0,\mathfrak{p}}$ are defined over the finite field $\mathbb{F}_{p^m} \cong \kappa(\mathfrak{p})$, for some $m > 0$.

If $D_{t_0,\mathfrak{p}}$ and $D'_{t_0,\mathfrak{p}}$ have no common components, then the intersection $D_{t_0,\mathfrak{p}} \cap D'_{t_0,\mathfrak{p}}$ is a zero-dimensional scheme over $\mathbb{F}_{p^m}$. Using MAGMA it is possible to compute its degree. Since we are considering divisors on a smooth surface, the degree of the zero-dimensional scheme given by the intersection of the two divisors equals the sum of the intersection multiplicities of the points of intersection of the two divisors (see [**HS00**, A·2·3]), and so the degree of $D_{t_0,\mathfrak{p}} \cap D'_{t_0,\mathfrak{p}}$ is the intersection number $D_{t_0,\mathfrak{p}} \cdot D'_{t_0,\mathfrak{p}} = D \cdot D'$. In this way, we get the intersection matrix of the lattice Λ generated by $D \in H \cdot \Omega$.

In our computations, we use $t_0 = 7$ and $p = 79$ and work over $\mathbb{F}_{79^2}$. We then compute an integral basis for Λ, and compute the intersection matrix of the basis; this is the Gram matrix of Λ. Finally, the rank, signature, and discriminant of Λ are the rank, signature, and

determinant of the Gram matrix, respectively. One also computes the discriminant group of Λ from the Gram matrix, as described in Appendix A. These quantities agree with those given in the statement of the result.

Using these data, the first statement of the result immediately follows from [**Nik80a**, corollary 1·13·3] (see Appendix A), noticing that Λ and the lattice in the statement are both even and indefinite, and have the same rank, discriminant, signature, discriminant form, and the same number of generators for the discriminant group; that is, $3 < 17 = 19 - 2$. For the MAGMA code with the effective computations, see [**BCFNW17**].

Before stating a corollary of Computations 3·4, recall that a class $D \in \operatorname{Pic}\overline{\mathcal{X}}$ is said to be defined over an extension $K/\mathbb{Q}(t)$ if D contains a divisor whose defining equations have coefficients in K. We also introduce the notation $\mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$ for the group of isometries of $\operatorname{Pic}\overline{\mathcal{X}}$.

COROLLARY 3·5. *The following statements hold*:

(i) *the lattice* Λ *is a finite index sublattice of* $\operatorname{Pic}\overline{\mathcal{X}}$;
(ii) *every class in* $\operatorname{Pic}\overline{\mathcal{X}}$ *is defined over* L;
(iii) *the Galois group* $\mathrm{Gal}(L/\mathbb{Q}(t))$ *injects into* $\mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$;
(iv) *the group* H *injects into* $\mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$.

Proof.

(i) This is immediate, since Λ is a sublattice of $\operatorname{Pic}\overline{\mathcal{X}}$ by construction, and from Proposition 3·1 and Corollary 3·5 we have that $\operatorname{Pic}\overline{\mathcal{X}}$ and Λ both have rank 19.

(ii) We have already seen that all the elements in $H \cdot \Omega$ are defined over L. Since these elements generate the lattice Λ, we have that all the elements of Λ are defined over L. Now let D be a class in $\operatorname{Pic}\overline{\mathcal{X}}$. By point (i) we have that Λ has finite index, say d, inside $\operatorname{Pic}\overline{\mathcal{X}}$. Then dD is an element of Λ, hence it can be defined over L. Since the action of the Galois group on $\operatorname{Pic}\overline{\mathcal{X}}$ is linear and $\operatorname{Pic}\overline{\mathcal{X}}$ is torsion free, it follows that D can be defined over L.

(iii) The Galois group $G_t = \mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t))$ naturally acts on $\operatorname{Pic}\overline{\mathcal{X}}$; that is, there is a map $G_t \to \mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$. We have seen that all the elements of $\operatorname{Pic}\overline{\mathcal{X}}$ are defined over L, hence this action factors through the Galois group $\mathrm{Gal}(L/\mathbb{Q}(t))$. More precisely, we have an exact sequence

$$0 \longrightarrow H_t \longrightarrow G_t \longrightarrow \mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}}),$$

where H_t is the kernel of the map $G_t \to \mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$. As the elements of $\operatorname{Pic}\overline{\mathcal{X}}$ are defined over L, we have that H_t contains $\mathrm{Gal}(\overline{\mathbb{Q}(t)}/L)$. Having an explicit description of $\mathrm{Gal}(L/\mathbb{Q}(t))$ and Λ, one can easily see that no element of $\mathrm{Gal}(L/\mathbb{Q}(t))$ acts as the identity on $\Lambda \subset \operatorname{Pic}\overline{\mathcal{X}}$, hence no element of $\mathrm{Gal}(L/\mathbb{Q}(t))$ acts as the identity on $\operatorname{Pic}\overline{\mathcal{X}}$ (see Appendix B for the explicit description of $\mathrm{Gal}(L/\mathbb{Q}(t))$ and use the explicit divisors given in Section 2 to see that for every element of $\mathrm{Gal}(L/\mathbb{Q}(t))$ there is at least one element in that list that is not fixed). It follows that the kernel H_t is exactly the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}(t)}/L)$. Therefore,

$$\mathrm{Gal}(L/\mathbb{Q}(t)) \cong G_t/\mathrm{Gal}(\overline{\mathbb{Q}(t)}/L) = G_t/H_t$$

injects into $\mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$, proving the statement.

(iv) Recall that H is the subgroup of $\operatorname{Aut}\overline{\mathcal{X}}$ defined in (2·5). From Proposition 3·1, we know that $\operatorname{Pic}\overline{\mathcal{X}}$ has Picard number 19; from Computation 3·4 we know that Λ has determinant $2^5 \cdot 3^3$; from point (1), we know that Λ is a finite index sublattice of $\operatorname{Pic}\overline{\mathcal{X}}$. It follows that $\operatorname{Pic}\overline{\mathcal{X}}$ has rank 19 and that its determinant is not a power of 2; in particular, the determinant is divisible by 3. The statement now immediately follows from [**Fes16**, proposition 1·2·47].

From Corollary 3·5, we have that both groups $\operatorname{Gal}(L/\mathbb{Q}(t))$ and H embed into $\mathrm{O}(\operatorname{Pic}\mathcal{X})$, so we can define the group

$$G := \langle \operatorname{Gal}(L/\mathbb{Q}(t)), H\rangle \subseteq \mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}}), \tag{3·3}$$

the subgroup of $\mathrm{O}(\operatorname{Pic}\overline{\mathcal{X}})$ generated by $\operatorname{Gal}(L/\mathbb{Q}(t))$ and H.

3·2. *Proving* $\Lambda = \operatorname{Pic}\overline{\mathcal{X}}$.

Recall that Λ is the sublattice of $\operatorname{Pic}\overline{\mathcal{X}}$ generated by the orbits of the divisors $\boldsymbol{\Omega}$ under the group H (cf. (3·2)).

We now show that Λ is in fact the whole geometric Picard lattice of $\mathcal{X}$, by showing that the quotient $\operatorname{Pic}\overline{\mathcal{X}}/\Lambda$ is trivial. From Corollary 3·5, we know that Λ is a finite index sublattice of $\operatorname{Pic}\overline{\mathcal{X}}$, and consequently that $\operatorname{Pic}\overline{\mathcal{X}}/\Lambda$ is a finite abelian group. This group is trivial if and only if there is no element of order p, for any prime p. An element of order p corresponds to a nontrivial element of the kernel of the natural map $\Lambda/p\Lambda \to \operatorname{Pic}\overline{\mathcal{X}}/p\operatorname{Pic}\overline{\mathcal{X}}$. Denote the kernel of this map by Λ_p. To complete the proof, it suffices to show that Λ_p is trivial for every prime p.

Remark 3·6. We can eliminate all but two primes by considering the possible order of $\operatorname{Pic}\overline{\mathcal{X}}/\Lambda$. Indeed, $\Lambda_p \neq 0$ if and only if there is an element of order p in $\operatorname{Pic}\overline{\mathcal{X}}/\Lambda$, which implies that p divides $\#\left(\operatorname{Pic}\overline{\mathcal{X}}/\Lambda\right) = [\operatorname{Pic}\overline{\mathcal{X}}\colon \Lambda]$. If L and L' are lattices of the same rank such that $L' \subseteq L$, then $\operatorname{disc} L' = [L\colon L']^2 \operatorname{disc} L$. From Computation 3·4, we have $\operatorname{disc}\Lambda = 2^5 \cdot 3^3$; thus $[\operatorname{Pic}\overline{\mathcal{X}}\colon \Lambda] \mid 2^2 \cdot 3$. Consequently, $\Lambda_p = 0$ for $p \notin \{2, 3\}$.

We are left to show that Λ_2 and Λ_3 are both zero. For this, we use the technique in [**ST10**], which is also used in [**VAV11**]: since we cannot compute Λ_p directly, we find a subset of $\Lambda/p\Lambda$ that contains Λ_p and that can be explicitly computed, then we show that none of the elements of this subset can be an element of Λ_p. If D is an element of Λ, we write $[D]_\Lambda = D \bmod p\Lambda$ to denote the class of D inside $\Lambda/p\Lambda$. The intersection pairing on Λ induces another symmetric pairing on $\Lambda/p\Lambda$,

$$\begin{aligned} \Lambda/p\Lambda \times \Lambda/p\Lambda &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ [D]_\Lambda \cdot [D']_\Lambda &\longmapsto D \cdot D' \bmod p. \end{aligned}$$

Let k_p denote the left kernel of this composition, and let M_p denote the subset of k_p given by

$$M_p := \{[D]_\Lambda \in k_p \mid [D]_\Lambda^2 \equiv 0 \bmod 2p^2\}. \tag{3·4}$$

LEMMA 3·7. *The subset M_p contains Λ_p and it is fixed by all the isometries of Λ_p.*

Proof. This proof is purely lattice-theoretic. For example, see [**Fes16**, lemma 1·1·23].

LEMMA 3·8. *The group G defined in* (3·3) *injects into* $\mathrm{O}(\Lambda)$.

Proof. By definition, G is a group of isometries of $\mathrm{Pic}\,\overline{\mathcal{X}}$. Using the explicit description of the elements of G and Λ, one can check that G preserves Λ and that no element of G acts as the identity on Λ. The statement follows.

We say that a class $E \in \mathrm{Pic}\,\overline{\mathcal{X}}$ is *effective* if it contains an effective divisor.

LEMMA 3·9. *Let S be a K3 surface. If $E \in \mathrm{Pic}\,S$ is a divisor class on S such that $E^2 = -2$, then either E or $-E$ is effective.*

Proof. This is a well known general result, see for example [**Fes16**, lemma 1·2·35] or [**Huy16**, section 1·2·3].

We are now ready to prove our main result.

LEMMA 3·10. *The kernel Λ_p is trivial for every prime p.*

Proof. By Remark 3·6, the statement holds for all primes $p \neq 2, 3$, so it suffices to prove the statement for $p = 2$ and $p = 3$. For this, we follow the proof of [**Fes16**, theorem 3·1·4].

Let p be equal to 2 or 3. From Lemma 3·8, we know that G acts on Λ. Since the $\mathbb{F}_p$-vector space Λ_p is the kernel of a G-equivariant homomorphism, it is G-invariant. So if an element $[x]_\Lambda$ is in Λ_p, its whole G-orbit, $G \cdot [x]_\Lambda$, is contained in Λ_p. Since the discriminant of Λ is $2^5\,3^3$, the $\mathbb{F}_p$-vector space Λ_p can have dimension at most 2 and 1, for $p = 2, 3$ respectively. Since Λ_p is stable under the action of G, it follows that the G-orbit of every element in Λ_p spans an $\mathbb{F}_p$-vector space of dimension at most 2 or 1, for $p = 2, 3$ respectively.

Analogous statements hold if we consider the action of just H (cf. (2·5)), instead of the whole of G.

Let $p = 2$. Using MAGMA, we explicitly compute the subset M_p. There is only one non-trivial H-orbit inside M_p spanning a vector subspace of dimension at most 2. Let W denote this subspace. The subspace W has dimension 2, and it admits a basis $\{w_1, w_2\}$ such that

$$w_1 = [E_1]_\Lambda$$
$$w_2 = [E_2]_\Lambda,$$

where the divisors are $E_1 := \psi_{0,3,0}B_3 - B_3$ and $E_2 := \tau_2^2\psi_{(x,y)}(\psi_{0,3,0}B_4 - B_4)$, and τ_2 denotes the automorphism in $\mathrm{Gal}(L/\mathbb{Q}(t))$ defined in Appendix B (cf. Table 1). Using the same technique as in Computations 3·4, one checks that $E_1^2 = E_2^2 = -8$. Assume w_1 is an element of Λ_p, then E_1 is an element of Λ that is 2-divisible in $\mathrm{Pic}\,\overline{\mathcal{X}}$, say $E_1 = 2C$, for some $C \in \mathrm{Pic}\,\overline{\mathcal{X}}$. Since $E_1^2 = -8$, the class C is a -2-class, and then either C' or $-C'$ is effective (cf. Lemma 3·9). By construction, $E_1 = E_{1,1} - E_{1,2}$, where $E_{1,1} = \psi_{0,3,0}B_4$ and $E_{1,2} = D_4$. Note that both $E_{1,1}$ and $E_{1,2}$ are elements of $G \cdot \Omega$, and so are isomorphic to plane conics; hence, $E_{1,1}^2 = E_{1,2}^2 = -2$. Let L be the hyperplane class in $\mathrm{Pic}\,\overline{\mathcal{X}}$, and notice that it is ample (in fact, $3L$ is very ample). Since $E_1 = 2C$, with C a -2-class, and L is ample, we have that the intersection number $H \cdot E_1 = 2H \cdot C$ is either positive or negative (according to whether C or $-C$ is effective); on the other hand, $E_1 = E_{1,1} - E_{1,2}$, and so $L \cdot E_1 = H \cdot E_{1,1} - L \cdot E_{1,2} = 2 - 2 = 0$, yielding a contradiction. Therefore E_1 cannot be 2-divisible. The same argument holds for E_2, as well as for any other element of W, since the

orbit of every element of W spans the whole of W; indeed, in M_p there are no 1-dimensional subspaces generated by H-orbits. Therefore Λ_2 is trivial.

Let $p = 3$. As before, we compute the subset M_p using MAGMA. Among the non-trivial vectors in M_p, we look for those whose orbit under G spans a 1-dimensional $\mathbb{F}_3$-vector space. It turns out that there are no such vectors. Thus Λ_3 is also trivial, completing the proof.

See [**BCFNW17**] for the MAGMA code used to perform the computations.

As noted before, Lemma 3·10 finally shows that

$$\operatorname{Pic} \overline{\mathcal{X}} = \Lambda.$$

This, together with Computations 3·4, completes the proof of Theorem 1·1.

4. *Consequences*

The explicit description of $\operatorname{Pic} \overline{\mathcal{X}}$ enables us to understand some arithmetic properties of the family X. For example, we can compute the Galois structure of $\operatorname{Pic} \overline{\mathcal{X}}$ and deduce the following result.

COMPUTATION 4·1. *Considering the action of* $\operatorname{Gal}(L/\mathbb{Q}(t))$ *on* $\operatorname{Pic} \overline{\mathcal{X}}$*, the following statements hold*:

(i) $H^0\big(\operatorname{Gal}(L/\mathbb{Q}(t)), \operatorname{Pic} \overline{\mathcal{X}}\big)$ *is isomorphic to* $\mathbb{Z}$*, and it is generated by the class of the hyperplane section of* $\mathcal{X}$;

(ii) $H^1\big(\operatorname{Gal}(L/\mathbb{Q}(t)), \operatorname{Pic} \overline{\mathcal{X}}\big)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^3$;

(iii) $H^2(\operatorname{Gal}(L/\mathbb{Q}(t)), \operatorname{Pic} \overline{\mathcal{X}}\big)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^{10}$;

(iv) *furthermore, for every non-trivial subgroup* $M \subset \operatorname{Gal}(L/\mathbb{Q}(t))$*, we have*

$$H^1(M, \operatorname{Pic} \mathcal{X}) \cong (\mathbb{Z}/2\mathbb{Z})^i$$

with $i \in \{0, 1, 2, 3, 4, 5, 6, 8, 10, 12\}$;

(v) *there are* 49 *normal subgroups* N *of* $\operatorname{Gal}(L/\mathbb{Q}(t))$ *for which* $H^1(N, \operatorname{Pic}(\overline{\mathcal{X}}))$ *is trivial*;

(vi) *there are* 47 *normal subgroups* N *of* $\operatorname{Gal}(L/\mathbb{Q}(t))$ *for which* $H^1(N, \operatorname{Pic}(\overline{\mathcal{X}}))$ *is non-trivial.*

Proof. By direct computations using MAGMA; see [**BCFNW17**] for the code.

Remark 4·2. Computation 4·1 can be useful for studying the existence of a Brauer-Manin obstruction on $\mathcal{X}$. In fact, the Hochschild–Serre spectral sequence implies the following isomorphism:

$$\frac{\operatorname{Br}_1 \mathcal{X}}{\operatorname{Br}_0 \mathcal{X}} \xrightarrow{\sim} H^1\big(\operatorname{Gal}\big(L/\mathbb{Q}(t)\big), \operatorname{Pic} \overline{\mathcal{X}}\big),$$

where $\operatorname{Br}_0 \mathcal{X}$ and $\operatorname{Br}_1 \mathcal{X}$ are the constant and the algebraic Brauer group of $\mathcal{X}$, respectively.

Theorem 1·1 not only gives us information about the arithmetic of $\mathcal{X}$, but also of the other fibers of X, as shown by the following results.

COROLLARY 4·3. *Any smooth fiber* X_{t_0} *of the family* X *has geometric Picard number at least* 19*. If the geometric Picard number of* X_{t_0} *is exactly* 19*, then* $\operatorname{Pic} X_{t_0,\overline{\mathbb{Q}}}$ *is isometric to* Λ*. The geometric Picard number of* X_{t_0} *is* 20 *if and only if* $-(4t_0)^3$ *is the* j*-invariant of an elliptic curve with complex multiplication.*

Proof. Theorem 1·1 tells us that $\operatorname{Pic}\overline{\mathcal{X}} = \Lambda$. From [**MP12**, proposition 3·6] we have that there is an embedding of $\operatorname{Pic}\overline{\mathcal{X}}$ inside $\operatorname{Pic} X_{t_0,\overline{\mathbb{Q}}}$ that respects the intersection pairing and has torsion free co-kernel. The existence of the embedding implies that $\operatorname{Pic} X_{t_0,\overline{\mathbb{Q}}}$ has rank at least 19. Since the embedding has torsion free co-kernel, if $\operatorname{Pic} X_{t_0,\overline{\mathbb{Q}}}$ has rank exactly 19, then the image of $\operatorname{Pic}\overline{\mathcal{X}}$ is the whole geometric Picard lattice of X_{t_0}. Finally, the last statement follows immediately from Proposition 2·3 and [**SS10**, 12·(26)].

Remark 4·4. It follows that there are only finitely many rational values of t_0 for which the Picard number of X_{t_0} is 20, namely

$$160080,\ 1320,\ 240,\ 24,\ 8,\ 15/4,\ 0,\ -3,\ -5,\ -33/2,\ -255/4.$$

Note that 0, -5, and $-33/2$ are the rational roots of the polynomial (2·8) from Section 2 whose roots are the values of t_0 for which X_{t_0} admits tri-tangent lines.

COROLLARY 4·5. *Let $t_0 \in \overline{\mathbb{Q}}$ be an algebraic number such that the fiber X_{t_0} is smooth. Then X_{t_0} is a K3 surface defined over the number field $\mathbb{Q}(t_0)$ and it has potentially dense rational points.*

Proof. Since X_{t_0} is smooth, it is a K3 surface, by Proposition 2·1; since t_0 is algebraic over $\mathbb{Q}$, the field $\mathbb{Q}(t_0)$ is a number field, and so the surface X_{t_0} can be defined over the number field $\mathbb{Q}(t_0)$. From Corollary 4·3 we have that X_{t_0} has geometric Picard number at least 19. Then the statement immediately follows from [**BT00**, theorem 1·1].

Remark 4·6. Let $a, b, c, d \in \overline{\mathbb{Q}}$ be four algebraic numbers, and let $X_{a,b,c,d}$ be the surface defined by

$$X_{a,b,c,d}\colon w^2 = ax^6 + by^6 + cz^6 + dx^2y^2z^2 \subset \mathbb{P}_{\overline{\mathbb{Q}}}. \tag{4·1}$$

Assume $X_{a,b,c,d}$ is smooth.

It is easy to see that $X_{a,b,c,d}$ is isomorphic, over $\overline{\mathbb{Q}}$, to $X_{e,\overline{\mathbb{Q}}}$, the fiber of the family X above the point $e = d \cdot \varepsilon$, where ε is a third-root of the product $a \cdot b \cdot c$.

This implies that the geometric Picard lattice of $X_{a,b,c,d}$ is isometric to $\operatorname{Pic} X_{e,\overline{\mathbb{Q}}}$, making it possible to use Corollaries 4·3 and 4·5 for K3 surfaces with defining equation as in (4·1).

Appendix A. Exposition on lattices

We briefly review the lattice theory that we use in Section 3, and refer the reader to [**Nik80a**] for more details.

In this article a *lattice* is a free abelian group, L, of finite rank equipped with a symmetric, non-degenerate, bilinear form $\langle\ ,\ \rangle : L \times L \to \mathbb{Z}$. We define the signature of L to be the signature of the extension to $\mathbb{R}$ of its bilinear form. We say that L is *positive definite* if it has signature $(b_+, 0)$, *negative definite* if it has signature $(0, b_-)$, and *indefinite* otherwise. We say that L is *even* if $\langle x, x\rangle \in 2\mathbb{Z}$ for all $x \in L$. Let $\{e_i\}$ be a basis for L; then the *Gram matrix* of L with respect to $\{e_i\}$ is the matrix $\left(\langle e_i, e_j\rangle\right)_{i,j}$. The *discriminant* of L, denoted $\operatorname{Disc}(L)$, is the determinant of the Gram matrix with respect to some basis; it is independent of the choice of basis.

We define $A_n(m)$ and $E_8(m)$ to be the lattices obtained from the root lattices A_n and E_8 (cf. [**CS99**, sections 4·6·1 and 4·8·1]), respectively, by multiplying their quadratic form by m.

Let L_1 and L_2 denote two lattices, with bases $\{e_i\}$ and $\{f_i\}$, respectively. Then $L_1 \oplus L_2$ denotes the lattice with basis $\{e_i\} \cup \{f_i\}$ and bilinear form extending that on L_1 and L_2 such that $\langle e_i, f_j \rangle = 0$ for all i, j. If $L_1 \subseteq L_2$ and $\mathrm{rk}(L_1) = \mathrm{rk}(L_2)$, then we say that L_1 is a *full rank sublattice* of L_2. In this situation, $\mathrm{Disc}(L_1)/\mathrm{Disc}(L_2) = [L_2 : L_1]^2$.

For any lattice L we define the *dual lattice*

$$L^* := \mathrm{Hom}(L, \mathbb{Z}) \cong \{x \in L \otimes \mathbb{Q} : \ \forall y \in L \ \ \langle x, y \rangle \in \mathbb{Z}\}.$$

The *discriminant group* of a lattice L is the finite abelian group $A_L := L^*/L$, and we denote by $\ell(A_L)$ the minimal number of generators of A_L. The discriminant group comes equipped with a bilinear form, $b_L : A_L \times A_L \to \mathbb{Q}/\mathbb{Z}$, defined by $b_L(x + L, y + L) = \langle x, y \rangle \bmod \mathbb{Z}$.

If L is an even lattice, we define the *discriminant form*,

$$\begin{aligned} q_L : A_L &\longrightarrow \mathbb{Q}/2\mathbb{Z} \\ x + L &\longmapsto \langle x, x \rangle \bmod 2\mathbb{Z}. \end{aligned}$$

We use the following theorem in Computation 3·4 to identify the lattice Λ.

THEOREM A·1 (Nikulin [**Nik80b**, corollary 1·13·3]). *If a lattice L is even and indefinite with* $\mathrm{rank}(L) > \ell(A_L) + 2$*, then L is determined up to isometry by its rank, signature and discriminant form.*

Appendix B. The Galois group in the generic case

Let K be the function field $\mathbb{Q}(t)$. In Section 2 we fixed an algebraic closure $\overline{K} = \overline{\mathbb{Q}(t)}$ of $\mathbb{Q}(t)$, and defined some elements in this algebraic closure. Recall that: ζ_{12} is defined to be a primitive 12th root of unity; ζ_n is defined to be the primitive nth root of unity given by $\zeta_{12}^{12/n}$, for $n = 3, 4, 6$; the elements β_i are such that $\beta_i^2 = t + 3\zeta_3^i$, for $i = 0, 1, 2$; the elements c_0, c_1, c_2 are the roots of the polynomial

$$h(x) := x^3 + tx^2 + 4 \in \mathbb{Q}(t)[x]; \tag{B 1}$$

the element δ is the product $4\zeta_4\beta_0\beta_1\beta_2$. We also defined the field L to be the Galois closure of the smallest extension of $\mathbb{Q}(t)$ containing all the elements defined above. In this section we explicitly describe L, as well as the Galois group $\mathrm{Gal}(L/\mathbb{Q}(t))$, proving the following theorem.

THEOREM B·1. *The field L is the field $K(\zeta_{12}, \beta_0, \beta_1, \beta_2, c_0)$. It is a Galois extension of degree $2^5 \cdot 3$ and its Galois group is isomorphic to the group*

$$S_3 \times \mathbb{Z}/2\mathbb{Z} \times D_4.$$

In the statement of the theorem, S_3, $\mathbb{Z}/2\mathbb{Z}$, and D_4 denote the permutation group of a set with three elements, the cyclic group with two elements, and the dihedral group with eight elements, respectively. In proving Theorem B·1 we will follow [**Fes16**, section 3·4].

Remark B·2. Recall that c_0, c_1, c_2 are the roots of the polynomial h defined in (B 1). Notice that h has discriminant $\Delta = -16(D^3 + 27) = (4\zeta_4\beta_0\beta_1\beta_2)^2 = \delta^2$. In particular, Δ is nonzero, so all the roots are distinct.

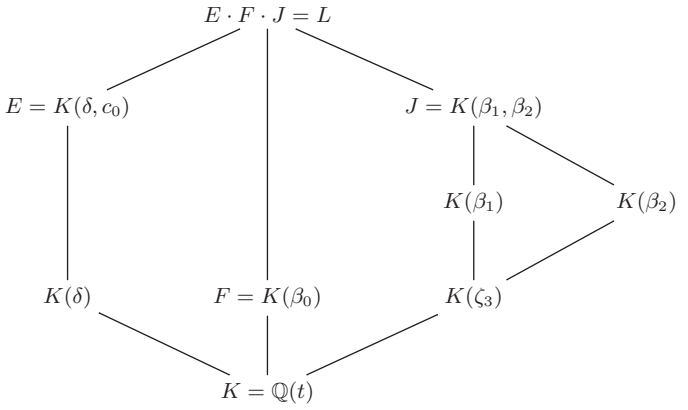

Fig. 1. An alternative description of L.

It is possible to explicitly write the roots c_1, c_2 in terms of the elements $\zeta_{12}, \beta_0, \beta_1, \beta_2$, and c_0. Namely, the other roots of h are

$$c_1 = \frac{-t - c_0 + \epsilon}{2} \text{ and } c_2 = \frac{-t - c_0 - \epsilon}{2},$$

where $\epsilon = \frac{\delta}{c_0(3c_0+2t)}$.

We now let E denote the field $K(\delta, c_0) \subset L$, and let F denote the field $K(\beta_0) \subset L$, and finally let J denote the field $K(\beta_1, \beta_2) \subset L$.

LEMMA B·3. *The following statements hold*:

(i) *the extension E/K is a Galois extension of degree* 6 *with Galois group* $\mathrm{Gal}(E/K) \cong S_3$;

(ii) *the extension F/K is a Galois extension of degree* 2 *with Galois group* $\mathrm{Gal}(F/K) \cong \mathbb{Z}/2\mathbb{Z}$;

(iii) *the extension J/K is a Galois extension of degree* 8 *with Galois group* $\mathrm{Gal}(J/K) \cong D_4$;

(iv) *the fields E, F, and J intersect pairwise trivially; that is, the intersection of any two of them equals K*;

(v) *the compositum field $E \cdot F \cdot J$ equals L.*

Proof.

(i) By construction, the field E is the splitting field of the cubic polynomial $h = x^3 + tx^2 + 4$, that is irreducible over K and whose discriminant is not a square in K. The statement follows.

(ii) The field F is the splitting field of the degree two polynomial $x^2 - (3+t)$. The statement trivially follows.

(iii) The field J is the splitting field of the polynomial

$$l = x^4 + (-2t + 3)x^2 + t^2 - 3t + 9,$$

and so J/K is a Galois extension. The roots of l are $\pm\beta_1, \pm\beta_2$, therefore the Galois group $\mathrm{Gal}(J/K)$ is generated by $\gamma_1, \gamma_2, \gamma$, where γ_1 changes the sign of β_1, γ_2 changes the sign of β_2, and γ switches β_1 and β_2. Since J/K is Galois, we have the following chain of equalities: $\#\mathrm{Gal}(L/K) = [L : K] = 8$. One can easily check that $\gamma\,\gamma_1 \neq \gamma_1\gamma$, and that these two are the only elements of order 4 of $\mathrm{Gal}(J/K)$. Summarising, $\mathrm{Gal}(J/K)$ is a non-abelian group of order 8 with exactly two elements of order 4. Thus $\mathrm{Gal}(J/K)$ is isomorphic to D_4.

(iv) By explicit computations using MAGMA ([**BCP97**]), code available at [**BCFNW17**]. As an example, we show the argument to prove the statement for F and J. By point *(ii)*, the field $F \cap J$ is an extension of degree at most 2 over K. If we assume that $F \cap J \neq K$, it follows that $F \cap J = F$ and, therefore, that $\beta_0 \in J$. By writing J as

$$\mathbb{Q} \oplus \zeta_3\mathbb{Q} \oplus \beta_1\mathbb{Q} \oplus \zeta_3\beta_1\mathbb{Q} \oplus \beta_2\mathbb{Q} \oplus \zeta_3\beta_2\mathbb{Q} \oplus \beta_1\beta_2\mathbb{Q} \oplus \zeta_3\beta_1\beta_2\mathbb{Q}$$

one can show, after some computations, that the equation $t^2 + 3$ has no solution in J, i.e., $\beta_0 \notin J$, getting a contradiction. We can hence conclude that $F \cap J = K$.

(v) Recall that L is, by definition, the Galois closure of the smallest field extension of K containing ζ_{12}, β_i, c_i, for $i = 0, 1, 2$. Hence notice that also δ is in L.
Let L' denote the compositum field $E \cdot F \cdot J$. By construction, L' contains the elements, $\delta, c_0, \beta_0, \beta_1, \beta_2$. Then, by Remark B·2, we have that also c_1 and c_2 are in L'. From $\beta_i \in L'$, it follows that $\frac{1}{3}(\beta_1^2 - t) = \zeta_3 \in L$. Hence, the ratio

$$\alpha := \frac{4\zeta_3\beta_0\beta_1\beta_2}{4\zeta_4\beta_0\beta_1\beta_2} = \frac{\zeta_3}{\zeta_4}$$

is also inside L'. Recall that $\zeta_3 = \zeta_{12}^4$ and $\zeta_4 = \zeta_{12}^3$, then

$$\alpha = \frac{\zeta_3}{\zeta_4} = \frac{\zeta_{12}^4}{\zeta_{12}^3} = \zeta_{12}.$$

Hence ζ_{12} is an element of L'. It follows that L' is the smallest field extension of K containing ζ_{12}, β_i, c_i, for $i = 0, 1, 2$.
In order to show that $L = L'$ it suffices to show that the extension L'/K is Galois. This follows from the fact that L' is the compositum of three Galois extensions of K that intersect pairwise trivially. Hence L' is Galois over K and therefore it equals its Galois closure, i.e., $L = L'$.

Proof of Theorem B·1 The fact that L equals the field $K(\zeta_{12}, \beta_0, \beta_1, \beta_2, c_0)$ immediately follows from Lemma B·3(v).

The field extension L/K is Galois by definition. Being Galois, its degree equals the cardinality of its Galois group.

From Lemma B·3(v), L equals the compositum of the fields E, F and J; from Lemma B·3(iv), these fields are pairwise distinct, and so

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \times \mathrm{Gal}(J/K).$$

The theorem now follows from Lemma B·3(i)-(iii).

Remark B·4. In order to perform explicit operations using the automorphisms of $\mathrm{Gal}(L/K)$, it is useful to give an isomorphism between $\mathrm{Gal}(L/K)$ and $S_3 \times \mathbb{Z}/2\mathbb{Z} \times D_4$. In order to do so, we will present five automorphisms $\tau_i \in \mathrm{Gal}(K_2/K)$, with $i = 1, 2, 3, 4, 5$, such that:

$$\begin{aligned} \mathrm{Gal}(E/K) &= \langle \tau_1, \tau_2 \rangle \cong S_3; \\ \mathrm{Gal}(F/K) &= \langle \tau_3 \rangle \cong \mathbb{Z}/2\mathbb{Z}; \\ \mathrm{Gal}(J/K) &= \langle \tau_4, \tau_5 \rangle \cong D_4. \end{aligned}$$

The field L is generated by $c_0, \zeta_{12}, \beta_0, \beta_1, \beta_2$ over K, so to describe an element $\tau \in \mathrm{Gal}(L/K)$ it is enough to describe its action on those elements. The action of τ_i on those

Table 1. *The action of $\tau_1, ..., \tau_5$ on a set of elements of L.*

	c_0	c_1	c_2	δ	ζ_{12}	ζ_4	ζ_3	β_0	β_1	β_2
τ_1	c_0	c_2	c_1	$-\delta$	ζ_{12}^7	$-\zeta_4$	ζ_3	β_0	β_1	β_2
τ_2	c_1	c_2	c_0	δ	ζ_{12}	ζ_4	ζ_3	β_0	β_1	β_2
τ_3	c_0	c_1	c_2	δ	ζ_{12}^7	$-\zeta_4$	ζ_3	$-\beta_0$	β_1	β_2
τ_4	c_0	c_1	c_2	δ	ζ_{12}^{11}	$-\zeta_4$	ζ_3^2	β_0	$-\beta_2$	β_1
τ_5	c_0	c_1	c_2	δ	ζ_{12}^7	$-\zeta_4$	ζ_3	β_0	β_1	$-\beta_2$

generators of L over K is listed in Table 1. For the convenience of the reader, the table also lists the action of τ_i, for $i = 1, ..., 5$, on other interesting elements of L.

Acknowledgments. We thank Anthony Várilly–Alvarado for bringing this problem to our attention, and the Arizona Winter School for creating opportunities for research and providing an excellent platform for collaboration. We thank Noam Elkies, Andreas–Stephan Elsenhans, Eric Larson, Ronald van Luijk, Abraham Varghese and Isabel Vogt for helpful discussions; and the anonymous referee for their detailed comments.

REFERENCES

[**BCFNW17**] F. Bouyer, E. Costa, D. Festi, C. Nicholls and M. West. Accompanying MAGMA code. `http://www.staff.uni-mainz.de/dfesti/ AWS2015Magma.txt` (2017).

[**BCP97**] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3-4) (1997), 235–265. Computational algebra and number theory (London, 1993).

[**BHPVdV04**] W. P. Barth, K. Hulek, C. A. M. Peters and A. Van de Ven. Compact complex surfaces volume 4 of *Ergeb. Math. Grenzgeb.* 3. *Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas.* 3*rd Series. A Series of Modern Surveys in Mathematics]*. (Springer-Verlag, Berlin, second edition, 2004).

[**BT00**] F. A. Bogomolov and Yu. Tschinkel. Density of rational points on elliptic K3 surfaces. *Asian J. Math.* **4**(2) (2000), 351–368.

[**Cha14**] F. Charles. On the Picard number of K3 surfaces over number fields. *Algebra Number Theory* **8**(1) (2014), 1–17.

[**CS99**] J. H. Conway and N. J. A. Sloane. Sphere packings, lattices and groups. Grundlehren Math Wiss vol. 290 *[Fundamental Principles of Mathematical Sciences]*. (Springer-Verlag, New York, third edition, 1999). With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[**Dol96**] I. V. Dolgachev. Mirror symmetry for lattice polarised K3 surfaces. *J. Math. Sci.* **81**(3) (1996), 2599–2630. Algebraic geometry, 4.

[**EJ08**] A.-S. Elsenhans and J. Jahnel. $K3$ surfaces of Picard rank one and degree two. In *Algorithmic number theory Lecture Notes in Comput. Sci.* vol. 5011 (Springer, Berlin, 2008), pp. 212–225.

[**EJ11**] A.-S. Elsenhans and J. Jahnel. The Picard group of a $K3$ surface and its reduction modulo p. *Algebra Number Theory* **5**(8) (2011), 1027–1040.

[**Fes16**] D. Festi. Topics in the arithmetic of del Pezzo and K3 surfaces. PhD. thesis. Universiteit Leiden (2016).

[**Har77**] R. Hartshorne. *Algebraic geometry* Graduate Texts in Math. No. 52. (Springer-Verlag, New York-Heidelberg, 1977).

[**HKT13**] B. Hassett, A. Kresch and Y. Tschinkel. Effective computation of Picard groups and Brauer–Manin obstructions of degree two K3 surfaces over number fields. *Rendiconti del Circolo Matematico di Palermo* **62**(1) (2013), 137–151.

[**HS00**] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction* Graduate Texts in Math. vol. 201 (Springer-Verlag, New York, 2000).

[**Huy16**] D. HUYBRECHTS. *Lectures on K3 surfaces Camb. Stud. Adv. Math*. vol. 158 (Cambridge University Press, Cambridge, 2016).

[**Ino78**] H. INOSE. Defining equations of singular $K3$ surfaces and a notion of isogeny. In *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto,* 1977*)* (Kinokuniya Book Store, Tokyo, 1978), pp. 495–502.

[**KT04**] A. KRESCH and Y. TSCHINKEL. On the arithmetic of del Pezzo surfaces of degree 2. *Proc. London Math. Soc.* (3) **89**(3) (2004), 545–569.

[**MP12**] D. MAULIK and B. POONEN. Néron-Severi groups under specialisation. *Duke Math. J.* **161**(11) (2012), 2167–2206.

[**Mum70**] D. MUMFORD. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay (Oxford University Press, London, 1970).

[**Nik80a**] V. V. Nikulin. Integer symmetric bilinear forms and some of their geometric applications. *Math USSR-Izv* **14**(1) (1980), 103–167.

[**Nik80b**] V. V. NIKULIN. Integral symmetric bilinear forms and some of their applications. *Mathematics of the USSR-Izvestiya*, **14**(1) (1980), 103.

[**PTvL15**] B. POONEN, D. TESTA and R. VAN LUIJK. Computing Néron-Severi groups and cycle class groups. *Compositio. Math.* **151**(4) (2015), 713–734.

[**SS10**] M. SCHÜTT and T. SHIODA. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul* 2008 Adv. Stud. Pure Math. vol. 60 (Math. Soc. Japan, Tokyo, 2010), pp. 51–160.

[**ST10**] M. STOLL and D. TESTA. The surface parametrising cuboids. `arXiv:1009.0388` (2010).

[**VAV11**] A. VÁRILLY–ALVARADO and B. VIRAY. Failure of the Hasse principle for Enriques surfaces. *Adv. Math.* **226**(6) (2011), 4884–4901.

[**vL07**] R. VAN LUIJK. An elliptic $K3$ surface associated to Heron triangles. *J. Number Theory* **123**(1) (2007), 92–119.