EXPLICIT FAMILIES OF $K3$ SURFACES HAVING REAL MULTIPLICATION

ANDREAS-STEPHAN ELSENHANS AND JÖRG JAHNEL

Abstract. For families of $K3$ surfaces, we establish a sufficient criterion for real or complex multiplication. Our criterion is arithmetic in nature. It may show, at first, that the generic fibre of the family has a nontrivial endomorphism field. Moreover, the endomorphism field does not shrink under specialisation. As an application, we present two explicit families of $K3$ surfaces having real multiplication by $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, respectively.

1. Introduction

Complex multiplication is a phenomenon that has been intensively studied, first and foremost for complex elliptic curves, cf. [Si, Chapter II] or [Cox, Chapter 3]. According to its very definition, it is a purely geometric property. Nevertheless, it has arithmetic consequences and much of the interest in complex multiplication stems from these. The generalisation to higher-dimensional abelian varieties is straightforward, except for the fact that, besides complex multiplication, the similar phenomena of real and quaternionic multiplication may occur. Abelian varieties are, however, not the limit.

For instance, let $\mathfrak{X}$ be a projective complex $K3$ surface. In this situation, the occurrence of real and complex multiplication phenomena has been observed by Yu. G. Zarhin [Za]. They are certainly deeper for $K3$ surfaces than for abelian varieties, because they do not concern the complex manifold directly, but merely its cohomology.

More concretely, the cohomology $\mathbb{Q}$-vector space $H^2(\mathfrak{X}, \mathbb{Q})$ is of dimension 22. On the other hand, the rank of the Picard group $\operatorname{Pic}\mathfrak{X}$ may vary between 1 and 20. Put $P := c_1(\operatorname{Pic}\mathfrak{X})\otimes_{\mathbb{Z}}\mathbb{Q} \subset H^2(\mathfrak{X}, \mathbb{Q})$ and $T := P^\perp$, these subspaces being called the algebraic and transcendental parts of $H^2(\mathfrak{X}, \mathbb{Q})$, respectively. Then T is not just a $\mathbb{Q}$-vector space, but a pure $\mathbb{Q}$-Hodge structure [De71, Section 2.2]. The endomorphism algebra $\operatorname{End}_{\mathrm{Hodge}}(T)$ is generically just $\mathbb{Q}$, but may as well be a totally real field $E \supsetneq \mathbb{Q}$ or a CM-field [Za, Theorems 1.6.a) and 1.5.1].

For an analysis of real and complex multiplications from the analytic point of view, we refer the reader to [vG], for an interesting application of real multiplication

---

Date: August 21, 2020.

2010 *Mathematics Subject Classification.* 14J28 primary; 14F20, 14F25, 14J10, 14J20, 11T06 secondary.

Key words and phrases. $K3$ surface, real multiplication, explicit examples.

to [Ch14]. On the other hand, at least as far as real multiplication is concerned, the only explicit example surfaces known seem to be the ones presented by the authors in [EJ14]. In that article, a few 1-parameter families were given, as well as some isolated examples, which conjecturally have RM. For one of these families, RM by $\mathbb{Q}(\sqrt{2})$ was proven, at least for countably many of its members.

Terminology. i) If $\mathbb{Q} \subsetneqq E = \mathrm{End}_{\mathrm{Hodge}}(T)$ is a totally real field then we say that $\mathfrak{X}$ has *real multiplication (RM)* by E. If E is a CM-field then we say that $\mathfrak{X}$ has *complex multiplication (CM)* by E.

ii) In either case, we call $E = \mathrm{End}_{\mathrm{Hodge}}(T)$ the *endomorphism field* of $\mathfrak{X}$ (and T).

iii) If it happens that $\mathbb{Q} \subseteq E' \subseteq E = \mathrm{End}_{\mathrm{Hodge}}(T)$ then $\mathfrak{X}$ (and T) are said to be *acted upon* by E'.

The main result–A sufficient criterion for RM or CM. The following criterion is the main result of this article. It is a relative version of [EJ14, Lemma 6.1].

Theorem 1.1 (Sufficient criterion for RM or CM in families)**.** *Consider a proper and smooth morphism $\underline{q}\colon \underline{X} \to \underline{B}$ of irreducible schemes of finite type over $\mathbb{Z}[\frac{1}{l}]$, every fibre of which is a $K3$ surface. Suppose that B is a normal scheme and has a $\mathbb{Q}$-rational point.*

a) *Assume that there exists a number field K that is Galois over $\mathbb{Q}$ and a conjugacy class c of elements in $\mathrm{Gal}(K/\mathbb{Q})$ with the property below: For every prime number p such that $\mathrm{Frob}_p \in c$ and every $\mathbb{F}_p$-rational point $\tau \in \underline{B}(\mathbb{F}_p)$, the special fibre $\underline{X}_\tau$ has point count*

$$\#\underline{X}_\tau(\mathbb{F}_p) \equiv 1 \pmod{p}\,. \tag{1}$$

Then the generic fibre X_η has real or complex multiplication.

b) *Assume that the generic fibre X_η has real or complex multiplication by some endomorphism field E. Then, for every complex point $z \in B(\mathbb{C})$, the $K3$ surface $X_z(\mathbb{C})$ is acted upon by E.*

Remarks 1.2. i) (Cyclotomic case) Put $K := \mathbb{Q}(\zeta_D)$, for an arbitrary positive integer D. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/D\mathbb{Z})^*$, which is an abelian group. Hence, the conjugacy classes of elements are singletons. Moreover, the condition $\mathrm{Frob}_p \in c$ simply means that $p \equiv a \pmod{D}$, for a certain integer a prime to D.

ii) Even under a congruence condition of the type described in i), the strongest and most unlikely looking of the assumptions above is, of course, formula (1) concerning the point count. Note, however, that real multiplication tends to cause exactly such a behaviour [EJ14, Corollary 4.13.i)]. In Examples 5.1 and 1.5, we present explicit families of $K3$ surfaces, for which (1) is established by elementary arguments.

Remark 1.3. In order to apply the criterion above, one further needs methods to determine the endomorphism field E of a particular $K3$ surface, under the assumption that $E \supsetneqq \mathbb{Q}$ is already known. For the convenience of the reader, in Section 6, we add some information on how to handle the case of a quadratic field. I.e., how to prove that $[E:\mathbb{Q}]=2$ and how to determine which quadratic field exactly occurs. The method described has essentially been known before, cf. [EJ14].

Remark 1.4. We prove Theorem 1.1.a) in Section 3, as Theorem 3.5, and Theorem 1.1.b) in Section 4. In fact, for part b), the assumptions may be somewhat weakened. Cf. Corollary 4.7 for an exact formulation.

The link to the arithmetic. Theorem 1.1.a) is arithmetic in nature, taking as its main assumption condition (1) on the numbers of points on the reductions modulo p, for infinitely many prime numbers p. The link between RM and CM, i.e. Hodge structures, and arithmetic works as follows.

Let X be a $K3$ surface over a field $k \subset \mathbb{C}$ that is finitely generated over $\mathbb{Q}$. Under the canonical isomorphism $\iota\colon H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1)) \to H^2(X(\mathbb{C}),\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_l(1)$ between étale and complex cohomology [SGA4, Exposé 11, Théorème 4.4.iii)], the algebraic classes and the cup product pairing are respected. Thus, $T \otimes_{\mathbb{Q}} \mathbb{Q}_l(1)$, for $T \subset H^2(Z(\mathbb{C}),\mathbb{Q})$ the transcendental part, gets identified with $\mathscr{T} \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$, the transcendental part of étale cohomology. As a consequence of this, by transport of structure, one has an operation

$$E = \mathrm{End}_{\mathrm{Hodge}}(T) \hookrightarrow \mathrm{End}(\mathscr{T}) \qquad (2)$$

of $E = \mathrm{End}_{\mathrm{Hodge}}(T)$ on $\mathscr{T}$.

It is well-known [Za, Ta90, Ta95, An] that the neutral component of the algebraic monodromy group of $\mathscr{T}$ is given by $\mathrm{MG}^0_{\mathscr{T},k,l} = (C_{\mathrm{GO}(\mathscr{T})}(E))^0$. Cf. Example 2.3.v). I.e., except for the case of geometric Picard rank 20, in which $\mathrm{GO}^0(\mathscr{T})$ is abelian and CM is automatic [Hu, Remark 3.3.10], one has $\mathrm{MG}^0_{\mathscr{T},k,l} \subsetneqq \mathrm{GO}^0(\mathscr{T})$ if and only if $E \supsetneqq \mathbb{Q}$.

Further results. We reverse this result in Theorem 4.1 and prove

$$C_{\mathrm{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) = E \otimes_{\mathbb{Q}} \mathbb{Q}_l\,.$$

Thus, the endomorphism field E is determined by the algebraic monodromy group, at least up to arithmetic equivalence [Pe]. This fixes the degree of E and in many situations E itself, for example when E is Galois over $\mathbb{Q}$ or when $[E\!:\!\mathbb{Q}] < 7$ [BdS]. It turns out (cf. Corollary 4.4) that there is another situation, in which E is independent of $k \hookrightarrow \mathbb{C}$, namely when the base field k is primary over $\mathbb{Q}$, i.e. does not contain any proper algebraic extension of $\mathbb{Q}$.

More terminology. Let k be a field that is finitely generated over $\mathbb{Q}$ and X a $K3$ surface over k. Assume that k is primary over $\mathbb{Q}$ or that $\mathrm{rk}\,\mathrm{Pic}\,X_{\overline{k}} > 15$.

i) We say that X has real or complex multiplication if $X(\mathbb{C})$ has. (This terminology is used in Theorem 1.1.a) for the generic fibre X_η.)

ii) Similarly, we shall fell free to speak of the endomorphism field of X, instead of $X(\mathbb{C})$.

Applications. As an application, in Section 5, we return to the family from [EJ14] and prove that actually every member is acted upon by $\mathbb{Q}(\sqrt{2})$. Moreover, we present a new family, all members of which are acted upon by $\mathbb{Q}(\sqrt{5})$.

Example 1.5 (An explicit family of $K3$ surfaces with RM by $\mathbb{Q}(\sqrt{5})$). Let $q\colon X \to B$, for $B := \operatorname{Spec} \mathbb{Q}[t, \frac{1}{(t-1)(t^4-t^3+t^2-t+1)}] \subset \mathbf{A}^1_{\mathbb{Q}}$, be the family of $K3$ surfaces that is fibre-by-fibre the minimal desingularisation of the double cover of $\mathbf{P}^2$, given by

$$\begin{aligned} w^2 = y(x - 2(t-1)y - tz) & \\ (x^4 + x^3y - x^3z + x^2y^2 - 2x^2yz + x^2z^2 + xy^3 - 3xy^2z - 2xyz^2 - xz^3 + y^4 & \\ + y^3z + y^2z^2 + yz^3 + z^4) \, . & \end{aligned} \tag{3}$$

i) Then the generic fibre X_η of q is of geometric Picard rank 16.

ii) The endomorphism field of X_η is $\mathbb{Q}(\sqrt{5})$.

iii) For every $\theta \in B(\mathbb{C})$, the transcendental part $T \subset H^2(X_\theta(\mathbb{C}), \mathbb{Q})$ of the cohomology of the fibre X_θ is acted upon by $\mathbb{Q}(\sqrt{5})$.

iv) Let the complex point $\theta \in B(\mathbb{C})$ be of the kind that the fibre X_θ has Picard rank 16. Then X_θ has real multiplication by $\mathbb{Q}(\sqrt{5})$.

Proof. We prove these results in Section 6. □

The Tate conjecture for $K3$ surfaces. Our arguments make use of the Tate conjecture, in situations where it is known to be true. More concretely, what we use is the following.

Facts 1.6 (Known cases of the Tate conjecture)**.** *Let k be field that is*

a) *finitely generated over $\mathbb{Q}$ or*

b) *a finite field*

and X a $K3$ surface over k. Then the subspace $H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))^{\operatorname{Gal}(\overline{k}/k)}$ of invariants coincides with $c_1(\operatorname{Pic} X) \otimes_{\mathbb{Z}} \mathbb{Q}_l \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$.

Proof. a) This is due to Y. André [An, Section 6.2]. More recent developments are described in [Mo, Proposition 9.2].

b) In this situation, the result is known due to the combined work of several people, most notably F. Charles [Ch13], M. Lieblich, D. Maulik, and A. Snowden [LMS], K. Madapusi Pera [MP], as well as W. Kim and K. Madapusi Pera [KM]. □

Conventions and Notation. We follow standard conventions and use standard notation from Algebra and Algebraic Geometry. More specifically,

i) For a field k, we denote by $\overline{k}$ a separable closure. For a point $t\colon \operatorname{Spec} k \to X$, we write $\overline{t}\colon \operatorname{Spec} \overline{k} \to \operatorname{Spec} k \to X$ for the resulting geometric point.

ii) We usually denote the generic point on a connected scheme by η.

iii) We say that a proper scheme X over a number field k has good reduction at a prime ideal $\mathfrak{p}$ of k, if there exists a proper model $\underline{X}$ over the integer ring $\mathscr{O}_k \subset k$ that is smooth above $\mathfrak{p}$.

iv) When $\underline{B}, \underline{X}, \ldots$ is a scheme of finite type over $\operatorname{Spec} \mathbb{Z}$, we write B, X etc. for its generic fibre. E.g., $B := \underline{B} \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Q}$.

v) For a $K3$ surface X over a field $k \subset \mathbb{C}$ that is finitely generated over $\mathbb{Q}$, the canonical comparison isomorphism [SGA4, Exposé 11, Théorème 4.4.iii)] induces an isomorphism $\mathscr{T} \cong T \otimes_{\mathbb{Q}} \mathbb{Q}_l(1)$, for $T \subset H^2(X(\mathbb{C}), \mathbb{Q})$ and $\mathscr{T} \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$ the transcendental parts. We identify the two $\mathbb{Q}_l$-vector spaces and consider T as a subset of $\mathscr{T}$.

Except for Corollary 4.2, we fix a prime number l throughout the article.

vi) For an algebraic group G, we denote by G^0 its neutral component with respect to the Zariski topology. Similarly for the group of the $\mathbb{Q}_l$-rational points on an algebraic group defined over $\mathbb{Q}_l$.

vii) We let $\mathrm{O}_n \subset \mathbf{A}_k^{n^2}$ be the orthogonal group and $\mathrm{SO}_n \subset \mathrm{O}_n$ the special orthogonal group. The base field k, which is suppressed in the notation, is of characteristic $\neq 2$ throughout the article. Usually, we have $k = \mathbb{Q}_l$.

The group of the $\mathbb{Q}_l$-rational points on O_n is $\mathrm{O}_n(\mathbb{Q}_l) = \{A \in \mathrm{M}_{n\times n}(\mathbb{Q}_l) \mid AA^t = E_n\}$.

viii) We denote by GO_n the linear algebraic group $\mathbb{G}_m{\cdot}\mathrm{O}_n$. In characteristic different from 2, GO_n is irreducible for n odd and has two components for n even. In any case, one has $\mathrm{GO}_n^0 = \mathbb{G}_m{\cdot}\mathrm{SO}_n$.

When $\mathscr{T}$ is a finite-dimensional $\mathbb{Q}_l$-vector space equipped with a non-degenerate symmetric bilinear form, we use the notation $\mathrm{GO}(\mathscr{T})$ for the group of all orthogonal similitudes of $\mathscr{T}$.

ix) When A is an algebra and $G, H \subseteq A$ are either subalgebras or subgroups of the multiplicative group $A^* \subset A$ then $C_H(G) := \{h \in H \mid \forall g \in G\colon hg = gh\}$ denotes the centraliser of G in H.

Computations. All computations are done with `magma` [BCP] on one core of an AMD Phenom II X4 955 processor running at 3.2 GHz.

2. Algebraic monodromy groups

Algebraic monodromy groups are the main tool that is used in the present article. The purpose of this section is primarily to recall the relevant facts and to fix notation.

Let B be an arbitrary connected scheme, on which a geometric point $\overline{s}$ is fixed as the base point. As is well-known [SGA5, Exposé VI, Lemme 1.2.4.2], associated with any $\mathbb{Q}_l$-sheaf $\mathscr{Q}$ on B that is twisted-constant with respect to the étale topology and of finite rank, one has a continuous representation

$$\varrho_{\overline{s}}^{\mathscr{Q}}\colon \pi_1^{\text{ét}}(B, \overline{s}) \longrightarrow \mathrm{GL}(\mathscr{Q}_{\overline{s}}) \tag{4}$$

of the étale fundamental group of B.

Definition 2.1. The Zariski closure of the image of $\varrho_{\overline{s}}^{\mathscr{Q}}$ is called the *algebraic monodromy group* $\mathrm{MG}_{\mathscr{Q},B,l}$ of $\mathscr{Q}$. This is the set of all $\mathbb{Q}_l$-rational points on an algebraic group defined over $\mathbb{Q}_l$. The algebraic group is possibly disconnected.

Remark 2.2. Let $\overline{s}'$ be another geometric point on B. One may then choose an étale path $\gamma \in \pi_1^{\text{ét}}(B, \overline{s}, \overline{s}')$, which yields an isomorphism $i_\gamma \colon \mathscr{Q}_{\overline{s}} \to \mathscr{Q}_{\overline{s}'}$. The diagram

$$\begin{array}{ccc} \pi_1^{\text{ét}}(B, \overline{s}) & \xrightarrow{\varrho_{\overline{s}}^{\mathscr{Q}}} & \mathrm{GL}(\mathscr{Q}_{\overline{s}}) \\ {\scriptstyle \sigma \mapsto \gamma\sigma\gamma^{-1}} \downarrow & & \downarrow {\scriptstyle M \mapsto i_\gamma M i_\gamma^{-1}} \\ \pi_1^{\text{ét}}(B, \overline{s}') & \xrightarrow{\varrho_{\overline{s}'}^{\mathscr{Q}}} & \mathrm{GL}(\mathscr{Q}_{\overline{s}'}) \end{array}$$

then commutes. I.e., γ induces an isomorphism between $\mathrm{GL}(\mathscr{Q}_{\overline{s}})$ and $\mathrm{GL}(\mathscr{Q}_{\overline{s}'})$ that maps the two instances of $\mathrm{MG}_{\mathscr{Q},B,l}$ onto each other.

Examples 2.3. i) Let $B = \operatorname{Spec} k$, for k a field. Then (4) specialises to a representation of $\mathrm{Gal}(\overline{k}/k) = \pi_1^{\text{ét}}(\operatorname{Spec} k, \operatorname{Spec} \overline{k})$. The algebraic monodromy group $\mathrm{MG}_{\mathscr{Q},k,l}$ of $\mathscr{Q}$ is the Zariski closure of the image of $\mathrm{Gal}(\overline{k}/k)$ in $\mathrm{GL}(\mathscr{Q}_{\overline{k}})$.

ii) When B is an arbitrary scheme of residue characteristics different from l and $q \colon X \to B$ a smooth and proper morphism then the proper and smooth base change theorems [SGA4, Exposé XVI, Corollaire 2.2] imply that the higher direct image sheaves $R^i q_* \mathbb{Q}_l(j)$ are twisted-constant $\mathbb{Q}_l$-sheaves, for all $i, j \in \mathbb{N}$. One has the algebraic monodromy group $\mathrm{MG}_{R^i q_* \mathbb{Q}_l(j),B,l} \subseteq \mathrm{GL}((R^i q_* \mathbb{Q}_l(j))_{\overline{s}}) = \mathrm{GL}(H^i_{\text{ét}}(X_{\overline{s}}, \mathbb{Q}_l(j)))$.

iii) Suppose that the fibres of q are of dimension i, for an even integer i. Then the stalks of $R^i q_* \mathbb{Q}_l(i/2)$ at the geometric point $\overline{s}$ are equipped with the symmetric pairing, induced by cup product and Poincaré duality. As a consequence of this,

$$\mathrm{MG}_{R^i q_* \mathbb{Q}_l(i/2),B,l} \subseteq \mathrm{GO}((R^i q_* \mathbb{Q}_l(i/2))_{\overline{s}}) = \mathrm{GO}(H^i_{\text{ét}}(X_{\overline{s}}, \mathbb{Q}_l(i/2)))\,.$$

iv) Assume, in addition, that there is given a decomposition $R^i q_* \mathbb{Q}_l(i/2) = \mathscr{P} \oplus \mathscr{T}$ into two twisted-constant subsheaves, whereas the restriction of the cup product pairing to $\mathscr{P}_{\overline{s}}$ is non-degenerate. Then the same is true for $\mathscr{T}_{\overline{s}}$ and the algebraic monodromy group $\mathrm{MG}_{\mathscr{T},B,l}$ is contained in $\mathrm{GO}(\mathscr{T}_{\overline{s}})$.

v) (Zarhin, Tankeev, André) Consider the situation that $B = \operatorname{Spec} k$, for k a field that is finitely generated over $\mathbb{Q}$, X is a $K3$ surface over k, and $\mathscr{T} \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$ is the transcendental part.

Then the neutral component of the algebraic monodromy group of $\mathscr{T}$ is equal to the neutral component of the centraliser of E in $\mathrm{GO}(\mathscr{T})$,

$$\mathrm{MG}^0_{\mathscr{T},k,l} = (C_{\mathrm{GO}(\mathscr{T})}(E))^0\,. \tag{5}$$

Here, the endomorphism field $E = \mathrm{End}_{\mathrm{Hodge}}(T)$ is considered as being contained in $\mathrm{End}(\mathscr{T})$ via the operation (2).

Indeed, (5) follows from Yu. G. Zarhin's explicit description of the Mumford-Tate group in the case of a complex $K3$ surface [Za, Theorem 2.2.1], together with the Mumford-Tate conjecture, cf. [Ch14, Theorem 13]. The Mumford-Tate conjecture was proven for $K3$ surfaces over number fields by S. G. Tankeev [Ta90, Ta95] and over arbitrary finitely generated extensions of $\mathbb{Q}$ by Y. André [An, Théorème 8.2]. Cf. [Com, Theorem 1.1] for recent developments.

2.4 (Base change). Let $i\colon B' \to B$ be a morphism of connected schemes and $\overline{s}$ any geometric point on B'. Then i induces an isomorphism $(i^*\mathscr{Q})_{\overline{s}} \cong \mathscr{Q}_{\overline{i(s)}}$ and a homomorphism $i_\#\colon \pi_1^{\text{ét}}(B',\overline{s}) \to \pi_1^{\text{ét}}(B,\overline{i(s)})$, via which one has a natural inclusion

$$\mathrm{MG}_{i^*\mathscr{Q},B',l} \hookrightarrow \mathrm{MG}_{\mathscr{Q},B,l}$$

of subgroups of $\mathrm{GL}((i^*\mathscr{Q})_{\overline{s}}) \cong \mathrm{GL}(\mathscr{Q}_{\overline{i(s)}})$.

i) This applies, of course, when $s\colon \operatorname{Spec} k \to B$ is a point,

$$\mathrm{MG}_{\mathscr{Q}|_s,k,l} \hookrightarrow \mathrm{MG}_{\mathscr{Q},B,l}\ .$$

Note here that, in view of Remark 2.2, one may assume the base point on B to be chosen as an extension of s.

ii) In the particular case that B is normal and locally Noetherian and that $\eta \in B$ is the generic point, the natural inclusion is actually a bijection,

$$\mathrm{MG}_{\mathscr{Q}|_\eta,k(\eta),l} = \mathrm{MG}_{\mathscr{Q},B,l}\ .$$

Indeed, the homomorphism $i_\#$ is then surjective, according to [SGA1, Exposé V, Proposition 8.2].

3. A criterion for RM or CM in families

Let $\underline{B}$ be a connected scheme of finite type over $\mathbb{Z}$, q an arbitrary prime power, and $\tau\colon \operatorname{Spec}\mathbb{F}_q \to \underline{B}$ an arbitrary closed point, defined over $\mathbb{F}_q$. Then, by functoriality, there is the natural homomorphism

$$\tau_\#\colon \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{F}_q, \operatorname{Spec}\overline{\mathbb{F}}_q) \to \pi_1^{\text{ét}}(\underline{B},\overline{\tau})\,,$$

so τ defines a unique element $\mathrm{F}_\tau \in \pi_1^{\text{ét}}(\underline{B},\overline{\tau})$ being the image of the canonical generator $\mathrm{Frob} \in \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. As $\underline{B}$ is connected, an étale path $\gamma \in \pi_1^{\text{ét}}(\underline{B},\overline{\tau},\overline{\eta})$ may be chosen. This yields an isomorphism

$$\pi_1^{\text{ét}}(\underline{B},\overline{\tau}) \longrightarrow \pi_1^{\text{ét}}(\underline{B},\overline{\eta}), \quad \sigma \mapsto \gamma\sigma\gamma^{-1}\,,$$

under which F_τ is sent to the *Frobenius element* $\mathrm{Frob}_\tau \in \pi_1^{\text{ét}}(\underline{B},\overline{\eta})$. The Frobenius element Frob_τ is unique only up to conjugation, as one may choose various étale paths.

Remark 3.1. In the particular case that $\underline{B} := \operatorname{Spec}\mathbb{Z}[\frac{1}{D}]$, for some integer $D \neq 0$, one has the Frobenius element $\mathrm{Frob}_p \in \pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{Z}[\frac{1}{D}],\overline{\eta})$, for any prime number $p\nmid D$. It causes an automorphism of every Galois étale covering of $\operatorname{Spec}\mathbb{Z}[\frac{1}{D}]$ and, in particular, an element in $\operatorname{Gal}(K/\mathbb{Q})$, as long as K is a number field that is normal over $\mathbb{Q}$ and ramified only at primes dividing D. This is the classical Frobenius element from Algebraic Number Theory.

Our argumentation in this section essentially relies on the Cebotarev density theorem in the extended version, due to J.-P. Serre [Serr]. This is the following result.

Proposition 3.2 (J.-P. Serre). *Let $\underline{B}$ be an irreducible scheme of finite type over $\mathbb{Z}$ and $U \subset \pi_1^{\text{ét}}(\underline{B},\overline{\eta})$ a normal subgroup of finite index.*

a) *Then the Frobenius elements* $\mathrm{Frob}_\tau \in \pi_1^{\text{ét}}(\underline{B}, \overline{\eta})$ *of the closed points* $\tau \in \underline{B}$ *take every conjugacy class of elements of* $\pi_1^{\text{ét}}(\underline{B}, .)/U$.

b) *Suppose, in addition, that* $\underline{B}$ *is flat over* $\mathbb{Z}$. *Then the Frobenius elements* Frob_τ *of the closed points* $\tau \in \underline{B}$ *defined over a prime field already take every conjugacy class of elements of* $\pi_1^{\text{ét}}(\underline{B}, .)/U$.

Proof. a) directly follows from [Serr, Theorem 7]. In fact, J.-P. Serre shows for every conjugacy class that the suitable closed points are of positive Dirichlet density.

b) Thus, to establish b), it suffices to show that the closed points defined over non-prime fields form a set of Dirichlet density zero. For this, let us write $n := \dim \underline{B}$. Then the special fibre over $\mathbb{F}_p$ is of dimension $(n-1)$. Hence, according to the Lang–Weil estimates [LW, Theorem 1], there is some constant $C \in \mathbb{R}$ such that $\#\underline{B}(\mathbb{F}_q) \leq Cq^{n-1}$, for every prime power q. Therefore,

$$\sum_{\substack{p \text{ prime} \\ k \geq 2, \tau \in \underline{B}(\mathbb{F}_{p^k})}} \frac{1}{N(\tau)^n} \leq C \sum_{\substack{p \text{ prime} \\ k \geq 2}} \frac{(p^k)^{n-1}}{(p^k)^n} = C \sum_{\substack{p \text{ prime} \\ k \geq 2}} \frac{1}{p^k} < \infty \,,$$

which implies the claim, cf. [Serr, formula (19)]. □

Theorem 3.3 (Strict inclusion for the algebraic monodromy group)**.** *Let* $D \neq 0$ *be an integer and* $\underline{q}\colon \underline{X} \to \underline{B}$ *a proper and smooth morphism of irreducible schemes of finite type over* $\mathbb{Z}[\frac{1}{lD}]$, *every fibre of which is a* $K3$ *surface. Suppose that* B *has a* $\mathbb{Q}$*-rational point.*

Let, moreover, $\mathscr{T} \subset R^2 q_* \mathbb{Q}_l(1)$ *be a twisted-constant sheaf of rank* ≥ 3 *of the kind that*

- *there is a decomposition* $R^2 q_* \mathbb{Q}_l(1) = (\mathscr{P} \otimes_\mathbb{Z} \mathbb{Q}_l) \oplus \mathscr{T}$, *for* $\mathscr{P}$ *a locally constant* $\mathbb{Z}$*-sheaf,*
- *the restriction of the cup product pairing to* $\mathscr{T}_{\overline{\eta}}$ *is non-degenerate.*

Finally, assume that there exists a number field K *of discriminant* D *that is Galois over* $\mathbb{Q}$ *and a conjugacy class* c *of elements in* $\mathrm{Gal}(K/\mathbb{Q})$ *with the property below: For every prime number* p *such that* $\mathrm{Frob}_p \in c$ *and every* $\mathbb{F}_p$*-rational point* $\tau \in \underline{B}(\mathbb{F}_p)$, *the special fibre* $\underline{X}_\tau$ *has point count*

$$\#\underline{X}_\tau(\mathbb{F}_p) \equiv 1 \pmod{p}\,. \tag{6}$$

Then the strict inclusion $\mathrm{MG}^0_{\mathscr{T},\underline{B},l} \subsetneqq \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$ *holds.*

Corollary 3.4 (Algebraic monodromy group of the generic fibre)**.** *Let* $\underline{q}\colon \underline{X} \to \underline{B}$ *and* $\mathscr{T} \subset R^2 q_* \mathbb{Q}_l(1)$ *be as in Theorem 3.3. Then*

$$\mathrm{MG}^0_{\mathscr{T}_{\overline{\eta}},k(\eta),l} \subsetneqq \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})\,.$$

Proof. This follows directly from Theorem 3.3, together with 2.4.i). □

Theorem 3.5 (Sufficient criterion for the generic fibre to have RM or CM with an unspecified endomorphism field)**.** *Let* $\underline{q}\colon \underline{X} \to \underline{B}$ *be a proper and smooth morphism* *of irreducible schemes of finite type over* $\mathbb{Z}[\frac{1}{l}]$*, every fibre of which is a* $K3$ *surface. Suppose that* B *is a normal scheme and has a* $\mathbb{Q}$*-rational point.*

Assume that there exists a number field K *that is Galois over* $\mathbb{Q}$ *and a conjugacy class* c *of elements in* $\mathrm{Gal}(K/\mathbb{Q})$ *with the property below: For every prime number* p *such that* $\mathrm{Frob}_p \in c$ *and every* $\mathbb{F}_p$*-rational point* $\tau \in \underline{B}(\mathbb{F}_p)$*, the special fibre* $\underline{X}_\tau$ *has point count*

$$\#\underline{X}_\tau(\mathbb{F}_p) \equiv 1 \pmod p\,.$$

Then the $K3$ *surface* $X_\eta(\mathbb{C}) = (X_\eta \times_{\operatorname{Spec} k(\eta)} \operatorname{Spec} \mathbb{C})(\mathbb{C})$ *has real or complex multiplication, for every embedding* $k(\eta) \hookrightarrow \mathbb{C}$*.*

Proof. Without restriction, $\underline{q}$ is a morphism of $\mathbb{Z}[\frac{1}{lD}]$-schemes, for D the discriminant of the field extension $K/\mathbb{Q}$. Indeed,

$$\underline{q} \times_{\operatorname{Spec} \mathbb{Z}[\frac{1}{l}]} \operatorname{Spec} \mathbb{Z}[\tfrac{1}{lD}] \colon \underline{X} \times_{\operatorname{Spec} \mathbb{Z}[\frac{1}{l}]} \operatorname{Spec} \mathbb{Z}[\tfrac{1}{lD}] \longrightarrow \underline{B} \times_{\operatorname{Spec} \mathbb{Z}[\frac{1}{l}]} \operatorname{Spec} \mathbb{Z}[\tfrac{1}{lD}]$$

still fulfils all the assumptions made.

Put $\mathscr{R} := R^2\underline{q}_*\mathbb{Q}_l(1)$ and $\mathscr{P}_{\overline{\eta}} := c_1(\operatorname{Pic} X_{\overline{\eta}}) \subset H^2_{\text{ét}}(X_{\overline{\eta}}, \mathbb{Q}_l(1)) = \mathscr{R}_{\overline{\eta}}$. Then $\mathscr{R}$ is a twisted-constant $\mathbb{Q}_l$-sheaf on $\underline{B}$, due to the smooth and proper base change theorems [SGA4, Exposé XVI, Corollaire 2.2]. Moreover, $\mathscr{P}_{\overline{\eta}}$ is clearly $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))$-invariant and stabilised by an open subgroup of finite index, as every invertible sheaf is defined over a finite extension of $k(\eta)$. Therefore, Lemma 3.6 applies and shows that $\mathscr{P}_{\overline{\eta}}$ extends to a locally constant $\mathbb{Z}$-sheaf $\mathscr{P}$ on $\underline{B}$.

Finally, write $\mathscr{T} := (\mathscr{P} \otimes_{\mathbb{Z}} \mathbb{Q}_l)^\perp$. If $\operatorname{rk} \mathscr{T} \geq 3$ then all assumptions of Theorem 3.3 are satisfied. Indeed, the cup product pairing on $\mathscr{P}$ is non-degenerate and this implies the same for $\mathscr{T}$. In view of formula (5), the assertion is then a direct consequence of Corollary 3.4. Otherwise, one has $\operatorname{rk} \mathscr{T} = 2$ and hence X_η is of geometric Picard rank 20. In this case, $X_\eta(\mathbb{C})$ is known to have CM [Hu, Remark 3.3.10]. □

Lemma 3.6. *Let* A *be a normal scheme that is connected and locally Noetherian and let* $\mathscr{R}$ *be a twisted-constant* $\mathbb{Q}_l$*-sheaf on* A*. Moreover, let* $S \hookrightarrow S \otimes_{\mathbb{Z}} \mathbb{Q}_l \subseteq \mathscr{R}_{\overline{\eta}}$ *be a free* $\mathbb{Z}$*-module of finite rank that is invariant under the* $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))$*-operation and stabilised by an open subgroup of finite index in* $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))$*.*

Then S *extends to the whole of* A *as a locally constant* $\mathbb{Z}$*-sheaf* $\mathscr{S}$*. Moreover, one has* $\mathscr{S} \otimes_{\mathbb{Z}} \mathbb{Q}_l \subseteq \mathscr{R}$*.*

Proof. The assumptions made on A are enough to imply that the étale fundamental group $\pi_1^{\text{ét}}(A, .)$ is a quotient of $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))$ [SGA1, Exposé V, Proposition 8.2]. Write $\pi_1^{\text{ét}}(A, .) = \mathrm{Gal}(\overline{k(\eta)}/k(\eta))/H$. The equivalence of categories between twisted-constant $\mathbb{Q}_l$-sheaves on A and $\mathbb{Q}_l$-vector spaces being continuously acted upon by $\pi_1^{\text{ét}}(A, .)$ [SGA5, Exposé VI, Lemme 1.2.4.2] therefore shows that $\mathscr{R}_{\overline{\eta}}$ is actually a $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))/H$-module. In particular, H operates trivially on S.

Thus, S is acted upon by $\mathrm{Gal}(\overline{k(\eta)}/k(\eta))/H = \pi_1^{\text{ét}}(A, .)$. The assumption implies that S is, furthermore, stabilised by an open subgroup $K \subset \pi_1^{\text{ét}}(A, .)$ of finite index. Consequently, there exists an étale covering $\widetilde{A} \to A$, which we may assume to be

Galois, on which S defines a constant $\mathbb{Z}$-sheaf $\widetilde{\mathscr{S}}$, together with an operation of the finite group $\mathrm{Gal}(\widetilde{A}/A) = \pi_1^{\text{ét}}(A,.)/K$.

Since every orbit of a finite group is finite, $\widetilde{\mathscr{S}}$ is represented [SGA4, Exposé VII, Section 2.a)] by an infinite disjoint union $\mathfrak{A}$ of trivial, finite étale coverings, i.e. such of type $\widetilde{A} \sqcup \cdots \sqcup \widetilde{A}$, each of which is acted upon by $\pi_1^{\text{ét}}(A,.)/K$. According to [SGA1, Exposé IX, Proposition 4.1], $\mathfrak{A}$ descends to an infinite disjoint union of finite étale coverings of A. This union, finally, represents a sheaf $\mathscr{S}$ of sets on A.

The sheaf $\mathscr{S}$ is locally constant, since it is trivialised by the étale covering $\widetilde{A} \to A$. As the group structure descends, too, the proof is complete. □

Proof of Theorem 3.3. *First step.* For an arbitrary $\mathbb{F}_p$-rational point $\tau \in \underline{B}(\mathbb{F}_p)$, for p of the kind that $\mathrm{Frob}_p \in c$, one has $\mathrm{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\mathrm{Frob}_\tau)) \in [-22, 22] \cap \mathbb{Z}$.
The Lefschetz trace formula [SGA5, Exposé XII, 6.3 and Exemple 7.3] yields that

$$\begin{aligned}\#\underline{X}_\tau(\mathbb{F}_p) &= p^2 + \mathrm{Tr}(\mathrm{Frob}\colon H^2_{\text{ét}}(X_{\overline{\tau}}, \mathbb{Q}_l(1)) \to H^2_{\text{ét}}(X_{\overline{\tau}}, \mathbb{Q}_l(1)))p + 1 \\ &= p^2 + \mathrm{Tr}(\mathrm{F}_\tau\colon (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}} \to (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}})p + 1\,.\end{aligned}$$

Note the factor p that is a result of the Tate twist. Consequently, Assumption (6) means nothing but

$$\mathrm{Tr}\big(\mathrm{F}_\tau\colon (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}} \to (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}}\big) \in \mathbb{Z}\,.$$

But, via any étale path $\gamma \in \pi_1^{\text{ét}}(\underline{B}, \overline{\tau}, \overline{\eta})$,

$$\begin{aligned}\mathrm{Tr}(\varrho_{\overline{\eta}}^{R^2q_*\mathbb{Q}_l(1)}(\mathrm{Frob}_\tau)) &= \mathrm{Tr}(\mathrm{Frob}_\tau\colon (R^2q_*\mathbb{Q}_l(1))_{\overline{\eta}} \to (R^2q_*\mathbb{Q}_l(1))_{\overline{\eta}}) \\ &= \mathrm{Tr}(\mathrm{F}_\tau\colon (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}} \to (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}})\,.\end{aligned}$$

On the other hand, $\mathrm{Tr}(\varrho_{\overline{\eta}}^{\mathscr{P}\otimes_{\mathbb{Z}}\mathbb{Q}_l}(\mathrm{Frob}_\tau)) = \mathrm{Tr}(\varrho_{\overline{\eta}}^{\mathscr{P}}(\mathrm{Frob}_\tau)) \in \mathbb{Z}$. Note here that Frob_τ operates already on the $\mathbb{Z}$-sheaf $\mathscr{P}$. Consequently, one has $\mathrm{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\mathrm{Frob}_\tau)) \in \mathbb{Z}$ too.

The argument above also shows that $\mathrm{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\mathrm{Frob}_\tau))$ is the same as the sum of the eigenvalues of Frob, operating on $\mathscr{T}_{\overline{\tau}} \subset (R^2q_*\mathbb{Q}_l(1))_{\overline{\tau}} = H^2_{\text{ét}}(X_{\overline{\tau}}, \mathbb{Q}_l(1))$. Since these are all of absolute value 1, according to the Weil conjectures, and the vector space to the right is of dimension 22, the claim follows.

Note that, for $K3$ surfaces, the Weil conjectures were established by I. I. Pjatetskij-Shapiro and I. R. Shafarevich [PSS, Teorema 3], as well as P. Deligne [De72], before the general case was treated [De74, Théorème 8.1].

Second step. A finite-index subgroup of $\pi_1^{\text{ét}}(\underline{B}, \overline{\eta})$.
The homomorphism $\mathrm{pr}_\#\colon \pi_1^{\text{ét}}(\underline{B}, \overline{\eta}) \to \pi_1^{\text{ét}}(\mathrm{Spec}\,\mathbb{Z}[\frac{1}{lD}], \mathrm{Spec}\,\overline{\mathbb{Q}})$, induced by the structural morphism $\mathrm{pr}\colon \underline{B} \to \mathrm{Spec}\,\mathbb{Z}[\frac{1}{lD}]$, is surjective. Indeed, for $t\colon \mathrm{Spec}\,\mathbb{Q} \to \underline{B}$ any $\mathbb{Q}$-rational point, it is sufficient to show that $\mathrm{pr}_\# \circ t_\# = (\mathrm{pr} \circ t)_\#$ is surjective. But as $\mathrm{pr} \circ t\colon \mathrm{Spec}\,\mathbb{Q} \to \mathrm{Spec}\,\mathbb{Z}[\frac{1}{lD}]$ is just the embedding of the generic point, this is true, due to [SGA1, Exposé V, Proposition 8.2].

Furthermore, there is the homomorphism

$$\chi\colon \pi_1^{\text{ét}}(\mathrm{Spec}\,\mathbb{Z}[\tfrac{1}{lD}], \mathrm{Spec}\,\overline{\mathbb{Q}}) \to \mathrm{Gal}(K/\mathbb{Q})\,,$$

induced by the operation on the $[K\!:\!\mathbb{Q}]$-fold étale covering

$$W := \operatorname{Spec} \mathscr{O}_K[\tfrac{1}{lD}] \to \operatorname{Spec} \mathbb{Z}[\tfrac{1}{lD}] .$$

The homomorphism χ is epic, too, as W is a connected scheme. Put $\chi_K := \chi \circ \mathrm{pr}_\#$,

$$U := \ker \chi_K \quad \text{and} \quad U^{(c)} := \chi_K^{-1}(c) .$$

Then $U \subset \pi_1^{\text{ét}}(\underline{B}, \overline{\eta})$ is an open subgroup of index $[K\!:\!\mathbb{Q}]$ and $U^{(c)} \subset \pi_1^{\text{ét}}(\underline{B}, \overline{\eta})$ is a non-empty union of cosets of U.

Third step. For every $\sigma \in U^{(c)}$, one has $\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\sigma)) \in [-22, 22] \cap \mathbb{Z}$.
Assume the contrary. Then $\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\sigma)) \notin \{-22, \ldots, 22\} \subset \mathbb{Q}_l$, for one particular such element σ.

In order to analyse this assumption further, let us consider a torsion-free $\mathbb{Z}_l$-sheaf $\mathscr{T}^{(\mathbb{Z}_l)}$ underlying $\mathscr{T}$. Such a sheaf must exist for very general reasons [SGA5, Exposé 6, Définition 1.4.3]. Consequently, there is a continuous representation

$$\varrho_{\overline{\eta}}^{\mathscr{T}^{(\mathbb{Z}_l)}} \colon \pi_1^{\text{ét}}(\underline{B}, \overline{\eta}) \to \mathrm{GL}(\mathscr{T}_{\overline{\eta}}^{(\mathbb{Z}_l)})$$

underlying $\varrho_{\overline{\eta}}^{\mathscr{T}}$. In particular, we have $\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}^{(\mathbb{Z}_l)}}(\sigma)) = \operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}}(\sigma))$ and may conclude $\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}^{(\mathbb{Z}_l)}}(\sigma)) \notin \{-22, \ldots, 22\} \subset \mathbb{Z}_l$. Thus, $\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}^{(\mathbb{Z}_l)}}(\sigma))$ has a positive l-adic distance from the finite set $\{-22, \ldots, 22\}$, which means that there exists some $e \in \mathbb{N}$ of the kind that

$$\operatorname{Tr}(\varrho_e(\sigma)) \notin \{\overline{-22}, \ldots, \overline{22}\} \subset \mathbb{Z}/l^e\mathbb{Z} , \tag{7}$$

for $\varrho_e \colon \pi_1^{\text{ét}}(\underline{B}, \overline{\eta}) \to \mathrm{GL}(\mathscr{T}_{\overline{\eta}}^{(\mathbb{Z}_l)}/l^e \mathscr{T}_{\overline{\eta}}^{(\mathbb{Z}_l)})$ the quotient representation.

We now apply Proposition 3.2.b) to the product representation

$$\varrho_e \times \chi_K \colon \pi_1^{\text{ét}}(\underline{B}, .) \to \mathrm{GL}(\mathscr{T}_{\overline{\eta}}^{(\mathbb{Z}_l)}/l^e \mathscr{T}_{\overline{\eta}}^{(\mathbb{Z}_l)}) \times \mathrm{Gal}(K/\mathbb{Q}) .$$

Note that $\underline{B}$ is certainly flat over $\mathbb{Z}$, since it is irreducible and has a $\mathbb{Q}$-rational point. Proposition 3.2.b) yields a prime number p and a closed point $\tau \colon \operatorname{Spec} \mathbb{F}_p \to \underline{B}$ having the property that

$$\mathrm{Frob}_\tau \equiv \sigma \pmod{\ker(\varrho_e \!\times\! \chi_K)} . \tag{8}$$

Here, Frob_τ is to be understood as a suitable representative up to conjugation.

Formula (8) shows, in particular, $\mathrm{Frob}_\tau \equiv \sigma \pmod{\ker \chi_K}$, which implies that $\mathrm{Frob}_p \in c$. Moreover, the congruence modulo $\ker \varrho_e$ yields

$$\operatorname{Tr}(\varrho_e(\sigma)) = \operatorname{Tr}(\varrho_e(\mathrm{Frob}_\tau)) .$$

However, $\operatorname{Tr}(\varrho_e(\mathrm{Frob}_\tau)) = \big(\operatorname{Tr}(\varrho_{\overline{\eta}}^{\mathscr{T}^{(\mathbb{Z}_l)}}(\mathrm{Frob}_\tau)) \bmod l^e\big) \in \{-\overline{22}, \ldots, \overline{22}\} \subset \mathbb{Z}/l^e\mathbb{Z}$, according to the first step. This is in contradiction with (7), and the claim is therefore established.

Fourth step. Conclusion.
To complete the argument, we first observe that the set $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \cong \mathrm{GO}^0_{\operatorname{rk} \mathscr{T}}(\mathbb{Q}_l)$, equipped with the Zariski topology, is irreducible as a topological space. Indeed, $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$ is Zariski dense in $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l)$, due to [Ro, Corollary in Section 3] or

[Che, Corollary 2 of Theorem 1], and $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l) \cong \mathrm{GO}^0_{\mathrm{rk}\,\mathscr{T}}(\overline{\mathbb{Q}}_l)$ is known to be irreducible.

Consequently, $\mathrm{GO}(\mathscr{T}_{\overline{\eta}})$ has at most two components. I.e.,

$$\mathrm{GO}(\mathscr{T}_{\overline{\eta}}) = \dot{\bigcup_{i=1}^{N}} x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})\,,$$

for $N = 1$ or 2. To be more precise, one has $N = 1$ when $\mathrm{rk}\,\mathscr{T}$ is odd and $N = 2$ for $\mathrm{rk}\,\mathscr{T}$ even.

Next, let us note that the trace morphism

$$\mathrm{Tr}\colon x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \longrightarrow \mathbf{A}^1_{\mathbb{Q}_l}$$

is dominant. Indeed, $\mathrm{diag}(\frac{\lambda}{\mathrm{rk}\,\mathscr{T}}, \ldots, \frac{\lambda}{\mathrm{rk}\,\mathscr{T}}) \in \mathrm{GO}^0_{\mathrm{rk}\,\mathscr{T}}(\mathbb{Q}_l)$ has trace λ, for an arbitrary $\lambda \in \mathbb{Q}_l$. Similarly, when $\mathrm{rk}\,\mathscr{T} \geq 3$ is even,

$$\mathrm{diag}(-\tfrac{\lambda}{\mathrm{rk}\,\mathscr{T}-2}, +\tfrac{\lambda}{\mathrm{rk}\,\mathscr{T}-2}, \ldots, +\tfrac{\lambda}{\mathrm{rk}\,\mathscr{T}-2}) \in \mathrm{GO}_{\mathrm{rk}\,\mathscr{T}}(\mathbb{Q}_l) \backslash \mathrm{GO}^0_{\mathrm{rk}\,\mathscr{T}}(\mathbb{Q}_l)$$

has trace λ.

As $[-22, 22] \cap \mathbb{Z} \subsetneqq \mathbf{A}^1_{\mathbb{Q}_l}$ is Zariski closed, the result of the previous step implies that $\varrho^{\mathscr{T}}_{\overline{\eta}}(U^{(c)}) \subset \mathrm{GO}(\mathscr{T}_{\overline{\eta}})$ cannot be Zariski dense in any of the components. I.e.,

$$\overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(U^{(c)})} \cap x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \subsetneqq x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})\,,$$

for $i = 1, \ldots, N$. Consequently, $\overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(U)} \cap x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \subsetneqq x_i \cdot \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$ too, since $\varrho^{\mathscr{T}}_{\overline{\eta}}(U^{(c)})$ is a nonempty union of cosets of $\varrho^{\mathscr{T}}_{\overline{\eta}}(U)$. Another application of the same argument shows that

$$x \cdot \overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(U)} \cap \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \subsetneqq \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})\,,$$

for every $x \in \mathrm{GO}(\mathscr{T}_{\overline{\eta}})$.

Thus, writing $\pi_1^{\text{ét}}(\underline{B}, \overline{\eta}) = \dot{\bigcup}_{i=1}^{\#\,\mathrm{Gal}(K/\mathbb{Q})} \sigma_i U$ as a union of cosets, one finds that

$$\mathrm{MG}_{\mathscr{T},\underline{B},l} = \bigcup_{i=1}^{\#\,\mathrm{Gal}(K/\mathbb{Q})} \overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(\sigma_i U)} = \bigcup_{i=1}^{\#\,\mathrm{Gal}(K/\mathbb{Q})} \varrho^{\mathscr{T}}_{\overline{\eta}}(\sigma_i) \cdot \overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(U)}\,.$$

Therefore,

$$\mathrm{MG}_{\mathscr{T},\underline{B},l} \cap \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) = \bigcup_{i=1}^{\#\,\mathrm{Gal}(K/\mathbb{Q})} \big(\varrho^{\mathscr{T}}_{\overline{\eta}}(\sigma_i) \cdot \overline{\varrho^{\mathscr{T}}_{\overline{\eta}}(U)} \cap \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})\big)$$

is the union of finitely many sets, each of which is Zariski closed and properly contained in $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$. Since $\mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$ is an irreducible topological space, this implies $\mathrm{MG}_{\mathscr{T},\underline{B},l} \cap \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}}) \subsetneqq \mathrm{GO}^0(\mathscr{T}_{\overline{\eta}})$, which completes the proof. □

4. The endomorphism field under specialisation

It turns out that formula (5) from Example 2.3.v) may be reversed.

Theorem 4.1 (Étale cohomological description of the endomorphism field)**.** *Let k be a field that is finitely generated over $\mathbb{Q}$, X a $K3$ surface defined over k, and $\mathscr{T} \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$ the transcendental part. Then*

$$C_{\text{End}(\mathscr{T})}(\text{MG}^0_{\mathscr{T},k,l}) = E \otimes_{\mathbb{Q}} \mathbb{Q}_l\,,$$

for E the endomorphism field of $X(\mathbb{C}) = (X \times_{\text{Spec}\,k} \text{Spec}\,\mathbb{C})(\mathbb{C})$. Here, k is arbitrarily embedded into $\mathbb{C}$.

Corollary 4.2 (Independence of E of the embedding into $\mathbb{C}$–elementary case)**.** *In the situation of Theorem 4.1, let $i_1, i_2 \colon k \hookrightarrow \mathbb{C}$ be two embeddings and denote by E_1, E_2 the corresponding endomorphism fields.*

a) *Then E_1 and E_2 are arithmetically equivalent.*

b) *In particular, $[E_1 : \mathbb{Q}] = [E_2 : \mathbb{Q}]$. Furthermore, E_1 and E_2 have the same normal closure. If $[E_1 : \mathbb{Q}] < 7$ then $E_1 \cong E_2$.*

Proof. a) The isomorphy $E_1 \otimes_{\mathbb{Q}} \mathbb{Q}_l \cong E_2 \otimes_{\mathbb{Q}} \mathbb{Q}_l$, for every prime number l, implies that E_1 and E_2 have the same Dedekind zeta function. This is what is called arithmetic equivalence [Pe].

b) The two consequences of arithmetic equivalence are shown in [Pe, Theorem 1] and the final statement is [BdS, Theorem 1]. □

Corollary 4.3. *In the situation of Theorem 4.1, choose, in addition, an embedding $k \hookrightarrow \mathbb{C}$. Then*

$$C_{\text{End}(\mathscr{T})}(\text{MG}^0_{\mathscr{T},k,l}) \cap \text{End}_{\mathbb{Q}}(T) = E\,.$$

Proof. "$\supseteq$": Clearly, on one hand, one has $E = \text{End}_{\text{Hodge}}(T) \subseteq \text{End}_{\mathbb{Q}}(T)$ and, on the other, $E \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_l = C_{\text{End}(\mathscr{T})}(\text{MG}^0_{\mathscr{T},k,l})$.

"$\subseteq$": Let us put $E' := C_{\text{End}(\mathscr{T})}(\text{MG}^0_{\mathscr{T},k,l}) \cap \text{End}_{\mathbb{Q}}(T)$. Then $E' \otimes_{\mathbb{Q}} \mathbb{Q}_l$ is contained in $\text{End}_{\mathbb{Q}}(T) \otimes_{\mathbb{Q}} \mathbb{Q}_l = \text{End}(\mathscr{T})$. Note here that $\mathbb{Q}_l(1)$ is free of rank 1 over $\mathbb{Q}_l$, and that we use the identification $\mathscr{T} \cong T \otimes_{\mathbb{Q}} \mathbb{Q}_l(1)$. Moreover, $E' \otimes_{\mathbb{Q}} \mathbb{Q}_l$ commutes with $\text{MG}^0_{\mathscr{T},k,l}$, simply because E' does so. Therefore,

$$E' \otimes_{\mathbb{Q}} \mathbb{Q}_l \subseteq C_{\text{End}(\mathscr{T})}(\text{MG}^0_{\mathscr{T},k,l}) = E \otimes_{\mathbb{Q}} \mathbb{Q}_l\,,$$

in view of the Theorem. As $E, E' \subseteq \text{End}_{\mathbb{Q}}(T)$ and $\mathbb{Q}_l$ is faithfully flat over $\mathbb{Q}$, this yields that $E' \subseteq E$. □

Recall that an extension field k of $\mathbb{Q}$ is called *primary,* if it does not contain any proper algebraic extension of $\mathbb{Q}$ [EGA IV, §4.3].

Corollary 4.4 (Independence of E of the embedding into $\mathbb{C}$–primary case)**.** *Let k be a field that is finitely generated and primary over $\mathbb{Q}$ and X a $K3$ surface over k. Then the endomorphism field of $X(\mathbb{C}) = (X \times_{\text{Spec}\,k} \text{Spec}\,\mathbb{C})(\mathbb{C})$ is independent of the embedding $k \hookrightarrow \mathbb{C}$ chosen.*

Proof. Take an integral scheme B of finite type over $\mathbb{Q}$ with function field k. Then, as k is primary, [EGA IV, Proposition 4.5.9] shows that B is geometrically irreducible. Moreover, according to H. Hironaka [Hi], one may assume that B is non-singular.

The usual spreading out argument provides a morphism $q\colon \mathscr{X} \to B$ of $\mathbb{Q}$-schemes of finite type with generic fibre X. Restricting B to an open subscheme, if necessary, one may assume that q is proper and smooth and that every fibre is a $K3$ surface.

Next, consider two embeddings $i_1, i_2\colon k = k(\eta) \hookrightarrow \mathbb{C}$. These yield two complex points $\eta_1^c, \eta_2^c\colon \operatorname{Spec}\mathbb{C} \to B$ on B, and hence on $B_\mathbb{C} := B \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{C}$, as well as on the complex manifold $B(\mathbb{C}) = B_\mathbb{C}(\mathbb{C})$. As $B(\mathbb{C})$ is connected, we may choose a path $w \in \pi_1(B(\mathbb{C}), \eta_1^c, \eta_2^c)$.

The higher direct image sheaf $R^2q(\mathbb{C})_*\mathbb{Q}$ is locally free on $B(\mathbb{C})$ of rank 22. Thus, the path w induces an isomorphism i_w between the stalks $(R^2q(\mathbb{C})_*\mathbb{Q})_{\eta_1^c}$ and $(R^2q(\mathbb{C})_*\mathbb{Q})_{\eta_2^c}$, which are, according to Grauert's Theorem [Gr, Satz 5], canonically isomorphic to $H^2(\mathscr{X}_{\eta_1^c}(\mathbb{C}), \mathbb{Q})$ and $H^2(\mathscr{X}_{\eta_2^c}(\mathbb{C}), \mathbb{Q})$, respectively.

On the other hand, as usual, w induces an étale path on $B_\mathbb{C}$, and, via the natural projection, an element $\widetilde{w} \in \pi_1^{\text{ét}}(B, \overline{\eta})$. By [SGA1, Exposé V, Proposition 8.2], this fundamental group is a quotient of $\operatorname{Gal}(\overline{k}/k)$. Thus, $\widetilde{w}$ operates as an automorphism of $\overline{k}$ and hence preserves the algebraic classes in $H^2_{\text{ét}}(\mathscr{X}_{\overline{\eta}}, \mathbb{Q}_l(1)) = H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$.

Consequently, one also has that $i_{\widetilde{w}}(\mathscr{T}) = \mathscr{T}$. I.e., the isomorphism

$$i_w\colon H^2(X_{\eta_1^c}(\mathbb{C}), \mathbb{Q}) \to H^2(X_{\eta_2^c}(\mathbb{C}), \mathbb{Q})$$

maps $T_{\eta_1^c} \otimes_\mathbb{Q} \mathbb{Q}_l(1)$ onto $T_{\eta_2^c} \otimes_\mathbb{Q} \mathbb{Q}_l(1)$. As $\mathbb{Q}_l(1)$ is faithfully flat over $\mathbb{Q}$, this implies $i_w(T_{\eta_1^c}) = T_{\eta_2^c}$.

Conjugation by i_w hence provides an isomorphism

$$c_w\colon \operatorname{End}_\mathbb{Q}(T_{\eta_1^c}) \to \operatorname{End}_\mathbb{Q}(T_{\eta_2^c}), \quad M \mapsto i_w \circ M \circ i_w^{-1},$$

which clearly induces the isomorphism $c_{\widetilde{w}}\colon \operatorname{End}(\mathscr{T}) \to \operatorname{End}(\mathscr{T})$, $M \mapsto i_{\widetilde{w}} \circ M \circ i_{\widetilde{w}}^{-1}$. Moreover, as noticed in Remark 2.2, $c_{\widetilde{w}}$ maps the algebraic monodromy group $\mathrm{MG}_{\mathscr{T},k,l}$, and therefore also the identity component $\mathrm{MG}^0_{\mathscr{T},k,l}$, onto itself. Consequently,

$$c_w\big(C_{\operatorname{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) \cap \operatorname{End}_\mathbb{Q}(T_{\eta_1^c})\big) \subseteq C_{\operatorname{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) \cap \operatorname{End}_\mathbb{Q}(T_{\eta_2^c}).$$

Corollary 4.3 shows that this means nothing but $c_w(E_1) \subseteq E_2$. As c_w is injective and one has $[E_1 : \mathbb{Q}] = [E_2 : \mathbb{Q}]$, due to Corollary 4.2.b), the assertion follows. □

In order to draw more conclusions from Theorem 4.1, we need a lemma.

Lemma 4.5. *Let k be a field that is finitely generated over $\mathbb{Q}$, X a $K3$ surface over k, and $\mathscr{T}' \subseteq H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$ a subvector space on which the cup product pairing is non-degenerate and which contains the transcendental part $\mathscr{T}$. Let $\mathscr{R} \subset \mathscr{T}'$ be the orthogonal complement of $\mathscr{T}$ in $\mathscr{T}'$.*

a) *Then $\mathrm{MG}^0_{\mathscr{T}',k,l} = \mathrm{MG}^0_{\mathscr{T},k,l}$, the operation of $\mathrm{MG}^0_{\mathscr{T}',k,l}$ on $\mathscr{R}$ being trivial.*

b) *The centraliser $C_{\operatorname{End}(\mathscr{T}')}(\mathrm{MG}^0_{\mathscr{T}',k,l})$ maps $\mathscr{R}$ to itself.*

Proof. a) Being perpendicular to $\mathscr{T}$, the direct summand $\mathscr{R}$ consists of algebraic classes. These are defined over a finite extension field of k, and therefore pointwise fixed under an open subgroup of finite index in $\mathrm{MG}_{\mathscr{T}',k,l}$. In other words, $\mathrm{MG}^0_{\mathscr{T}',k,l}$ operates as the identity map on $\mathscr{R}$. This yields $\mathrm{MG}^0_{\mathscr{T}',k,l} = \mathrm{MG}^0_{\mathscr{T},k,l}$, since the operation of Galois preserves orthogonality.

b) On the other hand, no non-zero element of $\mathscr{T}$ is fixed under $\mathrm{MG}^0_{\mathscr{T}',k,l}$. Indeed, such an element $x \in \mathscr{T}$ would be fixed under $\mathrm{Gal}(\overline{k}/k')$, for k' a certain finite extension field of k, and hence algebraic, according to the Tate conjecture (cf. Fact 1.6.a)), a contradiction. As elements commuting with $\mathrm{MG}^0_{\mathscr{T}',k,l}$ cannot interchange fixed points with non-fixed points, we see that $C_{\mathrm{End}(\mathscr{T}')}(\mathrm{MG}^0_{\mathscr{T}',k,l})$ maps $\mathscr{R}$ to itself. □

Corollary 4.6 (The endomorphism field under specialisation)**.** *Let $q\colon X \to B$ be a proper and smooth morphism of geometrically connected schemes of finite type over $\mathbb{Q}$, every fibre of which is a $K3$ surface.*

a) *Then the endomorphism field E of the generic fibre X_η is independent of the embedding $k(\eta) \hookrightarrow \mathbb{C}$.*

b) *Let $s \in B$ be a point. Choose arbitrary embeddings $k(\eta) \hookrightarrow \mathbb{C}$ and $k(s) \hookrightarrow \mathbb{C}$ and denote by $\eta^c, s^c \in B(\mathbb{C})$ the complex points corresponding to η and s, respectively. Let, moreover $w \in \pi_1(B(\mathbb{C}), \eta^c, s^c)$ be a path.*

i) *Then w induces an isomorphism $i_w\colon H^2(X_{\eta^c}(\mathbb{C}), \mathbb{Q}) \to H^2(X_{s^c}(\mathbb{C}), \mathbb{Q})$, which maps the transcendental part $T^{(X_{\eta^c})} \subset H^2(X_{\eta^c}(\mathbb{C}), \mathbb{Q})$ to some $T_{s^c} \supseteq T^{(X_{s^c})}$.*

ii) *Thus, by transport of structure, E operates on T_{s^c}, too. Under this operation, $T^{(X_{s^c})}$ is mapped to itself.*

iii) *For the endomorphism field $E^{(X_{s^c})}$ of $X_s(\mathbb{C})$, one has $E^{(X_{s^c})} \supseteq E$. Thereby, the operation of $E \subseteq E^{(X_{s^c})}$ coincides with that obtained by transport of structure.*

Proof. a) As B is geometrically connected, $k(\eta)$ is clearly primary over $\mathbb{Q}$. Thus, Corollary 4.4 implies the assertion.

b.i) The higher direct image sheaf $R^2q(\mathbb{C})_*\mathbb{Q}$ is locally free on $B(\mathbb{C})$ of rank 22. Thus, w induces an isomorphism $i_w\colon (R^2q(\mathbb{C})_*\mathbb{Q})_{\eta^c} \to (R^2q(\mathbb{C})_*\mathbb{Q})_{s^c}$. Note that these stalks are canonically isomorphic to $H^2(X_{\eta^c}(\mathbb{C}), \mathbb{Q})$ and $H^2(X_{s^c}(\mathbb{C}), \mathbb{Q})$, respectively, due to [Gr, Satz 5].

Moreover, algebraic classes remain algebraic under specialisation, i.e.

$$i_w(P^{(X_{\eta^c})}) \subseteq P^{(X_{s^c})}, \tag{9}$$

in the situation of a smooth family. Indeed, they are representable by Weil divisors and one may just take the Zariski closure of a representing Weil divisor. The claim follows immediately from (9) by taking orthogonal complements on both sides.

ii) The assertion descends under base change by a finite morphism $p\colon B' \to B$. Thus, we may assume without restriction that B is a normal scheme [Bo, Chapitre V, §1, Corollaire 1 du Proposition 18].

Let us switch to étale cohomology. The algebraic part $\mathscr{P}_{\overline{\eta}} \subset H^2_{\text{ét}}(X_{\overline{\eta}}, \mathbb{Q}_l(1))$ extends to a locally constant sheaf $\mathscr{P}$ on the whole of B, by virtue of of Lemma 3.6.

Consequently, the transcendental part $\mathscr{T}_{\overline{\eta}} \subset H^2_{\text{ét}}(X_{\overline{\eta}}, \mathbb{Q}_l(1))$ extends to a twisted-constant sheaf $\mathscr{T}$. Moreover, the comparison theorem between étale and complex cohomology [SGA4, Exposé 11, Théorème 4.4.iii)] shows that the commutative diagram of the given data

$$\begin{array}{ccc}
H^2(X_{\eta^c}(\mathbb{C}), \mathbb{Q}) & \xrightarrow{i_w} & H^2(X_{s^c}(\mathbb{C}), \mathbb{Q}) \\
\uparrow & & \uparrow \\
T^{(X_{\eta^c})} & \xrightarrow{i_w} & T_{s^c} \\
& & \uparrow \\
& & T^{(X_{s^c})}
\end{array}$$

goes over under tensoring with $\mathbb{Q}_l(1)$ into

$$\begin{array}{ccc}
H^2_{\text{ét}}(X_{\overline{\eta}}, \mathbb{Q}_l(1)) & \longrightarrow & H^2_{\text{ét}}(X_{\overline{s}}, \mathbb{Q}_l(1)) \\
\uparrow & & \uparrow \\
\mathscr{T}_{\overline{\eta}} & \longrightarrow & \mathscr{T}_{\overline{s}} \\
& & \uparrow \\
& & \mathscr{T}^{(X_{\overline{s}})} .
\end{array}$$

On the other hand, we have $\mathrm{MG}^0_{\mathscr{T}_{\overline{s}},k(s),l} \subseteq \mathrm{MG}^0_{\mathscr{T},B,l} = \mathrm{MG}^0_{\mathscr{T}_{\overline{\eta}},k(\eta),l}$, due to 2.4.i) and ii). Here, in view of Remark 2.2, the underlying identification may be supposed to be induced by w. The inclusion yields

$$C_{\mathrm{End}(\mathscr{T}_{\overline{s}})}(\mathrm{MG}^0_{\mathscr{T}_{\overline{s}},k(s),l}) \supseteq C_{\mathrm{End}(\mathscr{T}_{\overline{\eta}})}(\mathrm{MG}^0_{\mathscr{T}_{\overline{\eta}},k(\eta),l}) = E \otimes_{\mathbb{Q}} \mathbb{Q}_l \, . \qquad (10)$$

Now write $\mathscr{T}_{\overline{s}} = \mathscr{T}^{(X_{\overline{s}})} \oplus \mathscr{R}$, with a direct summand $\mathscr{R}$ that is perpendicular to $\mathscr{T}^{(X_{\overline{s}})}$. Then, according to Lemma 4.5, $C_{\mathrm{End}(\mathscr{T}_{\overline{s}})}(\mathrm{MG}^0_{\mathscr{T}_{\overline{s}},k(s),l})$ maps $\mathscr{R}$ to itself. Since $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ acts via self-adjoint endomorphisms [Za, Theorem 1.5.1], this shows that $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ maps $\mathscr{T}^{(X_{\overline{s}})}$ to itself, either.

Translating this back to complex cohomology, one finds that $E \subseteq \mathrm{End}(T_{s^c})$ has the property that $E \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_l \subseteq \mathrm{End}(T_{s^c} \otimes_{\mathbb{Q}} \mathbb{Q}_l(1))$ maps $T^{(X_{s^c})} \otimes_{\mathbb{Q}} \mathbb{Q}_l(1)$ into itself. As $\mathbb{Q}_l(1)$ is faithfully flat over $\mathbb{Q}$, this is enough to enforce the claim.

iii) By (10), the operation of $E \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ on $\mathscr{T}_{\overline{s}}$ commutes with $\mathrm{MG}^0_{\mathscr{T}_{\overline{s}},k(s),l}$. Moreover, according to Lemma 4.5.a), $\mathrm{MG}^0_{\mathscr{T}_{\overline{s}},k(s),l}$ maps $\mathscr{T}^{(X_{\overline{s}})} \subseteq \mathscr{T}_{\overline{s}}$ to itself, while $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ does the same, as shown in b). Restricting the endomorphisms to $\mathscr{T}^{(X_{\overline{s}})}$, we find that $E \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_l \subseteq \mathrm{End}(\mathscr{T}^{(X_{\overline{s}})})$ commutes with $\mathrm{MG}^0_{\mathscr{T}^{(X_{\overline{s}})},k(s),l}$. In other words,

$$E \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_l \subseteq C_{\mathrm{End}(\mathscr{T}^{(X_{\overline{s}})})}\big(\mathrm{MG}^0_{\mathscr{T}^{(X_{\overline{s}})},k(s),l}\big) \, .$$

Since, according to b), E maps $T^{(X_{s^c})}$ to itself, this yields

$$E \subseteq C_{\mathrm{End}(\mathscr{T}^{(X_{\overline{s}})})}\big(\mathrm{MG}^0_{\mathscr{T}^{(X_{\overline{s}})},k(s),l}\big) \cap \mathrm{End}_{\mathbb{Q}}(T^{(X_{s^c})}) = E^{(X_{s^c})} \, ,$$

as claimed. □

Corollary 4.7 (Complex fibres)**.** *Let $q\colon X \to B$ be a proper and smooth morphism of geometrically connected schemes of finite type over $\mathbb{Q}$, every fibre of which is a $K3$ surface. Suppose that the generic fibre X_η has real or complex multiplication by* *an endomorphism field* $E \supsetneqq \mathbb{Q}$*. Then, for every complex point* $\theta \in B(\mathbb{C})$*, the fibre* $X_\theta(\mathbb{C})$ *is acted upon by* E*.*

Proof. We suppose that $\dim B \geq 1$, as otherwise there is nothing to prove. Take an open neighbourhood $U \ni \theta$ that is connected and simply connected. Then $R^2(q|_{q^{-1}(U)})_*\mathbb{Q} = (\mathbb{Q}^{22})_U$ is a constant sheaf.

Moreover, the subset $U^{\rm alg} := B(\overline{\mathbb{Q}}) \cap U$ of algebraic points is dense in U with respect to the complex topology. $U^{\rm alg}$ is the same as the set of points of type s^c, for $s \in B$ a closed point. For each $z \in U^{\rm alg}$, the fibre $X_z(\mathbb{C})$ is acted upon by E, as shown in Corollary 4.6.

In order to make this more precise, let us take an embedding $k(\eta) \hookrightarrow \mathbb{C}$ and denote by $\eta^c \in B(\mathbb{C})$ the corresponding complex point. In addition, we choose one particular point $z_0 \in U^{\rm alg}$ and a path $w \in \pi_1(B(\mathbb{C}), \eta^c, z_0)$. For every other point $z \in U^{\rm alg}$, we choose a path $w_z \in \pi_1(U, z_0, z)$. Let us denote the element of $\pi_1(B(\mathbb{C}), z_0, z)$, induced by w_z, again by w_z. Then Corollary 4.6 applies to $w_z \circ w \in \pi_1(B(\mathbb{C}), \eta^c, z)$.

It shows that the fibre $X_z(\mathbb{C})$ is acted upon by E in the following manner. One has $i_{w_z \circ w}(T^{(X_{\eta^c})}) \supseteq T^{(X_z)}$ and the operation of E on $i_{w_z \circ w}(T^{(X_{\eta^c})})$, induced by that on $T^{(X_{\eta^c})}$, defines the action on $T^{(X_z)}$. Thus, the actions of E on all $i_{w_z \circ w}(T^{(X_{\eta^c})})$, for $z \in U^{\rm alg}$, are compatible among each other, via transport of structure under w_z. But the latter is the obvious one on the constant sheaf $R^2(q|_{q^{-1}(U)})_*\mathbb{Q}$.

The operation of E splits $i_w(T^{(X_{\eta^c})}) \otimes_\mathbb{Q} \mathbb{C}$ into $r = [E:\mathbb{Q}]$ eigenspaces $V_1, \ldots, V_r$. The same decomposition applies to every $z \in U^{\rm alg}$,

$$i_{w \circ w_z}(T^{(X_{\eta^c})}) \otimes_\mathbb{Q} \mathbb{C} = \bigoplus_{i=1}^r ((V_i)_U)_z \,.$$

As $E = \mathrm{End}_{\rm Hodge}(T^{(X_z)})$, this means that $H^{2,0}(X_z(\mathbb{C}), \mathbb{C}) \subseteq ((V_i)_U)_z$, for a certain i. In other words, the one-dimensional vector space

$$H^{2,0}(X_z(\mathbb{C}), \mathbb{C}) \in \mathbf{P}(H^2(X_z(\mathbb{C}), \mathbb{C})) \cong \mathbf{P}(H^2(X_{z_0}(\mathbb{C}), \mathbb{C}))\,,$$

represents a point lying on the union of the r projective subspaces $\mathbf{P}(V_1), \ldots, \mathbf{P}(V_r)$.

On the other hand, the mapping $\Pi\colon U \to \mathbf{P}(H^2(X_{z_0}(\mathbb{C}), \mathbb{C})), z \mapsto H^{2,0}(X_z(\mathbb{C}), \mathbb{C})$, is holomorphic [BHPV, Theorem IV.4.2]. Our argument will only need continuity. Indeed, we have $\Pi(U^{\rm alg}) \subseteq \bigcup_{i=1}^r \mathbf{P}(V_i)$. As the right hand side is a closed subset and Π is continuous, this implies that $\Pi(U) \subseteq \bigcup_{i=1}^r \mathbf{P}(V_i)$. But this means that $X_z(\mathbb{C})$ is acted upon by E, for any $z \in U$, and in particular for $z = \theta$. $\square$

In order to prove Theorem 4.1, we need a few auxiliary results.

Sublemma 4.8. *One has* $\mathrm{span}_{\overline{\mathbb{Q}}_l} \mathrm{SO}_n(\overline{\mathbb{Q}}_l) = \mathrm{M}_{n \times n}(\overline{\mathbb{Q}}_l)$*, for every natural number* $n \neq 2$*.*

Proof. Put $S := \mathrm{span}_{\overline{\mathbb{Q}}_l} \mathrm{SO}_n(\overline{\mathbb{Q}}_l)$. Then clearly $S \subseteq \mathrm{M}_{n \times n}(\overline{\mathbb{Q}}_l)$. Moreover, S is not just a $\overline{\mathbb{Q}}_l$-vector space, but a representation of $\mathrm{SO}_n(\overline{\mathbb{Q}}_l) \times \mathrm{SO}_n(\overline{\mathbb{Q}}_l)$, via

$$(\mathrm{SO}_n(\overline{\mathbb{Q}}_l) \times \mathrm{SO}_n(\overline{\mathbb{Q}}_l)) \times S \longrightarrow S\,, \quad ((M_1, M_2), s) \mapsto M_1 s M_2^{-1}\,.$$

Thus it suffices to show that $\mathrm{M}_{n\times n}(\overline{\mathbb{Q}}_l)$ is irreducible as an $\mathrm{SO}_n(\overline{\mathbb{Q}}_l)\times\mathrm{SO}_n(\overline{\mathbb{Q}}_l)$-representation. But $\mathrm{M}_{n\times n}(\overline{\mathbb{Q}}_l) \cong \overline{\mathbb{Q}}_l^n \otimes (\overline{\mathbb{Q}}_l^n)^*$ and $\overline{\mathbb{Q}}_l^n$ is irreducible as a $\mathrm{SO}_n(\overline{\mathbb{Q}}_l)$-module, due to [BtD, Chapter VI, (5.4.v)], for $n \geq 3$, and trivially, for $n = 1$. □

Lemma 4.9. *Let $\mathscr{T}$ be a finite-dimensional $\mathbb{Q}_l$-vector space equipped with a non-degenerate symmetric form that is acted upon by a totally real or CM field E via self-adjoint linear maps. In the case that E is totally real, suppose that $\mathscr{T}$ is free as an $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module of rank $\neq 2$. Then*

$$\mathrm{span}_{\overline{\mathbb{Q}}_l}(C_{\mathrm{O}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0 = C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\,.$$

.

Proof. *First case:* E is totally real.
Then $\mathscr{T} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$ is split under the operation of E into $r = [E : \mathbb{Q}]$ simultaneous eigenspaces $V_1, \ldots, V_r \subset \mathscr{T} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$, which are mutually perpendicular, due to the self-adjointness assumption. Hence,

$$C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E) = \{f\colon \mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l \to \mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l \mid f\ \overline{\mathbb{Q}}_l\text{-linear}, f(V_i) \subseteq V_i \text{ for } i = 1, \ldots, r\}$$

and $(C_{\mathrm{O}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0$ is given analogously, with the additional assumption that all restrictions $f|_{V_i}\colon V_i \to V_i$ be orthogonal maps of determinant 1. Since $\dim V_i = \mathrm{rk}_{E\otimes_{\mathbb{Q}}\overline{\mathbb{Q}}_l}(\mathscr{T} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l) = \mathrm{rk}_{E\otimes_{\mathbb{Q}}\mathbb{Q}_l} \mathscr{T} \neq 2$, Sublemma 4.8 implies the claim.

Second case: E is a CM field.
Here, $\mathscr{T} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$ is split under the operation of E into $2s = [E : \mathbb{Q}]$ simultaneous eigenspaces $V_1, \overline{V}_1, \ldots, V_s, \overline{V}_s \subset \mathscr{T} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l$. These are isotropic and mutually perpendicular, with the only exceptions that $V_i \not\perp \overline{V}_i$, for $i = 1, \ldots, s$. Indeed, if some primitive element $e \in E$ acts with eigenvalues λ_i and λ_j on V_i and V_j, respectively, then one finds

$$\lambda_i \langle v_i, v_j\rangle = \langle ev_i, v_j\rangle = \langle v_i, ev_j\rangle = \overline{\lambda}_j \langle v_i, v_j\rangle\,,$$

which yields $\langle v_i, v_j\rangle = 0$, as soon as $\lambda_i \neq \overline{\lambda}_j$.

Hence,

$$\begin{aligned}(C_{\mathrm{O}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0 &\\ = \{f\colon \mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l \to \mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l \mid{}& f\ \overline{\mathbb{Q}}_l\text{-linear}, f(V_i) \subseteq V_i, f(\overline{V}_i) \subseteq \overline{V}_i \\ &\text{and } f|_{V_i\oplus\overline{V}_i} \in \mathrm{SO}(V_i \oplus \overline{V}_i) \text{ for } i = 1, \ldots, r\}\end{aligned}$$

and $C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)$ is given in the same way, dropping the second condition.

But all matrices of type $\left(\begin{smallmatrix} A & 0 \\ 0 & (A^t)^{-1}\end{smallmatrix}\right)$, for $A \in \mathrm{GL}_{\dim V_i}(\overline{\mathbb{Q}}_l)$, represent orthogonal maps of determinant 1, as a direct calculation shows. The assertion immediately follows from this. □

Corollary 4.10. *In the situation of Lemma 4.9, one has*

$$\mathrm{span}_{\overline{\mathbb{Q}}_l}(C_{\mathrm{GO}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0 = C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\,. \qquad \square$$

Proposition 4.11. *Let $\mathscr{T}$ be a finite-dimensional $\mathbb{Q}_l$-vector space equipped with a non-degenerate symmetric form that is acted upon by a totally real or CM field E via self-adjoint linear maps. In the case that E is totally real, suppose that $\mathscr{T}$ is free as an $E\otimes_{\mathbb{Q}}\mathbb{Q}_l$-module of rank $\neq 2$. Then*

$$\operatorname{span}_{\mathbb{Q}_l}(C_{\mathrm{GO}(\mathscr{T})}(E))^0 = C_{\mathrm{End}(\mathscr{T})}(E)\,.$$

Proof. The inclusion "$\subseteq$" is obvious. In order to prove "$\supseteq$", assume the contrary. Then

$$(C_{\mathrm{GO}(\mathscr{T})}(E))^0 \subseteq \operatorname{span}_{\mathbb{Q}_l}(C_{\mathrm{GO}(\mathscr{T})}(E))^0 \subseteq C_{\mathrm{End}(\mathscr{T})}(E)\cap V(\lambda) \subseteq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\cap V(\lambda)\,,$$

for a certain $\mathbb{Q}_l$-linear form λ on the $\mathbb{Q}_l$-vector space $C_{\mathrm{End}(\mathscr{T})}(E)$. For the Zariski closure, this shows

$$\overline{(C_{\mathrm{GO}(\mathscr{T})}(E))^0} \subseteq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\cap V(\lambda) \subsetneqq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\,.$$

On the other hand, $(C_{\mathrm{GO}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0$ is the set of all $\overline{\mathbb{Q}}_l$-rational points on a connected linear algebraic group that is defined over $\mathbb{Q}_l$, while $(C_{\mathrm{GO}(\mathscr{T})}(E))^0$ is the set of all $\mathbb{Q}_l$-rational points. Therefore, it is known [Ro, Che] that $(C_{\mathrm{GO}(\mathscr{T})}(E))^0$ is Zariski dense in $(C_{\mathrm{GO}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0$. Hence,

$$(C_{\mathrm{GO}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0 \subseteq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\cap V(\lambda) \subsetneqq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\,,$$

implying $\operatorname{span}_{\overline{\mathbb{Q}}_l}(C_{\mathrm{GO}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E))^0 \subseteq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)\cap V(\lambda) \subsetneqq C_{\mathrm{End}(\mathscr{T}\otimes_{\mathbb{Q}_l}\overline{\mathbb{Q}}_l)}(E)$, too. Thus, we arrived at a contradiction with Corollary 4.10. $\square$

Proof of Theorem 4.1. By (5), $C_{\mathrm{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) = C_{\mathrm{End}(\mathscr{T})}((C_{\mathrm{GO}(\mathscr{T})}(E))^0)$. But every endomorphism of $\mathscr{T}$ that commutes with a certain set, commutes with its $\mathbb{Q}_l$-span. I.e.,

$$C_{\mathrm{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) = C_{\mathrm{End}(\mathscr{T})}(\operatorname{span}_{\mathbb{Q}_l}(C_{\mathrm{GO}(\mathscr{T})}(E))^0)\,.$$

Moreover, E can only be a totally real or a CM field by [Za, Theorems 1.6.a) and 1.5.1], $\mathscr{T} = T\otimes_{\mathbb{Q}}\mathbb{Q}_l(1)$ is free over $E\otimes_{\mathbb{Q}}\mathbb{Q}_l$, and in the totally real case $\dim_E T = 2$ is not possible [vG, Lemma 3.2]. Thus, Proposition 4.11 yields that

$$C_{\mathrm{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) = C_{\mathrm{End}(\mathscr{T})}(\operatorname{span}_{\mathbb{Q}_l}(C_{\mathrm{GO}(\mathscr{T})}(E))^0) = C_{\mathrm{End}(\mathscr{T})}(C_{\mathrm{End}(\mathscr{T})}(E))\,.$$

Moreover, the elements of $C_{\mathrm{End}(\mathscr{T})}(E)$ actually commute with $E\otimes_{\mathbb{Q}}\mathbb{Q}_l \supset E$, which is still contained in $\mathrm{End}(\mathscr{T})$. I.e., $C_{\mathrm{End}(\mathscr{T})}(E) = C_{\mathrm{End}(\mathscr{T})}(E\otimes_{\mathbb{Q}}\mathbb{Q}_l)$. Finally, the classical double centraliser theorem [Is, Corollary 13.18] applies and shows that

$$C_{\mathrm{End}(\mathscr{T})}(\mathrm{MG}^0_{\mathscr{T},k,l}) = C_{\mathrm{End}(\mathscr{T})}(C_{\mathrm{End}(\mathscr{T})}(E\otimes_{\mathbb{Q}}\mathbb{Q}_l)) = E\otimes_{\mathbb{Q}}\mathbb{Q}_l\,. \qquad \square$$

5. An explicit family

The example below gives an illustration on how to apply Theorem 1.1. The family considered has been treated before [EJ14], so most of its properties needed in the proof can simply be cited.

Example 5.1 (An explicit family of $K3$ surfaces with RM by $\mathbb{Q}(\sqrt{2})$). Let $q\colon X \to B$, for $B := \operatorname{Spec} \mathbb{Q}[t, \frac{1}{t(t^2-2)(t^2+2)(t^2-4t+2)(t^2+4t+2)}] \subset \mathbf{A}^1_\mathbb{Q}$, be the family of $K3$ surfaces that is fibre-by-fibre the minimal desingularisation of the double cover of $\mathbf{P}^2$, given by

$$\begin{aligned} w^2 = {} & [(\tfrac{1}{8}t^2 - \tfrac{1}{2}t + \tfrac{1}{4})y^2 + (t^2-2t+2)yz + (t^2-4t+2)z^2] \\ & [(\tfrac{1}{8}t^2 + \tfrac{1}{2}t + \tfrac{1}{4})x^2 + (t^2+2t+2)xz + (t^2+4t+2)z^2][2x^2 + (t^2+2)xy + t^2y^2]\,. \end{aligned}$$

Then

i) the generic fibre X_η of q is of geometric Picard rank 16.

ii) The endomorphism field of X_η is $\mathbb{Q}(\sqrt{2})$.

iii) For every $\theta \in B(\mathbb{C})$, the transcendental part $T \subset H^2(X_\theta(\mathbb{C}), \mathbb{Q})$ of the cohomology of the fibre $X_\theta(\mathbb{C})$ is acted upon by $\mathbb{Q}(\sqrt{2})$.

iv) Let the complex point $\theta \in B(\mathbb{C})$ be of the kind that the fibre $X_\theta(\mathbb{C})$ has Picard rank 16. Then $X_\theta(\mathbb{C})$ has real multiplication by $\mathbb{Q}(\sqrt{2})$.

Proof. For $t_0 \in B$, the ramification locus of the double cover underlying X_{t_0} is a union of six lines, all of which are defined over $\mathbb{Q}(\sqrt{2}, t_0)$. Moreover, a direct calculation shows that no three of these lines have a point in common, except for $t_0 = 0$, $\pm\sqrt{2}$, $\pm\sqrt{-2}$, and $\pm 2 \pm \sqrt{2}$, which are exactly the points excluded from B. Thus, q is indeed a well-defined family of $K3$ surfaces.

i) Certainly, $\operatorname{Pic} X_{\overline{\eta}}$ contains the $\binom{6}{2} = 15$ classes of the exceptional curves, obtained by blowing up the intersection points of the ramification locus, and the pull-back of the class of the general line on $\mathbf{P}^2$. Hence, $\operatorname{rk} \operatorname{Pic} X_{\overline{\eta}} \geq 16$. On the other hand, for $t_0 \equiv 1 \pmod{17{\cdot}23}$, one has $\operatorname{rk} \operatorname{Pic} X_{\overline{t}_0} = 16$ [EJ14, Theorem 6.6]. As the geometric Picard rank does not increase under generisation, the claim is established.

ii) Spreading out, one finds a morphism $\underline{q}\colon \underline{X} \to \underline{B}$ of schemes of finite type over $\mathbb{Z}$, where $\underline{B} \subset \mathbf{A}^1_{\mathbb{Z}[\frac{1}{l}]}$ is an open subscheme. Restricting to a further open subscheme, one may assume that every fibre is a $K3$ surface.

Let us put $D := 8$ and $a := 3$ or 5 and consider an arbitrary $\mathbb{F}_p$-rational point $\tau \in \underline{B}(\mathbb{F}_p)$, for $p \equiv a \pmod 8$ any prime number. Then one has $\sqrt{2} \notin \mathbb{F}_p$. From this, one directly deduces that Frobenius operates on the six lines of the ramification locus by a permutation of type $(12)(34)(5)(6)$. Therefore, the induced operation on the fifteen pairs fixes only three of them, $\{1,2\}$, $\{3,4\}$, and $\{5,6\}$, while the other twelve form six 2-cycles.

On the other hand, write $\underline{X}'_\tau$ for the double cover of $\mathbf{P}^2$ underlying $\underline{X}_\tau$. Then, since $p \equiv 3, 5 \pmod 8$, it is known [EJ14, Theorem 6.3] that $\#\underline{X}'_\tau(\mathbb{F}_p) = p^2 + p + 1$. Furthermore, the lines $E_{12}, \ldots, E_{56}$ are blown down, exactly three of which contain $\mathbb{F}_p$-rational points. Consequently,

$$\#\underline{X}_\tau(\mathbb{F}_p) = \#\underline{X}'_\tau(\mathbb{F}_p) + 3p = p^2 + 4p + 1 \equiv 1 \pmod p\,.$$

In other words, Theorem 1.1.a) applies and shows that the generic fibre X_η has indeed real or complex multiplication. Write E for the endomorphism field of X_η.

Moreover, for $t_0 \equiv 1 \pmod{17{\cdot}23}$, the special fibre X_{t_0} has real multiplication by $\mathbb{Q}(\sqrt{2})$, according to [EJ14, Theorem 6.6]. Thus, Corollary 4.6 yields $E \subseteq \mathbb{Q}(\sqrt{2})$.

Together with the fact that $E \supsetneqq \mathbb{Q}$, this shows that X_η has real multiplication exactly by $\mathbb{Q}(\sqrt{2})$.

iii) This is just an application of Theorem 1.1.b).

iii) Here, the transcendental part $T \subset H^2(X_\theta(\mathbb{C}), \mathbb{Q})$ is of dimension 6. By Theorem 1.1.b), once again, about its endomorphism field E_θ we know that $E_\theta \supseteq \mathbb{Q}(\sqrt{2})$.

Assume that equality does not hold. Then $2 \mid [E_\theta : \mathbb{Q}] \mid 6$ and $2 \neq [E_\theta : \mathbb{Q}]$, which together leave $[E_\theta : \mathbb{Q}] = 6$ as the only option. In this case, real multiplication is impossible, due to [Za, Remark 1.5.3.c)]. Thus, E_θ must be a CM field of degree 6. Its totally real subfield is hence cubic and contains $\mathbb{Q}(\sqrt{2})$, a contradiction. □

6. A second explicit family

In order to specify the endomorphism field $E \supsetneqq \mathbb{Q}$, whose existence follows from Theorem 1.1.a), a few particular assumptions are necessary. We will use the result below for $d = 2$.

Proposition 6.1. *Let d and n be positive integers, k a number field, X a $K3$ surface over k, and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two prime ideals of k at which X has good reduction. Suppose that*

- $\operatorname{rk} \operatorname{Pic} X_{\overline{k}} \geq n$, *and*
- $\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_1}} = \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_2}} = n + d$, *whereas* $\operatorname{disc} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_1}} / \operatorname{disc} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_2}} \notin (\mathbb{Q}^*)^2$.

I.e., that the Picard lattices are incompatible in that sense that the quotient of their discriminants is a non-square in $\mathbb{Q}^*$.

a) (Degree bound for the endomorphism field) *Then, for the degree of the endomorphism field E, the inequality $[E : \mathbb{Q}] \leq d$ is true.*

b) (Van Luijk's method) *One has $n \leq \operatorname{rk} \operatorname{Pic} X_{\overline{k}} \leq n + d - [E : \mathbb{Q}]$.*

Proof. a) Applying van Luijk's method (cf. [vL, Remark 3.2]) in the most naive way, one sees that $\operatorname{rk} \operatorname{Pic} X_{\overline{k}} \leq n + d - 1$. Therefore,

$$1 = (n + d) - (n + d - 1) \leq \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_1}} - \operatorname{rk} \operatorname{Pic} X_{\overline{k}} \leq (n + d) - n = d\,. \tag{11}$$

Lemma 6.2 below shows that this yields $[E : \mathbb{Q}] \leq d$.

b) Again according to Lemma 6.2, one has that $[E : \mathbb{Q}] \mid (\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}_1}} - \operatorname{rk} \operatorname{Pic} X_{\overline{k}})$. Thus, inequality (11) shows that the difference between the two ranks is at least $[E : \mathbb{Q}]$. This is exactly the asserted inequality to the right. The inequality to the left is part of the assumptions. □

Lemma 6.2. *Let k be a number field, X a $K3$ surface over k, and $\mathfrak{p}$ be a prime ideal of k at which X has good reduction. Suppose that X has real or complex multiplication by an endomorphism field E. Then*

$$[E : \mathbb{Q}] \mid (\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_{\mathfrak{p}}} - \operatorname{rk} \operatorname{Pic} X_{\overline{k}})\,.$$

Proof. Let $\mathscr{P}_{\mathfrak{p}} \subseteq H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$ be the vector space of those classes that are algebraic after specialisation to $H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_{\mathfrak{p}}}, \mathbb{Q}_l(1))$, and put $\mathscr{T}_{\mathfrak{p}} := (\mathscr{P}_{\mathfrak{p}})^\perp$. In particular,

$\mathscr{T}_\mathfrak{p} \subseteq \mathscr{T}$, as algebraic classes remain algebraic under specialisation. To specify this inclusion more precisely, let us write down an orthogonal decomposition

$$\mathscr{T} = \mathscr{T}_\mathfrak{p} \oplus \mathfrak{S} \,. \tag{12}$$

I.e., $\mathfrak{S}$ consists of the classes in $\mathscr{T}$ that become algebraic after specialisation to $X_{\overline{\mathbb{F}}_\mathfrak{p}}$. As all these are defined over a finite extension $\mathbb{F}_{\mathfrak{p}^m}$ of $\mathbb{F}_\mathfrak{p}$, for a certain $m \in \mathbb{N}$, the power $(\mathrm{Frob}_\mathfrak{p})^m$ operates on $\mathfrak{S}$ with only eigenvalue 1.

On the other hand, there is some $n \in \mathbb{N}$ such that the operation of $(\mathrm{Frob}_\mathfrak{p})^n$ on $\mathscr{T} \subset H^2_\text{ét}(X_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_l(1))$ commutes with that of E, cf. [EJ14, Corollary 4.2]. The further power $(\mathrm{Frob}_\mathfrak{p})^{nm}$ operates on $\mathfrak{S}$ again with only eigenvalue 1. However, the Tate conjecture in the variant of Fact 1.6.b) implies that eigenvalue 1 does not occur on $\mathscr{T}_\mathfrak{p}$. Since E and $(\mathrm{Frob}_\mathfrak{p})^{nn'}$ commute, this enforces that E maps $\mathfrak{S}$ to itself.

Finally, by Sublemma 6.3, the splitting (12) descends to $T \subset H^2(X(\mathbb{C}), \mathbb{Q})$,

$$T = T_\mathfrak{p} \oplus S \,.$$

Moreover, the operation of E on T must map S to itself, as this is true after tensoring with $\mathbb{Q}_l(1)$, and $\mathbb{Q}_l(1)$ is faithfully flat over $\mathbb{Q}$. In other words, S is not just a $\mathbb{Q}$-vector space, but an E-vector space. Consequently,

$$[E:\mathbb{Q}] \mid \dim_\mathbb{Q} S = \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} - \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{k}} \,,$$

as claimed. □

Sublemma 6.3. *Let k be a number field, X a $K3$ surface over k, and $\mathfrak{p}$ be a prime ideal of k at which X has good reduction. Denote by $\mathscr{P}_\mathfrak{p} \subseteq H^2_\text{ét}(X_{\overline{k}}, \mathbb{Q}_l(1))$ the vector space of the classes being algebraic after specialisation to $H^2_\text{ét}(X_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_l(1))$. Then there is some subvector space $P_\mathfrak{p} \subset H^2(X(\mathbb{C}), \mathbb{Q})$ such that, under the comparison isomorphism* [SGA4, Exposé 11, Théorème 4.4.iii)], *$\mathscr{P}_\mathfrak{p} = P_\mathfrak{p} \otimes_\mathbb{Q} \mathbb{Q}_l(1)$.*

Proof. For A any $\mathbb{Q}_l$-vector space, the Chern class homomorphism, combined with the specialisation and comparison isomorphisms, yields an injection

$$c_1^{(A)}\colon\ \mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} \otimes_\mathbb{Z} A \longrightarrow H^2_\text{ét}(X_{\overline{\mathbb{F}}_\mathfrak{p}}, A) \cong H^2_\text{ét}(X_{\overline{k}}, A) \cong H^2(X(\mathbb{C}), \mathbb{Q}) \otimes_\mathbb{Q} A \,,$$

which is natural in A. In particular, the difference kernels of the vertical arrows of the commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} \otimes_\mathbb{Z} \mathbb{Q}_l(1) \otimes_\mathbb{Q} \mathbb{Q}_l(1) & \xrightarrow{c_1^{(\mathbb{Q}_l(1)\otimes_\mathbb{Q}\mathbb{Q}_l(1))}} & H^2(X(\mathbb{C}), \mathbb{Q}) \otimes_\mathbb{Q} \mathbb{Q}_l(1) \otimes_\mathbb{Q} \mathbb{Q}_l(1) \\ {\scriptstyle \mathrm{id}\otimes 1\otimes \mathrm{id}} \uparrow\uparrow {\scriptstyle \mathrm{id}\otimes\mathrm{id}\otimes 1} & & {\scriptstyle \mathrm{id}\otimes 1\otimes \mathrm{id}} \uparrow\uparrow {\scriptstyle \mathrm{id}\otimes\mathrm{id}\otimes 1} \\ \mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} \otimes_\mathbb{Z} \mathbb{Q}_l(1) & \xrightarrow{c_1^{(\mathbb{Q}_l(1))}} & H^2(X(\mathbb{C}), \mathbb{Q}) \otimes_\mathbb{Q} \mathbb{Q}_l(1) \end{array}$$

are connected by a descent homomorphism

$$c_\mathfrak{p}\colon\ \mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} \otimes_\mathbb{Z} \mathbb{Q} \longrightarrow H^2(X(\mathbb{C}), \mathbb{Q}) \,.$$

Its image $\mathrm{im}\, c =: P_\mathfrak{p}$ is the desired subvector space. □

Notation. Let X be a $K3$ surface over a number field k and $\mathfrak{p}$ a prime ideal of k, at which X has good reduction.

i) We denote by $\chi_{\mathfrak{p}^n}^{\mathscr{T}}$ the characteristic polynomial of $(\mathrm{Frob}_\mathfrak{p})^n \in \mathrm{Gal}(\overline{k}/k)$ on the transcendental part $\mathscr{T} \subset H^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Q}_l(1))$.

ii) We factorise $\chi_{\mathfrak{p}^n}^{\mathscr{T}} \in \mathbb{Q}[Z]$ completely in the form $\chi_{\mathfrak{p}^n}^{\mathscr{T}}(Z) = \chi_{\mathfrak{p}^n}^{\mathrm{tr}}(Z) \cdot \prod_{i=1}^d (Z - \zeta_{k_i}^{e_i})$, for $k_1, \ldots, k_d \in \mathbb{N}$. I.e. in such a way that $\chi_{\mathfrak{p}^n}^{\mathrm{tr}} \in \mathbb{Q}[Z]$ does not have any further zeroes being roots of unity.

Remarks 6.4. i) The power $(\mathrm{Frob}_\mathfrak{p})^n$ of the Frobenius element is uniquely determined up to conjugation, so $\chi_{\mathfrak{p}^n}^{\mathscr{T}}$ is well-defined. By [SGA4, Exposé XVI, Corollaire 2.2], it coincides with the characteristic polynomial of Frob on the corresponding part of $H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_l(1))$. In particular, $\chi_{\mathfrak{p}^n}^{\mathscr{T}}$ is, in fact, a polynomial with coefficients in $\mathbb{Q}$ [De74, Théorème 1.6].
By definition, one has $\deg \chi_{\mathfrak{p}^n}^{\mathscr{T}} = 22 - \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{k}}$.
ii) According to the Tate conjecture (Fact 1.6.b)), $\chi_{\mathfrak{p}^n}^{\mathrm{tr}}$ is the characteristic polynomial of Frob^n on the transcendental part of $H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_l(1))$. Let us note, in particular, that $\deg \chi_{\mathfrak{p}^n}^{\mathrm{tr}} = 22 - \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}}$.
iii) Consequently, one has that $d = \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{\mathbb{F}}_\mathfrak{p}} - \mathrm{rk}\,\mathrm{Pic}\, X_{\overline{k}}$.

In order to decide which quadratic number field exactly is the endomorphism field, the following result is useful.

Proposition 6.5. *Let $\mathfrak{p}$ be a prime of good reduction of the $K3$ surface X over a number field k, having real or complex multiplication by a field E containing the quadratic number field $\mathbb{Q}(\sqrt{\delta})$. Then at least one of the following two statements is true.*
i) *The polynomial $\chi_{\mathfrak{p}}^{\mathrm{tr}} \in \mathbb{Q}[Z]$ is the norm of a polynomial from $\mathbb{Q}(\sqrt{\delta})[Z]$.*
ii) *For some $n \in \mathbb{N}$, the polynomial $\chi_{\mathfrak{p}^n}^{\mathrm{tr}}$ is a square in $\mathbb{Q}[Z]$.*

Proof. This is essentially [EJ14, Theorem 4.9]. Note that the proof given in [EJ14] works over an arbitrary number field. □

Notation. Let $q\colon X \to B$ be the family from Example 1.5 and $q'\colon X' \to B$ the underlying family of double covers of $\mathbf{P}^2$.
i) Spread out in the obvious way, i.e. put $\underline{B} := \mathrm{Spec}\, \mathbb{Z}[T, \frac{1}{(T-1)(T^4-T^3+T^2-T+1)}] \subset \mathbf{A}^1_\mathbb{Z}$ and let $\underline{X}'$ be the double cover of $\mathbf{P}^2_{\underline{B}}$ given by the same equation as (3). We denote the family of schemes thus obtained by $\underline{q}'\colon \underline{X}' \to \underline{B}$.
ii) Let $\underline{X}$ be the blow-up of $\underline{X}'$ in the 15 codimension-2 subschemes being the Zariski closures of the 15 singular points on the generic fibre $\underline{X}'_\eta$. For the resulting family, let us write $\underline{q}\colon \underline{X} \to \underline{B}$.

Proof for Example 1.5. For $t_0 \in B$, the ramification locus of the double cover underlying X_{t_0} is a union of six lines, all of which are defined over $\mathbb{Q}(\zeta_5, t_0)$. Indeed, the quartic occurring in (3) is the norm form of the linear form $x - \zeta_5 y + \zeta_5^2 z$ defined over $\mathbb{Q}(\zeta_5)$.

Moreover, no three of the five lines in the ramification locus that do not depend of t have a point in common, the ten points of intersection being $(1 : \frac{\sqrt{5}-1}{2} : 1)$,

$(1\!:\!\zeta_5\!+\!\zeta_5^3\!:\!\zeta_5^4)$, $(1\!:\!0\!:\!-\zeta_5)$, and their conjugates. A direct calculation shows that the sixth line passes through one of these points if and only of $t_0 = 1$ or t_0 is a proper tenth root of unity. As these are exactly the points excluded from B, q is indeed a family of $K3$ surfaces.

i) Having spread out as described, one has the morphism $\underline{q}\colon \underline{X} \to \underline{B}$ of schemes of finite type over $\mathbb{Z}$. Restricting to a suitable open subscheme, one may assume that $\underline{B} \subseteq \mathbf{A}^1_{\mathbb{Z}[\frac{1}{l}]}$ and that every fibre is a $K3$ surface.

Furthermore, since $\operatorname{Pic} X_{\overline{\eta}}$, contains the span of the $\binom{6}{2} = 15$ classes of the exceptional curves, obtained by blowing up the intersection points of the ramification locus, and the pull-back of the class of the general line on $\mathbf{P}^2$, one certainly has $\operatorname{rk}\operatorname{Pic} X_{\overline{\eta}} \geq 16$.

In order to apply Theorem 1.1, let us put $D := 5$ and $a := 2$ or 3 and consider an arbitrary $\mathbb{F}_p$-rational point $\tau \in \underline{B}(\mathbb{F}_p)$, for $p \equiv a \pmod 5$ any prime number. Then $\sqrt{5} \notin \mathbb{F}_p$. Therefore, Frobenius operates on the six lines of the ramification locus by a permutation of type (1)(2)(3456). Hence, the induced operation on the fifteen pairs fixes only one of them, $\{1, 2\}$, while the other twelve form two 4-cycles and two 2-cycles.

On the other hand, Lemma 6.7 below shows that $\#\underline{X}'_\tau(\mathbb{F}_p) = p^2 + p + 1$. As the lines $E_{12}, \ldots, E_{56}$ are blown down, exactly one of which contains $\mathbb{F}_p$-rational points, this yields
$$\#\underline{X}_\tau(\mathbb{F}_p) = \#\underline{X}'_\tau(\mathbb{F}_p) + p = p^2 + 2p + 1\,.$$
In other words, Theorem 1.1.a) applies and shows that X_η has indeed real or complex multiplication. Write E for the endomorphism field of X_η. Clearly, $[E\!:\!\mathbb{Q}] \geq 2$.

Next, consider the closed point $t_0 := 15 \in B$. Then $\operatorname{rk}\operatorname{Pic} X_{\overline{t}_0} \geq \operatorname{rk}\operatorname{Pic} X_{\overline{\eta}} \geq 16$, as the geometric Picard rank cannot drop under specialisation. Moreover, by Corollary 4.6, for the endomorphism field, one has $E_{t_0} \supseteq E$ and, in particular, $[E_{t_0}\!:\!\mathbb{Q}] \geq 2$. On the other hand, X_{t_0} has two reductions of geometric Picard rank 18 with incompatible discriminants, cf. Lemma 6.6. Thus, Proposition 6.1 applies to X_{t_0} with $n = 16$ and $d = 2$. It yields that $\operatorname{rk}\operatorname{Pic} X_{\overline{t}_0} = 16$ and that $[E_{t_0}\!:\!\mathbb{Q}] = 2$.

As η is a generisation of t_0, one finds that $\operatorname{rk}\operatorname{Pic} X_{\overline{\eta}} \leq 16$. As we saw the other inequality above, the proof of i) is complete.

ii) Recall the facts that $[E : \mathbb{Q}] \geq 2$, $[E_{t_0} : \mathbb{Q}] = 2$, and $E \subseteq E_{t_0}$, which were all found during the proof of i). Together, they immediately show that $[E : \mathbb{Q}] = 2$. Consequently, $E_{t_0} = E$, so it is enough to verify that $E_{t_0} = \mathbb{Q}(\sqrt{5})$.

As E_{t_0} is known to be a quadratic number field, this follows from Proposition 6.5. Indeed,
$$\chi_{19}^{\mathrm{tr}} = Z^4 - \tfrac{14}{19}Z^3 + \tfrac{34}{19}Z^2 - \tfrac{14}{19}Z + 1 = (Z^2 - \tfrac{7+5\sqrt{5}}{19}Z + 1)(Z^2 - \tfrac{7-5\sqrt{5}}{19}Z + 1)$$
splits over $\mathbb{Q}(\sqrt{5})$ and over no other quadratic field. In fact, $\operatorname{Gal}(\chi_{19}^{\mathrm{tr}}) = D_4$, which has only one intransitive subgroup of index two. Observe, moreover, that the splitting field of χ_{19}^{tr} does not contain any roots of unity, except for (-1). Thus, if $\chi_{19^n}^{\mathrm{tr}}$ were a perfect square for some $n \in \mathbb{N}$ then this would happen for $n = 2$, already, which is not the case.

iii) According to Corollary 4.7, this is a direct consequence of ii).

iv) This is exactly the same argument as in Example 5.1.iv). $\square$

Lemma 6.6. a) *Put* $\tau_1 := (0 \bmod 3) \in \underline{B} \subset \mathbf{A}^1_{\mathbb{Z}}$. *Then the special fibre* $\underline{X}_{\tau_1}$ *of* $\underline{q}$ *is a* $K3$ *surface over* $\mathbb{F}_3$ *of geometric Picard rank* 18. *The discriminant of the Picard lattice is* $\overline{(-1)} \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ *and one has* $\chi_3^{\rm tr}(Z) = Z^4 - \frac{4}{3}Z^2 + 1$.

b) *Put* $\tau_2 := (15 \bmod 19) \in \underline{B} \subset \mathbf{A}^1_{\mathbb{Z}}$. *Then the special fibre* $\underline{X}_{\tau_2}$ *of* $\underline{q}$ *is a* $K3$ *surface over* $\mathbb{F}_{19}$ *of geometric Picard rank* 18. *The discriminant of the Picard lattice is* $\overline{(-11)} \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ *and one has* $\chi_{19}^{\rm tr}(Z) = Z^4 - \frac{14}{19}Z^3 + \frac{34}{19}Z^2 - \frac{14}{19}Z + 1$.

Proof. One first has to check that the family $\underline{q}$ has good reduction at these two closed points. For this, let us note the following.

The five lines in the ramification locus that are independent of t are distinct in every characteristic $\neq 5$. Their ten points of intersection are distinct in every characteristic $\neq 2, 5$. Moreover, the sixth ramification line is distinct from the others, for every value of t, in every characteristic $\neq 5$. Thus, if $p \neq 2, 5$, $a \not\equiv 1 \pmod p$, and $a^5 \not\equiv -1 \pmod p$ then q has good reduction at $(a \bmod p) \in \underline{B} \subset \mathbf{A}^1_{\mathbb{Z}}$. This criterion applies to $\tau_1 = (0 \bmod 3)$, as well as to $\tau_2 = (15 \bmod 19)$.

In order to determine the characteristic polynomials and geometric Picard ranks, one has to count the points on $\underline{X}_{\tau_1}$ and $\underline{X}_{\tau_2}$ that are defined over the prime field and some of its extensions. We applied routine methods for this, using `magma`. For some background, the reader might consult [EJ16]. Finally, the discriminants are easily calculated, using the Artin–Tate formula [Mi, Theorem 6.1]. $\square$

Lemma 6.7. *For every prime number* $p \equiv 2, 3 \pmod 5$ *and every* $\mathbb{F}_p$*-rational point* $\tau \in \underline{B}(\mathbb{F}_p)$, *the special fibre* $\underline{X}'_\tau$ *of* $\underline{q}'$ *has point count*

$$\#\underline{X}'_\tau(\mathbb{F}_p) = p^2 + p + 1\,.$$

Proof. Write $\widetilde{\mathbf{P}}^2_{\mathbb{F}_p}$ for the blow-up of $\mathbf{P}^2_{\mathbb{F}_p}$ in $(2:(-1):2)$ and put $\widetilde{X} := \underline{X}' \times_{\mathbf{P}^2_{\underline{B}}} \widetilde{\mathbf{P}}^2_{\mathbb{F}_p}$. Since $(2:(-1):2)$ is, independently of the value of τ, a point on the ramification locus, the assertion is equivalent to $\#\widetilde{X}_\tau(\mathbb{F}_p) = p^2 + 2p + 1$.

Furthermore, $\widetilde{\mathbf{P}}^2_{\mathbb{F}_p}$ is fibred into the lines through $(2:(-1):2)$. We parametrise the fibration by $(v_0:v_1) \in \mathbf{P}^1$ and let $l_{(v_0:v_1)}$ be the line parametrised by

$$u \mapsto ((-2u+v_0):(u+v_1):(-2u))\,. \tag{13}$$

Note here that the line $l_{(v_0:v_1)}$ is indeed independent of the choice of representatives for $(v_0:v_1)$. Moreover, all these lines have $(2:(-1):2)$ as their point at infinity.

Correspondingly, $\widetilde{X}_\tau$ is fibred into genus-2-curves $C_{\tau,(v_0:v_1)}$. It is clearly sufficient to show that $\#C_{\tau,(v_0:v_1)}(\mathbb{F}_p) = p+1$, for every $\tau \in \underline{B}(\mathbb{F}_p)$ and every $(v_0:v_1) \in \mathbf{P}^1(\mathbb{F}_p)$.

A direct calculation, which is easily performed in any computer algebra system, shows that these curves are given by

$$C_{\tau,(v_0:v_1)}\colon w^2 = 25(v_0+(-2t+2)v_1)\cdot P_{(v_0,v_1)}(u)\,, \tag{14}$$

for

$$\begin{aligned} P_{(v_0,v_1)}(u) := u^5 &+ (-v_0+v_1)u^4 \\ &+ (\tfrac{3}{5}v_0^2 - \tfrac{6}{5}v_0v_1 - \tfrac{2}{5}v_1^2)u^3 + (-\tfrac{1}{5}v_0^3 + \tfrac{3}{5}v_0^2v_1 - \tfrac{2}{5}v_1^3)u^2 \\ &+ (\tfrac{1}{25}v_0^4 - \tfrac{4}{25}v_0^3v_1 + \tfrac{1}{25}v_0^2v_1^2 + \tfrac{6}{25}v_0v_1^3 + \tfrac{1}{25}v_1^4)u \\ &+ \tfrac{1}{25}v_0^4v_1 + \tfrac{1}{25}v_0^3v_1^2 + \tfrac{1}{25}v_0^2v_1^3 + \tfrac{1}{25}v_0v_1^4 + \tfrac{1}{25}v_1^5 \,. \end{aligned} \tag{15}$$

One just has to plug the parametrisation (13) into formula (3). Note here that (13) only parametrises an affine open part of the line $l_{(v_0:v_1)}$. Thus, equation (14) describes only a double cover of an affine line, which is the usual way to write down a hyperelliptic curve.

In (14), the coefficient $(v_0+(-2t+2)v_1)$ might be zero. Then the curve is a double line and $\#C_{\tau,(v_0:v_1)}(\mathbb{F}_p) = p+1$ is obviously true. Otherwise, $C_{\tau,(v_0:v_1)}$ is a, possibly trivial, quadratic twist of the curve $C_{(v_0:v_1)}$, given by

$$C_{(v_0:v_1)}\colon w^2 = P_{(v_0,v_1)}(u)\,.$$

Therefore, it suffices to show that $\#C_{(v_0:v_1)}(\mathbb{F}_p) = p+1$.

For this, let us note that $P_{(v_0,v_1)}$ is a permutation polynomial, according to Sublemma 6.8. Thus the number of $\mathbb{F}_p$-rational points on $C_{(v_0:v_1)}$ is the same as that on the curve, given by $w^2 = u$, which is isomorphic to the projective line. $\square$

Sublemma 6.8. *Let $p \equiv 2,3 \pmod 5$ be a prime number. Then, for arbitrary $v_0, v_1 \in \mathbb{F}_p$, the quintic polynomial $P_{(v_0,v_1)} \in \mathbb{F}_p[u]$, defined in (15), is a permutation polynomial. I.e., it induces a bijection of $\mathbb{F}_p$ onto itself.*

Proof. Define $\widetilde{P} \in \mathbb{F}_p[u]$ by $\widetilde{P}(u) := P_{(v_0,v_1)}(u + \frac{v_0-v_1}{5}) - C$, for $C := P_{(v_0,v_1)}(\frac{v_0-v_1}{5})$. This is a normalised form of P, cf. [LN, the remarks before Theorem 7.11]. It is clearly sufficient to show that $\widetilde{P}$ is a permutation polynomial.

For this, a direct calculation shows that

$$\begin{aligned} \widetilde{P}(u) &= u^5 + (\tfrac{1}{5}v_0^2 - \tfrac{2}{5}v_0v_1 - \tfrac{4}{5}v_1^2)u^3 + (\tfrac{1}{125}v_0^4 - \tfrac{4}{125}v_0^3v_1 - \tfrac{4}{125}v_0^2v_1^2 + \tfrac{16}{125}v_0v_1^3 + \tfrac{16}{125}v_1^4)u \\ &= u^5 - 5\alpha u^3 + 5\alpha^2 u\,, \end{aligned}$$

when putting $\alpha := -\frac{1}{25}v_0^2 + \frac{2}{25}v_0v_1 + \frac{4}{25}v_1^2$. This means that $\widetilde{P}$ coincides with the Dickson polynomial $g_5(u,\alpha)$, which is known [LN, Theorem 7.16] to be a permutation polynomial, for every prime number $p \equiv 2,3 \pmod 5$. The proof is therefore complete. $\square$

References

[An] André, Y.: Pour une théorie inconditionnelle des motifs, *Publ. Math. IHES* **83** (1996), 5–49

[BHPV] Barth, W., Hulek, K., Peters, C., and van de Ven, A.: Compact complex surfaces, Second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete 4, *Springer,* Berlin 2004

[BCP] Bosma, W., Cannon, J., and Playoust, C.: The Magma algebra system I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265

[BdS] Bosma, W. and de Smit, B.: On arithmetically equivalent number fields of small degree, in: Algorithmic number theory (Sydney 2002), Lecture Notes in Comput. Sci. 2369, *Springer,* Berlin 2002, 67–79

[Bo] Bourbaki, N.: Éléments de mathématique. Algèbre commutative. Chapitres 1 á 4, *Masson,* Paris 1985

[BtD] Bröcker, T. and tom Dieck, T.: Representations of compact Lie groups, Graduate Texts in Mathematics 98, *Springer,* New York 1985

[Ch13] Charles, F.: The Tate conjecture for $K3$ surfaces over finite fields, *Invent. Math.* **194** (2013), 119–145

[Ch14] Charles, F.: On the Picard number of $K3$ surfaces over number fields, *Algebra Number Theory* **8** (2014), 1–17

[Che] Chevalley, C.: On algebraic group varieties, *J. Math. Soc. Japan* **6** (1954), 303–324

[Com] Commelin, J.: The Mumford-Tate conjecture for the product of an abelian surface and a $K3$ surface, *Doc. Math.* **21** (2016), 1691–1713

[Cox] Cox, D. A.: Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication, *John Wiley & Sons,* New York 1989

[De71] Deligne, P.: Théorie de Hodge II, *Publ. Math. IHES* **40** (1971), 5–57

[De72] Deligne, P.: La conjecture de Weil pour les surfaces $K3$, *Invent. Math.* **15** (1972), 206–226

[De74] Deligne, P.: La conjecture de Weil I, *Publ. Math. IHES* **43** (1974), 273–307

[EGA IV] Grothendieck, A. and Dieudonné, J.: Étude locale des schémas et des morphismes de schémas (EGA IV), *Publ. Math. IHES* **20** (1964), **24** (1965), **28** (1966), **32** (1967)

[EJ14] Elsenhans, A.-S. and Jahnel, J.: Examples of $K3$ surfaces with real multiplication, in: Proceedings of the ANTS XI conference (Gyeongju 2014), *LMS Journal of Computation and Mathematics* **17** (2014), 14–35

[EJ16] Elsenhans, A.-S. and Jahnel, J.: Point counting on $K3$ surfaces and an application concerning real and complex multiplication, in: Algorithmic number theory (Kaiserslautern 2016), *LMS Journal of Computation and Mathematics* **19** (2016), 12–28

[vG] van Geemen, B.: Real multiplication on $K3$ surfaces and Kuga-Satake varieties, *Michigan Math. J.* **56** (2008), 375–399

[Gr] Grauert, H.: Ein Theorem der analytischen Garbentheorie und die Modulräume komplexer Strukturen, *Publ. Math. IHES* **5** (1960), 5–64

[Hi] Hironaka, H.: Resolution of singularities of an algebraic variety over a field of characteristic zero, *Annals of Math.* **79** (1964), 109–326

[Hu] Huybrechts, D.: Lectures on K3 surfaces, Cambridge Studies in Advanced Mathematics 158, *Cambridge University Press,* Cambridge 2016

[Is] Isaacs, I. M.: Algebra. A graduate course, *Brooks/Cole Publishing Co.,* Pacific Grove 1994

[KM] Kim, W. and Madapusi Pera, K.: 2-adic integral canonical models, *Forum Math. Sigma* **4** (2016), e28, 34 pp.

[LW] Lang, S. and Weil, A.: Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827

[LN] Lidl, R. and Niederreiter, H.: Finite fields, Second edition, Encyclopedia of Mathematics and its Applications 20, *Cambridge University Press,* Cambridge 1997

[LMS] Lieblich, M., Maulik, D., and Snowden, A.: Finiteness of $K3$ surfaces and the Tate conjecture, *Ann. Sci. Éc. Norm. Supér.* **47** (2014), 285–308

[vL] van Luijk, R.: $K3$ surfaces with Picard number one and infinitely many rational points, *Algebra & Number Theory* **1** (2007), 1–15

[MP] Madapusi Pera, K.: The Tate conjecture for $K3$ surfaces in odd characteristic, *Invent. Math.* **201** (2015), 625–668

[Mi] Milne, J. S.: On a conjecture of Artin and Tate, *Ann. of Math.* **102** (1975), 517–533

[Mo] Moonen, B.: On the Tate and Mumford-Tate conjectures in codimension 1 for varieties with $h^{2,0} = 1$, *Duke Math. J.* **166** (2017), 739–799

[Pe] Perlis, R.: On the equation $\zeta_K(s) = \zeta_{K'}(s)$, *J. Number Theory* **9** (1977), 342–360

[PSS] Pjatetskij-Shapiro, I. I. and Shafarevich, I. R.: The arithmetic of surfaces of type $K3$ (Russian), Proceedings of the International Conference on Number Theory (Moscow 1971), *Trudy Mat. Inst. Steklova* **132** (1973), 44–54

[Ro] Rosenlicht, M.: Some rationality questions on algebraic groups, *Ann. Mat. Pura Appl.* **43** (1957), 25–50

[SGA1] Grothendieck, A.: Revêtements étales et groupe fondamental (SGA 1), Lecture Notes Math. 224, *Springer,* Berlin 1971

[SGA4] Artin, M., Grothendieck, A. et Verdier, J.-L. (avec la collaboration de Deligne, P. et Saint-Donat, B.): Théorie des topos et cohomologie étale des schémas, Séminaire de Géométrie Algébrique du Bois Marie 1963–1964 (SGA 4), Lecture Notes in Math. 269, 270, 305, *Springer,* Berlin, Heidelberg, New York 1972–1973

[SGA5] Grothendieck, A. (avec la collaboration de Bucur, I., Houzel, C., Illusie, L. et Serre, J.-P.): Cohomologie l-adique et Fonctions L, Séminaire de Géométrie Algébrique du Bois Marie 1965–1966 (SGA 5), Lecture Notes in Math. 589, *Springer,* Berlin, Heidelberg, New York 1977

[Serr] Serre, J.-P.: Zeta and L functions, in: Arithmetical Algebraic Geometry, Proc. Conf. Purdue Univ. 1963 (ed. by O. F. G. Schilling), *Harper & Row,* New York 1965, 82–92

[Si] Silverman, J. H.: Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 151, *Springer,* New York 1994

[Ta90] Tankeev, S. G.: Surfaces of $K3$ type over number fields and the Mumford–Tate conjecture (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), 846–861

[Ta95] Tankeev, S. G.: Surfaces of $K3$ type over number fields and the Mumford–Tate conjecture II (Russian), *Izv. Ross. Akad. Nauk Ser. Mat.* **59** (1995), 179–206

[Za] Zarhin, Yu. G.: Hodge groups of $K3$ surfaces, *J. Reine Angew. Math.* **341** (1983), 193–220

Institut für Mathematik, Universität Würzburg, Emil-Fischer-Strasse 30, D-97074 Würzburg, Germany
Email address: stephan.elsenhans@mathematik.uni-wuerzburg.de
URL: https://www.mathematik.uni-wuerzburg.de/computeralgebra/team/elsenhans-stephan-prof-dr/

Department Mathematik, Univ. Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany
Email address: jahnel@mathematik.uni-siegen.de
URL: http://www.uni-math.gwdg.de/jahnel