Under consideration for publication in Math. Proc. Camb. Phil. Soc.

On the computation of the Picard group for $K3$ surfaces

By Andreas-Stephan Elsenhans[‡]

Mathematisches Institut, Universität Bayreuth, Universitätsstraße 30, D-95440 Bayreuth, Germany

e-mail: `Stephan.Elsenhans@uni-bayreuth.de`

and Jörg Jahnel

Fachbereich 6 Mathematik, Universität Siegen, Walter-Flex-Straße 3, D-57068 Siegen, Germany

e-mail: `jahnel@mathematik.uni-siegen.de`

(*Received* 18 *Octobre* 2010)

Abstract

We present a method to construct examples of $K3$ surfaces of geometric Picard rank 1. Our approach is a refinement of that of R. van Luijk. It is based on an analysis of the Galois module structure on étale cohomology. This allows us to abandon the original limitation to cases of Picard rank 2 after reduction modulo p. Furthermore, the use of Galois data enables us to construct examples that require significantly less computation time.

1. *Introduction*

1·1. The Picard group $\mathrm{Pic}(S)$ of a $K3$ surface S is a highly interesting invariant. When the base field is of characteristic zero, $\mathrm{Pic}(S) \cong \mathbb{Z}^n$ for some $n = 1, \ldots, 20$.

The first explicit examples of $K3$ surfaces over $\mathbb{Q}$ with geometric Picard rank 1 were constructed by R. van Luijk [**12**]. His method is based on reduction modulo p. It works as follows.

i) At a place p of good reduction, the Picard group $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ of the surface injects into the Picard group $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$ of its reduction modulo p.

ii) Furthermore, $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$ injects into the second étale cohomology group $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$.

iii) Only roots of unity can arise as eigenvalues of the geometric Frobenius Frob on the image of $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$ in $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$. The number of eigenvalues of this form, counted with multiplicities, is therefore an upper bound for the Picard rank of $S_{\overline{\mathbb{F}}_p}$. One can compute the eigenvalues of Frob by counting the points on S, defined over $\mathbb{F}_p$ and some finite extensions. Doing this for one prime, one obtains an upper bound for $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$, which is always even. The Tate conjecture asserts that this bound is actually sharp.

[‡] The first author was partially supported by the Deutsche Forschungsgemeinschaft (DFG) through a funded research project.

Therefore, the best that could happen is to find a prime that yields an upper bound of 2 for $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$.

iv) In this case, the assumption that the surface would have Picard rank 2 over $\overline{\mathbb{Q}}$ implies that the discriminants of both Picard groups, $\operatorname{Pic}(S_{\overline{\mathbb{Q}}})$ and $\operatorname{Pic}(S_{\overline{\mathbb{F}}_p})$, belong to the same square class. Note here that reduction modulo p respects the intersection product.

v) When one combines information from two primes, it may happen that one gets the rank bound 2 at both places but that different square classes for the discriminant arise. Then, these data are incompatible with Picard rank 2 over $\overline{\mathbb{Q}}$.

On the other hand, there is a non-trivial divisor known explicitly. Altogether, rank 1 is proven.

REMARK 1·2. This method has been applied by several authors in order to construct $K3$ surfaces with prescribed Picard rank [**12**, **9**, **4**].

1·3. *The refinement.* In this note, we will refine van Luijk's method. Our idea is the following. We do not look at the ranks, only. We analyze the Galois module structures on the Picard groups, too. The point here is that a Galois module typically has submodules by far not of every rank.

As an example, we will construct $K3$ surfaces of geometric Picard rank 1 such that the reduction modulo 3 has geometric Picard rank 4 and the reduction modulo 5 has geometric Picard rank 14.

REMARK 1·4. This work continues our investigations on Galois module structures on the Picard group. In [**5**, **6**, **7**], we constructed cubic surfaces S over $\mathbb{Q}$ with prescribed Galois module structure on $\operatorname{Pic}(S)$.

2. *The Picard group as a Galois module, Global case*

2·1. Let K be a field and S an algebraic surface defined over K. Denote by V the $\mathbb{Q}$-vector space $\operatorname{Pic}(S_{\overline{K}})\otimes_{\mathbb{Z}}\mathbb{Q}$. On V, there is a natural $\operatorname{Gal}(\overline{K}/K)$-operation. The kernel of this representation is a normal subgroup of finite index. It corresponds to a finite Galois extension L of K. In fact, we have a $\operatorname{Gal}(L/K)$-representation.

The group $\operatorname{Gal}(\overline{K}/L)$ acts trivially on $\operatorname{Pic}(S_{\overline{K}})$. I.e.,

$$\operatorname{Pic}(S_{\overline{K}}) = \operatorname{Pic}(S_{\overline{K}})^{\operatorname{Gal}(\overline{K}/L)} .$$

Within this, $\operatorname{Pic}(S_L)$ is, in general, a subgroup of finite index. Equality is true under the hypothesis that $S(L) \neq \emptyset$.

2·2. Now suppose that K is a number field and $\mathfrak{p}$ is a prime ideal of K. We will denote the residue class field by k. Further, let S be a $K3$ surface over K having good reduction at $\mathfrak{p}$.

In this situation, there is the specialization homomorphism from $\operatorname{Pic}(S_{\overline{K}})$ to $\operatorname{Pic}(S_{\overline{k}})$. As intersection products are respected by specialization, the standard argument from [**1**, Proposition VIII.3.6.i)] shows that this is an injection. Taking the tensor product, it yields an inclusion of $\mathbb{Q}$-vector spaces

$$\mathrm{sp}\colon \operatorname{Pic}(S_{\overline{K}})\otimes_{\mathbb{Z}}\mathbb{Q} \hookrightarrow \operatorname{Pic}(S_{\overline{k}})\otimes_{\mathbb{Z}}\mathbb{Q} .$$

Here, both spaces are equipped with a Galois operation. On $\operatorname{Pic}(S_{\overline{K}})\otimes_{\mathbb{Z}}\mathbb{Q}$, we have a $\operatorname{Gal}(L/K)$-action. On $\operatorname{Pic}(S_{\overline{k}})\otimes_{\mathbb{Z}}\mathbb{Q}$, only $\operatorname{Gal}(\overline{k}/k) = \overline{\langle \mathrm{Frob} \rangle}$ operates.

LEMMA 2·3. *The field extension L/K is unramified at $\mathfrak{p}$.*

Proof. Assume the contrary. Then, there are a prime $\mathfrak{q}$ lying above $\mathfrak{p}$ and some element $\sigma \neq \mathrm{id}$ of the decomposition group $G_\mathfrak{q} \subseteq \mathrm{Gal}(L/K)$ that operates trivially on the residue field $\mathscr{O}_L/\mathfrak{q}$.

As $\mathrm{Gal}(\overline{K}/L)$ is the exact kernel of the Galois representation V, there is some $\mathscr{D} \in \mathrm{Pic}(S_L)$ that is not fixed by σ. Let $D \in \mathrm{Div}(S_L)$ be a corresponding divisor. By good reduction, D extends to a divisor on a smooth model $\mathscr{S}$ over the integer ring $\mathscr{O}_L$. In particular, we have the reduction $D_\mathfrak{q}$ of D on the special fiber $S_\mathfrak{q}$.

By assumption, the divisor $D_\mathfrak{q}^\sigma - D_\mathfrak{q}$ is linearly equivalent to zero. The injectivity of the restriction homomorphism $\mathrm{Pic}(S_{\overline{K}}) \to \mathrm{Pic}(S_{\overline{k}})$ implies that $D^\sigma - D$ is linearly equivalent to zero, too. This is a contradiction. □

2·4. There is a Frobenius lift to L, which is unique up to conjugation. When we choose a particular prime $\mathfrak{q}$, lying above $\mathfrak{p}$, we fix a concrete Frobenius lift. Then, $\mathrm{Pic}(S_{\overline{K}}) \otimes_\mathbb{Z} \mathbb{Q}$ becomes a $\mathrm{Gal}(\overline{k}/k)$-submodule of $\mathrm{Pic}(S_{\overline{k}}) \otimes_\mathbb{Z} \mathbb{Q}$.

3. *The Picard group as a Galois module, Local case*

3·1. To describe $\mathrm{Pic}(S_{\overline{k}}) \otimes_\mathbb{Z} \mathbb{Q}$ as a $\mathrm{Gal}(\overline{k}/k) = \overline{\langle \mathrm{Frob} \rangle}$-module, it is sufficient to know the characteristic polynomial χ_{Frob} of Frob. As a certain power of Frob acts as the identity, χ_{Frob} is a product of cyclotomic polynomials.

3·2. *Computability of the Galois representation.* The simplest way to understand the $\mathrm{Gal}(\overline{k}/k)$-representation on $\mathrm{Pic}(S_{\overline{k}}) \otimes_\mathbb{Z} \mathbb{Q}$ in a concrete situation is to use étale cohomology. Counting the numbers of points that S has over finite extensions of k, one may compute the characteristic polynomial Φ of Frobenius on $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Q}_l(1))$. This is actually a polynomial with coefficients in $\mathbb{Q}$ and independent of the choice of $l \neq p$ [**3**, Théorème 1.6].

Via the Chern class homomorphism, $\mathrm{Pic}(S_{\overline{k}}) \otimes_\mathbb{Z} \mathbb{Q}_l$ is a $\mathrm{Gal}(\overline{k}/k)$-submodule of $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Q}_l(1))$. Hence, the polynomial χ_{Frob} divides Φ. According to Tate, it is expected to be maximal product Φ_{cycl} of cyclotomic polynomials dividing Φ.

3·3. Denote by V_{Tate} the largest subspace of $H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Q}_l(1))$, on which all eigenvalues of Frobenius are roots of unity. On the other hand, let P_{expl} be a subgroup of $\mathrm{Pic}(S_{\overline{k}})$ generated by the conjugates of some divisors that are explicitly known.

Then, we have the following chain of $\mathrm{Gal}(\overline{k}/k)$-invariant $\mathbb{Q}_l$-vector spaces,

$$H^2_{\text{ét}}(S_{\overline{k}}, \mathbb{Q}_l(1)) \supseteq V_{\mathrm{Tate}} \supseteq \mathrm{Pic}(S_{\overline{k}}) \otimes_\mathbb{Z} \mathbb{Q}_l \supseteq P_{\mathrm{expl}} \otimes_\mathbb{Z} \mathbb{Q}_l\,.$$

In an optimal situation, the quotient space $V_{\mathrm{Tate}}/(P_{\mathrm{expl}} \otimes_\mathbb{Z} \mathbb{Q}_l)$ has only finitely many $\mathrm{Gal}(\overline{k}/k)$-submodules.

REMARKS 3·4. i) This finiteness condition generalizes the codimension one condition, applied in van Luijk's method, step v).

ii) A sufficient criterion for a vector space V with a $\mathrm{Gal}(\overline{k}/k)$-operation to have only finitely many $\mathrm{Gal}(\overline{k}/k)$-invariant subspaces is that the characteristic polynomial χ_V of Frob has only simple roots. Then, the invariant subspaces are in bijection with the monic polynomials dividing χ_V.

3·5. Our main strategy to prove $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = 1$ for a $K3$ surface S over $\mathbb{Q}$ will now be as follows.

i) Choose distinct prime numbers $p_1, \dots, p_n$ of good reduction. Typically, $n = 2$ should suffice. For each of these primes, execute step ii).

ii) Take as P_{expl} the group generated by the hyperplane section. Verify that the characteristic polynomial χ of Frob on $V_{\text{Tate}}/(P_{\text{expl}} \otimes_{\mathbb{Z}} \mathbb{Q}_l)$ has no multiple roots. Then, $(\text{Pic}(S_{\overline{k}}) \otimes_{\mathbb{Z}} \mathbb{Q})/(P_{\text{expl}} \otimes_{\mathbb{Z}} \mathbb{Q})$ has only finitely many $\text{Gal}(\overline{k}/k)$-invariant subvector spaces. Each of them corresponds to a monic polynomial $p \in \mathbb{Q}[T]$ dividing χ.

iii) Verify $\text{Pic}(S_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q} = P_{\text{expl}} \otimes_{\mathbb{Z}} \mathbb{Q}$ by excluding all other options. Observe here that

$$(\text{Pic}(S_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q})/(P_{\text{expl}} \otimes_{\mathbb{Z}} \mathbb{Q}) \subseteq (\text{Pic}(S_{\overline{k}}) \otimes_{\mathbb{Z}} \mathbb{Q})/(P_{\text{expl}} \otimes_{\mathbb{Z}} \mathbb{Q})$$

is a $\text{Gal}(\overline{k}/k)$-invariant subvector space for $k = \mathbb{F}_{p_1}, \dots, \mathbb{F}_{p_n}$. Thus, we have an n-tuple $(P_1, \dots, P_n)$ of such subspaces that are compatible concerning dimensions and intersection forms. It has to be shown that $(0, \dots, 0)$ is the only such n-tuple.

REMARK 3·6. Our method is inspired by the classical van der Waerden criterion [**15**, Proposition 2.9.35]. This means to use reduction modulo p in order to obtain information about a permutation representation $\iota\colon \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to S_n$. A typical reasoning is as follows.

Suppose $\iota(\text{Frob}_p)$ is a product of disjoint cycles of lengths $l_1, \dots, l_k$. Then, a subset $M \subset \{1, \dots, n\}$ of size k may be ι-invariant only when k is a sum of some of the l_i. Combining information from several primes, it might be possible to establish properties of ι such as transitivity or surjectivity.

Our kind of argument is very similar except that we work with endomorphism (matrix) representations instead of permutation representations.

4. *Discriminants, The Artin-Tate formula*

4·1. The Picard group of a smooth, proper surface is equipped with a $\mathbb{Z}$-valued symmetric bilinear form, the intersection form. For $K3$ surfaces, this form is known to be non-degenerate [**1**, Proposition VIII.3.5)]. Therefore, associated with $\text{Pic}(S_{\overline{k}})$, we have its discriminant, an integer different from zero. The same applies to every subgroup of $\text{Pic}(S_{\overline{k}})$.

For a $\mathbb{Q}$-vector space contained in $\text{Pic}(S_{\overline{k}}) \otimes_{\mathbb{Z}} \mathbb{Q}$, the discriminant is an element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. We will typically choose a representative being an integer and speak of its *square class.*

4·2. Let us recall the Artin-Tate conjecture in the special case of a $K3$ surface.

CONJECTURE (Artin-Tate). *Let Y be a $K3$ surface over $\mathbb{F}_q$. Denote by ρ the rank and by Δ the discriminant of the Picard group* $\text{Pic}(Y)$*, defined over $\mathbb{F}_q$. Then,*

$$|\Delta| = \frac{q \cdot \lim\limits_{T \to 1} \frac{\Phi(T)}{(T-1)^\rho}}{\#\text{Br}(Y)}\,.$$

Here, Φ is the characteristic polynomial of Frobenius on $H^2_{\text{ét}}(Y_{\overline{\mathbb{F}}_q}, \mathbb{Q}_l(1))$. Finally, $\text{Br}(Y)$ *denotes the Brauer group of Y.*

REMARKS 4·3. a) The Artin-Tate formula allows to compute the square class of the discriminant of the Picard group over a finite field without any knowledge of explicit generators.

b) Observe that $\#\text{Br}(Y)$ is always a perfect square [**11**].

c) The Artin-Tate formula is proven for most $K3$ surfaces. Most notably, the Tate conjecture implies the Artin-Tate formula [**14**]. We will use the Artin-Tate formula only in situations where the Tate conjecture is true. Thus, our final result will not depend on unproven statements.

d) The Artin-Tate formula has been used before by R. Kloosterman [**9**] in his investigations on elliptic $K3$ surfaces.

5. *An example*

5·1. *Formulation*

EXAMPLE 5·1·1. Let $S\colon w^2 = f_6(x, y, z)$ be a $K3$ surface of degree 2 over $\mathbb{Q}$. Assume the congruences

$$f_6 \equiv y^6 + x^4y^2 + 3x^2y^4 + 2x^5z + 3xz^5 + z^6 \pmod 5$$

and

$$f_6 \equiv 2x^6 + x^4y^2 + 2x^3y^2z + x^2y^2z^2 + x^2yz^3 + 2x^2z^4 + xy^4z + xy^3z^2 + xy^2z^3 + 2xz^5 + 2y^6 + y^4z^2 + y^3z^3 \pmod 3 .$$

Then, S has geometric Picard rank 1.

5·2. *Explicit divisors*

NOTATION 5·2·1. We will write $\mathrm{pr}\colon S \to \mathbf{P}^2$ for the canonical projection. On S, there is the ample divisor $H := \pi^*L$ for L a line on $\mathbf{P}^2$.

5·2·2. Let C be any irreducible divisor on S. Then, $D := \pi(C)$ is a curve in $\mathbf{P}^2$. We denote its degree by d. The projection from C to D is generically 2:1 or 1:1. In the case it is 2:1, we have $C = \pi^*D \sim dH$.

Thus, to generate a Picard group of rank >1, divisors are needed that are generically 1:1 over their projections. This means, π^*D must be reducible into two components which we call the *splittings* of D.

A divisor D has a split pull-back if and only if f_6 is a perfect square on (the normalization of) D. A necessary condition is that the intersection of D with the ramification locus given by $f_6 = 0$ is a 0-cycle divisible by 2.

5·3. *The modulo 3 information*

5·3·1. The sextic curve in $\mathbf{P}^2_{\mathbb{F}_3}$ given by $f_6 = 0$ has three conjugate conics, each being tangent in six points. Indeed, note that, for

$$f_3 := x^3 + 2x^2y + x^2z + 2xy^2 + xyz + xz^2 + y^3 + y^2z + 2yz^2 + 2z^3,$$

the term $f_6 - f_3^2$ factors into three quadratic forms over $\mathbb{F}_{27}$. Consequently, we have three divisors on $\mathbf{P}^2_{\mathbb{F}_{27}}$, the pull-backs of which split.

5·3·2. Counting the points on S over $\mathbb{F}_{3^n}$ for $n = 1, \ldots, 11$ yields the numbers $(-2), (-8), 28, 100, 388, 2\,458, 964, (-692), 26\,650, (-20\,528)$, and $(-464\,444)$ for the traces of the iterated Frobenius on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_3}, \mathbb{Q}_l)$. Taking into account the fact that 1 is a root, these data uniquely determine the characteristic polynomial Φ of Frob on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_3}, \mathbb{Q}_l(1))$,

$$\Phi(t) = t^{22} + \tfrac{2}{3}t^{21} + \tfrac{2}{3}t^{20} - \tfrac{1}{3}t^{18} - \tfrac{2}{3}t^{17} - t^{16} - \tfrac{2}{3}t^{15} - \tfrac{1}{3}t^{14} + \tfrac{1}{3}t^{12} + \tfrac{2}{3}t^{11} + \tfrac{1}{3}t^{10} - \tfrac{1}{3}t^{8} - \tfrac{2}{3}t^{7} - t^{6} - \tfrac{2}{3}t^{5} - \tfrac{1}{3}t^{4} + \tfrac{2}{3}t^{2} + \tfrac{2}{3}t + 1 .$$

The functional equation holds with the plus sign. We factorize and obtain

$$\begin{aligned}\Phi(t) = {} & (t-1)^2(t^2+t+1) \\ & (t^{18} + \tfrac{5}{3}t^{17} + \tfrac{7}{3}t^{16} + \tfrac{10}{3}t^{15} + \tfrac{11}{3}t^{14} + \tfrac{11}{3}t^{13} + \tfrac{11}{3}t^{12} + \tfrac{10}{3}t^{11} + 3t^{10} \\ & \quad + 3t^9 + 3t^8 + \tfrac{10}{3}t^7 + \tfrac{11}{3}t^6 + \tfrac{11}{3}t^5 + \tfrac{11}{3}t^4 + \tfrac{10}{3}t^3 + \tfrac{7}{3}t^2 + \tfrac{5}{3}t + 1)\,.\end{aligned}$$

5·3·3. The first two factors are cyclotomic polynomials while the last one is not. In the notation of section 3, V_{Tate} is a $\mathbb{Q}_l$-vector space of dimension four. On the other hand, P_{expl} is generated by H. As H corresponds to one of the factors $(t-1)$, the characteristic polynomial of Frobenius on $V_{\mathrm{Tate}}/(P_{\mathrm{expl}} \otimes_{\mathbb{Z}} \mathbb{Q}_l)$ is

$$(t-1)(t^2+t+1)\,.$$

It has only simple roots.

Consequently, for each of the dimensions 1, 2, 3, and 4, there is at most one $\mathrm{Gal}(\overline{\mathbb{F}}_3/\mathbb{F}_3)$-invariant subvector space in $\mathrm{Pic}(S_{\overline{\mathbb{F}}_3}) \otimes_{\mathbb{Z}} \mathbb{Q}$ containing the Chern class of H. The existence of these subspaces would be assured by the Tate conjecture.

5·3·4. Let us discuss the corresponding discriminants.

i) The one-dimensional invariant subspace has discriminant 2.

ii) As Φ has a double zero at 1, the conjectural two dimensional invariant subspace is necessarily equal to $\mathrm{Pic}(S_{\mathbb{F}_3}) \otimes_{\mathbb{Z}} \mathbb{Q}$. We may compute the square class of the corresponding discriminant according to the Artin-Tate formula. The result is (-489).

REMARK 5·3·5. The Tate conjecture predicts Picard rank 2 for $S_{\mathbb{F}_3}$. The absolute value of the discriminant is rather large. The implications of this are annoying.

i) Let C be an irreducible divisor on $S_{\mathbb{F}_3}$, linearly independent of H. Then, C is a splitting of a curve D of degree $d \geq 23$. Indeed, H is a genus-2 curve. Hence, $H^2 = 2$. For the discriminant, we find $-489 \geq 2C^2 - d^2$. As $C^2 \geq -2$, the assertion follows.

ii) Further, D must be highly singular on the ramification locus. In fact, we have $C^2 \leq \frac{d^2-489}{2}$ and $D^2 = d^2$. Hence, going from D to C lowers the arithmetic genus by at least $\frac{d^2+489}{4}$.

As a consequence of these calculations, we are afraid that there is no way to find a second generator of $\mathrm{Pic}(S_{\mathbb{F}_3})$, explicitly.

5·3·6. iii) It turns out that the divisors given by splitting the conics that are six times tangent to the ramification sextic generate a rank three submodule of $\mathrm{Pic}(S_{\overline{\mathbb{F}}_3})$. Its discriminant is

$$\det \begin{pmatrix} -2 & 6 & 0 \\ 6 & -2 & 4 \\ 0 & 4 & -2 \end{pmatrix} = 96\,.$$

Hence, for the three-dimensional invariant subspace, the discriminant is in the square class of 6.

iv) For the conjectural invariant subspace of dimension four, the Artin-Tate formula yields a discriminant of (-163).

REMARK 5·3·7. We will not need the discriminants of the invariant subspaces of dimensions 3 and 4.

5·4. *The modulo 5 information*

5·4·1. The sextic curve in $\mathbf{P}^2_{\overline{\mathbb{F}}_5}$ given by $f_6 = 0$ has six tritangent lines. These are given by $L_a \colon t \mapsto [1 : t : a]$ where a is a zero of $a^6 + 3a^5 + 2a$. The pull-back of each of these lines splits on the $K3$ surface $S_{\overline{\mathbb{F}}_5}$.

5·4·2. On the other hand, counting points yields the following traces of the iterated Frobenius on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_5}, \mathbb{Q}_l)$,

$$15, 95, (-75), 2\,075, (-1\,250), (-14\,875), 523\,125, 741\,875, 853\,125, 11\,293\,750\,.$$

This leads to the characteristic polynomial

$$\begin{aligned}\Phi(t) = {}& t^{22} - 3t^{21} + \tfrac{13}{5}t^{20} + \tfrac{7}{5}t^{19} - \tfrac{24}{5}t^{18} + \tfrac{21}{5}t^{17} - \tfrac{2}{5}t^{16} - \tfrac{22}{5}t^{15} + \tfrac{34}{5}t^{14}\\ & - \tfrac{17}{5}t^{13} - \tfrac{17}{5}t^{12} + \tfrac{34}{5}t^{11} - \tfrac{17}{5}t^{10} - \tfrac{17}{5}t^{9} + \tfrac{34}{5}t^{8} - \tfrac{22}{5}t^{7} - \tfrac{2}{5}t^{6} + \tfrac{21}{5}t^{5}\\ & - \tfrac{24}{5}t^{4} + \tfrac{7}{5}t^{3} + \tfrac{13}{5}t^{2} - 3t + 1\\ = {}& (t-1)^2(t^4+t^3+t^2+t+1)(t^8-t^7+t^5-t^4+t^3-t+1)\\ & (t^8 - t^7 - \tfrac{2}{5}t^6 + \tfrac{3}{5}t^5 - \tfrac{1}{5}t^4 + \tfrac{3}{5}t^3 - \tfrac{2}{5}t^2 - t + 1)\,.\end{aligned}$$

Observe here that the first two factors correspond to the part of the Picard group that is generated by the splittings of the six tritangent lines.

Indeed, the intersection matrix of these divisors turns out to be of rank six. One could have selected six linearly independent elements from $\mathrm{Pic}(S_{\overline{\mathbb{F}}_5})$ and determined these two factors directly.

REMARK 5·4·3. The knowledge of these two factors allows to compute the characteristic polynomial Φ from only the numbers of points over $\mathbb{F}_5, \ldots, \mathbb{F}_{5^8}$. Counting them takes approximately five minutes when one uses the method described in [**4**, Algorithm 15].

5·4·4. Here, V_{Tate} is a $\mathbb{Q}_l$-vector space of dimension 14. Again, P_{expl} is generated by H. The characteristic polynomial of Frobenius on $V_{\mathrm{Tate}}/(P_{\mathrm{expl}} \otimes_{\mathbb{Z}} \mathbb{Q}_l)$ is

$$(t-1)(t^4+t^3+t^2+t+1)(t^8-t^7+t^5-t^4+t^3-t+1)\,,$$

which has only simple roots.

This shows that, for each of the dimensions 1, 2, 5, 6, 9, 10, 13, and 14, there is at most one $\mathrm{Gal}(\overline{\mathbb{F}}_5/\mathbb{F}_5)$-invariant subvector space in $\mathrm{Pic}(S_{\overline{\mathbb{F}}_5}) \otimes_{\mathbb{Z}} \mathbb{Q}$ containing the Chern class of H. Again, the existence of these subspaces would be assured by the Tate conjecture.

5·4·5. For the cases of low dimension, let us compute the square classes of the discriminants.

i) The one-dimensional invariant subspace has discriminant 2.

ii) For the two-dimensional invariant subspace, recall that we know six tritangent lines of the ramification locus. One of them, L_0, is defined over $\mathbb{F}_5$. Splitting $\pi^* L_0$ already yields a rank-two sublattice. For its discriminant, we find

$$\det \begin{pmatrix} -2 & 3 \\ 3 & -2 \end{pmatrix} = -5\,.$$

REMARK 5·4·6. Using the Artin-Tate conjecture, we may compute conditional values for the square classes of the discriminants for the 6- and 14-dimensional subspaces. Both are actually equal to (-1).

5·5. *The situation over* $\overline{\mathbb{Q}}$

Now we can put everything together and show that the $K3$ surfaces described in Example 5·1·1 indeed have geometric Picard rank 1.

5·5·1. *Proof of* 5·1·1. The vector space $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Q}$ injects as a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-invariant $\mathbb{Q}$-subvector space into $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})\otimes_{\mathbb{Z}}\mathbb{Q}$ for $p = 3$ and 5. The modulo 3 data show that this vector space has dimension $1, 2, 3$, or 4. The reduction modulo 5 allows the dimensions $1, 2, 5, 6, 9, 10, 13$, and 14. Consequently, $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is either 1 or 2.

To exclude the possibility of rank 2, we compare the discriminants. The reduction modulo 3 enforces discriminant (-489) while the reduction modulo 5 yields discriminant (-5). As these integers are not in the same square class, this is a contradiction. □

REFERENCES

[**1**] W. BARTH, C. PETERS, and A. VAN DE VEN. *Compact complex surfaces,* Ergebnisse der Mathematik und ihrer Grenzgebiete 4, Springer, Berlin 1984

[**2**] A. BEAUVILLE. *Surfaces algébriques complexes,* Astérisque 54, Société Mathématique de France, Paris 1978

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

[**4**] A.-S. ELSENHANS and J. JAHNEL. $K3$ surfaces of Picard rank one and degree two, in: *Algorithmic Number Theory* (ANTS 8) 212–225, Springer, Berlin 2008

[**5**] A.-S. ELSENHANS and J. JAHNEL. The discriminant of a cubic surface, *Preprint,* `http://arxiv.org/pdf/1006.0721v1`

[**6**] A.-S. ELSENHANS and J. JAHNEL. Cubic surfaces with a Galois invariant double-six, *Central European Journal of Mathematics* **8** (2010) 646–661

[**7**] A.-S. ELSENHANS and J. JAHNEL. Cubic surfaces with a Galois invariant pair of Steiner trihedra, to appear in: *International Journal of Number Theory*

[**8**] W. FULTON. *Intersection theory,* Springer, Berlin 1984

[**9**] R. KLOOSTERMAN. Elliptic $K3$ surfaces with geometric Mordell-Weil rank 15, *Canad. Math. Bull.* **50** (2007) 215–226

[**10**] D. I. LIEBERMAN. Numerical and homological equivalence of algebraic cycles on Hodge manifolds, *Amer. J. Math.* **90** (1968) 366–374

[**11**] Q. LIU, D. LORENZINI, and M. RAYNAUD. On the Brauer group of a surface, *Invent. Math.* **159** (2005) 673–676

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

[**13**] J. S. MILNE. *Étale Cohomology,* Princeton University Press, Princeton 1980

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

[**15**] M. POHST and H. ZASSENHAUS. *Algorithmic algebraic number theory,* Cambridge University Press, Cambridge 1989

[**16**] J. TATE. Conjectures on algebraic cycles in l-adic cohomology, in: *Motives,* Proc. Sympos. Pure Math. 55-1, Amer. Math. Soc., Providence 1994, 71–83