The Picard group of a $K3$ surface and its reduction modulo p

Andreas-Stephan Elsenhans and Jörg Jahnel

Abstract

We present a method to compute the geometric Picard rank of a $K3$ surface over $\mathbb{Q}$. Contrary to a widely held belief, we show it is possible to verify Picard rank 1 using reduction only at a single prime. Our method is based on deformation theory for invertible sheaves.

1 Introduction

1.1. —— For $K3$ surfaces, the Picard group is a highly interesting invariant. In general, it is isomorphic to $\mathbb{Z}^n$ for some $n = 1, \ldots, 20$. A generic $K3$ surface over $\mathbb{C}$ has Picard rank 1. Nevertheless, the first explicit examples of $K3$ surfaces over $\mathbb{Q}$ with geometric Picard rank 1 were constructed by R. van Luijk [vL] as late as 2004. Van Luijk's method is based on reduction modulo p. It works as follows.

1.2. Approach (van Luijk)**.** —— Let S be a $K3$ surface.

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) On its part, $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$ 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 Frobenius 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 is therefore an upper bound for the Picard rank of $S_{\overline{\mathbb{F}}_p}$. One may 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. For proving that the Picard rank over $\overline{\mathbb{Q}}$ is equal to 1, the best that could happen is to find a prime which yields an upper bound of 2.

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, $\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ and $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$, are in the same square class. Note here that reduction modulo p respects the intersection product.

v) To obtain a contradiction, one combines information from two primes. It may happen that one has a rank bound of 2 at both places but different square classes for the discriminant do arise. Then, these data are incompatible with Picard rank 2 over $\overline{\mathbb{Q}}$.

1.3. *The improvement.* — Approach 1.2 accepts the possibility that $\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) \subset \mathrm{Pic}(S_{\overline{\mathbb{F}}_p})$ might be a proper sublattice of full rank. If that occurred then one knows at least that the two discriminants differ by a perfect square. This is a standard observation from the theory of lattices.

We will show in this article that such provisions need not be made. From the technical point of view, our main result states that, at least for $p \neq 2$, the quotient $\mathrm{Pic}(S_{\overline{\mathbb{F}}_p})/\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}})$ is always torsion-free. This is true actually in much more generality than just for $K3$ surfaces. It follows in a rather straightforward manner from deformation theory, a tool developed by A. Grothendieck and M. Artin in the sixties of the last century. To be precise, our result is as follows.

1.4. Theorem. — *Let $p \neq 2$ be a prime number and X be a scheme proper and flat over $\mathbb{Z}$. Suppose that the special fiber X_p is non-singular and satisfies $H^1(X_p, \mathscr{O}_{X_p}) = 0$.*

Then, the specialization homomorphism $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \to \mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$ has a torsion-free cokernel.

1.5. Remarks. — a) Recall that, for a $K3$ surface S, one has $H^1(S, \mathscr{O}_S) = 0$ [BPV, Chap. VI, Table 10].

b) We will prove this theorem in 3.4. As an application, one may prove $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = 1$ for a $K3$ surface S using its reduction only at a single prime. This works as follows.

Approach. Let a $K3$ surface S be given.

i) For a prime $p \neq 2$ of good reduction, perform steps i), ii) and iii) as in 1.2. Thereby, the hope is to prove $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{F}}_p}) \leq 2$. Further, compute the discriminant giving two explicit generators. Alternatively, one might use the Artin-Tate formula.

ii) Assume $\mathrm{rk}\,\mathrm{Pic}(S_{\overline{\mathbb{Q}}}) = 2$. Then, according to Theorem 1.4, every invertible sheaf on $S_{\overline{\mathbb{F}}_p}$ lifts to $S_{\overline{\mathbb{Q}}}$. Use reduction theory of binary quadratic forms or explicit arguments to estimate the degree of a hypothetical effective divisor. Finally, use Gröbner bases to verify that such a divisor does not exist.

1.6. Example. — Consider the $K3$ surface S over $\mathbb{Q}$, given by

$$w^2 = x^5y + x^4y^2 + 2x^3y^3 + x^2y^4 + xy^5 + 4y^6 + 2x^5z + 2x^4z^2 + 4x^3z^3 + 2xz^5 + 4z^6\,.$$

Then, $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

Proof. For the reduction of S at the prime 5, one sees that the branch locus has a tritangent line given by $z - 2y = 0$. It meets the branch locus at $(1 : 0 : 0)$, $(1 : 3 : 1)$, and $(0 : 1 : 2)$.

The numbers of points over $\mathbb{F}_{5^d}$ are, in this order, 41, 751, 15 626, 392 251, 9 759 376, 244 134 376, 6 103 312 501, 152 589 156 251, 3 814 704 296 876, and 95 367 474 609 376. Thus, the traces of the Frobenius on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_5}, \overline{\mathbb{Q}}_l)$ are 15, 125, 0, 1 625, −6 250, −6 250, −203 125, 1 265 625, 7 031 250, and 42 968 750. Algorithm 23 of [EJ1] shows that the sign in the functional equation is positive. The characteristic polynomial of the Frobenius is therefore completely determined. For its decomposition into prime polynomials, we find (after scaling)

$$\begin{aligned}(t-5)^2(t^{20} &- 5\,t^{19} - 25\,t^{18} + 250\,t^{17} - 250\,t^{16} - 1\,875\,t^{15} + 12\,500\,t^{14} - 31\,250\,t^{13} \\ &- 156\,250\,t^{12} + 390\,625\,t^{11} + 5\,859\,375\,t^{10} + 9\,765\,625\,t^{9} - 97\,656\,250\,t^{8} \\ &- 488\,281\,250\,t^{7} + 4\,882\,812\,500\,t^{6} - 18\,310\,546\,875\,t^{5} - 61\,035\,156\,250\,t^{4} \\ &+ 1\,525\,878\,906\,250\,t^{3} - 3\,814\,697\,265\,625\,t^{2} - 19\,073\,486\,328\,125\,t \\ &+ 95\,367\,431\,640\,625)\,.\end{aligned}$$

This shows $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_5}) \leq 2$.

The splits of the pull-back of the tritangent line are explicit generators for $\operatorname{Pic}(S_{\overline{\mathbb{F}}_5})$. Such a split l, being a projective line, has self-intersection number $l^2 = -2$. Further, $lh = 1$ for h the pull-back of a line. If we had $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 2$ then the invertible sheaf $\mathscr{O}(l)$ would lift to $S_{\overline{\mathbb{Q}}}$. We had a divisor L on $S_{\overline{\mathbb{Q}}}$ such that $HL = 1$ and $L^2 = -2$. By [BPV, Ch. VIII, Proposition 3.6.i], such a divisor is automatically effective.

$HL = 1$ shows that L is obtained from a line on $\mathbf{P}^2$, the pull-back of which splits into two components. This is possible only for a tritangent line of the branch locus. [EJ1, Algorithm 8] shows, however, that such a tritangent line does not exist. □

2 The sequence of the Picard lattices

2.1. Remark. —— The proof of Theorem 1.4 relies on deformation-theoretic methods [Ar, Kl]. For $K3$ surfaces and prime-to-p torsion, one could have used étale cohomology which appears to be more natural.

In fact, to show $\operatorname{Pic}(X_{\overline{\mathbb{F}}_p})/\operatorname{Pic}(X_{\overline{\mathbb{Q}}})$ has no l-torsion, it is sufficient to consider $\operatorname{Pic}(X_{\overline{\mathbb{F}}_p})\otimes_{\mathbb{Z}}\mathbb{Z}_l/\operatorname{Pic}(X_{\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Z}_l$. But $\operatorname{Pic}(X_{\overline{\mathbb{F}}_p})\otimes_{\mathbb{Z}}\mathbb{Z}_l \subseteq H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_p}, \mathbb{Z}_l(1))$ which, by standard comparison theorems, is isomorphic to $H^2_{\text{sing}}(X(\mathbb{C}), \mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Z}_l$. On the other hand, $\operatorname{Pic}(X_{\overline{\mathbb{Q}}}) \cong \operatorname{Pic}(X_{\mathbb{C}})$. Finally, $H^2_{\text{sing}}(X(\mathbb{C}), \mathbb{Z})/\operatorname{Pic}(X_{\mathbb{C}})$ is torsion-free according to the Lefschetz $(1,1)$-theorem.

2.2. Notation. — Let X be a $\mathbb{Z}_p$-scheme. Then, we will write X_p for the special fiber and, more generally, $X_{p^n} := X \times_{\operatorname{Spec} \mathbb{Z}_p} \operatorname{Spec} \mathbb{Z}/p^n\mathbb{Z}$. Finally, let $\widehat{X}$ be the formal scheme obtained by completing X along (p).

2.3. Lemma. — *Let $p \neq 2$ be a prime number and X a $\mathbb{Z}_p$-scheme which is Noetherian,separated, and fulfills $H^1(X_p, \mathscr{O}_{X_p}) = 0$. Denote by $P \subseteq \operatorname{Pic}(X_p)$ the subset of all invertible sheaves allowing a lift as an invertible sheaf on $\widehat{X}$.*

Then, $\operatorname{Pic}(X_p)/P$ *is torsion-free.*

Proof. *First step.* Preliminaries.

Assume, to the contrary, that $\operatorname{Pic}(X_p)/P$ has torsion. Then, there are a prime number l and an invertible sheaf $\mathscr{L} \in \operatorname{Pic}(X_p) \backslash P$ such that $\mathscr{L}^{\otimes l} \in P$. This means that $\mathscr{L}^{\otimes l}$ lifts to $\widehat{X}$ but $\mathscr{L}$ does not. We have to show that this situation is impossible.

By [Ha, Proposition II.9.6], an invertible sheaf on $\widehat{X}$ is the same as an inverse system $(\mathscr{I}_n)_n$ of invertible sheaves $\mathscr{I}_n \in \operatorname{Pic}(X_{p^n})$ such that $\mathscr{I}_{n+1}|_{X_{p^n}} = \mathscr{I}_n$ for all n. By assumption, we have such a system for $\mathscr{I}_0 = \mathscr{L}^{\otimes l}$. It has to be shown that the invertible sheaf $\mathscr{L}$, too, lifts to X_{p^n} for all n.

Second step. Obstructions.

We will construct sheaves $\mathscr{L}_n \in \operatorname{Pic}(X_{p^n})$ lifting $\mathscr{L}$, inductively. These will satisfy, in addition, the relation $\mathscr{L}_n^{\otimes l} \cong \mathscr{I}_n$. First, we put $\mathscr{L}_0 := \mathscr{L}$.

For the induction step, consider the short exact sequence

$$0 \longrightarrow \mathscr{K} \longrightarrow \mathscr{O}^*_{X_{p^{n+1}}} \longrightarrow \mathscr{O}^*_{X_{p^n}} \longrightarrow 0\,.$$

Here, we have $\mathscr{O}_{X_p} \cong \mathscr{K}$ via the exponential map $x \mapsto 1 + p^n x \pmod{p^{n+1}}$. This yields the commutative diagram with exact rows,

$$\begin{array}{ccccccc} 0 \longrightarrow & \operatorname{Pic}(X_{p^{n+1}}) & \longrightarrow & \operatorname{Pic}(X_{p^n}) & \longrightarrow & H^2(X_p, \mathscr{O}_{X_p}) \\ & \Big\downarrow {\scriptstyle (.)^{\otimes l}} & & \Big\downarrow {\scriptstyle (.)^{\otimes l}} & & \Big\downarrow {\scriptstyle \cdot l} \\ 0 \longrightarrow & \operatorname{Pic}(X_{p^{n+1}}) & \longrightarrow & \operatorname{Pic}(X_{p^n}) & \longrightarrow & H^2(X_p, \mathscr{O}_{X_p})\,. \end{array}$$

The group $H^2(X_p, \mathscr{O}_{X_p})$ is p-torsion as the sheaf $\mathscr{O}_{X_p}$ is annihilated by p. In particular, it is uniquely l-divisible. Further, $\mathscr{I}_n \in \operatorname{Pic}(X_{p^n})$ is the image of $\mathscr{I}_{n+1} \in \operatorname{Pic}(X_{p^{n+1}})$ and $\mathscr{L}_n \in \operatorname{Pic}(X_{p^n})$. A standard diagram argument yields some invertible sheaf $\mathscr{L}_{n+1} \in \operatorname{Pic}(X_{p^{n+1}})$ which is mapped to $\mathscr{L}_n$ and $\mathscr{I}_{n+1}$. This completes the proof for $l \neq p$.

Third step. The case $l = p$.

Here, we first observe the congruence

$$(1 + p^n c)^p \equiv 1 + p^{n+1} c \pmod{p^{n+2}}$$

which, as $p > 2$, is valid for every $n \geq 1$. This has the striking consequence that, for $s \in \Gamma(U, \mathscr{O}^*_{X_{p^n}})$, the power s^p automatically defines a section of $\mathscr{O}^*_{X_{p^{n+1}}}$. Further, we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{O}_{X_p} & \longrightarrow & \mathscr{O}^*_{X_{p^{n+1}}} & \longrightarrow & \mathscr{O}^*_{X_{p^n}} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle (.)^p} & & \downarrow{\scriptstyle (.)^p} & & \\ 0 & \longrightarrow & \mathscr{O}_{X_p} & \longrightarrow & \mathscr{O}^*_{X_{p^{n+2}}} & \longrightarrow & \mathscr{O}^*_{X_{p^{n+1}}} & \longrightarrow & 0 \end{array}$$

with exact rows. Taking cohomology, this yields the commutative diagram with exact rows,

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Pic}(X_{p^{n+1}}) & \longrightarrow & \mathrm{Pic}(X_{p^n}) & \longrightarrow & H^2(X_p, \mathscr{O}_{X_p}) \\ & & \downarrow{\scriptstyle (.)^{\otimes p}} & & \downarrow{\scriptstyle (.)^{\otimes p}} & & \| \\ 0 & \longrightarrow & \mathrm{Pic}(X_{p^{n+2}}) & \longrightarrow & \mathrm{Pic}(X_{p^{n+1}}) & \longrightarrow & H^2(X_p, \mathscr{O}_{X_p})\,. \end{array}$$

We see, in particular, that the lift of an invertible sheaf, if possible, is unique up to isomorphism.

We will inductively construct a sequence of sheaves $\mathscr{L}_n \in \mathrm{Pic}(X_{p^n})$ lifting $\mathscr{L}$ such that $\mathscr{L}_n^{\otimes p} \cong \mathscr{I}_n$. To start, simply put $\mathscr{L}_0 := \mathscr{L}$. For the induction step, we observe that $\mathscr{L}_n^{\otimes p} \cong \mathscr{I}_n$ implies that $\mathscr{L}_n$ is mapped to $\mathscr{I}_{n+1}$ under the middle vertical arrow in the diagram. Indeed, the lifting of an invertible sheaf is unique. The same diagram argument as in the second step completes the proof. $\square$

2.4. Remark. —— For $p = 2$, the same argument shows that $\mathrm{Pic}(X_2)/P$ may only have 2-power torsion.

2.5. —— To illustrate the effect of the obstructions, suppose that $\mathrm{Pic}(X_p) = \mathbb{Z}^n$ and $H^2(X_p, \mathscr{O}_{X_p}) \cong \mathbb{F}_p$. Then, the lattices $\Lambda_i := \mathrm{Pic}(X_{p^i})$ form a system $\{\Lambda_i\}_{i\in\mathbb{N}}$ such that

$$\ldots \subseteq \Lambda_i \subseteq \ldots \subseteq \Lambda_2 \subseteq \Lambda_1\,,$$

$\Lambda_i \subseteq \Lambda_{i-1}$ is always of index 1 or p, and $\mathscr{L}^{\otimes p} \in \Lambda_i$ if and only if $\mathscr{L} \in \Lambda_{i-1}$.

According to Lemma 2.7 below, the system $\{\Lambda_i \otimes_\mathbb{Z} \mathbb{Z}_p\}_{i\in\mathbb{N}}$ is isomorphic to $\{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \oplus p^i\mathbb{Z}_p\}_{i\in\mathbb{N}}$. I.e., there is a linear functional

$$H\colon\ \mathrm{Pic}(X_p) = \mathbb{Z}^n \to \mathbb{Z}_p, \quad (x_1, \ldots, x_n) \mapsto a_1x_1 + \cdots + a_nx_n$$

with coefficients $a_1, \ldots, a_n \in \mathbb{Z}_p$ such that, for $\mathscr{L} \in \mathrm{Pic}(X_p)$ arbitrary, $p^i | H(\mathscr{L})$ if and only if $\mathscr{L}$ lifts to $\mathrm{Pic}(X_{p^i})$.

H somehow collects all the obstruction maps into a single homomorphism. Further, $H(\mathscr{L}) = 0$ if and only if $\mathscr{L} \in P$. This shows again that $\mathrm{Pic}(X_p)/P \hookrightarrow \mathbb{Z}_p$ is torsion-free.

2.6. Remark. —— This formulation also indicates that it is difficult to show $\operatorname{rk} P \leq \operatorname{rk} \operatorname{Pic}(X_p) - 2$. For this, one had to ensure that the $\mathbb{Z}$-rank of $\operatorname{im} H$ is at least 2. But this is impossible knowing only p-adic approximations of $a_1, \ldots, a_n$.

2.7. Lemma. —— *Let $\{\Lambda_i\}_{i \in \mathbb{N}}$ be a sequence of p-adic lattices such that*

i) $\Lambda_{i+1} \subset \Lambda_i$,

ii) $\Lambda_i / \Lambda_{i+1} = \mathbb{Z}/p\mathbb{Z}$,

iii) $x \in \Lambda_i \backslash \Lambda_{i+1} \Longrightarrow px \in \Lambda_{i+1} \backslash \Lambda_{i+2}$.

Then, there exists a basis $(b_1, \ldots, b_n)$ of Λ_1 such that $\Lambda_i = \langle b_1, \ldots, b_{n-1}, p^{i-1} b_n \rangle$.

Proof (cf. [We])**.** We first observe that $\Lambda_1/\Lambda_i \cong \mathbb{Z}/p^{i-1}\mathbb{Z}$. Indeed, the quotient Λ_1/Λ_i is precisely of order p^{i-1}. Further, for $x \in \Lambda_1 \backslash \Lambda_2$, we find $px \in \Lambda_2 \backslash \Lambda_3$ and, finally, $p^{i-2}x \in \Lambda_{i-1} \backslash \Lambda_i$. In particular, we see that Λ_0/Λ_i has an element of order p^{i-1}.

Let now i be fixed. By the elementary divisor theorem, there exists a basis $(b_1, \ldots, b_n)$ of Λ_0 such that $(p^{e_1} b_1, \ldots, p^{e_n} b_n)$ is a basis of Λ_i. As this yields $\Lambda_1/\Lambda_i \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$, we may conclude $e_1 = \cdots = e_{n-1} = 0$ and $e_n = i-1$. The only lattices between Λ_0 and Λ_i are $\langle b_1, \ldots, b_{n-1}, p^j b_n \rangle$ for $j = 1, \ldots, i-2$. Thus, we have shown the assertion for a finite chain of lattices.

To prove it for the infinite sequence, we observe that the space of all bases of Λ_1 is compact in the p-adic topology. For every $i \in \mathbb{N}$, there is a basis $B^{(i)} = (b_1^{(i)}, \ldots, b_n^{(i)})$ of Λ_1 having the desired property for the finite subsequence $\Lambda_1, \ldots, \Lambda_i$. Consider the limit $(b_1, \ldots, b_n)$ of a convergent subsequence of $\{B^{(i)}\}_{i \in \mathbb{N}}$.

We claim that $(b_1, \ldots, b_{n-1}, p^{i-1} b_n)$ is a basis for Λ_i. Indeed, $(b_1, \ldots, b_{n-1}, p^{i-1} b_n)$ is arbitrarily close to a basis which completes the proof. $\square$

3 The quotient $\operatorname{Pic}(X_{\overline{\mathbb{F}}_p}) / \operatorname{Pic}(X_{\overline{\mathbb{Q}}})$

3.1. Sublemma. —— *Let p be a prime number and X be a $\mathbb{Z}_p$-scheme which is proper and flat. Suppose that the generic fiber X_η is connected and the special fiber X_p is non-singular.*

Then, X_p is irreducible.

Proof. The function field $K := \Gamma(X_\eta, \mathscr{O}_{X_\eta})$ is a finite extension of $\mathbb{Q}_p$. Further, $O := \Gamma(X, \mathscr{O}_X)$ is a finite $\mathbb{Z}_p$-algebra being an integral domain with quotient field K. Clearly, O/pO is contained in $\Gamma(X_p, \mathscr{O}_{X_p})$. But, according to the assumption, the latter does not have nilpotent elements other than zero. Hence, p generates the maximal ideal of O. This means, $K/\mathbb{Q}_p$ is necessarily unramified and $O = \mathscr{O}_K$ is its ring of integers. Stein factorization provides us with a morphism $X \to \operatorname{Spec} \mathscr{O}_K$ with connected fibers. From this, we immediately see that X_p is connected. As X_p is non-singular, this is enough for irreducibility. $\square$

3.2. Lemma. —— *Let $p \neq 2$ be a prime number and X be a $\mathbb{Z}_p$-scheme which is proper and flat. Suppose that the special fiber X_p is non-singular and satisfies $H^1(X_p, \mathscr{O}_{X_p}) = 0$.*

Then, the specialization homomorphism $\mathrm{sp}\colon \mathrm{Pic}(X_\eta) \to \mathrm{Pic}(X_p)$ *from the generic fiber has a torsion-free cokernel.*

Proof. As each connected component may be treated separately, we assume without restriction that X is connected. Further, the assumption implies that X is non-singular. Hence, X is actually irreducible. This implies that X_η is irreducible, too. Finally, we conclude irreducibility of X_p from Sublemma 3.1.

There is a specialization map $\mathrm{Pic}(X_\eta) \to \mathrm{Pic}(X)$ given by taking the Zariski closure in X of a Weil divisor on X_η. This map is injective as the restriction forms a section to it. It is a surjection, too, as the only vertical divisors are principal, associated to the powers of (p).

Further, by A. Grothendieck's existence theorem [EGA III, Corollaire (5.1.6)], one has $\mathrm{Pic}(X) = \mathrm{Pic}(\widehat{X})$. The assertion now follows from Lemma 2.3. □

3.3. Corollary. —— *Let $p \neq 2$ be a prime number and X be a $\mathbb{Z}_p$-scheme which is proper and flat. Suppose that the special fiber X_p is non-singular and satisfies $H^1(X_p, \mathscr{O}_{X_p}) = 0$. Further, let $K/\mathbb{Q}_p$ be an unramified field extension and denote the residue field of K by k.*

Then, the cokernels of the specialization homomorphisms

i) $\mathrm{sp}_K\colon \mathrm{Pic}(X_K) \to \mathrm{Pic}(X_k)$,

ii) $\mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}\colon \mathrm{Pic}(X_{\mathbb{Q}_p^{\mathrm{nr}}}) \to \mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$, *and*

iii) $\mathrm{sp}_{\overline{\mathbb{Q}}_p}\colon \mathrm{Pic}(X_{\overline{\mathbb{Q}}_p}) \to \mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$

are torsion-free.

Proof. i) Apply Lemma 3.2 to the fiber product $X \times_{\mathrm{Spec}\,\mathbb{Z}_p} \mathrm{Spec}\,\mathscr{O}_K$.

ii) As the filtered direct limit functor is exact, the desired cokernel is the same as

$$\varinjlim \mathrm{coker}(\mathrm{sp}_K\colon \mathrm{Pic}(X_K) \to \mathrm{Pic}(X_k))$$

where K is running over the unramified extensions of $\mathbb{Q}_p$ and k denotes the residue field of K. As all the cokernels are torsion-free, the assertion follows.

iii) We claim that $\mathrm{sp}_{\overline{\mathbb{Q}}_p}$ has the same image in $\mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$ as $\mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}$. Let $\mathscr{L} \in \mathrm{Pic}(X_{\overline{\mathbb{Q}}_p})$. The Galois group $\Gamma := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}})$ sends $\mathscr{L}$ to a finite orbit $\{\mathscr{L}_1, \ldots, \mathscr{L}_m\}$. The specializations of $\mathscr{L}_1, \ldots, \mathscr{L}_m$ in $\mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$ are all the same. Therefore,

$$m \cdot \mathrm{sp}_{\overline{\mathbb{Q}}_p}(\mathscr{L}) = \mathrm{sp}_{\overline{\mathbb{Q}}_p}(\mathscr{L}^{\otimes m}) = \mathrm{sp}_{\overline{\mathbb{Q}}_p}(\mathscr{L}_1 \otimes \cdots \otimes \mathscr{L}_m) = \mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}(\mathscr{L}_1 \otimes \cdots \otimes \mathscr{L}_m)$$

since $\mathscr{L}_1 \otimes \cdots \otimes \mathscr{L}_m$ is Γ-invariant. Hence, $m \cdot \mathrm{sp}_{\overline{\mathbb{Q}}_p}(\mathscr{L}) \in \mathrm{im}\,\mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}$. As $\mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}$ has a torsion-free cokernel, we see that $\mathrm{sp}_{\overline{\mathbb{Q}}_p}(\mathscr{L}) \in \mathrm{im}\,\mathrm{sp}_{\mathbb{Q}_p^{\mathrm{nr}}}$, too. □

3.4. Theorem. —— *Let $p \neq 2$ be a prime number and X be a scheme proper and flat over $\mathbb{Z}$. Suppose that the special fiber X_p is non-singular and satisfies $H^1(X_p, \mathscr{O}_{X_p}) = 0$.*

Then, the specialization homomorphism $\mathrm{sp}_{\overline{\mathbb{Q}}}\colon \mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \to \mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$ has a torsion-free cokernel.

Proof. There is a canonical injection $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \hookrightarrow \mathrm{Pic}(X_{\overline{\mathbb{Q}}_p})$. We have to show that both Picard groups have the same image under specialization to $\mathrm{Pic}(X_{\overline{\mathbb{F}}_p})$.

For this, we switch at first to the scheme X_Z for $Z = \mathbb{Z}[\frac{1}{m}]$ where m is an integer divisible by all primes of bad reduction but not by p. Again, we may assume without restriction that X_Z is connected. Further, by construction, X_Z is non-singular and, therefore, irreducible. By virtue of Sublemma 3.1, all the special fibers of X_Z are irreducible.

According to a theorem of Grothendieck (cf. [Kl, Theorem 4.8]), the Picard scheme $\mathbf{Pic}_{X_Z/Z}$ exists in this situation as a scheme, locally of finite type over Z. This means, we are given a morphism $i\colon \operatorname{Spec}\overline{\mathbb{Q}}_p \to \mathbf{Pic}_{X_Z/Z}$ and have to show that there is a morphism $\operatorname{Spec}\overline{\mathbb{Q}} \to \mathbf{Pic}_{X_Z/Z}$ such that the specializations modulo p are the same.

Locally, near the image of i, we have an affine open subset $U \cong \operatorname{Spec} R \subseteq \mathbf{Pic}_{X_Z/Z}$ for R a finitely generated Z-algebra. We are thus given a ring homomorphism $\iota\colon R \to \overline{\mathbb{Q}}_p$. This actually maps R to $\mathscr{O}_K$ for a suitable finite extension $K/\mathbb{Q}_p$. Unfortunately, as a Z-algebra, $\mathscr{O}_K$ is not finitely generated. On the other hand, $\operatorname{im}\iota =: S \subset \mathscr{O}_K$ is clearly a finitely generated Z-algebra. We fix a set of generators $\{T_1, \ldots, T_n\}$ of S.

Preserving the induced homomorphism to $\mathbb{F}_q := \mathscr{O}_K/\mathfrak{m}_K$, our goal is to replace ι by a homomorphism to another subring $S' \subset \mathscr{O}_K$ such that S is finite as a Z-module. For this, we will construct an algebra homomorphism $\varphi\colon S \to S'$ such that $\nu(x - \varphi(x)) \geq 1$ for every $x \in S$. Here, ν denotes the discrete valuation on $\mathscr{O}_K$.

To perform this construction, we apply Noether normalization [ZS, Ch. V, §4, Theorem 8] to $S \otimes_\mathbb{Z} \mathbb{Q}$. This states that $S \otimes_\mathbb{Z} \mathbb{Q}$ is an integral extension of a polynomial ring $\mathbb{Q}[X_1, \ldots, X_k] \subseteq S \otimes_\mathbb{Z} \mathbb{Q}$. We send $X_1, \ldots, X_k$ to elements of $\mathscr{O}_K$ algebraic over $\mathbb{Q}$ such that $\nu(X_i - \varphi(X_i)) \gg 0$. Then, this extends to a homomorphism of the whole of $S \otimes_\mathbb{Z} \mathbb{Q}$. We claim that $\nu(T_i - \varphi(T_i)) \geq 1$ for $i = 1, \ldots, n$. Indeed, as T_i is integral over $\mathbb{Q}[X_1, \ldots, X_k, T_1, \ldots, T_{i-1}]$, this follows from an iterated application of Hensel's lemma in the form of [Na, Proposition 5.5].

Since S is generated by $T_1, \ldots, T_n$ as a Z-algebra and $\nu(z) \geq 0$ for every $z \in Z$, we see that $\nu(x - \varphi(x)) \geq 1$ for every $x \in S$. This completes the proof. $\square$

4 An explicit obstruction

4.1. Proposition. — *Let S be a $K3$ surface of degree 2 over $\mathbb{Q}$, given explicitly by*

$$w^2 = f_6(x, y, z)$$

for $f_6 \in \mathbb{Z}[x, y, z]$ of degree 6. Suppose, for a prime $p \neq 2$, there is an $\mathbb{F}_p$-rational tritangent line "$\ell = 0$" of the ramification locus of S_p. Write l for a split of the pull-back of the tritangent.

One has $f_6 \equiv f_3^2 + \ell f_5 \pmod p$ for homogeneous forms $f_3, f_5 \in \mathbb{Z}[x, y, z]$. Put

$$G(x, y, z) := (f_6 - f_3^2 - \ell f_5)/p\,.$$

Then, the obstruction to lifting $\mathscr{O}(l)$ to S_{p^2} is $((-G) \bmod (p, \ell, f_3, f_5))$.

Proof. *First step.* An affine open covering of S_p.

On S_p, we have $w^2 = f_3^2 + \ell f_5$ and, for h a quadric, $w^2 = (f_3 + \ell h)^2 + \ell f_5'$ where $f_5' := f_5 - 2f_3 h - \ell h^2$. On "$\ell = 0$", f_3 and f_5 have no common zero as this would cause a singularity on S_p. Hence, for a suitably chosen h, the three forms ℓ, f_5, and f_5' do not have a common zero. For this, it may be necessary to extend the ground field. The sets "$\ell \neq 0$", "$f_5 \neq 0$", and "$f_5' \neq 0$", form an affine open covering of S_p. We may extend them in the obvious manner to an affine open covering of S.

Second step. The invertible sheaf $\mathscr{O}(5l)$.

We start with $\mathscr{O}(5l)$ instead of $\mathscr{O}(l)$ as this will turn out to be easier. $\mathscr{O}(5l)$ is given by the rational functions 1 on "$\ell \neq 0$", $\frac{f_5^3}{(w+f_3)^5}$ on "$f_5 \neq 0$", and $\frac{f_5'^3}{(w+f_3+\ell h)^5}$ on "$f_5' \neq 0$". Thus, the transition functions are

$$\frac{f_5^3}{(w+f_3)^5} = \frac{(w-f_3)^5}{\ell^5 f_5^2}\,, \qquad \frac{(w+f_3)^5 f_5'^3}{(w+f_3+\ell h)^5 f_5^3} = \frac{(w+f_3)^5 (w-f_3-\ell h)^5}{\ell^5 f_5^3 f_5'^2}\,,$$

$$\text{and} \quad \frac{(w+f_3+\ell h)^5}{f_5'^3}\,.$$

Third step. The obstruction.

We may lift the first and third transition functions naively. The middle one is a transition function between "$f_5 \neq 0$" and "$f_5' \neq 0$" and, thus, must not have a pole at "$\ell \neq 0$". We lift $(w + f_3)(w - f_3)$ as ℓf_5 and obtain, in total,

$$\frac{[f_5 - h(w+f_3)]^5}{f_5^3 f_5'^2}\,.$$

The product of the three lifts is

$$\frac{(w-f_3)^5 [f_5 - h(w+f_3)]^5 (w+f_3+\ell h)^5}{\ell^5 f_5^5 f_5'^5}\,.$$

Observe that, in the form described, the transition functions may be lifted even to the affine open subsets of S, not just to S_{p^2}. Hence, the exponential of the obstruction for $\mathscr{O}(l)$ is $\frac{(w-f_3)[f_5-h(w+f_3)](w+f_3+\ell h)}{\ell f_5 f_5'}$, also in the case that $p = 5$.

Evaluating this expression, making use of the identity $w^2 - f_3^2 = \ell f_5 + pG$, we end up with $1 + p\,\frac{G(f_5-hw-hf_3-\ell h^2)}{\ell f_5 f_5'}$. Therefore, the obstruction to lifting $\mathscr{O}(l)$ is given by the Čech cocycle

$$\frac{G(f_5 - hw - hf_3 - \ell h^2)}{\ell f_5 f_5'}\,.$$

Fourth step. Simplification.

Any rational function having poles in only two of the three divisors considered is a Čech coboundary. Without changing the cohomology class, we may therefore add to the numerator forms being homogeneous of degree 11 and belonging to the ideal (ℓ, f_5, f_5').

On the line "$\ell = 0$", f_5 and f_5' have no zeroes in common. Thus, they are coprime in the graded ring $\mathbb{F}_p[x,y,z]/(\ell)$. Consequently, f_5 and f_5' already generate the full 10-dimensional space of forms of degree 9. Even more, they must generate the space of forms of degree 11. This shows that we may simplify the Čech cocycle to $\frac{-Ghw}{\ell f_5 f_5'}$.

Hence, the obstruction to lifting $\mathscr{O}(l)$ is $((-Gh) \mod (p, \ell, f_5, f_5'))$. The ideal is the same as (p, ℓ, hf_3, f_5). Thus, the question is whether $((-Gh) \mod (p, \ell))$ is a combination of hf_3 and f_5. As, on the line "$\ell = 0$" on S_p, h and f_5 have no common zeroes, they are coprime. $((-Gh) \mod (p, \ell))$ must be a combination of hf_3 and hf_5. We may, as well, consider $((-G) \mod (p, \ell, f_3, f_5))$. □

4.2. Example. — Let S be a $K3$ surface over $\mathbb{Q}$ given by $w^2 = f_6(x,y,z)$. Suppose

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

Assume further that the coefficient of y^2z^4 is not divisible by 9.

Then, $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 1$.

Proof. A direct calculation shows that, modulo 3, the right hand side is $f_3^2 + xf_5$ for $f_3 = 2x^3 + 2x^2z + xz^2 + 2y^3$ and $f_5 = 2x^3y^2 + x^2z^3 + 2xy^4 + 2z^5$. Thus, the branch locus of S_3 has a tritangent line given by $x = 0$.

The numbers of points over $\mathbb{F}_{3^d}$ are, in this order, 19, 127, 676, 6 751, 58 564, 532 414, 4 791 232, 43 038 703, 387 383 311, and 3 486 675 052. For the decomposition of the characteristic polynomial of the Frobenius, we find

$$(t-3)^2(t^{20} - 3\,t^{19} - 9\,t^{18} + 72\,t^{17} - 8\,1t^{16} - 324\,t^{15} + 1\,458\,t^{14} - 2\,916\,t^{13} + 4\,374\,t^{12} + 26\,244\,t^{11} - 137\,781\,t^{10} + 236\,196\,t^9 + 354\,294\,t^8 - 2\,125\,764\,t^7 + 9\,565\,938\,t^6 - 19\,131\,876\,t^5 - 43\,046\,721\,t^4 + 344\,373\,768\,t^3 - 387\,420\,489\,t^2 - 1\,162\,261\,467\,t + 348\,6784\,401)\,.$$

This shows $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}_3}}) \leq 2$.

Let l be a split of the pull-back of the tritangent line. We have to show that the obstruction to lifting $\mathscr{O}(l)$ is non-zero. For this, we observe that x, f_3, and f_5 do not generate the monomial y^2z^4. However, G contains this monomial by its very definition. □

4.3. Example. —— Consider the $K3$ surface S over $\mathbb{Q}$, given by $w^2 = f_6(x,y,z)$ for

$$\begin{aligned} f_6(x,y,z) = {} & 4x^6 + 2x^5y + 12x^5z + 2x^4y^2 + 4x^4yz + 12x^4z^2 + 24x^3y^3 - 57x^3y^2z \\ & - 9x^3yz^2 + 6x^3z^3 + 8x^2y^4 - 5x^2y^3z - 72x^2y^2z^2 + 7x^2yz^3 + 4x^2z^4 \\ & + 20xy^4z - 52xy^3z^2 - 57xy^2z^3 + 7xyz^4 + 4y^5z - 7y^4z^2 - 18y^3z^3 \\ & + 7y^2z^4 + 12yz^5 + 2z^6 \,. \end{aligned}$$

Then, $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = 3$.

Proof. We have

$$\begin{aligned} f_6 = {} & (2x^3 + 2x^2z + 2y^2z + yz^2 + z^3)^2 \\ & + (2x^2 + 2xz + yz + z^2)(x^3y + 2x^3z + x^2y^2 + x^2yz + 2x^2z^2 + 12xy^3 \\ & - 34xy^2z - 9xyz^2 - 2xz^3 + 4y^4 - 15y^3z - 7y^2z^2 + 9yz^3 + z^4) \end{aligned}$$

and

$$\begin{aligned} f_6 = {} & 4(x^3 + 2x^2y + 2x^2z + xy^2 + xyz + xz^2 + y^2z + yz^2 + z^3)^2 \\ & - (x^2 + xz + yz + z^2)(14x^3y + 4x^3z + 22x^2y^2 + 22x^2yz + 8x^2z^2 - 8xy^3 \\ & + 61xy^2z + 9xyz^2 + 6xz^3 - 4y^4 + 15y^3z + 11y^2z^2 - 6yz^3 + 2z^4) \,. \end{aligned}$$

Hence, there are two conics C_1 and C_2 each of which is six times tangent to the ramification locus of S. The splits of their pull-backs yield the intersection matrix

$$\begin{pmatrix} -2 & 6 & 1 & 3 \\ 6 & -2 & 3 & 1 \\ 1 & 3 & -2 & 6 \\ 3 & 1 & 6 & -2 \end{pmatrix}$$

which is of rank 3. Hence, $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \geq 3$.

On the other hand, S has good reduction at the prime $p = 3$. Point counting over extensions of $\mathbb{F}_3$ shows that the characteristic polynomial of the Frobenius operating on S_3 is

$$\begin{aligned} (t-3)^4(t^{18} & + 3\,t^{17} + 6\,t^{16} + 18\,t^{15} + 108\,t^{14} + 405\,t^{13} + 972\,t^{12} + 2\,187\,t^{11} \\ & + 13\,122\,t^{10} + 52\,488\,t^9 + 118\,098\,t^8 + 177\,147\,t^7 + 708\,588\,t^6 + 2\,657\,205\,t^5 \\ & + 6\,377\,292\,t^4 + 9\,565\,938\,t^3 + 28\,697\,814\,t^2 + 129\,140\,163\,t + 387\,420\,489) \,. \end{aligned}$$

Consequently, we have $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_3}) \leq 4$.

In particular, the assumption $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) > 3$ implies $\operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{Q}}}) = \operatorname{rk}\operatorname{Pic}(S_{\overline{\mathbb{F}}_3})$. Theorem 3.4 guarantees that the specialization map $\mathrm{sp}_{\overline{\mathbb{Q}}}\colon \operatorname{Pic}(S_{\overline{\mathbb{Q}}}) \to \operatorname{Pic}(S_{\overline{\mathbb{F}}_3})$ must be bijective. Giving one line bundle $\mathscr{L} \in \operatorname{Pic}(S_{\overline{\mathbb{F}}_3})$ with a non-trivial obstruction will be enough to yield a contradiction.

For this, observe that the ramification locus of S_3 has a tritangent line given by $x + y + z = 0$. Indeed,

$$f_6(x,y,z) \equiv (x^3 + x^2y + xy^2 + y^3)^2 + (x+y+z)(2x^3y^2 + x^3yz + 2x^2yz^2 + 2xy^4 + xy^3z + xy^2z^2 + 2xyz^3 + xz^4 + 2y^5 + 2y^4z + yz^4 + 2z^5) \pmod 3 .$$

Modulo the ideal $(3, x + y + z)$, we have $f_3 \equiv x^3 + x^2y + xy^2 + y^3$, $f_5 \equiv -(x^5 + x^3y^2 + x^2y^3 + xy^4 + y^5)$, and $G \equiv x^6 + 2x^5y + x^4y^2 + 2xy^5 + y^6$. Trying to generate G by 3, $x+y+z$, f_3, and f_5 now leads to linear system of seven equations in six unknowns which is easily seen to be unsolvable. □

References

[Ar] Artin, M.: Algebraization of formal moduli I, in: Global Analysis, Papers in Honor of K. Kodaira, *Univ. Tokyo Press,* Tokyo 1969, 21–71

[BPV] Barth, W., Peters, C., and Van de Ven, A.: Compact complex surfaces, Ergebnisse der Mathematik und ihrer Grenzgebiete 4, *Springer,* Berlin 1984

[EJ1] Elsenhans, A.-S. and Jahnel J.: $K3$ surfaces of Picard rank one and degree two, in: Algorithmic Number Theory (ANTS 8), *Springer,* Berlin 2008, 212–225

[EJ2] Elsenhans, A.-S. and Jahnel J.: K3 surfaces of Picard rank one which are double covers of the projective plane, in: The Higher-dimensional geometry over finite fields, *IOS Press,* Amsterdam 2008, 63–77

[EJ3] Elsenhans, A.-S. and Jahnel J.: On the computation of the Picard group for K3 surfaces, *Preprint*

[EJ4] Elsenhans, A.-S. and Jahnel J.: On Weil polynomials of K3 surfaces, *Preprint*

[EGA III] Grothendieck, A. and Dieudonné, J.: Étude cohomologique des faisceaux cohérents (EGA III), *Publ. Math. IHES* **11** (1961),**17** (1963)

[FGA 232] Grothendieck, A.: Technique de descente et théorèmes d'existence en géométrie algébrique, V. Les schémas de Picard: théorèmes d'existence, *Séminaire Bourbaki* **7**, Exp. **232** (1961-62), 143–161

[FGA 236] Grothendieck, A.: Technique de descente et théorèmes d'existence en géométrie algébrique, VI. Les schémas de Picard: propriétés générales, *Séminaire Bourbaki* **7**, Exp. **236** (1961-62), 221–243

[Ha] Hartshorne, R.: Algebraic Geometry, Graduate Texts in Mathematics 52, *Springer,* New York 1977

[Kl] Kleiman, Steven L.: The Picard scheme, in: Fundamental algebraic geometry, Math. Surveys Monogr. 123, *AMS,* Providence 2005, 235–321

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

[Na] Narkiewicz, W.: Elementary and analytic theory of algebraic numbers, Monografie Matematyczne 57, *PWN—Polish Scientific Publishers,* Warsaw 1974

[We] Werner, A.: Compactification of the Bruhat-Tits building of PGL by lattices of smaller rank, *Documenta Math.* **6** (2001), 315–342

[ZS] Zariski, O. and Samuel, P.: Commutative algebra, Vol. I., *Van Nostrand,* Princeton 1958